Techniques de sécurisation ISR

Par `Titouan RICHARD-CARRERE`, `Alan GUILLET` et `Marion GUERIN`.

Techniques de sécurisation ISR

Introduction :

Nous avons travaillé avec :

- VMware
- PNETLAB
- VirtualBox
- GNS3
- Pfsense
- et d’autres modules.

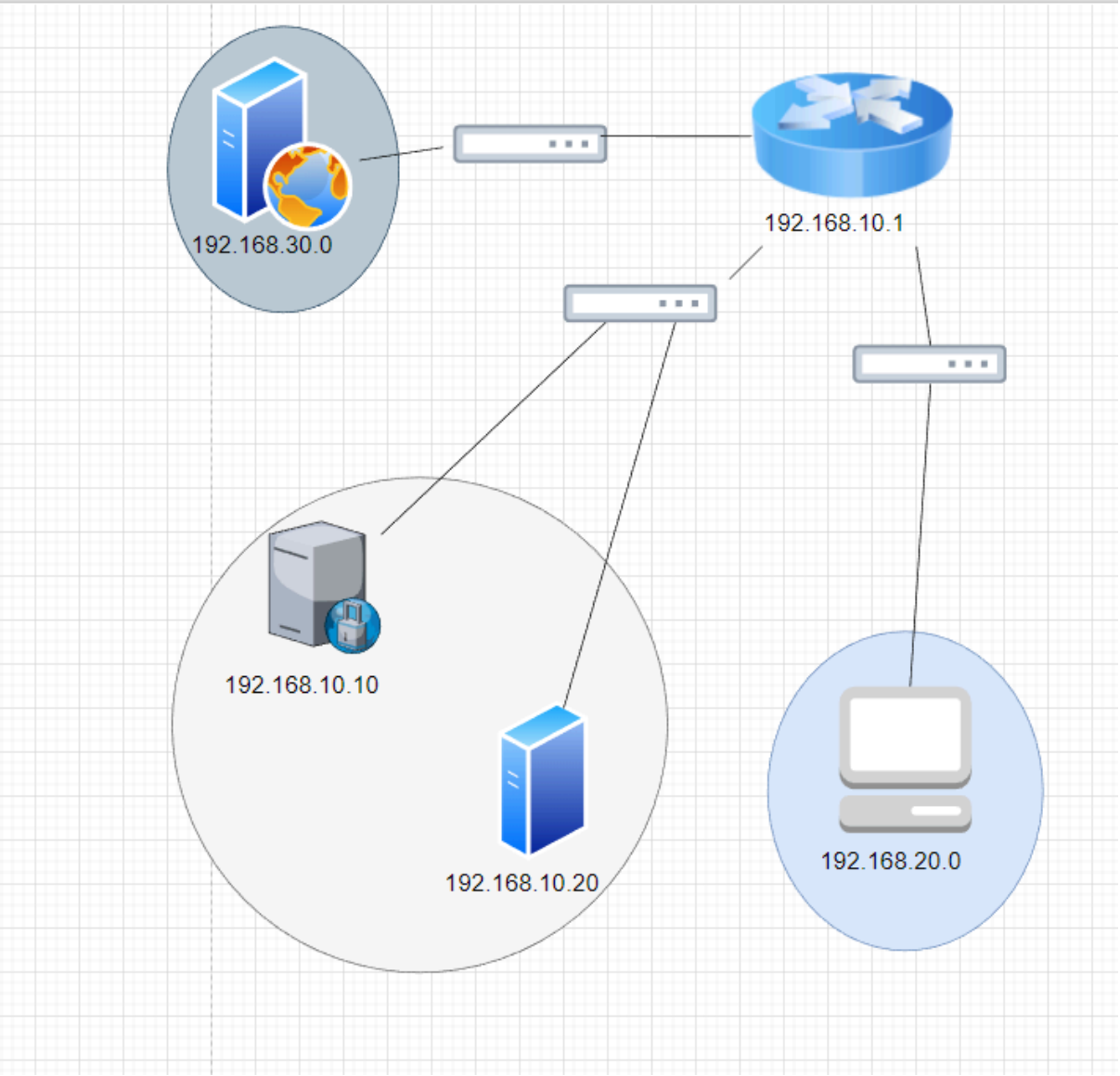
On à tous fait le projet sur nos propres postes, mais principalement sur celui du milieu. L’avancement et la majorité des photos prises ont été faits sur celui-ci. L’ordinateur du milieu étant celui du chef de projet, on à repartis les autres tâches avec le power point par `Alan GUILLET`, le rapport par `Marion GUERIN` et `Titouan RICHARD-CARRERE`.

