

# RAPPORT DE PROJET

---



# SOMMAIRE

**01**

---

**MISE EN PLACE DE  
L'ENVIRONNEMENT**

**02**

---

**ROUTAGE INTER-  
VLAN ET ACL**

**03**

---

**CONFIGURATION  
NAT ET PROXY**

**04**

---

**DMZ ET SÉCURITÉ  
PÉRIMÉTRIQUE**

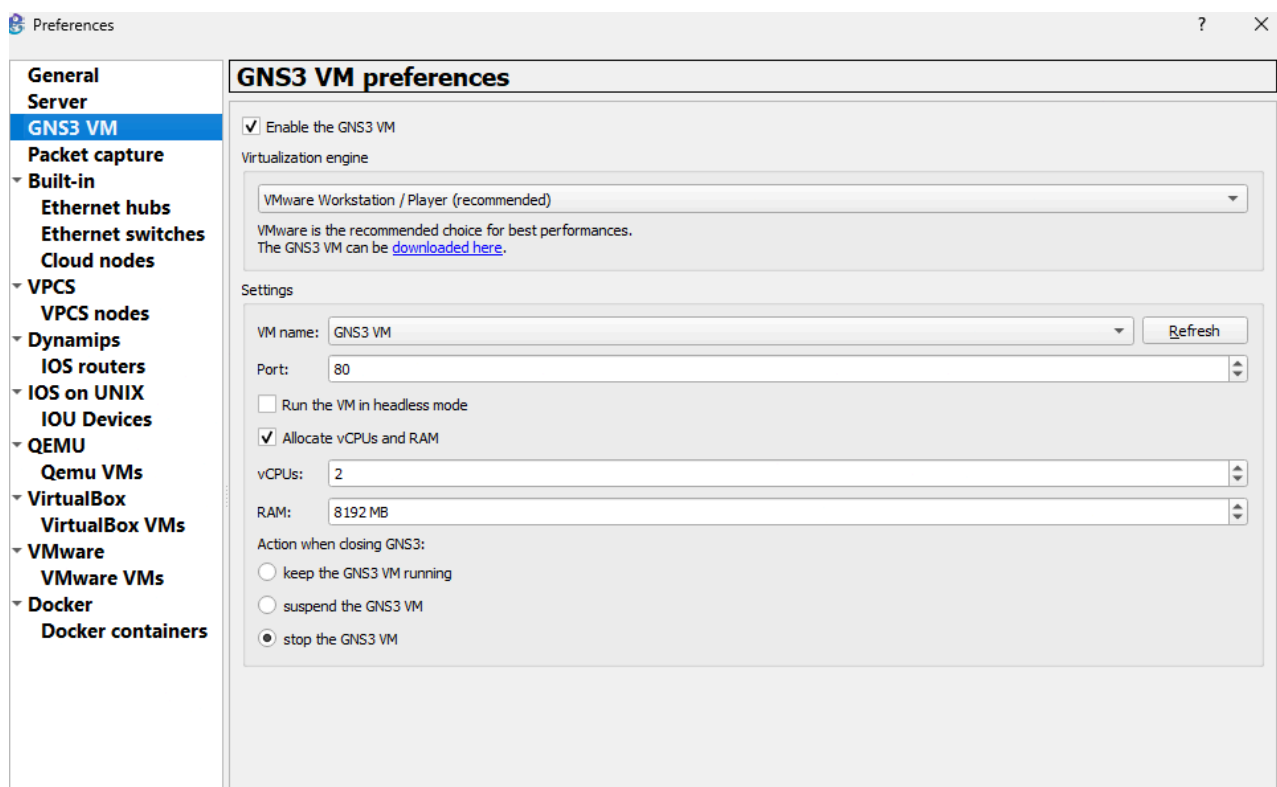
# Mise en place de l'environnement

## Installation

On commence par installer GNS3 pour windows sur <https://www.gns3.com/software/download> en se créant un compte.

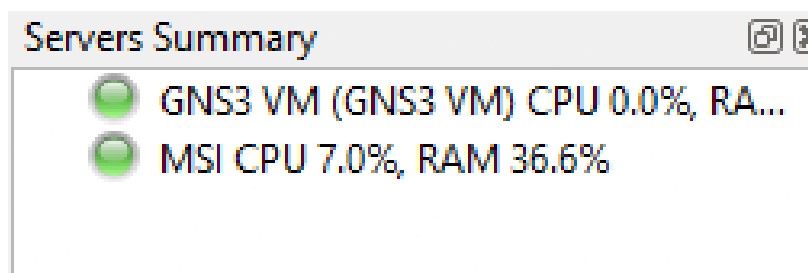
Ensuite on installe GNS3 VM pour VMware sur <https://www.gns3.com/software/download-vm>.

Une fois l'installation de GNS3 terminée, on se rend dans Edit > Préférences > GNS3 VM, on coche Enable the GNS3 VM, ensuite dans Virtualization engine on sélectionne VM Ware, puis on appuie sur le bouton Refresh et on sélectionne GNS3 VM, pour finir on appuie sur Apply et OK

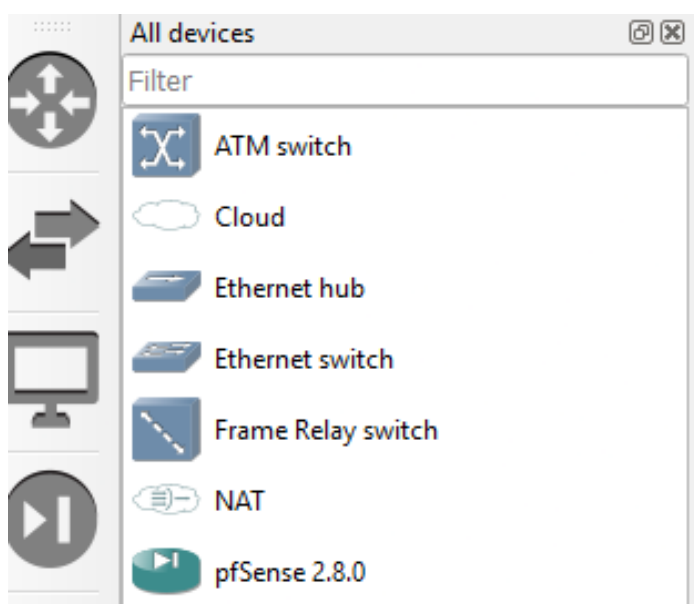


# Mise en place de l'environnement

On peut vérifier que la connexion entre notre machine virtuelle GNS3 VM et GNS3 en regardant en bas à droite si un rond vert apparaît devant le nom de la machine virtuelle.



