# Hướng dẫn cài đặt & sử dụng VPN Client-to-Site (OpenVPN) dành cho người dùng cuối

> Tài liệu dành cho **người dùng cuối (VPN user)** có gateway loại **OpenVPN**: khách hàng cần kết nối từ máy tính cá nhân vào VPC private network được bảo vệ bởi **FPT Cloud Native Firewall**.
>
> Nếu gateway của bạn là **IPsec**, hãy dùng tài liệu "VPN Client-to-Site (IPsec)" riêng.
>
> File cấu hình `.ovpn` được quản trị viên hệ thống cấp cho bạn trên **FPT Cloud Portal** (mỗi user một file riêng).

---

## 0. Mục đích sử dụng

Dịch vụ **VPN Client-to-Site (C2S)** cho phép máy tính của bạn (ở nhà, quán cafe, hoặc mạng ngoài) kết nối an toàn vào **VPC private network** được bảo vệ bởi FPT Cloud Native Firewall. Sau khi kết nối:

- Bạn truy cập được các tài nguyên nội bộ (server, database, VM, private subnet) của tổ chức từ xa, như đang ngồi trong văn phòng.
- Mọi traffic giữa máy bạn và firewall đều được mã hóa đầu cuối bằng **OpenVPN (UDP + TLS-crypt)**.
- Chế độ định tuyến (**split** hoặc **full**) do quản trị viên quyết định phía server; bạn không cần cấu hình thêm:
  - **split** (tương ứng `Split Tunnel` trên Portal): chỉ traffic tới các subnet nội bộ cụ thể mới đi qua VPN. Mọi traffic khác (Internet, web thông thường) đi đường cũ.
  - **full** (tương ứng `Full Tunnel` trên Portal): toàn bộ traffic Internet và nội bộ đều đi qua VPN. Máy bạn dùng DNS/server bên trong tổ chức.
- Một firewall có thể chạy **nhiều VPN gateway song song**; mỗi gateway có tên riêng (`vpn_gateway_name`) mà bạn thấy trên Portal. Bạn chỉ dùng 1 gateway tại một thời điểm.

OpenVPN dùng chứng chỉ người dùng (client cert + key) nhúng sẵn trong file `.ovpn` profile; mỗi user 1 file riêng. Không cần username/password (xác thực dựa trên TLS). Toàn bộ CA/cert/key/tls-crypt đã nằm trong `.ovpn`, không cần cấu hình thêm.

---

## 1. Trước khi bắt đầu

### 1.1 Bắt đầu từ đâu (chọn đúng mục để làm theo)

1. **Xác nhận gateway của bạn là OpenVPN.** Xem trên Portal (trang chi tiết gateway, mục VPN Type). Gateway OpenVPN có nút "Download .ovpn" ở tab Users. Nếu gateway là IPsec (có nút "Download Client Config Script (.sh)"), hãy dùng tài liệu IPsec riêng.
2. **Máy bạn chạy hệ điều hành nào?** Chọn mục tương ứng:

| Hệ điều hành | Làm theo mục |
|---|---|
| Ubuntu / Debian | §2 |
| Windows 10 / 11 | §3 |

## 1.2 Quy ước ký hiệu trong tài liệu

- Phần đặt trong dấu ngoặc nhọn như `<vpn_gateway_name>` là **chỗ bạn phải thay bằng giá trị thật** của mình (lấy từ Portal), và **bỏ luôn dấu** `< >`.
  - Ví dụ: tài liệu ghi `/etc/openvpn/client/<vpn_gateway_name>.ovpn`; nếu gateway của bạn tên `gw-58f160f9` thì đường dẫn là `/etc/openvpn/client/gw-58f160f9.ovpn`.
- Trong các khối lệnh, dòng bắt đầu bằng `#` là **chú thích giải thích**, không cần gõ.
- Các IP và tên gateway ví dụ (vd `192.168.45.1`, `gw-58f160f9`) chỉ là minh họa; luôn dùng giá trị Portal cấp cho bạn.

