



Rapport de projet :

**Mise en place d'une architecture
réalisant par la segmentation d'un
réseau : VLAN PfSense**

Réaliser par :

ADJIMON Olawole Gérard

Technicien réseau et système

E-mail : adjigerard1@gmail.com

Tel : +228 69172383

02 Novembre 2024

PLAN :

INTRODUCTIONS :

- I- PREREQUIS**
- II- ARCHITECTURE**
- III- DEPLOIEMENT**
- IV- TEST ET VALIDATION**
- V- CONCLUSION**

Introductions

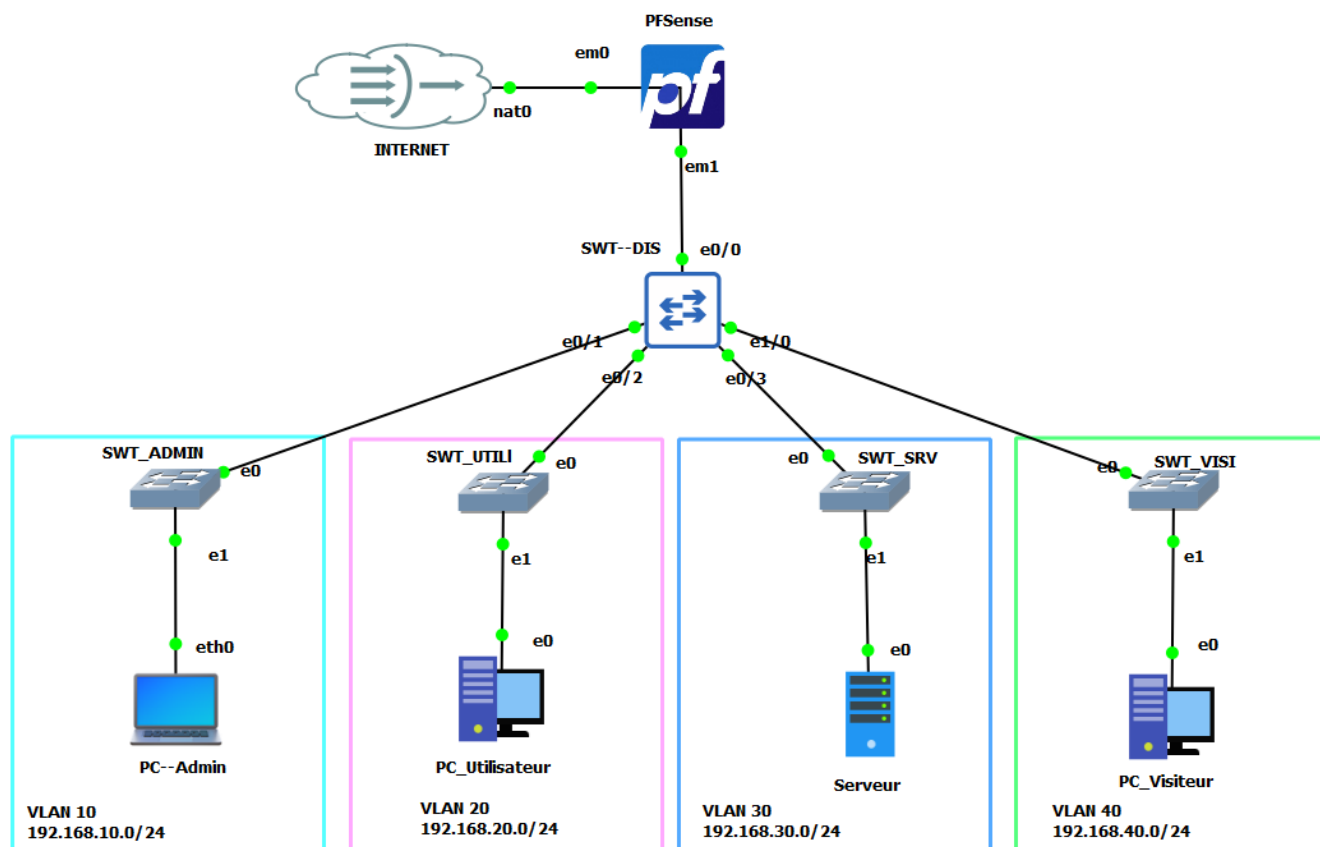
Avec l'évolution des besoins en matière de sécurité, de gestion et de performance des réseaux, la segmentation devient une composante essentielle pour les infrastructures informatiques modernes. Ce projet vise à mettre en place une architecture de réseau segmentée en utilisant des VLANs (Virtual Local Area Networks) gérés par le pare-feu PfSense. L'objectif est de structurer le réseau de manière sécurisée, en séparant les différents groupes d'utilisateurs et services pour optimiser la sécurité, réduire les risques de propagation d'attaques et améliorer la gestion du trafic réseau.

I - Prérequis

Pour la mise en place de notre architecture réseau sous GNS3, nous aurons besoin de ces différents prérequis, à savoir :

- ✓ GNS3 VM et GNS3 Client
- ✓ VMware Workstation
- ✓ PfSense
- ✓ VPCS (Virtual PC Simulator) ou Clients Simulés
- ✓ Image de Commutateur L2/L3

II - Architecture



Cette architecture représente notre réseau informatique où différents équipements sont connectés et interagissent les uns avec les autres. Voici une description détaillée :

1. PfSense

Interfaces

Em0 : Connecter a L'internet via DHCP

Em1 : Connecter au réseau local

Rôle : PfSense fonctionne ici comme un routeur pare-feu assurant la sécurité du Réseau. Il filtre le trafic entre le réseau interne et le routeur HQ.

2. SWT__DIS (Switch L2)

Port :

Eth0/0 : connecter à l'interface em1 du PfSense

Eth0/1 : Connecter au switch du Vlan 10 (Administrations)

Eth0/2 : Connecter au switch du Vlan 20 (Utilisateurs)

Eth0/3 : Connecter au switch du Vlan 30 (Serveurs)

Eth1/0 : Connecter au switch du Vlan 40 (Visiteurs)

Rôle : Le SWT_DIS relie les switches de chaque Vlan et assure leur communication

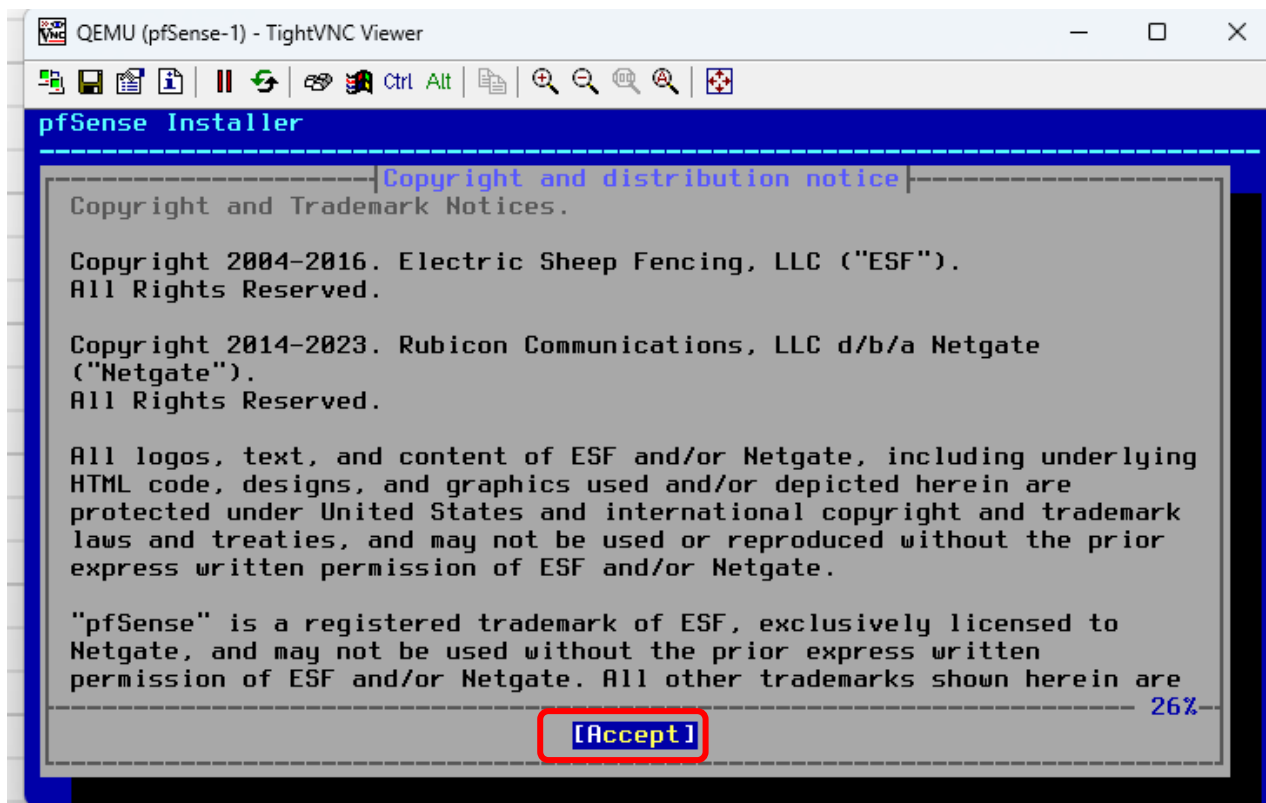
3. Equipement connecter

PC : sont des VPCS dans GNS3 pour simuler des clients de chaque VLAN. Cela permet de tester la connectivité, les adresses IP, et les règles d'accès.

