27/10 - 07/11

Guardia CS

RAPPORT DE PROJET

(ANONYME),
(ANONYME),
Tim (ANONYME)

UE1-3 Techniques de sécurisation ISR

SOMMAIRE

Mise en place de l'environement

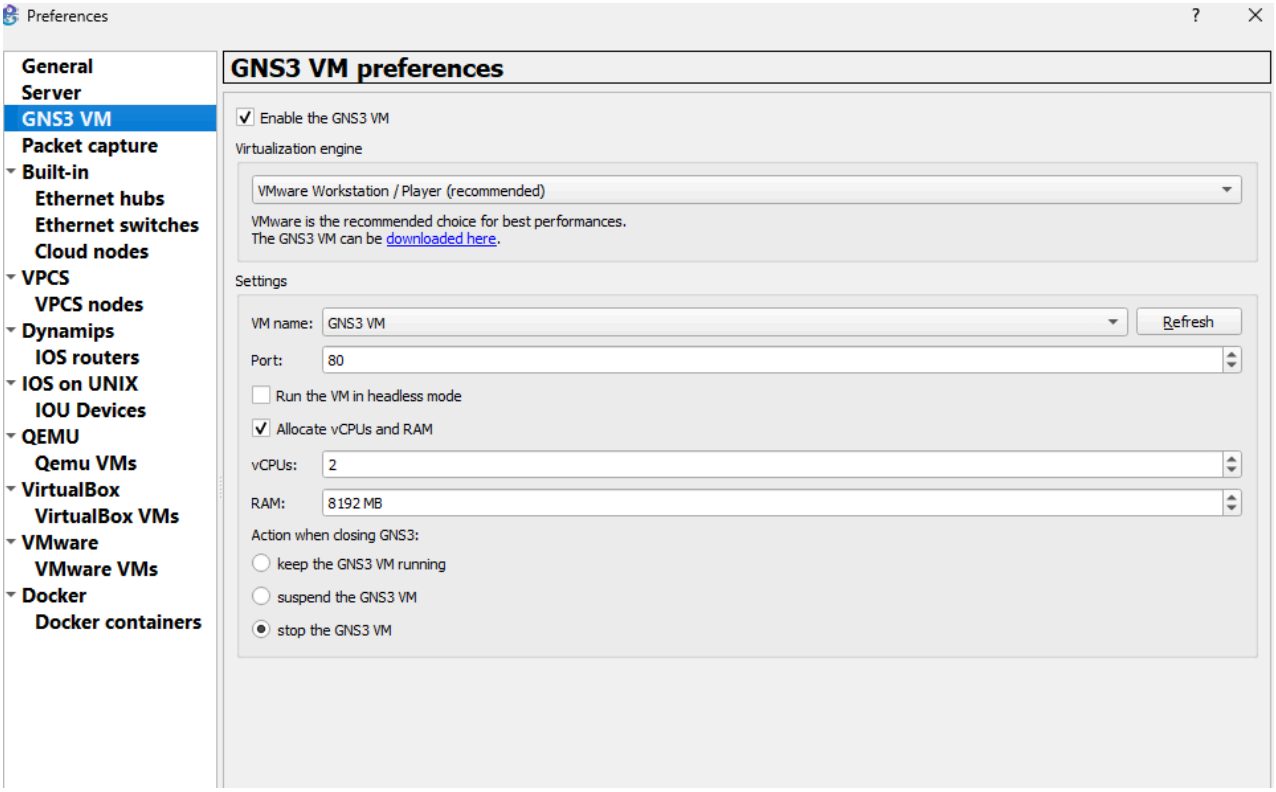
01

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.

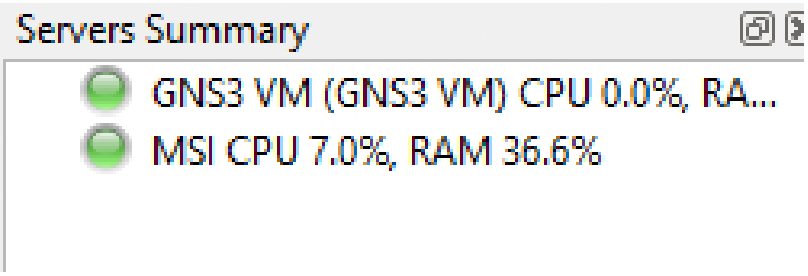
Une fois l'installation de GNS3 terminé, on se rend dans Edit > Préférences > GNS3 VM, on coche Enable the GNS3 VM, ensuite dans Virtualization engine on selection VM Ware, puis on appuie sur le bouton Refresh et on sélectionne GNS3 VM, pour finir on appuie sur Apply et OK



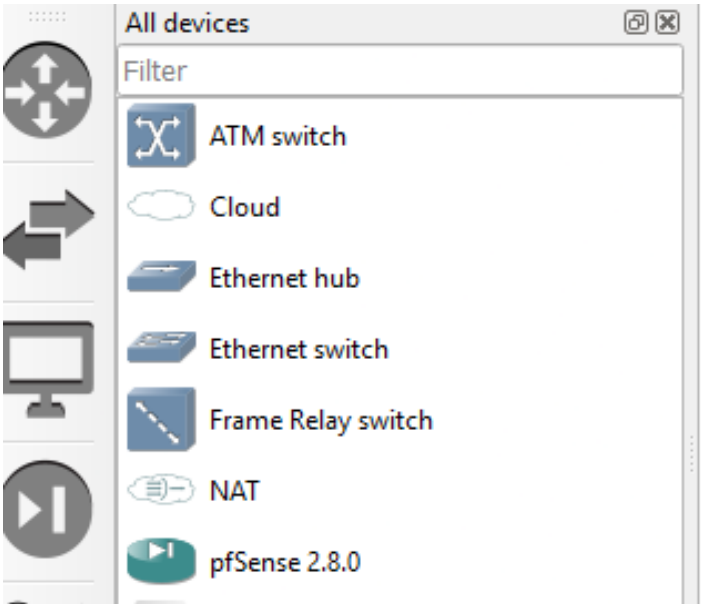
Mise en place de l'environement

01

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.

