

Restructuration réseau – Salle 101



Contexte :

En tant que Technicien Supérieur Système et réseau, et grâce aux compétences récemment acquises, vous allez réfléchir de manière logique à l'installation la plus optimale du réseau de votre salle, sans pour autant négliger l'aspect sécurité.

✂ Planification et conception :

- *Commencez par cartographier la salle et identifier les emplacements des prises électriques, des fenêtres et des portes.*
- *Déterminez où vous souhaitez exploiter/installer les points d'accès Wi-Fi, les commutateurs et les prises réseau.*

✂ Installation du câblage ?**✂ Installation des points d'accès Wi-Fi ?****✂ Installation des commutateurs réseau ?****✂ Configuration du réseau ?**

✂ Configurez les adresses IP statiques ou utilisez DHCP pour attribuer automatiquement des adresses IP aux appareils.

✂ Configurez les règles de pare-feu pour protéger le réseau.

✂ Testez la connectivité entre les appareils.

✂ Documentation :

- *Créez un schéma physique et logique.*
- *Documentez les adresses IP, les noms d'hôte et les mots de passe.*

✂ Formation :

- *Formez les utilisateurs sur l'utilisation du réseau, les mots de passe et les bonnes pratiques de sécurité.*

Sommaire

BRIEF – La salle 101.....	1
1. L'idée : quoi ? Et comment ?	4
2. Fonctionnement détaillé – procédure de réalisation	5
3. Schéma du réseau et plan de salle	8
4. Evolutivité	9

1. L'idée : quoi ? Et comment ?

Projet de restructuration réseau de la salle 101.

Notre objectif en tant que TSSR, proposer une architecture la plus simple possible en terme d'administration tout en offrant un niveau de sécurité acceptable et offrant également une possibilité dévolution facilité.

Pour se faire nous avons opté pour une segmentation de réseau par Vlan, en effet, cela permet d'avoir des espaces de travail indépendants ou la sécurité est accrue lors de test ou TP car les flux de réseau seront isolé.

Nous avons besoin pour mettre en œuvre cette architecture des éléments suivants :

- _4 switches (dont 1 N3) en fonction de la configuration (2 choix proposé)
- _1 prises Ethernet brassée
- _1 borne wifi
- _1 serveur (Proxmox, pare-feu, etc...)

Les prises électrique sont au nombre suffisant pour ce projet et une éventuelle évolution.

Description de l'architecture :

Le réseau logique est composé de 4 Vlan, chaque Ilot fait partie d'un Vlan afin d'isoler les travaux de groupe, test etc... (Ethernet, switch N2)

Le 4^{ème} Vlan est le réseau Wifi accessible à toute la promo, formateur, Guest...

L'imprimante et NAS sont accessible sur le Vlan « Wifi » (Borne wifi sur switch N2)

Chacun des switch N2 est relié au Switch N3 qui lui sert de relais DHCP (voir schéma 1)

Le serveur tourne sous Proxmox, dans lequel sont installées des VM dont PFsense qui fait office de serveur DHCP, Pare-feu, gestion Vlan, un VPN (conteneur Wireguard, ou OpenVPN par exemple), etc...

Le VPN servirait de connexion sécurisé lors de travaux en distanciel.

Également sur Proxmox : est mis en place un serveur d'impression et un NAS (ISO, utilitaire, documentation...).

Pour une visibilité sur le réseau des utilisateurs : chaque PC devra être renommé pour correspondre une nomenclature spécifique « prenom.1ere lettre du nom ».

Par exemple : « allie.m »

2. Fonctionnement détaillé – procédure de réalisation

Notre serveur aurait comme hyperviseur Proxmox,

Nous avons choisi d'y installer notre pare-feu PfSense qui fera office non seulement de pare-feu mais également de serveur DHCP, surveillance du réseau dans une éventuelle évolution.

Notre choix s'est porté vers cette solution qui offre une grande marge de manœuvre en terme d'évolution, de sécurité.

De plus, le pare-feu PfSense permet d'attribuer si besoin des règles différentes sur chaque Vlan configuré dans son système, pratique pour des travaux de groupes où nous aurions besoin de règles plus ou moins permissive selon les TP envisagé.