SOMMAIRE :

Techniques de sécurisation ISR

Partie 1 :

On commence par installer PNETLAB, via le lien dans le cahier des charges donné. On ouvre alors VMware, d'ici on ouvre une nouvelle machine virtuelle et utilisant le fichier PNETLAB.
On a lancé la machine VMware avec PNETLAB, on a configuré celle ci, cependant on à rencontré une issue, on n'arrivait pas à lancer la virtualisation alors on la lancé sans et ça marchait, ensuite, à partir de l'adresse IP bridge que la machine nous à donné on a accéder au site PNETLAB afin de faire des simulations. On à également fait un schéma

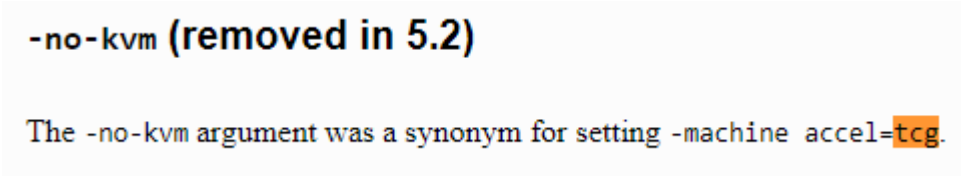


modélisant l'architecture de notre réseau initial.

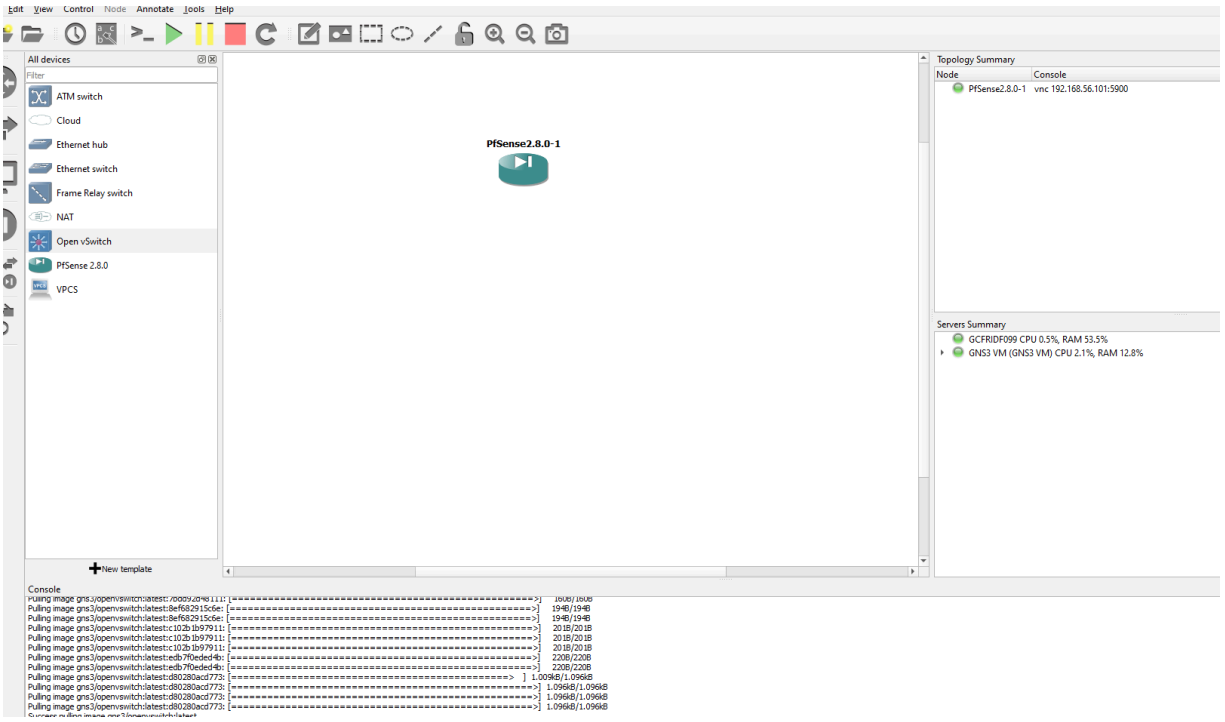
Partie 2 : Installation et configuration du réseau sous GNS3

On passe sur GNS3 comme PNETLAB ne marche pas à cause de la virtualisation. On à réussi à lancer la machine sans problème, on à ouvert le logiciel GNS3, tout marchait, cependant quand on installe des templates on rencontrait des problèmes. Principalement lié à la virtualisation et au KVM, dont on à résolu une partie :

- par exemple pour le KVM sur pfsense on à eu de l'aide de la part de l'intervenant qui nous à dit de mettre la commande suivante avec les machines qui demandait du Linux, la commande est : -machine accel=tcg