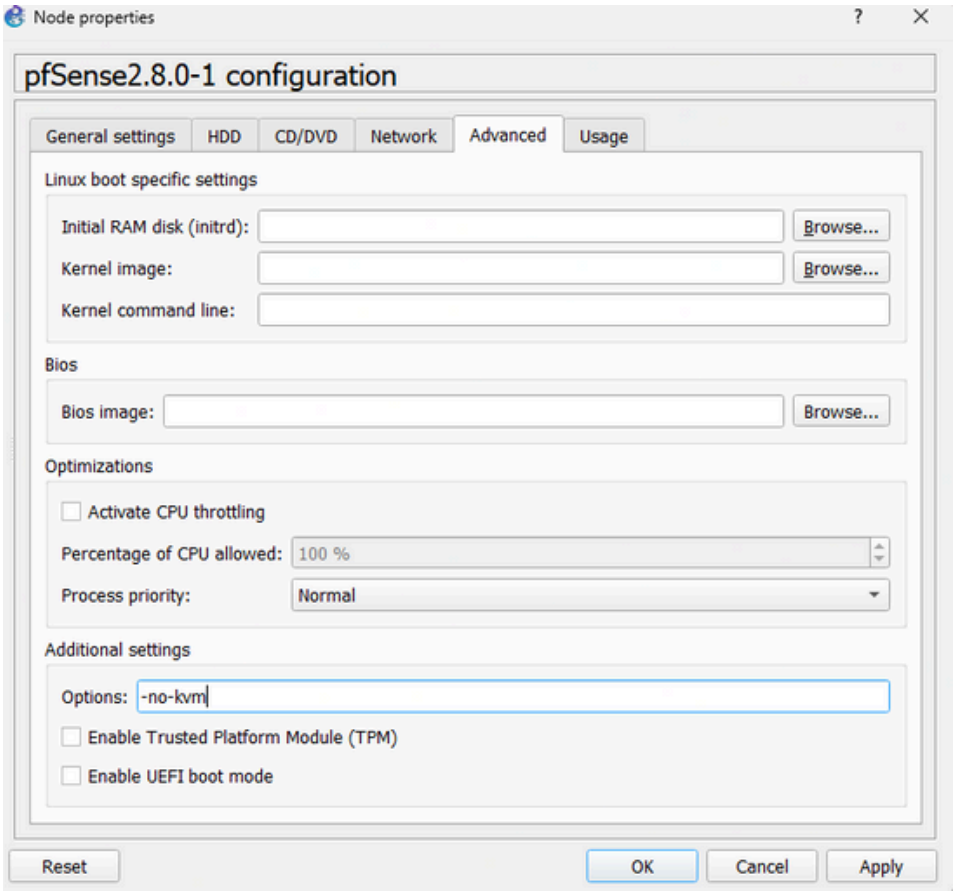


Mise en place de l'environement

01

Erreur KVM

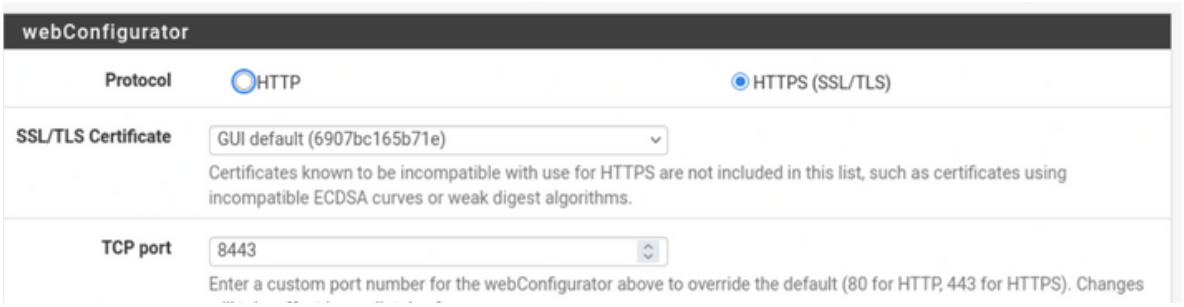
On glisse **pfSense** sur le tableau de bord et on le lance, a cette étape nous avons rencontré un problème **KVM**, pour y remédier nous avons été dans les **options** avancées de pfSense et à la ligne options nous avons écrit **—no-kvm**, ce qui a résolu le problème, après ça nous avons pu le lancer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