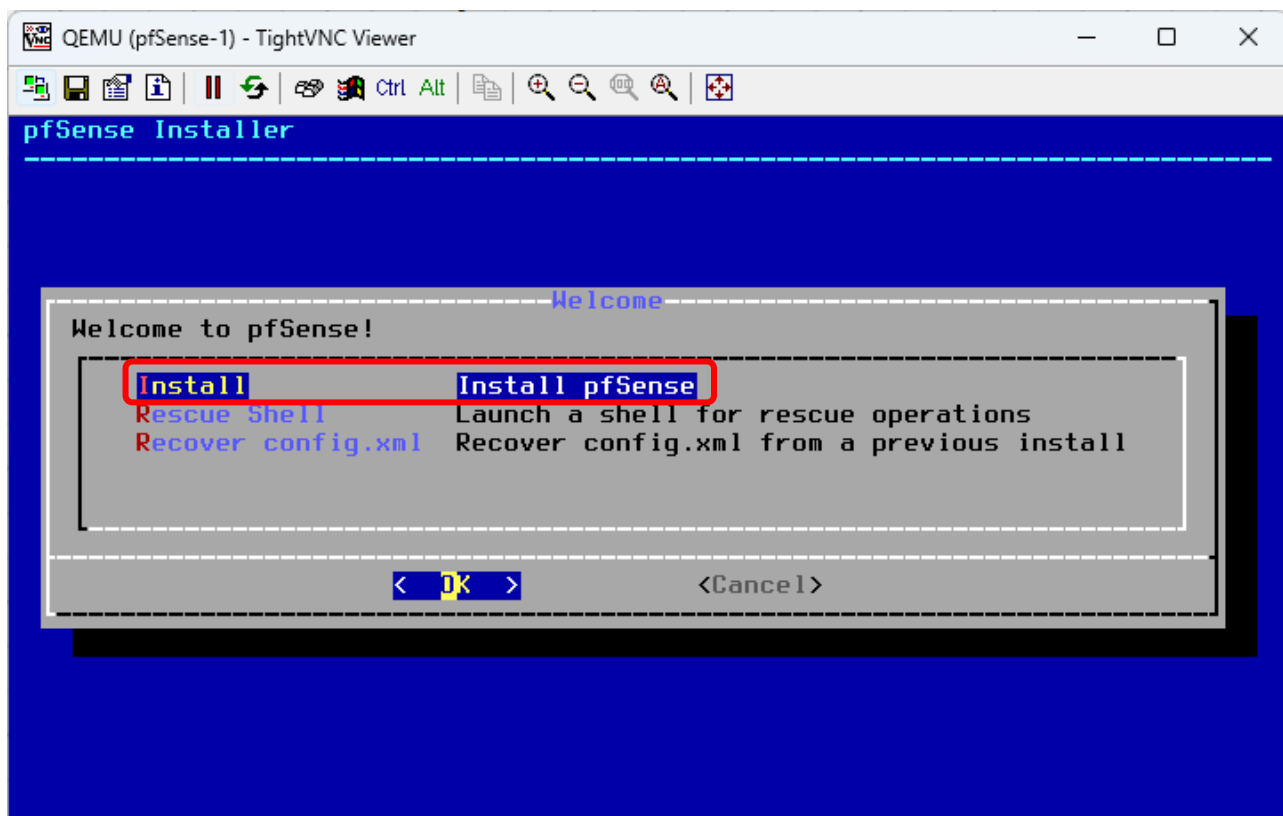
III – Déploiements

Tout d'abord, la première chose à faire c'est de mettre en place l'architecture réseau. Et pour ce faire, nous avons opter d'utiliser GNS3 comme plateforme de simulation. Et la mise place de tous ces périphériques sur GNS3 nécessite un processus, ce qui n'est pas détaillé sur ce rapport. Toute fois, la mise là de ces périphériques est disponible sur documentation du site officiel de GNS3.

