

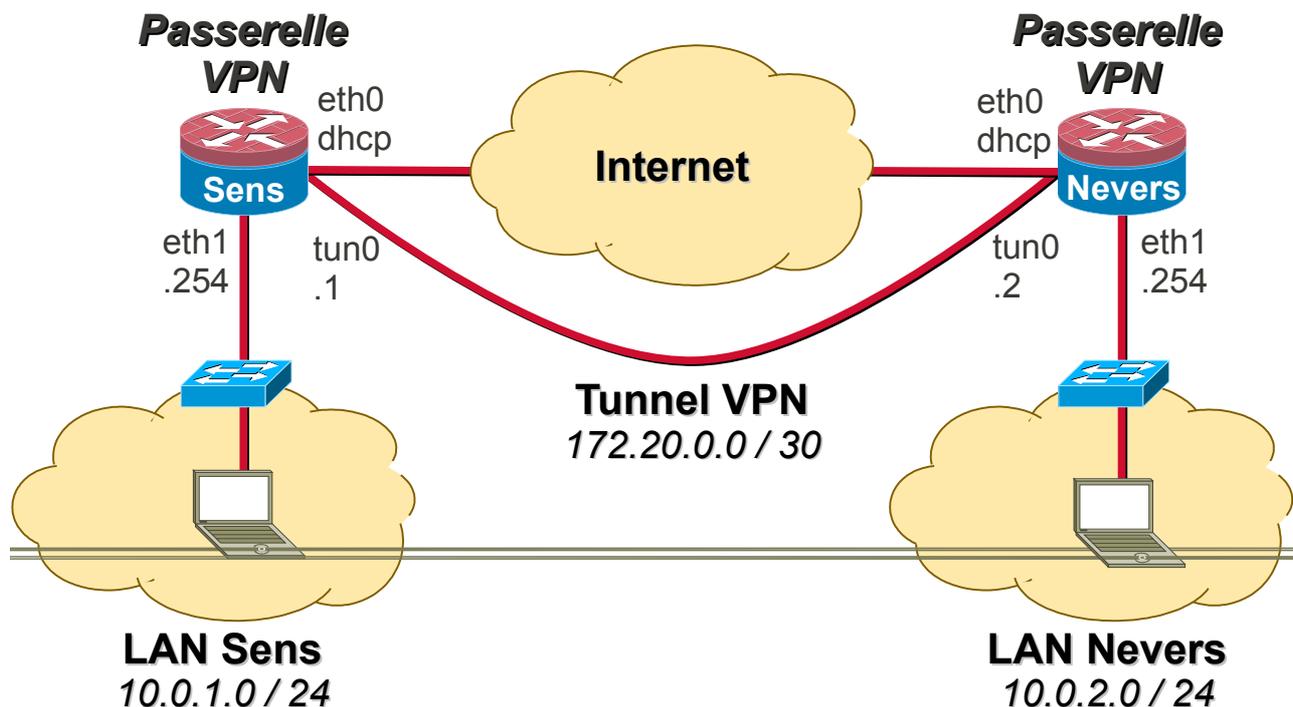
# TP 4

## Réseaux privés virtuels

Réseaux et Télécoms – IUT d'Auxerre – Université de Bourgogne

### 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.



La passerelle sera une machine virtuelle DebianServer (faites attention à la correspondance interfaces physiques / interfaces virtuelles, et pensez à initialiser les adresses MAC de chaque interface virtuelle).

- Câblez le schéma réseau ci-dessus. Ensuite, configurez la passerelle (interfaces, routage, NAT) et un client (interface, routage) dans chaque réseau de l'entreprise. Validez le fonctionnement du réseau à l'aide de commandes de diagnostic.
- Configurez un tunnel GRE entre les deux sites de l'entreprise (sans oublier de configurer la table de routage des passerelles). Validez le fonctionnement du tunnel à l'aide de commandes de diagnostic (adresse des interfaces, tables de routage, connexion client-à-client).
- Quelle est la valeur de la MTU dans le tunnel ? Expliquez le résultat.
- Démarrez une capture de trafic réseau avec Wireshark sur l'interface publique (eth0), et effectuez une requête ping du client d'un site vers le client de l'autre site. Commentez l'encapsulation de protocole à l'intérieur du tunnel.
- Quels sont les inconvénients d'un tunnel GRE ? Dans quel cas ce type de tunnel peut être utile ?

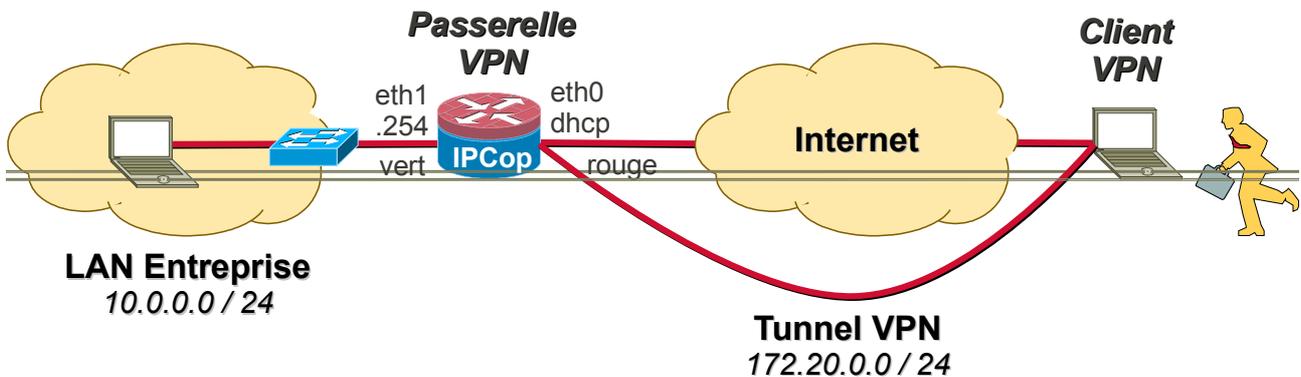
## Exercice 2 : VPN site-à-site avec OpenVPN

Supprimez le tunnel précédemment configuré sur la passerelle.