Mise en place de l'environement

01

Configuration



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
```

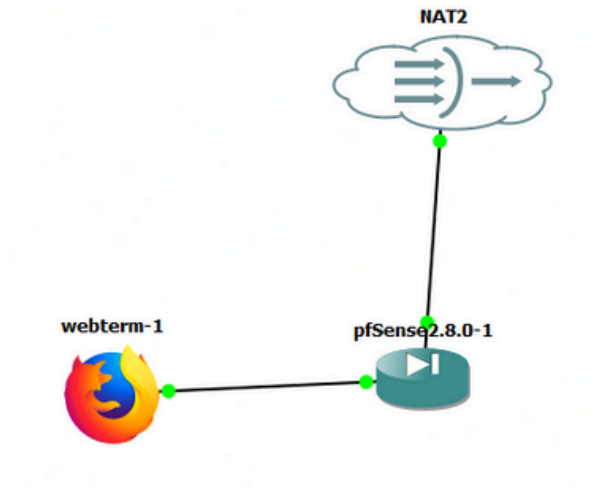
Routage inter-VLAN et ACL

Après ça on peut accéder a pfSense en marquant 192.168.1.1 dans la barre de recherche de Firefox pour ensuit 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.

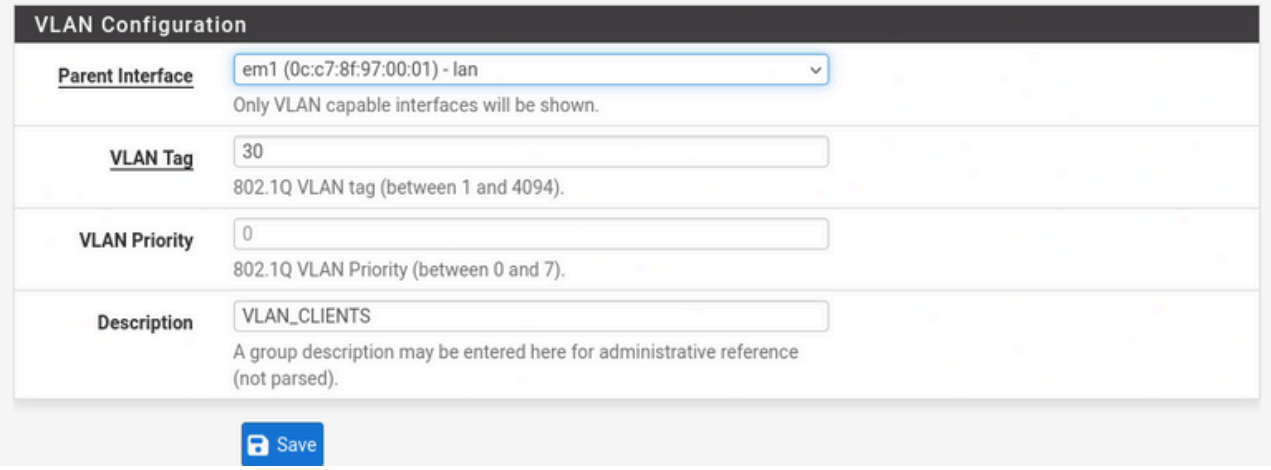


Dans le terminal du webterm on lui donne **192.168.1.50/24** comme adresse ip, **192.168.1.1** comme passerelle pare défaut et 8.8.8.8 comme DNS.

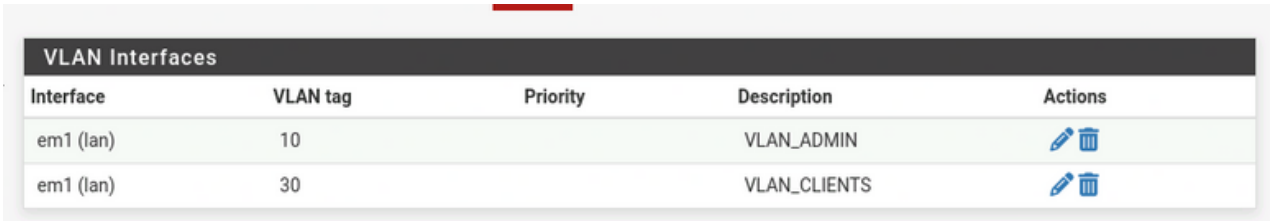
```
root@webterm-1:~# ip addr add 192.168.1.50/24 dev eth0
root@webterm-1:~# ip route add default via 192.168.1.1
root@webterm-1:~# echo "nameserver 8.8.8.8" > /etc/resolv.conf
```

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.



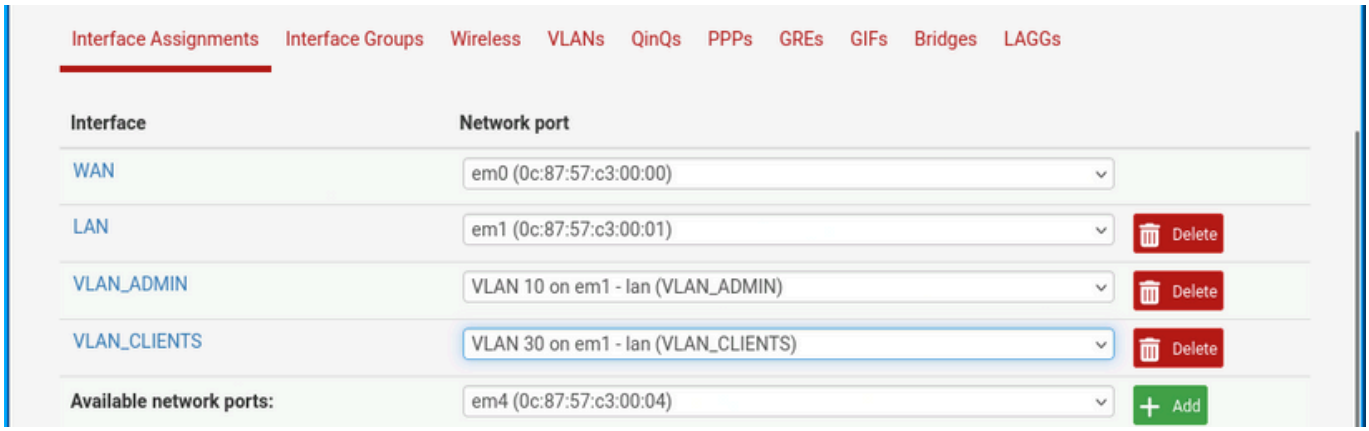
Sur cette image on a créer le VLAN clients, on fait pareil pour le VLAN admin en changeant les valeurs expliqué plus haut.

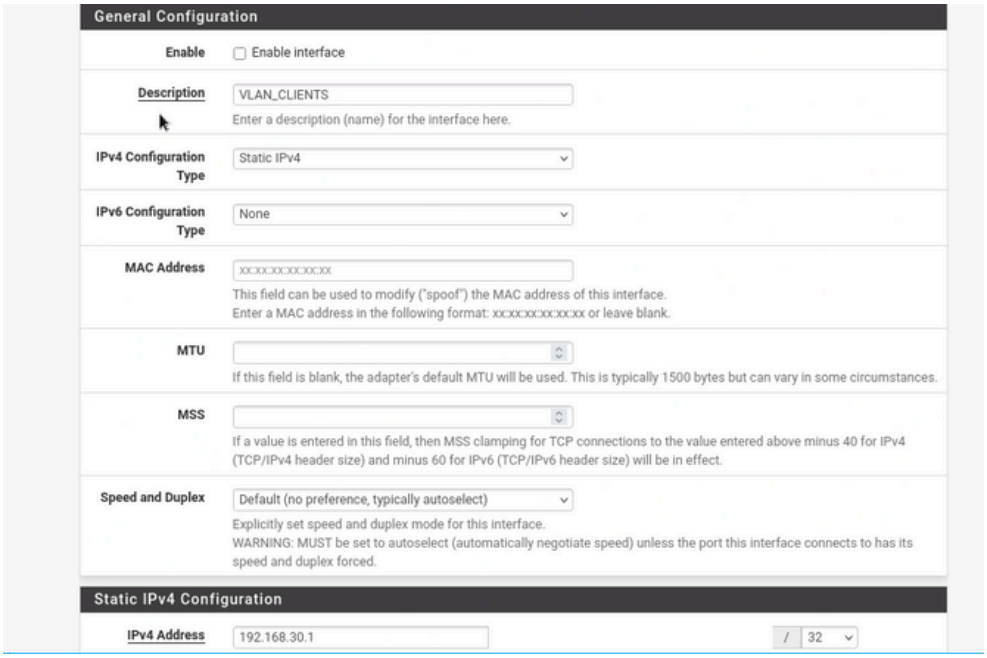


On peut ensuite voir que les VLANs ont bien étés créés.

Routage inter-VLAN et ACL

Configuration des VLans

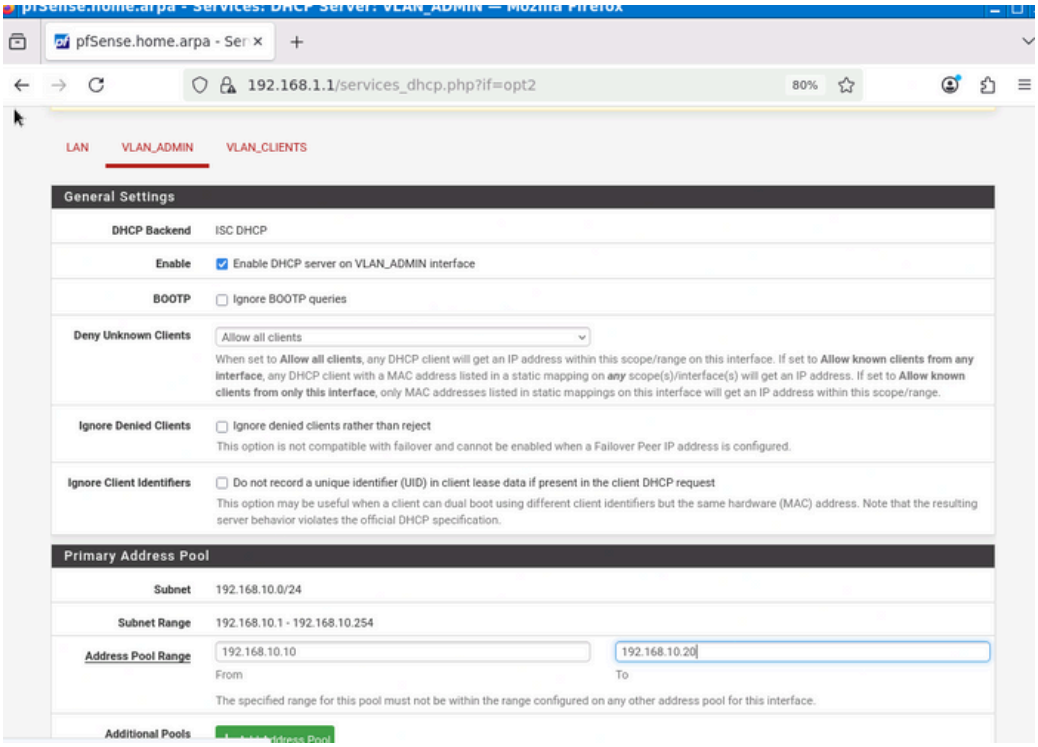




Sur cette image on a configuré le VLAN_Clients et on a fait de même pour le VLAN_Admin en changeant la description par VLAN_Admin et l'IPv4 Address par 192.168.10.1

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).

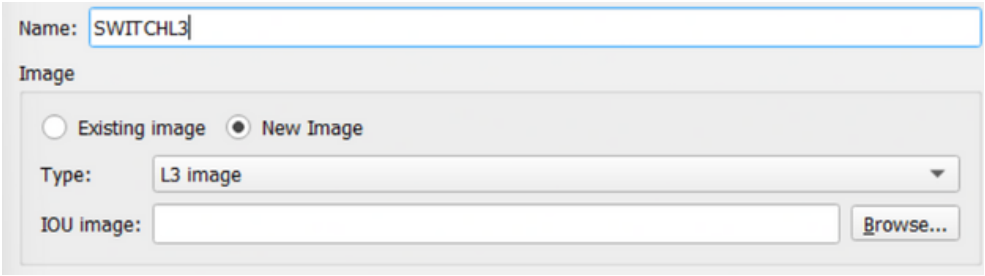
Routage inter-VLAN et ACL



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.

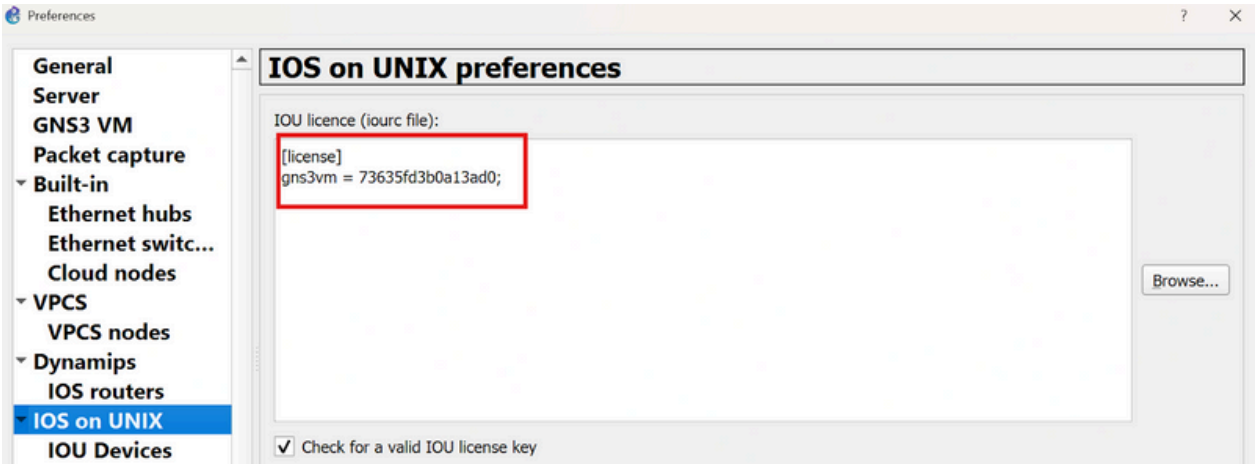
On commence par télécharger le switch de niveau 3 avec l'image :

Aller dans IOU devices > new et sélectionnez l'image



Routage inter-VLAN et ACL

Et enfin mettre la license :



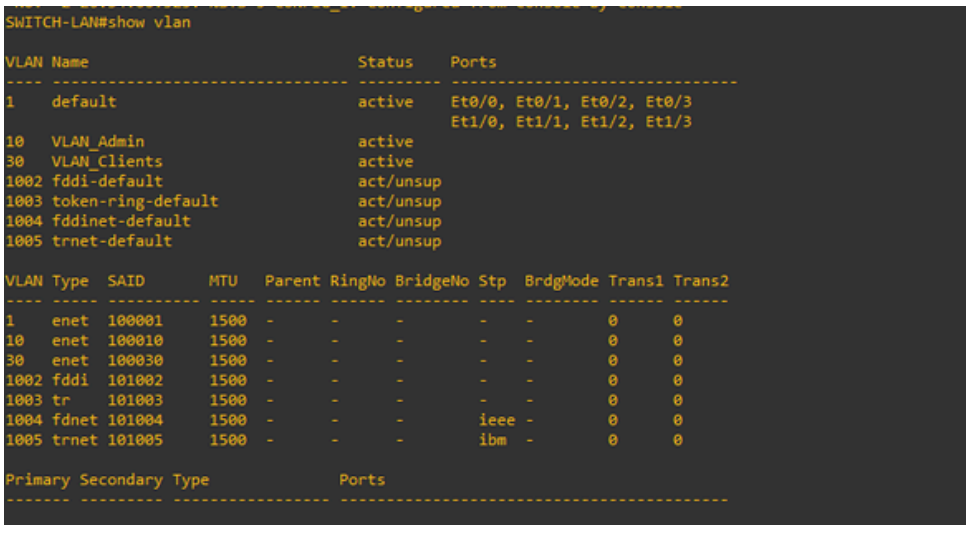
Pour cela, on tape cette suite commande :

- 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.



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>
```