Ensuite on installe **pfSense**, dans la listes de tous les dispositifs, on clique sur **New template**, puis on sélectionne la première options (**Install an appliance from the GNS3 server**), on se rend dans l'onglet Firewalls on clique sur pfSense on sélectionne /bin/qemu/-system-x86\_64(v8.0.4), installé plus tôt, ensuite on clique sur **Create a new version**, on marque le numéro de la version (**2.8.0**), et enfin on importe l'image de pfsense et on valide.

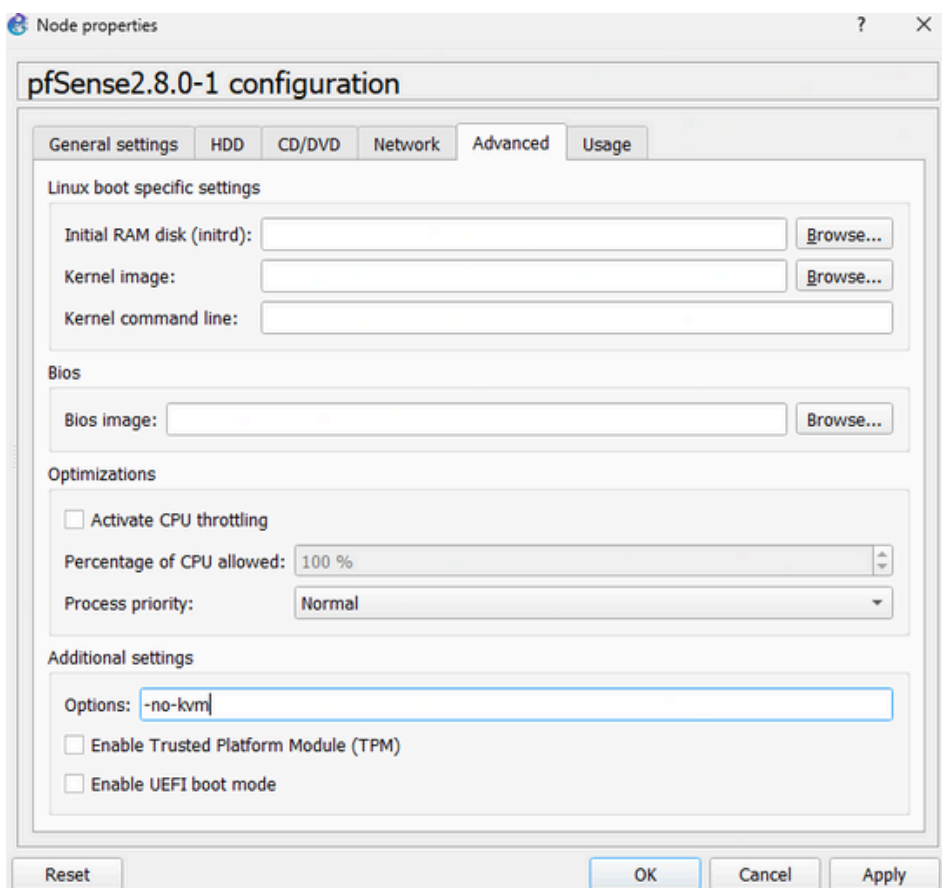


# Mise en place de l'environnement

01

## Erreur KVM

On glisse **pfSense** sur le tableau de bord et on le lance, a cette étape nous avons rencontré un problème **KVM**, pour y remédier nous avons été dans les **options** avancées de pfSense et à la ligne options nous avons écrit **-no-kvm**, ce qui a résolu le problème, après ça nous avons pu le lancer pour le configurer.



# Mise en place de l'environnement

01

## Configuration



webConfigurator

Protocol ☐ HTTP ☒ HTTPS (SSL/TLS)

SSL/TLS Certificate  Certificates known to be incompatible with use for HTTPS are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

TCP port  Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes

Après son lancement nous l'avons **configurer**, pour cela on a sélectionné l'interface réseau **em0** que nous avons laissé en dhcp qui nous sert de réseau WAN, puis l'interface réseau em1 que nous avons laissé en statique qui sera l'interface ou se trouvera notre **réseau LAN**, après cela nous avons d'abord relier l'interface **em0** a un **cloud**, mais nous n'arrivons pas a installer pfSense car ça bloquais, nous avons alors remplacé le cloud par un **NAT**, ce qui a résolu le problème ensuite nous avons pu finir d'installer pfSense.

Pour finir cet objectif nous avons **installer** le Switch de niveau 3

Configurer les interfaces réseau et l'adressage IP de base.

```
root@webterm-1:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=3.67 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=3.15 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2.52 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=2.57 ms
^C
```

```
root@webterm-1:~# 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=14.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=28.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=32.7 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 13.986/25.048/32.704/8.012 ms
```

# Routage inter-VLAN et ACL

02

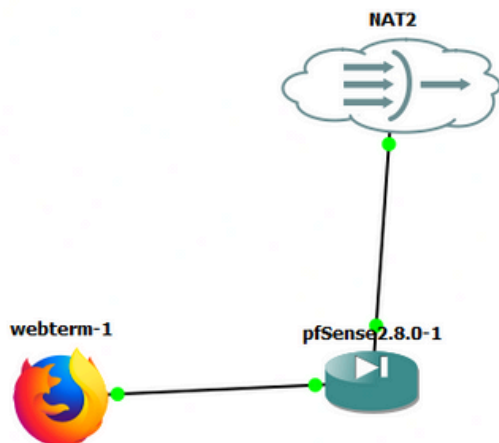
Après ça on peut accéder a pfSense en marquant 192.168.1.1 dans la barre de recherche de Firefox pour ensuite commencer la créations et la configurations des VLANs

Pour cela on se rend dans Interfaces puis VLANs on clique sur pour créer un VLAN,

En Parent Interface on met em1 (...) –lan, en VLAN Tag on met le numéro 10 pour le VLAN Admin et 30 pour le VLAN clients et en description le nom du VLAN

## Création et configuration des VLans

Pour configurer pfSense on relit un Webterm a l'interface em1 de pfSense.