## 1.3 Mở cửa sổ dòng lệnh đúng quyền

- **Ubuntu / Debian (mở Terminal):** nhấn `Ctrl + Alt + T`, hoặc tìm "Terminal" trong danh sách ứng dụng.
- **Windows (mở PowerShell quyền Administrator):** bấm nút Start, gõ `PowerShell`, bấm chuột phải vào **Windows PowerShell**, chọn **Run as administrator**, rồi bấm **Yes** ở hộp thoại UAC.

> **Lưu ý về `sudo` (Ubuntu/Debian):** lần đầu chạy một lệnh có `sudo`, máy sẽ hỏi **mật khẩu đăng nhập máy tính của bạn**. Khi gõ mật khẩu này, màn hình không hiện ký tự nào là bình thường; cứ gõ xong rồi Enter.

## 1.4 Thông tin cần lấy từ Portal

Đăng nhập **FPT Cloud Portal**, mở trang chi tiết VPN gateway, vào tab **Users** để tải file `.ovpn` của bạn:

| Thông tin | Loại | Phục vụ cho |
|---|---|---|
| `vpn_gateway_name` | Tên gateway (vd `gw-58f160f9`) | Dùng để đặt tên file và ghi chú |
| `vpn_server_endpoint` | IP public của firewall (vd `100.72.253.70`) | Đã nhúng sẵn trong file `.ovpn`, bạn không cần gõ |
| `vpn_listen_port` | UDP port (vd `1194`, `1195`...) | Đã nhúng sẵn trong file `.ovpn` |
| File `client.ovpn` | OpenVPN profile (mỗi user 1 file riêng, đã nhúng CA + client cert + key + tls-crypt) | Tải từ nút "Download .ovpn" ở tab Users |

> **Lưu ý bảo mật:** file `.ovpn` chứa chứng chỉ riêng của bạn, không chia sẻ cho người khác. OpenVPN **không dùng username/password**, nên không cần nhớ mật khẩu VPN. Khi cần cấp lại chứng chỉ, nhờ quản trị viên trên Portal rồi tải lại file `.ovpn` mới.

---

## 2. Hướng dẫn sử dụng trên Ubuntu / Debian

### 2.1 Yêu cầu

- Ubuntu 20.04+ hoặc Debian 11+ (x86_64).
- Quyền `sudo`.
- Có Internet để cài `openvpn` (apt).
- Đã tải từ Portal: **file** `client.ovpn` (mỗi user 1 file, có nhúng CA cert + client cert + key + tls-crypt). Không cần username/password vì profile đã có cert của bạn.

### 2.2 Cài đặt

**Bước 1. Cài OpenVPN client** (nếu chưa có):

```
sudo apt update
sudo apt install -y openvpn
```

Kiểm tra:

```
openvpn --version
# In ra OpenVPN 2.5+ → OK
```

**Bước 2. Đặt file `.ovpn` vào vị trí chuẩn** (tuỳ chọn nhưng khuyến nghị):

```
sudo mkdir -p /etc/openvpn/client
sudo cp ~/Downloads/client.ovpn /etc/openvpn/client/<vpn_gateway_name>.ovpn
```

(Hoặc giữ tại `~/Downloads/client.ovpn` cũng được vì `.ovpn` là self-contained.)

### 2.3 Kiểm tra cài đặt thành công

```
# Kiểm tra file có nhúng CA cert + client cert
grep -c "<ca>\|<cert>\|<key>\|<tls-crypt>" /etc/openvpn/client/<vpn_gateway_name>.ovpn
# Phải in ra ≥3 (CA + cert + key). Nếu có tls-crypt thì = 4.

# Dry-run test profile (không connect, chỉ check cú pháp)
sudo openvpn --config /etc/openvpn/client/<vpn_gateway_name>.ovpn --test-crypto
# Hoặc nếu không dùng --test-crypto:
sudo openvpn --config /etc/openvpn/client/<vpn_gateway_name>.ovpn --verb 4 --daemon --writepid
        /tmp/ovpn.pid; sleep 2; sudo kill $(cat /tmp/ovpn.pid)
# Nếu log không báo lỗi cú pháp → profile OK
```

## 2.4 Cách dùng

**Kết nối (chạy foreground để xem log):**

```
sudo openvpn --config /etc/openvpn/client/<vpn_gateway_name>.ovpn
```

Khi thấy dòng `Initialization Sequence Completed` là tunnel đã up. Giữ terminal mở. (Nhấn `Ctrl+C` để ngắt.)

