Scénario N°1 :

Sécurisation réseau et Segmentation VLAN

BOUCAUD Bastien

BTS SIO 2 SISR / Groupe 3

Année :2025/2026

Table des matières

CONTEXTE GENERAL DU PROJET :

EcoSolar Solutions c'est quoi :

Fondée en 2010, EcoSolar Solutions est une entreprise dédiée à un domaine en pleine croissance, les panneaux photovoltaïques.

La société a mis au point une solution breveté visant à offrir une efficacité maximale de leurs panneaux, tout en maintenant un apport de matériels LOCAL, Français pour réduire au plus possible leur empreinte Carbonne bien trop élevée dans les différents domaines du monde du travail aujourd'hui (l'informatique n'échappe pas à la chose, mais là n'est pas le sujet).

Basée à Toulouse, EcoSolar Solutions regroupe sur un même site ses bureaux administratifs, son atelier de production et son laboratoire RCD. Elle emploie environ cinquante collaborateurs et prévoit une croissance rapide pour atteindre quatre-vingts salariés dans les prochaines années.

Qui sommes-nous dans le cadre du Projet :

Nous sommes WildCorp, prestataire informatique de EcoSolar Solution

Missionnés pour effectuer une maquette fonctionnelle de leur prochaine infrastructure, nous allons nous séparer sur quatre scénarios d'amélioration ,

- VLAN et réseau
- Mise en place de sauvegardes centralisées
- Supervision centralisée
- Redondance et haute disponibilité

(Ce dossier se concentrera sur le premier scénario, (le tout présenté ultérieurement).)

Pourquoi son SI se doit d'évoluer :

Le système d'information (SI) d'EcoSolar Solutions a longtemps été sous-dimensionné et peu structuré, son évolution basée sur des ajouts successifs plutôt que sur une véritable stratégie.

Géré entièrement en interne, il souffrait d'un manque de sécurité et de cohérence globale dans l'avancée des projets, et face à la croissance de l'entreprise et aux nouveaux besoins, la direction pense désormais qu'une refonte complète est indispensable.

Cette modernisation passe par la remise à niveau de l'infrastructure locale et par l'intégration d'une baie dédiée dans un datacenter à Marseille

L'objectif est de faire évoluer un SI principalement local et centré sur les moyens techniques vers un système, plus sécurisé, plus fiable et adapté aux besoins actuels comme futurs, notamment en matière de gestion des risques et d'accès distants.

Qu'est-ce que mon projet tend à améliorer :

Par une segmentation en VLAN et une sécurisation du réseau, mon scénario vise à améliorer plusieurs points :

1. **Segmentation du réseau** : création de VLAN, pour isoler les flux et limiter les risques.
2. **Plan d'adressage IP**: organisation structurée du réseau facilitant sa gestion.
3. **Accès distant sécurisé** : mise en place d'un VPN site to client *(permettant aux utilisateurs de se connecter de manière sécurisée au réseau de leur entreprise depuis des endroits tels que leur domicile, un hôtel, un restaurants…)* pour que les techniciens puissent se connecter en toute sécurité aux servers depuis leurs machines .
4. **Fiabilité et contrôle** : tests de connectivité et vérification de la sécurité pour s'assurer que tout fonctionne correctement (vu en fin de projet) .
5. **Sécurité du réseau** : protection renforcée des données et des systèmes via firewall (OPNSense) et règles adaptées.

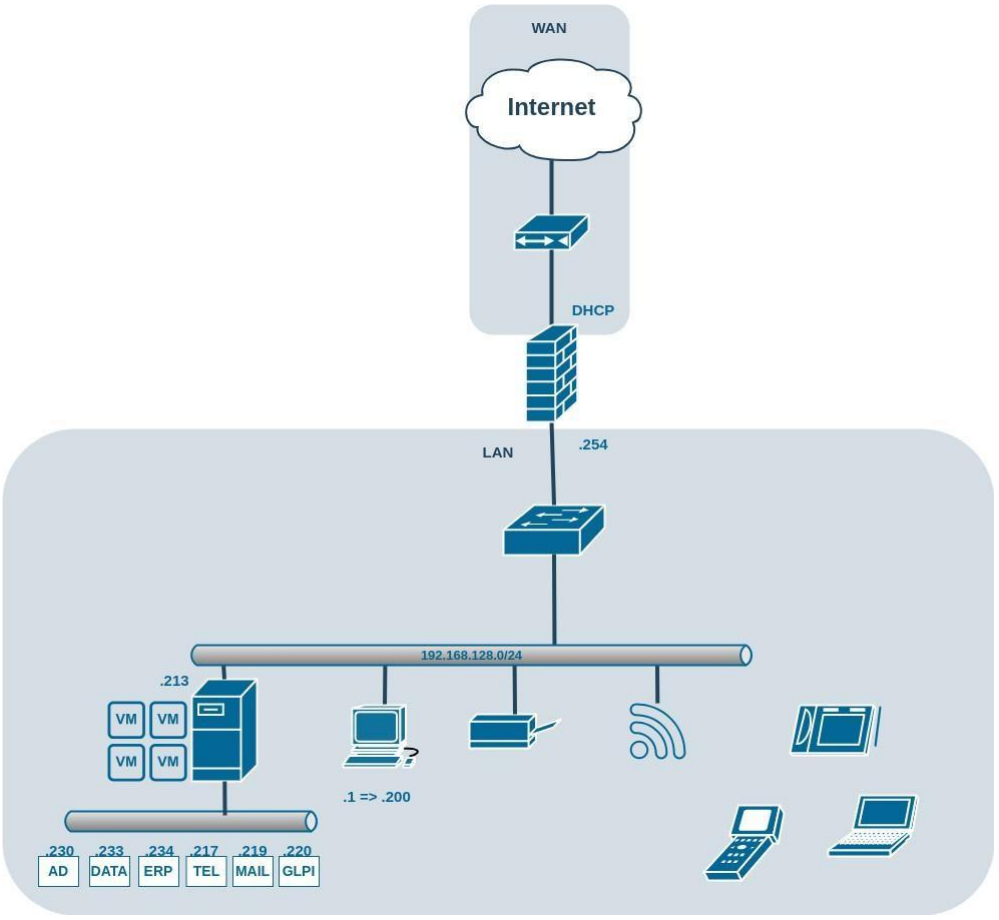
CONTEXTE TECHNIQUE INITIAL :

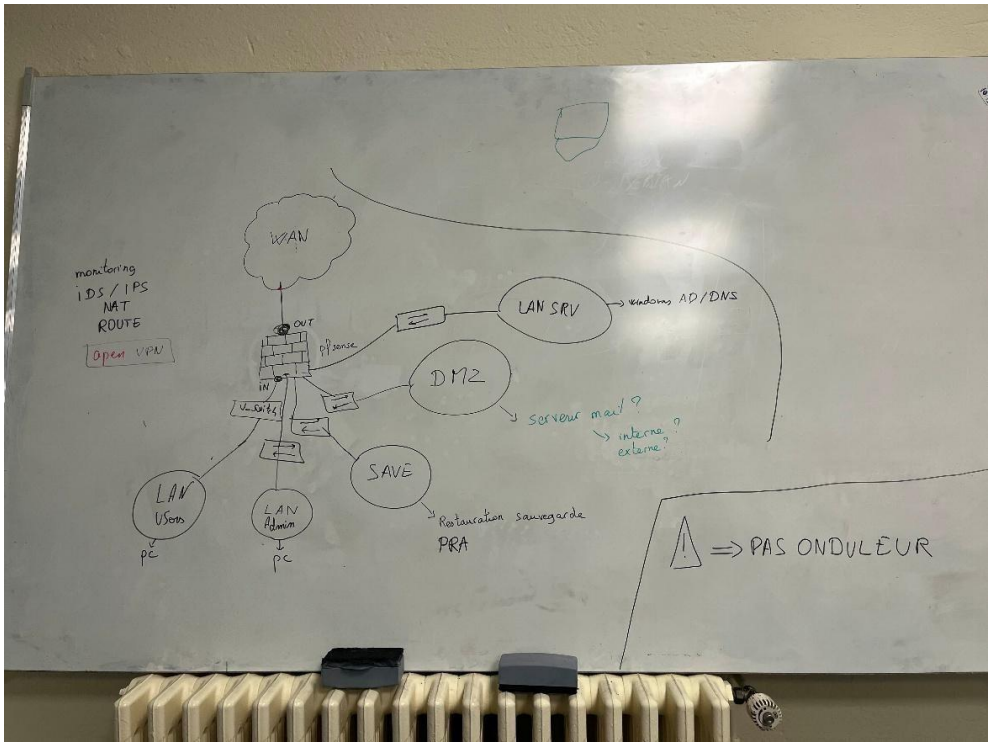
Tableau du matériel réseau ou infrastructure du projet

Catégorie	Élément	Détails / Configuration
Réseau	Switch	Cisco 3560, 48 ports, configuration par défaut : un seul VLAN, pas de routage inter-VLAN, pas d'accès distant
	Point d'accès Wi-Fi	Cisco C9136I, WPA2, pour bureaux et atelier
	Adressage IP	IPv4 privée 192.168.128.0/24, DHCP .1 à .200, pas d'IPv6
	Accès Internet	Firewall pfSense Netgate SG-2440, règle LAN : permit all any any
	VLAN	Aucun (réseau non segmenté)
	Baie locale	42U, sans onduleur, salle serveur Toulouse
Infrastructure Serveurs	Hyperviseur	Proxmox VE v8.3-1 sur DELL PowerEdge R720, CPU Xeon E5-2640, RAM 64 Go, stockage SAS 50 Go OS + 10 x 300 Go données
	VM Windows	1 AD/DNS/DHCP, 1 serveur fichiers
	VM Linux	1 ERP Dolibarr, 1 téléphonie XIVO, 1 mail Poste.io, 1 inventaire/ticketing GLPI
Périphériques	Postes	PC fixes et portables Windows intégrés au domaine
	Mobiles	Tablettes Android, smartphones des commerciaux et responsables
	Softphones	Installés sur ordinateurs fixes
	Imprimantes/photocopieurs	Connectés au réseau
Datacenter (Marseille)	Baie	42U, vide et non brassée, IPv4 /30 et IPv6 /56
	Sécurité physique	Badge + biométrie, vidéosurveillance, gardiennage, onduleurs, groupe électrogène
	Sécurité incendie	Détection par aspiration d'air, extinction gaz inerte
	Climatisation C énergie	Free-cooling basse consommation + panneaux solaires et accumulateurs

(à partir du contexte donné dans le sujet)

Schéma de l'infrastructure :





QUELS ETAIENT LES BESOINS ? :

En se basant sur le contexte de projet, les besoins principaux se concentrent sur une modernisation, une sécurisation du SI.

Concernant la sécurisation, il y a un réel besoin d'une segmentation réseau, type configuration de VLAN. Cette segmentation implique forcément la création de plusieurs règles sur le pare-feu.

En visant toujours plus loin dans la sécurisation, on relève la demande d'un accès distant sécurisé, ici on peut placer un VPN (dans le cadre du projet_scenario_1, un site-to-client)

Pour soutenir son expansion, EcoSolar Solutions doit exploiter son datacenter à Marseille en concevant une architecture hybride à haute disponibilité. Cette infrastructure, qui reliera le site principal au datacenter, permettra d'héberger des services critiques (comme le site web) et d'absorber la croissance, tout en garantissant la continuité d'activité. Cette transformation devra s'appuyer sur une supervision robuste, une politique de sauvegarde externalisée et une gouvernance IT formalisée (politique de sécurité) pour assurer la performance, la résilience et la maîtrise du SI orienté services.

OBJECTIFS DU PROJET :

Disponibilité ? :

La grande croissance de l'entreprise et la volonté d'héberger le site web en interne vont augmenter considérablement la charge de l'infrastructure.

L'objectif ? éviter une panne du SI qui bloquerait l'ensemble des activités de EcoSolar

Pour cela, Élever le niveau de résilience. Cela passe par l'exploitation du datacenter à Marseille pour créer une infrastructure hautement disponible, l'ajout d'un onduleur sur site.

Plusieurs risques identifiés :

- Infrastructure unique et centralisée sur site (pas de redondance).
- Absence d'onduleur dans la baie locale, la rendant vulnérable aux coupures de courant.
- Serveur web hébergé chez un tiers.

Intégrité ? :

L'entreprise s'appuie sur Dolibarr pour gérer ses stocks, commandes, factures et clients. La modification frauduleuse ou accidentelle de ces données pourrait entraîner des erreurs de production, des pertes financières et une perte de clients

L'objectif ? Assurer la traçabilité et la protection des données critiques via un contrôle d'accès strict, la mise en place d'un système de supervision et d'alertes, et l'établissement d'une politique de sauvegarde automatisée.

Plusieurs risques identifiés :

- Infrastructure vieillissante et mal maintenue augmentant ainsi le risque de défaillance.
- Absence de supervision centralisée, empêchant de détecter des activités anormales ou des modifications non autorisées.

Confidentialité ? :

La société détient un brevet exclusif et des données de Recherche C Développement qui constituent son avantage concurrentiel principal. Une fuite potentielle pourrait anéantir sa valeur.

L'objectif ? Mettre en place des cloisonnements stricts (VLANs, règles de pare-feu) pour isoler les secteurs sensibles, sécuriser les accès distants (VPN).

Plusieurs risques identifiés :

- Accès réseau non segmenté
- Politique de pare-feu trop permissive (permit any any sur le LAN).
- Accès Wi-Fi en WPA2 UNIQUEMENT

CONDITIONS DE REALISATION :

CONDITIONS GENERALES DE REALISATION :

Durée :

Le projet en lui-même rentre dans le cadre du projet E6 pour le diplôme du BTS SIO SIR

Il est donc prolongé jusqu'à Avril 2026 où les documentations de projets doivent être rendues

OR la conception TECHNIQUE du projet, a essentiellement été faite lors de la semaine intensive du 01/12/2025 au 05/12/2025

Individuel/équipe :

BOUCAUD Bastien : Scénario 1 : VLAN et Sécurisation Réseau

CHAPEAU Lucas : Scénario 3 : Supervision et alerting des services critiques

SAUTIE Thomas : Scénario 2 : Sauvegarde Centralisée C PRA

Contraintes pédagogiques / Contraintes techniques :

- **Pédagogiques :**
  - Les configuration techniques devaient être achevées lors de la semaine intensive (même si rien n'empêche de poursuivre depuis chez soi)
  - Devoir traiter UN scénario sur les quatre proposés

- **Techniques :**
  - Proxmox à utiliser
  - Grosse latence sur le réseau (IRIS2 Projet)
  - Pas possible de créer de VLANS sur le switch fourni

RESSOURCES FOURNIES :

Matérielles/Logicielles :

PROXMOX 	**MACHINE PERSO** 
PFSENSE	**RESEAU PRIVE** 

RESULTAT QUI ETAIT ATTENDU :

D'après le document des projets E6, le Résultat attendu du Projet 1 est la modernisation et la sécurisation de l'infrastructure locale de Toulouse, pour la rendre fiable, supervisée et résiliente.

Concrètement, cela se traduit par une infrastructure où le réseau est segmenté (VLANs), sécurisé par des règles de pare-feu strictes (plus performantes et filtrante qu'un ANY ANY) et accessible à distance de manière sécurisée (VPN).

Une solution centralisée de sauvegarde automatisée et testé doit être opérationnelle, ainsi qu'un système de supervision (type Zabbix) fournissant des tableaux de bord et des alertes.

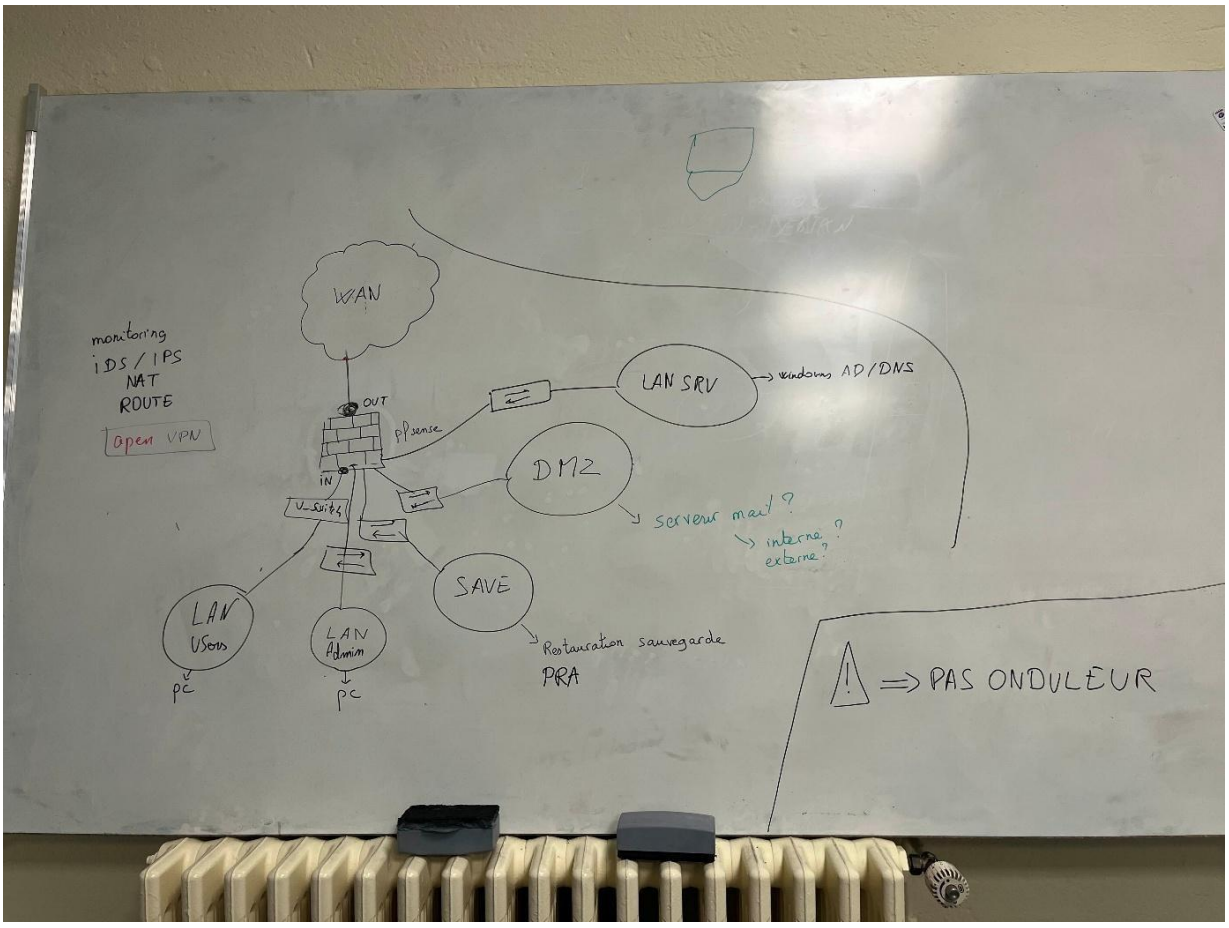
Enfin, l'ensemble doit être documenté par un dossier projet complet (celui que vous lisez en ce moment), des schémas techniques.

