

VLAN

Document d'exploitation

Kim LAUGAUDIN





Table des matières

1. Définition.....	2
2. Configuration sur le commutateur.....	3
3. Configuration dans le Proxmox Virtual Environment	9

1. Définition

Un VLAN, pour Virtual Local Area Network, décrit un type de réseau local. On le traduit en français par réseau local virtuel.

Le VLAN regroupe, de façon logique et indépendante, un ensemble de machines informatiques. On peut en retrouver plusieurs coexistant simultanément sur un même commutateur réseau.

Le VLAN améliore la gestion du réseau en apportant plus de souplesse dans son administration. Il apporte davantage de sécurité en imposant, par exemple, le passage par un routeur pour la communication entre deux machines. Il optimise la bande passante, sépare les flux et réduit la diffusion du trafic.

Il existe trois différents types de réseau local virtuel : de niveau 1 (aussi appelé VLAN par port), de niveau 2 (VLAN par adresse MAC) et de niveau 3 (VLAN par adresse IP).

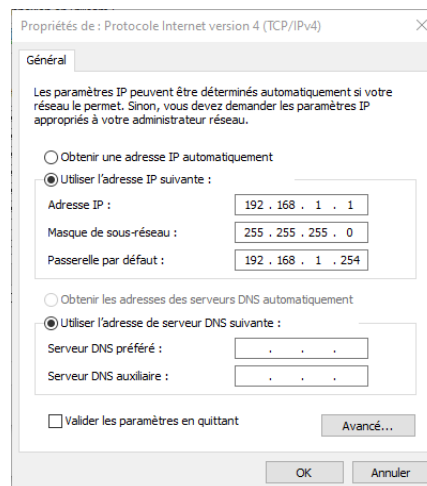
2. Configuration sur le commutateur

Pour notre infrastructure réseau nous possédons un commutateur Cisco SG300-28 28 ports.



Afin de pouvoir le configurer, une première fois, nous devons modifier notre adresse IP afin de nous connecter une première fois dessus.

Vous trouverez ci dessous les paramètres à rentrer dans la carte réseau :



Une fois ces paramètres enregistrés, il faut alors se connecter à l'aide d'un câble RJ45 au commutateur Cisco.

Il faut alors ouvrir un navigateur Web et se connecter à l'adresse suivante : <http://192.168.1.254>

Ce lien nous redirige vers l'interface Web du commutateur, où nous pourrions alors modifier son mot de passe administrateur dans un premier temps.

Change Password

Please change your password from the default settings for better protection of your network

The minimum requirements are as follows:

- Cannot be the same as the user name.
- Cannot be the same as the current password.
- Minimum length is 8.
- Minimum number of character classes is 3. Character classes are upper case, lower case, numeric, and special characters.

New Password Configuration

Old Password:

New Password:

Confirm Password:

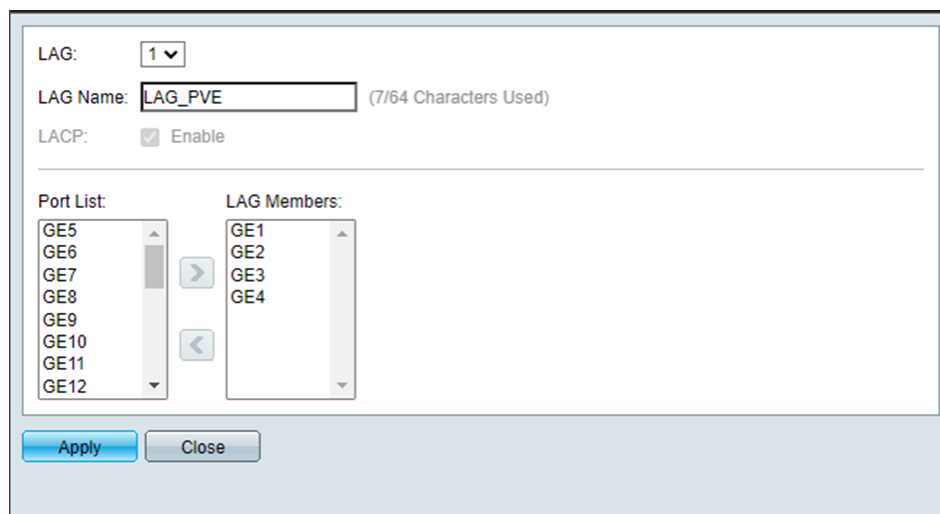
Password Strength Meter: Below Minimum

Password Strength Enforcement: Disable

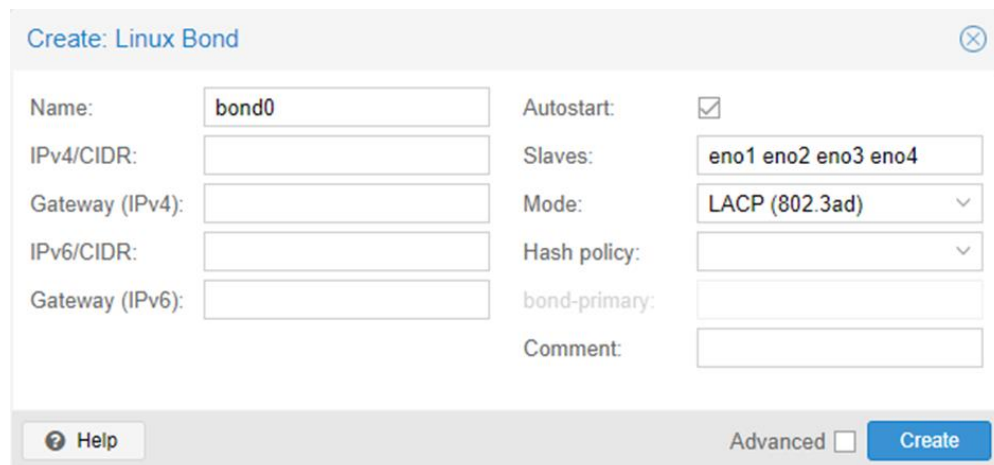
Par la suite, nous avons changé son adresse IP fixe.

Nous pouvons dès lors passer à la création de nos VLANs par ports, car son avantage principal est qu'il permet une étanchéité maximale des VLANs. Une attaque extérieure ne pourra se faire qu'en branchant le PC pirate sur un port tagué. Le pirate a donc besoin d'avoir accès au commutateur pour pénétrer le VLAN.

Nous avons tout d'abord créé des agrégations de liens pour nos Proxmox Virtual Environment et Proxmox Backup Server, pour se faire, nous avons créé des Linux Bond sur nos Proxmox et avons créé des LAGs sur notre commutateur :



LAG 1 pour le Proxmox VE sur le commutateur



Linux Bond dans Proxmox VE

Nous avons alors répété l'opération pour Proxmox BS.

Nous avons alors défini l'état de nos ports : s'ils sont en Access ou en Trunk :