**Kết nối chạy nền (background):**

```
# Dùng systemd @.service của openvpn
sudo cp /etc/openvpn/client/<vpn_gateway_name>.ovpn /etc/openvpn/<vpn_gateway_name>.conf
sudo systemctl start openvpn@<vpn_gateway_name>
sudo systemctl status openvpn@<vpn_gateway_name>
# Bật auto-start sau reboot:
sudo systemctl enable openvpn@<vpn_gateway_name>
```

> Lưu ý: tên service là `openvpn@<prefix>` với prefix là tên file `.conf` (bỏ đuôi `.conf`). Vd file `/etc/openvpn/gw-58f160f9.conf` -> service `openvpn@gw-58f160f9`.

**Kiểm tra tunnel đang hoạt động:**

```
# Xem interface tun
ip addr show | grep -E "tun[0-9]+"
# Thấy interface tun0 (hoặc tun1 ...) với IP từ VPN pool → đã kết nối

# Hoặc xem bảng route, thấy route qua tun
ip route | grep tun
```

**Ping thử máy chủ nội bộ:**

```
ping -c 3 192.168.45.1
```

**Ngắt kết nối:**

- Foreground (terminal đang mở): `Ctrl + C`.
- Background systemd:

  ```
  sudo systemctl stop openvpn@<vpn_gateway_name>
  # (Tắt auto-start nếu không dùng nữa: sudo systemctl disable openvpn@<vpn_gateway_name>)
  ```

**Xem log khi gặp lỗi:**

- Foreground: log in ra terminal.
- systemd: `sudo journalctl -u openvpn@<vpn_gateway_name> -f`.
- Lỗi thường gặp: port bị chặn, hoặc firewall mạng của bạn chặn UDP 1194/1195. Thử đổi mạng khác, hoặc liên hệ quản trị viên để chạy OpenVPN qua TCP.

**Cập nhật khi quản trị viên cấp lại cert/key:**

Tải file `.ovpn` mới (đã nhúng cert mới) từ Portal, ghi đè lên `/etc/openvpn/client/<vpn_gateway_name>.ovpn`, rồi restart service hoặc chạy lại lệnh foreground. Không cần đổi username/password (OpenVPN dùng cert, không dùng username).

**Gỡ profile** (khi quản trị viên deprovision gateway):

```
sudo systemctl stop openvpn@<vpn_gateway_name>
sudo systemctl disable openvpn@<vpn_gateway_name>
sudo rm /etc/openvpn/<vpn_gateway_name>.conf /etc/openvpn/client/<vpn_gateway_name>.ovpn
sudo apt remove openvpn  # (tuỳ chọn, nếu không dùng openvpn nữa)
```

---

## 3. Hướng dẫn sử dụng trên Windows 10 / 11

Windows không có OpenVPN client native. Cách đơn giản nhất: tải **OpenVPN Connect** (ứng dụng chính thức của OpenVPN), import file `.ovpn` Portal cấp, rồi bấm connect. Toàn bộ CA/cert/key/tls-crypt đã nhúng trong `.ovpn`, không cần cấu hình thêm.

### 3.1 Yêu cầu

- Windows 10 hoặc 11 (x64).
- Quyền Administrator để cài OpenVPN Connect.
- Đã tải từ Portal: file **`client.ovpn`** (mỗi user 1 file, có nhúng cert). Không cần username/password.

### 3.2 Cài đặt

**Bước 1. Cài OpenVPN Connect:**

1. Tải installer từ https://openvpn.net/vpn-client/, chọn "OpenVPN Connect for Windows".
2. Chạy installer `.exe` (UAC prompt, bấm cho phép), Next, Install, Finish.
3. Mặc định installer đã bật "Launch on Windows startup" và icon ở system tray (góc dưới phải).

**Bước 2. Import profile `.ovpn`:**

Cách dễ nhất là kéo thả:

1. Mở **OpenVPN Connect** (Start menu hoặc icon system tray).
2. Kéo file `client.ovpn` (tải từ Portal) thẳng vào cửa sổ OpenVPN Connect.

