VPN : l'exemple d'openvpn

initiation à la notion de VPN via OpenVPN

VPN ?

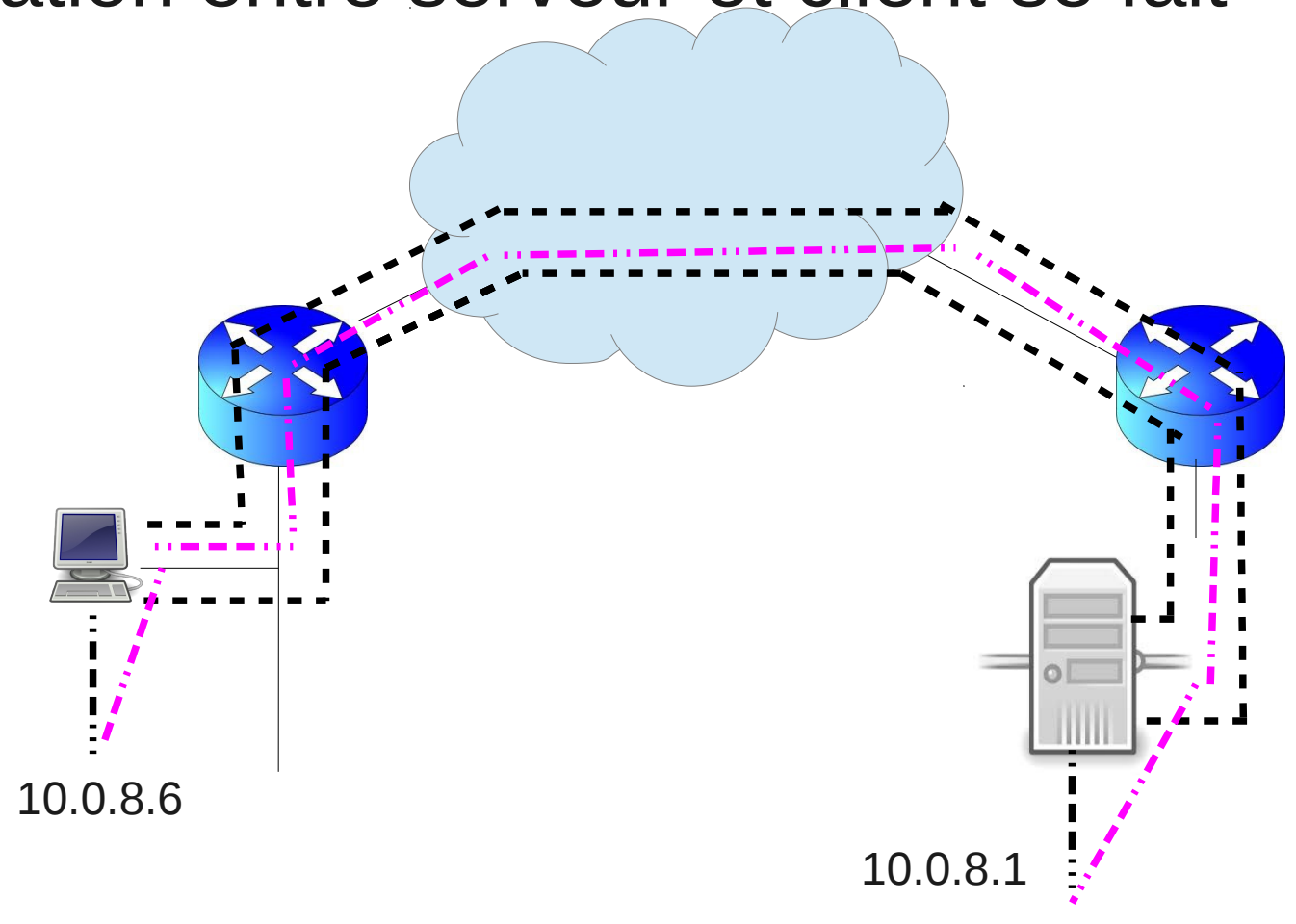
- VPN : Virtual Private Network
- Réseau privé virtuel
  - créer un réseau privé au dessus d'un réseau public
  - permet de faire croire à des machines distantes ou à des réseaux distants qu'ils sont sur le même réseau
  - chiffrement : interdit toute interception de trafic sur le réseau public
  - cas typiques d'utilisation :
    - permettre à une machine nomade de se connecter aux ressources de l'entreprise
    - relier 2 réseaux distants pour n'en faire virtuellement qu'un seul