Interface Settings

Interface Setting Table Showing 1-28 of 28 All per page

Filter: *Interface Type equals to* Port

Entry No.	Interface	Interface VLAN Mode	Administrative PVID	Frame Type	Ingress Filtering	
<input type="radio"/>	1	GE1	Trunk	1	Admit All	Enabled
<input type="radio"/>	2	GE2	Trunk	1	Admit All	Enabled
<input type="radio"/>	3	GE3	Trunk	1	Admit All	Enabled
<input type="radio"/>	4	GE4	Trunk	1	Admit All	Enabled
<input type="radio"/>	5	GE5	Access	10	Admit All	Enabled
<input type="radio"/>	6	GE6	Access	10	Admit All	Enabled
<input type="radio"/>	7	GE7	Trunk	1	Admit All	Enabled
<input type="radio"/>	8	GE8	Trunk	1	Admit All	Enabled
<input type="radio"/>	9	GE9	Trunk	1	Admit All	Enabled
<input type="radio"/>	10	GE10	Trunk	1	Admit All	Enabled
<input type="radio"/>	11	GE11	Access	20	Admit All	Enabled
<input type="radio"/>	12	GE12	Access	20	Admit All	Enabled
<input type="radio"/>	13	GE13	Access	40	Admit All	Enabled
<input type="radio"/>	14	GE14	Access	40	Admit All	Enabled
<input type="radio"/>	15	GE15	Access	40	Admit All	Enabled
<input type="radio"/>	16	GE16	Trunk	1	Admit All	Enabled
<input type="radio"/>	17	GE17	Trunk	1	Admit All	Enabled
<input type="radio"/>	18	GE18	Trunk	1	Admit All	Enabled

Les ports Trunk vont envoyer les paquets taggés destinés aux ports en mode Access.

Un port en mode Access a accès à un VLAN ce qui veut dire qu'il ne recevra que les paquets qui lui sont destinés.

Nous devons alors nous rendre dans l'onglet "Gestion des VLAN" puis "Créer un VLAN" :

Créer un VLAN

Table VLAN

<input type="checkbox"/>	ID de VLAN	Nom du VLAN	Type
<input type="checkbox"/>	1		Par défaut
<input type="checkbox"/>	10	VLAN_MZ	Statique
<input type="checkbox"/>	20	VLAN_DMZ	Statique
<input type="checkbox"/>	32	VLAN_INFO	Statique
<input type="checkbox"/>	40	VLAN_SLAM	Statique
<input type="checkbox"/>	99	VLAN_WAN	Statique

Le VLAN 1 est le VLAN administratif et il est fortement déconseillé de le modifier.

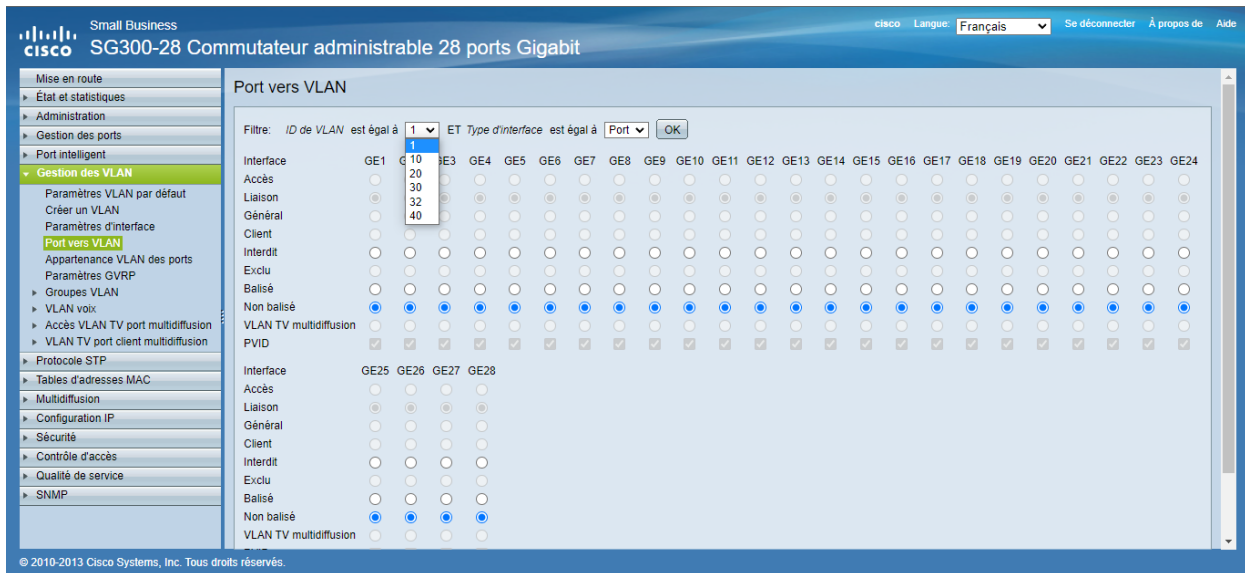
Nous avons alors créé 5 VLANs :