Dans un premier temps, il s'agit de paramétrer les VLAN souhaitées dans PfSense :

Réseau 1

Masque réseau: **255.255.255.224**

Adresse réseau: **172.16.0.0**

Adresse du premier hôte: **172.16.0.1**

Adresse du dernier hôte: **172.16.0.30**

Adresse de diffusion: **172.16.0.31**

Nombre maximal d'hôtes: **30**

Réseau 2

Masque réseau: **255.255.255.224**

Adresse réseau: **172.16.0.32**

Adresse du premier hôte: **172.16.0.33**

Adresse du dernier hôte: **172.16.0.62**

Adresse de diffusion: **172.16.0.63**

Nombre maximal d'hôtes: **30**

Réseau 3

Masque réseau: **255.255.255.224**

Adresse réseau: **172.16.0.64**

Adresse du premier hôte: **172.16.0.65**

Adresse du dernier hôte: **172.16.0.94**

Adresse de diffusion: **172.16.0.95**

Nombre maximal d'hôtes: **30**

Réseau 4

Masque réseau: **255.255.255.224**

Adresse réseau: **172.16.0.96**










Adresse du premier hôte: **172.16.0.97**

Adresse du dernier hôte: **172.16.0.126**






Adresse de diffusion: **172.16.0.127**

Nombre maximal d'hôtes: **30**

On crée d'abord les VLAN sur Pfsense, dans *Interfaces > Assignement > VLAN*

VLAN Interfaces				
Interface	VLAN tag	Priority	Description	Actions
em1 (lan)	10		Groupe 1	 
em1 (lan)	20		Groupe 2	 
em1 (lan)	30		Groupe 3	 
em1 (lan)	40		Formateur /serveur	 
				 Add

Ensuite on crée nos interfaces logiques en se rendant dans *Interface > Assignments* :

LAN	em1 (00:0c:29:b7:4e:bf)	 Delete
OPT1	VLAN 10 on em1 - lan (Groupe 1)	 Delete
OPT2	VLAN 20 on em1 - lan (Groupe 2)	 Delete
OPT3	VLAN 30 on em1 - lan (Groupe 3)	 Delete
Available network ports:	VLAN 40 on em1 - lan (Formateur /serveur)	 Add

Sur CHAQUE interface ainsi créée, on clique sur son nom pour la paramétrer : on l'active et on lui fixe une IP :

Enable ☒ Enable interface

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

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
The MAC address of a VLAN interface must be set on its parent interface