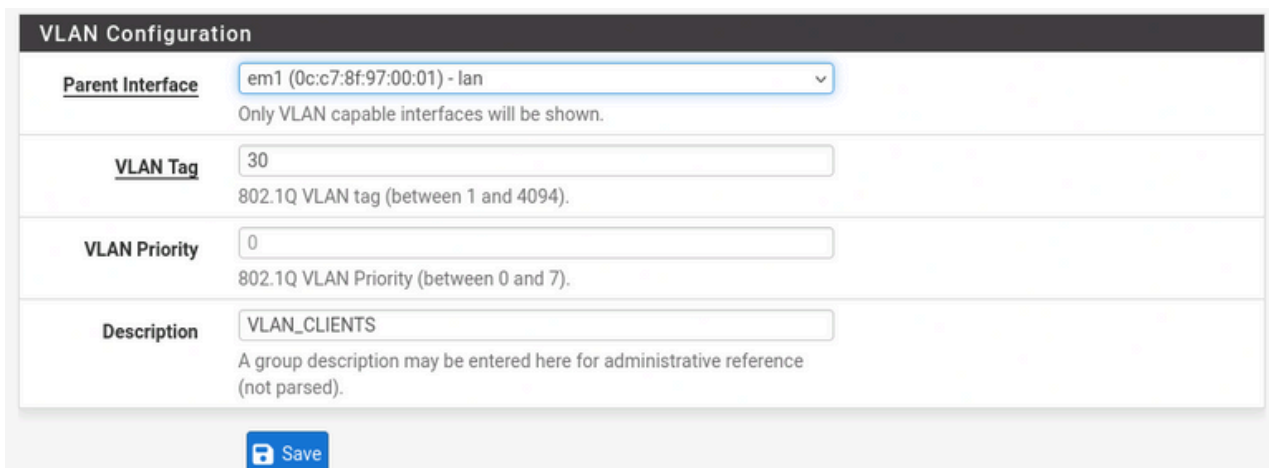


Dans le terminal du webterm on lui donne **192.168.1.50/24** comme adresse ip, **192.168.1.1** comme passerelle par défaut et 8.8.8.8 comme DNS.

```
root@webterm-1:~# ip addr add 192.168.1.50/24 dev eth0
root@webterm-1:~# ip route add default via 192.168.1.1
root@webterm-1:~# echo "nameserver 8.8.8.8" > /etc/resolv.conf
```

# Routage inter-VLAN et ACL

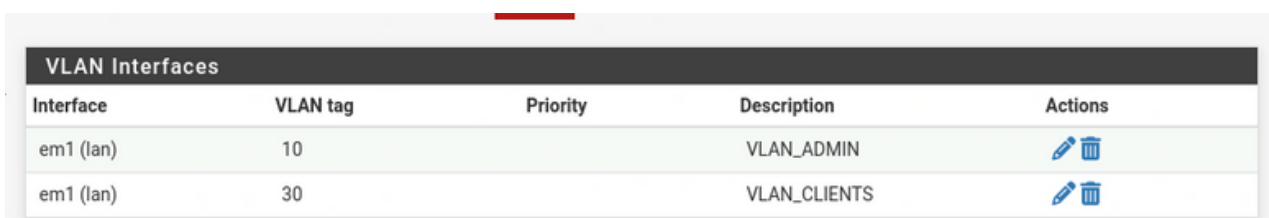
Pour commencer nous avons été dans la **console du Switch** et nous avons créé deux VLans (un Vlan est un sous réseau virtuel qui permet de **découper** un LAN physiques en plusieurs LAN logiques, pour **isoler** les différents domaines et réseaux et limiter le broadcast ), une nommé VLAN\_Admin et une nommé VLAN\_Clients.







The screenshot shows the 'VLAN Configuration' form. It includes a dropdown for 'Parent Interface' set to 'em1 (0c:c7:8f:97:00:01) - lan', a text input for 'VLAN Tag' set to '30', a text input for 'VLAN Priority' set to '0', and a text input for 'Description' set to 'VLAN\_CLIENTS'. A 'Save' button is at the bottom.

Field	Value
Parent Interface	em1 (0c:c7:8f:97:00:01) - lan
VLAN Tag	30
VLAN Priority	0
Description	VLAN_CLIENTS

Sur cette image on a créer le VLAN clients, on fait pareil pour le VLAN admin en changeant les valeurs expliquée plus haut.



VLAN Interfaces				
Interface	VLAN tag	Priority	Description	Actions
em1 (lan)	10		VLAN_ADMIN	 
em1 (lan)	30		VLAN_CLIENTS	 

On peut ensuite voir que les VLANs ont bien été créés.



# Routage inter-VLAN et ACL

02

## Configuration des VLans

The screenshot shows the 'Interface Assignments' tab in pfSense. It lists several interfaces: WAN, LAN, VLAN\_ADMIN, and VLAN\_CLIENTS. Each interface is assigned to a specific network port. The 'Available network ports' section at the bottom shows 'em4 (0c:87:57:c3:00:04)' with an 'Add' button.

Interface	Network port	Action
WAN	em0 (0c:87:57:c3:00:00)	
LAN	em1 (0c:87:57:c3:00:01)	Delete
VLAN_ADMIN	VLAN 10 on em1 - lan (VLAN_ADMIN)	Delete
VLAN_CLIENTS	VLAN 30 on em1 - lan (VLAN_CLIENTS)	Delete
Available network ports:	em4 (0c:87:57:c3:00:04)	+ Add

The screenshot shows the 'General Configuration' tab for the 'VLAN\_CLIENTS' interface. It includes fields for 'Enable', 'Description', 'IPv4 Configuration Type', 'IPv6 Configuration Type', 'MAC Address', 'MTU', 'MSS', and 'Speed and Duplex'. The 'Static IPv4 Configuration' section is also visible at the bottom.