3. Profile mới xuất hiện trong danh sách với tên = `vpn_gateway_name` (lấy từ comment trong file). Không cần đổi gì thêm.

Hoặc import qua giao diện:

1. Mở OpenVPN Connect, vào tab **PROFILE**, bấm **+ (Add new profile)**.
2. Chọn file `client.ovpn`, bấm **Open**.
3. Profile xuất hiện trong danh sách.

## 3.3 Kiểm tra cài đặt thành công

- Mở OpenVPN Connect, thấy tên profile (vd `gw-58f160f9`) trong tab **PROFILE** với trạng thái `Disconnected` (xám) là đã import xong, sẵn sàng connect.

## 3.4 Cách dùng

**Kết nối:**

1. Mở OpenVPN Connect.
2. Click profile VPN, gạt công tắc sang **ON**.
3. Trạng thái chuyển `Connecting` (vàng xoay) rồi `Connected` (xanh lá) trong vài giây. Icon system tray OpenVPN đổi sang **màu xanh lá**.

**Kiểm tra kết nối thành công:**

- Icon system tray xanh lá là đã kết nối.
- Hoặc ping thử máy chủ nội bộ:

  ```
  ping 192.168.45.1
  ```

  Có reply là tunnel OK.

**Ngắt kết nối:**

- Gạt công tắc trên profile sang **OFF**, trạng thái chuyển `Disconnected`.
- Hoặc icon system tray, click "Disconnect" trong menu.

**Đổi cert/key khi quản trị viên cấp lại:**

1. Tải file `.ovpn` mới từ Portal (đã nhúng cert mới).
2. OpenVPN Connect > PROFILE > trỏ vào profile > **More (⋮)** > **Delete**.
3. Kéo thả file `.ovpn` mới vào OpenVPN Connect, rồi Connect lại.

> Không cần username/password vì OpenVPN xác thực bằng client cert trong `.ovpn`.

**Gỡ profile và ứng dụng:**

- Gỡ profile: OpenVPN Connect > PROFILE > ⋮ > Delete.
- Gỡ app: Settings > Apps > OpenVPN Connect > Uninstall.

---

## 4. Xác định chế độ tunnel (split/full) đang hoạt động

> **Mục nâng cao (tùy chọn):** chỉ cần đọc nếu bạn muốn biết traffic nào đang đi qua VPN. Để dùng VPN cơ bản (kết nối và truy cập tài nguyên nội bộ), bạn có thể bỏ qua mục này.

Chế độ tunnel **do quản trị viên quyết định phía server** (cấu hình trên Portal). Bạn không cần (và không nên) cấu hình chế độ trên máy; server OpenVPN sẽ đẩy route phù hợp khi tunnel thiết lập.

Khi đã connect tunnel và muốn biết đang ở chế độ nào, dùng 1 trong các cách dưới đây.

### 4.1 Cách nhanh: Ping test

Tunnel đang UP, mở terminal/Command Prompt:

```
# Ubuntu/Debian
traceroute -n 8.8.8.8 | head -3

# Windows
tracert -d 8.8.8.8
# (chỉ 3 hop đầu: tracert -d -h 3 8.8.8.8)
```

> Trên Ubuntu/Debian, nếu báo "command not found", cài bằng `sudo apt install -y traceroute` (hoặc dùng `tracepath 8.8.8.8` thường có sẵn).

- **Hop đầu là IP VPN pool** (vd `10.100.0.1` của VPN gateway, hiển thị trong `ip addr show tun0`): **full mode**, toàn bộ traffic Internet và nội bộ đều đi qua VPN.
- **Hop đầu là router/gateway nhà bạn** (vd `192.168.1.1` hoặc `10.0.0.1` như trước khi bật VPN): **split mode**, chỉ traffic tới các subnet nội bộ mới đi VPN, Internet đi đường cũ.