- VLAN 10 : VLAN_MZ pour notre Proxmox Virtual Environment
- VLAN 20 : VLAN_DMZ pour notre Proxmox Backup Server
- VLAN 32 : VLAN_INFO pour un accès total à l'infrastructure
- VLAN 40 : VLAN_SLAM pour un accès à leur site hébergé ainsi qu'à internet
- VLAN 99 : VLAN_WAN pour l'accès internet

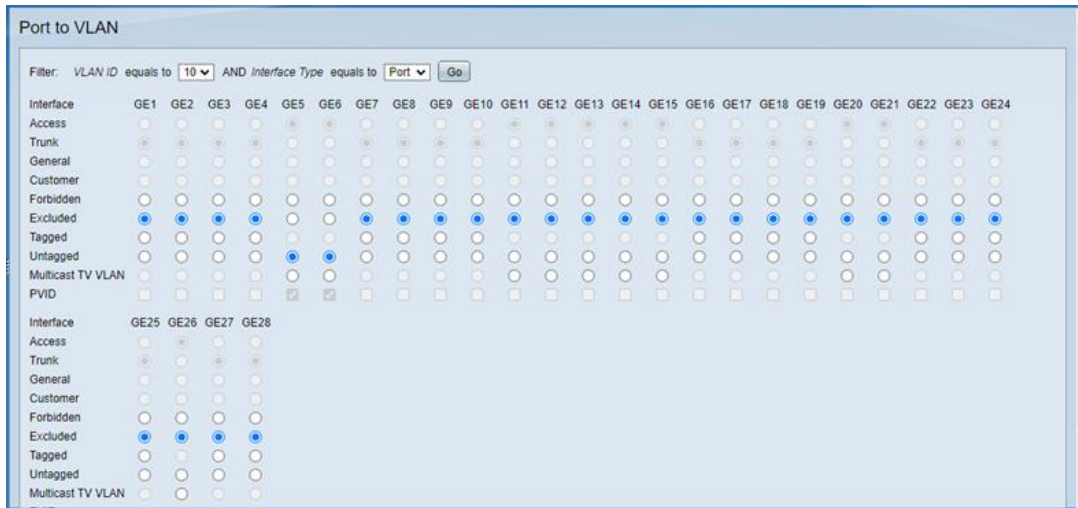
Une fois créés, nous devons attribuer nos VLANs à nos ports.

Pour ce faire, nous devons nous rendre dans l'interface "Ports vers VLAN" et y sélectionner le VLAN que l'on souhaite attribuer aux ports

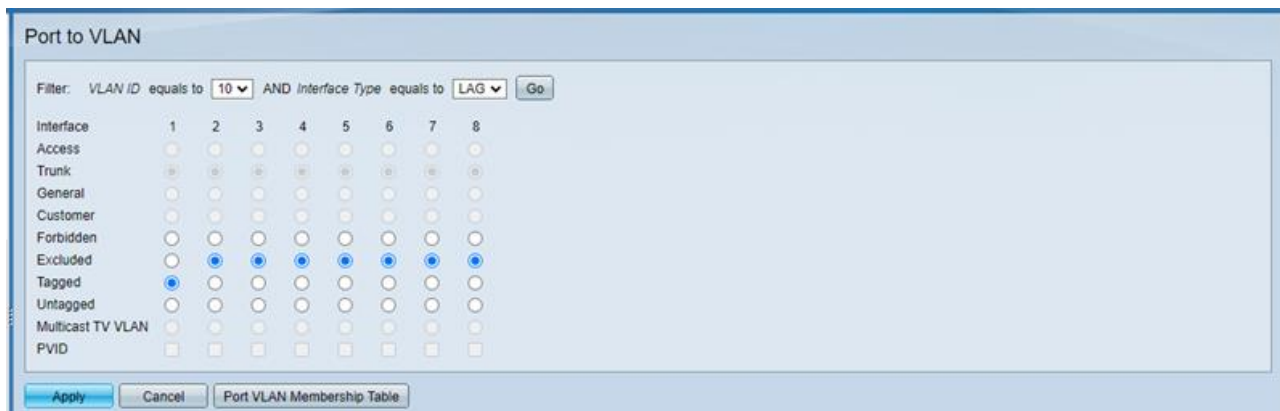
:



Ci-dessous, l'attribution du VLAN_MZ pour les ports du commutateur :



Configuration pour les ports



Configuration pour les LAG

Nous avons alors effectué cette opération pour chaque VLAN respectivement avec des accès limités.

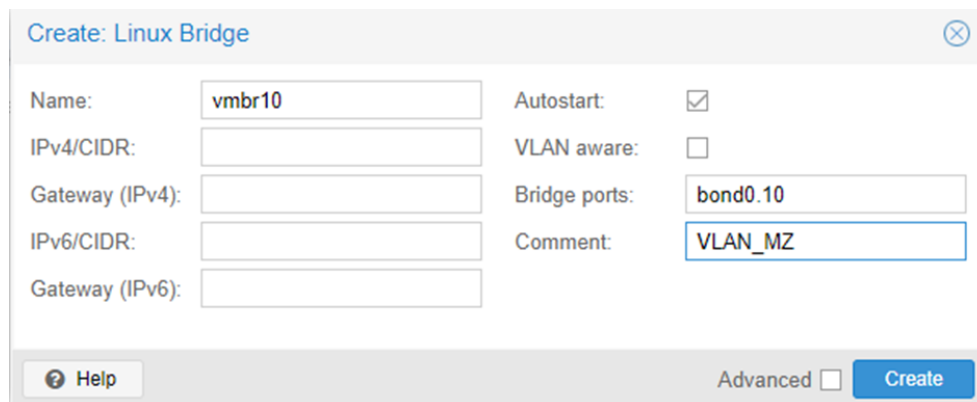
Nous avons alors effectué cette opération pour chaque VLANs créés précédemment.

Les VLANs du commutateur étant maintenant configurés, passons à la configuration dans le Proxmox Virtual Environment.

3. Configuration dans le Proxmox Virtual Environment

Vient alors la configuration dans Proxmox Virtual Environment, nous allons alors créer des Linux Bridge (VMBR), qui sont des cartes réseaux virtuelles fonctionnant comme des commutateurs.

Nous avons donc créé 5 VMBRs :



Name:	vmbr10	Autostart:	<input checked="" type="checkbox"/>
IPv4/CIDR:		VLAN aware:	<input type="checkbox"/>
Gateway (IPv4):		Bridge ports:	bond0.10
IPv6/CIDR:		Comment:	VLAN_MZ
Gateway (IPv6):			

Help Advanced Create

L'option "Bridge ports" est assignée au bond0, qui est notre agrégation de lien, et ".10" permet de taguer les paquets dans le VLAN 10.

Pour le VLAN_INFO, nous avons attribué une adresse afin de se connecter au Proxmox dans le bon VLAN, ainsi qu'une adresse de routage afin que Proxmox ait accès à internet pour les mises à jour :

Create: Linux Bridge
⊗

Name:

IPv4/CIDR:

Gateway (IPv4):

IPv6/CIDR:

Gateway (IPv6):

Autostart:

VLAN aware:

Bridge ports:

Comment:

Help
Advanced
Create

Voici alors notre configuration réseau pour le Proxmox VE :