**General Configuration**

**Enable** ☐ Enable interface

**Description**   
Enter a description (name) for the interface here.

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**MAC Address**   
This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.

**MTU**   
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

**MSS**   
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

**Speed and Duplex**   
Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

**Static IPv4 Configuration**

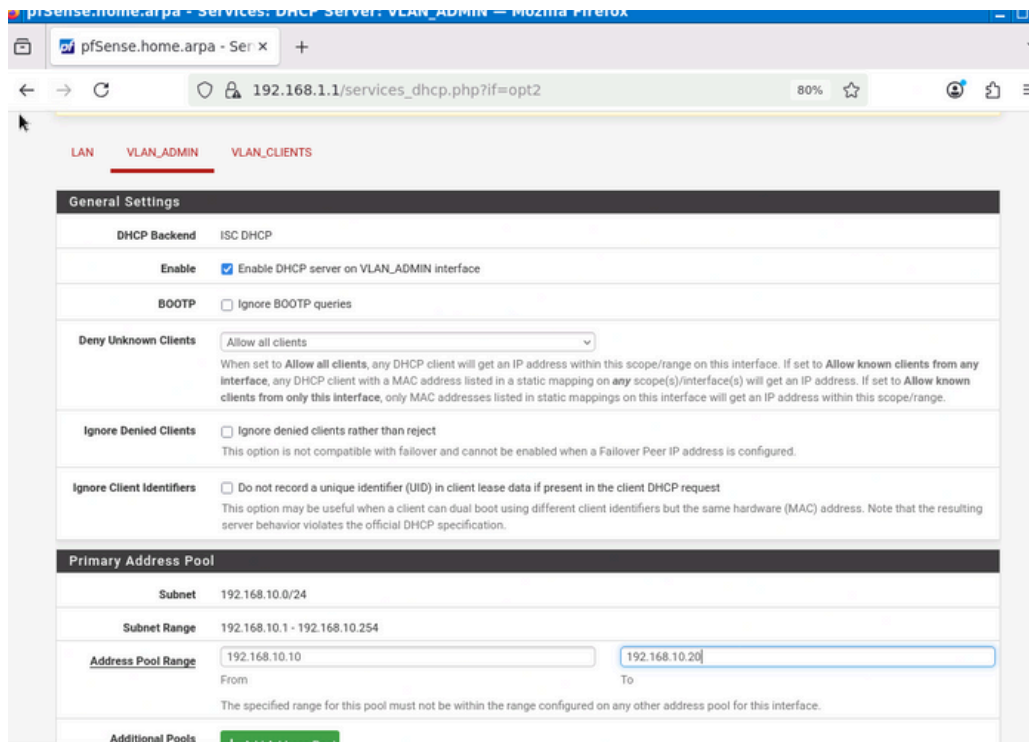
**IPv4 Address**  / 32

Sur cette image on a configuré le VLAN\_Clients et on a fait de même pour le VLAN\_Admin en changeant la description par VLAN\_Admin et l'IPv4 Address par 192.168.10.1

Puis on finit la configuration pfSense en configurant le DHCP sur chaque VLAN, pour cela on se rend dans services dhcp et pour chaque VLAN on coche l'option **Enable DHCP server** on VLAN\_ADMIN (ou VLAN\_CLIENTS selon les VLAN qu'on configure) interface et dans Address Pool Range on configure la plage ip du dhcp de 192.168.x.10 à 192.168.x.20 (x -> numéro du VLAN, 10 pour VLAN\_ADMIN et 30 pour VLAN\_CLIENT).

# Routage inter-VLAN et ACL

02

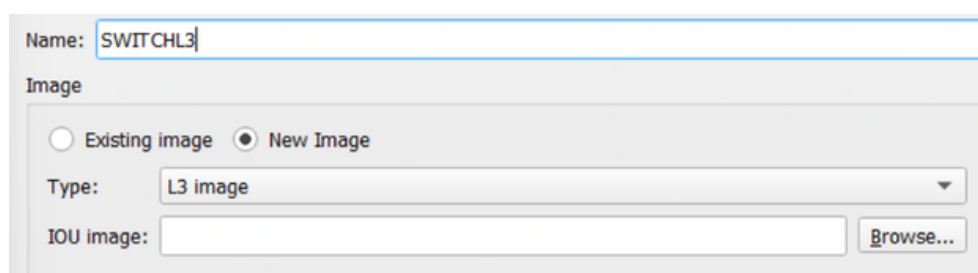


Après avoir créer et configurer les VLans sur pfSense on les créer et les configures aussi sur le switch de niveau 3 depuis son terminal.

On commence par télécharger le switch de niveau 3 avec l'image :



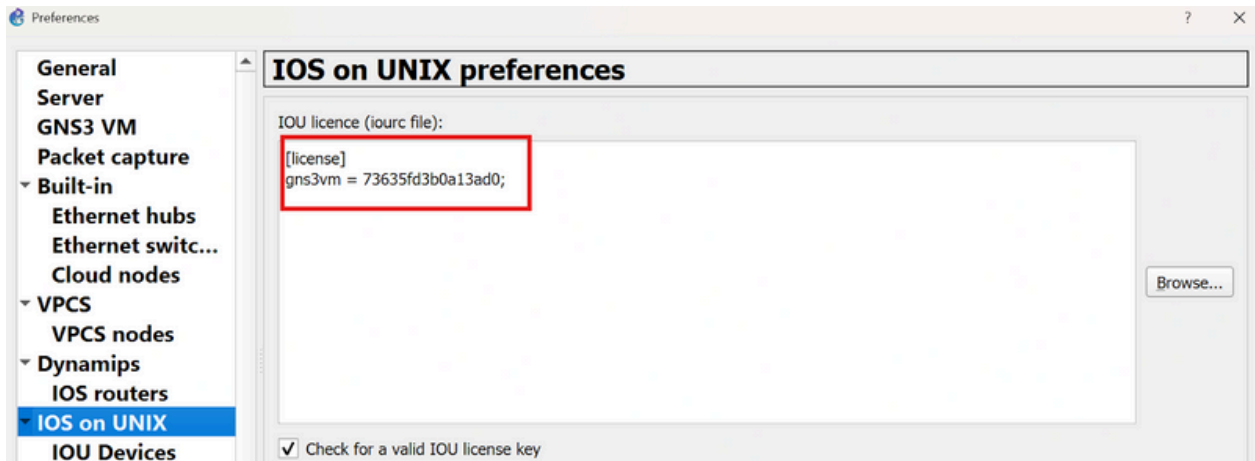
Aller dans IOU devices > new et sélectionnez l'image