OpenVPN

- opensource
- multiplateforme
- de nombreux modes d'authentification (dont certificats, mot de passe, …)
- s'appuie sur SSL
- le VPN consiste à créer une interface réseau virtuelle sur le client et sur le serveur

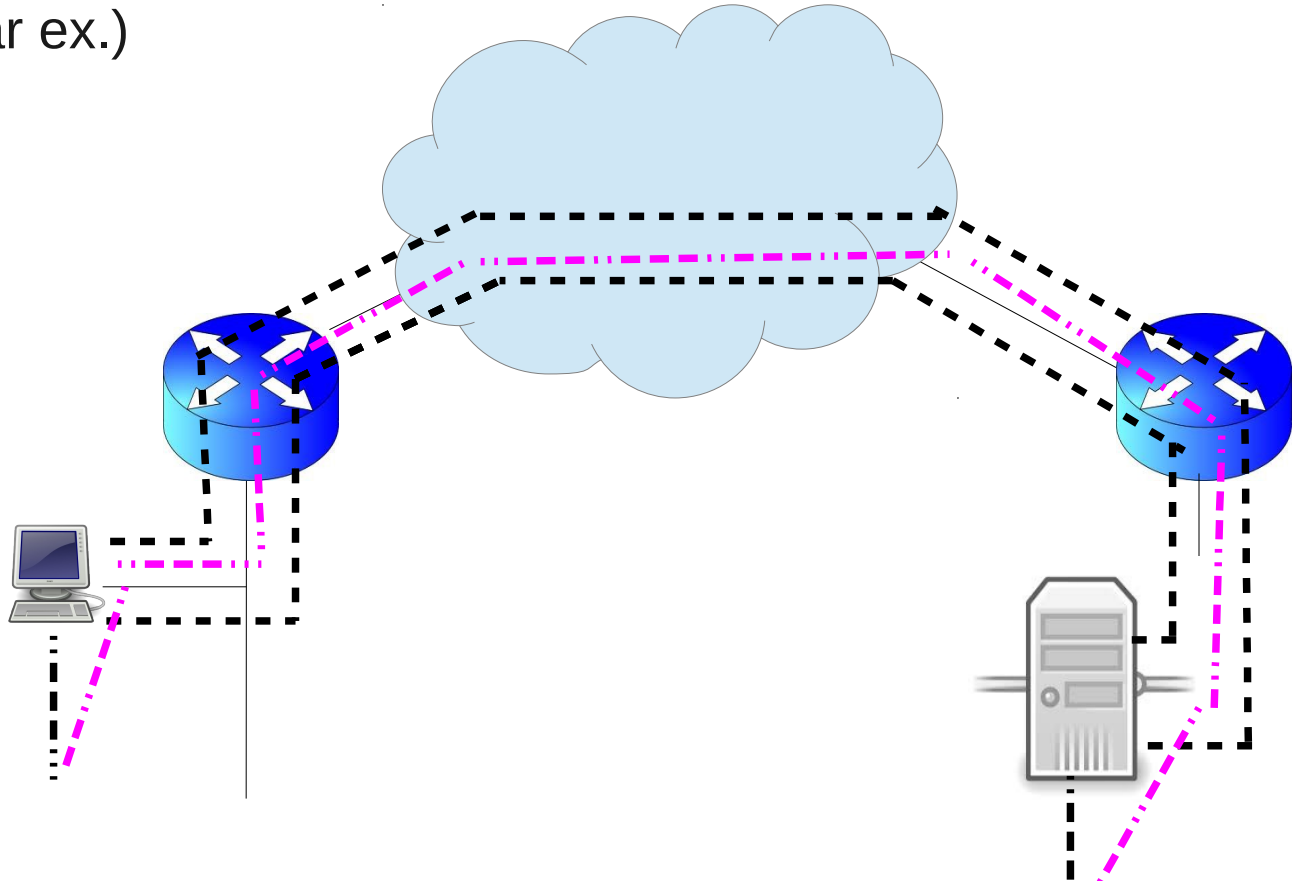
OpenVPN : mode routé (tun)