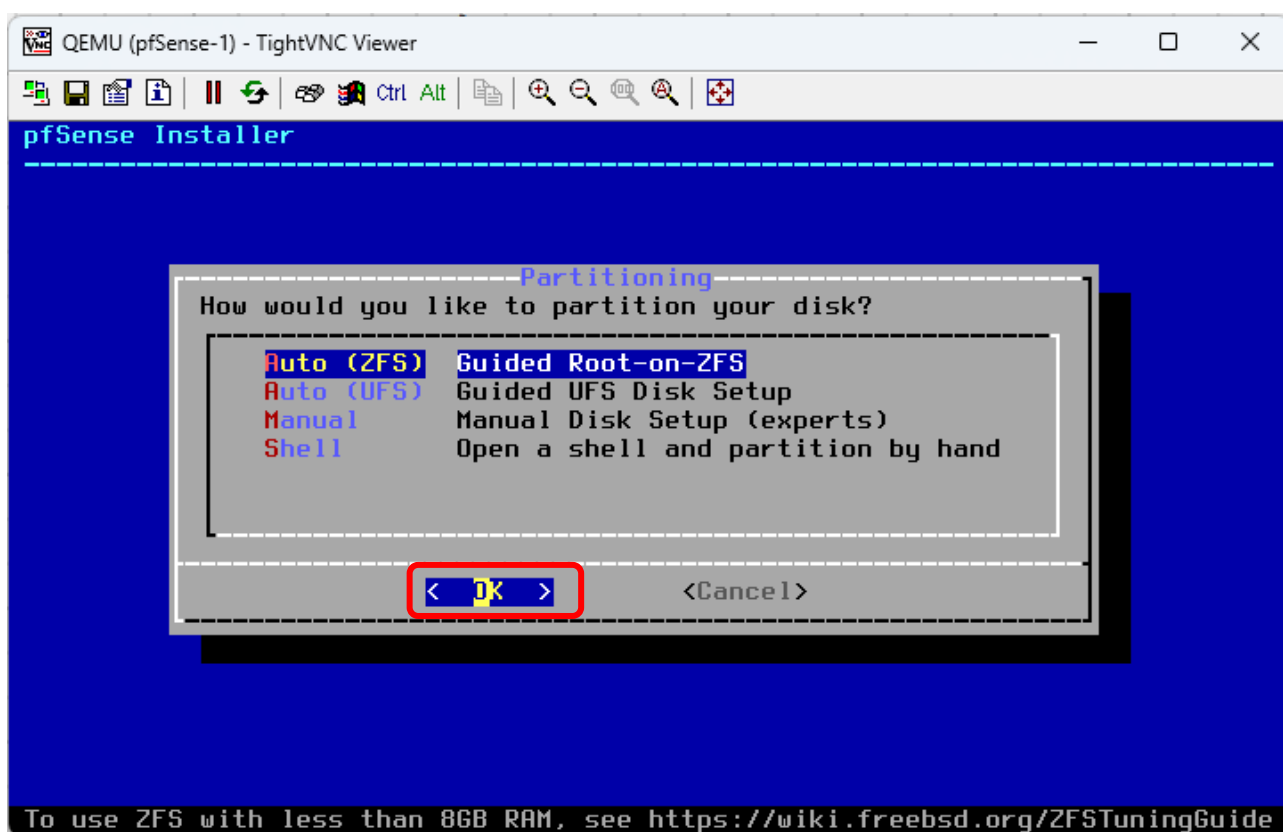
3.1. Installations de PfSense



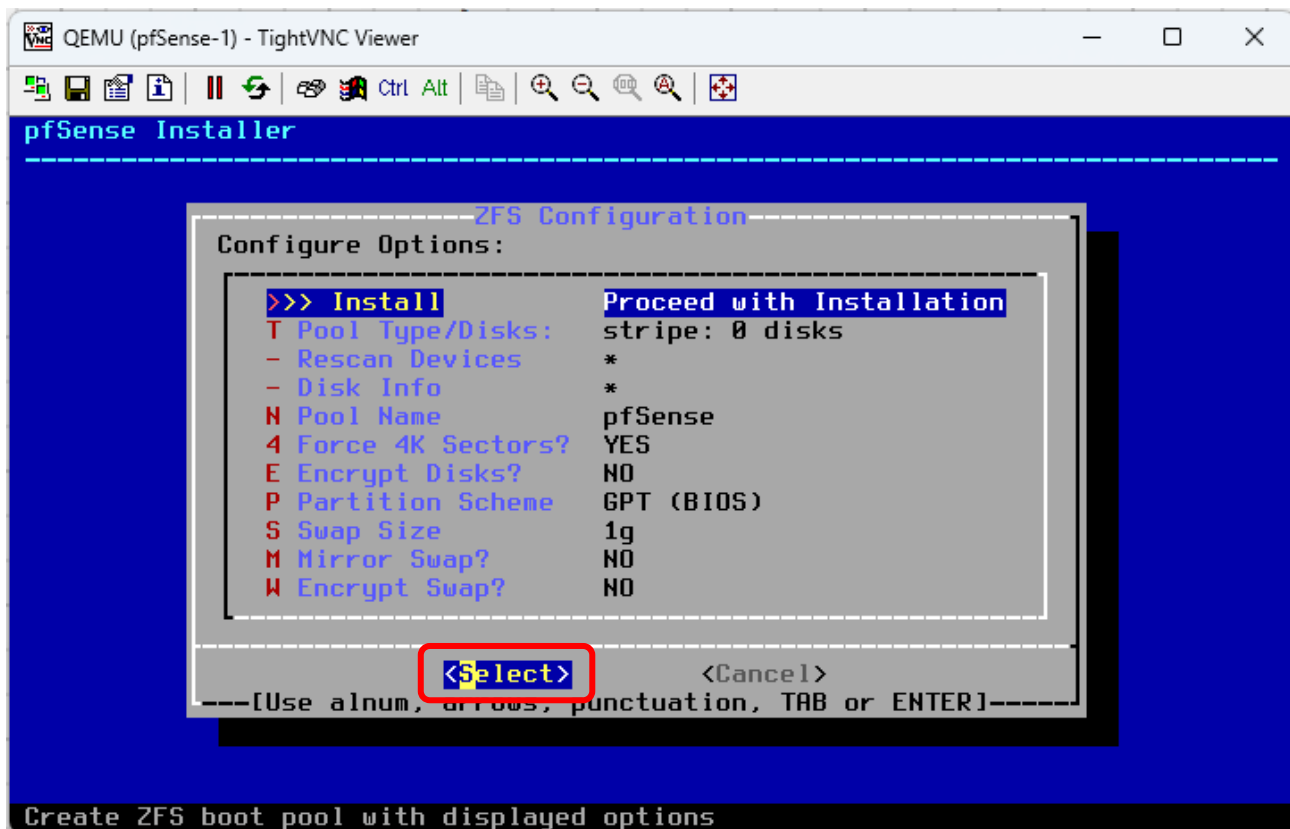
Accepter les afin d'installer PfSense



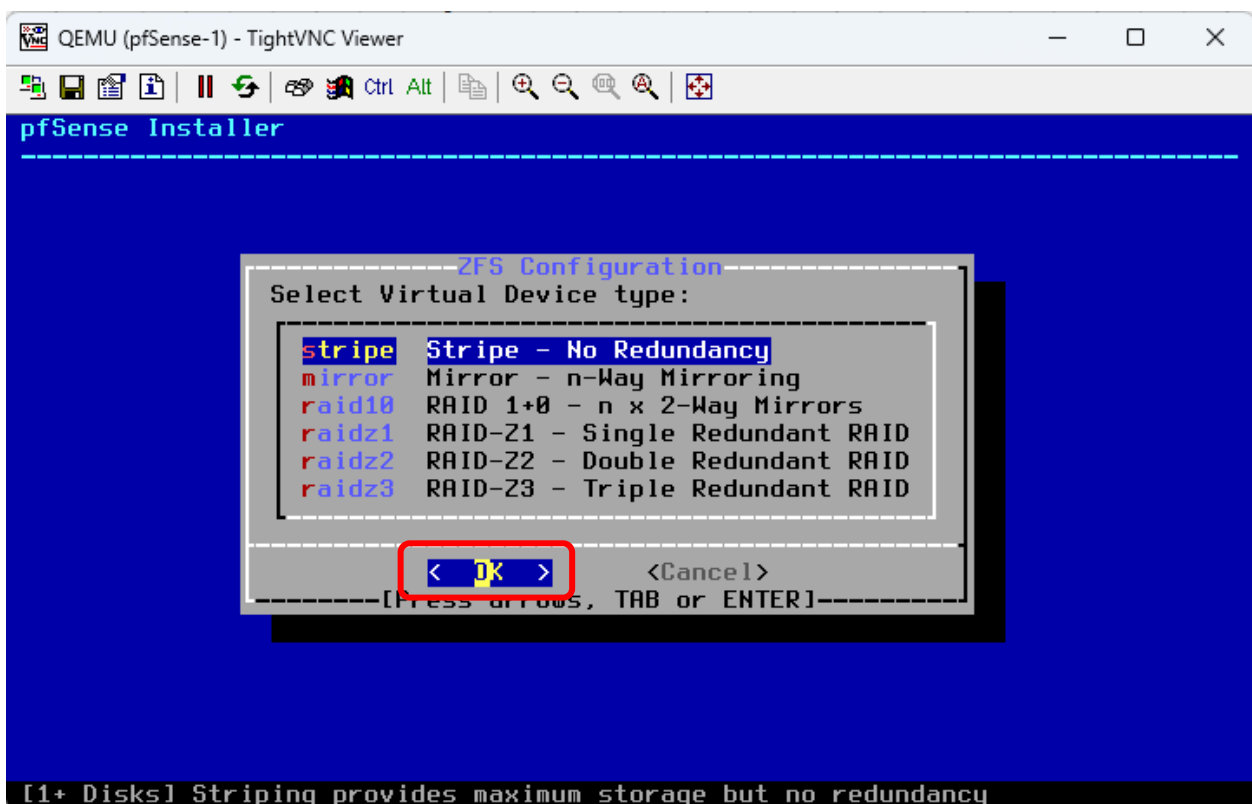
Sélectionne <<Install PfSense>>



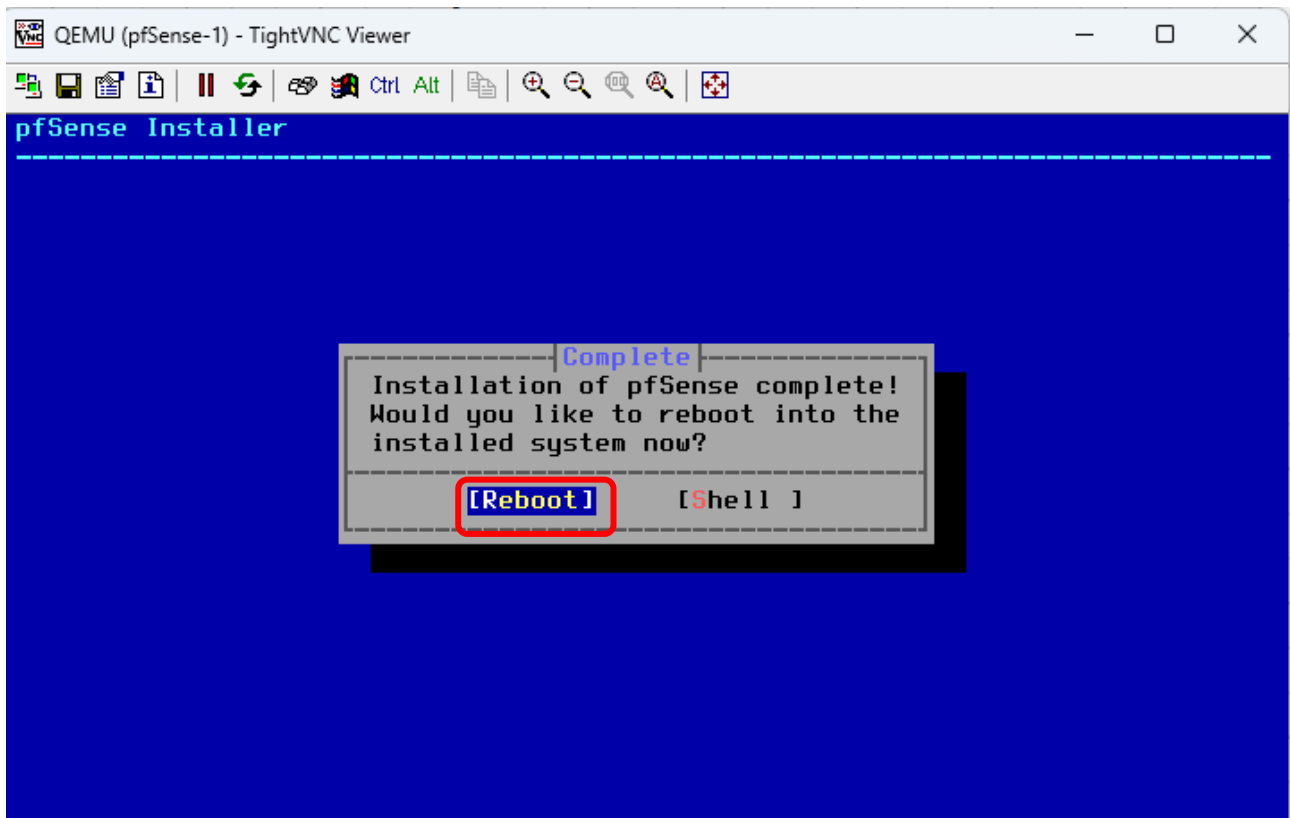
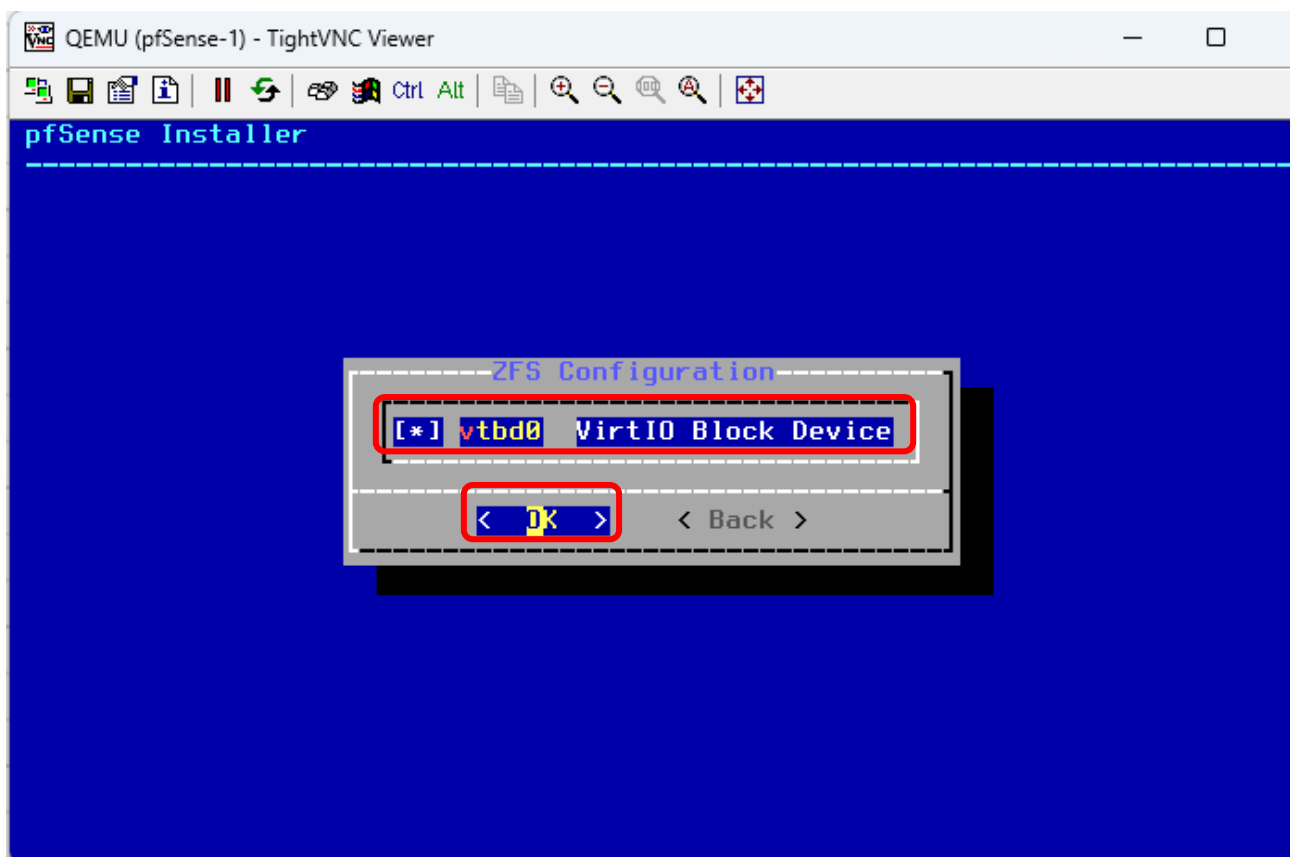
Sélectionne <<OK>> pour installer le PfSense sur le disque