# Routage inter-VLAN et ACL

02

Et enfin mettre la license :



Pour cela, on tape cette suite commande :

- conf t
- vlan 10
- name VLAN\_Admin
- exit

Puis on fait de même pour créer le Vlan clients :

- vlan 30
- name VLAN\_Client
- exit
- exit

On peut faire la commande show vlan pour voir les VLAN qu'on vient de mettre en place.

```
SWITCH-LAN#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Et0/0, Et0/1, Et0/2, Et0/3 Et1/0, Et1/1, Et1/2, Et1/3
10	VLAN_Admin	active	
30	VLAN_Clients	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Primary	Secondary	Type	Ports
---------	-----------	------	-------

# Routage inter-VLAN et ACL

Ensuite on configure la liaison entre pfSense et le switch en mode trunk :

```
SWITCH-LAN(config)#int et0/0
SWITCH-LAN(config-if)#switchport trunk encapsulation dot1q
SWITCH-LAN(config-if)#switchport mode trunk
SWITCH-LAN(config-if)#switchport trunk allowed vlan 10,30
SWITCH-LAN(config-if)#desc Trunk vers pfSense
SWITCH-LAN(config-if)#exit
SWITCH-LAN(config)#exit
SWITCH-LAN#
*Nov  2 20:41:50.156: %SYS-5-CONFIG_I: Configured from console by console
SWITCH-LAN#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 2008 bytes to 1112 bytes[OK]
```

Nous allons alors tenter d'obtenir une adresse ip avec le dhcp que nous venons configurer avec la commande **ip dhcp**,  
Depuis le pc situer sur le Vlan admin :

```
ip dhcp
DDORA IP 192.168.10.10/24 GW 192.168.10.1
PC1>
```

Et depuis le **pc** situé sur le Vlan clients :

```
ip dhcp
DDORA IP 192.168.30.10/24 GW 192.168.30.1
PC1>
```

# Routage inter-VLAN et ACL

02

Ensuite nous avons mis en place des règles de filtrage pour pouvoir avoir accès au vlan clients depuis le **VLAN\_ADMIN** mais pas l'inverse. Pour cela nous avons configuré des règles de base Pour avoir un accès complet au sein de chaque vlan, puis nous avons mis en place une règle qui bloque la connexion du **VLAN\_CLIENTS** vers le VLAN admin en faisant comme sur les images ci dessous :

**Edit Firewall Rule**

**Action**   
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**   
Choose the interface from which packets must come to match this rule.

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

**Protocol**   
Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match   /

**Destination**

**Destination** ☐ Invert match   /

**Extra Options**

**Log** ☐ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**   
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the

Sur cette image nous avons configuré l'accès complet au sein du Vlan admin, nous avons fait exactement pareil pour le Vlan client en changeant seulement l'interface par **VLAN\_CLIENTS** et la source par **VLAN\_CLIENTS** subnets et pour commentaire « **Clients FULL ACCESS** »

# Routage inter-VLAN et ACL

02

**Edit Firewall Rule**

**Action:** Block  
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:** VLAN\_CLIENTS  
Choose the interface from which packets must come to match this rule.

**Address Family:** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol:** Any  
Choose which IP protocol this rule should match.

**Source:**  
☐ Invert match VLAN\_CLIENTS subnets Source Address /

**Destination:**  
☐ Invert match VLAN\_ADMIN subnets Destination Address /

**Extra Options**

**Log:** ☐ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description:** Bloque VLAN\_CLIENTS -> VLAN\_ADMIN

Et sur cette image nous pouvons voir la configuration que nous avons réalisées pour bloquer la connexion du VLANs clients vers le VLAN admin.

Nous pouvons donc voir avec les images qui suivent que les règles ont bien été configurées :

Floating WAN LAN **VLAN\_ADMIN** VLAN\_CLIENTS

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗	0/0 B	IPv4 *	VLAN_CLIENTS subnets	*	VLAN_ADMIN subnets	*	*	none	Bloque VLAN_CLIENTS -> VLAN_ADMIN	
<input type="checkbox"/>	✓	0/0 B	IPv4 *	VLAN_CLIENTS subnets	*	*	*	*	none	Clients FULL ACCESS	

Floating WAN LAN **VLAN\_ADMIN** VLAN\_CLIENTS

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	VLAN_ADMIN subnets	*	*	*	*	none	Admin FULL ACCESS	

# Routage inter-VLAN et ACL

Pour finir nous avons testé la communication et le filtrage, pour cela nous avons fait un ping depuis un Vlan vers un autre, sur la première image on voit bien que depuis le **VLAN\_Admin(192.168.10.1)** on peut ping le **VLAN\_Clients(192.168.30.1)**.

```
PC2> ping 192.168.30.11
84 bytes from 192.168.30.11 icmp_seq=1 ttl=63 time=6.844 ms
84 bytes from 192.168.30.11 icmp_seq=2 ttl=63 time=5.089 ms
```

A l'inverse sur cette deuxième image nous voyons que nous ne pouvons pas faire l'inverse ( depuis le **VLAN\_Clients** on ne peut pas ping le **VLAN\_Admin**).