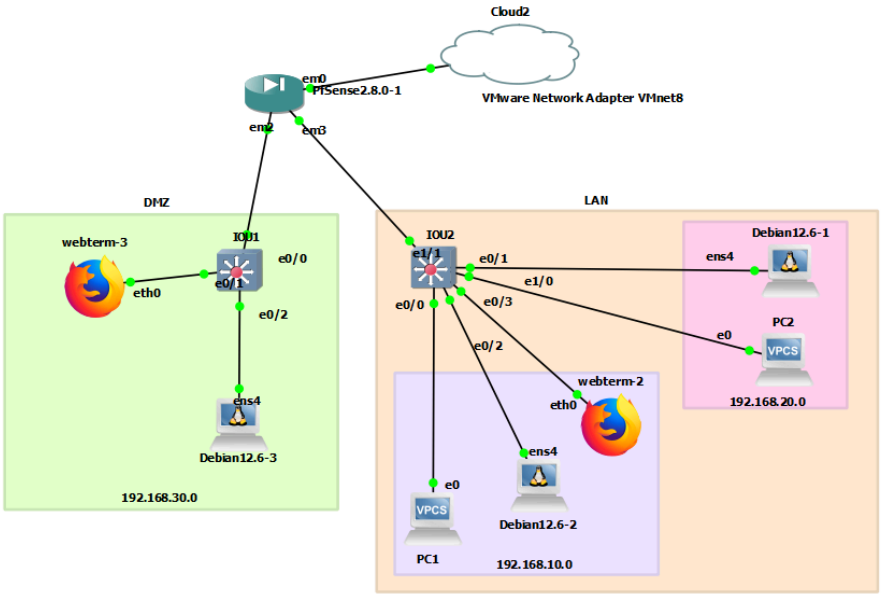
Après une recherche sur internet on peut comprendre que l'utilité de cette commande est de forcer le CPU à faire du software au lieu de virtualisation comme les ordinateurs qu'on utilisait ne prenait pas cette option.



On retrouve également d'autres erreurs récurrentes comme une erreur de requête du client vers le serveur. Dans ces cas-là, on se contente de fermer complètement GNS3 et de rouvrir le projet.

Techniques de sécurisation ISR

On commence vraiment le travail à partir d'ici,QQ
on définit notre nouvelle architecture réseau avec cette topologie



Maintenant il faut que nous configurons les switchs pour avoir les VLAN ainsi que les câbles ethernet pour les ajouter aux VLAN créé (on configurera la DMZ plus tard) :

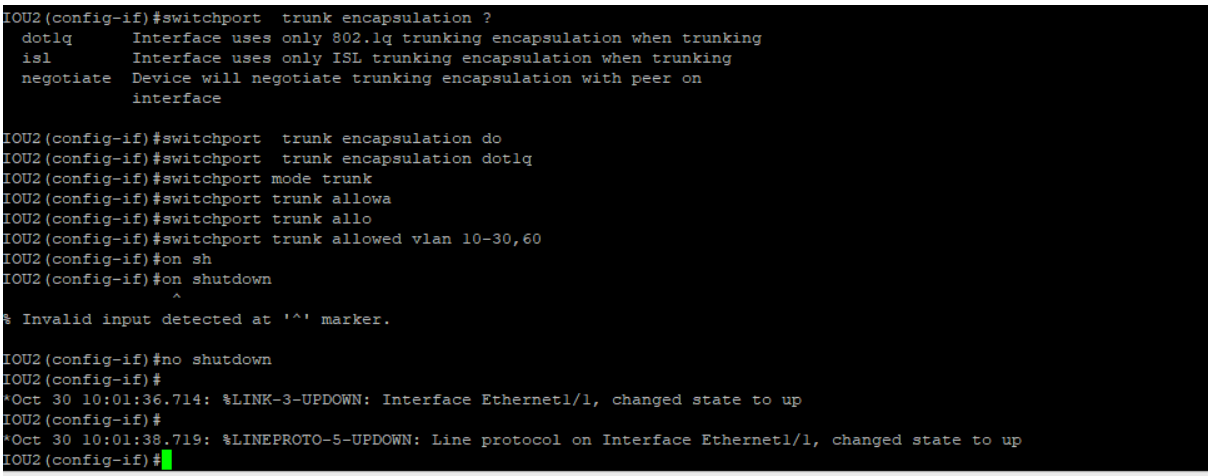
```
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/2, Et1/3
10   VLAN_ADMIN                       active    Et0/0, Et0/2, Et0/3
20   VLAN_CLIENT                      active    Et0/1, Et1/0
30   teste                            active
```

commande utilisée

- conf t
- vlan {numéro du vlan}
- name {nom du vlan}
- exit
- interface {interface}
- switchport mode access
- switchport access vlan {numéro du vlan}
- no shutdown
- exit
- exit
- wr

On a également attribué statiquement les adresses IP aux machines. Comme on n'avait pas encore fait de DHCP on ne pouvait le faire que statiquement.

On a également mis l'interface trunk sur le câble qui lit le switch au routeur pour pouvoir envoyer les paquets au pfsense. L'idée était de pouvoir faire du routage inter-VLAN.