Sélectionne << **Install** >> et << **OK** >> et appui sur la touche Entre du claviers pour valider la configuration



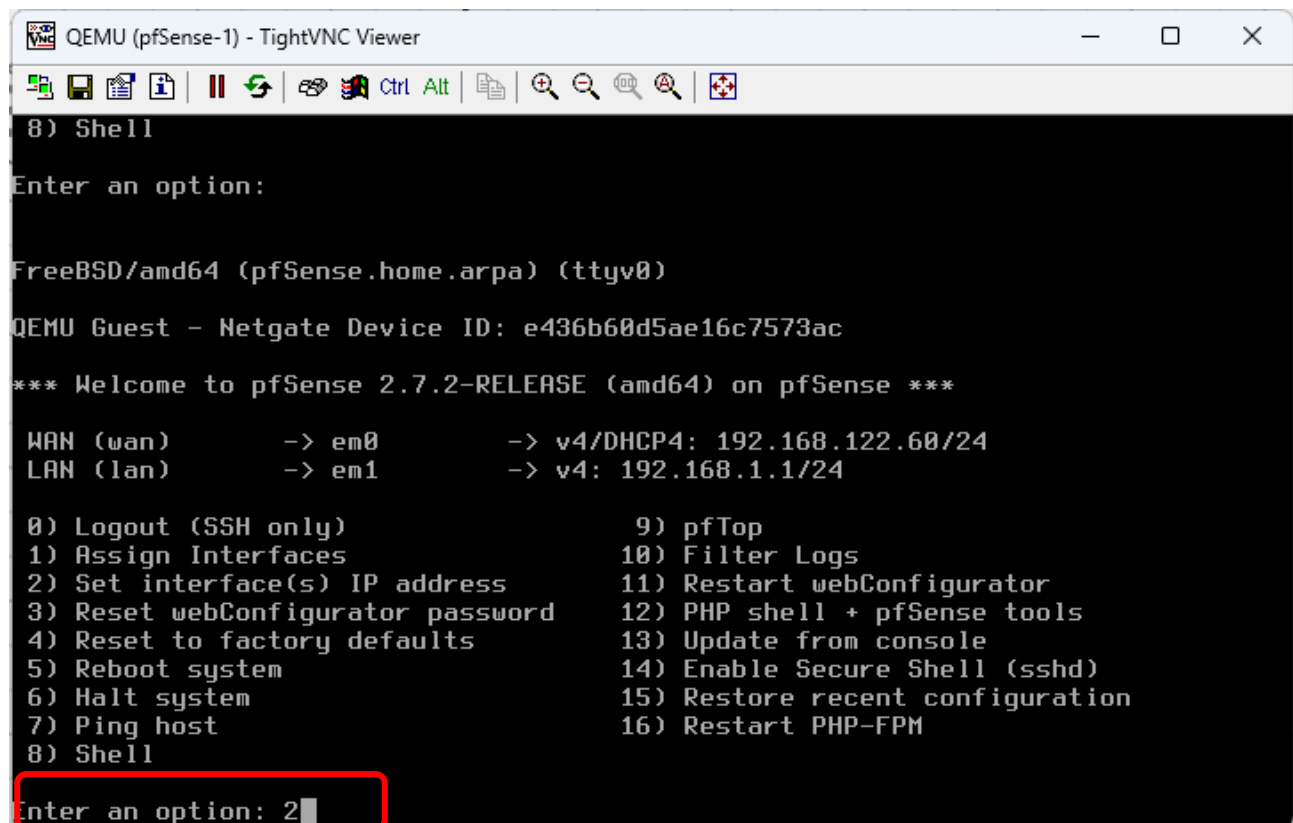
Utiliser la touche espace du clavier pour sélectionner le disque VTBD0 et valider par OK pour continuer l'installations



Sélectionner <<**Reboot**>> pour redémarrer le système

3.2. Configurations du PfSense

Une fois redémarrer, nous avons l'interface de PfSense qui est afficher.



```
QEMU (pfSense-1) - TightVNC Viewer
8) Shell
Enter an option:

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
QEMU Guest - Netgate Device ID: e436b60d5ae16c7573ac
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.122.60/24
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
```

Nous devons changer l'adresses de l'interface « Lan », pour cela sélectionner « 2 »

```
QEMU (pfSense-1) - TightVNC Viewer
QEMU Guest - Netgate Device ID: e436b60d5ae16c7573ac
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.122.60/24
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
```

On sélectionne l'interface « **Lan** », qui est le choix « 2 »

```
QEMU (pfSense-1) - TightVNC Viewer
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

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.254
```

Ont défini l'adresse IP de notre interface : **192.168.1.254**

```
QEMU (pfSense-1) - TightVNC Viewer
6) Halt system
7) Ping host
8) Shell
15) Restore recent configuration
16) Restart PHP-FPM

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

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.254

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
```

Et l'on indique le masque de sous réseau de notre réseau en « **CIDR** » : **24**

```
QEMU (pfSense-1) - TightVNC Viewer

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
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:
> 192.168.1.254

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:
>

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

On ignore la question demander, en appuyant sur « **Entrer** »

```
QEMU (pfSense-1) - TightVNC Viewer
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:
> 192.168.1.254

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:
>

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) ☐
```

On fait de même, car nous avons un réseau en IPv4

```
QEMU (pfSense-1) - TightVNC Viewer
> 192.168.1.254

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:
>

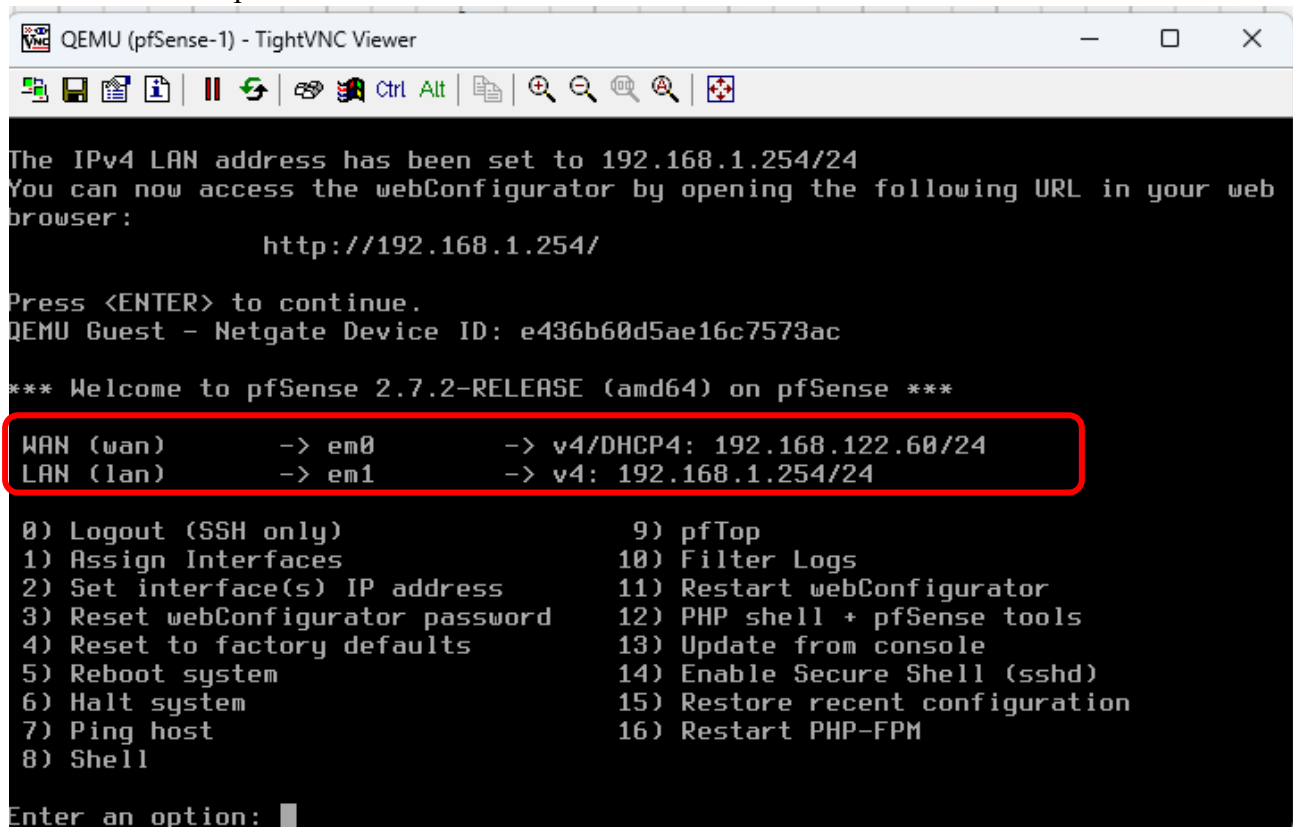
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.1
Enter the end address of the IPv4 client address range: 192.168.1.100
Disabling IPv6 DHCPD...