```
PC1> ping 192.168.10.10
192.168.10.10 icmp_seq=1 timeout
192.168.10.10 icmp_seq=2 timeout
```

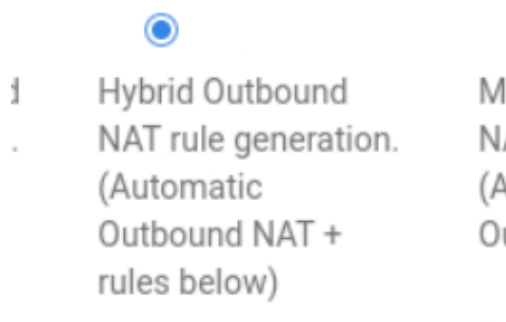
# Configuration

## NAT et Proxy

03

### Configuration du NAT

Pour configurer le NAT on se rend dans **Firewall > NAT > onglet "Outbound"** et on sélectionne **Hybrid Outbound...**



Ensuite on se rend dans **Port Forward** et on fait:

☒ Disabled ☐ Disable this rule

**No RDR (NOT)** ☐ Disable redirection for traffic matching this rule  
This option is rarely needed. Don't use this without thorough knowledge of the implications.

**Interface** DMZ  
Choose which interface this rule applies to. In most cases "WAN" is specified.

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

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

**Source** Hide Advanced

**Source** ☐ Invert match. DMZ subnets Type Address/mask

**Source port range** Any From port Custom Any To port Custom  
Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be 'any'). The 'to' field may be left empty if only filtering a single port.

**Destination** ☒ Invert match. This Firewall (self) Type Address/mask

**Destination port range** HTTPS From port Custom HTTPS To port Custom  
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

**Redirect target IP** Address or Alias 127.0.0.1 Type Address  
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4  
In case of IPv6 addresses, in must be from the same "scope".  
i.e. it is not possible to redirect from link-local addresses scope (fe80::) to local scope (::1)

**Redirect target port** Other 3129 Port Custom

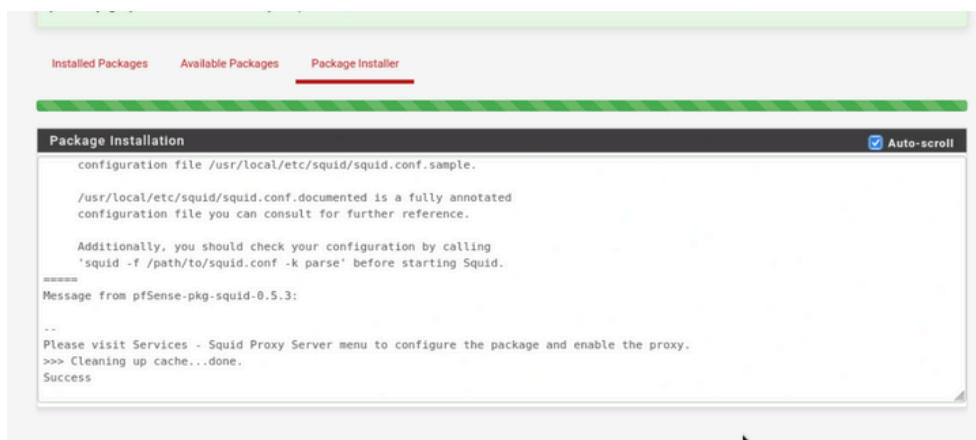


# Configuration NAT et Proxy

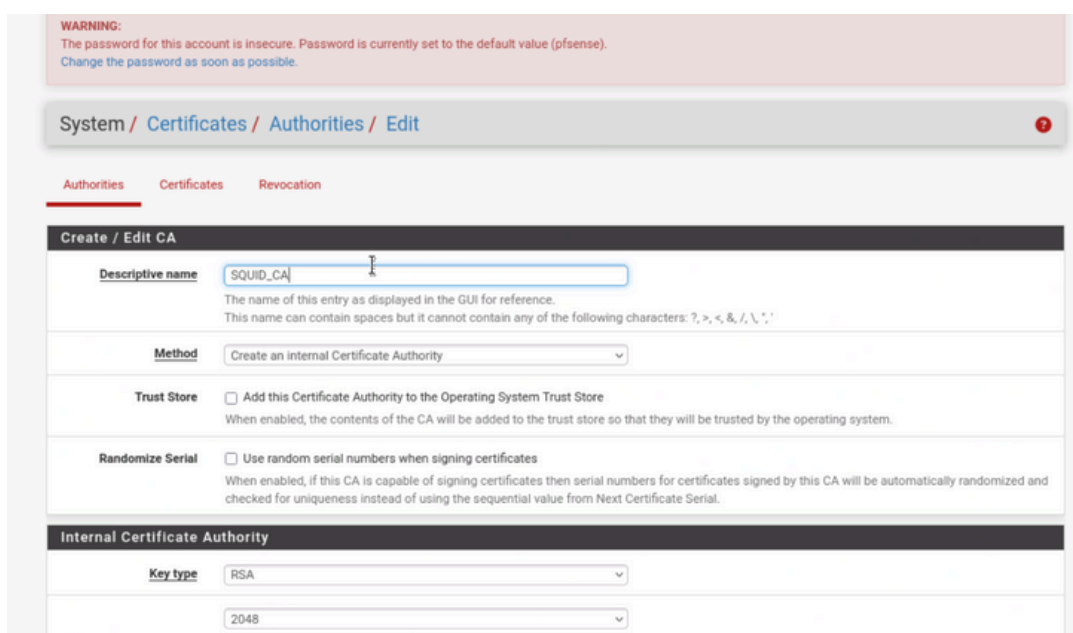
03

## Installation et configuration du proxy Squid:

Pour installer Squid depuis pfSense nous avons fait **Services > Packet Manager > Available > squid > download**



Une fois squid fini d'installer on vas créer une certification d'autorisation pour Squid, pour ça on se rend sur **System > Certificates > Authorities > Edit**, puis dans **Descriptive Name** on écrit **SQUID\_CA** et dans méthode on sélectionne **Create an internal Certificate Authority**



# Configuration

## NAT et Proxy

Après nous avons pus commencer à configurer Squid, pour cela nous avons été dans **Services > Squid Proxy Server > General** puis nous avons