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

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

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

Static IPv4 Configuration

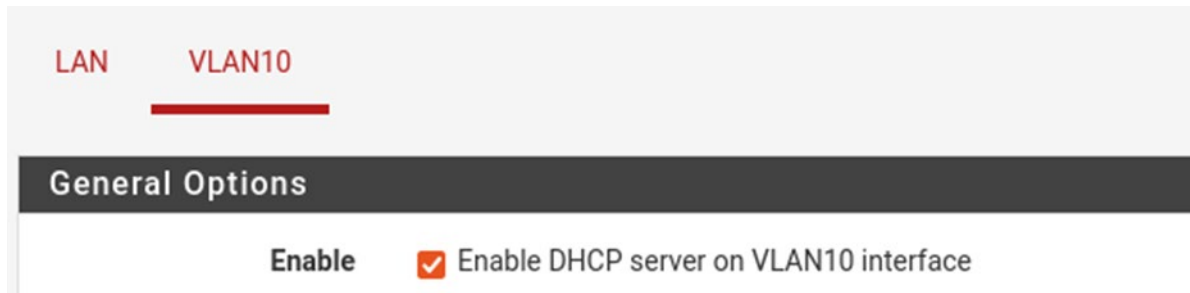
IPv4 Address /

IPv4 Upstream gateway  Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

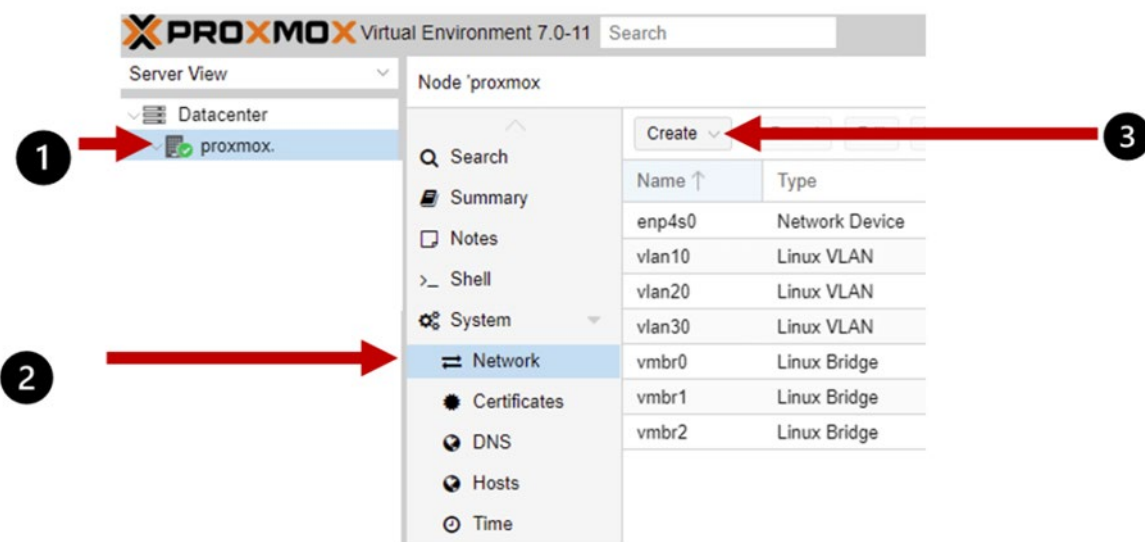
Maintenant il nous reste à configurer le DHCP sur chaque interface logique.

Pour se faire, on va se rendre sur *Service > DHCP server > VLAN 10* et configurer notre DHCP :



Une fois la configuration effectuée, on peut définir les règles de pare-feu en se rendant sur *Firewall > Rules* et notre vlan.

Dernière étape importante : il faut aussi créer les VLAN sur le serveur Proxmox :



Outil ou plug-in pour PfSense .

Pour une sécurité encore accrue, il serait également possible d'ajouter un « outil » à Pfsense :

CROWDSEC

C'est une solution gratuite et open source capable de détecter et bloquer des attaques grâce à de nombreux scénarios de détection.

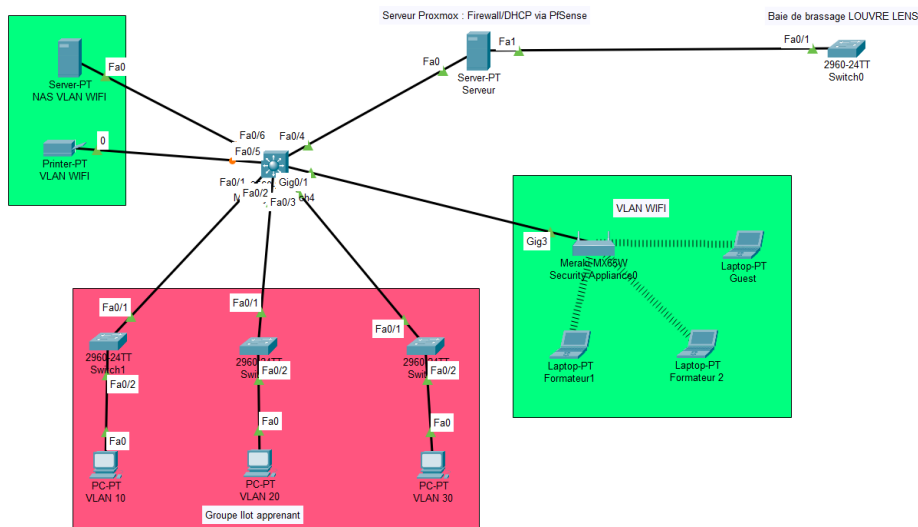
Il fonctionne de la manière suivant : Une fois mis en place, il va analyser les journaux du système pour identifier les comportement malveillants et bloquer les adresse IP associées. EN complément, les adresses IP Présentes dans les listes communautaire de CROWDSEC sont également Bloquées.

Ainsi, si une personne souhaite ne serais ce que faire un scan réseau sur notre infra, CROWDSEC saura le détecter et bloquera l'IP qui sera à l'initiative de ce comportement.