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

Appuyez sur <<Y>> pour activer le DHCP et saisir le début de la plage d'adresse

Et ensuite <<Y>> pour activer l'interface Web



```
QEMU (pfSense-1) - TightVNC Viewer

The IPv4 LAN address has been set to 192.168.1.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://192.168.1.254/

Press <ENTER> to continue.
QEMU Guest - Netgate Device ID: e436b60d5ae16c7573ac

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

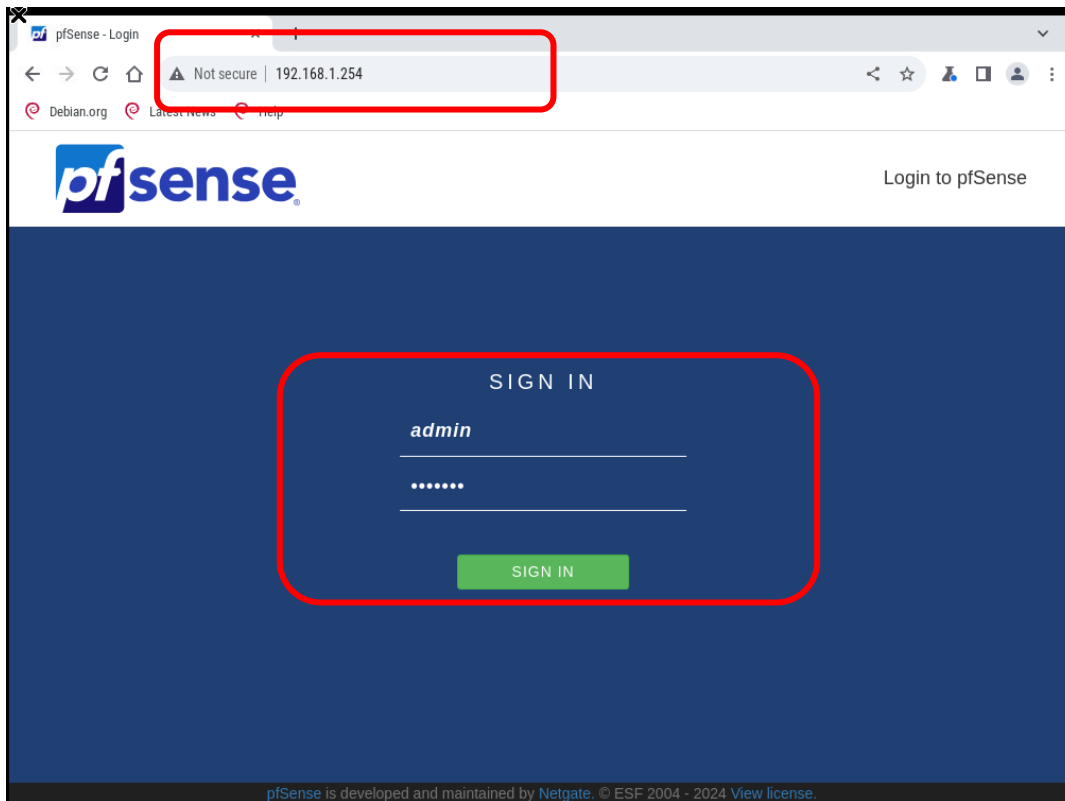
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.122.60/24
LAN (lan)      -> em1      -> v4: 192.168.1.254/24

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

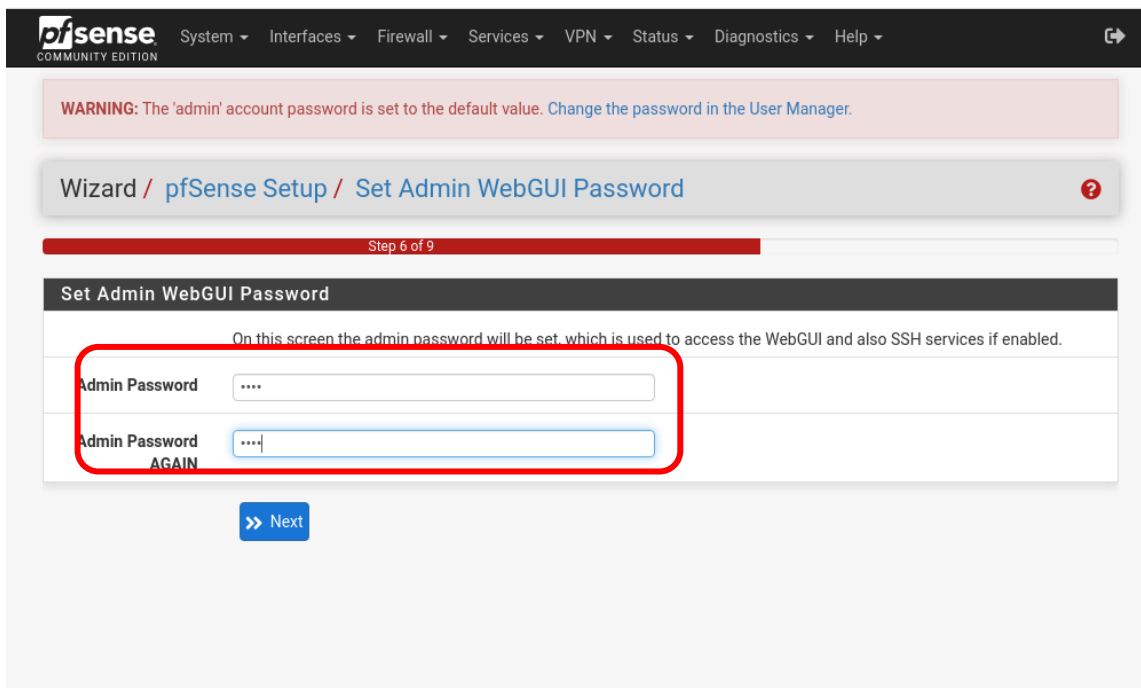
Enter an option: 
```

3.3. Interface Web du PfSense

Pour cela, se connecter sur le panel PFSense avec l'adresse IP de l'interface LAN = 192.168.1.254



Login : **admin** Password : **pfsense**



Cliquer sur <<Next>> jusqu'à ce que vous alliez tomber <<Set Admin WebGUI Password >> pour changer le mot de passe par défaut

Nous avons le Dashboard de PFSense, avec les informations principales et les informations système.

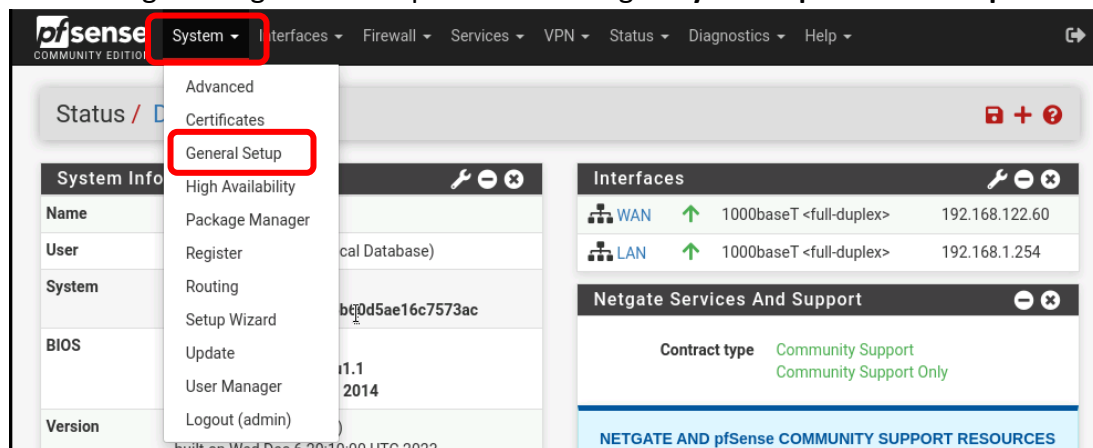
The screenshot displays the pfSense Community Edition dashboard. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled 'Status / Dashboard' and features three primary sections:

- System Information:** A table providing details about the system, including the name (pfSense.home.arpa), user (admin@192.168.1.1), system type (QEMU Guest), BIOS version (1.13.0-1ubuntu1.1), and the current pfSense version (2.7.2-RELEASE).
- Interfaces:** A table showing the status of network interfaces, including WAN and LAN, both configured as 1000baseT <full-duplex> with their respective IP addresses.
- Netgate Services And Support:** A section detailing the contract type (Community Support) and providing links to Netgate and pfSense community support resources.

The dashboard also includes a 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES' section with a detailed explanation of the support options available to users.

3.4. Configuration du General setup (changer le Hostname, Domain, DNS, Langue du système ...)

Pour configurer le général setup allez dans l'onglet **Système | General Setup**



Et changer les informations comme :
Hostname, Domain, DNS server, etc. ...

System

Hostname Name of the firewall host, without domain part.

Domain Domain name for the firewall.

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.

DNS Server Settings

DNS Servers	Address	Hostname	
<input type="text" value="8.8.8.8"/>	<input type="text" value="1.1.1.1"/>	<input type="text" value="google.com"/>	<input type="button" value="Delete"/>
	<input type="text" value="one.one.one.one"/>	<input type="text" value="one.one.one.one"/>	<input type="button" value="Delete"/>

Address
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.

Hostname
Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).

Add DNS Server

DNS Server Override ☐ Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if

Localization

Timezone Select a geographic region name (Continent/Location) to determine the timezone for the firewall. Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.

