

# Configuration OpenVPN sécurisée Serveur & Client Windows

Projet réalisé dans le cadre de la société  
Poly-Tech Engineering SA

Esteban BARRACHO

20 juin 2025



# Vue d'ensemble

Ce document décrit la configuration d'un VPN sécurisé avec OpenVPN, depuis le serveur (Windows) jusqu'à la connexion client. Le système repose sur des certificats uniques, une whitelist des utilisateurs autorisés, et un chiffrement fort.

# 1 Serveur VPN (Windows)

## 1. Installation

- Télécharger OpenVPN Community : <https://openvpn.net/community-downloads/>
- Installer avec l'option "Install as a service" cochée.

## 2. Initialisation Easy-RSA

```
1 cd "C:\Program Files\OpenVPN\easy-rsa"  
2 xcopy .\ "C:\OpenVPN-CA" /E /I  
3 cd C:\OpenVPN-CA  
4 EasyRSA-Start.bat
```

## 3. Génération des certificats

```
1 ./easyrsa init-pki  
2 ./easyrsa build-ca nopass  
3 ./easyrsa gen-req server nopass  
4 ./easyrsa sign-req server server  
5 ./easyrsa gen-dh  
6 ./easyrsa gen-crl  
7 ./easyrsa gen-req client1 nopass  
8 ./easyrsa sign-req client client1  
9 openvpn --genkey --secret ta.key
```

## 4. Copier vers le dossier config

- ca.crt, server.crt, server.key, dh.pem, ta.key, crl.pem → C:Files

## 5. Fichier server.ovpn

```
1 port 1194  
2 proto udp  
3 dev tun  
4 ca ca.crt  
5 cert server.crt  
6 key server.key  
7 dh dh.pem  
8 crl-verify crl.pem  
9 tls-auth ta.key 0  
10 cipher AES-256-CBC  
11 auth SHA256  
12 tls-version-min 1.2  
13 tls-cipher TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384  
14 server 10.8.0.0 255.255.255.0  
15 verify-client-cert require  
16 username-as-common-name  
17 client-connect "C:\\Program Files\\OpenVPN\\scripts\\check_cn.bat"  
18 keepalive 10 120  
19 persist-key  
20 persist-tun  
21 verb 3
```

## 6. Script de vérification de CN (whitelist)

check\_cn.bat :

```
1 @echo off
2 setlocal
3 set "CN=%common_name%"
4 findstr /x /c:"%CN%" "C:\Program Files\OpenVPN\config\allowed-clients.txt" >nul
5 if errorlevel 1 (
6     echo %date% %time% Rejet : %CN% >> C:\Program Files\OpenVPN\log\rejected.log
7     exit 1
8 )
9 exit 0
```

## 7. Whitelist allowed-clients.txt

```
1 MarcelH
2 VicentPirnay
```

## 8. Pare-feu Windows

```
1 netsh advfirewall firewall add rule name="OpenVPN UDP" dir=in action=allow protocol
   =UDP localport=1194
```

## 2 Client VPN (Windows)

### 1. Installer OpenVPN

- Télécharger OpenVPN GUI sur le site officiel
- Lancer en tant qu'administrateur

### 3. Exemple de fichier client1.ovpn

```
1 client
2 dev tun
3 proto udp
4 remote vpn.polybase.be 1194
5 resolv-retry infinite
6 nobind
7 persist-key
8 persist-tun
9 remote-cert-tls server
10 tls-auth ta.key 1
11 cipher AES-256-CBC
12 auth SHA256
13 verb 3
14
15 <ca>
16 # contenu de ca.crt
17 </ca>
18 <cert>
19 # contenu de client1.crt
20 </cert>
21 <key>
22 # contenu de client1.key
23 </key>
24 <tls-auth>
25 # contenu de ta.key
26 </tls-auth>
```

### 4. Connexion VPN

1. Lancer “OpenVPN GUI” avec clic droit → Exécuter en tant qu’administrateur
2. Clic droit sur l’icône dans la barre de tâches → “Connecter”
3. Si le CN (Common Name) est accepté et le certificat valide, la connexion s’établit.

## Conclusion

Ce VPN offre une sécurité de niveau entreprise avec :

- contrôle d'accès par certificat signé,
- filtrage par nom (whitelist),
- cryptographie forte,
- audit des connexions refusées.

Il garantit que seules les personnes explicitement autorisées peuvent établir une communication sécurisée avec le serveur.

---

© 2025 Esteban BARRACHO.

Ce document est distribué selon les termes de la licence Creative Commons CC BY-ND (Attribution - Pas de Modification).

This work is licensed under a Creative Commons “Attribution-NoDerivatives 4.0 International” license.