CONCEPTION :

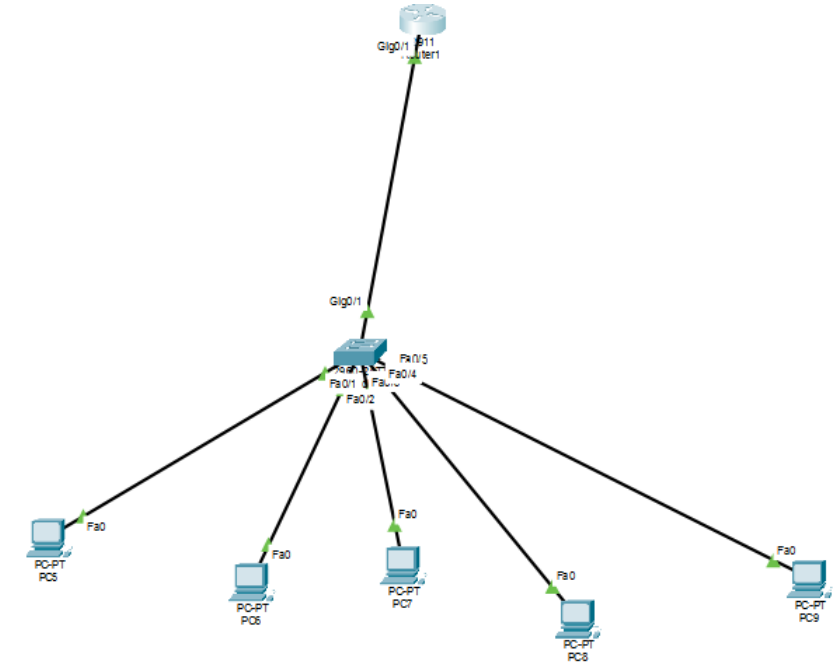
Architecture / plan d'adressage IP :

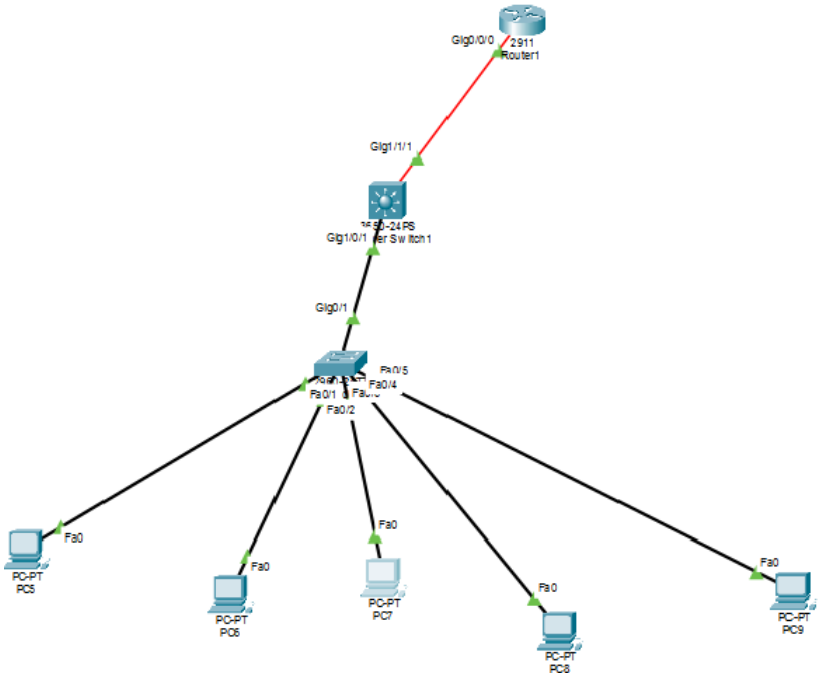
Au cours de ce projet, on a pu passer par plusieurs concepts et idées d'architecture,

Les différentes architectures dépendaient de la technique suivie, la première à partir de Proxmox, la seconde avec des machines virtuelles et des Virtual switch et enfin a partir de GNS3

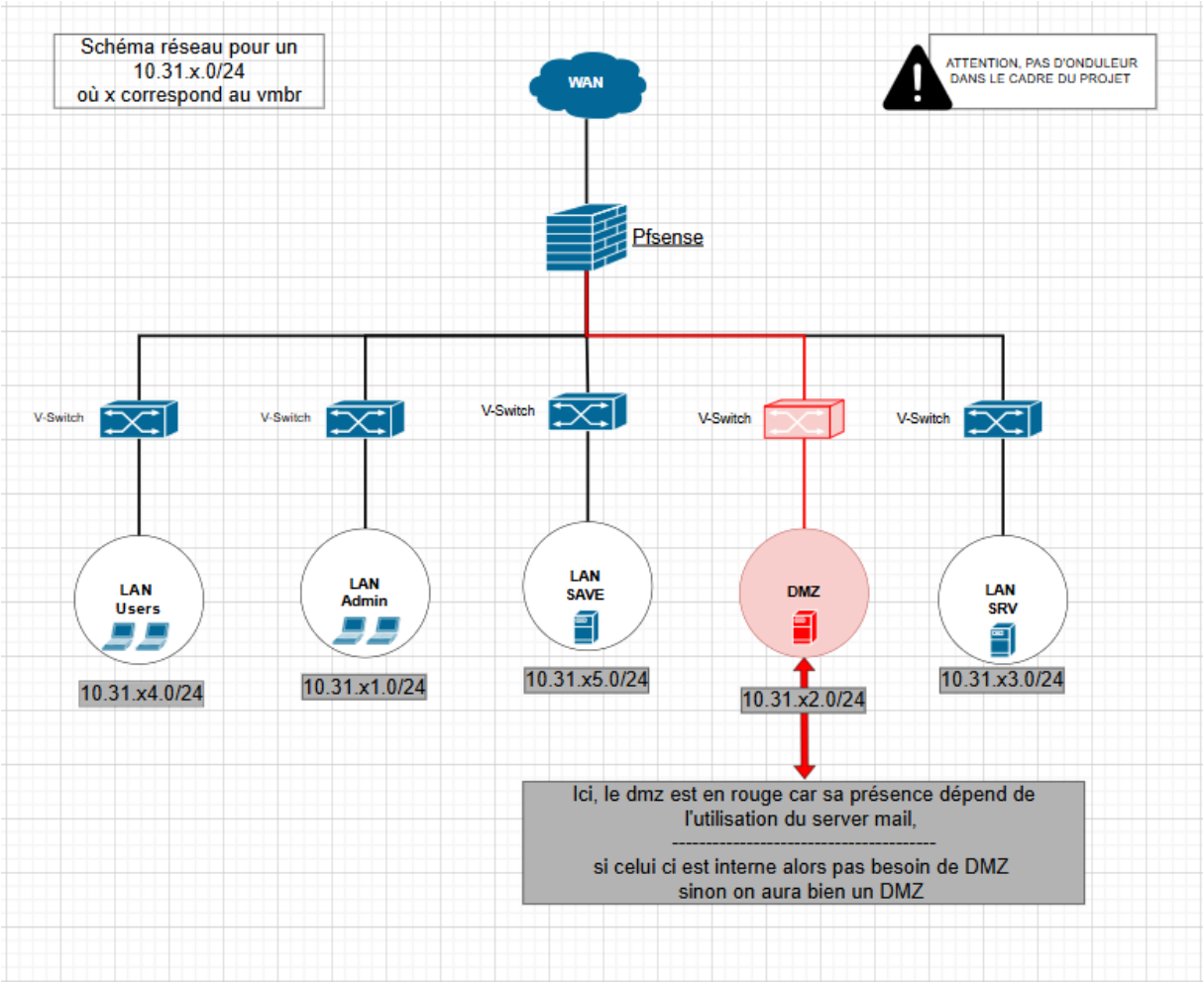


ARCHITECTURE CONCEPTUELLE AVANT DE COMMENCER LE PROJET

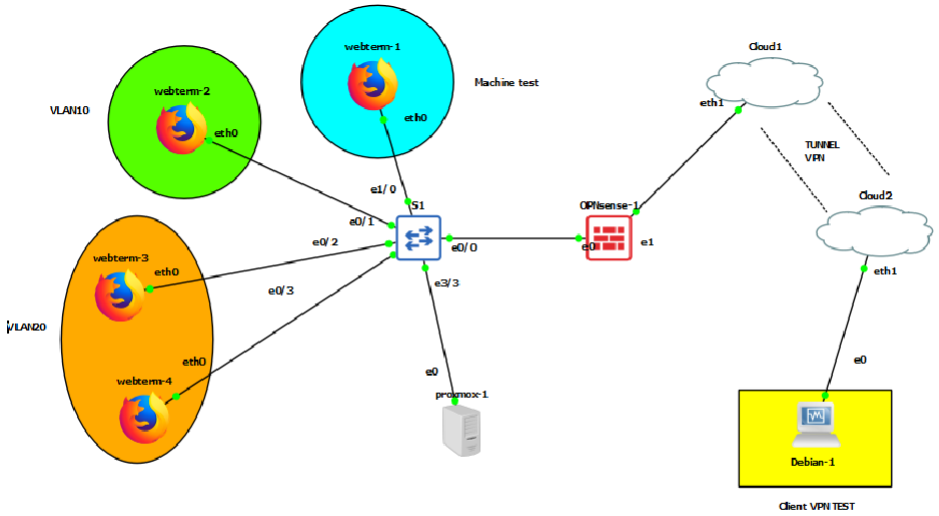




PREMIER TEST CISCOPKT UN AVEC SWITCH DE NIVEAU 1 L'AUTRE EN AJOUTANT UN NIVEAU 3



CONFIGURATION TEST SUR DRAW.IO POUR IMAGER AU MIEUX L'INFRASTRUCTURE DU PROJET



DERNIERE CONFIGURATION DE L'INFRA SUR GNS3 (pare-feu ensuite remplacé par pfsense)

Plan d'adressage IP :

Ici deux tableaux, un avec le réseau réel et utilisé dans le cadre du projet, l'autre avec le réseau fictif utilisé dans le cadre du projet :

PLAN D'ADRESSAGE IP PROJET					
GROUPE CONCERNE	VLAN	VLAN-NAME	PROJECT-NETWORK	MASK	VLAN-NETWORK
Accueil	10	Accueil	192.168.128.0/24	255.255.255.0	192.168.10.0/24
Atelier	20	Atelier	192.168.128.0/24	255.255.255.0	192.168.20.0/24
Administratifs / finaces	30	Administratifs / finaces	192.168.128.0/24	255.255.255.0	192.168.30.0/24
Expédition	40	Expédition	192.168.128.0/24	255.255.255.0	192.168.40.0/24
Informatique	50	Informatique	192.168.128.0/24	255.255.255.0	192.168.50.0/24
Logistique	60	Logistique	192.168.128.0/24	255.255.255.0	192.168.60.0/24
Production	70	Production	192.168.128.0/24	255.255.255.0	192.168.70.0/24
R&D / qualité	80	R&D / qualité	192.168.128.0/24	255.255.255.0	192.168.80.0/24
Commercials	90	Commercials	192.168.128.0/24	255.255.255.0	192.168.90.0/24
Direction	100	Direction	192.168.128.0/24	255.255.255.0	192.168.100.0/24

Et le second :

PLAN D'ADRESSAGE A PARTIR DES VMBR DES USERS						
plan d'adressage machines Bastien				plan d'adressage machines Lucas		
NETWORK	**IP-ADDRESS**	**MASK**		**NETWORK**	**IP-ADDRESS**	**MASK**
WAN	10.31.20.0	255.255.255.0		WAN	10.31.30.0	255.255.255.0
LAN-ADMIN	10.31.21.0	255.255.255.0		LAN-ADMIN	10.31.31.0	255.255.255.0
DMZ	10.31.22.0	255.255.255.0		DMZ	10.31.32.0	255.255.255.0
LAN-SRV	10.31.23.0	255.255.255.0		LAN-SRV	10.31.33.0	255.255.255.0
LAN-USERS	10.31.24.0	255.255.255.0		LAN-USERS	10.31.34.0	255.255.255.0
LAN-SAUVEGARDE	10.31.25.0	255.255.255.0		LAN-SAUVEGARDE	10.31.35.0	255.255.255.0
plan d'adressage machines Thomas						
NETWORK	**IP-ADDRESS**	**MASK**				
WAN	10.31.90.0	255.255.255.0				
LAN-ADMIN	10.31.91.0	255.255.255.0				
DMZ	10.31.92.0	255.255.255.0				
LAN-SRV	10.31.93.0	255.255.255.0				
LAN-USERS	10.31.94.0	255.255.255.0				
LAN-SAUVEGARDE	10.31.95.0	255.255.255.0				

Technologies retenues et pourquoi ? :

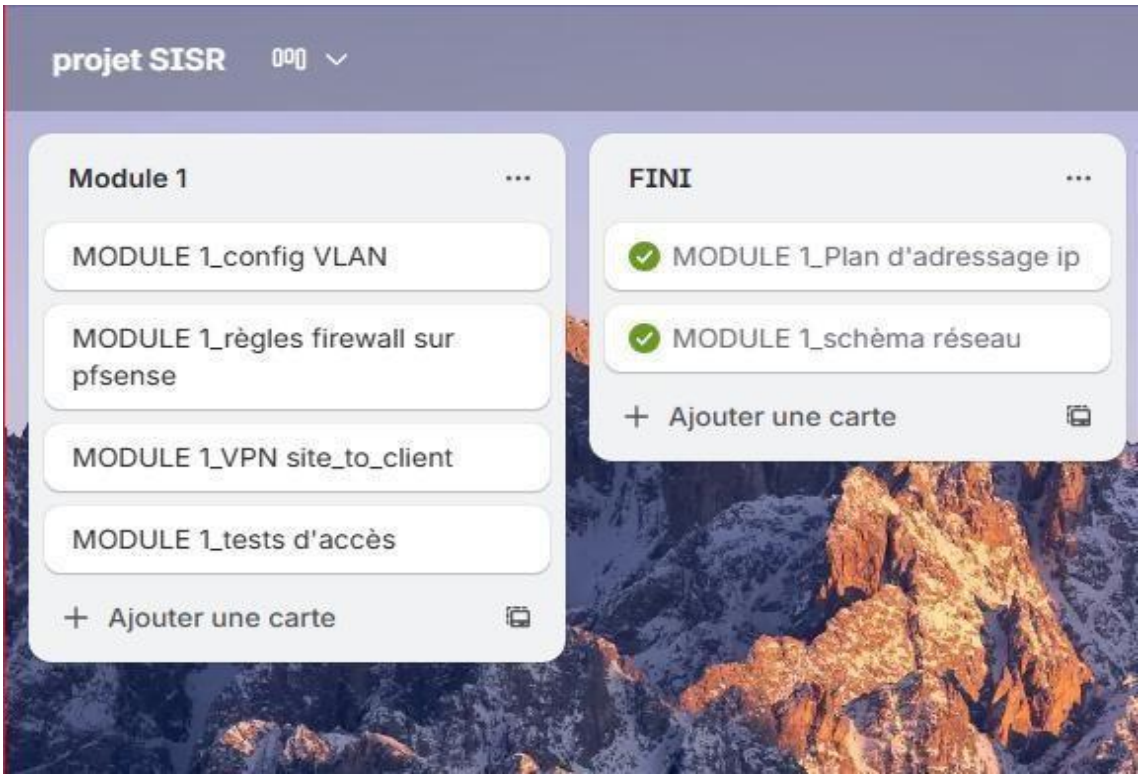
Dans le cadre de ce projet nous avons ajouté notre petite touche en ce qui concerne les logiciels ou outils que nous avons utilisés :

Dans le cadre du projet il nous est demandé d'adopter une méthode SCRUM ou AGILE donc nous avons choisi d'utiliser Trello, plateforme TRES connue et utilisée pour de la gestion de tickets et de taches, Trello est un outil de gestion de projet en ligne.

En parallèle de cela, nous aurions pu faire un diagramme de GANTT, mais la charge de travail étant déjà assez conséquente, nous avons préférés nous concentrer sur le côté technique et conception

Trello permet en plus de créer des taches, jalons et priorités, de créer des tableaux partagés dans lesquels un groupe peux gérer leurs parties respectives.

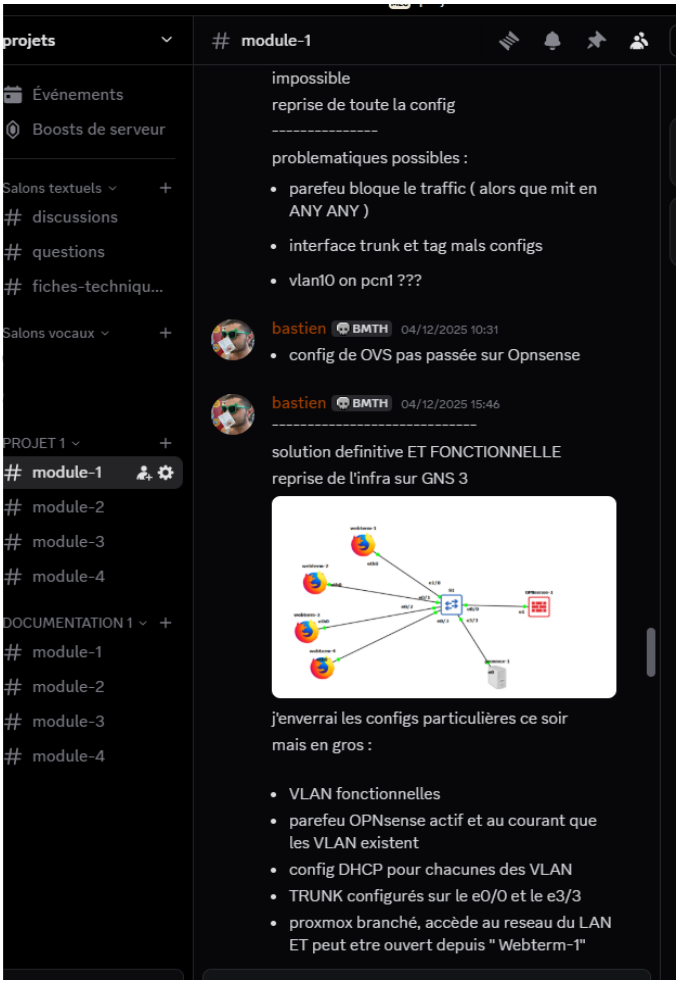
Prenons par exemple notre Trello, édité en fonction des taches qui ont été effectuées



Outil aujourd'hui beaucoup utilisé, Discord est « un réseau social » dans lequel on peut autant échanger textuellement que avec des pièces jointes (photos/fichiers)

En tant qu'étudiants en informatique, beaucoup de nos communications se font par Discord, nous avons donc crée un groupe pour le projet séparé en plusieurs Salons, où chacun a pu expliquer son avancé, ses difficultés et surtout poser des questions à son groupe lorsqu'il travaillait depuis chez lui

Ci-joint un exemple type des échanges :



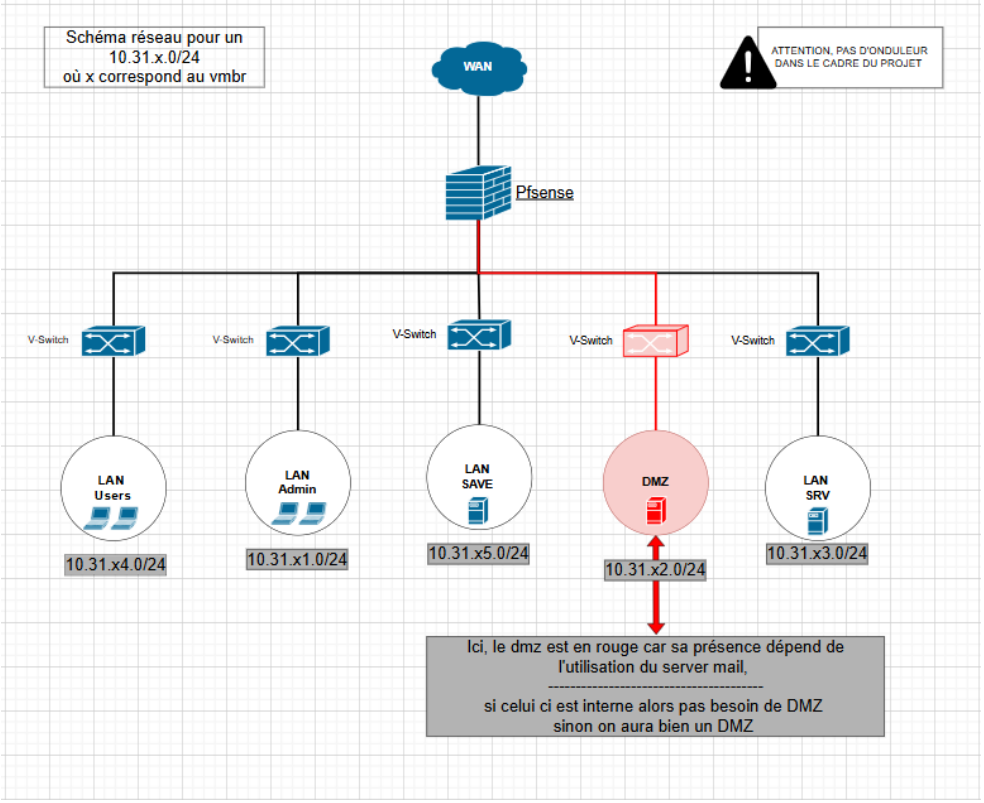
On ne le présente plus, aujourd'hui c'est l'éditeur de texte par excellence !

La rédaction de ce dossier n'échappe pas à la règle, il est entièrement rédigé et présenté sur Word ! Choisi je pense pour sa facilité d'utilisation, l'ensemble des documents que j'ai pu rédiger pour ce projet ont été édités à un moment ou un autre sur Word

Drawio est une plateforme de design graphique utilisée dans l'informatique pour créer tous types de diagrammes.