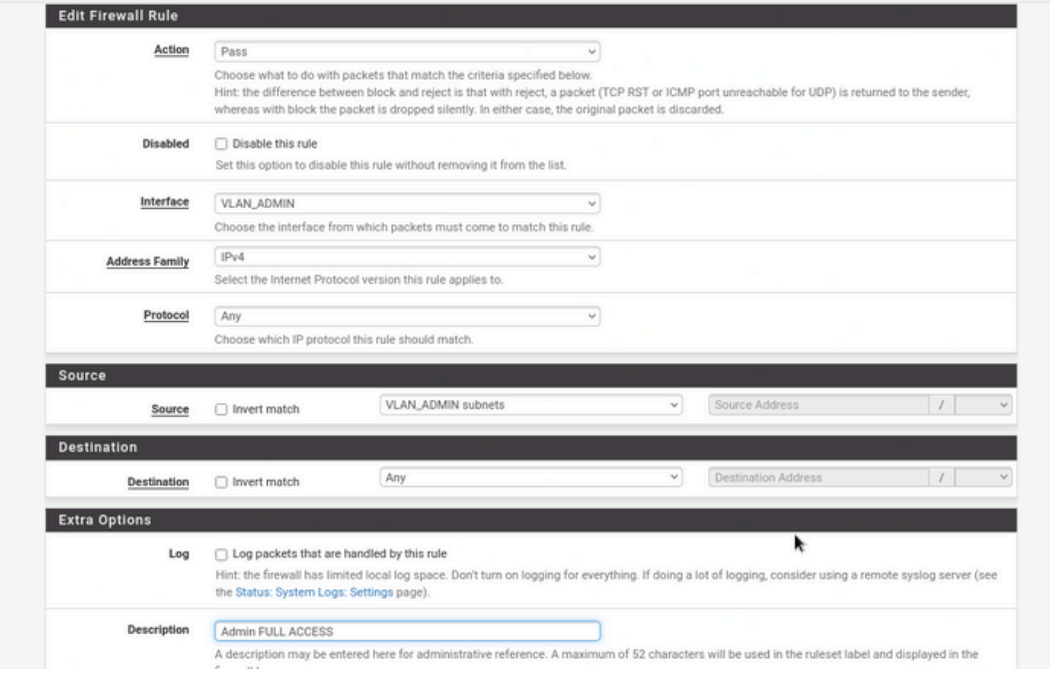
Et depuis le **pc** situé sur le VLan clients :