Commande utilisé pour configurer l'interface trunk :

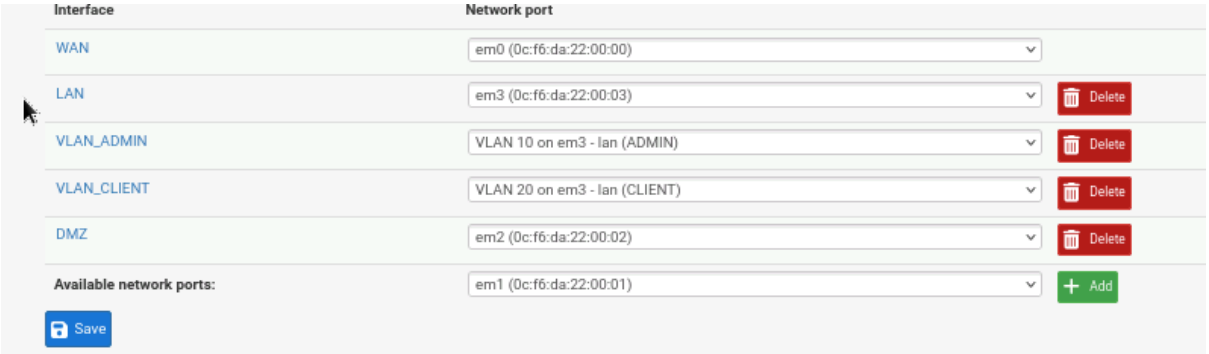
- conf t
- int {interface}
- switchport trunk encapsulation dot1q
- switchport mode trunk
- switchport trunk allowed VLAN …
- no shutdown
- exit

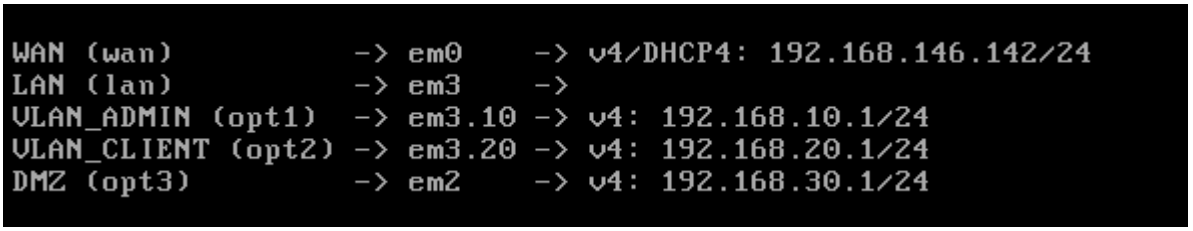
Pour vérifier la configuration nous voulions tenter de ping nos deux machines entre eux, donc pour cela nous avons configuré notre routeur pour faire du routage inter-vlan .
pour ce faire nous avons simplement déclarer les vlan que nous avons précement créer sur notre switch dans notre routeur,
précisons que pour configurer nos vlans sur pfsense nous nous sommes servie du webtern de la DNZ car les machines sur les VLAN ne pouvais plus accéder au pfsense justement car nous avions pas encore définit les vlan sur le pfsense

Cependant nous avons malheureusement rencontré un contretemps lié à un problème de configuration réseau. En effet, les paquets étaient bloqués au niveau du routeur,

Après 2 heures de recherche nous avons fini par comprendre que c'était car nous avions attribué une adresse IP à l'interface LAN. Cette configuration a provoqué un conflit : le même câble était utilisé à la fois pour le trunk et pour le LAN, ce qui entraînait la présence de la même interface et des adresses IP identiques. Ainsi, lorsque les paquets quittent le routeur pour rejoindre le switch, ils ne savaient pas s'ils devaient être acheminés vers le réseau LAN ou vers les VLANs, ce qui bloquait la communication.

une fois l'erreur corrigé cela donnait cette configuration

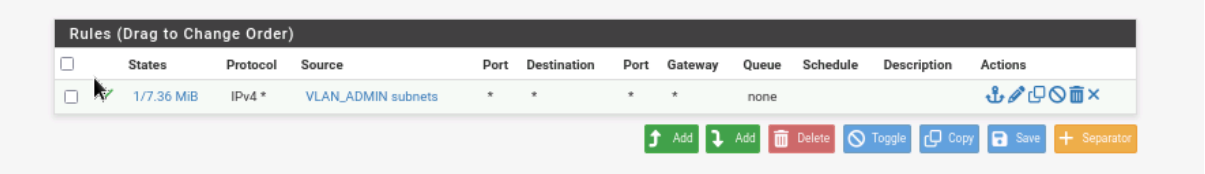


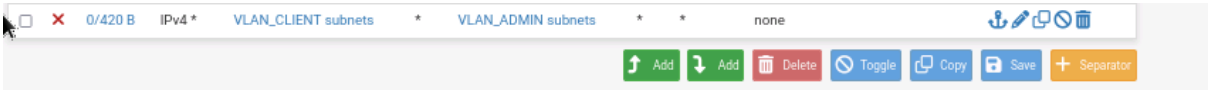


Partie 3 : configuration des règles de sécurité

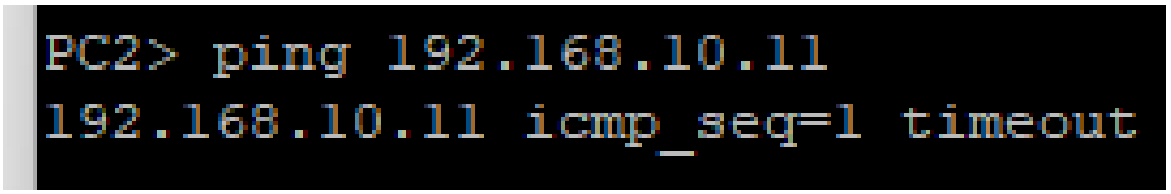
Maintenant que nos appareil sont correctement configuré et que le trafic réseau est fonctionnel nous passons à la configuration de notre firewall pour plus de sécurité :

Nous avons commencé par mettre 2 règles de filtrage afin que les machines du VLAN_ADMIN puissent joindre les machines du VLAN_CLIENT mais pas l'inverse.