### Squid General Settings

Enable Squid Proxy

☒ Check to enable the Squid proxy.  
**Important:** If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data

☒ If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.  
**Important:** If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

Listen IP Version

IPv4  
 Select the IP version Squid will use to select addresses for accepting client connections.

CARP Status VIP

none  
 Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.  
**Important:** Don't forget to generate Local Cache on the secondary node and configure **XMLRPC Sync** for the settings synchronization.

Proxy Interface(s)

WAN  
 LAN  
 DMZ  
 VLAN\_ADMIN

 The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

Outgoing Network Interface

Default (auto)  
 The interface the proxy server will use for outgoing connections.

Proxy Port

3128  
 This is the port the proxy server will listen on. Default: 3128

ICP Port

This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

Allow Users on Interface

☒ If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.

### Transparent Proxy Settings

Transparent HTTP Proxy

☒ Enable transparent mode to forward all requests for destination port 80 to the proxy server.  
 Transparent proxy mode works without any additional configuration being necessary on clients.  
**Important:** Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.  
**Hint:** In order to proxy both HTTP and HTTPS protocols **without intercepting SSL connections**, configure WPAD/PAC options on your DNS/DHCP servers.

Transparent Proxy Interface(s)

WAN  
 LAN  
 DMZ  
 VLAN\_ADMIN

 The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.

Bypass Proxy for Private Address Destination

☒ Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations. Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.

Bypass Proxy for These Source IPs

Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall. **Applies only to transparent mode. Separate entries by semi-colons (;)**

Bypass Proxy for These Destination IPs

Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. **Applies only to transparent mode. Separate entries by semi-colons (;)**