- Créez une clé partagée de chiffrement avec OpenVPN sur une des passerelles, et copiez cette clé sur l'autre passerelle (via SSH ou une clé USB).
- Configurez un tunnel sécurisé entre les deux sites de l'entreprise à l'aide la clé partagée de chiffrement précédemment créée. Validez le fonctionnement du tunnel à l'aide de commandes de diagnostic (adresse des interfaces, tables de routage, connexion client-à-client).
- Démarrez une capture de trafic réseau avec Wireshark sur l'interface publique (eth0), et effectuez une requête ping du client d'un site vers le client de l'autre site. Commentez l'encapsulation de protocole à l'intérieur du tunnel.

## Exercice 3 : VPN nomade avec IPCop

Nous considérons maintenant le schéma réseau d'une entreprise avec des utilisateurs nomades VPN représenté ci-dessous.



La passerelle sera une machine virtuelle IPCop (faites attention à la correspondance interfaces physiques / interfaces virtuelles, et pensez à initialiser les adresses MAC de chaque interface virtuelle).

Les utilisateurs nomades seront des machines virtuelles Linux et Windows situées dans Internet (c'est-à-dire un autre poste de la salle de TP).

- Connectez-vous à l'interface d'administration de IPCop avec un navigateur Web, et vérifiez la configuration des interfaces réseaux.
- Créez une autorité de certification, et générez les certificats racine et système.
- Configurez le serveur OpenVPN sur l'interface rouge en poussant les routes du réseau vert. Ensuite démarrez le serveur.
- Créez les certificats pour deux clients VPN nomades, et téléchargez la configuration des clients (archive ZIP).
- Configurez les deux clients nomades (Windows et Linux), et validez le fonctionnement de la connexion VPN.

# Annexe

## Configuration d'une passerelle Linux

- **Activation d'une interface réseau**

```
ip link set dev nom_interface up
```

- **Configuration d'une adresse statique**

```
ip addr add adresse/masque dev nom_interface
```

- **Configuration d'une adresse dynamique**

```
dhclient nom_interface
```

- **Configuration d'une route statique**

```
ip route add adresse_reseau/masque via adresse_passerelle  
dev nom_interface
```

- **Configuration d'une route par défaut**

```
ip route add default via adresse_passerelle dev  
nom_interface
```

- **Activation du routage**

```
sysctl -w net.ipv4.ip_forward=1
```

- **Configuration du NAT**

```
iptables -t nat -A POSTROUTING -o interface_public -j  
MASQUERADE
```

## Configuration d'un tunnel GRE

- Configuration d'un tunnel GRE

```
# Création de l'interface du tunnel
ip tunnel add nom_interface_tunnel mode gre remote
adresse_public_distante local adresse_public_locale

# Activation de l'interface du tunnel
ip link set dev nom_interface_tunnel up

# Configuration de l'adresse du tunnel
ip addr add adresse_tunnel/masque dev nom_interface_tunnel
```

- Suppression d'un tunnel GRE

```
# Désactivation de l'interface du tunnel
ip link set dev nom_interface_tunnel down

# Suppression de l'interface du tunnel
ip tunnel del nom_interface_tunnel
```

## Configuration d'un tunnel OpenVPN

- Création d'une clé partagée de chiffrement

```
openvpn --genkey --secret static.key
```

- Copie de la clé partagée via SSH

```
scp static.key etudiant@adresse:/chemin
```

- Création d'un tunnel sécurisé avec une clé partagée

```
openvpn --remote adresse_public_distante --dev
nom_interface_tunnel --ifconfig adresse_privée_locale
adresse_privée_distante --secret static.key
```

## Configuration de IPCop

- **Configuration des interfaces réseaux (console)**

setup

- **Accès à l'interface Web d'administration (réseau vert)**

URL : https://adresse\_passerelle\_ipcop:8443

Login / Password : admin / tprezo

- **Création d'une autorité de certification**

Menu → RPVs → CA

Génération des certificats racine et système

- **Configuration d'un serveur OpenVPN**

Menu → RPVs → OpenVPN

Cocher la case OpenVPN sur rouge → Configurer le sous-réseau OpenVPN

Enregistrer

Options avancées → Pousser routes → Green network → Enregistrer

Démarrer le serveur OpenVPN

- **Configuration d'un client nomade OpenVPN**

Menu → RPVs → OpenVPN

Contrôle et statut de la connexion → Ajouter

RPV Système à réseau (RoadWarrior) → Enregistrer

Télécharger le programme client (zip)

- **Activation d'une connexion client nomade OpenVPN sous Linux**

openvpn configuration\_client.opvn

- **Activation d'une connexion client nomade OpenVPN sous WindowsXP**

Copier la configuration client dans le répertoire suivant :

C:\Program Files\OpenVPN\Config

Démarrer OpenVPN GUI

- **Activation d'une connexion client nomade OpenVPN sous Windows7**

Copier la configuration client dans le répertoire suivant :

C:\Programmes\OpenVPN\config

Démarrer OpenVPN GUI en tant qu'administrateur