Create Revert Edit Remove Apply Configuration								
Name ↑	Type	Active	Autos...	VLAN aware	Ports/Slaves	Bond Mode	CIDR	Gatew
bond0	Linux Bond	Yes	Yes	No	eno1 eno2 ...	LACP (802.3...		
eno1	Network De...	Yes	Yes	No				
eno2	Network De...	Yes	Yes	No				
eno3	Network De...	Yes	Yes	No				
eno4	Network De...	Yes	Yes	No				
vmbr10	Linux Bridge	Yes	Yes	No	bond0.10			
vmbr20	Linux Bridge	Yes	Yes	No	bond0.20			
vmbr32	Linux Bridge	Yes	Yes	No	bond0.32		192.168.32.50/...	192.1
vmbr40	Linux Bridge	Yes	Yes	No	bond0.40		192.168.40.50/...	
vmbr99	Linux Bridge	Yes	Yes	No	bond0.99			

Nous devons alors créer une machine virtuelle pfSense et une machine maître afin de servir de pare-feu et gérer les routages de nos VMBRs.

Pour ce faire, nous devons attribuer chaque VMBRs créés précédemment à notre machine :

Virtual Machine 119 (pfSense) on node 'M2L'

Start Shutdown Console More Help

Add Remove Edit Disk Action Revert

Summary

Console

Hardware

Cloud-Init

Options

Task History

Monitor

Backup

Replication

Snapshots

Firewall

Permissions

Memory	4.00 GiB
Processors	2 (1 sockets, 2 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	Default (LSI 53C895A)
CD/DVD Drive (ide2)	none,media=cdrrom
Hard Disk (virtio0)	datastorage.vm-119-disk-0,size=32G
Network Device (net0)	virtio=52:55:20:F5:E0:4E,bridge=vibr99
Network Device (net1)	virtio=0E:4B:45:B9:F5:8A,bridge=vibr10
Network Device (net2)	virtio=1E:8F:E5:86:D7:09,bridge=vibr20
Network Device (net3)	virtio=76:4B:B8:4C:7E:7C,bridge=vibr32
Network Device (net4)	virtio=EA:4A:01:20:16:FA,bridge=vibr40

Pour la machine maître :

Virtual Machine 115 (DebianMaster) on node 'M2L'