### SSL Man In the Middle Filtering

HTTPS/SSL Interception

☒ Enable SSL filtering.

SSL/MITM Mode

Splice All  
 The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled. Default: Splice Whitelist, Bump Otherwise. **Click Info for details.**

SSL Intercept Interface(s)

WAN  
 LAN  
 DMZ  
 VLAN\_ADMIN

 The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.

SSL Proxy Port

3129  
 This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129

SSL Proxy Compatibility Mode

Modern  
 The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. **Click Info for details.**

DHParams Key Size

2048 (default)  
 DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.

CA

SQUID\_CA  
 Select Certificate Authority to use when SSL interception is enabled.

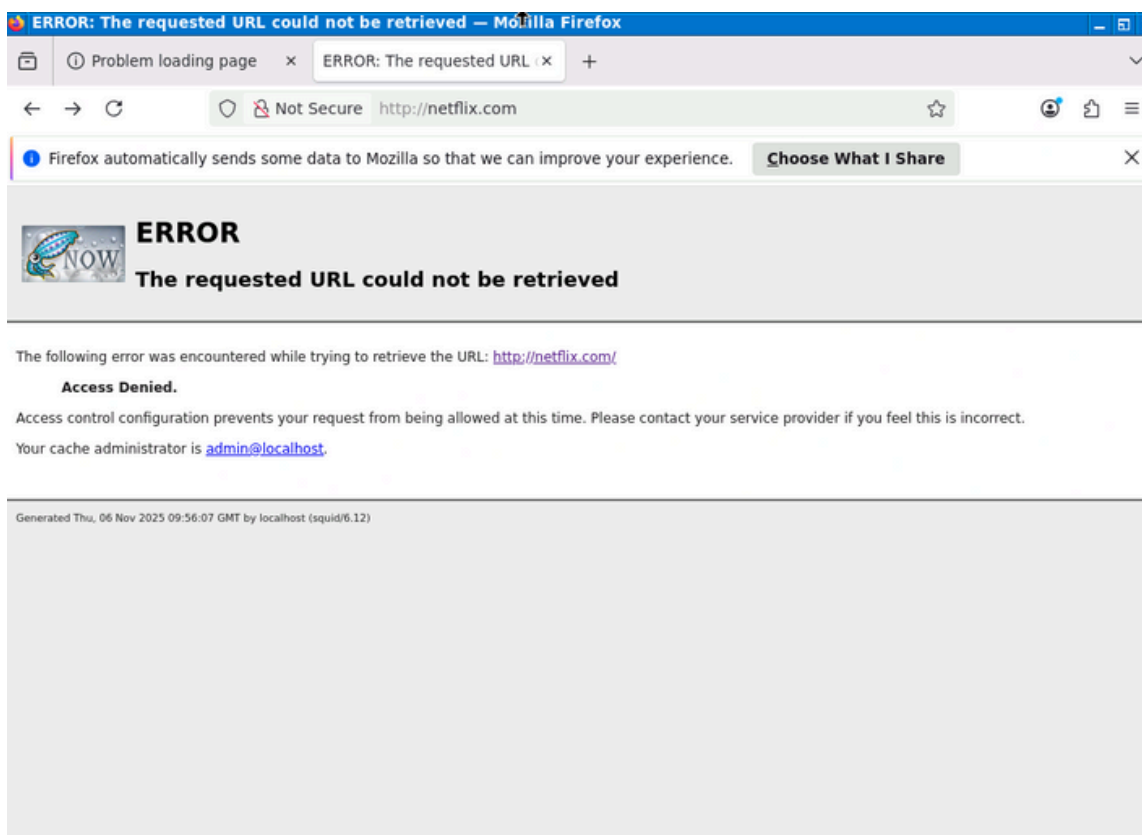
# Configuration NAT et Proxy

03

Puis on a ajouter des sites internet dans la **Blacklist**, comme par exemple netflix.com



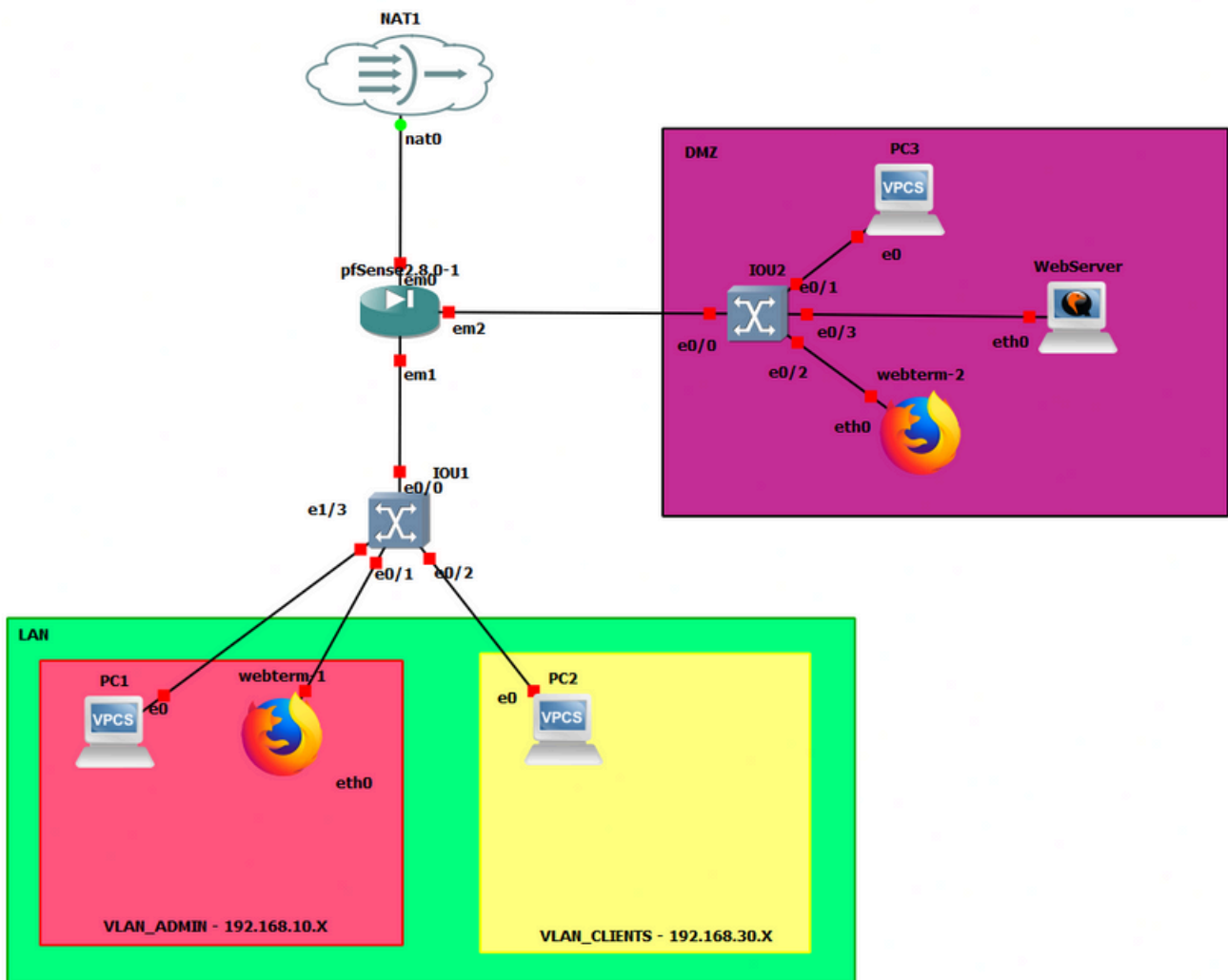
Après avoir blacklisté netflix.com on a tenté d'y accéder mais nous n'y êtes pas parvenu ce qui prouve que le filtrage est fonctionnel.



# DMZ et sécurité périmétrique

04

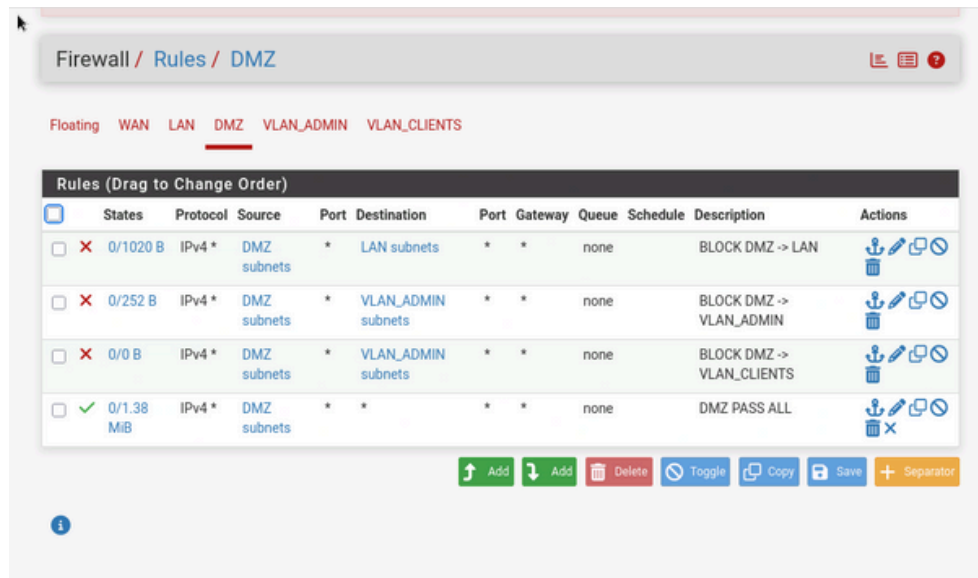
## DMZ



Nous avons ensuite rajouté un **switch** qui s'occupera de la **DMZ**, et ensuite un **serveur web** avec apache, un **pc** et un **webterm** pour effectuer des tests.

# DMZ et sécurité périmétrique

04



Nous **bloquons** toute requête venant de la **DMZ** au **LAN**, et aux **VLANs**. Et les VLANs Admin et Clients peuvent communiquer avec la DMZ.

```
PC3> ip dhcp
DDORA IP 192.168.90.10/24 GW 192.168.90.1

PC3> ping 192.168.10.10
192.168.10.10 icmp_seq=1 timeout
192.168.10.10 icmp_seq=2 timeout
192.168.10.10 icmp_seq=3 timeout
192.168.10.10 icmp_seq=4 timeout
192.168.10.10 icmp_seq=5 timeout

PC3> █
```

```
PC1>
PC1> ping 192.168.90.10
84 bytes from 192.168.90.10 icmp_seq=1 ttl=63 time=3.789 ms
84 bytes from 192.168.90.10 icmp_seq=2 ttl=63 time=2.714 ms
84 bytes from 192.168.90.10 icmp_seq=3 ttl=63 time=3.337 ms
84 bytes from 192.168.90.10 icmp_seq=4 ttl=63 time=3.138 ms
84 bytes from 192.168.90.10 icmp_seq=5 ttl=63 time=15.614 ms

PC1> █
```

Nous pouvons **vérifier** que la DMZ est bien isolée avec les pings, le PC1 de la VLAN\_ADMIN peut communiquer avec la DMZ mais pas l'inverse.

# MERCI !

---