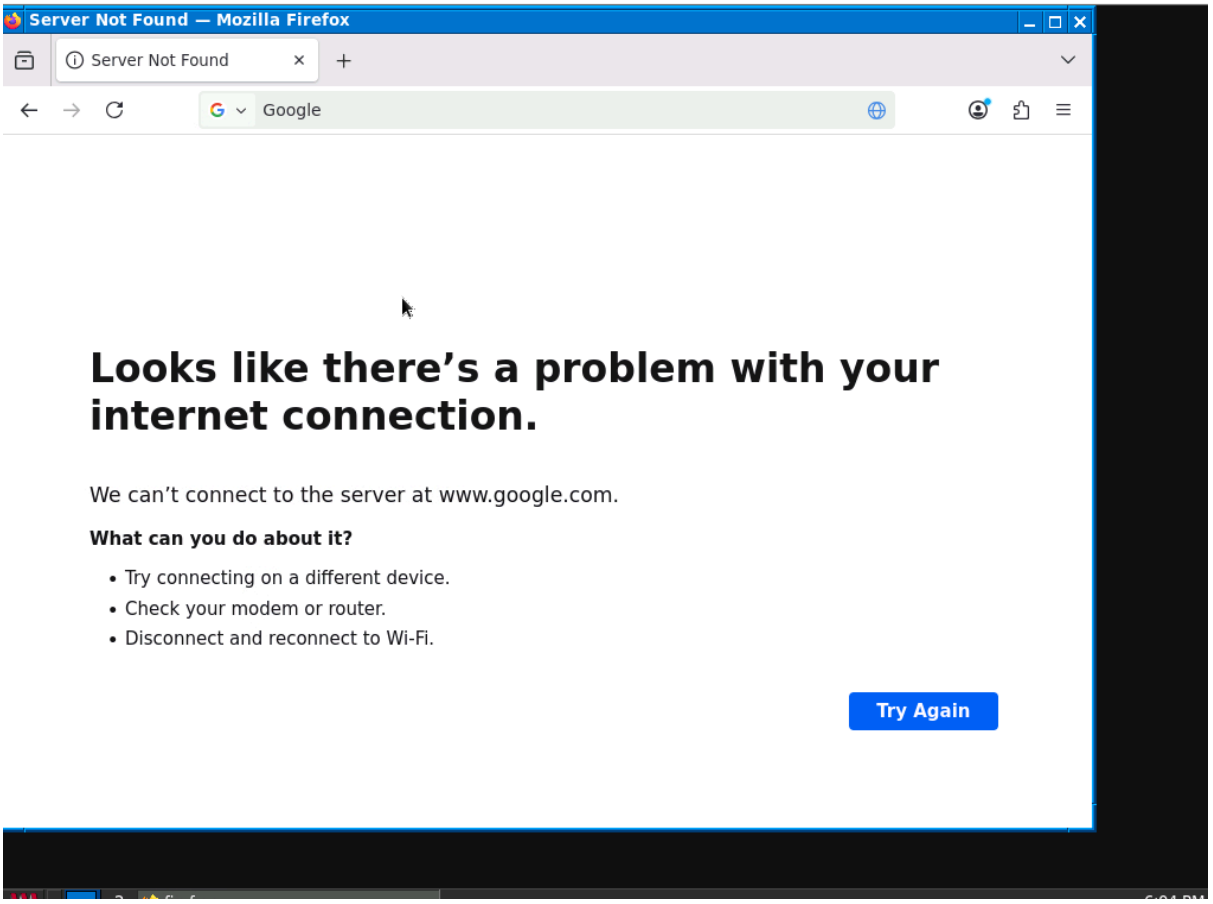


Désormais si on essaie de ping la machine admin à partir de la machine client on obtient :