Start Shutdown Console More Help

Add Remove Edit Disk Action Revert

Summary

Console

Hardware

Cloud-Init

Options

Task History

Monitor

Backup

Replication

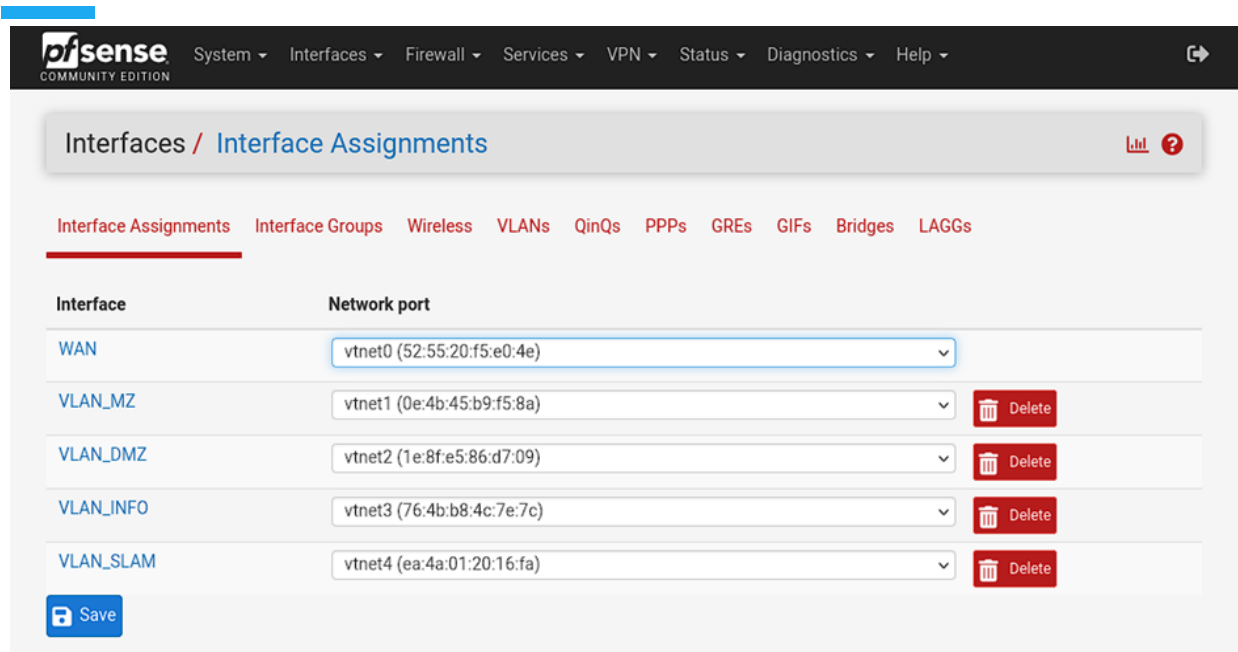
Snapshots

Firewall

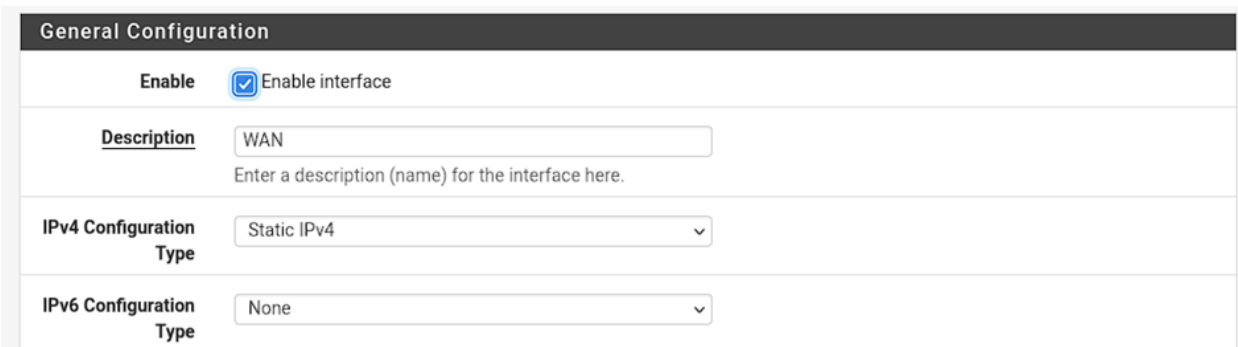
Permissions

Memory	4.00 GiB
Processors	2 (1 sockets, 2 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI
Hard Disk (virtio0)	datastorage.vm-115-disk-0,size=30G
Network Device (net0)	virtio=46:CA:14:D0:0C:3E,bridge=vibr10
Network Device (net1)	virtio=BE:ED:1F:51:85:96,bridge=vibr20
Network Device (net2)	virtio=5E:6E:16:FB:99:31,bridge=vibr32
Network Device (net3)	virtio=CA:81:5F:AD:24:CE,bridge=vibr40

Une fois notre pfSense installé et prêt à configurer, nous nous connectons via la machine maître et commençons par ajouter les interfaces de nos VMBRs :



Nous devons alors, pour chaque interfaces, les autoriser à fonctionner avec le bouton "Enable interface", les renommer, leur donner un adresse IPv4 ainsi qu'une ip de routage pour le WAN afin que la connexion à Internet soit établie :