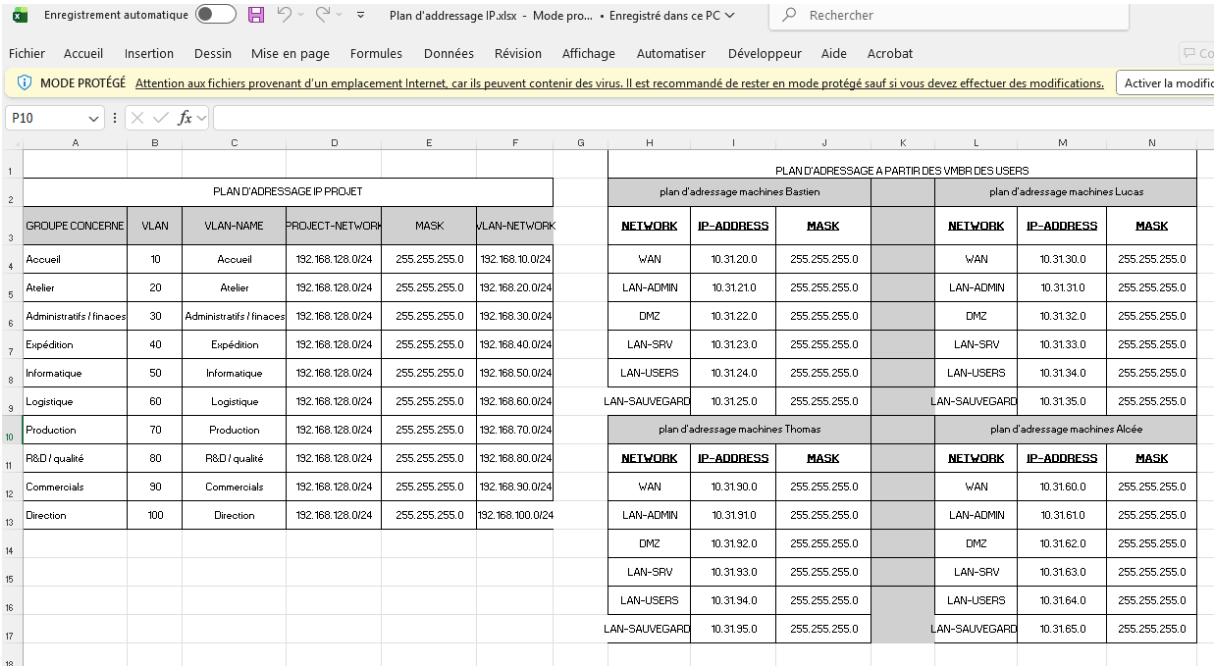
Complètement gratuit (sauf certaines icones par exemple), on peut tout faire en ce qui concerne les designs plutôt basiques

Dans notre cas, surtout utilisé pour la création d'une première maquette graphique du projet, il nous a servi à nous projeter et imaginer au mieux comment nous allions paramétrer toute notre infrastructure.



Du pack office également, il est le tableur par excellence, tout ce qui est traitement de données ou bien configuration de tableaux

Dans le cadre de ce projet, je me suis servi d'Excel pour créer les tableau d'adressage IP. J'ai choisi ce logiciel pour la facilité de prise en main et l'expérience que j'avais déjà dessus.



Enregistrement automatique — Plan d'addressage IP.xlsx - Mode pro... • Enregistré dans ce PC — Rechercher

Fichier Accueil Insertion Dessin Mise en page Formules Données Révision Affichage Automatiser Développeur Aide Acrobat

MODE PROTÉGÉ Attention aux fichiers provenant d'un emplacement Internet, car ils peuvent contenir des virus. Il est recommandé de rester en mode protégé sauf si vous devez effectuer des modifications. Activer la modific

P10

PLAN D'ADRESSAGE IP PROJET

GROUPE CONCERNE	VLAN	VLAN-NAME	PROJECT-NETWORK	MASK	VLAN-NETWORK
Accueil	10	Accueil	192.168.128.0/24	255.255.255.0	192.168.10.0/24
Atelier	20	Atelier	192.168.128.0/24	255.255.255.0	192.168.20.0/24
Administratifs / finaces	30	Administratifs / finaces	192.168.128.0/24	255.255.255.0	192.168.30.0/24
Expédition	40	Expédition	192.168.128.0/24	255.255.255.0	192.168.40.0/24
Informatique	50	Informatique	192.168.128.0/24	255.255.255.0	192.168.50.0/24
Logistique	60	Logistique	192.168.128.0/24	255.255.255.0	192.168.60.0/24
Production	70	Production	192.168.128.0/24	255.255.255.0	192.168.70.0/24
R&D / qualité	80	R&D / qualité	192.168.128.0/24	255.255.255.0	192.168.80.0/24
Commercials	90	Commercials	192.168.128.0/24	255.255.255.0	192.168.90.0/24
Direction	100	Direction	192.168.128.0/24	255.255.255.0	192.168.100.0/24

PLAN D'ADRESSAGE A PARTIR DES VMBR DES USERS

plan d'adressage machines Bastien

NETWORK	IP-ADDRESS	MASK
WAN	10.31.20.0	255.255.255.0
LAN-ADMIN	10.31.21.0	255.255.255.0
DMZ	10.31.22.0	255.255.255.0
LAN-SRV	10.31.23.0	255.255.255.0
LAN-USERS	10.31.24.0	255.255.255.0
LAN-SAUVEGARD	10.31.25.0	255.255.255.0

plan d'adressage machines Lucas

NETWORK	IP-ADDRESS	MASK
WAN	10.31.30.0	255.255.255.0
LAN-ADMIN	10.31.31.0	255.255.255.0
DMZ	10.31.32.0	255.255.255.0
LAN-SRV	10.31.33.0	255.255.255.0
LAN-USERS	10.31.34.0	255.255.255.0
LAN-SAUVEGARD	10.31.35.0	255.255.255.0

plan d'adressage machines Thomas

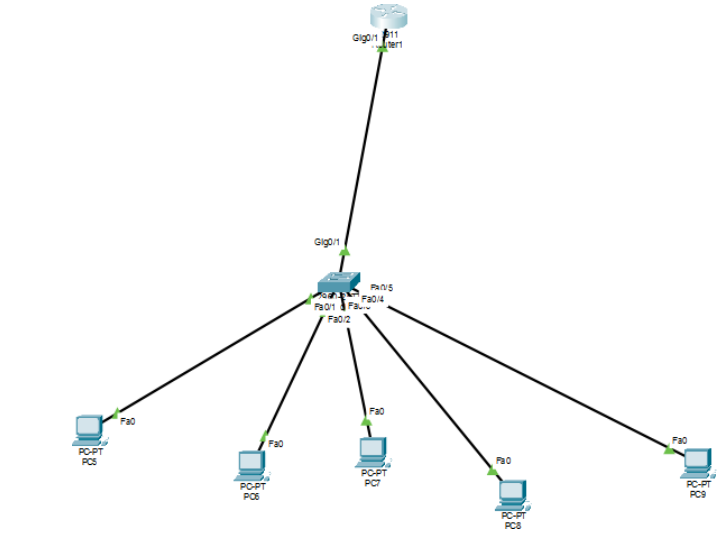
NETWORK	IP-ADDRESS	MASK
WAN	10.31.90.0	255.255.255.0
LAN-ADMIN	10.31.91.0	255.255.255.0
DMZ	10.31.92.0	255.255.255.0
LAN-SRV	10.31.93.0	255.255.255.0
LAN-USERS	10.31.94.0	255.255.255.0
LAN-SAUVEGARD	10.31.95.0	255.255.255.0

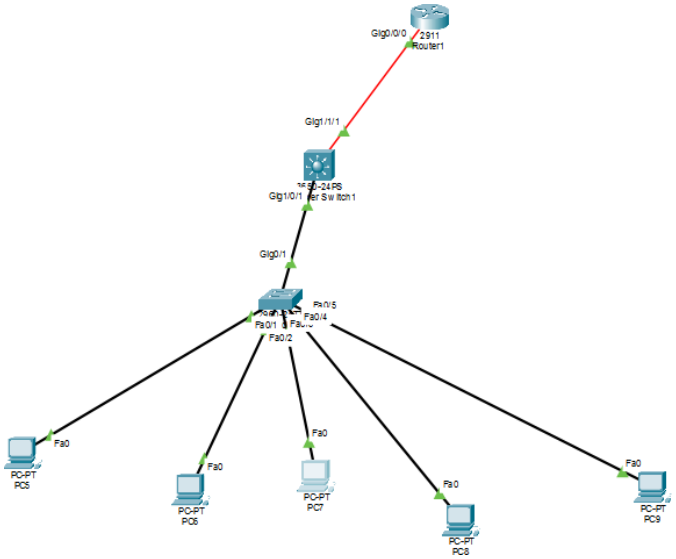
plan d'adressage machines Alcée

NETWORK	IP-ADDRESS	MASK
WAN	10.31.60.0	255.255.255.0
LAN-ADMIN	10.31.61.0	255.255.255.0
DMZ	10.31.62.0	255.255.255.0
LAN-SRV	10.31.63.0	255.255.255.0
LAN-USERS	10.31.64.0	255.255.255.0
LAN-SAUVEGARD	10.31.65.0	255.255.255.0

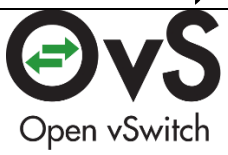
Plus précisément packet tracer, est un logiciel permettant de simuler des infrastructures informatiques (que ce soit les routeurs, switch ou PC pour tester tout y est !!)

Dans ma formation, j'ai déjà eu l'occasion de beaucoup l'utiliser, donc j'ai voulu mettre à profit ce que j'avais appris pour offrir une première infrastructure à présenter.





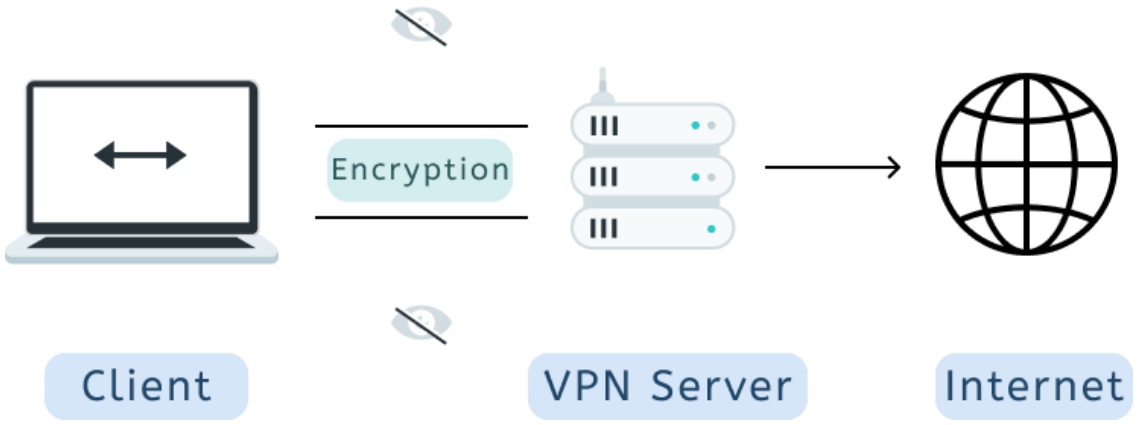
Outil de virtualisation, c'est ici que j'ai mis toutes les machines que j'ai utilisé, que ce soit des Debian ou des machines plus poussées, je les ai toutes mises ici

NOM	OVS (Virtual switch)	OPNSense
ICONE		
UTILISATION	Simuler un switch sur une machine virtuelle, se servir de la machine hôte comme switch	Le pare-feu utilisé sur le projet, C'est ici que toutes les règles seront faites, que tous les pools DHCP seront faits, que toutes les VLANS et Interfaces seront configurées
POURQUOI	Le switch fourni à l'origine n'était pas configurable en VLAN,	Ayant déjà travaillé avec pfSense, c'était l'occasion d'essayer quelque chose de nouveau PUIS pour la configuration VPN il y avait un paquet inclus (présenté juste en dessous)

Client VPN utilisé dans le cadre du projet pour configurer les accès distants

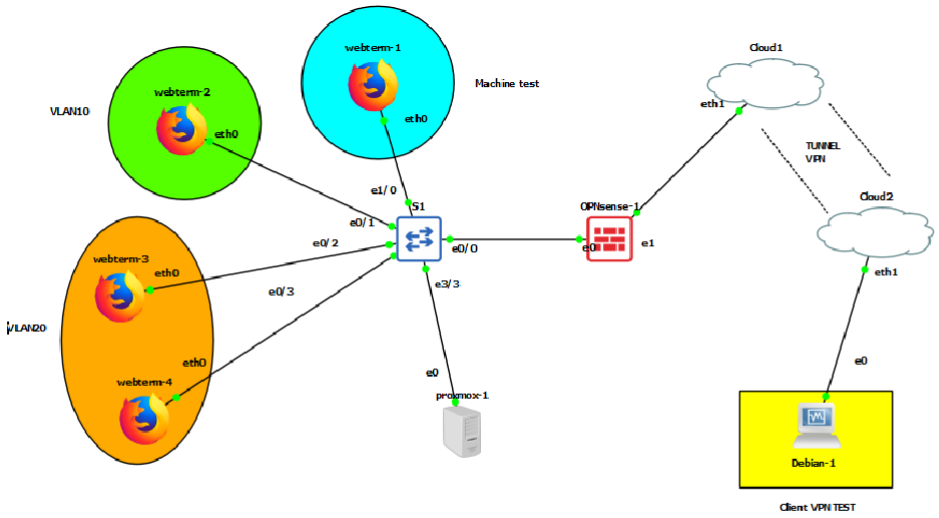
Choisi pour deux raisons

- L'intuitivité des commandes pour la configuration
- Le fait qu'il soit interne a OPNSense (le pare-feu) c'était donc bien plus rapide que d'installer des packages qui n'auraient peut être pas fonctionnés



MISE EN ŒUVRE :

Configuration finale sur GNS3 :



Le principe de cette architecture est assez simple, exploiter au mieux les VLAN , découvrir comment bien configurer cela :

- Il m'a fallu faire toute la configuration des VLAN (access, trunk)
- Mettre en place un pare-feu,(les configurations ici présentent un OPNSense qui sera ensuite remplacé par un pfSense pour plus de stabilité sur GNS3)
- Enfin créer des accès VPN depuis le pare-feu

Première étape identique aux autres test, ajouter les VLAN au switch et configurer le port trunk

Pour au final obtenir :

```
S1(config)#do sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2
10   VLAN0010                         active    Et0/1
20   VLAN0020                         active    Et0/2, Et0/3
30   VLAN0030                         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
20   enet  100020     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
------- --------- ----------------- ------------------------------------------
```

Ici on voit les VLAN configurées, et les ports qui leurs ont été donnés

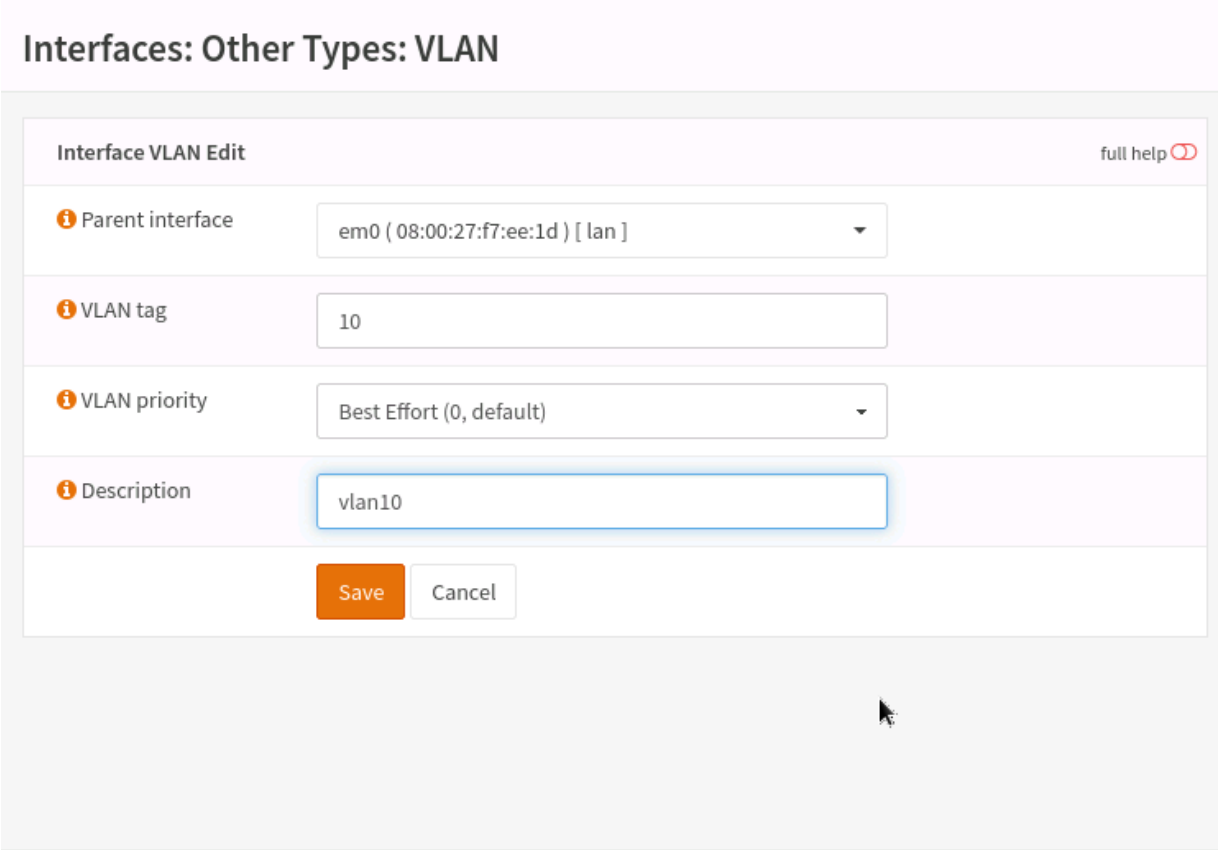
```
S1(config)#do sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1
Et3/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       1-4094
Et3/3       10,20,30

Port        Vlans allowed and active in management domain
Et0/0       1,10,20,30
Et3/3       10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1,10,20,30
Et3/3       10,20,30
S1(config)#
```

Et ici, les trunks configurés vers le Wan et le Proxmox

Le plus « complexe des configurations sur le switch sont terminées, maintenant il faut surtout connecter le tout, donc on va sur le pare-feu et on commence les configuration :

- Créer l'interface pour la VLAN
- L'allumer
- Configurer le DHCP en fonction de l'interface choisie
- Créer une règle sur le pare-feu pour autoriser le traffic DHCP
- Puis au final passer les machines en DHCP

Création des interfaces :



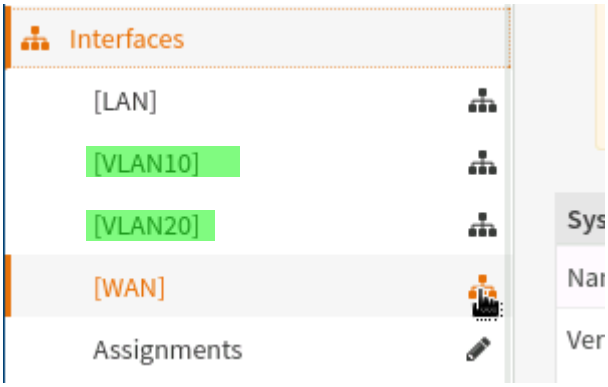
Très important,

Il faut renseigner sur quelle interface on veut que le VLAN soit connecté,

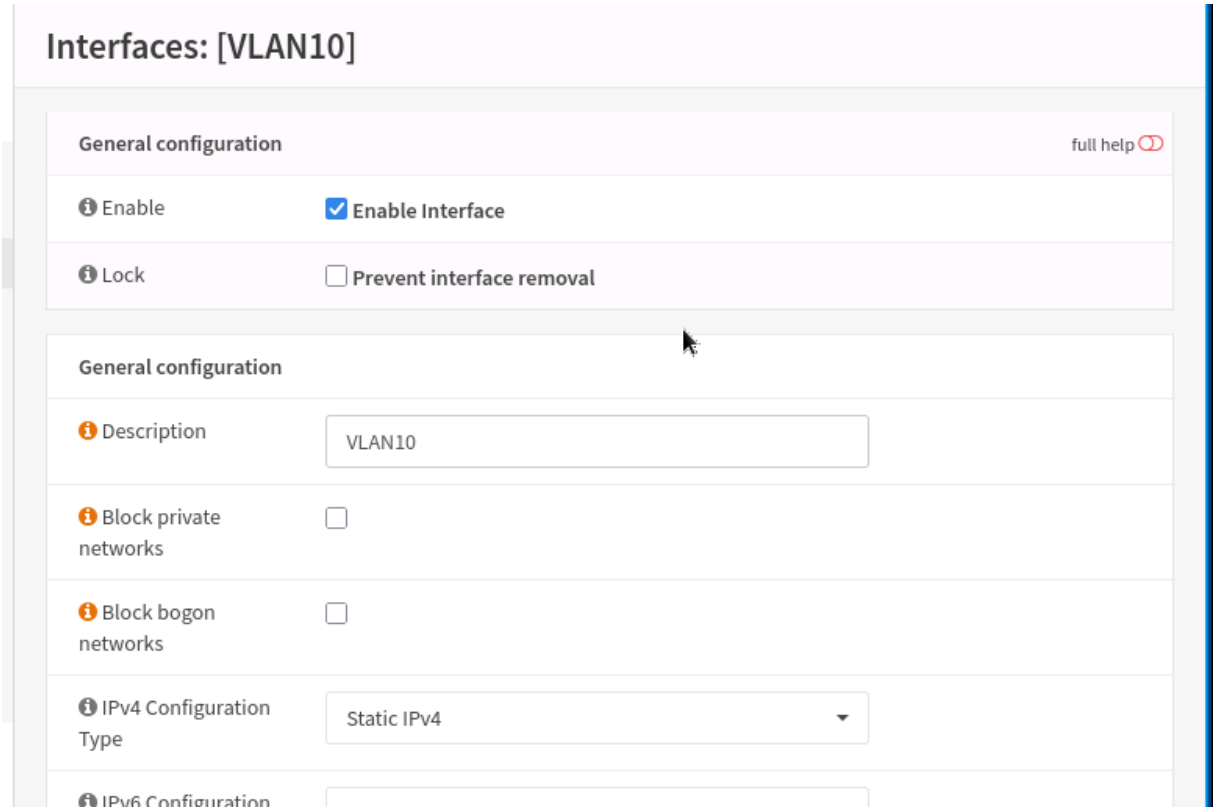
Il faut IMPERATIVEMENT que ce soit sur le LAN, le VLAN est là pour segmenter le réseau, on ne va pas le connecter sur le WAN, non seulement cela ne marchera pas, mais ça serait inutile

