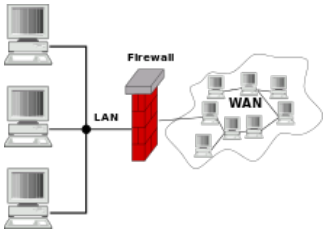
Mise en place d'une infrastructure Réseau virtuelle

Installation et configuration du service



Dans le contexte nous allons créer une passerelle, en informatique une passerelle qui se traduit Gateway en anglais, ce permet de relier deux réseaux informatiques, comme exemple une réseau local (LAN) et internet (WAN).

Dans notre phase de test, nous utiliserons un PVE Proxmox Virtual Environnement qui est une solution de virtualisation qui se base sur du Linux KVM (Kernel-based Virtual Machine).

Configuration :

Pour commencer, il faut configurer les interfaces, car pour fonctionner il nous faut deux cartes réseau, une pour le côté LAN et une autre pour le côté WAN.

Pour les configurer il faut se rendre dans ce fichier : **/etc/network/interface**

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens18
iface ens18 inet dhcp
# The second netwok interface
allow-hotplug ens19
iface ens19 inet static
        address 192.168.1.254/24

pre-up iptables-restore < /etc/network/iptables_rules
```

Dans ce fichier nous avons la première interface principale (ens18), cette interface est celle du côté WAN. La seconde interface (ens19) et celle du côté LAN, le réseau local que nous voulons créer.
La 1er interface est en DHCP pour récupérer une IP du côté du serveur DHCP, il est possible de le configurer en IP fixe, comme la seconde interface.
Pour le côté LAN, comme celle-ci sera la passerelle (Gateway) il lui faut une IP fixe, nous ajoutons **allow-hotplug** puis suivie de l'interface que vous voulez, ceci nous permet de démarrer l'interface au

démarrage, mais que si elle est connectée à un réseau. Il est possible de les démarrer automatiquement même si elles ne sont pas connectées à un réseau, il suffit de remplacer par **iface**. Si vous avez branché la carte réseau, mais que vous n'avez pas d'IP vous pouvez l'activer en effectuant cette commande **ifup** suivie du nom de votre carte réseau. (ifup ens19)
Attention, ne pas oublier de redémarrer le service réseau **systemctl restart networking.service**

Pour pouvoir aller sur internet sans avoir de problème, il nous faudrait un pare-feu. Nous allons utiliser **Iptables,** c'est un logiciel libre auquel nous pouvons configurer des règles de pare-feu.

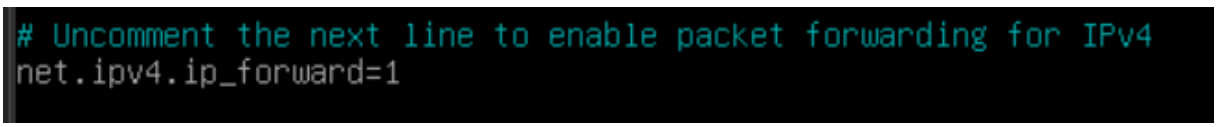
Attention si nous ne sauvegardons pas les règles, elles sont remises à zéro, c'est pourquoi il faut les enregistrer et les réinjecter, pour ceci nous utilisons le fichier de configuration des interfaces réseau, car il est préchargé au démarrage de la machine, ce qui réécrit les règles à chaque redémarrage de la machine.