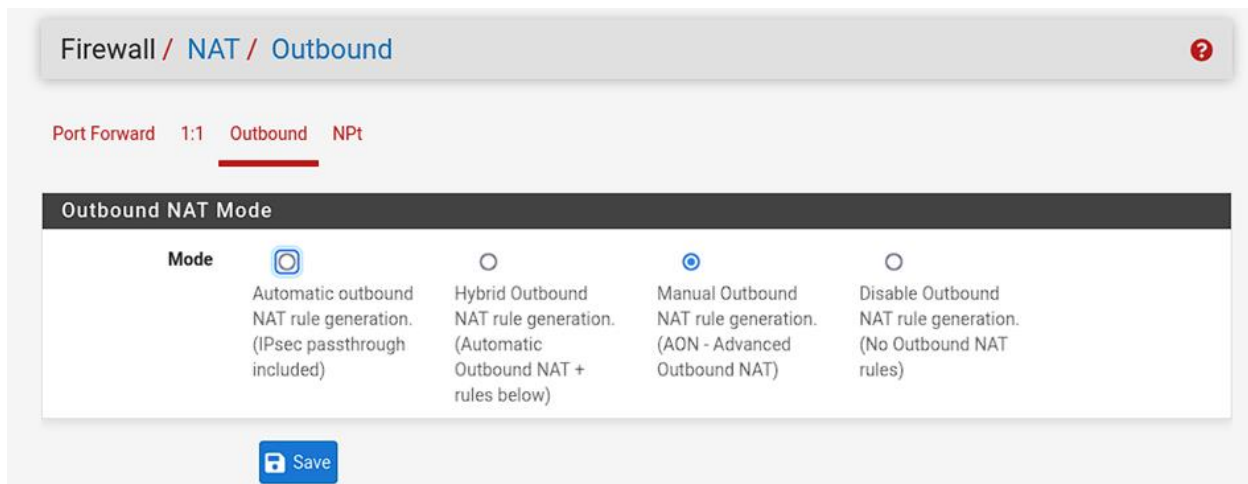
ici, pour l'interface du WAN

Chaque interfaces possédant sa propre adresse, nous avons fait comme suit :

- VLAN_MZ : 192.168.10.1
- VLAN_DMZ : 192.168.20.1
- VLAN_INFO : 192.168.32.1

- VLAN_SLAM : 192.168.40.1

Nous reste alors l'interconnexion entre nos VLANs et le WAN pour donner accès à Internet, pour ce faire nous allons dans "Firewall", "NAT" et "Outbound" puis nous passons en mode manuel :



Puis nous avons créé nos règles de transitions d'IPv4 propre à chaque VLANs :

Mappings										
<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	192.168.10.0/24	*	*	*	WAN address	*		VLAN_MZ to WAN	
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	192.168.20.0/24	*	*	*	WAN address	*		VLAN_DMZ to WAN	
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	192.168.32.0/24	*	*	*	WAN address	*		VLAN_INFO to WAN	
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	192.168.40.0/24	*	*	*	WAN address	*		VLAN_SLAM to WAN	

Il nous reste une dernière étape qui est la création de règles dans le pare-feu, il faut se rendre dans "Firewall" et "Rules" :

Firewall / Rules / WAN

Floating WAN VLAN_MZ VLAN_DMZ VLAN_INFO VLAN_SLAM

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4+6 *	WAN address	*	*	*	*	none		

ici une règle sur le réseau WAN permettant de tout autoriser en IPv4 et IPv6 afin de tester que le réseau sort bien

Plusieurs options sont disponibles lors de la création d'une règle :

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface WAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4+IPv6
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

Source

Source Invert match WAN address Source Address /

Destination

Destination Invert match any Destination Address /

- **Action** : permet de choisir entre autoriser ou bloquer
- **Disabled** : permet de désactiver la règle
- **Interface** : choix de l'interface sur laquelle la règle va s'appliquer
- **Adress Family** : IPv4, IPv6 ou les 2
- **Protocol** : choix du protocole, tel que UDP ou TCP
- **Source** : adresse ou réseau de provenance de notre règle
- **Destination** : adresse ou réseau de destination de notre règle

Les règles étant maintenant créées selon nos besoins, le réseau des VLANs est configuré. Il faut cependant noter qu'il faut créer des règles et les adapter à chaque besoin, l'exemple de règle pour le WAN vu précédemment n'était que pour tester le bon transit des paquets vers Internet.