On notifie également le « tag » de la vlan qui permettra de l'identifier

Une fois tout cette partie configurée, l'interface apparait et devient disponible :



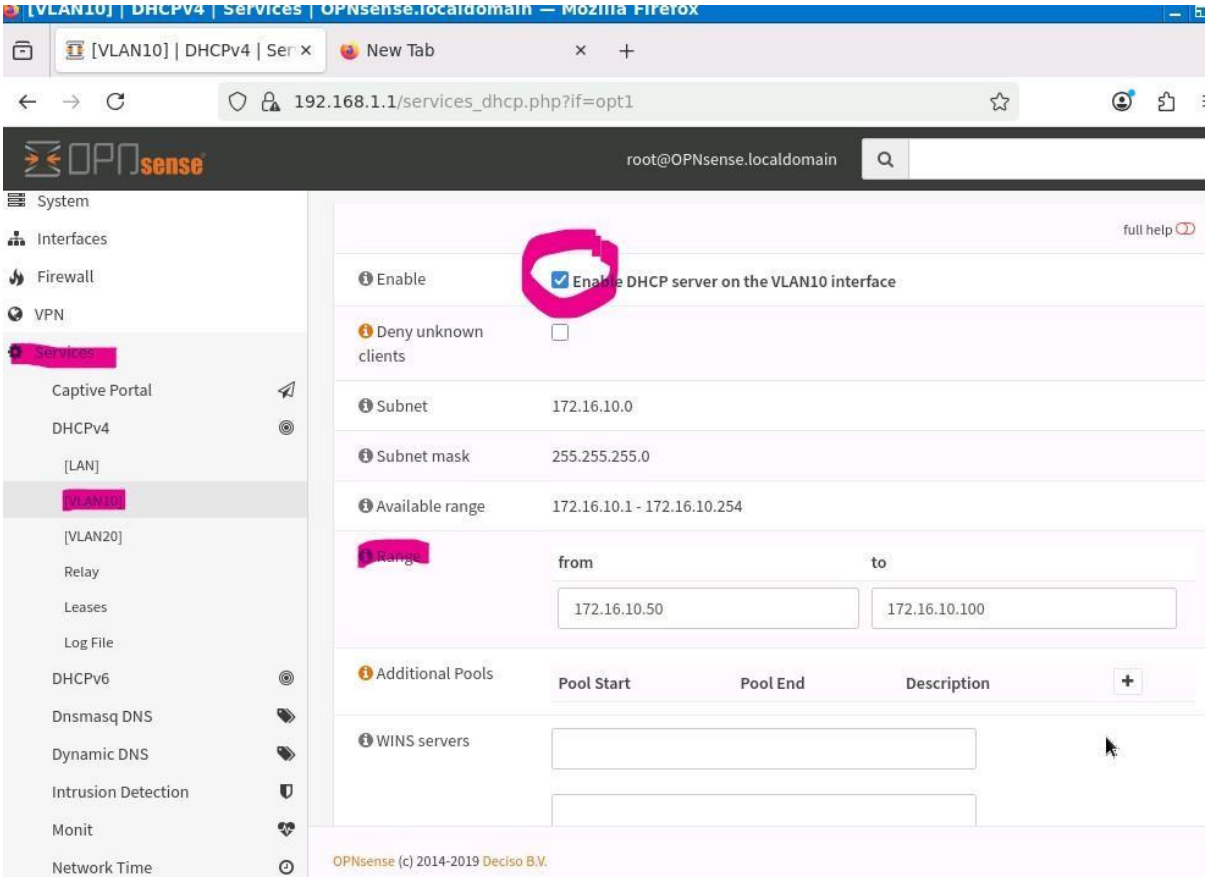
Puis en cliquant dessus, pour assurer leurs bon fonctionnement, on les allumes :



C'est seulement une fois que tout cela est fait, que les interfaces crées apparaissent dans la section DHCP,

On peut donc créer les pool DHCP de sorte que toutes les VLAN puissent avoir une adresse dynamiquement.

Un des avantages de OPNSense et pfsense sont la facilité de prise en main, la création du pool est très intuitive, il suffit de cocher des cases et renseigner les informations requises :



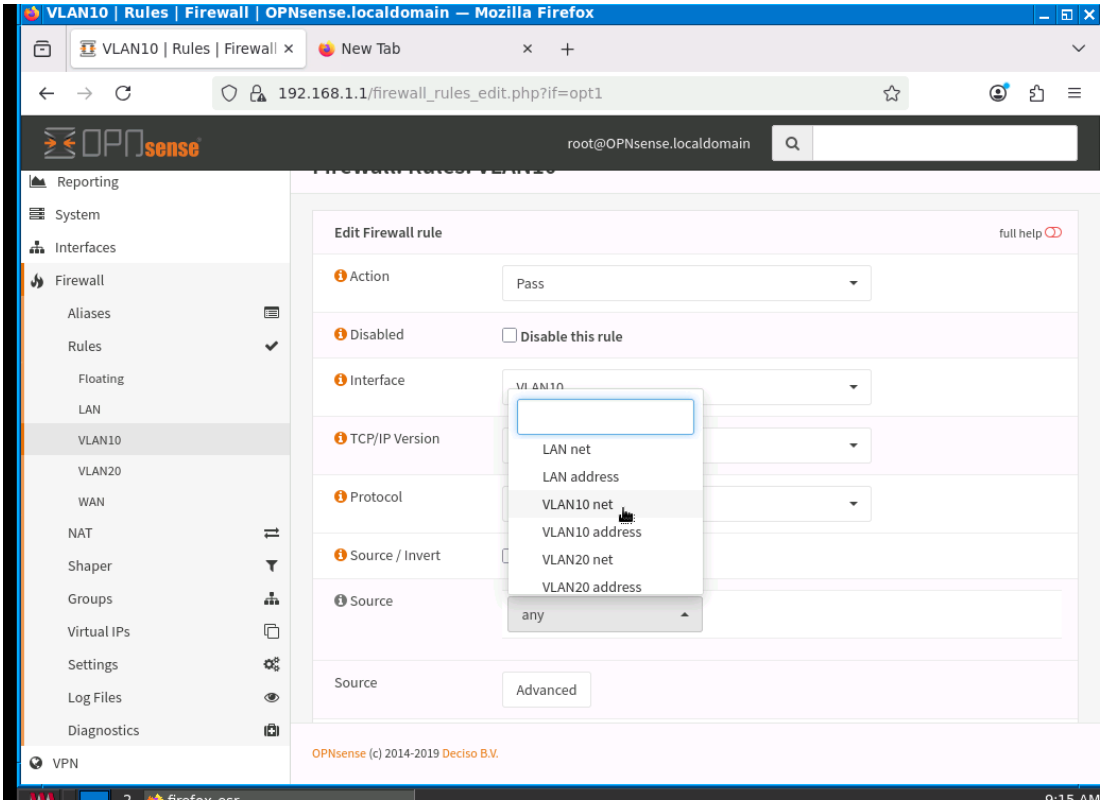
On active le DHCP pour l'interface choisie (processus ici répété pour les différentes VLAN)

On renseigne le range (écart) des adresses que l'on veut donner

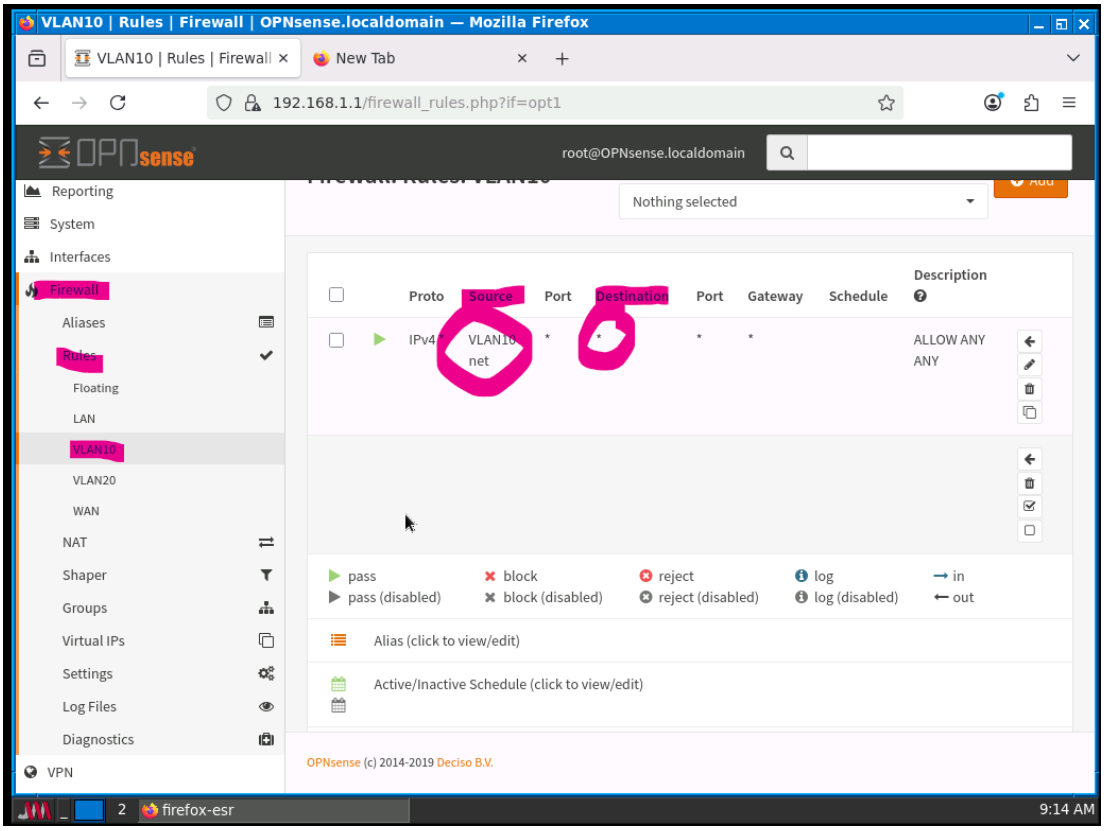
Un peu plus bas sur la page, on renseigne le DNS

Et la création du pool est finie !

Puis comme sur la situation avec OVS, il faut autoriser le passage sur le pare-feu :



On choisit les nets de la vlan en tant que sources et on laisse passer tous types de protocoles pour avoir une règle comme celle-ci-dessous :



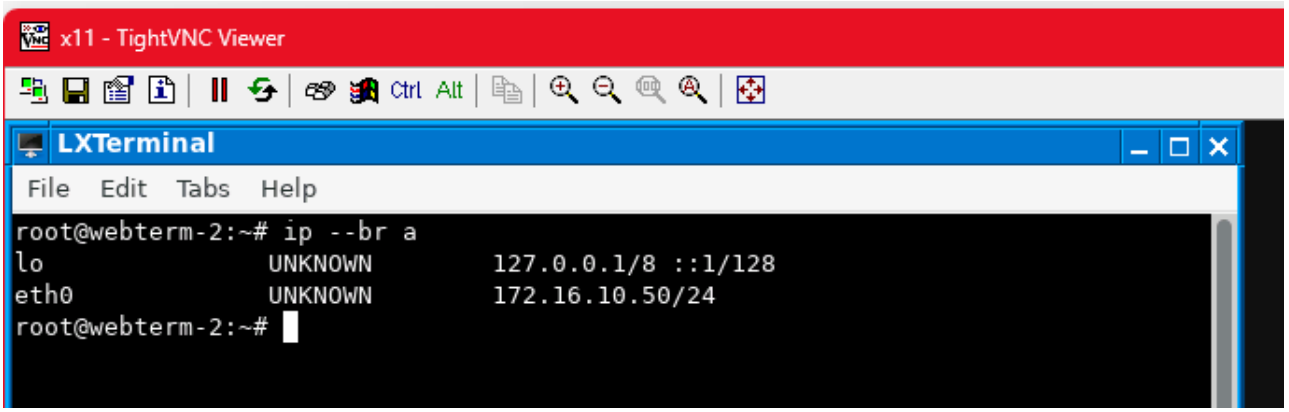
Enfin pour vérifier que tout fonctionne on passe les machines sur un mode DHCP

La première et seule étape c'est dans modifier le /etc/network/interfaces

```
lo                UNKNOWN        127.0.0.1/8 ::1/128
eth0              UNKNOWN        172.16.10.50/24
root@webterm-2:~# cat /etc/network/interfaces
#
# This is a sample network config, please uncomment lines to configure the netwo
rk
#

# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
#auto eth0
#iface eth0 inet static
#       address 192.168.0.2
#       netmask 255.255.255.0
#       gateway 192.168.0.1
#       up echo nameserver 192.168.0.1 > /etc/resolv.conf

# DHCP config for eth0
auto eth0
iface eth0 inet dhcp
#       hostname webterm-2
root@webterm-2:~#
```

On décoche la zone concernant le DHCP commentée et on redémarre le réseau avec Systemctl restart networking

Puis en redémarrant la machine, on vérifie notre IP et si tout va bien alors on a une adresse IP dynamique, prenons ici le cas d'un webterms sur le VLAN 10 :



Dernière étape de ce projet, la configuration VPN pour accès distant

Pour rappel, on configure ici un VPN site to client, l'objectif est que depuis l'extérieur de l'entreprise, on puisse accéder au réseau interne.

Sur cette configuration qui était encore parfaitement inconnue pour moi j'ai suivi une configuration précise (seul les informations importantes sont présentées ici) :

1. **Creer un CA (Certificate Authority, est une autorité de certification interne)**

System -> Trust- > Authorities > Add

Type : Internal CA

Nom : VPN-CA

Key : 2048

Save

2. **Créer certificat serveur**

System -> Trust -> Certificates -> Add

CA : VPN-CA (celui qui vient d'etre crée)

Type : Server Certificate

Nom : VPN-Server

Save

3. **Configurer serveur OpenVPN**

VPN -> OpenVPN -> Servers -> Add

Mode : Remote Access (User Auth)

Interface : WAN, Port 1194

TLS : Enabled

Certificat : VPN-Server

Tunnel Network : 10.10.10.0/24 (différent des VLANs)

IPv4 Local Network : 192.168.10.0/24,192.168.20.0/24,192.168.30.0/24

Save C Apply

4. **Ajouter utilisateurs VPN**

System -> Access -> Users -> Add

Username/Password

Ajouter certificat utilisateur

Save

5. **Configurer firewall**

WAN : Pass UDP 1194

OpenVPN : Pass VPN net vers VLANs

Save C Apply

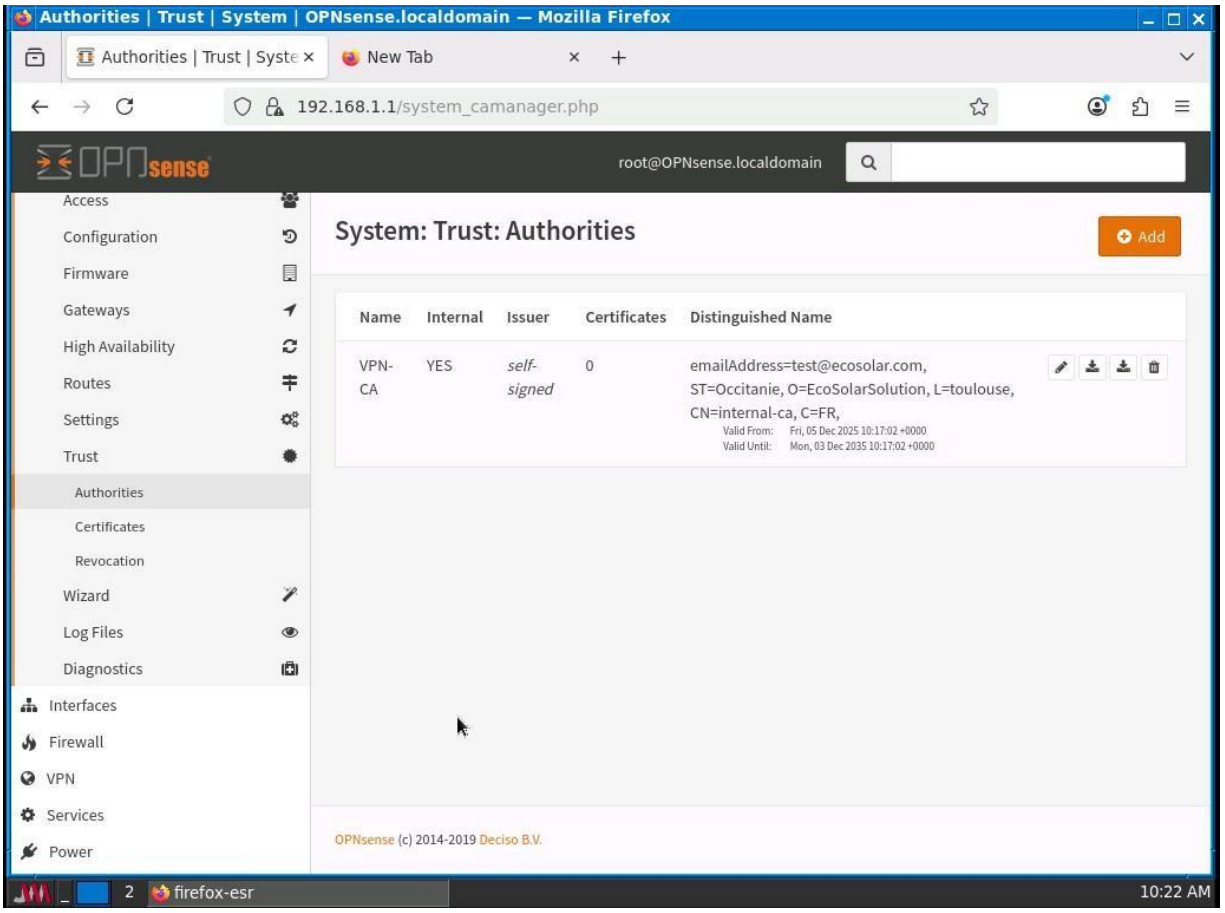
6. **Exporter client VPN**

Installer plugin client-export

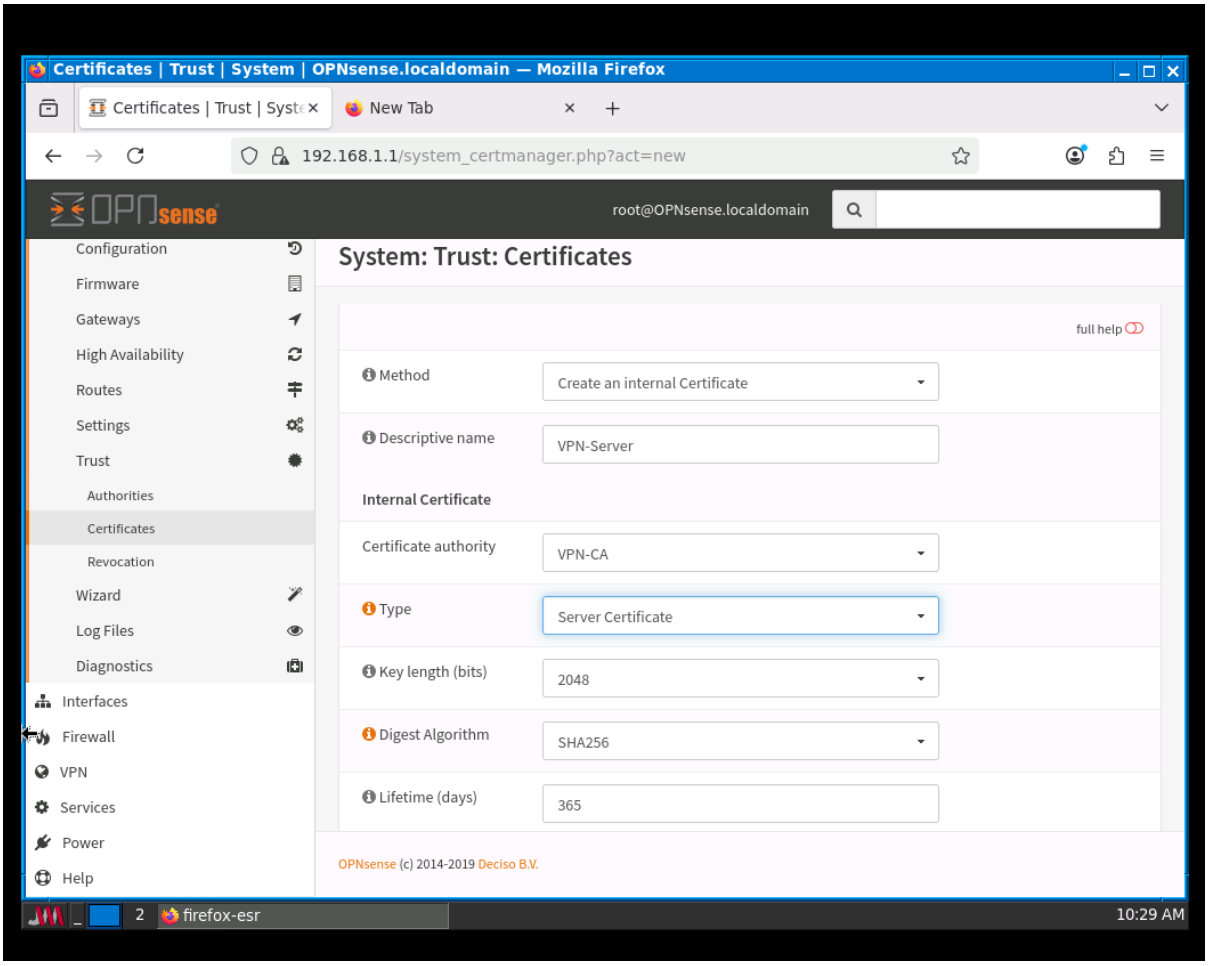
VPN -> OpenVPN -> Client Export

Télécharger .ovpn

Maintenant, à quoi tout cela ressemble de manière graphique ?