Pour ceci nous n'avons pas besoin d'installer un paquet, il est déjà près installé.

Nous devons effectuer cette commande pour faire le pont avec le côté LAN et WAN.
iptables -t nat -A POSTROUTING -o ens18 -j MASQUERADE
Voici la règle qui utilise la table de correspondance de paquets NAT (-t nat) elle spécifie la chaîne intégrée POSTROUTING pour le NAT (-A POSTROUTING) qui part sur le réseau externe donc le côté WAN (-o ens18). POSTROUTING permet aux paquets d'être modifié l'lorsqu'ils quittent le périphérique externe (WAN) du pare-feu. -j MASQUERADE est spécifique, il va masquer l'adresse IP privée du côté LAN (192.168.2.30/24) avec l'adresse IP externe du pare-feu, donc la passerelle.

Une fois la règles iptables inscrite, si vous avez fait une erreur il suffit d'utiliser ceci ce qui équivaut à effacer toutes les règles une par une. **iptables -X** # Efface la chaîne spécifiée définie par l'utilisateur. **iptables -t nat -F** #Efface toutes les règles une par une de la table nat. **iptables -t nat -X** # Efface la chaîne spécifiée définie par l'utilisateur de la table nat., mais pour vérifier si vous ne vous étiez pas trompé il suffit de taper cette commande **iptables -t nat -L** ce qui permet de voir si la règle c'est bien mis en place. Et ne pas oublier de les sauvegardées, avec cette commande **iptables-save > /etc/network/iptables_rules**

Remarque, par défaut la politique IPV4 de la redirection d'IP est désactivée par Red Hat Entreprise Linux, ceci évite de transformer les machines en routeur. Comme nous devons transiter sur le WAN il faut l'activer, il faut nous rendre dans ce fichier **/etc/sysctl.conf** il suffit de décommander la ligne.



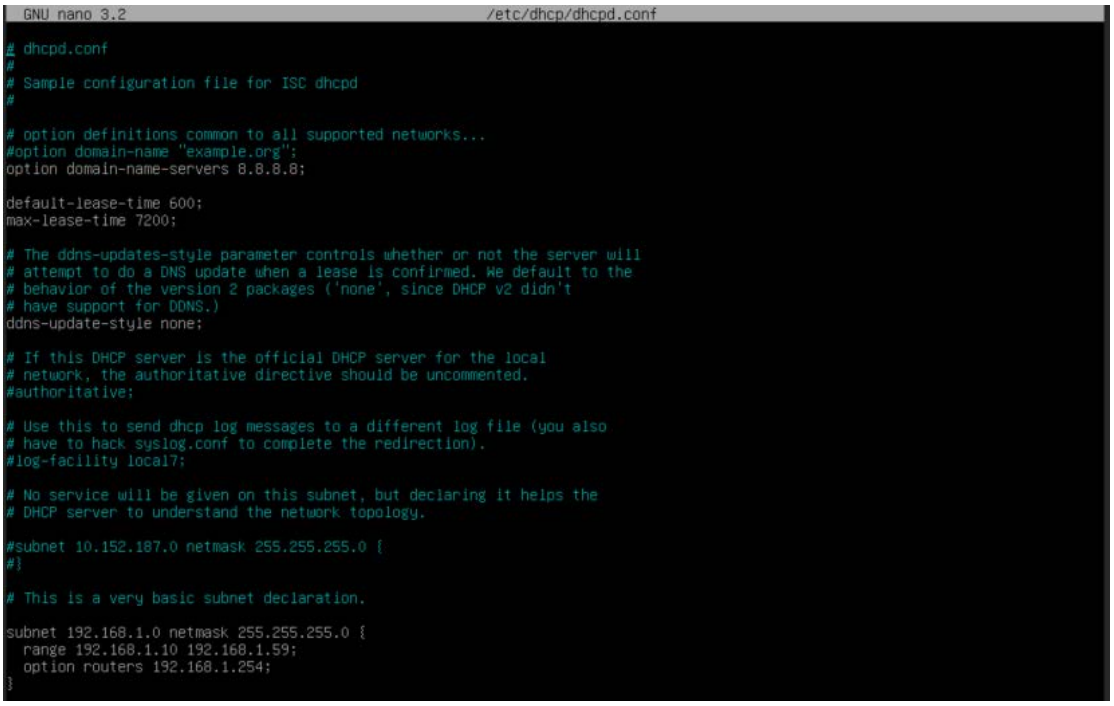
Dans un réseau local, nous avons un serveur DHCP, votre box (routeur) fait office de serveur DHCP, qui vous attribue une IP sur votre matérielle informatique, si vous vous connectez sur ce réseau.

Pour tester notre passerelle, nous allons installer un service DHCP.

Installation DHCP:

Apt install isc-dhcp-dhcpd-server, ceci va nous permettre d'installer le service DHCP.

Si vous avez un message rouge ne pas paniquer, c'est normal, le service que vous venez d'installer n'est pas configuré, pour ce faire il faut se rendre dans ce fichier, **/etc/dhcp/dhcpd.conf**



