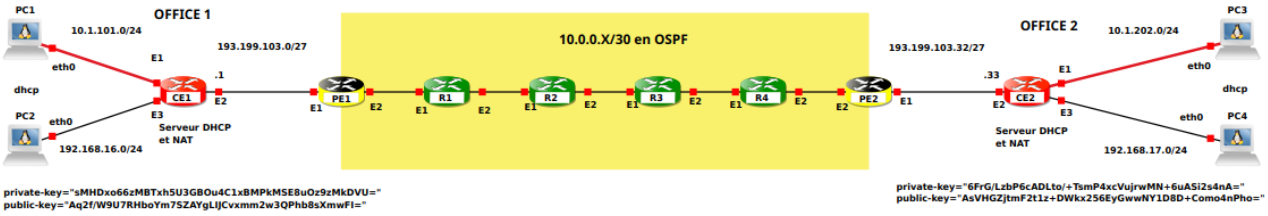
UNIVERSITÉ CAEN NORMANDIE

TP-VPN WireGuard

21.03.2023

On "blinde" le fil☺

Auteur : Pascal Fougeray



Source : Moi ☺

1 Introduction

Dans ce TP, je vous propose de voir comment deux machines en @IP privées sur des sites éloignés géographiquement peuvent communiquer malgré le NAT et malgré leurs @IP privées ! ! !

2 La structure

Elle reprend en partie celle vu d'un précédent TP, le TP Ping
Le routeur CE fait du NAT et sert aussi de serveur DHCP, mais pas le même réseau pour les 4 PC ! ! !
On a 2 plans d'adressage :

1. 192.168.16.0/24 et 192.168.17.0/24 pour PC2 et PC4 qui eux ne peuvent pas se pinguer car ils ne passent pas par le Tunnel VPN
2. 10.1.101.0/24 et 10.1.202.0/24 pour PC1 et PC qui eux peuvent se pinguer car ils passent par le Tunnel VPN

3 Les technologies utilisées

1. Le routage avec OSPF qui ne doit plus vous poser de souci. Nous n'avons qu'une seule aire, aucun intérêt de complexifier le système
2. Le NAT et le DHCP sur les 2 routeurs CE
3. La technologie VPN dernière génération : **WireGuard**
4. **Le chiffrement asymétrique à l'aide de la paire de clefs publique/privée**
   https://fr.wikipedia.org/wiki/Chiffrement_de_bout_en_bout

   On chiffre avec la clef publique et on déchiffre avec la clef privée

   https://fr.wikipedia.org/wiki/Cryptographie_asymétrique

À la fin de ce TP vous devrez me donner un modèle logique de la structure physique utilisée durant ce TP.

4 TP

1. **Allumez** les routeurs , sauf CE1 et CE2 (Pas les PC1 à 4 !)
2. **Mettez** une sonde wireshark entre **PE1** et **PE2** et **sélectionnez ICMP**
3. **Allumez** les 2 routeurs CE l'un après l'autre en attendant 1mn entre les 2. Car ces routeurs demandent beaucoup plus de ressources !

   Après le login il affiche : **new password> faites** CTRL-C
4. **Vérifiez** que CE1 peut pinguer CE2 : ***ping 193.199.103.33***

   Si ça marche alors c'est que tout fonctionne, ouf ☺
5. **Vérifiez** sur wireshark que vous avez bien des trames de type **ICMP**.
6. **Allumez** les 4 PC
7. **Relevez** les adresses @IP des 4 PC et **notez** les pour la suite du TP !

4.0.1 Partie Wireguard - VPN !

1. Sur CE1 et CE2 **lancez** la commande ***/interface/wireguard/print***

```
[admin@CE1] > /interface/wireguard/print
Flags: X - disabled; R - running
 0  R name="wireguard1" mtu=1420 listen-port=61664 private-key="sMHDxo66zMBTxh5U3GBOu4C1xBMPkMSE8uOz9zMkDVU=" public-key="Aq2f/W9U7RHboYm7SZAYgLIJCvxmm2w3QPhb8sXmwFI="
[admin@CE1] >
```

   Vous y voyez **la paire de clefs publique/privée**

2. Sur CE1 et CE2 **lancez** la commande ***/interface/wireguard/export***

```
[admin@CE1] > /interface/wireguard/export
# mar/20/2023 10:53:29 by RouterOS 7.7
# software id =
#
/interface wireguard
add listen-port=61664 mtu=1420 name=wireguard1
/interface wireguard peers
add allowed-address=10.1.202.0/24 endpoint-address=193.199.103.33 endpoint-port=61664 interface=wireguard1 public-key="AsVHGZjtmF2t1z+DWkx256EyGwwNY1D8D+Como4nPho="
[admin@CE1] >
```

   On peut remarquer que la clef publique de CE1 est dans la conf du tunnel wireguard de CE2 et réciproquement.

   Normal on chiffre avec la clef publique et on déchiffre avec la clef privée

3. **Lancez** un ping de PC2 à PC4 : ***ping 192.168.17.xx***

   Expliquez pourquoi cela ne fonctionne pas en regardant ce que vous obtenez sur wireshark
4. **Lancez** un ping de PC1 à PC3 : ***ping 10.1.202.xx***

   Expliquez pourquoi cela fonctionne !

   Regardez sur wireshark les nouvelles trames ICMP, mince elles sont où, ça ping et pourtant on a rien sur wireshark ☺

Réponse dans le cours ! ! !

Voilà ce que ça donne avec wireshark (Capture du TP...)

On peut en conclure cette fois-ci :

— Le ping est passé par le tunnel, les 2 machines avec des @IP privées peuvent communiquer. Si ICMP passe alors tous les protocoles des couches supérieurs vont pouvoir passer !

— Les paquets originels, ceux entre le PC et le CE, sont encapsulés et chiffrés dans le protocole **Wireguard** !

— Les adresses utilisées pour le routage ne sont pas les @IP privées mais les @IP publiques ! ! !

— Donc si on veut les voir avec wireshark, il faut non pas sélectionner le protocole **ICMP** mais **WG** (Acronyme de **Wireguard**) comme le montre la figure suivante

5 Conclusion

1. **Dessinez** le modèle logique de la structure physique entre PC1 et PC3 ☺
2. **Concluez**