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

PC1>
```

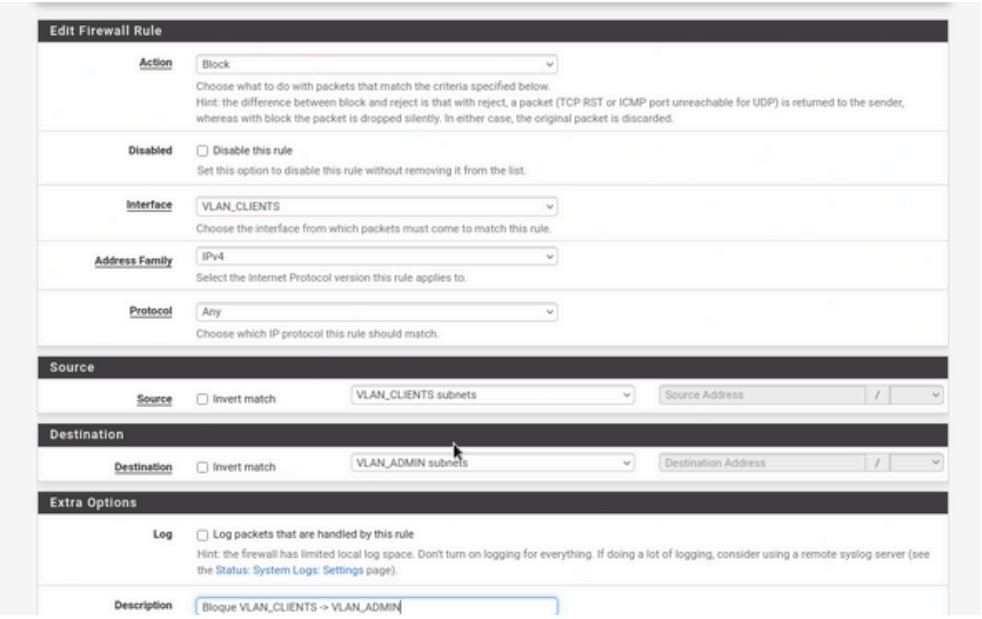
Routage inter-VLAN et ACL

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 :



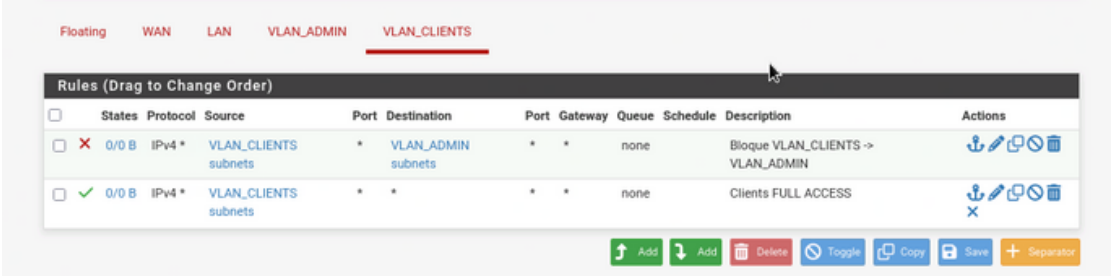
Sur cette image nous avons configuré l'accès complet au sein du VLan admin, nous avons fait exactement pareil pour le VLan client en changeant seulement l'interface par **VLAN_CLIENTS** et la source par **VLAN_CLIENTS** subnets et pour commentaire **« Clients FULL ACCESS »**

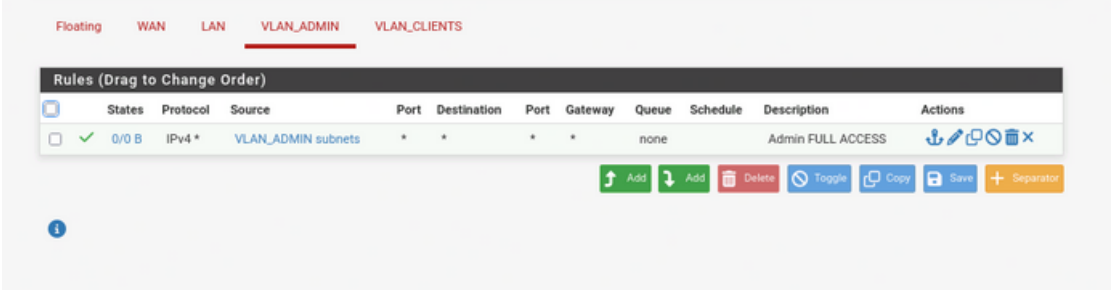
Routage inter-VLAN et ACL



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 étés configurées :





Routage inter-VLAN et ACL

Pour finir nous avons testé le communication et le filtrage, pour cela nous avons fait un ping depuis un Vlan vers un autre, sur la première image on vois 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
```

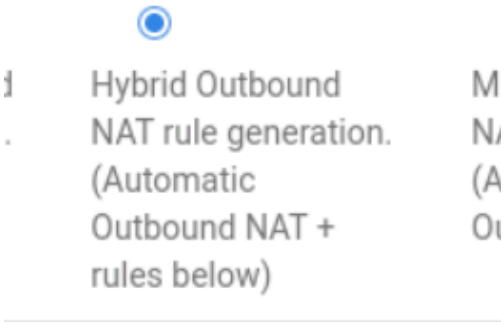
A l'inverse sur cette deuxième image nous voyons que nous ne pouvons pas faire l'inverse (depuis le **VLAN_Clients** on ne peut pas ping le **VLAN_Admin**).

