VPN avec OpenVPN

et OpenVPN-NL

Matthieu Herrb

9 octobre 2018

OpenVPN

https://openvpn.net/

- solution libre,
- multi-platformes (Windows, Linux, *BSD, MacOS X, Android),
- utilise OpenSSL pour la cryptographie,
- implémentation sécurisée (réduction des privilèges, chroot, ...),
- fonctionne en mode TUN (routage) ou TAP (pont),
- scriptable + interface de management,

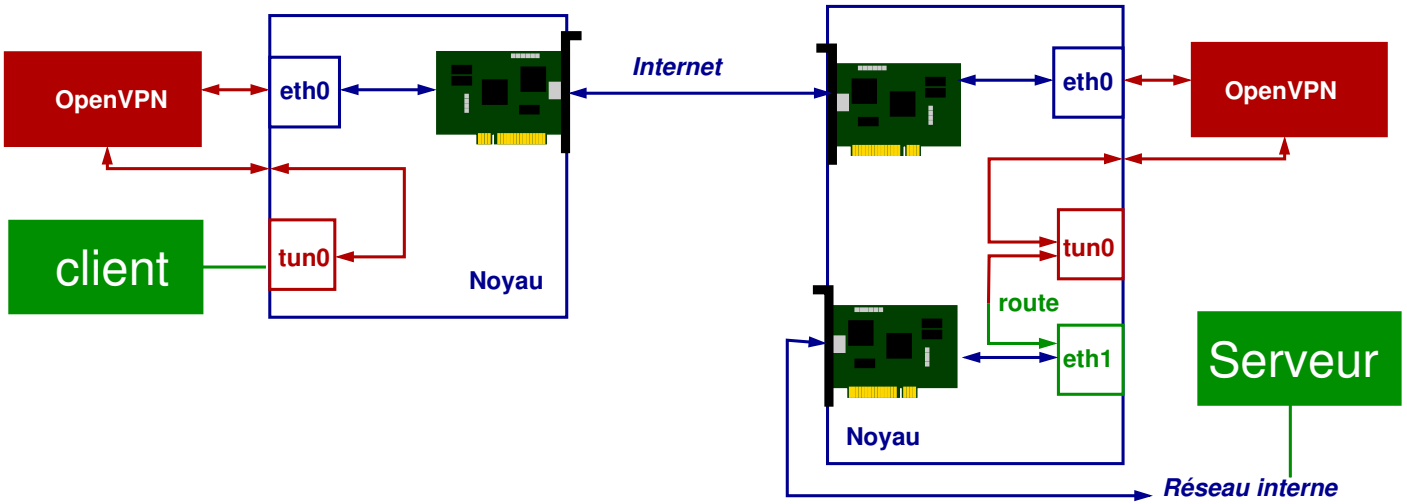
OpenVPN-nl:

- https://openvpn.fox-it.com/index.html
- version durcie développée pour le gouvernement néerlandais.
- certifié par la NS-NCSA (équivalent NL de l'ANSSI)

OpenVPN : fonctionnalités

- Mode point à point ou client/serveur,
- Authentification mutuelle par certificats,
- Scripts pluggables lors de chaque étape (connexion, authentification, vérification certificat, déconnexion...),
- Le serveur peut se comporter comme un serveur DHCP pour envoyer des infos (DNS, routeur par défaut) aux clients,
- Possibilité de 'push' de commandes de configuration vers les clients,
- interface de contrôle (socket) pour créer des interfaces utilisateur,
- Adapte le MTU automatiquement,
- Passe le NAT.