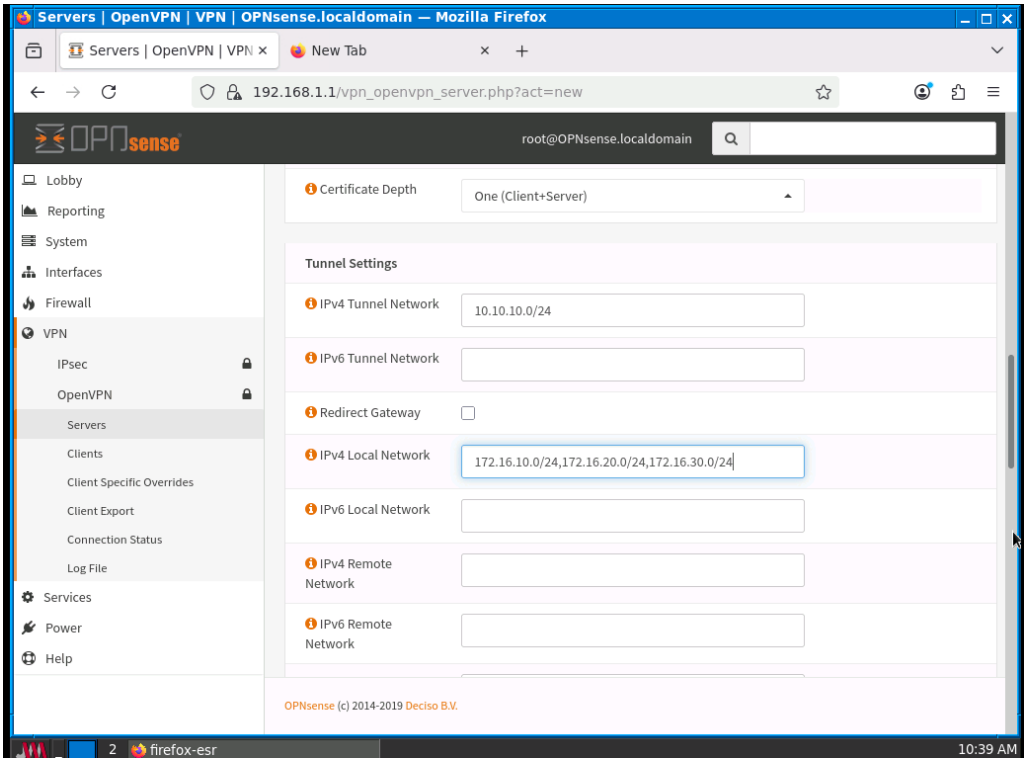


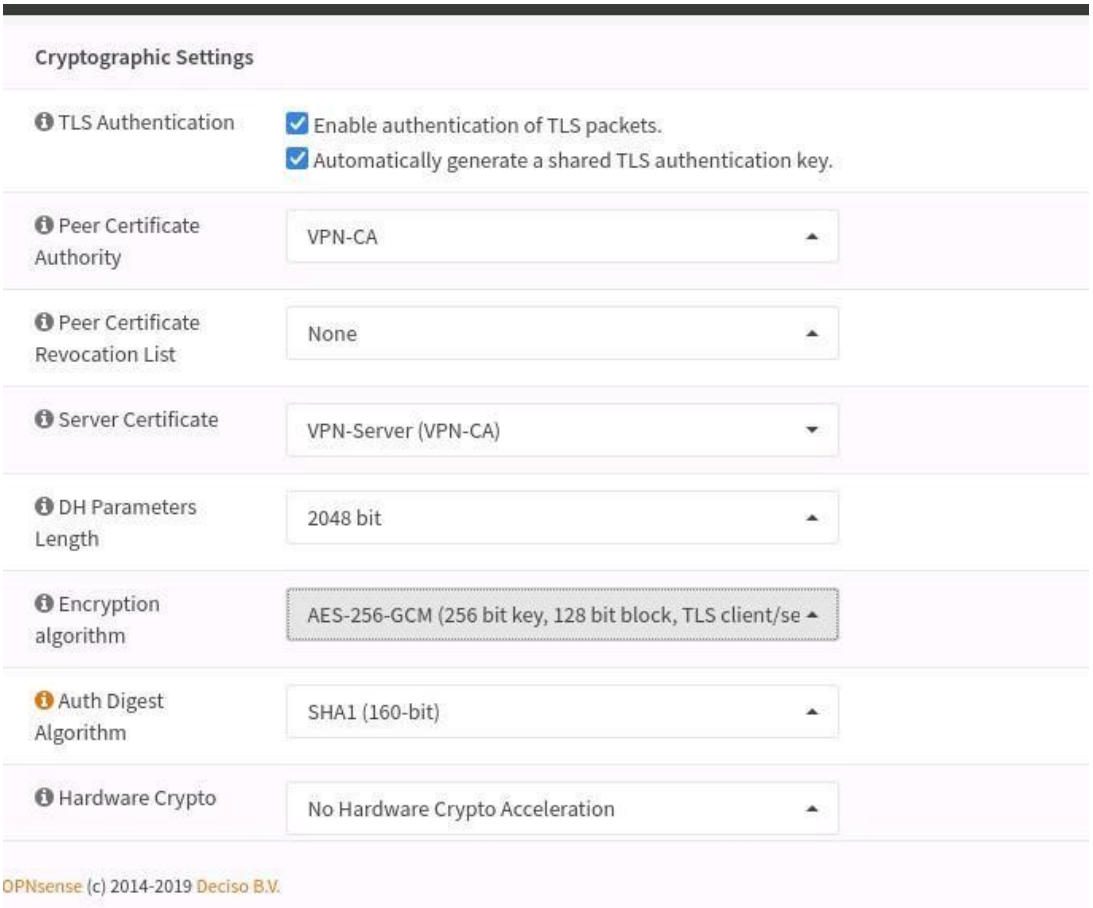
On configure le CA (autorité de certification interne pour le VPN)

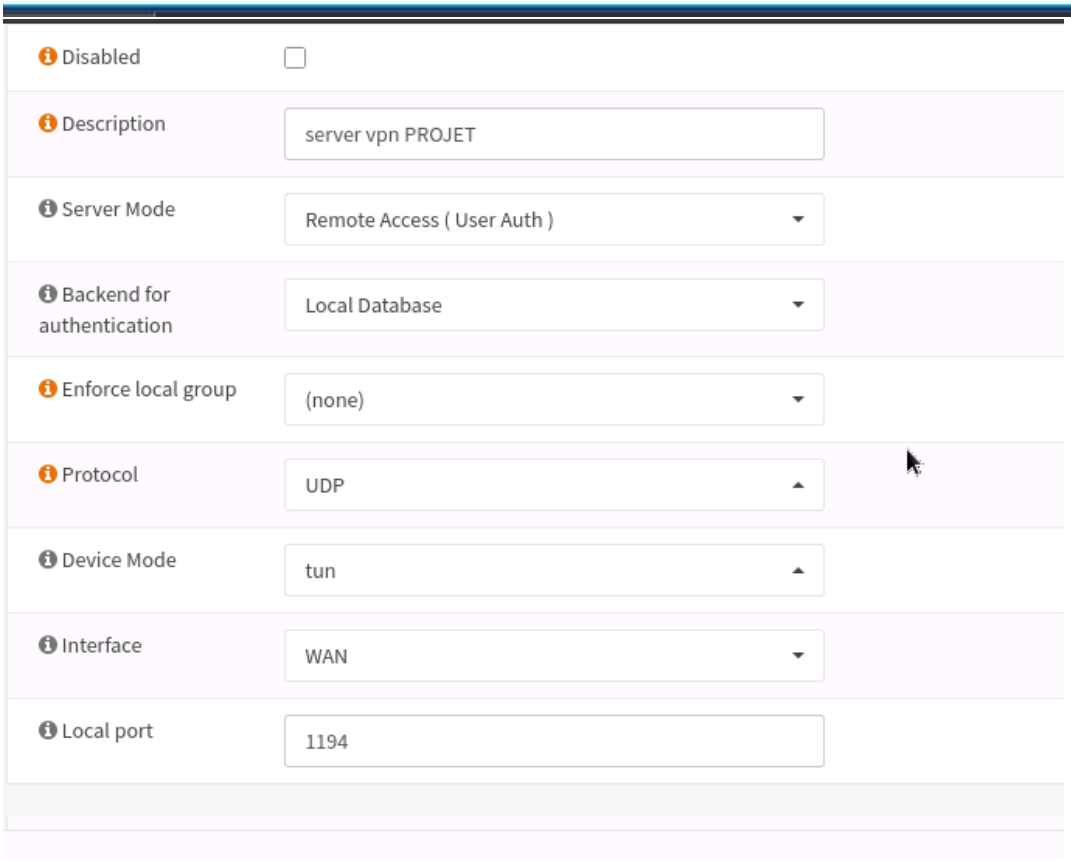


Ensuite on ajoute le certificat, à partir du CA que l'on vient de créer

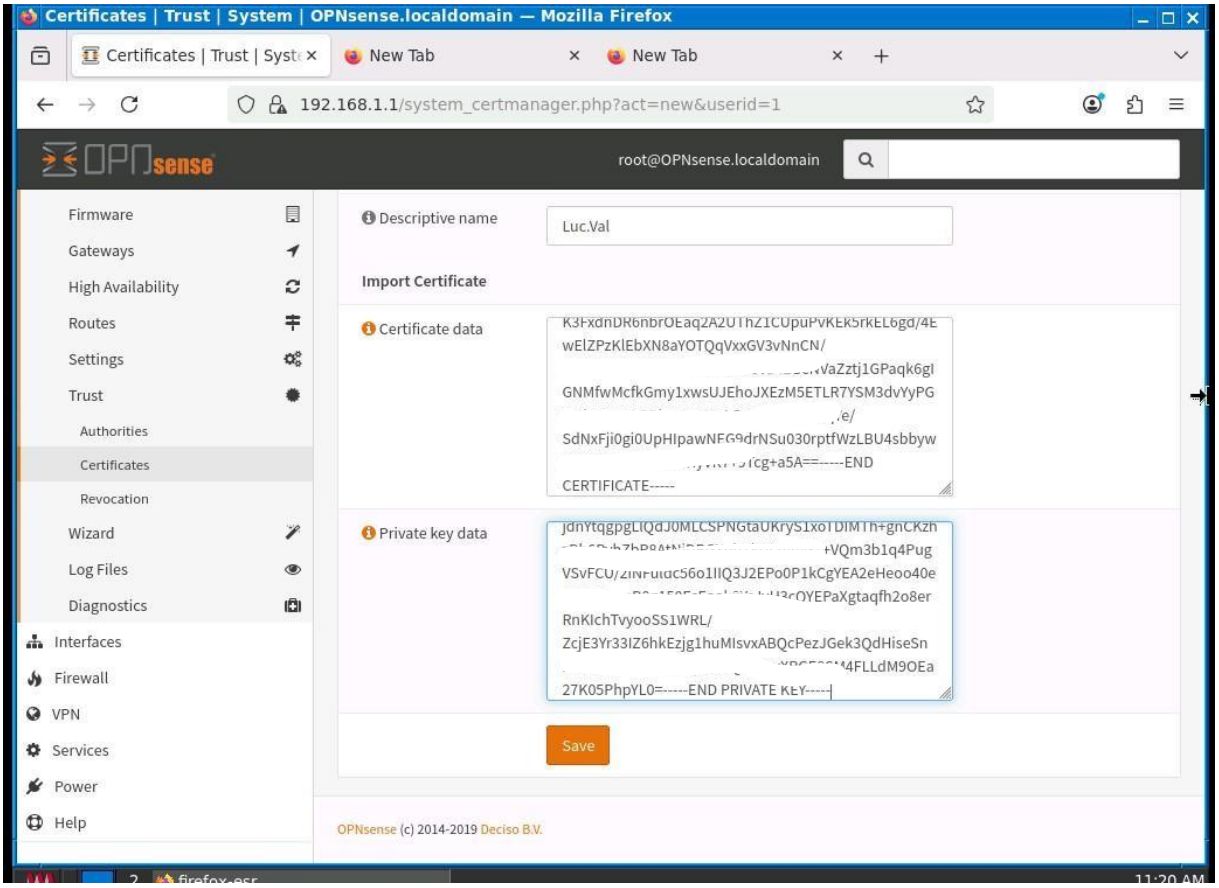
Une fois ces deux étapes faites on peut monter le server :



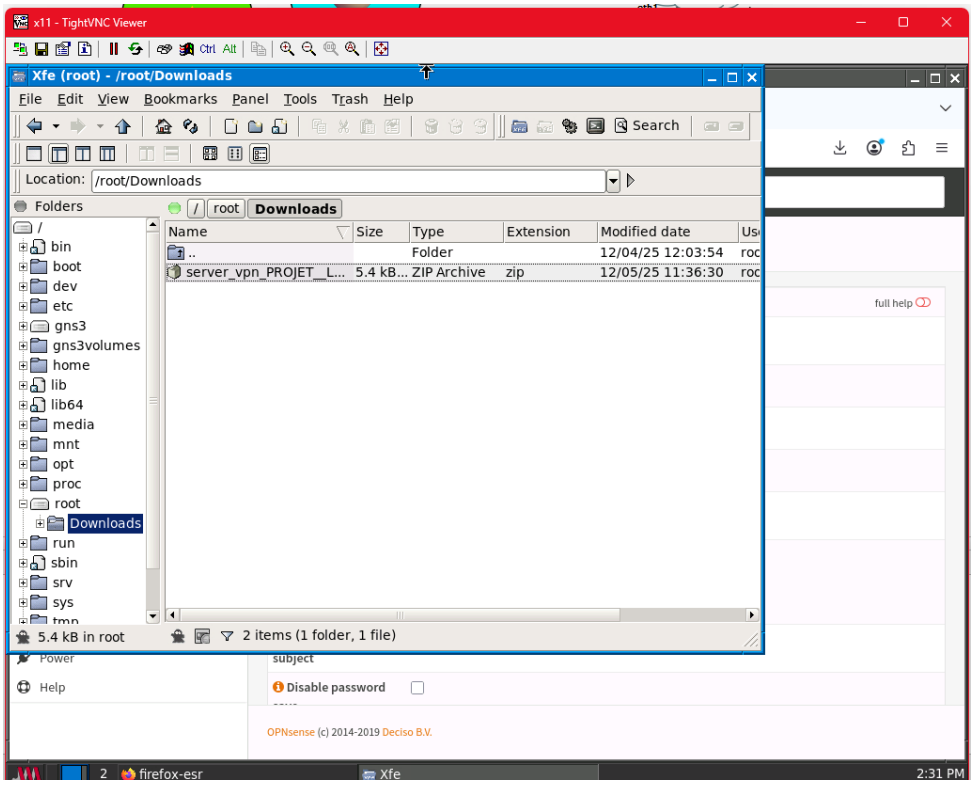

Cryptographic Settings
TLS Authentication
Enable authentication of TLS packets.
Automatically generate a shared TLS authentication key.
Peer Certificate Authority
VPN-CA
Peer Certificate Revocation List
None
Server Certificate
VPN-Server (VPN-CA)
DH Parameters Length
2048 bit
Encryption algorithm
AES-256-GCM (256 bit key, 128 bit block, TLS client/se
Auth Digest Algorithm
SHA1 (160-bit)
Hardware Crypto
No Hardware Crypto Acceleration
OPNsense (c) 2014-2019 Deciso B.V.


Disabled
Description
server vpn PROJET
Server Mode
Remote Access (User Auth)
Backend for authentication
Local Database
Enforce local group
(none)
Protocol
UDP
Device Mode
tun
Interface
WAN
Local port
1194

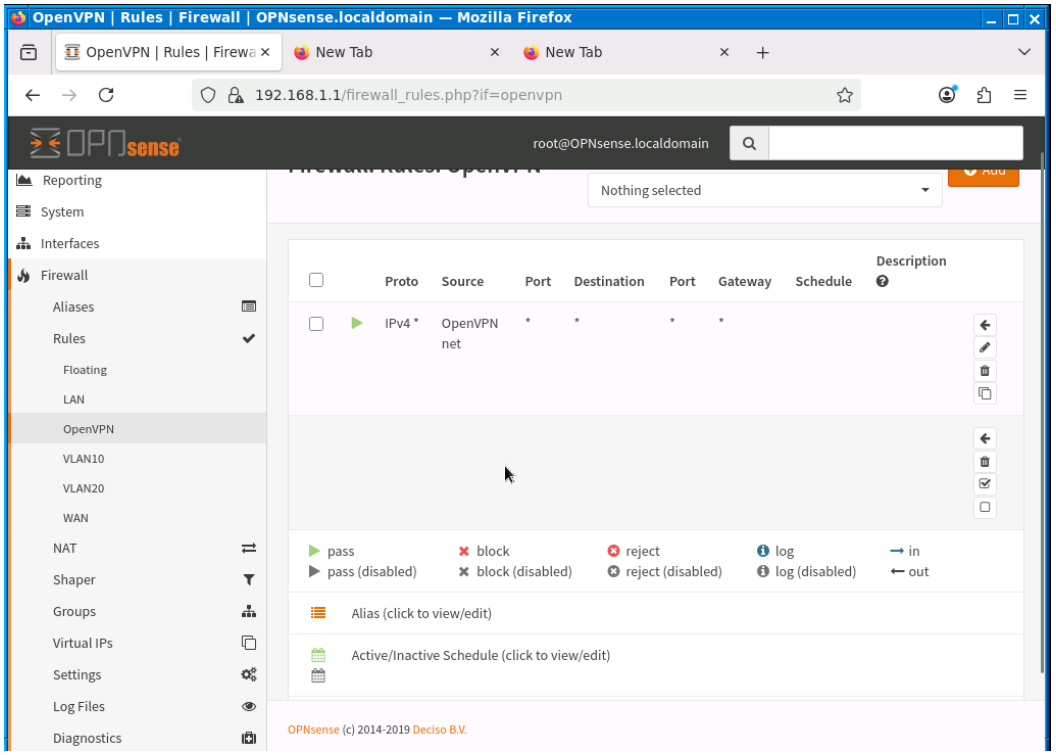
PUIS on ajoute le certificat reçu au futur client (dont une partie a été censurée volontairement)



Informations récupérée par le file manager



Puis au final on crée une rule sur le pare-feu pour permettre de laisser passer les packages VPN



CONNEXION EN SSH AU SWITCH :

Les première étapes sont de configurer le switch, pour cela plusieurs points de passage impératif :

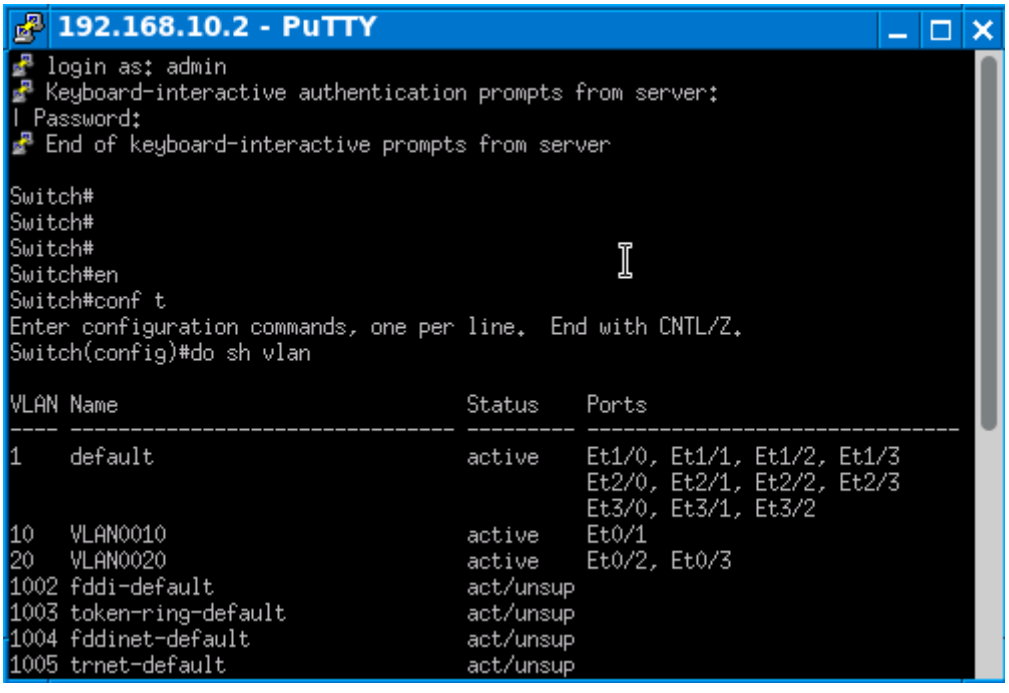
Générer la clé RSA pour la connexion
Créer un user pour sur lequel on va se connecter

```
Switch(config)#ip domain-name lab.ecosolarsolution
Switch(config)#username admin privilege 15 secret 112233
Switch(config)#crypto key generate rsa
```