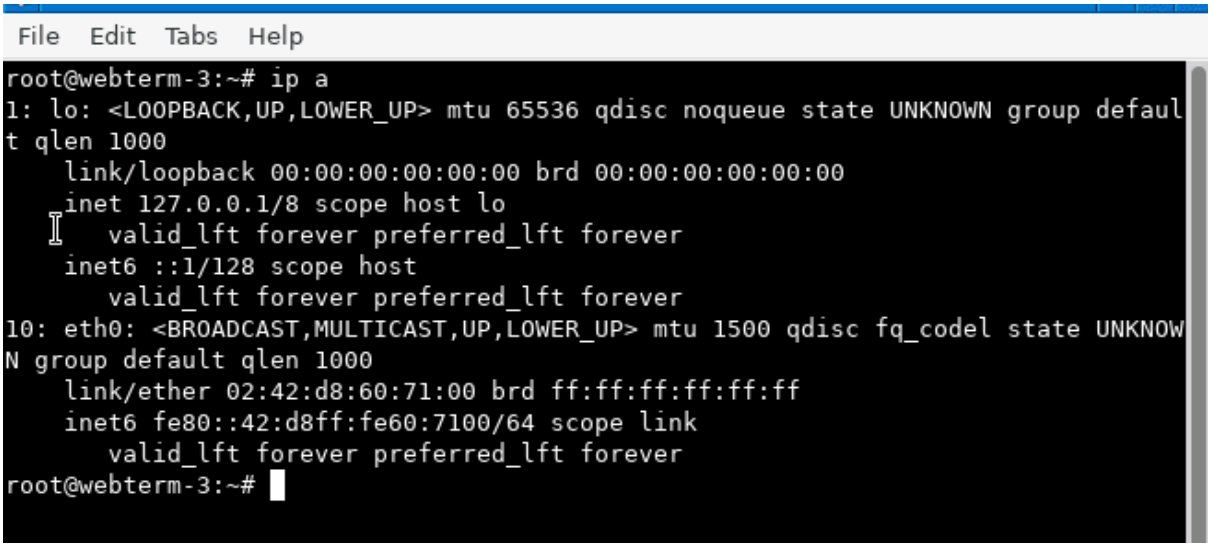


Donc maintenant que les communications entre les différents VLANs sont configurés, on va essayer d'accéder à Internet.

Voilà le résultat :

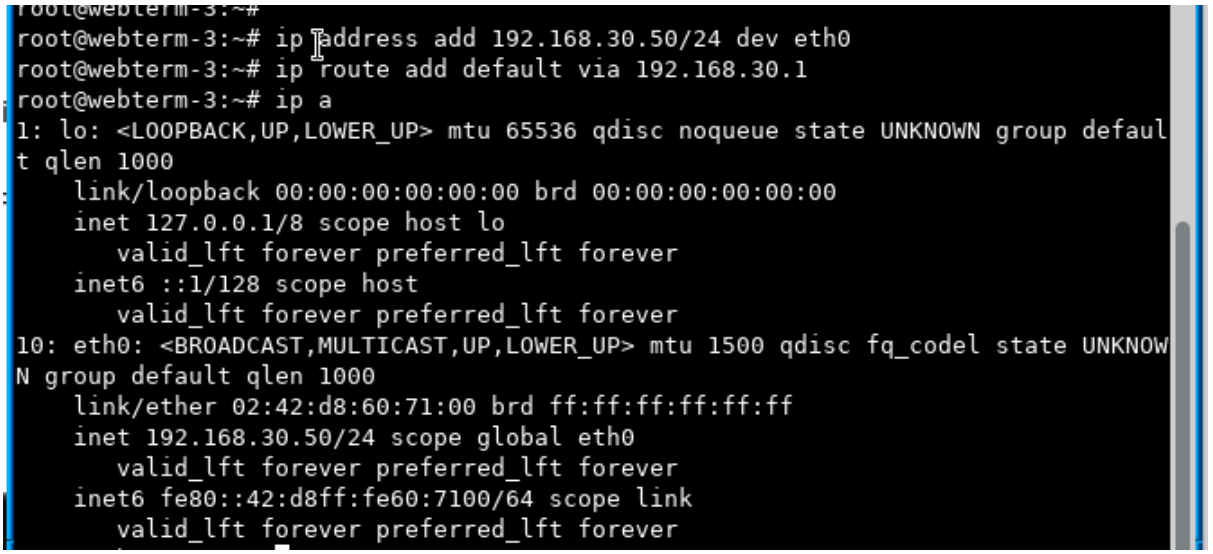


Après avoir regarder notre configuration réseau, nous remarquons que notre webtern n’a pas d’adresse IP défini :



Nous allons donc faire notre configuration réseau, avec les commandes suivantes :

- ip address add 192.168.30.50/24 dev eth0
- ip route add default via 192.168.30.1

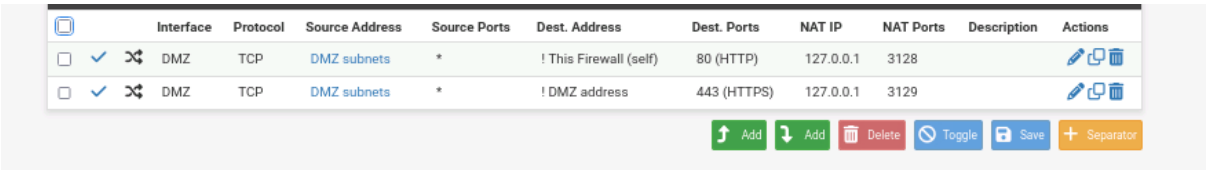


Nous réessayons et nous obtenons toujours l'erreur précédente. nous allons vérifier le contenu du fichier /etc/resolv.conf. nous voyons qu'il est vide alors nous ajoutons la ligne :