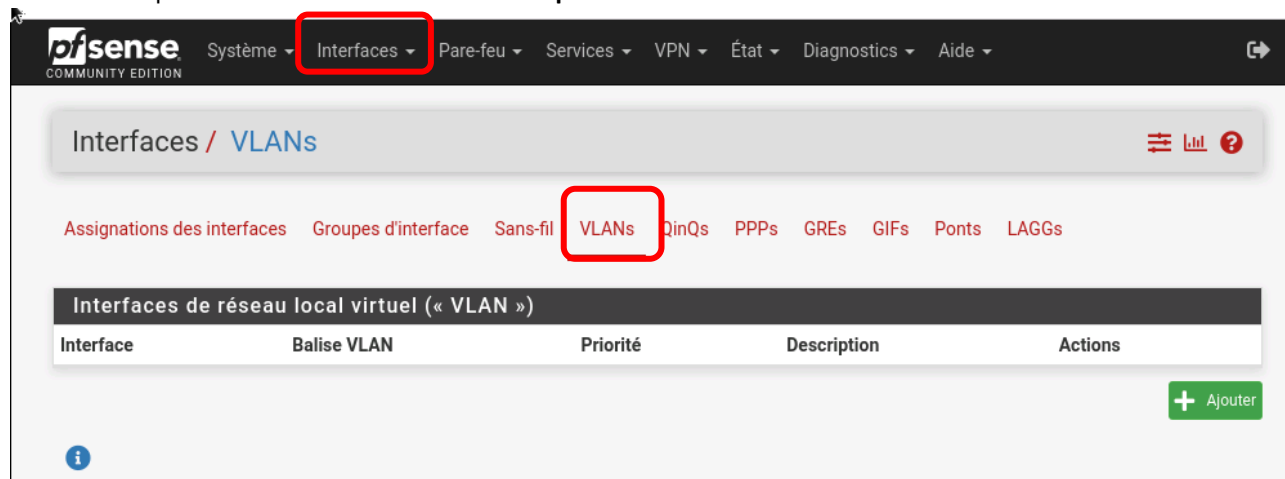
Timeservers Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!

Language Choose a language for the webConfigurator

3.5. Créations des VLAN

Les VLAN (Virtual LAN) nous permettent de séparer le trafic des différents réseaux pour augmenter la sécurité du réseau, nous pouvons créer plusieurs VLAN pour séparer les réseaux et avoir différents niveaux d'autorisations et d'accès dans chaque réseau local créé.

La première chose que nous devons faire pour créer des VLAN sur le LAN est d'accéder au **Interfaces | Affectations d'interface section | VLANs**



Pour créer un nouveau VLAN, cliquez sur « Ajouter », puis effectuez les étapes suivantes :

1. Interface parent : assurez-vous que nous Choisissons le port attribué au LAN (pas au WAN Internet).
2. Balise VLAN : Créez l'ID VLAN qui correspond à celui du commutateur.
3. Priorité VLAN : on peut le laisser vide.
4. Détails : nous mettons un nom descriptif, par exemple « Administrations »

Interfaces / VLANs / Modifier

Configuration VLAN

Interface parente	em1 (0c:07:05:73:00:01) - lan <small>Seules les interfaces compatibles VLAN seront affichées.</small>
Balise VLAN	10 <small>Balise VLAN 802.1Q (entre 1 et 4094).</small>
Priorité du VLAN	0 <small>Priorité VLAN 802.1Q (entre 0 et 7).</small>
Description	VLAN_Administrations <small>Une description du groupe est proposée ici pour aider l'administrateur (non pris en compte).</small>

Enregistrer

La procédure est exactement la même pour créer les autres VLAN









pfSense COMMUNITY EDITION

Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

Interfaces / VLANs

Assignations des interfaces Groupes d'interface Sans-fil VLANs QinQs PPPs GREs GIFs Ponts LAGGs

Interfaces de réseau local virtuel (« VLAN »)

Interface	Balise VLAN	Priorité	Description	Actions
em1 (lan)	10		VLAN_Administrations	 
em1 (lan)	20		VLAN_Utilisateurs	 
em1 (lan)	30		VLAN_Serveurs	 
em1 (lan)	40		VLAN_Visiteurs	 

+ Ajouter

Une fois créé, nous reviendrons à <<Interfaces | Affectations d'interface >>, Ici nous pouvons voir un résumé des interfaces physiques et du port réseau. Par défaut, nous aurons le WAN Internet (avec ou sans VLAN), ainsi que le LAN. Pour ajouter ces nouvelles interfaces au LAN, il suffit de sélectionner l'interface « VLAN 2 sur em1 ... » et de cliquer sur « Ajouter », et de même avec les autres, comme vous pouvez le voir sur les captures d'écran suivantes :

Interfaces / Assignations des interfaces



Assignations des interfaces Groupes d'interface Sans-fil VLANs QinQs PPPs GREs GIFs Ponts LAGGs

Interface	Port réseau	
WAN	em0 (0c:07:05:73:00:00)	
LAN	em1 (0c:07:05:73:00:01)	Supprimer
Ports réseau disponibles	em2 (0c:07:05:73:00:02)	Ajouter

Enregistrer

Les interfaces configurées comme membres d'une interface lagg(4) ne sont pas affichées.

Les interfaces sans-fil doivent être créées dans l'onglet Sans-fil avant de pouvoir être assignées.

Interfaces / Assignations des interfaces



Assignations des interfaces Groupes d'interface Sans-fil VLANs QinQs PPPs GREs GIFs Ponts LAGGs

Interface	Port réseau	
WAN	em0 (0c:07:05:73:00:00)	
LAN	em1 (0c:07:05:73:00:01)	Supprimer
Ports réseau disponibles	em2 (0c:07:05:73:00:02)	Ajouter




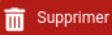


Enregistrer

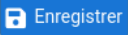
Les interfaces configurées comme membres d'une interface lagg(4) ne sont pas affichées.

Les interfaces sans-fil doivent être créées dans l'onglet Sans-fil avant de pouvoir être assignées.

em2 (0c:07:05:73:00:02)
em3 (0c:07:05:73:00:03)
em4 (0c:07:05:73:00:04)
em5 (0c:07:05:73:00:05)
VLAN 10 Marche em1 - lan (VLAN_Administrations)
VLAN 20 Marche em1 - lan (VLAN_Utilisateurs)
VLAN 30 Marche em1 - lan (VLAN_Serveurs)
VLAN 40 Marche em1 - lan (VLAN_Visiteurs)

Assignations des interfaces Groupes d'interface Sans-fil VLANs QinQs PPPs GREs GIFs Ponts LAGGs

Interface	Port réseau	
WAN	em0 (0c:07:05:73:00:00)	
LAN	em1 (0c:07:05:73:00:01)	
OPT1	VLAN 10 Marche em1 - lan (VLAN_Administrations)	
OPT2	VLAN 20 Marche em1 - lan (VLAN_Utilisateurs)	
OPT3	VLAN 30 Marche em1 - lan (VLAN_Serveurs)	
OPT4	VLAN 40 Marche em1 - lan (VLAN_Visiteurs)	
Ports réseau disponibles	em2 (0c:07:05:73:00:02)	



Une fois que nous les avons créés, ils apparaîtront tous dans la liste déroulante « Interfaces », le nom par défaut étant « OPT1 », « OPT2 » et ainsi de suite. Par défaut, nous avons activé l'interface LAN, avec son adresse IPv4 privée correspondante

Configuration générale

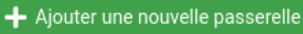
Activer ☒ Activer interface

Description Administrations
Entrez ici une description (nom) pour cette interface.

Type de configuration IPv4 IPv4 statique

Configuration statique IPv4


Adresse IPv4 192.168.10.254 / 24

Passerelle IPv4 en amont Aucun 

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](#).

Interfaces / Visiteurs (em1.40)

La configuration de Visiteurs a été modifiée.
Ces modifications doivent être appliquées pour prendre effet.
N'oubliez pas d'ajouter la plage du serveur DHCP si besoin, après avoir appliqué.



La configuration du reste des interfaces est exactement la même, nous devons l'activer, mettre un nom descriptif, mettre la configuration IPv4 et / ou IPv6 correspondante, enregistrer les modifications et les appliquer.

VLAN Administrations 192.168.10.254

VLAN Utilisateur 192.168.20.254

VLAN Serveurs 192.168.30.254

VLAN Visiteurs 192.168.40.254

Assignations des interfaces Grupos d'interface Sans-fil VLANs QinQs PPPs GREs GIGs Ports LAGGs

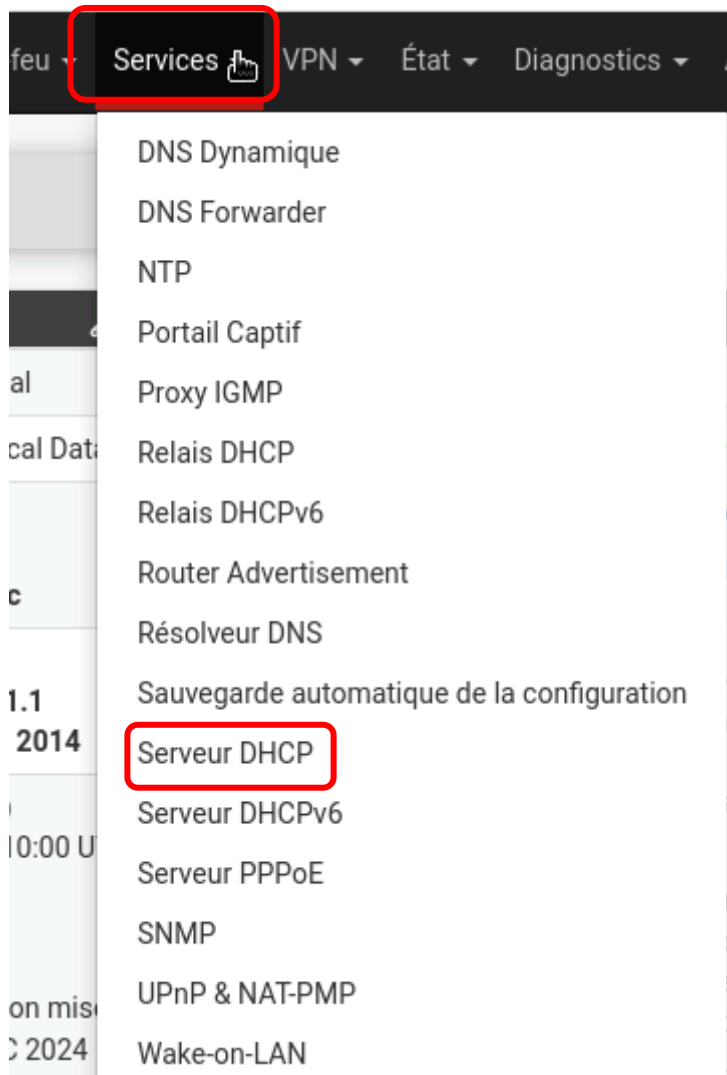
Interface	Port réseau
WAN	em0 (0c:07:05:73:00:00)
LAN	em1 (0c:07:05:73:00:01) Supprimer
Administrations	VLAN 10 Marche em1 - lan (VLAN_Administrations) Supprimer
Utilisateurs	VLAN 20 Marche em1 - lan (VLAN_Utilisateurs) Supprimer
Serveurs	VLAN 30 Marche em1 - lan (VLAN_Serveurs) Supprimer
Visiteurs	VLAN 40 Marche em1 - lan (VLAN_Visiteurs) Supprimer
Ports réseau disponibles	em2 (0c:07:05:73:00:02) + Ajouter

