Fiche TP N°1 : Technologies Réseaux

Partie 2 : Réseaux Privés Virtuels (VPN)

Prérequis

Adressage IP, configuration de topologie avec GNS3.

NB

Chaque étudiant a une note individuelle par séance. (Si absence, 0 si non justifiée, pas de note sinon).
Note de séance = interrogation et question traitées en séance + rapport individuel
Chaque étudiant fait la totalité des manipulations individuellement (ou par binôme) sur sa machine, vérifiées périodiquement par l'enseignant.

1. Objectifs

- Comprendre le fonctionnement de tunnel VPN.
- Maîtriser les technologies réseau et de sécurité sous-jacentes aux VPN.
- Mettre en œuvre un VPN Site à Site avec linux.

2. Présentation

Un réseau privé virtuel (VPN) est utilisé pour créer une communication privée ou pour fournir une extension sécurisée d'un réseau privé dans un réseau non sécurisé tel qu'Internet. VPN est une technologie de sécurité largement utilisée. Le type de VPN qu'on va utiliser dans ce travail pratique est un VPN Site à Site. La conception et la mise en œuvre des VPN illustrent un certain nombre de principes et de technologies de sécurité, notamment la cryptographie, l'intégrité, l'authentification, la gestion des clés, l'échange de clés pour une infrastructure à clé publique.

3. Commandes et configuration

NB : dans les textes de TP, le texte en ***gras-italique*** désigne des commandes et <t*exte*> désigne une valeur qui va devoir être indiquée.

3.1. Configuration d'une passerelle Linux (Serveur VPN)

- Configuration d'une adresse statique
  sudo ip address add *<adresse>/<masque>* ***dev*** *<nom_interface>*
- Activation d'une interface réseau
  sudo ip link set dev *<nom_interface>* ***up***
- Configuration d'une route par défaut
  sudo ip route add default via *<adresse_passerelle>* ***dev*** *<nom_interface>*
- Activation du routage
  sysctl -w net.ipv4.ip_forward=1
- Configuration du NAT
  sudo iptables -t nat -A POSTROUTING -o *<interface_publique>* ***-j MASQUERADE***

3.2. Configuration d'un tunnel GRE

- Configuration d'un tunnel GRE
  # Création de l'interface du tunnel
  sudo ip tunnel add *<nom_intf_tunnel>* ***mode gre remote*** *<adr_public_distante>* ***local*** *<adresse_public_locale>*
  # Activation de l'interface du tunnel
  sudo ip link set dev *<nom_interface_tunnel>* ***up***
  # Configuration de l'adresse du tunnel
  sudo ip address add *<adresse_tunnel>/<masque>* ***dev*** *<nom_interface_tunnel>*

Configuration d'un route par un tunnel
sudo ip route add *<adresse_reseau>* *<masque>* ***dev*** *<nom_interface_tunnel>*

- Suppression d'un tunnel GRE
  # Désactivation de l'interface du tunnel
  sudo ip link set dev *<nom_interface_tunnel>* ***down***
  # Suppression de l'interface du tunnel
  sudo ip tunnel del *<nom_interface_tunnel>*

3.3. Configuration d'un tunnel OpenVPN

- Création d'une clé partagée de chiffrement
  sudo openvpn --genkey --secret *<nom_cle>**.key***
- Copie de la clé partagée via SSH
  sudo scp *<nom_cle>**.key*** *<user>**@***<adresse_ip>***:/chemin***
- Création d'un tunnel sécurisé avec une clé partagée
  sudo openvpn --dev *<nom_intf_tunnel>* ***--local*** *<adr_public_local>* ***--remote*** *<adr_public_distante>*
  --ifconfig *<adr_privée_local>* *<adr_privée_distante>* ***--secret*** *<nom_cle>**.key***

3.4. Sauvegarde des configurations pour le serveur VPN

- Pour sauvegarder dans les machines linux, d'abord il faut ajouter les commandes à sauvegarder dans le fichier « /opt/bootlocal.sh » avec la commande:
  vi /opt/bootlocal.sh
- Ensuite il faut faire une sauvegarde avec la commande :
  backup

3.5. Commandes de diagnostique

- Affichage de la liste des interfaces réseaux
  ip link show ou ***ifconfig -a***
- Affichage de la table de routage
  ip route show
- Tester la connectivité
  ping *<adresse_ip>*

3.6. Rappel configuration VPC

- Configuration de l'adresse IP et passerelle : ***ip*** *<adresse_pc>/<masque>* *<passerelle>*
- Sauvegarde de la configuration : ***save*** *<nom_pc>*
- Chargement de la configuration : ***load*** *<nom_pc>*