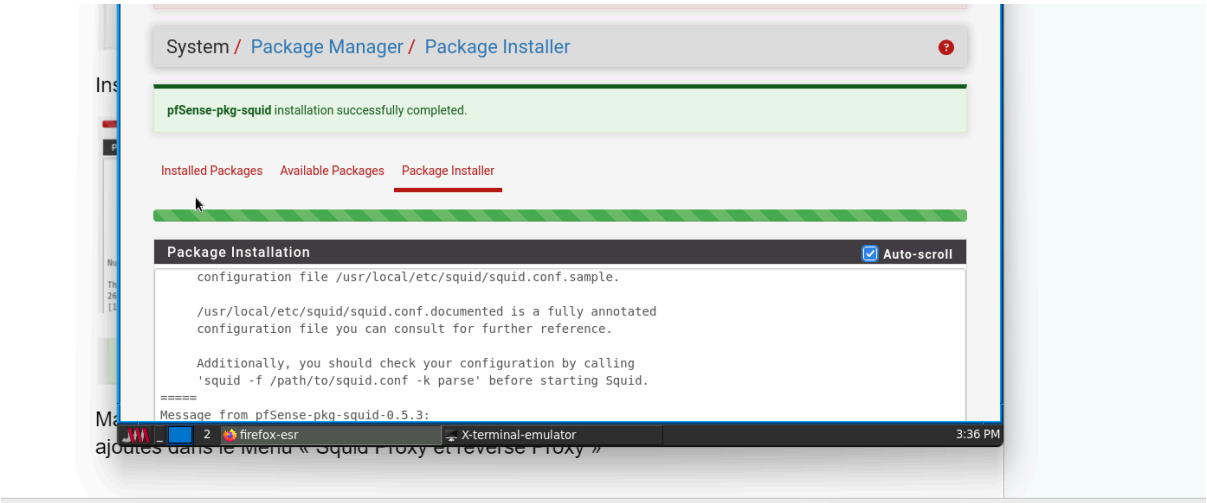
nameserver 8.8.8.8

Cette ligne indique à la machine du serveur DNS quel DNS elle doit utiliser et nous observons alors que désormais nous pouvons accéder à internet.

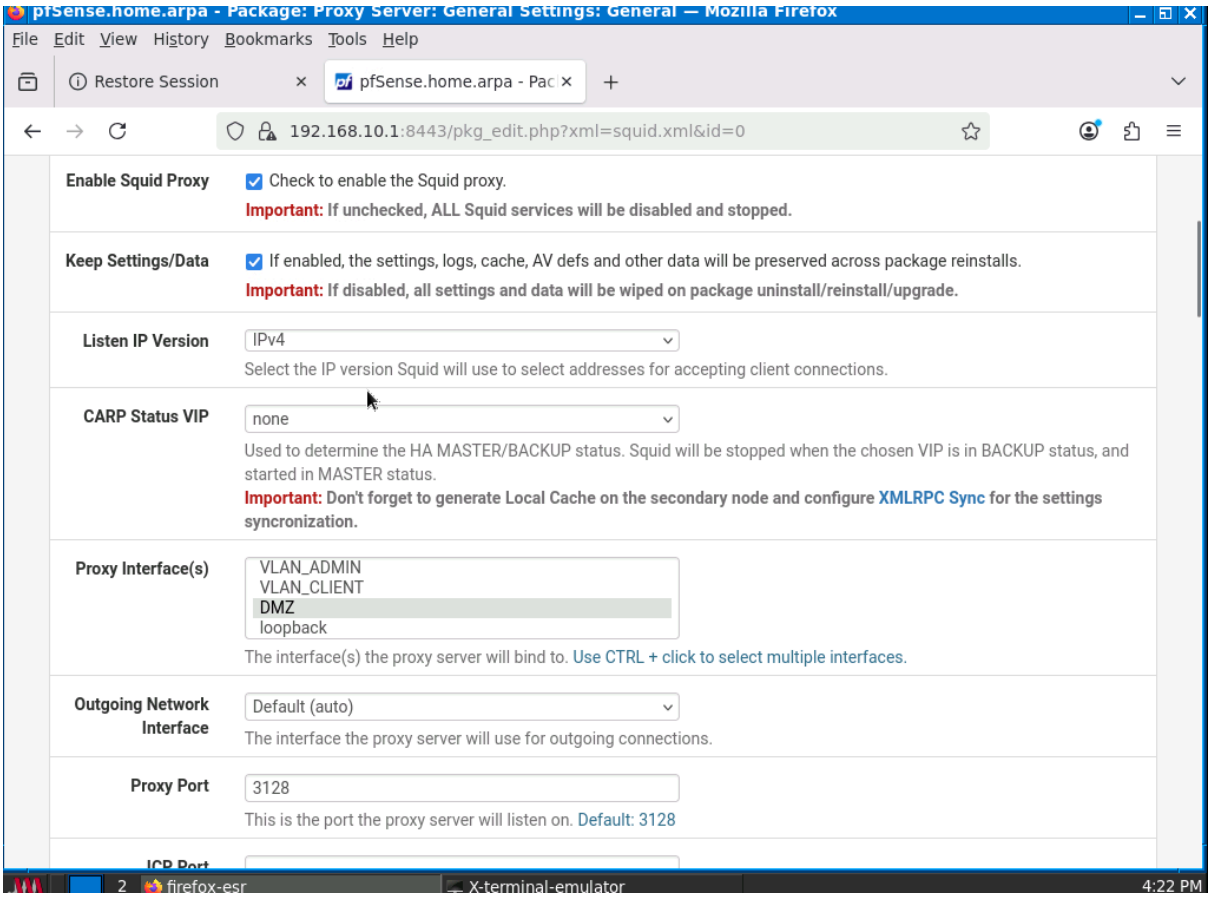
Maintenant qu'on a réussi configurer notre routage inter-vlan sécurisé et qu'on peut accéder à internet il nous faut configurer le NAT pour pouvoir accéder à internet
Ces deux règles stipulent comment le réseau de la DMZ accède à internet



