TP WireGuard

Qu’est-ce que WireGuard:

WireGuard est un protocol VPN (Virtual Private Network) open source, développé par Jason A. Donenfeld et a été introduit pour la première fois en 2016. Conçu pour fournir une connexion sécurisée et rapide.

Source : https://www.purevpn.fr/blog/wireguard-vs-openvpn/

Voici une comparaison pour connaître quelle est la performance de ces protocoles VPN, nous pouvons voir que WireGuard a de meilleures performances.

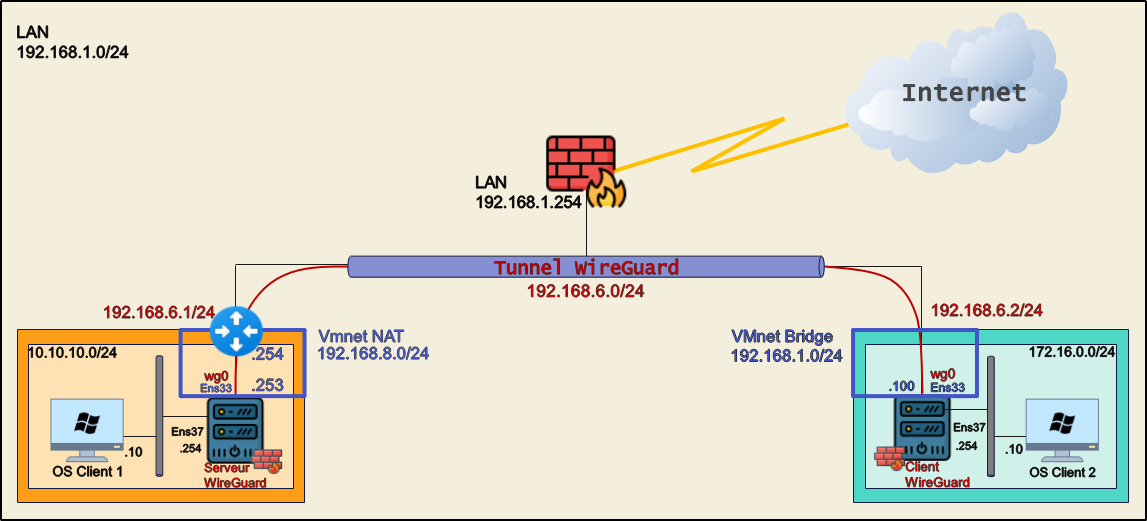
Mise en place TP

Pour effectuer ce TP nous aurons besoin de :

* Deux Windows XP (Représente le utilisateurs)
* Deux Linux Ubuntu Servers

Ce TP sera réalisé sur VMware WorkStation 17 l’adressage utiliser ci-dessous :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Names | Network | Mask | Interfaces | MAC addresses |
| OS Client 1 | 10.10.10.10 | 255.255.255.0 |  |  |
| OS Client 2 | 172.16.0.10 | 255.255.255.0 |  |  |
| Linux 1  Serveur WireGuard | 192.168.8.253 | 255.255.255.0 | Ens33 |  |
| 10.10.10.254 | 255.255.255.0 | Ens37 |  |
| 192.168.6.2 | 255.255.255.0 | Wg0 |  |
| Linux 2  Client WireGuard | 172.16.0.254 | 255.255.255.0 | Ens33 |  |
| 192.168.1.100 | 255.255.255.0 | Ens37 |  |
| 192.168.6.1 | 255.255.255.0 | Wg0 |  |
| Tunnel WireGuard | 192.168.6.0 | 255.255.255.0 | /////////////////// | /////////////////// |
| LAN | 192.168.1.0 | 255.255.255.0 | ////////////////// | /////////////////// |
| 192.168.1.254 | 255.255.255.0 | ///////////////// | /////////////////// |

Topologie du TP :

Wireguard Server

## Set Up WireGuard VPN on Ubuntu By Editing/Creating wg0.conf File ##

[Interface]

## My VPN server private IP address ##

Address = 192.168.6.1/24

## My VPN server port ##

ListenPort = 41194

## VPN server's private key i.e. /etc/wireguard/privatekey ##

PrivateKey = KORTxD9Eekp9iEjXDJ7+ABZGFcBolclJQaN54mZ1sXc=

[Peer]

## Desktop/client VPN public key ##

PublicKey = U9k8lCadf/IeJ02gfs/C8TUwt/AVPW0dkCrcaMS4v2E=

## client VPN IP address (note the /32 subnet) ##

AllowedIPs = 192.168.6.2/32

Wireguard Client

[Interface]

## This Desktop/client's private key ##

PrivateKey = QBcGDJf1FBvCTw+B15F+zK5BEw7kjv2tR4BpJw4LD1M=

## Client ip address ##

Address = 192.168.6.2/24

[Peer]

## Ubuntu 20.04 server public key ##

PublicKey = ibxJpDOazPiRBQra2GNRvm/wYW7NQGg85TrseADOzGI=

## set ACL ##

AllowedIPs = 192.168.6.0/24

## Your Ubuntu 20.04 LTS server's public IPv4/IPv6 address and port ##

Endpoint = 192.168.1.56:41194

## Key connection alive ##

PersistentKeepalive = 15

IP Tables

Configure iptables:

sudo iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE

sudo iptables -A FORWARD -i ens33 -o ens37 -m state --state RELATED,ESTABLISHED -j ACCEPT

sudo iptables -A FORWARD -i ens37 -o ens33 -j ACCEPT

Server Wireguard

ip route add 172.16.0.0/24 via 192.168.6.2

Client Wireguard

ip route add 10.10.10.0/24 via 192.168.6.1