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

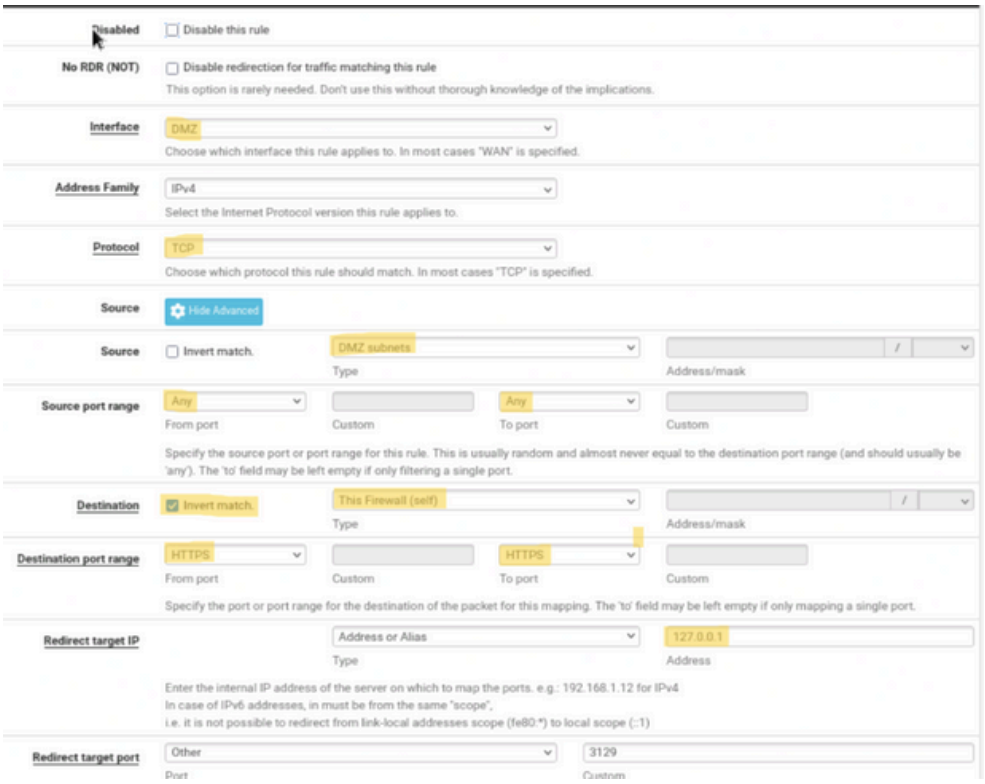
Configuration NAT et Proxy

Configuration du NAT

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



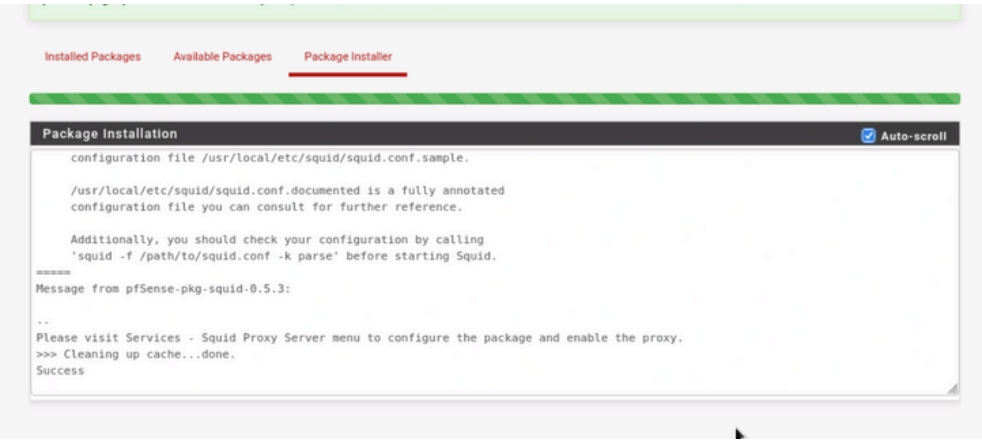
Ensuite on se rend dans **Port Forward** et on fait:



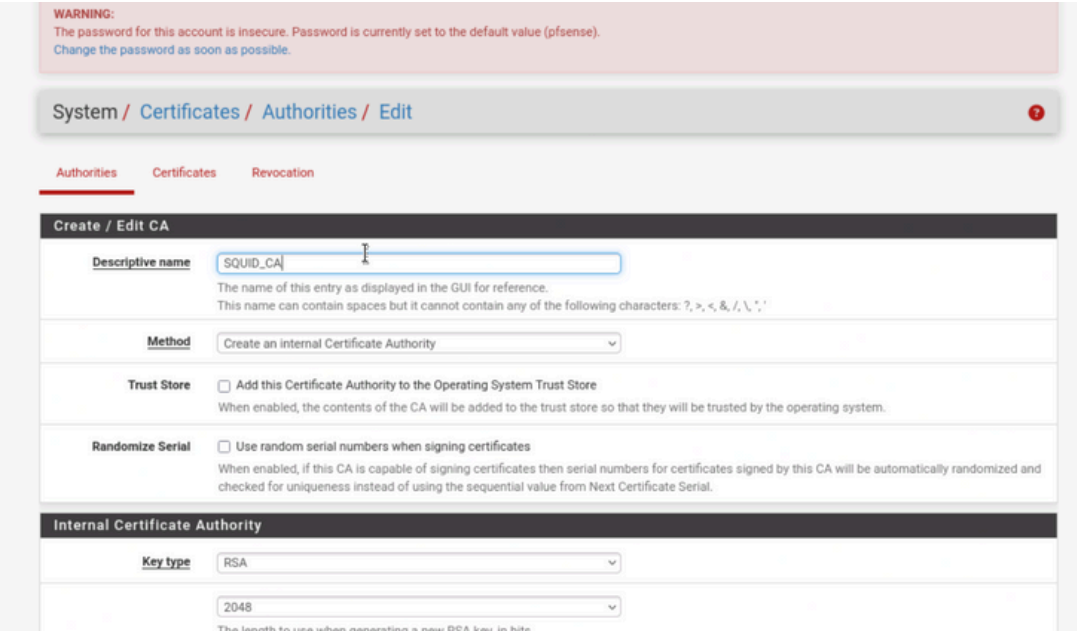
Configuration NAT et Proxy

Installation et configuration du proxy Squid:

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

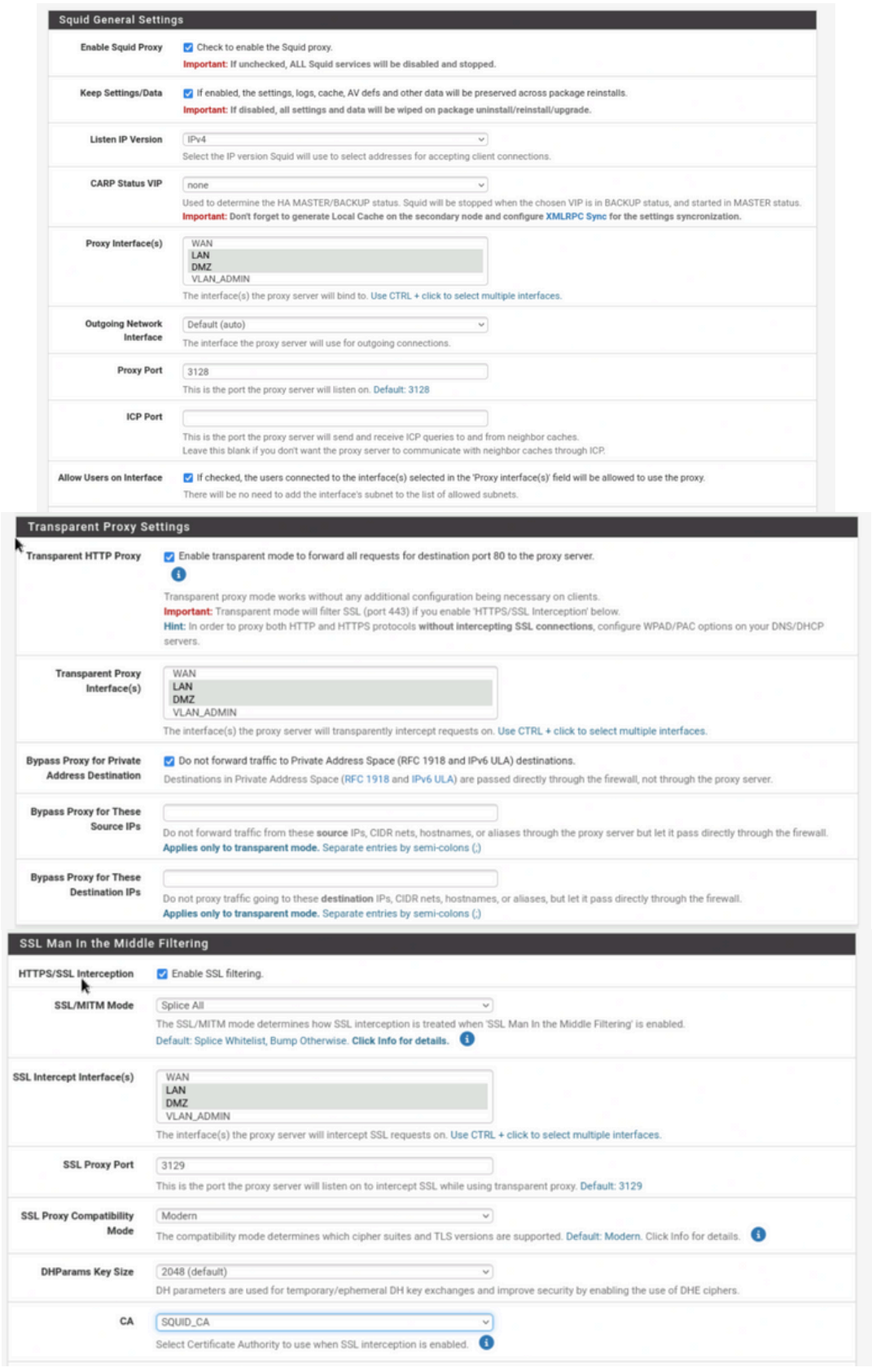


Une fois squid fini d'installer on vas créer une certification d'autorisation pour Squid, pour ça on se rend sur **System** > **Certificates** > **Authorities** > **Edit**, puis dans **Descriptive Name** on écrit **SQUID_CA** et dans méthode on sélectionne **Create an internal Certificate Authority**