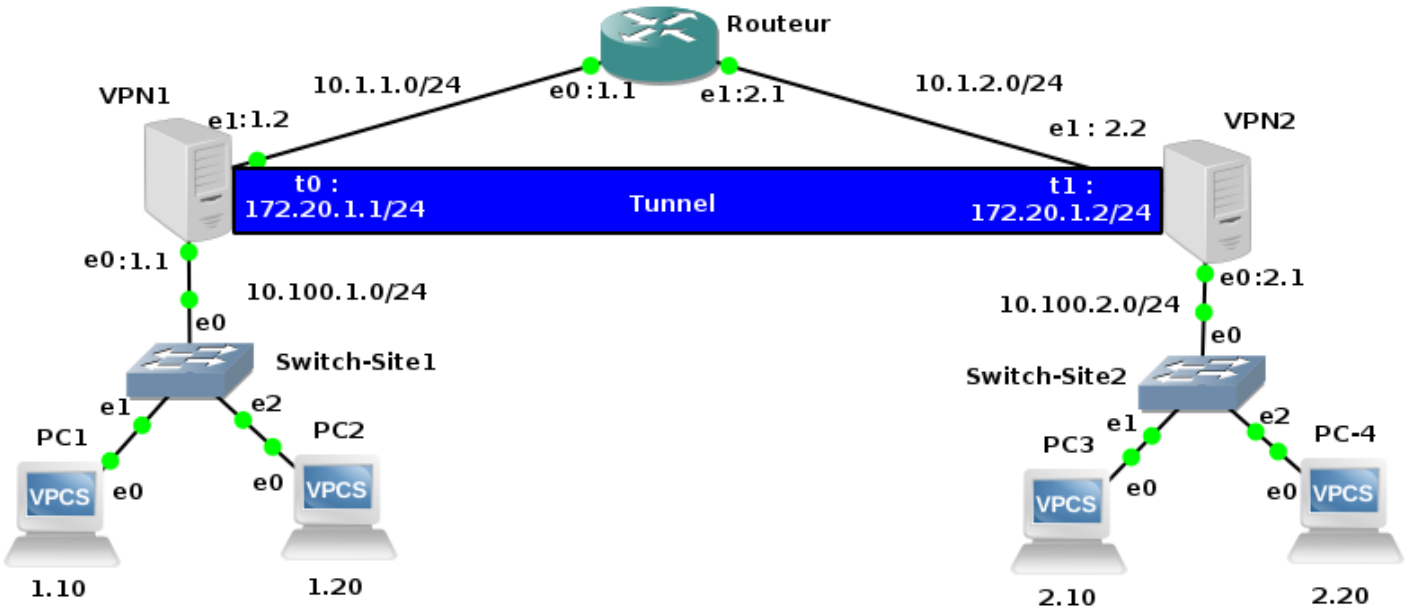
4. Exercice

1. VPN site-à-site avec GRE

Nous considérons le schéma réseau d'une entreprise avec deux sites reliés par un tunnel VPN représenté ci-dessous.

Remarque :

1. Le login et mot de passe pour les serveurs VPN sont :
   Login : gns3
   Password : gns3
2. La passerelle dans les deux sites sera une machine virtuelle VPN avec un système linux (TinyCore).



a) Câbler le schéma réseau ci-dessus. Ensuite, configurer :
   - Les clients de chaque réseau de l'entreprise (PC1, PC2, PC4, PC4).
   - les serveurs VPN : VPN1 et VPN2 (interfaces, routage, NAT).
   - Les interfaces du routeur et le routage.
   - Valider le fonctionnement du réseau à l'aide de commandes de diagnostic (ping).
   - Quel est l'intérêt des commandes : ***sysctl -w net.ipv4.ip_forward=1sudo*** et ***iptables -t nat -A POSTROUTING -o <interface_publique> -j MASQUERADE***
b) Utiliser la commande ***trace <adresse_pc>*** pour noter le chemin entre le pc1 et pc3.
c) Configurer un tunnel GRE entre les deux sites de l'entreprise.
   - Valider le fonctionnement du tunnel à l'aide de commandes de diagnostique.
   - Utiliser la commande ***trace <adresse_pc>*** pour noter le chemin entre le pc1 et pc3. Que remarquez-vous ?
d) Quelle est la valeur de la MTU dans le tunnel ? Expliquer le résultat.
e) Démarrer une capture de trafic réseau dans VPN1 avec la commande : ***sudo tcpdump -vi eth1 proto gre***
   Ensuite lancer un ping à partir du PC1 vers le PC3: ***ping 10.100.2.10***
   - Commenter le résultat
f) Quels sont les inconvénients d'un tunnel GRE ? Dans quels cas ce type de tunnel peut être utile ?

2. VPN site-à-site avec OpenVPN

a) Supprimer les tunnel précédemment configuré sur les passerelles.
b) Démarrer d'abors SSH en tapant la commande suivante dans les passerlles VPN1 et VPN2 :
   sudo /usr/local/etc/init.d/openssh start
c) Créer une clé partagée de chiffrement avec OpenVPN sur une des passerelles, et copier cette clé sur l'autre passerelle (via la commande SSH : scp).
d) Configurer un tunnel sécurisé entre les deux sites de l'entreprise à l'aide la clé partagée de chiffrement précédemment créée.
   Valider le fonctionnement du tunnel à l'aide de commandes de diagnostique.
e) Commenter la différence entre les deux méthodes (GRE et OpenVPN).