Enregistrer

Interfaces			
WAN	↑	1000baseT <full-duplex>	192.168.122.60
LAN	↑	1000baseT <full-duplex>	192.168.1.254
ADMINISTRATIONS	↑	1000baseT <full-duplex>	192.168.10.254
UTILISATEURS	↑	1000baseT <full-duplex>	192.168.20.254
SERVEURS	↑	1000baseT <full-duplex>	192.168.30.254
VISITEURS	↑	1000baseT <full-duplex>	192.168.40.254

3.6. Configurations du serveur DHCP sur chaque interfaces VLAN

Pour ce faire, nous allons dans la section « Services | Serveur DHCP ». Juste en dessous, nous aurons quelques onglets de LAN, et les mêmes réseaux que nous avons créés précédemment VLANs.



Choisissons un VLAN et remplir les informations comme suite :

Cocher la case activer le sur l'interfaces

Définir la plage d'adresse

VLAN 10 : 192.168.10.10 – 192.168.10.100

VLAN 20 : 192.168.20.10 – 192.168.20.100

VLAN 30 : 192.168.30.10 – 192.168.30.100

VLAN 40 : 192.168.40.10 – 192.168.40.100

General DHCP Options	
DHCP Backend	ISC DHCP
Activer	<input checked="" type="checkbox"/> Activer le serveur DHCP sur l'interface ADMINISTRATIONS
BOOTP	<input type="checkbox"/> Ignorer les requêtes BOOTP
Deny Unknown Clients	<div> Allow all clients </div> <p>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.</p>
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject Cette option n'est pas compatible avec le failover et ne peut pas être activée lorsqu'une adresse Failover Peer IP est configurée.
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request Cette option peut être utile lorsqu'un client peut dual boot en utilisant différents identifiants client, mais avec la même adresse matérielle (MAC). Notez que ce comportement du serveur est contraire aux spécifications officielles de DHCP.
Primary Address Pool	
Sous-réseau	192.168.10.0/24
Subnet Range	192.168.10.1 - 192.168.10.254
Address Pool Range	<div> 192.168.10.10 192.168.10.100 </div>

Les options de configuration des autres VLAN sont exactement les mêmes.

3.7. Configurations des règles de pare-feu

Les règle de pare-feu permet d'autoriser ou refuser certaine Trafic qui transitent les différents interfaces physique et logique de réseau.

Dans notre cas nous allons bloquer tous les trafics et autoriser certain trafic : (HTTP, HTTPS, DNS, ICMP)

Dans l'onglet <<**Pare-feu | Règle**>> choisissez un réseau (vlan _admin, LAN ...)

➤ 1ère règle : Bloquer tous les trafic et protocole

Modifier la règle de Pare-Feu

Action Bloquer
Choisissez que faire des paquets qui correspondent aux critères ci-dessous.
Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'expéditeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.

Désactivé ☐ Désactiver cette règle
Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.

Interface ADMINISTRATIONS
Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.

Famille d'adresse IPv4
Choisissez la version du protocole IP à laquelle cette règle s'applique.

Protocole Tous
Choisissez quel protocole IP cette règle devrait correspondre.

Source

Source ☐ Invert match Tous Source Address /

Destination

Destination ☐ Invert match Tous Destination Address /

- 2^{ème} règle : Autoriser le protocole http et HTTPS pour permettre au réseau d'avoir accès à l'internet

Modifier la règle de Pare-Feu

Action Autoriser

Choisissez que faire des paquets qui correspondent aux critères ci-dessous.
Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'expéditeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.

Désactivé ☐ Désactiver cette règle
Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.

Interface ADMINISTRATIONS
Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.

Famille d'adresse IPv4+IPv6
Choisissez la version du protocole IP à laquelle cette règle s'applique.

Protocole TCP
Choisissez quel protocole IP cette règle devrait correspondre.

Source

Source ☐ Invert match ADMINISTRATIONS subnets Source Address /

[Afficher les options avancées](#)

La **plage de ports source** d'une connexion est généralement aléatoire et presque jamais égale au port de destination. Dans la plupart des cas, ce paramètre doit rester à sa valeur par défaut, **any**.

Destination

Destination ☐ Invert match Tous Destination Address /

Plage de port de destination HTTP (80) Personnalisé(e) À HTTPS (443) Personnalisé(e)

Spécifiez le port destination ou la plage de port pour cette règle. Le champ « A » peut rester vide seulement si le filtre est sur un seul port.

Même procédure pour autoriser le protocole DNS sauf la plage de port destination change DNS (53)

- 3^{ème} règle : Autorisations du protocole ICMP pour permettre au VLAN d'envoyer et recevoir des requêtes ICMP (ping)

Modifier la règle de Pare-Feu

Action Autoriser

Choisissez que faire des paquets qui correspondent aux critères ci-dessous.
Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'expéditeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.

Désactivé ☐ Désactiver cette règle
Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.

Interface ADMINISTRATIONS
Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.

Famille d'adresse IPv4
Choisissez la version du protocole IP à laquelle cette règle s'applique.

Protocole ICMP
Choisissez quel protocole IP cette règle devrait correspondre.

Sous-types ICMP
 tout
 Alternate Host
 Datagram conversion error
 Echo reply

pour les règles ICMP sur IPv4, un ou plusieurs de ces sous-types ICMP peuvent être spécifiés

Source

Source ☐ Invert match ADMINISTRATIONS subnets Source Address /

Destination

Destination ☐ Invert match Tous Destination Address /

Les processus restent la même pour créer les règles de pare-feu pour les autres VLANs

Flottant(e) WAN LAN **ADMINISTRATIONS** UTILISATEURS SERVEURS VISITEURS GEST

Règles (Faire glisser pour changer l'ordre)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input type="checkbox"/>	✓ B	0/0 ICMP any	ADMINISTRATIONS subnets	*	*	*	*	aucun		ICMP Autoriser	
<input type="checkbox"/>	✓ B	0/0 IPv4 TCP	ADMINISTRATIONS subnets	*	*	53 (DNS)	*	aucun		DNS Autoriser	
<input type="checkbox"/>	✓ B	0/0 IPv4+6 TCP	ADMINISTRATIONS subnets	*	*	80 - 443	*	aucun		HTTP, HTTPS Autoriser	
<input type="checkbox"/>	✗ B	0/0 IPv4 *	*	*	*	*	*	aucun		Tous les trafic Bloquer	

Règles (Faire glisser pour changer l'ordre)											
<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input type="checkbox"/>		0/0 B	IPv4 ICMP any	UTILISATEURS subnets	*	*	*	*	aucun	ICMP	
<input type="checkbox"/>		0/0 B	IPv4 TCP	UTILISATEURS subnets	*	*	53 (DNS)	*	aucun	DNS Autoriser	
<input type="checkbox"/>		0/0 B	IPv4 TCP	UTILISATEURS subnets	*	*	80 - 443	*	aucun	HTTP, HTTPS Autoriser	
<input type="checkbox"/>		0/0 B	IPv4+6 *	*	*	*	*	*	aucun	Tous traffic bloquer	

Règles (Faire glisser pour changer l'ordre)											
<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input type="checkbox"/>		0/0 B	IPv4 ICMP any	SERVEURS subnets	*	*	*	*	aucun	ICMP	
<input type="checkbox"/>		0/0 B	IPv4 TCP	SERVEURS subnets	*	*	53 (DNS)	*	aucun	DNS Autoriser	
<input type="checkbox"/>		0/0 B	IPv4 TCP	SERVEURS subnets	*	*	80 - 443	*	aucun	HTTP, HTTPS Autoriser	
<input type="checkbox"/>		0/0 B	IPv4+6 *	*	*	*	*	*	aucun	Tous Traffic Bloquer	

Règles (Faire glisser pour changer l'ordre)											
<input type="checkbox"/>	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input type="checkbox"/>		0/0 B	IPv4 ICMP any	VISITEURS subnets	*	*	*	*	aucun	ICMP Autoriser	
<input type="checkbox"/>		0/0 B	IPv4 TCP	VISITEURS subnets	*	*	53 (DNS)	*	aucun	DNS Autoriser	
<input type="checkbox"/>		0/0 B	IPv4 TCP	VISITEURS subnets	*	*	80 - 443	*	aucun	HTTP, HTTPS Autoriser	
<input type="checkbox"/>		0/0 B	IPv4+6 *	*	*	*	*	*	aucun	Tous Traffic bloquer	

3.8. Configurations du switch SWT—DST

Sur le switch SWT_DST nous allons créer des VLANs avec des même identifiant comme sur le pare-feu PfSense et configurer les ports du switch

➤ Créations des VLAN

```
IOU1(config)#vlan 10
IOU1(config-vlan)# name VLAN_Administrations
IOU1(config-vlan)# vlan 20
IOU1(config-vlan)# name VLAN_Utilisateurs
IOU1(config-vlan)# vlan 30
IOU1(config-vlan)# name VLAN_Serveurs
IOU1(config-vlan)# vlan 40
IOU1(config-vlan)# name VLAN_Visiteurs
```