Puis on configure combien de sessions en simultané on veut pouvoir accueillir
Ici de 0 à 4 donc 5 sessions

```
line vty 0 4
login local
transport input ssh
exit
```

Enfin, on installe PUTTY pour pouvoir se connecter en SSH car les versions sont différentes et parfois trop anciennes



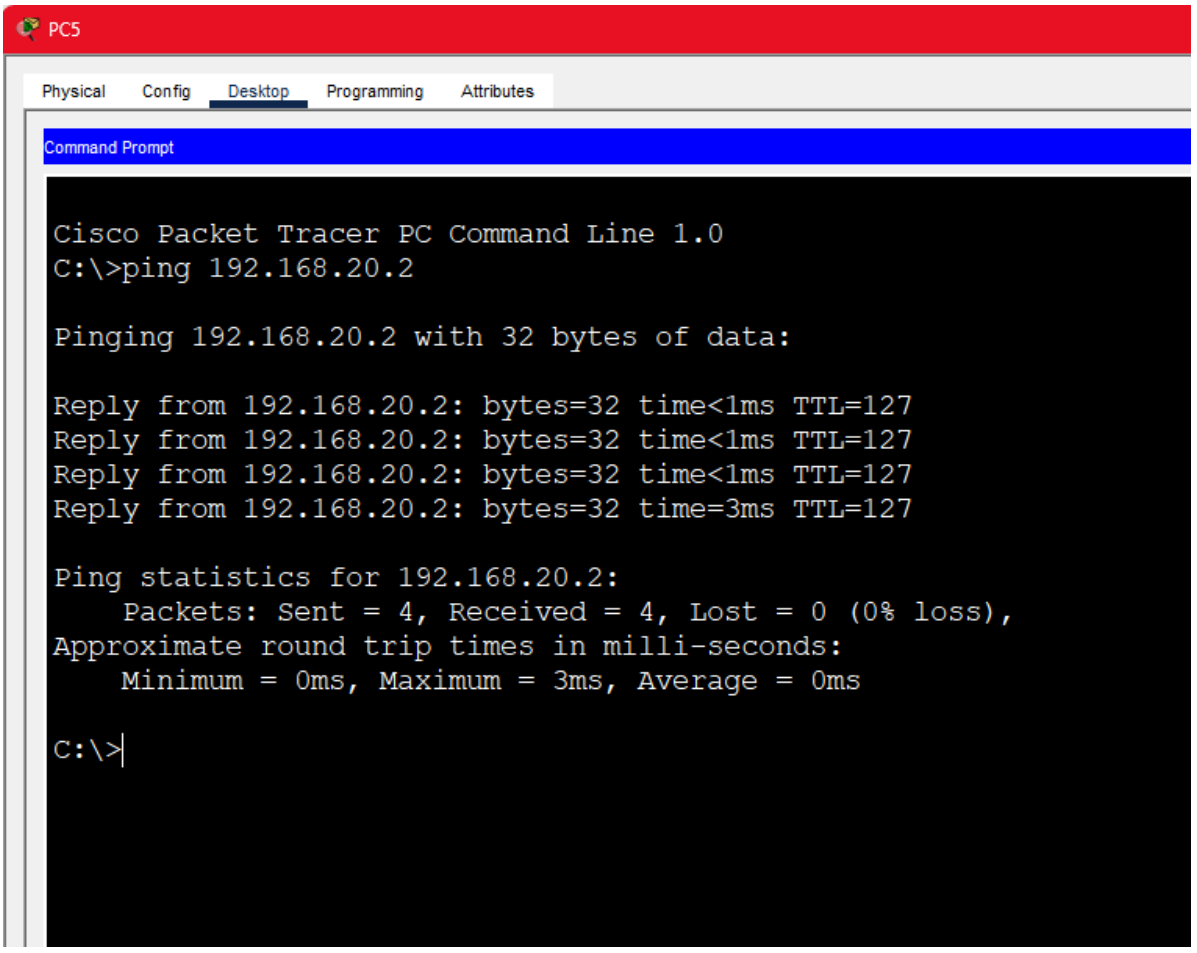
FIN DES PROCEDURES

TESTS :

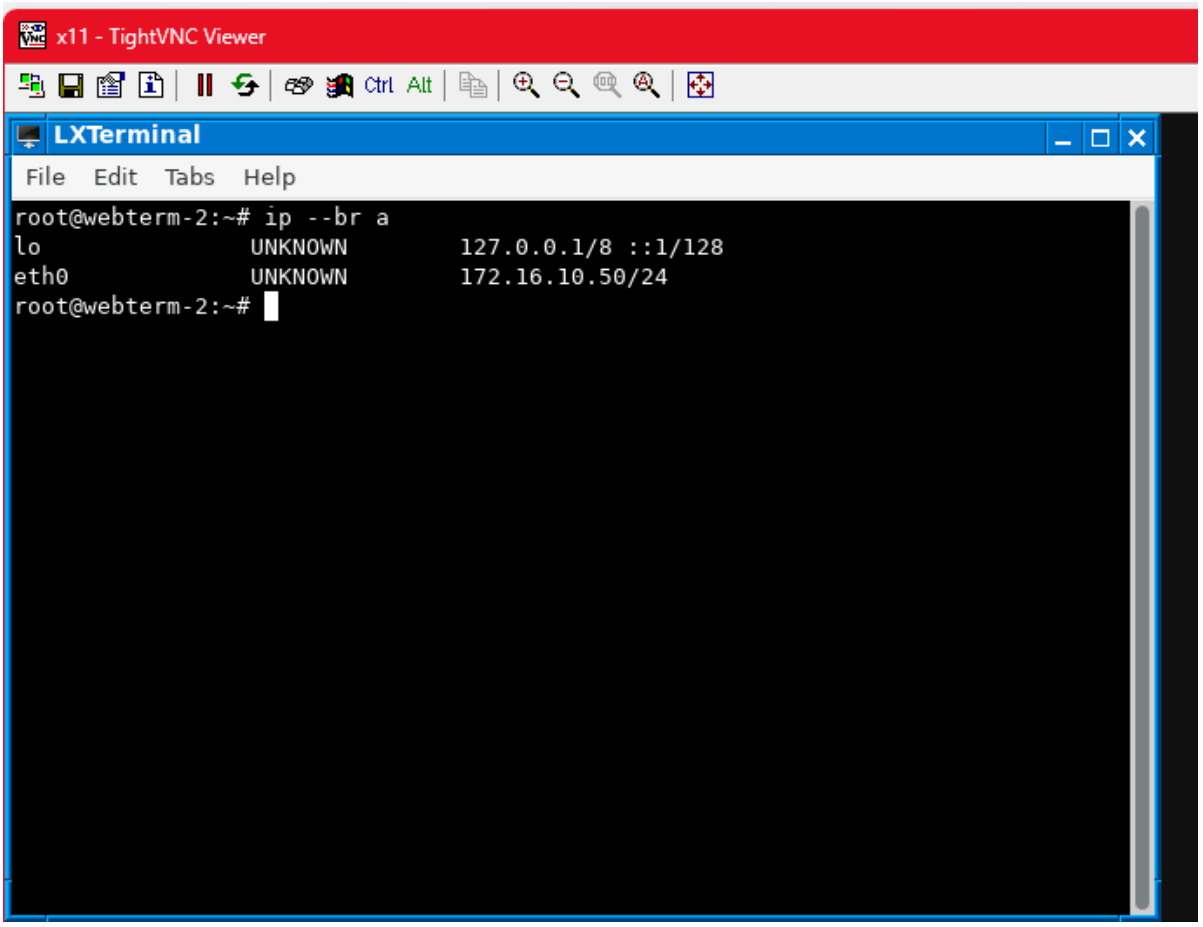
En ce qui concerne cette section du dossier, elle présentera TOUS les test, mêmes ceux des pistes explorées (voir section correspondante)

Pour la configuration faite sur Cisco, le test est des plus classiques,

Un ping inter VLAN ,



(il faut prendre en compte également que la connexion au DHCP en elle-même fait partie des tests, elle nous permet de voir si la configuration est bien aboutie)



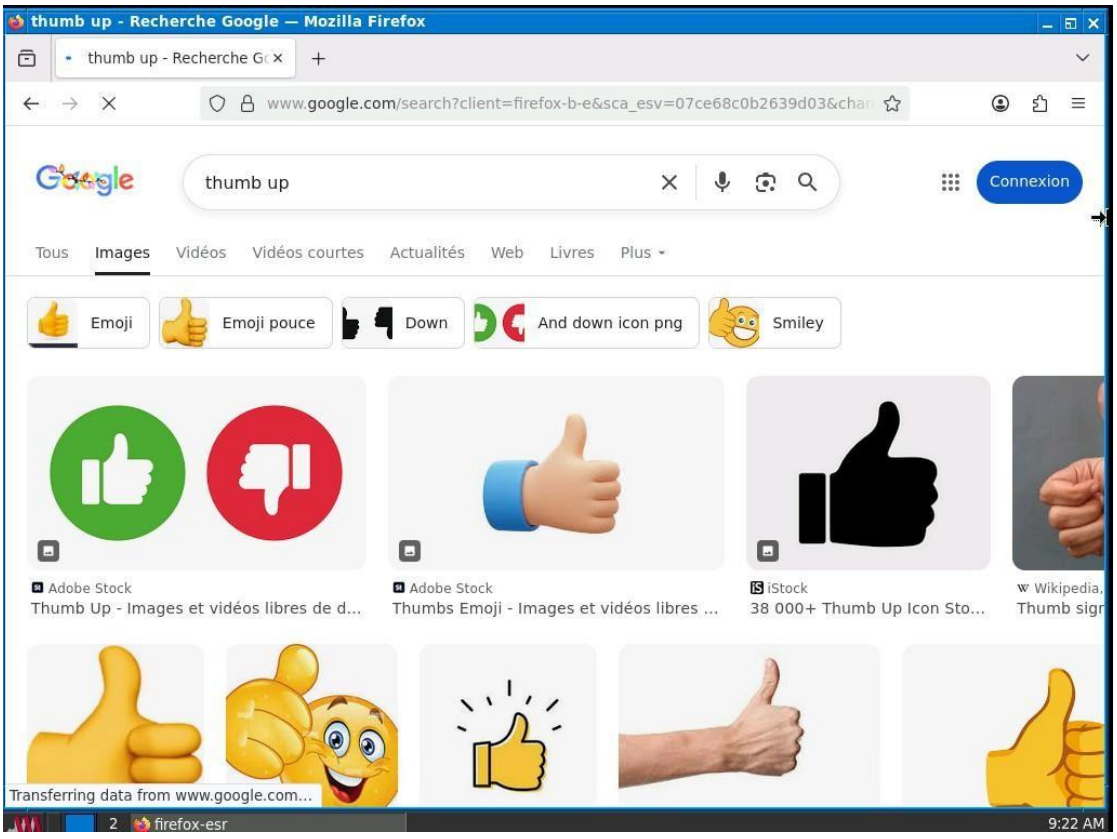
Sur la configuration de GNS 3

On a pu tester des classiques pings pour vérifier que le réseau passe bien

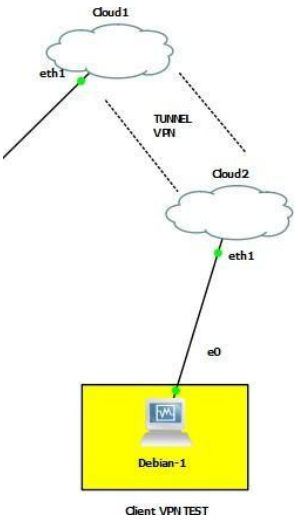
```
root@webterm-2:~# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=53 time=43.0 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=53 time=33.7 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=53 time=23.6 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=53 time=27.3 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=53 time=23.4 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=53 time=29.5 ms
64 bytes from 1.1.1.1: icmp_seq=7 ttl=53 time=48.2 ms
```

```
root@webterm-2:~# ping google.com
4PING google.com (142.250.200.238) 56(84) bytes of data.
64 bytes from mrs08s18-in-f14.1e100.net (142.250.200.238): icmp_seq=1 ttl=111 time=28.5 ms
64 bytes from mrs08s18-in-f14.1e100.net (142.250.200.238): icmp_seq=2 ttl=111 time=30.7 ms
64 bytes from mrs08s18-in-f14.1e100.net (142.250.200.238): icmp_seq=3 ttl=111 time=24.8 ms
64 bytes from mrs08s18-in-f14.1e100.net (142.250.200.238): icmp_seq=4 ttl=111 time=26.8 ms
64 bytes from mrs08s18-in-f14.1e100.net (142.250.200.238): icmp_seq=5 ttl=111 time=22.9 ms
64 bytes from mrs08s18-in-f14.1e100.net (142.250.200.238): icmp_seq=6 ttl=111 time=48.1 ms
64 bytes from mrs08s18-in-f14.1e100.net (142.250.200.238): icmp_seq=7 ttl=111 time=30.2 ms
64 bytes from mrs08s18-in-f14.1e100.net (142.250.200.238): icmp_seq=8 ttl=111 time=25.7 ms
64 bytes from mrs08s18-in-f14.1e100.net (142.250.200.238): icmp_seq=9 ttl=111 time=25.9 ms
64 bytes from mrs08s18-in-f14.1e100.net (142.250.200.238): icmp_seq=10 ttl=111 time=24.2 ms
64 bytes from mrs08s18-in-f14.1e100.net (142.250.200.238): icmp_seq=11 ttl=111 time=23.1 ms
```

Puis, pour essayer, tenter d'aller sur le net, étant donné que les machins sont en trunk vers le WAN, elles devrait pouvoir y accéder sans trop de difficultés :



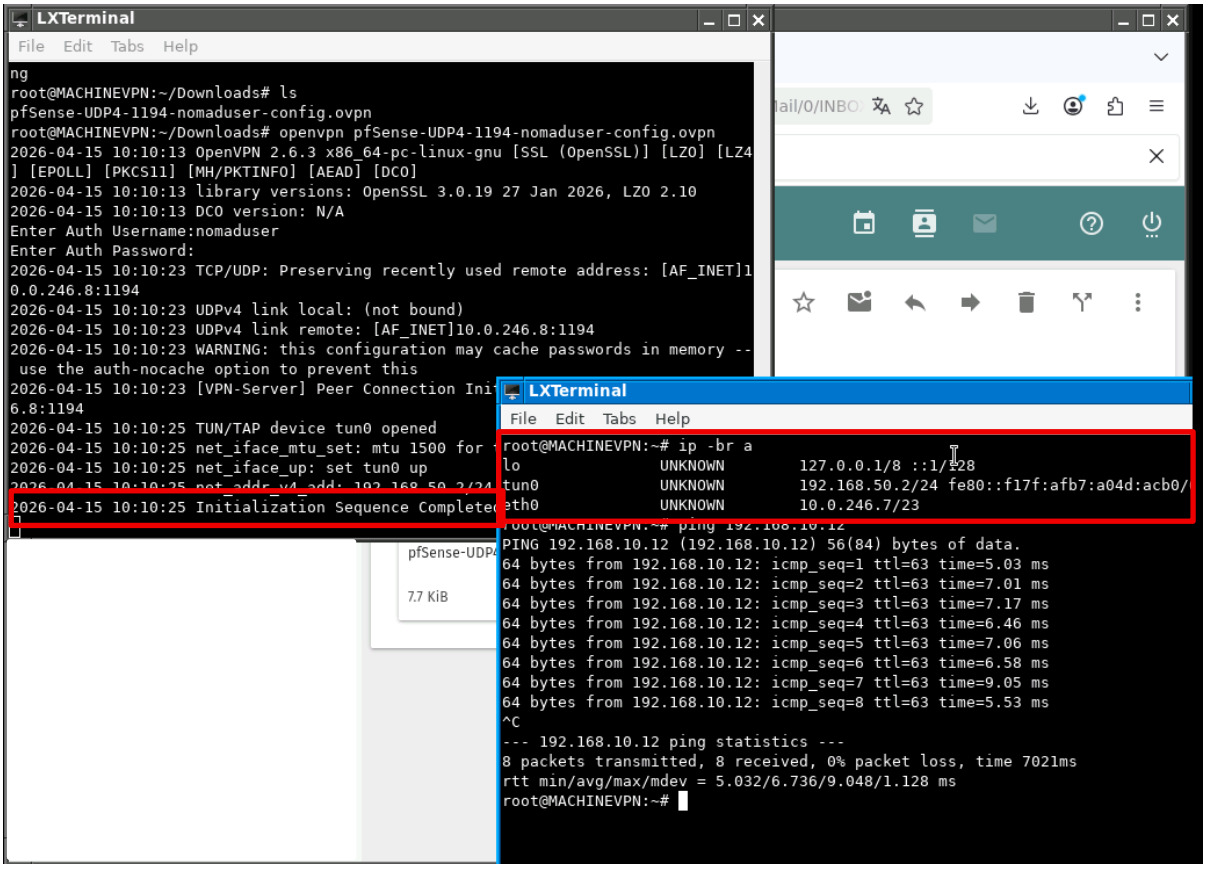
Enfin, sur le VPN



Dans cette zone de travail on se connecte à la Debian et plusieurs tests sont à faire :

- La debian a déjà les certificats entrés
- On peut se connecter en DHCP depuis la machine
- Tenter de ping les différentes VLAN (10,20,30)

L'important ici est de voir si la machine se connecte bien au réseau et peut communiquer avec le reste des machines du réseau (les différentes VLAN)

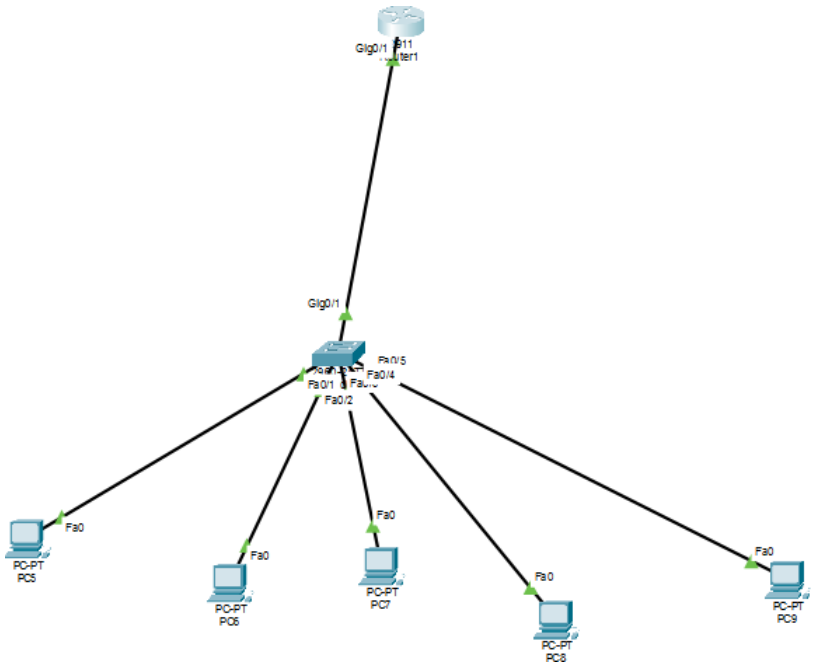


Pistes Explorées

La création de ce projet a nécessité plusieurs phases, à cause de divers bugs, j'ai du changer de manière de composer pour pouvoir mener au plus loin le projet :

- Configuration TEST sur ciscopkt (donner un aperçu de la charge de travail)
- Utilisation de l'architecture proposée par le projet (le Proxmox etc.)
- En voyant la latence et l'impossibilité de créer des VLAN on passe sur un switch virtuel et branché sur des VM
- Comme la configuration ne fonctionnait pas bien, (le pool DHCP restait bloqué et répondait pas) faire une configuration secours sur GNS3

Configuration par Cisco PKT :



En partant de cette première configuration, un routeur, un switch et des pc clients,

Il fallait configurer 2 choses importantes

- VLAN
- DHCP

En se posant sur le switch, on entre en mode de configuration, (enable puis configure terminal)