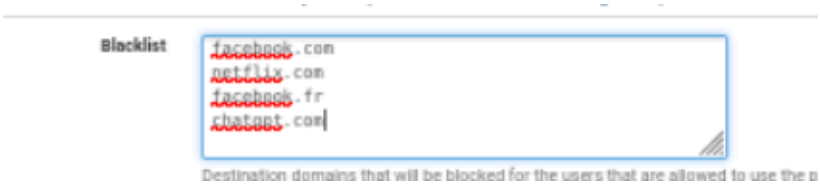
Configuration NAT et Proxy

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

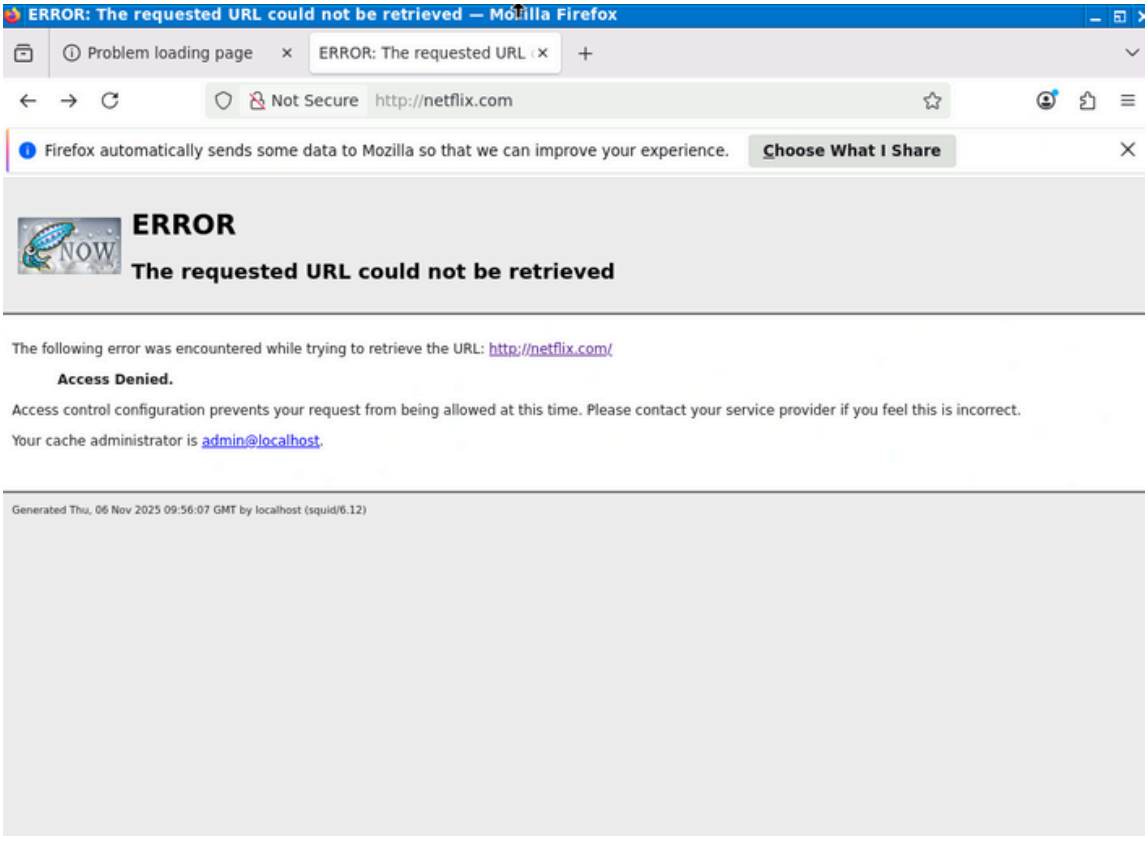


Configuration NAT et Proxy

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

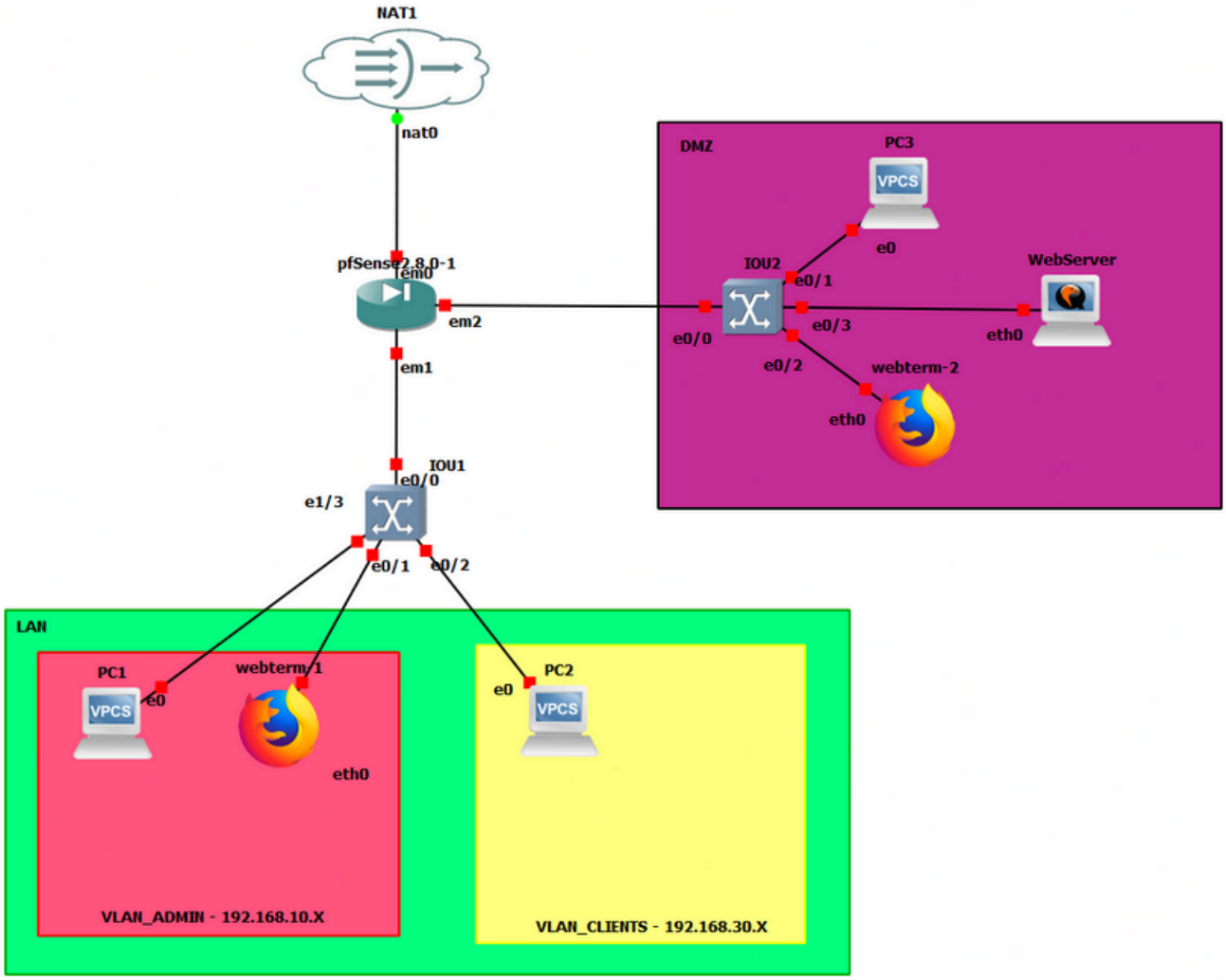


Après avoir blacklisté **netflix.com** on a tenté d'y accéder mais nous n'y êtes pas parvenu ce qui prouve que le filtrage est fonctionnel.



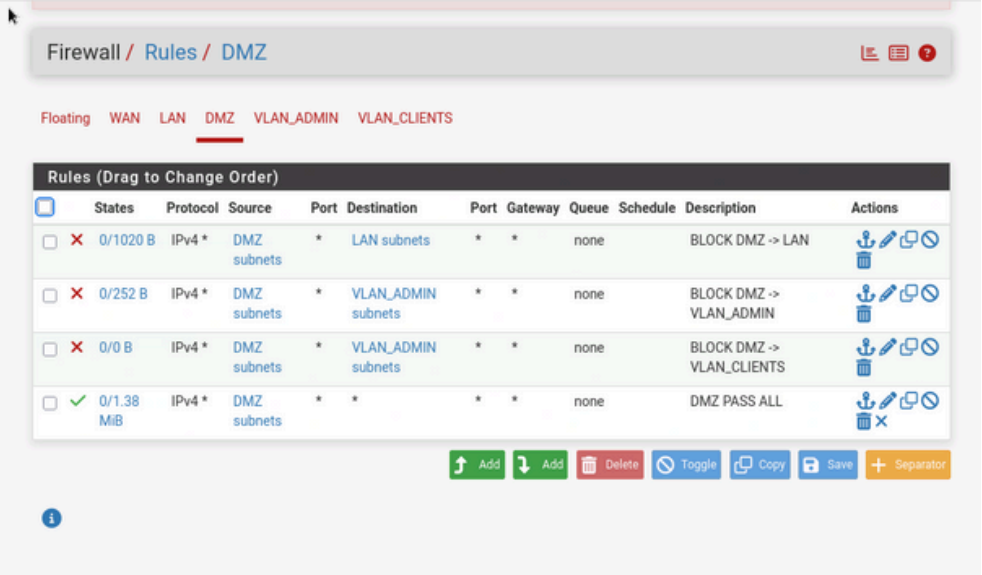
DMZ et sécurité périmétrique

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



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 !

(ANONYME),
(ANONYME),
Tim (ANONYME)

27/10 - 07/11

Guardia CS

UE1-3 Techniques de sécurisation ISR