- en mode routé, une adresse ip est associée à chaque interface virtuelle
- la communication entre serveur et client se fait donc via IP

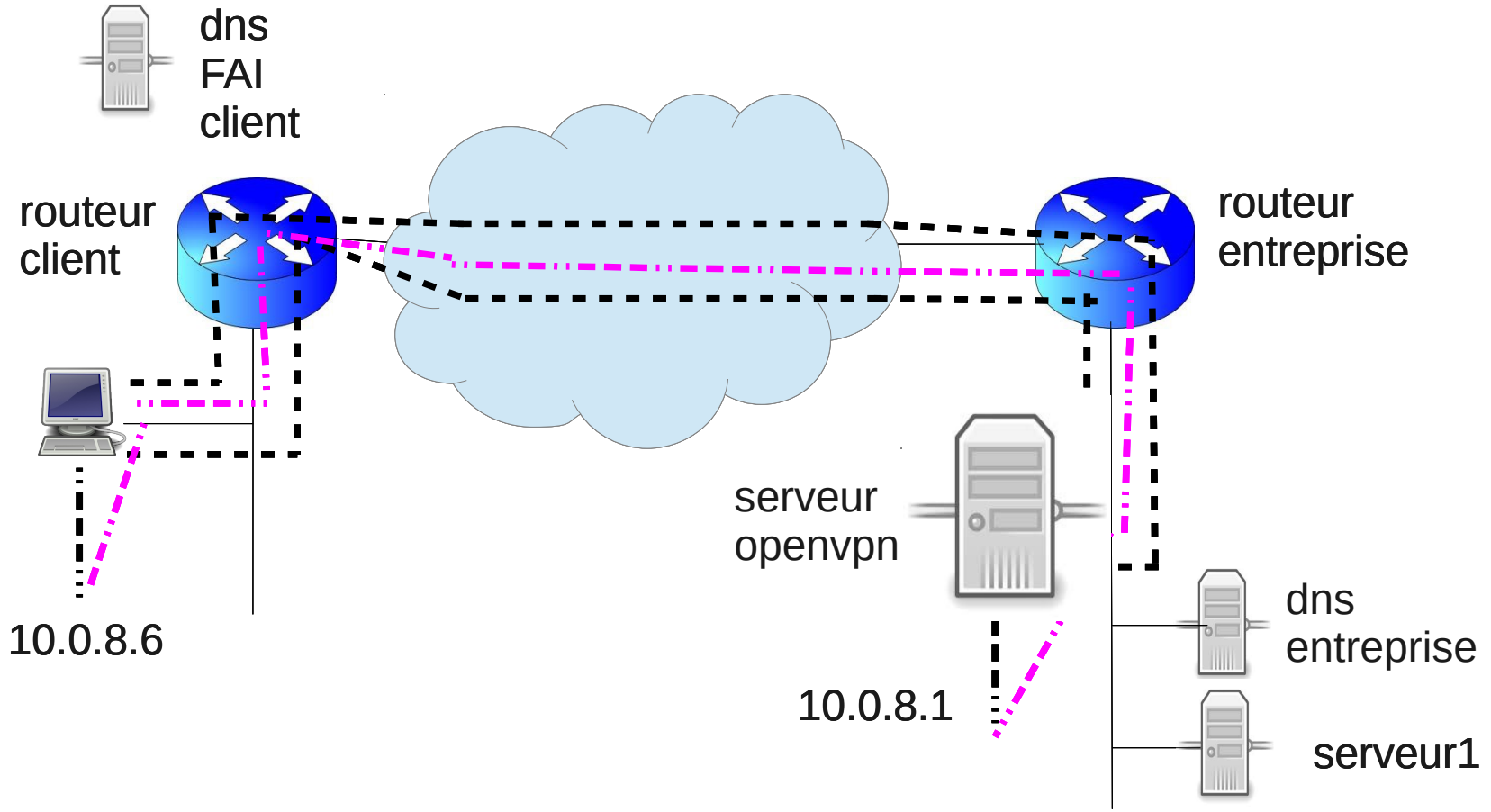


OpenVPN : mode bridge (tap)

- en mode tap, un pont ethernet est crée entre l'interface virtuelle et le réseau local
- on travail au niveau de la couche 2
- les protocoles autres qu'ip sont utilisables
- les messages diffusés passent dans le tunnel (possibilité d'utiliser un serveur dhcp distant par ex.)



Quelques études de cas en mode routé (tun)



Quelques études de cas en mode routé (tun)

- quelques uns des points posant soucis
  - pour que le vpn existe, le poste client doit passer par routeur client pour accèder au serveur vpn (i.-e. : les paquets du tunnel ne doivent pas passer par le tunnel)
  - pour l'instant, le vpn fournit une connexion point à point entre les deux interfaces virtuelles
  - pour utiliser les ressources du FAI, le client doit utiliser le dns FAI et passer par le routeur FAI
  - pour utiliser les ressources internes de l'entreprise, le client doit passer par le VPN et avoir des routes ad hoc le permettant
  - pour identifier les postes de l'entreprise, le client doit utiliser le dns de l'entreprise