On commence par configurer les interfaces après avoir créé les VLAN :

```
Switch(config)#int fa0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if)#exit
Switch(config)#
Switch(config)#
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#int gi0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30
Switch(config-if)#exit
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

Les commandes ici veulent dire :

Int x	Choix de l'interface que l'on configure, ici la fa0/5 (tout à droite sur le graphique)
Switchport mode access	Ce port est configuré comme un port d'accès. Cela signifie qu'il est destiné à connecter un seul appareil final
Switchport access vlan x	Spécifie que l'appareil connecté à ce port d'accès fera partie du VLAN numéro X
Switchport mode trunk	Ce port est configuré comme un port trunk. Il est destiné à interconnecter des équipements réseau qui doivent transporter le trafic de plusieurs VLANs
Switchport trunk allowed vlan x,y,z	Seuls les VLANs dont les numéros sont listés (X, Y, Z...) auront le droit de passer par ce lien trunk

Une fois tout cela configuré on peut afficher les VLAN et TRUNK pour vérifier si on a bien tout paramétré :

Do show vlan

```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/2
10   VLAN10                           active    Fa0/1
20   VLAN20                           active    Fa0/2, Fa0/3
30   VLAN30                           active    Fa0/4, Fa0/5
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
 --More--
```

Ici, on voit apparaitre les 3 vlan créés et les ports qui leur sont attribués par exemple, le Vlan 30 est sur les ports Fa0/4 et Fa0/5

Do show interface trunk

```
Switch#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      10,20,30

Port        Vlans allowed and active in management domain
Gig0/1      10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      10,20,30

Switch#
```

Ici, on voit que sur le port vers le routeur, le trunk laisse passer les vlan 10,20 et 30

Ensuite, sur le routeur, on fait POUR CHAQUE PORTS une configuration DHCP très simple :

```
[OK]
Router(config)#ip dhcp pool VLAN10
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool VLAN20
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool VLAN30
Router(dhcp-config)#network 192.168.30.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.30.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#
Router(config)#
Router(config)#do wr
Building configuration...
[OK]
```

Les commandes ici veulent dire :

Ip dhcp pool intx	Sur l'interface choisie, on crée le pool dhcp (c'est-à-dire la requête qui va plus tard adresser)
network	On donne le réseau que l'on souhaite donner sur le port et son masque de sous réseau
Default-router	Ici on définit l'adresse IP de la Passerelle, c'est le point de connexion direct sur le routeur, c'est d'ici que part le réseau configuré
Dns-server	On ajoute un server DNS pour le réseau ici par exemple, le DNS de google 8.8.8.8

Puis connecté sur une machine on teste de faire une requête DHCP :

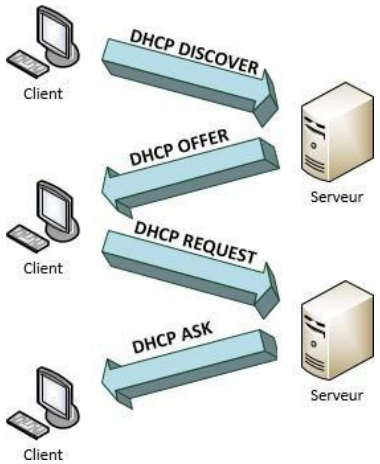
Pour rappel une requête DHCP se fait en 4 étapes : D O R A :

DISCOVER

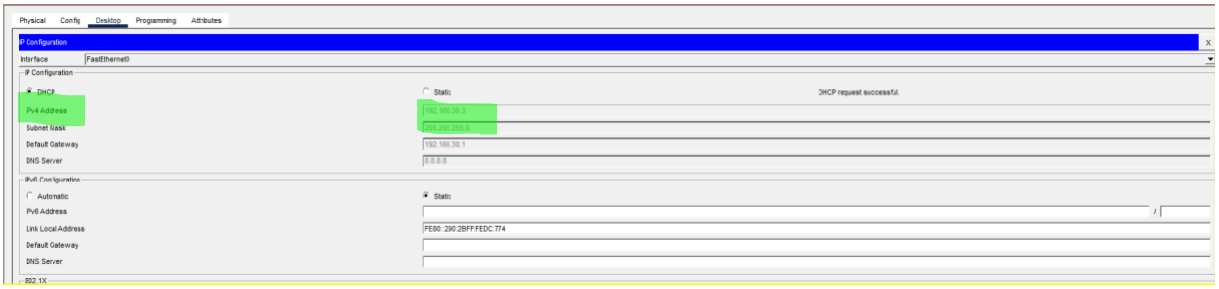
OFFER

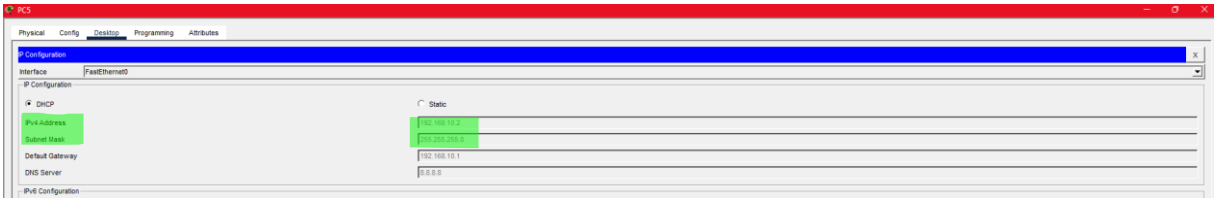
REQUEST

ACKNOLEDGE



Ensuite on lance une requête sur les PC pour voir si cela s'adresse bien :



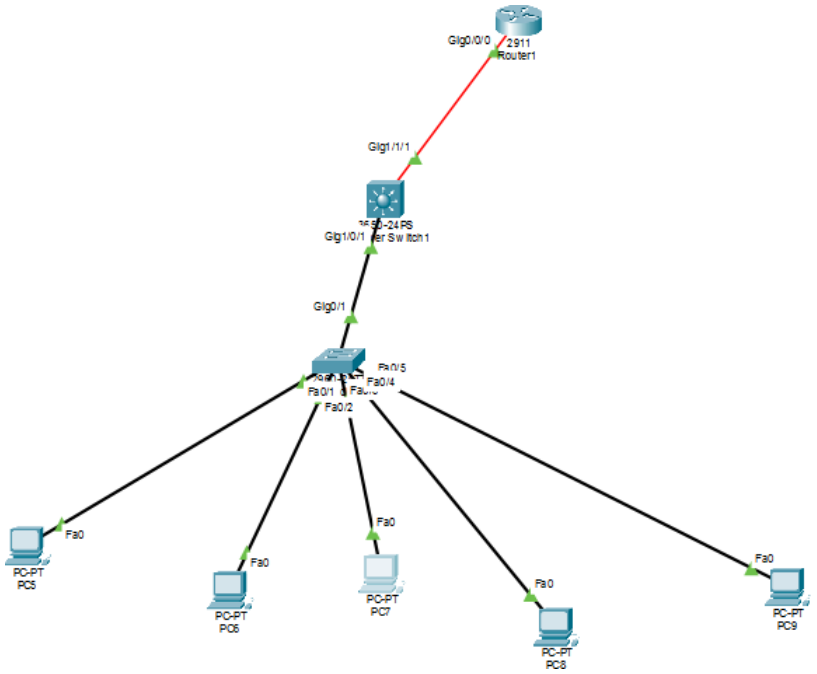


Et on voit bien que les machines récupèrent bien leur IP

Les tests seront disponibles dans leur partie attitrée

Configuration plus complexe par Cisco PKT :

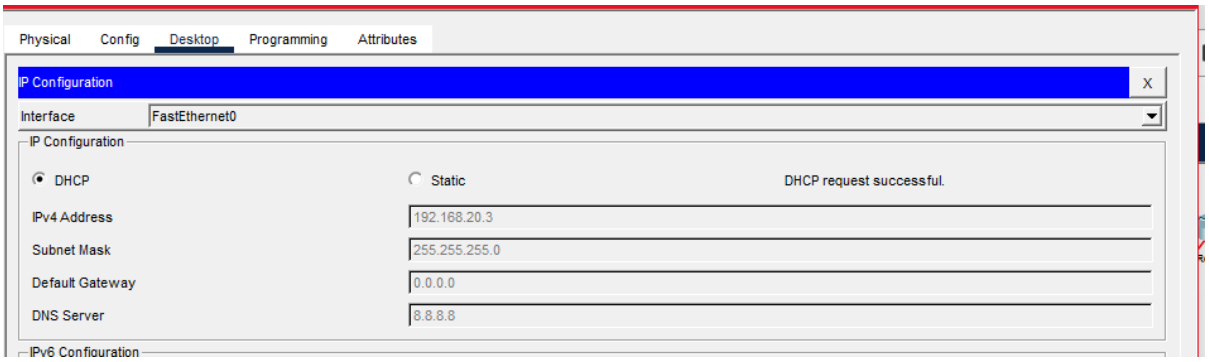
Après avoir fini la première configuration, mon intervenant me demande, « pourquoi ne pas complexifier un peu la chose ? » Donc pour essayer, on ajoute un switch de niveau 3 à l'architecture précédente



Plusieurs étapes pour inclure le switch de niveau 3 à l'infrastructure :

- Re créer toutes les VLANs
- Définir à nouveau le TRUNK
- Attribuer les interfaces
- Supprimer le pool DHCP du routeur et le refaire sur le switch de niveau 3

L'objectif au final est qu'au moins une des machines client ai son adresse IP :

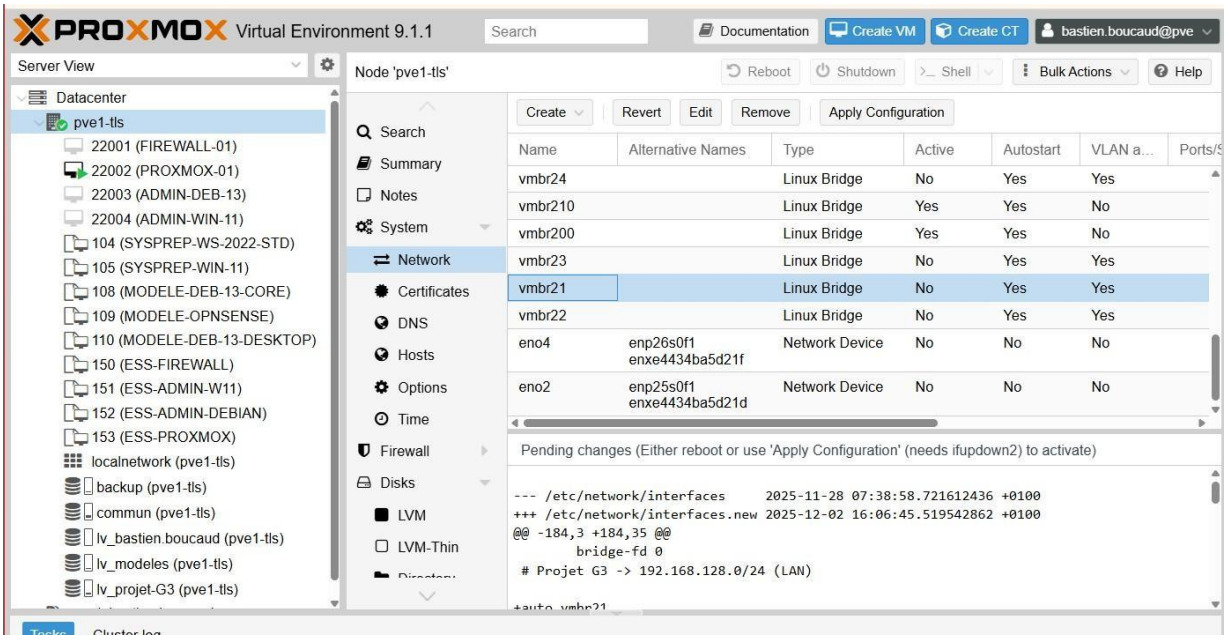


Ici le DHCP passe, la configuration avec le nouveau switch est donc valide.

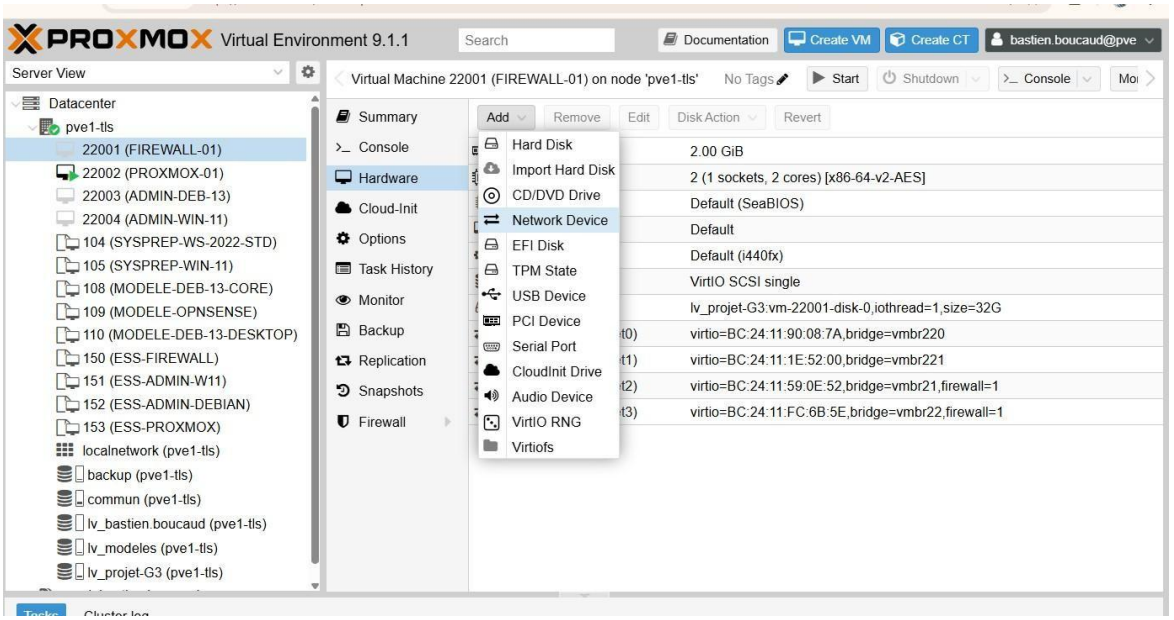
Premiers tests sur le Proxmox :

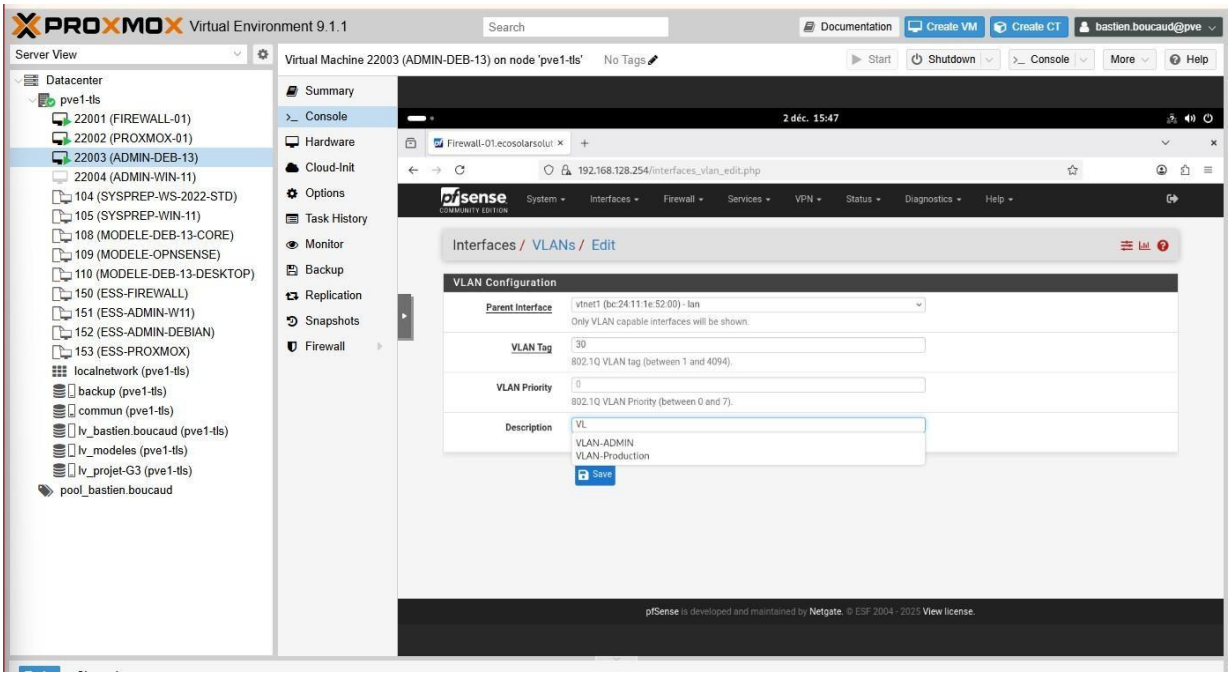
Le début de configurations sur Proxmox a été très courte, en effet, très rapidement, j'ai rencontré des bugs, une impossibilité de faire quoi que ce soit et surtout une latence énorme sur le réseau rendant toutes tentatives d'ajouts techniques vraiment lentes.

Mais des tests ont quand même été faits, pour découvrir et pratiquer l'outils



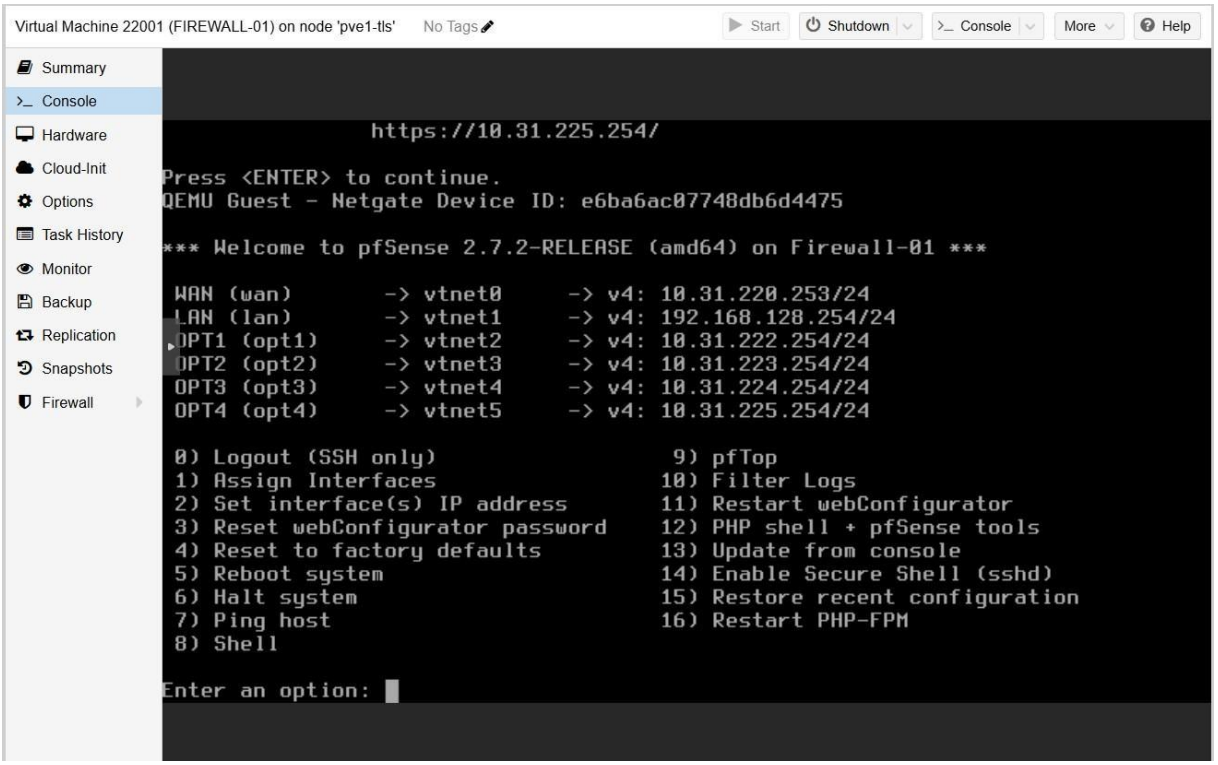
On crée d'abord les Vmbr qui seront utilisés, ça aurait été sur ces bridges que les VLAN auraient dû passer. Puis on ajoute les devices (c'est-à-dire les futures VLAN)





En se connectant sur une machine au Pfsense on ajoutes aux interfaces les VLAN

Puis on vérifie si tout est passé

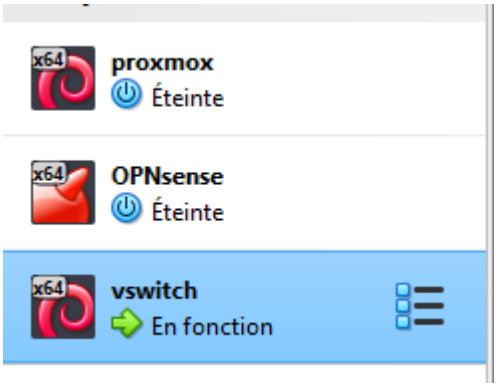


Sur ce support nous avons arrêté les configurations ici et n'avons pas expérimentés plus au vu des difficultés pour avancer dues au réseau

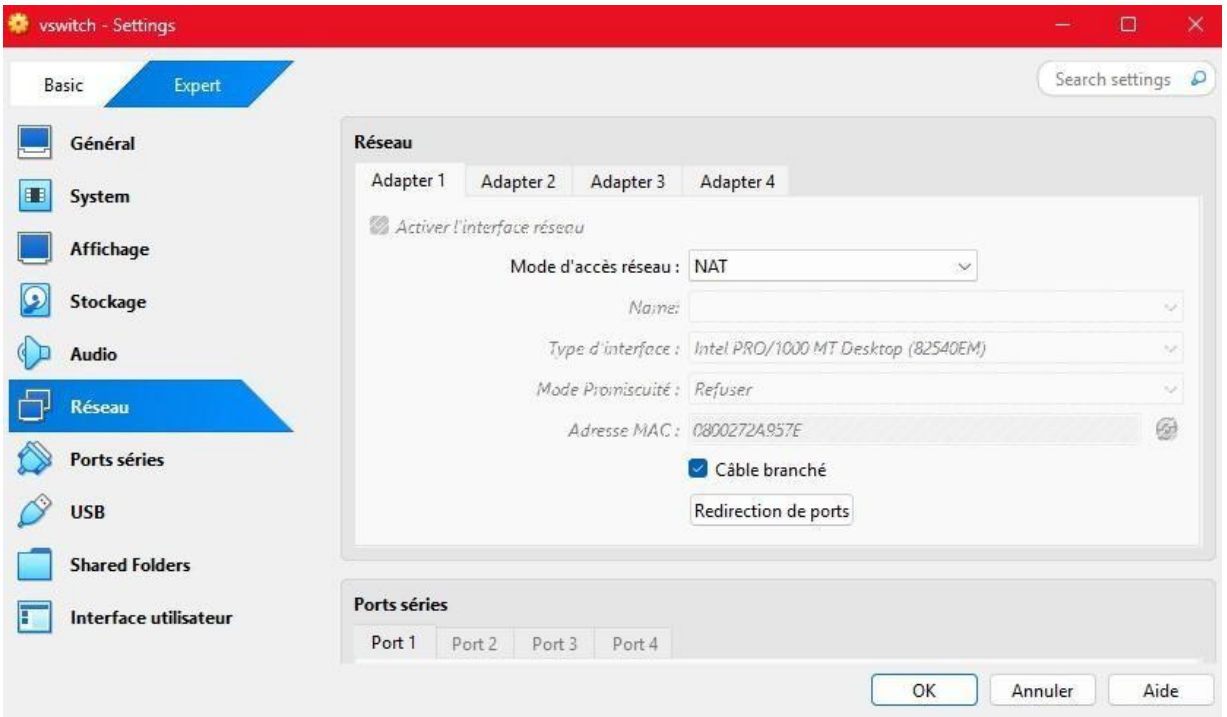
Configuration VM et OVS (switch virtuel) :

Pour cette version de la configuration, bien qu'on ai plus avancé, elle n'a pas permis de mener au terme le projet, pour cela nous verrons la 3e et dernière configuration.

Ici, 3 machines virtuelles qui vont communiquer entre elles

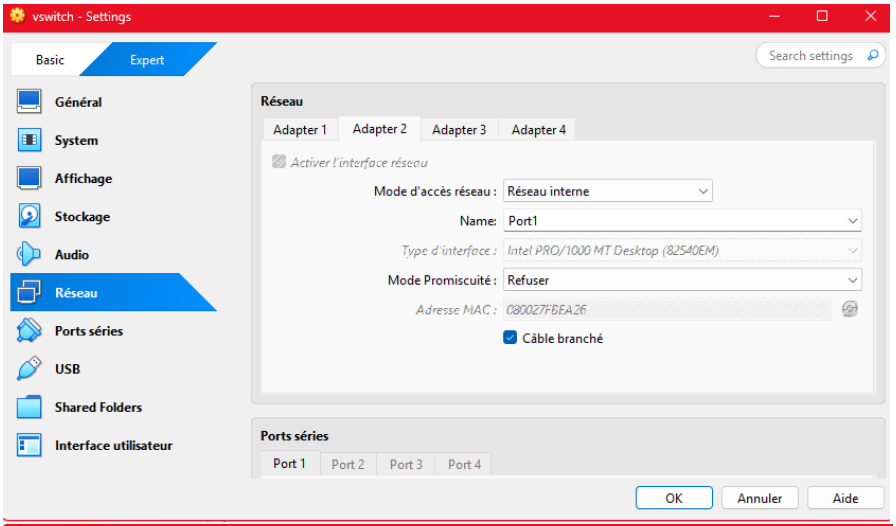


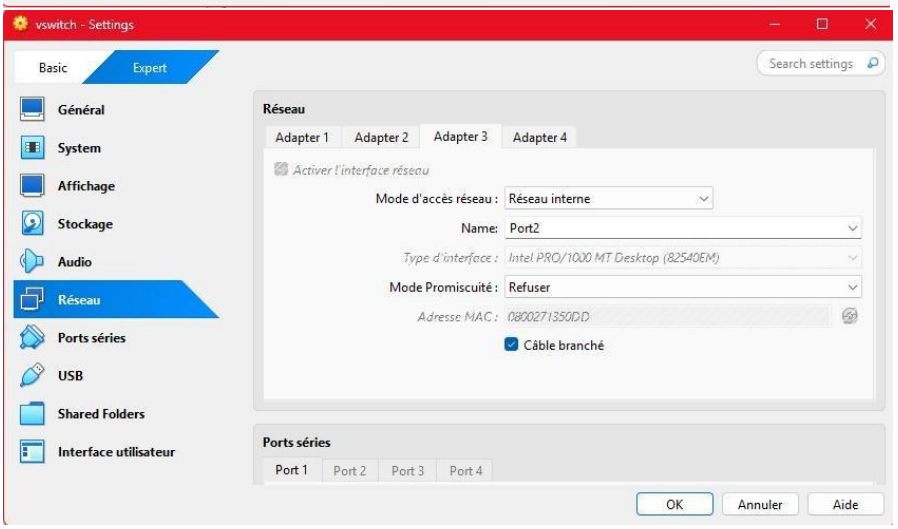
En premier lieu et avant même de lancer les machines, on configure les port réseaux du vswitch :

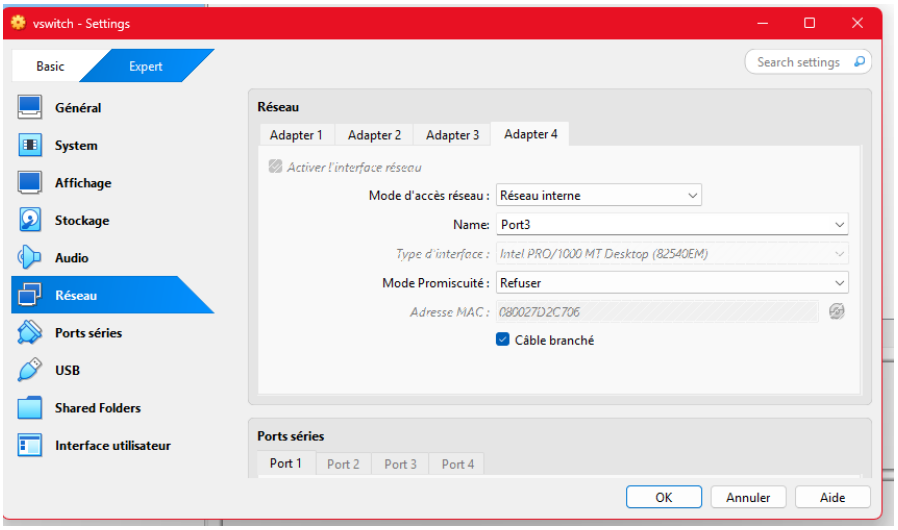


Sur le premier port, on laisse un réseau NAT, c'est ce port qui permet à la machine de continuer à capter du réseau et pouvoir faire des installations

Pour les autres ports, on les configure en réseau interne







Dans l'idée il faut que 1 port donne une VLAN ainsi sur les machines client on aura en tant que ports, un des réseaux internes de l'OVS

La machine switch n'est pas une ISO qui configure directement,

Il s'agit d'une machine Debian12 sur laquelle on a ajouté un paquet ovs pour ajouter une fonction de switch virtuel

On vérifie donc une fois le paquet installé la version et les informations concernant le logiciel :

