2ème année 2024-2025

Réseaux privés virtuels

Octobre 2024

Objectifs

Réseaux privés virtuels : les VPN permettent de mettre en place des réseaux privés au dessus d'une infrastructure publique.

Imaginons une société possédant un parc informatique réparti sur plusieurs sites distants. Chacun de ces sites possède une connexion à l'Internet et un certain nombre d'adresses IP officiellement attribuées.

Certains de ces sites regroupent éventuellement un nombre de postes supérieur à celui des adresses qui leur sont allouées. Ils utilisent alors en interne des adresses IP privées telles que définies par la RFC 1918.

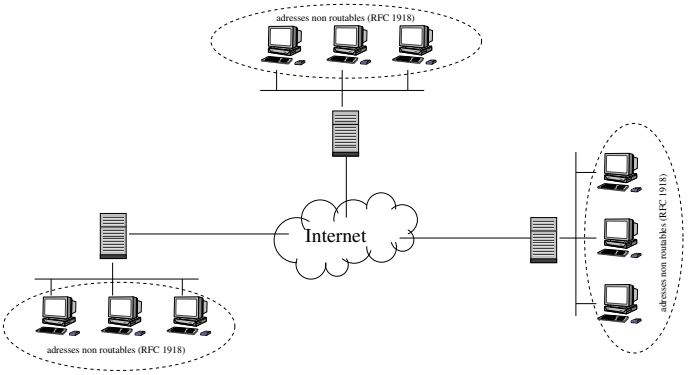

FIGURE 1 – Un réseau multisite.

▷ **Exercice 1 : Mise en place du réseau**

Construisez un réseau comparable à celui de la figure 1. L'enseignant vous fournira une adresse IP *par site ainsi que l'adresse* IP *du routeur de votre fournisseur d'accès. L'un des sites comportera deux stations, l'autre une seule.* ■

Les administrateurs de ces sites doivent alors apporter des solutions techniques aux problèmes suivants :

— Comment permettre aux stations dotées d'une adresse non routable de communiquer avec des stations situées hors du site local ?
— Comment assurer entre les différents sites une communication comparable à celle d'un site unique, en termes de confidentialité ou de plan d'adressage ?

Nous avons déjà étudié et mis en place la traduction d'adresse (ou NAT) qui permet de répondre partiellement à la première question. Ce n'est qu'une réponse partielle dans la mesure où il reste impossible à deux hôtes situés sur des sites différents de communiquer entre eux.

Les réseaux privés virtuels, ou VPN (virtual private network), apportent une réponse à la seconde question et permettent ainsi de compléter la réponse partielle apportée par le NAT à la première.

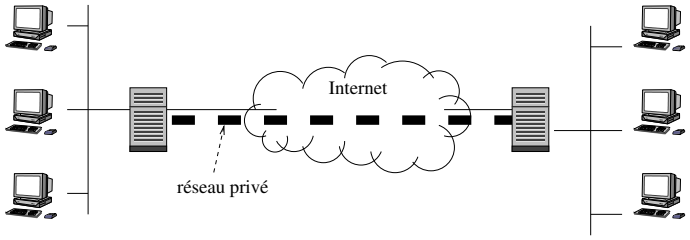

FIGURE 2 – Un réseau multisite.

Comme l'illustre la figure 2, un VPN permet de mettre en place un réseau privé au dessus d'un réseau public. Le réseau est privé au sens où il n'implique que des stations appartenant à une même organisation privée ; il est virtuel car il ne correspond à aucune architecture matérielle privée.

L'outil de base permettant le déploiement d'un réseau privé est le tunnel. Un tunnel peut être vu comme un flux de communication entre deux routeurs configurés pour encapsuler les données de ce flux dans des paquets conformes au réseau qui interconnecte les deux routeurs et qui serait, sans cette encapsulation incapable d'acheminer correctement ces données.

Les tunnels sont donc particulièrement intéressants pour déployer une nouvelle fonctionnalité sur un réseau puisqu'ils permettent de relier des ilôts sur lesquels cette fonctionnalité est opérationnelle. Ils sont donc largement utilisés pour le passage à IPv6, la mise en place du multipoint, ...

L'un des protocoles permettant de réaliser des tunnels sur IP se nomme GRE (generic routing encapsulation) et réalise l'encapsulation de tout protocole dans des paquets IP.

Sous Linux, un tunnel se configure de la façon suivante sur chacun des deux routeurs d'extrémité :

```
# ip tunnel add <nom> mode gre local <iplocal>  remote <ipremote>
```

où :

`nom` est le nom du tunnel du point de vue de ce routeur, c'est-à-dire le nom de l'interface IP représentant cette extrémité du tunnel ;

`iplocal` est l'adresse IP de l'interface locale située à l'entrée du tunnel ;

`ipremote` est l'adresse IP de l'interface distante située à la sortie du tunnel.

La figure 3 montre le positionnement de ces adresses du point de vue de la machine `R1`.

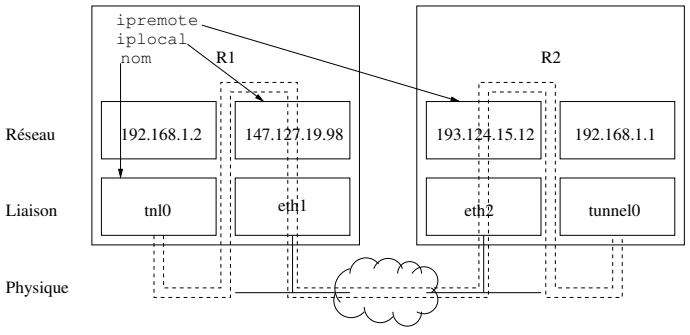

FIGURE 3 – Configuration d'un tunnel.

Lorsque le tunnel a été créé, une nouvelle interface IP apparaît et peut (et doit) être configurée par la commande `ifconfig`.

▷ **Exercice 2 : Mise en place d'un tunnel**

Mettez en place un tunnel et faites en sorte que toutes les machines des différents sites puissent communiquer. Quelle précaution doit-on prendre pour que les machines puissent encore communiquer avec l'Internet (par exemple via *le* NAT*) ?* ■

Notons que la confidentialité des communications circulant dans le tunnel n'est assurée qu'à condition de mettre en place un mécanisme de chiffrement (par exemple par IPsec).