openvpn/tun : accès à des serveurs internes de l'entreprise

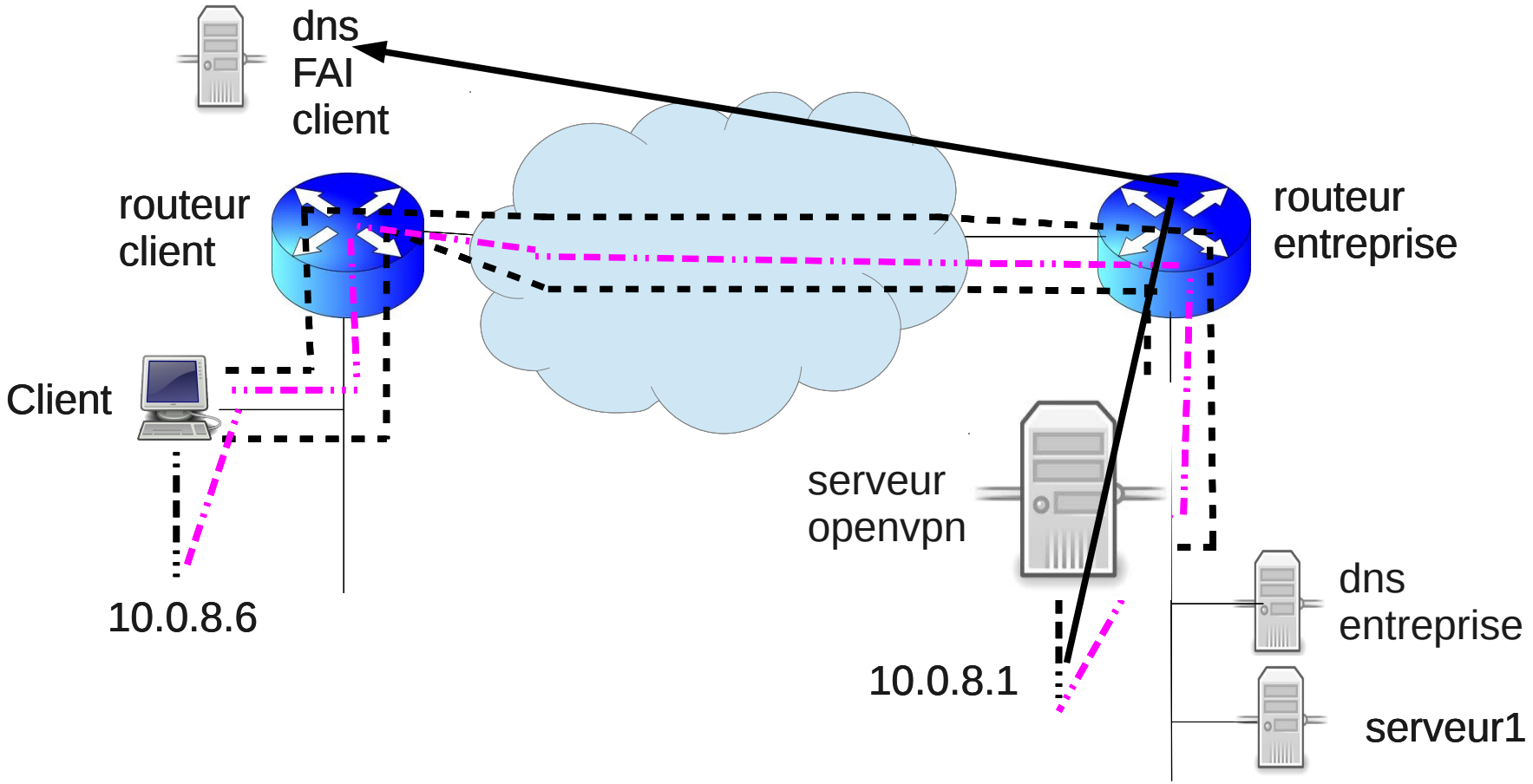
- il faut ajouter une route vers le réseau interne de l'entreprise
  - si le réseau interne de l'entreprise est le 192.168.10.0/24,
  - sur le client :
    - route add -net 192.168.10.0 netmask 255.255.255.0 gw 10.0.8.1
  - le dns utilisé est toujours celui du FAI
  - le trafic autre que vers l'entreprise passe par le FAI

openvpn/tun : accès à internet par l'entreprise

- on va utiliser l'entreprise pour router tous les paquets SAUF ceux nécessaires à la mise en œuvre du tunnel
  - créer un route statique d'hôte pour joindre le serveur openvpn :
    - route add -host *IPserveuropenvpn* gw *IProuteurClient*
  - *indiquer que le routeur par défaut est le serveur openvpn :*
    - *route add default gw 10.0.8.1*
- *tout le trafic passe par l'entreprise SAUF celui à destination du serveur openvpn*
- *Problème : le dns du FAI refuse nos requêtes car les requêtes lui viennent de l'entreprise et pas du client :*
  - *voir schéma page suivante*
  - *la requête suit le chemin rose pointillé puis noir gras*
  - *solution : définir le dns de l'entreprise comme dns pour le poste client.*
- *avec cette solution, tout se passe comme si le poste client était dans l'entreprise*

openvpn/tun : accès à internet par l'entreprisee

- *la requête dns du client suivait le trait rose puis le trait épais noir : refus du dns du FAI*



openvpn/tun : routage

- *en pratique, si on demande à openvpn de configurer lui-même le vpn comme route par défaut, nous obtenons une table de routage de la forme suivante :*

```
$ netstat -rn
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic   MSS Fenêtre irtt Iface
0.0.0.0         192.168.20.1     0.0.0.0         UG        0 0          0 wlan0
0.0.0.0         10.8.0.5        128.0.0.0       UG        0 0          0 tun0
128.0.0.0       10.8.0.5        128.0.0.0       UG        0 0          0 tun0
192.168.20.0     0.0.0.0         255.255.255.0   U         0 0          0 wlan0
10.8.0.1        10.8.0.5        255.255.255.255 UGH       0 0          0 tun0
10.8.0.5        0.0.0.0         255.255.255.255 UH        0 0          0 tun0
195.221.159.140 192.168.20.1     255.255.255.255 UGH       0 0          0 wlan0
```

