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

> Tài liệu dành cho **người dùng cuối (VPN user)** có gateway loại **IPsec**: 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 **OpenVPN**, hãy dùng tài liệu "VPN Client-to-Site (OpenVPN)" riêng.
>
> Các thông tin kết nối (tên gateway, endpoint, tài khoản, file cấu hình) được quản trị viên hệ thống cấp cho bạn trên **FPT Cloud Portal**.

---

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 **IPsec (IKEv2 + EAP-MSCHAPv2)**.
- 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.

IPsec là giao thức VPN chuẩn IETF. Windows 10/11 có sẵn adapter IKEv2 native (không cần cài phần mềm bên thứ 3). Ubuntu/Debian cài `strongswan` qua script tự động.

---

1. Trước khi bắt đầu

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

1. **Xác nhận gateway của bạn là IPsec.** Xem trên Portal (trang chi tiết gateway, mục VPN Type). Gateway IPsec có nút "Download Client Config Script (.sh)" ở màn chi tiết. Nếu gateway là OpenVPN, hãy dùng tài liệu OpenVPN 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>`, `<username>` là **chỗ bạn phải thay bằng giá trị thật** của mình (lấy từ Portal), và **bỏ luôn dấu** `< >`.
  - Ví dụ: tài liệu ghi `sudo <vpn_gateway_name> up`; nếu gateway của bạn tên `gw-58f160f9` thì bạn gõ: `sudo gw-58f160f9 up`.
- Trong các khối lệnh, dòng bắt đầu bằng `#` là **chú thích giải thích**, không cần gõ.
- Các IP và tên gateway ví dụ (vd `100.72.253.70`, `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** (không phải username/password VPN). 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** và mở trang chi tiết của VPN gateway được cấp. Tại đó có các thông tin sau:

Thông tin	Loại	Phục vụ cho
`vpn_gateway_name`	Tên gateway (vd `gw-58f160f9`)	Xác định profile và lệnh điều khiển
`vpn_server_endpoint`	IP public của firewall (vd `100.72.253.70`)	Windows nhập vào profile; Ubuntu đã nhúng sẵn vào file cấu hình
`vpn_listen_port`	UDP port (`500` và `4500`)	Đã nhúng sẵn vào cấu hình
`username`	Tên đăng nhập VPN do quản trị viên tạo trên Portal	Cần khi cài đặt và kết nối
`password`	Mật khẩu VPN (cấp 1 lần trên Portal)	Cần khi cài đặt và kết nối
File `vpn_client_to_site.sh`	Script cài đặt (dùng cho Ubuntu/Debian)	Tải từ nút "Download Client Config Script (.sh)"
File `<vpn_gateway_name>.crt`	CA Certificate (dùng cho Windows)	Tải từ nút "Download CA Certificate (.crt)"

> **Lưu ý bảo mật:** `username` và `password` chỉ dành cho bạn. Không chia sẻ qua Slack/Email công khai. Khi cần đổi mật khẩu, nhờ quản trị viên cấp lại thông tin đăng nhập trên Portal, hoặc tự đổi bằng lệnh `rotate` ở §2 (Ubuntu/Debian).

---

2. Hướng dẫn sử dụng trên Ubuntu / Debian

2.1 Yêu cầu

- Hệ điều hành: **Ubuntu 20.04/22.04/24.04 LTS** hoặc **Debian 11/12** (x86_64).
- Quyền `sudo` trên máy.
- Có Internet để script cài `strongswan` + `libcharon-extra-plugins` + `libstrongswan-extra-plugins` qua apt.
- Đã tải từ Portal: file `vpn_client_to_site.sh` và ghi nhớ `username`, `password`.
- (Tuỳ chọn) Cài `ca-certificates` + `curl` + `openssh-client`; thường đã có sẵn.