Kết hợp ping:

```
ping -c 3 <ip_subnet_noi_bo>   # vd 192.168.45.1, phải REPLY trong cả 2 mode
ping -c 3 8.8.8.8              # full: REPLY qua VPN; split: vẫn REPLY nhưng đi đường Internet
        cũ
```

### 4.2 Kiểm tra bảng route

```
# Ubuntu/Debian
ip route | grep -E "tun|default"
# Full mode: 'default dev tun0' (default route qua tunnel)
# Split mode: '<subnet> dev tun0' (chỉ subnet nội bộ qua tunnel), default route qua eth0/wlan0
        cũ
```

```
# Windows
route print -4 | findstr /R "0.0.0.0/0.*tun  0.0.0.0/0.*TAP  0.0.0.0/0.*Wintun"
# Có dòng = full mode (default route qua VPN adapter)
# Không có dòng = split mode

# Xem tất cả route qua VPN adapter
route print | findstr /R "192.168  10.  172.16  172.17  172.18  172.19"
# (các subnet nội bộ chỉ đi qua VPN trong cả 2 mode)
```

### 4.3 Khi quản trị viên đổi chế độ trên Portal

Khi quản trị viên đổi chế độ (split sang full hoặc ngược lại) trên Portal, server áp dụng vào `push-route` / `replace-default-route`. Phía bạn cần **ngắt và kết nối lại** tunnel (bảng route phía client chỉ áp dụng khi tunnel up). Sau khi connect lại, kiểm tra như §4.2.

> **Quan trọng:** Bạn không cần cấu hình gì ở client để "đổi chế độ". Chỉ cần "reconnect" tunnel để client nhận lại route mới từ server.

---

## 5. FAQ: Các câu hỏi thường gặp

### Q1: Làm sao xác nhận gateway của tôi là OpenVPN?

Xem trên Portal: trang chi tiết VPN gateway hiển thị loại VPN (VPN Type). Gateway OpenVPN có nút "Download .ovpn" ở tab Users. Nếu màn chi tiết có nút "Download Client Config Script (.sh)" thì gateway là IPsec, hãy dùng tài liệu IPsec riêng.

### Q2: Chế độ split/full từ đâu mà biết? Lệnh kiểm tra thế nào?

Chế độ do quản trị viên quyết định trên Portal (cấu hình phía server). Bạn không cần cấu hình trên máy. Để xác định chế độ đang chạy, xem §4. Xác định chế độ tunnel (split/full) đang hoạt động, có hướng dẫn `traceroute` và `ip route`.

### Q3: Reboot xong tunnel có tự kết nối lại không?

- **Ubuntu/Debian**: có thể bật auto-start qua systemd (`sudo systemctl enable openvpn@<gw>`).
- **Windows**: OpenVPN Connect > Preferences > bật "Auto-connect on launch", và cài OpenVPN Connect tự chạy cùng Windows.

### Q4: Đổi hoặc cấp lại chứng chỉ thế nào?

OpenVPN không có password; chứng chỉ nằm trong file `.ovpn`. Để cấp lại chứng chỉ, nhờ quản trị viên trên Portal rồi tải lại file `.ovpn` mới, sau đó import/ghi đè profile như hướng dẫn ở §2.4 (Ubuntu) hoặc §3.4 (Windows).

### Q5: Dùng nhiều VPN gateway song song trên cùng một máy?

Mỗi gateway có 1 file `.ovpn` riêng, có thể import nhiều profile vào OpenVPN Connect, nhưng chỉ connect 1 profile tại một thời điểm.

### Q6: Gỡ hoàn toàn sau khi quản trị viên deprovision gateway

Tham khảo phần "Gỡ profile" (Ubuntu, §2.4) và "Gỡ profile và ứng dụng" (Windows, §3.4). Nên đợi quản trị viên xác nhận deprovision xong rồi mới gỡ; nếu gỡ sớm, cấu hình phía server vẫn còn mà máy bạn không kết nối được.

---

## 6. Thông tin hỗ trợ

Nếu gặp lỗi không xử lý được sau khi thử FAQ, reboot và re-import profile, hãy liên hệ quản trị viên hệ thống kèm theo:

- `vpn_gateway_name`, `vpn_server_endpoint`, hệ điều hành và phiên bản.
- Log OpenVPN: `sudo journalctl -u openvpn@<gw> -n 200` (Ubuntu) hoặc trình xem log của OpenVPN Connect (Windows).
- Lần cuối kết nối thành công, và các thay đổi gần đây trên hệ thống (firewall, antivirus, mạng công ty...).