Voici le fichier à configurer, pas grande chausse à faire :

Option domain-name-server 8.8.8.8 = ceci est le DNS sur quel nom de domaine fait -il autorité, vers qui il va chercher les informations correspondent vers les IPs et les noms. Et surtout donner un DNS au client.

Le défaut-lease-time 600 et max-lease-time = 7200 = ceci veut dire combien de temps il va recharger les beaux DHCP. Généralement on laisse par défaut.

Ddns-update-style none = pour le moment je n'arrive pas bien à comprendre cette ligne. Dans notre configuration il n'est pas nécessaire de le modifier.

Nous arrivons sur la partie DHCP, c'est à dire quelle IP réseau nous allons attribuer, nous partons sur une déclaration basique, il nous faut un sous-réseau, un masque, une plage d'IP à attribuer, et la passerelle. Pour que le service fonctionne correctement il devra écouter sur une interface réseau donc l'interface LAN, pour ce faire il faut modifier le fichier **/etc/defaults/isc-dhcp-server**

Ne pas se tromper d'interface bien prendre l'interface qui sera du côté LAN et non du côté WAN.

Phase de test :

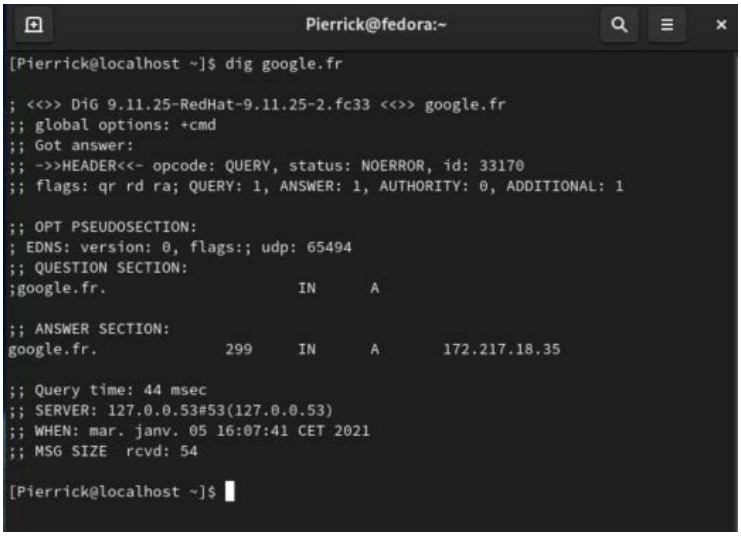
Maintenant nous allons tester notre LAN, à savoir si nous récupérons bien une IP, et si nous pouvons consulter une page web.

Pour ce faire nous avons un ordinateur client, l'ordinateur client n'a pas d'IP, nous allons voir ce que le serveur DHCP nous donne.

Nous pouvons voir que notre client a récupérerez une IP.

Utilisation de la commande DIG (domain information groper) :
Cette commande nous permet d'interroger des serveurs DNS, ce qui nous donnera une réponse positive ou négative sur notre routage, si la réponse et positive ceci veut dire que la communication entre le LAN et le WAN fonctionne, si c'est négatif alors ceci voudrait dire qu'il y a un problème de résolution nom et IP ou alors un problème de routage.

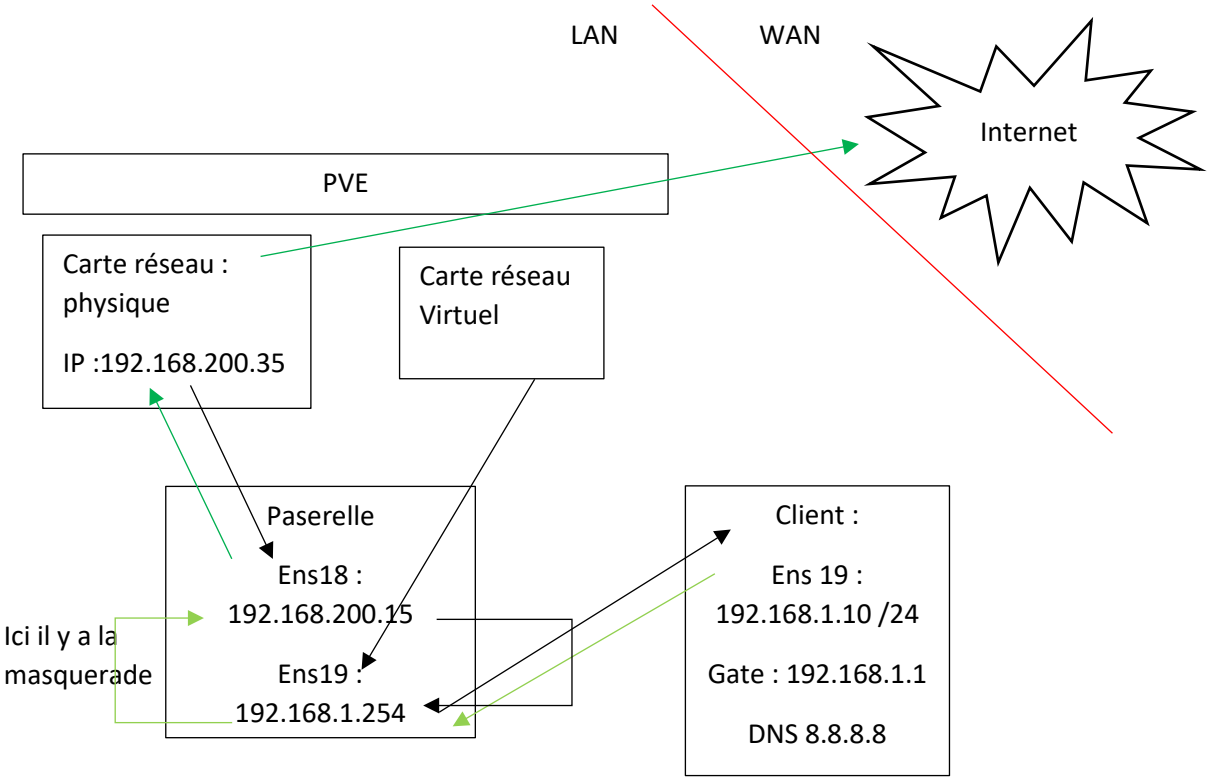
Explication :



Dans un premier temps on demande qui est googl.fr, dans la ligne ->>HEADER<<- il y a de marquer NOERROR ceci veut dire que la requête à fonctionner, nous pouvons voir que nous avons bien posé la question « Question SECTION » google.fr et dans la réponse « Answer SECTION » google.fr et 172.217.18.35, donc la requête a fonctionné. Conclusion la passerelle fonctionne l'objectif et atteint.

Schéma :

Voici un Schéma pour mieux comprendre le fonctionnement :



En vert se sera les flues sortant (comme la commande dig google.fr) on va questionner les DNSs donc on sort sur le côté WAN.