Les lignes 2 et 3 sont une astuce : à elles deux, elles équivalent à la ligne 1 et grâce à leur masque, elles sont prioritaires par rapport à elle et définissent donc le routeur par défaut

Tant qu'elles sont là, la ligne 1 ne sert à rien.

Quand openvpn s'arrêté, il lui suffit de supprimer les lignes 2 et 3 pour revenir à l'état initial. Il supprime aussi les ligne 5 à 7.

Cette astuce permet à openvpn d'éviter de sauver le routeur par défaut.

La ligne 7 garantit que les paquets à destination du serveur openvpn ne passeront pas par le vpn.

VPN : l'exemple d'openvpn

initiation à la notion de VPN via OpenVPN

VPN ?

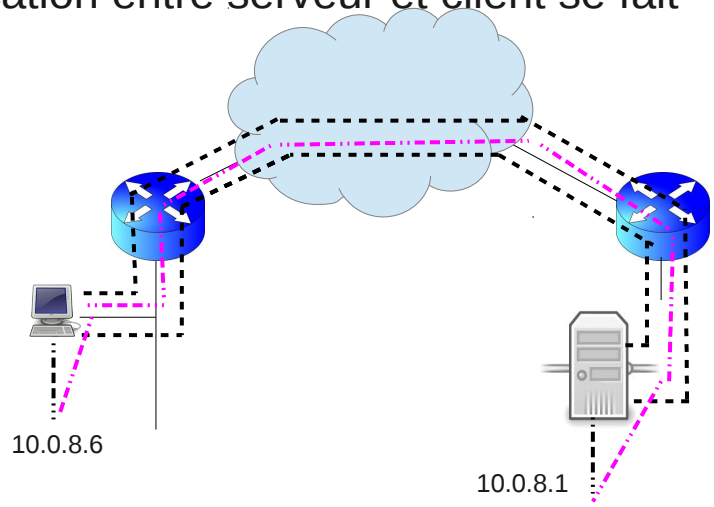
- VPN : Virtual Private Network
- Réseau privé virtuel
  - créer un réseau privé au dessus d'un réseau public
  - permet de faire croire à des machines distantes ou à des réseaux distants qu'ils sont sur le même réseau
  - chiffrement : interdit toute interception de trafic sur le réseau public
  - cas typiques d'utilisation :
    - permettre à une machine nomade de se connecter aux ressources de l'entreprise
    - relier 2 réseaux distants pour n'en faire virtuellement qu'un seul

OpenVPN

- opensource
- multiplateforme
- de nombreux modes d'authentification (dont certificats, mot de passe, …)
- s'appuie sur SSL
- le VPN consiste à créer une interface réseau virtuelle sur le client et sur le serveur

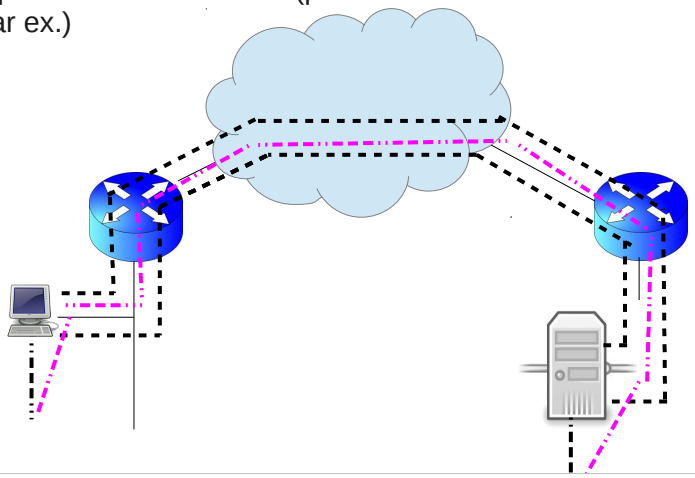
OpenVPN : mode routé (tun)