Serveur OpenVPN routeur



eth0 adresse IP externe

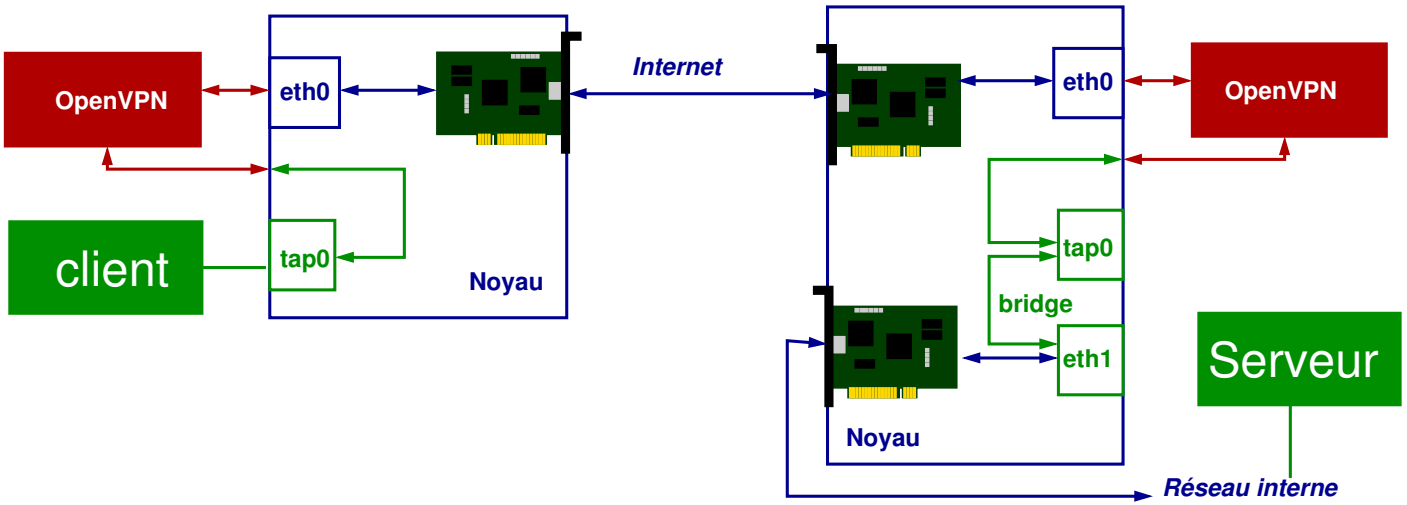
tun0 adresse IP interconnexion

eth0 adresse IP externe

tun0 adresse IP interconnexion

eth1 adresse IP interne

Serveur OpenVPN pont



eth0 adresse IP externe

tap0 adresse IP interne

eth0 adresse IP externe

tap0 adresse IP interne

eth1 adresse IP interne

Routeur ou pont ?

Bridge :

- un seul réseau IP,
- les broadcast sont diffusés dans le VPN - rend possible l'utilisation de protocoles tels que NetBIOS ou NIS,
- fonctionne avec tous les protocoles au dessus d'ethernet (IPX, AppleTalk,...
- simplifie les contrôles d'accès basés sur adresses IP,
- pas de routage à configurer.

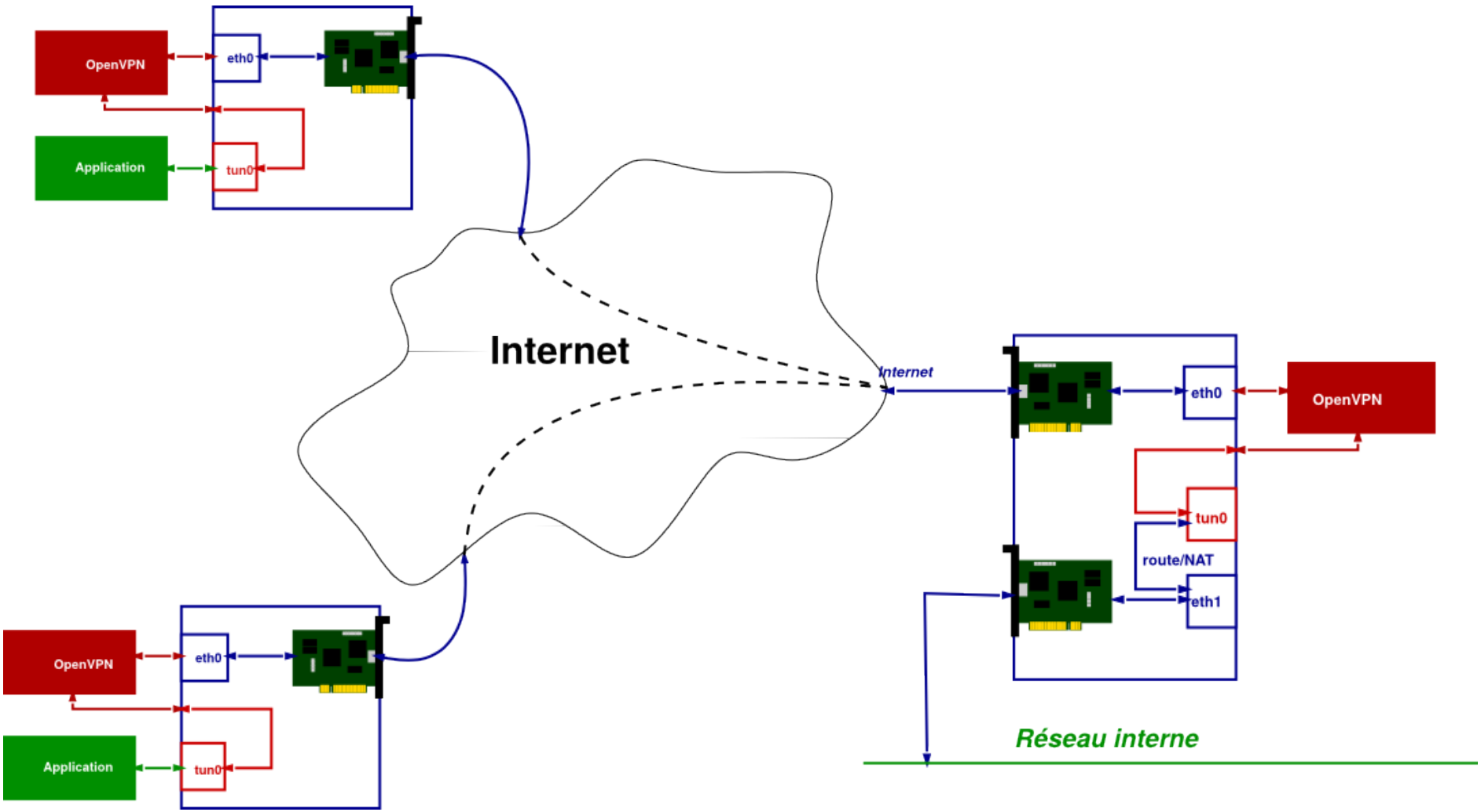
Mais :