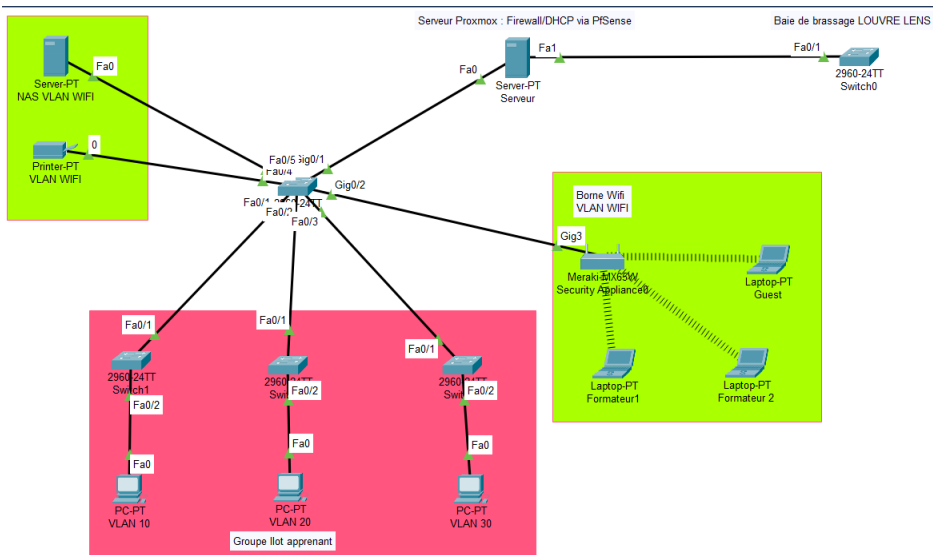
3. Schéma du réseau et plan de salle

Schéma réseau : (2 possibilités)

Schema 1 avec Switch N3



Schema 2 avec switch N2



Configuration des switch L2

Assignation des port 1 à 12 au vlan (ilot 1 vlan 10 de 1 à 12, ilot 2 vlan 20 de 1 à 12, ilot 3 vlan 30 de 1 à 12)

L'interface 24 de chaque switch est en mode « trunk » c'est celui-ci qui sera connecté au switch L3

L'interface 23 de chaque switch assigné au vlan 40 (réseau global, wifi)

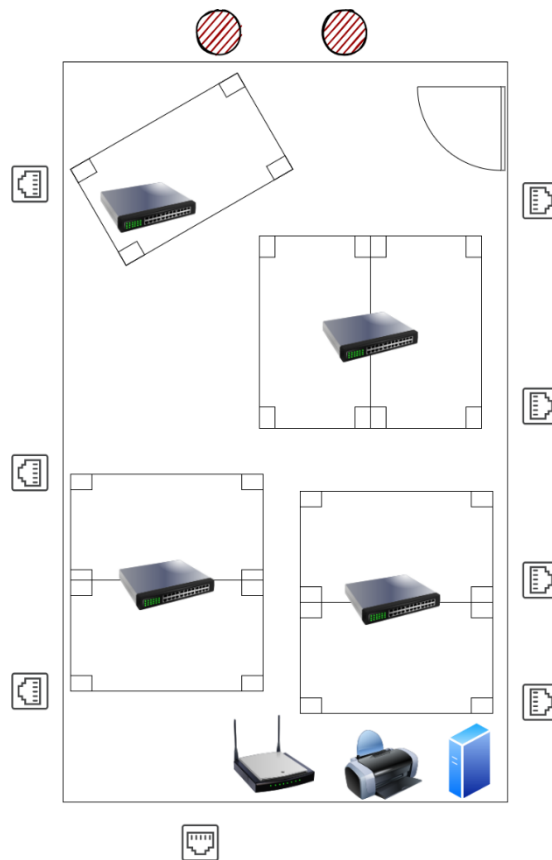
Configuration du switch L3

L'interface Gig1/0/1 est en mode trunk dot1q vers le serveur Proxmox/Pfsense)

L'interface Gig1/0/2, Gig1/0/3, Gig1/0/4 sont en mode trunk, connecté au Switch L2

L'interface Gig1/0/5 est assigné au Vlan 40 (réseau global/Wifi)

Plan de salle :



4. Evolutivité

Notre proposition d'architecture nous permet de faire évoluer notre infra sans trop de difficultés. En effet, les éléments les plus importants étant virtualisés, l'évolution pourrait se faire sans difficulté en ajoutant des couches de sécurité.

Exemple d'évolution possible et relativement simple à mettre en place :

Evolution au niveau Software

Installation d'un Windows Server avec mise en place d'un Active Directory, un domaine, une stratégie de groupes (privilèges configurés au niveau des groupes).

Des mots de passe robustes obligatoires renouvelables à 90 jours.

Désactivation du service *Print spooler*, restriction de l'accès au contrôleur de domaine...

Planification de la récupération de l'AD (plan de restauration).

Evolution au niveau Hardware (Serveur) :

Pour assurer une disponibilité et une sécurité maximale du serveur, l'idéal serait d'ajouter 2 serveurs

supplémentaire identique afin de créer un cluster.

En cas de panne d'un des serveurs le relais sera automatique et rapide.