- en mode routé, une adresse ip est associée à chaque interface virtuelle
- la communication entre serveur et client se fait donc via IP

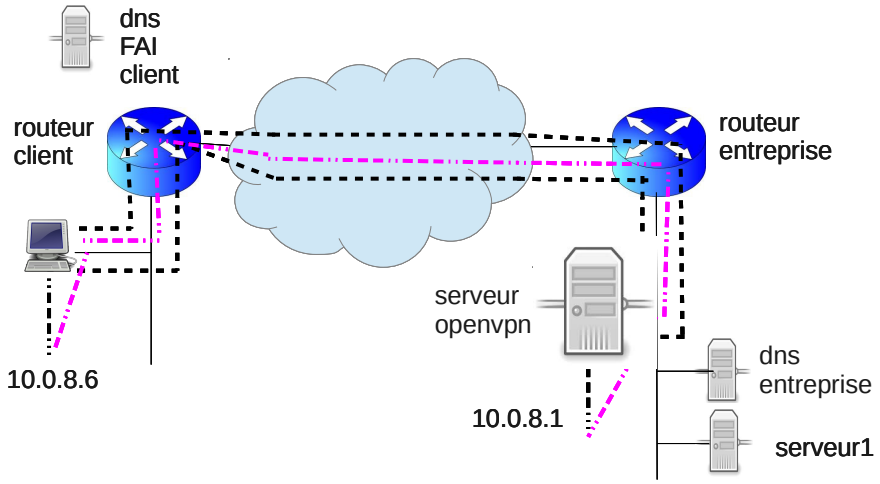


OpenVPN : mode bridge (tap)

- en mode tap, un pont ethernet est crée entre l'interface virtuelle et le réseau local
- on travail au niveau de la couche 2
- les protocoles autres qu'ip sont utilisables
- les messages diffusés passent dans le tunnel (possibilité d'utiliser un serveur dhcp distant par ex.)



Quelques études de cas en mode routé (tun)



Quelques études de cas en mode routé (tun)

- quelques uns des points posant soucis
  - pour que le vpn existe, le poste client doit passer par routeur client pour accèder au serveur vpn (i.-e. : les paquets du tunnel ne doivent pas passer par le tunnel)
  - pour l'instant, le vpn fournit une connexion point à point entre les deux interfaces virtuelles
  - pour utiliser les ressources du FAI, le client doit utiliser le dns FAI et passer par le routeur FAI
  - pour utiliser les ressources internes de l'entreprise, le client doit passer par le VPN et avoir des routes ad hoc le permettant
  - pour identifier les postes de l'entreprise, le client doit utiliser le dns de l'entreprise