- moins efficace que le routage,
- ne s'adapte pas à l'échelle de très nombreux clients.

Dans les 2 cas, il vaut mieux que le serveur VPN soit aussi routeur.

Scénario - connexion de postes nomades

Mode routeur.



Utilisation de Easy-RSA pour générer les certificats

https://github.com/OpenVPN/easy-rsa

1. générer un certificat racine auto-signé
2. générer le certificat du serveur
3. générer un certificat pour chaque client

Distribuer aux clients :

- un fichier de configuration
- leur certificat client

serveur

```
tls-server
port 1194
proto udp
dev tun
ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh /etc/openvpn/dh2028.pem
crl-verify /etc/openvpn/server.crl
topology subnet
server 10.8.0.0 255.255.255.0
user openvpn
group openvpn
plugin /usr/lib64/openvpn/plugin/lib/openvpn-auth-ldap.so \
    /etc/openvpn/auth/ldap.conf
username-as-common-name
```

client

```
tls-client
dev tun
proto udp
remote vpn.labo.cnrs.fr
port 1194
remote-cert-tls server
resolv-retry infinite
ca ca.crt
key client.key
cert client.crt
cipher AES-256-GCM
auth SHA256
auth-user-pass
pull
verb 3
```

→ importable dans les interfaces graphiques coté client:

- MacOS : TunnelBlick
- Linux : Network Manager
- Windows : client OpenVPN

Points durs

- Nécessite de pouvoir passer du trafic UDP sur le port 1194
  Normalement autorisé sur Eduroam et équivalents
  - ou bien TCP dans TCP...
- Sécurisation des postes clients...
- Politique de routage sur les postes clients ?
  - tout le trafic dans le VPN ?
  - seulement le trafic vers le réseau du laboratoire ?
- Attention IPv6 : si config VPN v4 seulement,
  le trafic IPv6 passe en dehors...
- Expiration/révocation/renouvellement des certificats...
  - $\rightarrow$ authentification LDAP ou Radius en complément

Wireguard

https://www.wireguard.com/

- Nouvelle technologie de VPN en mode noyaux Linux
- Algorithmes de chiffrement modernes
- Meilleures performances qu'OpenVPN
- Existe aussi une implémentation en mode utilisateur pour clients *BSD, MacOS, Windows, Android
- Configuration plutôt simple
- Mais pas encore largement diffusé / analysé.

Conclusion

- Solution d'accès distants sécurisée
  - pour utilisateurs nomades / télétravail
  - pour multi-sites
- Évite d'exposer aux Internets des applications pas sécurisées
- Ligne de défense supplémentaire pour applications critiques
- Permet un genre d'authentification 2 facteurs
- Faire attention aux politiques de routage du trafic