➤ Configurations des ports

Le port ethernet0/0 est configurer en mode trunk et permet de faire passer les Traffic de chaque VLAN ver le Pfsense

```
IOU1(config)# int et0/0
IOU1(config-if)# switchport trunk encapsulation dot1q
IOU1(config-if)# switchport mode trunk
IOU1(config-if)# no shut
```

Et les 4 autre ports sont configurer en mode Access et sont intègre dans des VLANs

Ethernet0/1 = vlan 10

Ethernet0/2 = vlan 20

Ethernet0/3 = vlan 30

Ethernet1/0 = vlan 40

```
IOU1(config)#int et0/1
IOU1(config-if)#switchport mode access
IOU1(config-if)#switchport access vlan 10
IOU1(config-if)#no sh
IOU1(config-if)#
IOU1(config-if)#int et0/2
IOU1(config-if)#switchport mode access
IOU1(config-if)#switchport access vlan 20
IOU1(config-if)#no sh
IOU1(config-if)#
IOU1(config-if)#int et0/3
IOU1(config-if)#switchport mode access
IOU1(config-if)#switchport access vlan 30
IOU1(config-if)#no sh
IOU1(config-if)#
IOU1(config-if)#int et1/0
IOU1(config-if)#switchport mode access
IOU1(config-if)#switchport access vlan 40
IOU1(config-if)#no sh
```

➤ Vérifications des configurations

```
IOU1(config-if)#do sh vlan br
```

VLAN	Name	Status	Ports
1	default	active	Et1/1, Et1/2, Et1/3, Et2/0 Et2/1, Et2/2, Et2/3, Et3/0 Et3/1, Et3/2, Et3/3
10	VLAN_Administrations	active	Et0/1
20	VLAN_Utilisateurs	active	Et0/2
30	VLAN_Serveurs	active	Et0/3
40	VLAN_Visiteurs	active	Et1/0
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```
IOU1(config-if)#
```

```
IOU1(config-if)#do sh int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/0	on	802.1q	trunking	1
Port Et0/0	Vlans allowed on trunk 1-4094			
Port Et0/0	Vlans allowed and active in management domain 1,10,20,30,40			
Port Et0/0	Vlans in spanning tree forwarding state and not pruned 1,10,20,30,40			

```
IOU1(config-if)#
```

IV- Test et Validations

4.1. Vérifions que chaque VLAN reçoit la bonne adresse IP via le DHCP

Utiliser << **IP DHCP** >> pour activer le DHCP sur les VPCS et <<**show IP** >> pour vérifier les informations reçues par le DHCP

```
PC1> ip dhcp
DORA IP 192.168.10.11/24 GW 192.168.10.254

PC1> show ip

NAME       : PC1[1]
IP/MASK    : 192.168.10.11/24
GATEWAY    : 192.168.10.254
DNS        : 192.168.10.254
DHCP SERVER : 192.168.10.254
DHCP LEASE  : 7195, 7200/3600/6300
DOMAIN NAME : BynariSecProjet.Local
MAC        : 00:50:79:66:68:03
LPORT      : 10010
RHOST:PORT  : 127.0.0.1:10011
MTU        : 1500

PC1> █
```

```
VPCS> ip dhcp
DORA IP 192.168.20.10/24 GW 192.168.20.254

VPCS> show ip

NAME       : VPCS[1]
IP/MASK    : 192.168.20.10/24
GATEWAY    : 192.168.20.254
DNS        : 192.168.20.254
DHCP SERVER : 192.168.20.254
DHCP LEASE  : 7195, 7200/3600/6300
DOMAIN NAME : BynariSecProjet.Local
MAC        : 00:50:79:66:68:00
LPORT      : 10007
RHOST:PORT  : 127.0.0.1:10008
MTU        : 1500

VPCS> █
```

```
PC_Serveur> ip dhcp
DORA IP 192.168.30.10/24 GW 192.168.30.254

PC_Serveur> show ip

NAME       : PC_Serveur[1]
IP/MASK    : 192.168.30.10/24
GATEWAY    : 192.168.30.254
DNS        : 192.168.30.254
DHCP SERVER : 192.168.30.254
DHCP LEASE  : 7194, 7200/3600/6300
DOMAIN NAME : BynariSecProjet.Local
MAC        : 00:50:79:66:68:01
LPORT      : 10005
RHOST:PORT  : 127.0.0.1:10006
MTU        : 1500

PC_Serveur> █
```

```
PC1> ip dhcp
DORA IP 192.168.10.11/24 GW 192.168.10.254

PC1> show ip

NAME       : PC1[1]
IP/MASK    : 192.168.10.11/24
GATEWAY    : 192.168.10.254
DNS        : 192.168.10.254
DHCP SERVER : 192.168.10.254
DHCP LEASE  : 7195, 7200/3600/6300
DOMAIN NAME : BynariSecProjet.Local
MAC        : 00:50:79:66:68:03
LPORT      : 10010
RHOST:PORT  : 127.0.0.1:10011
MTU        : 1500

PC1> █
```

Dans l'onglet <<**services |Bails DHCP** >> vérifions les adresses qui ont été attribué et les adresse MAC des Clients DHCP

Baux							
	Adresse IP	Adresse MAC	Nom d'hôte	Description	Démarrer	Fin	Actions
☑️⬇️	192.168.1.10	06:85:26:b8:8f:24			2024/11/01 05:38:04	2024/11/01 07:38:04	⊕⊕🔌🗑️
☑️⬆️	192.168.10.10	ca:d4:fc:06:48:cb			2024/11/01 06:21:43	2024/11/01 08:21:43	⊕⊕
☑️⬆️	192.168.10.11	00:50:79:66:68:03	pc11		2024/11/01 06:26:07	2024/11/01 08:26:07	⊕⊕
☑️⬆️	192.168.20.10	00:50:79:66:68:00	vpcs1		2024/11/01 06:22:32	2024/11/01 08:22:32	⊕⊕
☑️⬆️	192.168.30.10	00:50:79:66:68:01	pcserveur1		2024/11/01 06:23:35	2024/11/01 08:23:35	⊕⊕
☑️⬆️	192.168.40.10	00:50:79:66:68:02	pcvisiteur1		2024/11/01 06:24:14	2024/11/01 08:24:14	⊕⊕

Lease Utilization					
Interface	Début du Pool	Fin du Pool	Used	Capacity	Utilization
LAN	192.168.1.10	192.168.1.245	1	236	0% of 236
ADMINISTRATIONS	192.168.10.10	192.168.10.100	2	91	2% of 91
UTILISATEURS	192.168.20.10	192.168.20.100	1	91	1% of 91
SERVEURS	192.168.30.10	192.168.30.100	1	91	1% of 91
VISITEURS	192.168.40.10	192.168.40.100	1	91	1% of 91

4.2. Testez la connectivité entre les VLANs et d'accès à internet

```

PC1> ping 192.168.20.10
84 bytes from 192.168.20.10 icmp_seq=1 ttl=63 time=37.069 ms
84 bytes from 192.168.20.10 icmp_seq=2 ttl=63 time=7.036 ms
84 bytes from 192.168.20.10 icmp_seq=3 ttl=63 time=7.545 ms
84 bytes from 192.168.20.10 icmp_seq=4 ttl=63 time=7.093 ms
84 bytes from 192.168.20.10 icmp_seq=5 ttl=63 time=32.508 ms

PC1> ping 192.168.30.10
84 bytes from 192.168.30.10 icmp_seq=1 ttl=63 time=9.579 ms
84 bytes from 192.168.30.10 icmp_seq=2 ttl=63 time=7.916 ms
84 bytes from 192.168.30.10 icmp_seq=3 ttl=63 time=8.244 ms
84 bytes from 192.168.30.10 icmp_seq=4 ttl=63 time=12.450 ms
84 bytes from 192.168.30.10 icmp_seq=5 ttl=63 time=8.211 ms

PC1> ping 192.168.40.10
84 bytes from 192.168.40.10 icmp_seq=1 ttl=63 time=12.757 ms
84 bytes from 192.168.40.10 icmp_seq=2 ttl=63 time=19.215 ms
84 bytes from 192.168.40.10 icmp_seq=3 ttl=63 time=9.966 ms
84 bytes from 192.168.40.10 icmp_seq=4 ttl=63 time=13.872 ms
84 bytes from 192.168.40.10 icmp_seq=5 ttl=63 time=10.633 ms



PC1> █

```


Test d'accès à internet

← → ↻ 🏠 🔒 duckduckgo.com/?q=google&ia=web 🔍 ☆ 🧑🏿 📱 👤 ⋮

🌀 Debian.org 🌀 Latest News 🌀 Help




Privacy, simplified. ☰

 **All** Images Videos News Maps

🔍 Assist 💬 Chat ⚙️

🟢 Always private ▾ All regions ▾ Safe search: moderate ▾ Any time ▾

 <https://www.google.com> ⋮

Google

Search the world's information, including webpages, images, videos and more. **Google** has many special features to help you find exactly what you're looking for.


Gmail
We would like to show you a description here but the site won't allow us.

Search
The Google app can help you plan your next evening out (or in), with the perfe...

Maps
We would like to show you a description here but the site won't allow us.

Translate
Google Translate lets you translate words, phrases, and web pages...

Google Scholar
Search in the author, title, and publication fields, as well as limit your...

 **News for google**

**Googl
e**
American multinati...
technolo...
company,
a
subsidiary
of
Alphabet
Inc.

Google LLC is an American multinational corporation and technology company focusing on online advertising, search engine technology, cloud computing, computer software, quantum

V– Conclusion

Ce projet a permis de concevoir et de déployer une architecture réseau segmentée et sécurisée grâce aux VLANs et à PfSense, le tout simulé sous GNS3. En isolant les différents segments du réseau, nous avons pu contrôler finement les accès, optimiser la sécurité, et simplifier la gestion du trafic. Cette segmentation offre une protection accrue face aux menaces internes et facilite l'évolution du réseau selon les besoins futurs. Ce travail démontre l'efficacité de PfSense dans la gestion et la sécurisation des réseaux, en faisant un outil idéal pour des environnements professionnels nécessitant robustesse et flexibilité.

MERCI !!!