openvpn/tun : accès à des serveurs internes de l'entreprise

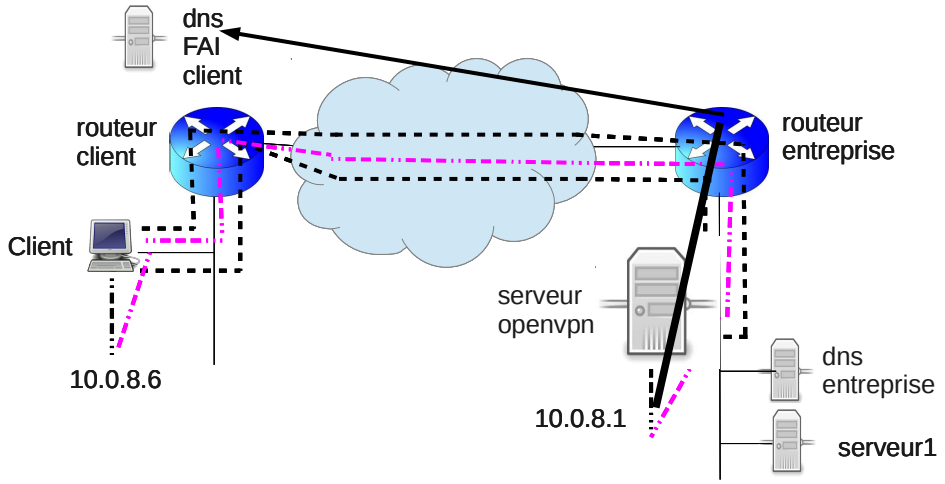
- il faut ajouter une route vers le réseau interne de l'entreprise
  - si le réseau interne de l'entreprise est le 192.168.10.0/24,
  - sur le client :
    - route add -net 192.168.10.0 netmask 255.255.255.0 gw 10.0.8.1
  - le dns utilisé est toujours celui du FAI
  - le trafic autre que vers l'entreprise passe par le FAI

openvpn/tun : accès à internet par l'entreprise

- on va utiliser l'entreprise pour router tous les paquets SAUF ceux nécessaires à la mise en œuvre du tunnel
  - créer un route statique d'hôte pour joindre le serveur openvpn :
    - route add -host *IPserveuropenvpn* gw *IProuteurClient*
  - *indiquer que le routeur par défaut est le serveur openvpn :*
    - *route add default gw 10.0.8.1*
- *tout le trafic passe par l'entreprise SAUF celui à destination du serveur openvpn*
- *Problème : le dns du FAI refuse nos requêtes car les requêtes lui viennent de l'entreprise et pas du client :*
  - *voir schéma page suivante*
  - *la requête suit le chemin rose pointillé puis noir gras*
  - *solution : définir le dns de l'entreprise comme dns pour le poste client.*
- *avec cette solution, tout se passe comme si le poste client était dans l'entreprise*

openvpn/tun : accès à internet par l'entreprisee

- *la requête dns du client suivait le trait rose puis le trait épais noir : refus du dns du FAI*



openvpn/tun : routage

- *en pratique, si on demande à openvpn de configurer lui-même le vpn comme route par défaut, nous obtenons une table de routage de la forme suivante :*

```
$ netstat -rn
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic   MSS Fenêtre irtt Iface
0.0.0.0         192.168.20.1     0.0.0.0         UG        0 0          0 wlan0
0.0.0.0         10.8.0.5        128.0.0.0       UG        0 0          0 tun0
128.0.0.0       10.8.0.5        128.0.0.0       UG        0 0          0 tun0
192.168.20.0     0.0.0.0         255.255.255.0   U         0 0          0 wlan0
10.8.0.1        10.8.0.5        255.255.255.255 UGH       0 0          0 tun0
10.8.0.5        0.0.0.0         255.255.255.255 UH        0 0          0 tun0
195.221.159.140 192.168.20.1     255.255.255.255 UGH       0 0          0 wlan0
```

Les lignes 2 et 3 sont une astuce : à elles deux, elles équivalent à la ligne 1 et grâce à leur masque, elles sont prioritaires par rapport à elle et définissent donc le routeur par défaut

Tant qu'elles sont là, la ligne 1 ne sert à rien.

Quand openvpn s'arrêté, il lui suffit de supprimer les lignes 2 et 3 pour revenir à l'état initial. Il supprime aussi les ligne 5 à 7.

Cette astuce permet à openvpn d'éviter de sauver le routeur par défaut.

La ligne 7 garantit que les paquets à destination du serveur openvpn ne passeront pas par le vpn.