```
bastien@vbox:~$ sudo ovs-vsctl show
9f6d8200-a345-4c63-b71c-3615076c51f3
    ovs_version: "3.1.0"
bastien@vbox:~$
```

```
bastien@vbox:~$ sudo systemctl status openvswitch-switch
● openvswitch-switch.service - Open vSwitch
     Loaded: loaded (/lib/systemd/system/openvswitch-switch.service; enabled; p>
     Active: active (exited) since Wed 2025-12-03 14:18:36 CET; 1min 6s ago
    Process: 3468 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 3468 (code=exited, status=0/SUCCESS)
        CPU: 1ms

Dec 03 14:18:36 vbox systemd[1]: Starting openvswitch-switch.service - Open vSw>
Dec 03 14:18:36 vbox systemd[1]: Finished openvswitch-switch.service - Open vSw>
lines 1-9/9 (END)
```

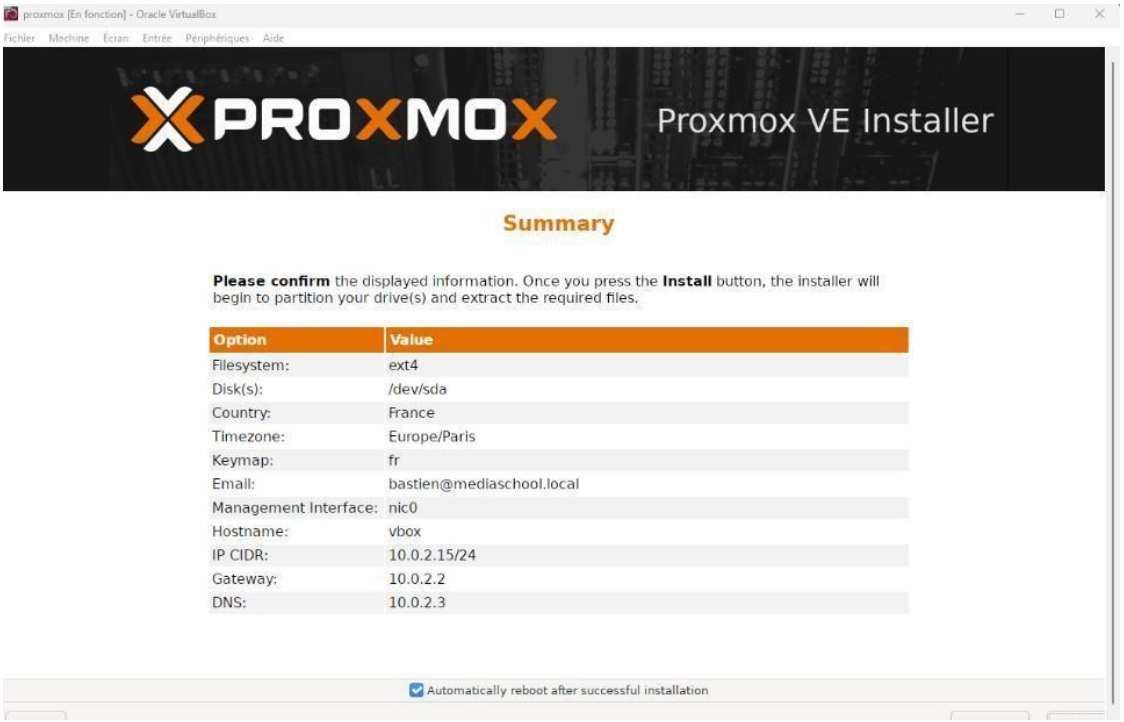
On crée le bridge principal qui accueillera les différents ports :

```
bastien@vbox:~$ sudo ovs-vsctl add-br ovs-br0
bastien@vbox:~$
```

Et on ajoute les interfaces au bridge :

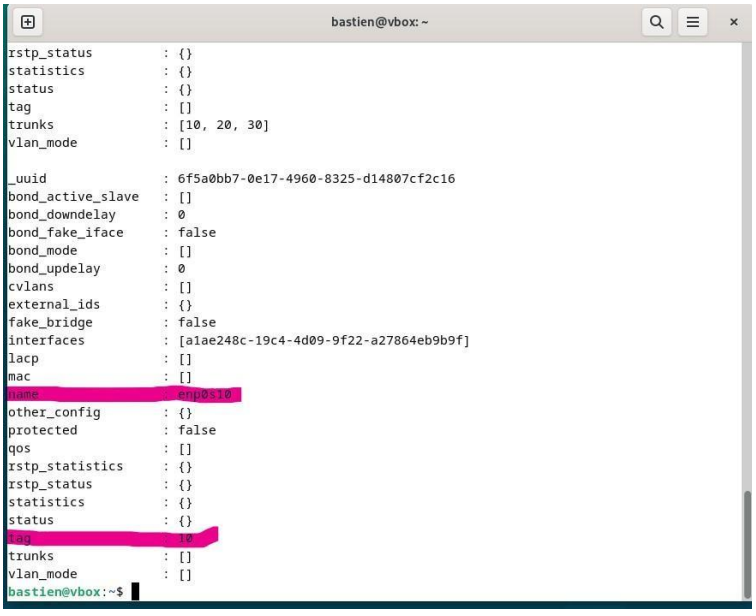
```
bastien@vbox:~$ sudo ovs-vsctl add-port ovs-br0 enp0s8
bastien@vbox:~$ sudo ovs-vsctl add-port ovs-br0 enp0s9
bastien@vbox:~$ sudo ovs-vsctl add-port ovs-br0 enp0s10
bastien@vbox:~$
```

Ensuite on installe la machine Proxmox :



Avec des configuration identiques à celles que l'on peut faire sur Cisco on obtient une configuration trunk et VLAN Parfaite

```
_uuid               : 65ba6823-e82e-4a42-80b7-7c8fc21e0db9
bond_active_slave   : []
bond_downdelay      : 0
bond_fake_iface     : false
bond_mode           : []
bond_updelay        : 0
cvlans              : []
external_ids        : {}
fake_bridge         : false
interfaces          : [aa8d86be-c50c-42d3-8cc8-c2ccbfa6dd81]
lacp                : []
mac                 : []
name                : enp0s9
other_config        : {}
protected           : false
qos                 : []
rstp_statistics     : {}
rstp_status         : {}
statistics          : {}
status              : {}
tag                 : []
trunks              : [10, 20, 30]
vlan_mode           : []
```



Commandes suivies :

Configuration VLANs

Scénario configuré :

- eth1 : trunk (10,20,30)
- eth2 : trunk (10,20,30)
- eth3 : access VLAN 10

Passer les ports en trunk

sudo ovs-vsctl set port eth1 trunks=10,20,30

sudo ovs-vsctl set port eth2 trunks=10,20,30

Passer le port en access

sudo ovs-vsctl set port eth3 tag=10

Redémarrer le service réseau :

sudo systemctl restart networking

RESULTAT :

```
bastien@vbox:~$ sudo ovs-vsctl show
*9f6d8200-a345-4c63-b71c-3615076c51f3
    Bridge ovs-br0
        Port ovs-br0
            Interface ovs-br0
                type: internal
        Port enp0s8
            trunks: [10, 20, 30]
            Interface enp0s8
        Port enp0s9
            trunks: [10, 20, 30]
            Interface enp0s9
        Port enp0s10
            tag: 10
            Interface enp0s10
    ovs_version: "3.1.0"
bastien@vbox:~$
```

Mais arrivé à ce point on rencontre un problème,

Malgré la configuration du pare-feu en ANY ANY, la requête DHCP ne passe pas

(celle-ci reste bloquée à la phase OFFER)

Plusieurs idées en tête de ce qui pourrait bloquer,

- les règles du pare-feu qui malgré tout bloquent quelque part
- les interfaces TRUNK ou les TAG de VLAN Mal configurés
- le VLAN placé sur le mauvais port
  ➔ le VLAN sur le WAN plutôt que le LAN (cas observé sur prochain tests)
- La configuration du OVS n'est pas passée sur le OPNSense

COMPETENCES :

Acquises par le projet :

- **OVS et notions de switch virtuel :**

Alors que jusqu'ici le seul lien que je pouvais avoir avec les switchs était sur Cisco packet tracer, pour ce projet j'ai non seulement découvert et appris à utiliser les switchs de niveau 3 mais j'ai aussi découvert la possibilité de faire des switchs virtuels internes à une machine, cette connaissances m'a accompagné sur toute une tentative pour répondre aux demandes du projet

- **Configuration de VPN :**

Encore jamais expérimenté, bien que je sache comment fonctionne un VPN et à quoi celui-ci peut nous servir, ce projet m'a permis de découvrir comment le paramétrer, Au final je me rend compte de la complexité de ce sujet

- **Utilisation de GNS3 :**

De la même manière que le switch, j'ai plus souvent eu l'occasion d'utiliser Cisco, donc ce projet m'a permis de découvrir et d'utiliser de manière assez poussée GNS3 qui peut être plus performant à partir du moment où l'on peut inclure nos propres machines virtuelles.

- **Configuration de Pare-feu :**

Découverte sur le projet, bien que travaillé un peu auparavant, j'ai eu l'occasion de manipuler plusieurs outils (pfSense, OPNSense). J'ai ainsi pu me rendre compte du panel d'options que l'on peut configurer sur un pare-feu, allant des règles jusqu'au VPN.

Connues et utilisées :

- **Virtualisation**

Une compétence essentielle dans notre domaine, l'utilisation de Machines virtuelles pour faire des test ou simplement simuler un LAB, Dans notre situation nous avons eu l'occasion de se servir beaucoup de debian qui ont accueillis par exemple le switch virtuel.

- **Pare-feu**

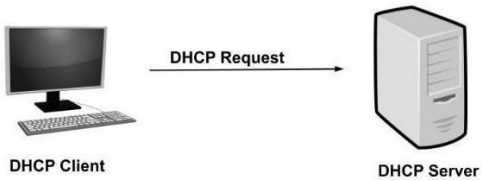
Bien que sur le projet nous avons eu l'occasion de pousser plus loin nos connaissances sur le domaine, nous avion déjà pu explorer les quelques fonctionnalités du pare-feu. Savoir en avance comment fonctionne un outil aussi complexe a permis une avancée plus efficace du projet.

- **Commandes configuration VLAN**

```
10   VLAN10                           active    Fa0/1
20   VLAN20                           active    Fa0/2, Fa0/3
30   VLAN30                           active    Fa0/4, Fa0/5
```

Etant donné que en classe nous avons déjà configuré maintes et maintes fois des VLAN, savoir les différentes commandes (du type : encapsulation, vlan x ….)
Pour le projet cela a permis d'aller beaucoup plus vite et être certains de la validité de nos commandes

- **Configuration DHCP**



Pareil que pour les commandes VLAN, savoir les commandes a permis d'avancer BEAUCOUP plus vite.

- **Notion d'architecture** 

Ici, pour réaliser les infrastructures que ce soit sur Cisco ou Drawio, savoir qui connecter à qui était assez utile, j'ai pu rapidement réaliser des schémas d'architectures du projet

CONCLUSION :

Ce projet de sécurisation réseau et segmentation VLAN pour EcoSolar Solutions a constitué une expérience technique importante dans l'avancée de ma formation. Il m'a permis de concrétiser des apprentissages théoriques vu en classes en appliquant sur une solution tout ce qu'on pouvait faire.

L'objectif initial était de moderniser et sécuriser le réseau par une segmentation en VLANs, modifier les règles du pare–feu et enfin créer un accès distant par VPN. Bien que le parcours ait été semé d'obstacles techniques significatifs (infrastructure incompatible, lenteurs, perte de contenus). Ces difficultés, loin d'être des échecs, ont été de véritables opportunités d'apprentissage. Elles m'ont enseigné la résilience, la capacité à pivoter vers des solutions alternatives (comme OVS ou GNS3) et l'importance d'avoir une documentation rigoureuse pour conserver, sur chaque étapes, le plus d'informations possibles , même lorsqu'elle ne menait pas au résultat attendu.

Si la maquette finale sur GNS3 a validé les principes de base de la segmentation et du routage inter-VLAN, elle a aussi mis en lumière les limites d'un environnement instable.

Au-delà de l'aspect technique, ce projet m'a conforté dans l'importance cruciale d'une infrastructure réseau robuste et pensée pour la sécurité.

Pour une entreprise comme EcoSolar Solutions, dont l'innovation et les données sensibles sont le cœur de métier, une telle refonte semble obligatoire et agréable pour l'évolution exponentielle du domaine exploré.

Enfin, ce travail réalisé en synergie avec les autres scénarios du groupe a renforcé ma compréhension de l'interdépendance des composants d'un SI : la sécurité réseau n'est qu'une pierre d'un édifice comprenant une supervision, une sauvegarde et la haute disponibilité.


MediaSchool


iris


EcoSolar
SOLUTIONS