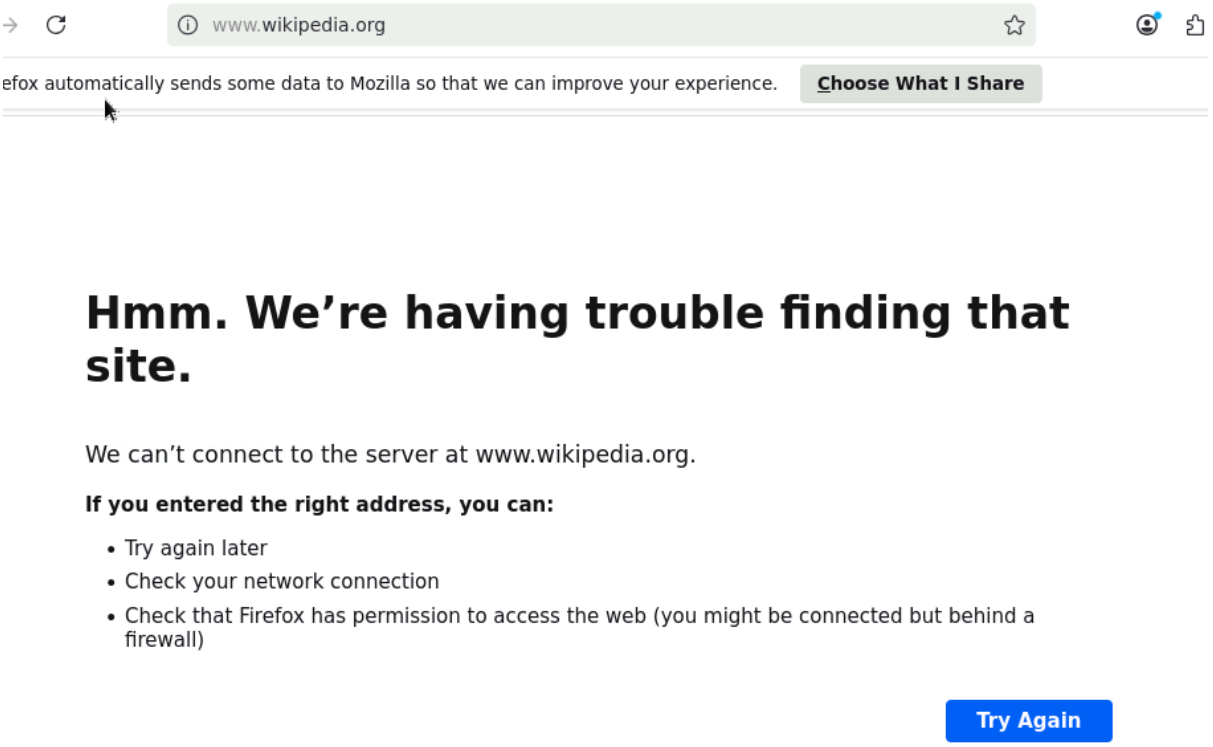
Maintenant que nous avons configuré la dmz pour accéder à internet et que nos vlan communiquent entre eux de manière sécurisé. nous allons faire le proxy qui servira d'intermédiaire.
L'objectif de notre proxy ici sera notamment de pouvoir bloquer certains sites.
Nous allons configurer le proxy, pour cela on commence à l'installer par le pfsense :



Et on suit les étapes du documents donnés.



enfin pour l'exemple on décide de bloquer le site wikipédia.org



Voilà , nous avons donc une architecture réseau fonctionnelle et sécurisée. Ce projet nous aura beaucoup appris, notamment car nos connaissances avec les logiciels de topologie réseau comme GNS3 étaient très limitées.

Merci d’avoir lu ce rapport.