2.2 Cài đặt

Di chuyển tới thư mục chứa file tải về (vd `~/Downloads`):

```
cd ~/Downloads
```

Bước 1. Cấp quyền thực thi cho script (chỉ làm 1 lần):

```
chmod +x vpn_client_to_site.sh
```

Bước 2. Chạy script với sudo (script là wizard tương tác, sẽ hỏi username/password):

```
sudo ./vpn_client_to_site.sh
```

Script sẽ:

1. Tự kiểm tra và cài `strongswan` cùng các plugin nếu thiếu.
2. Hỏi bạn **Username** (hiện khi gõ): nhập username Portal đã cấp.
3. Hỏi bạn **Password** (không hiện khi gõ): nhập password đã cấp rồi Enter.
4. Ghi CA cert vào `/etc/ipsec.d/cacerts/<vpn_gateway_name>.crt` (CA đã nhúng sẵn trong script, không cần tải thêm).
5. Ghi cấu hình VPN vào `/etc/ipsec.d/<vpn_gateway_name>.conf` và `/etc/ipsec.secrets`.
6. Khởi động daemon `charon` và test kết nối 1 lần (up, kiểm tra ESTABLISHED, rồi down).
7. Cài **lệnh kết nối nhanh** tại `/usr/local/bin/<vpn_gateway_name>`: đây là lệnh chính bạn sẽ dùng về sau.
8. In thông báo "Success!". Khi thấy "Success!" kèm tóm tắt các thông số là bạn đã cài xong.

Ví dụ output khi thành công (tóm tắt):

```
[8.5/9] Installing reconnect + control shortcut at /usr/local/bin/gw-58f160f9 ...
[9/9] Done.
Success! VPN client config installed for:
  VPN Gateway     : gw-58f160f9
  Connection name : vpn-client-to-site_gw-58f160f9
  Public endpoint : 100.72.253.70
  Username        : vpnuser01
   ...
```

2.3 Kiểm tra cài đặt thành công

Dùng 1 trong các cách sau:

```
# Cách 1: Kiểm tra lệnh kết nối nhanh đã được cài
ls -l /usr/local/bin/<vpn_gateway_name>
# Vd: ls -l /usr/local/bin/gw-58f160f9  →  -rwxr-xr-x 1 root root ... /usr/local/bin/gw-
        58f160f9

# Cách 2: Xem trạng thái kết nối (lần đầu sẽ là "down" vì script test xong tự down)
sudo <vpn_gateway_name> status
# Kết quả dạng:
#   vpn-client-to-site_gw-58f160f9(1): IKE_SA ... not found
#   (tức chưa up; vẫn OK, daemon đã sẵn sàng)

# Cách 3: Kiểm tra CA cert và file conf đã có
ls -l /etc/ipsec.d/cacerts/<vpn_gateway_name>.crt
ls -l /etc/ipsec.d/<vpn_gateway_name>.conf
```

Nếu các file đều tồn tại và `status` chạy không lỗi, cài đặt đã thành công.

2.4 Cách dùng

Sau khi cài, daemon `charon` đang chạy (sẽ tự chạy lại sau reboot nếu `strongswan-starter` được enable; nếu không, xem phần khắc phục ở cuối).

Kết nối lên VPN (lệnh mặc định, có thể bỏ `up`):

```
sudo <vpn_gateway_name>            # = 'up' nếu không có tham số
sudo <vpn_gateway_name> up         # tường minh
```

Ví dụ:

```
sudo gw-58f160f9 up
```

Kết quả thành công dạng:

```
establishing connection 'vpn-client-to-site_gw-58f160f9' ...
connection 'vpn-client-to-site_gw-58f160f9' established successfully
```

Kiểm tra trạng thái tunnel:

```
sudo <vpn_gateway_name> status
# Hoặc:
sudo ipsec status vpn-client-to-site_<vpn_gateway_name>
```

Tìm dòng `ESTABLISHED` và `INSTALLED`: tức SA đã tạo xong, traffic đang đi qua tunnel.

Ping thử một máy chủ trong VPC private network (quản trị viên cho bạn IP, vd `192.168.45.1`):

```
ping -c 3 192.168.45.1
```

Nếu có reply thì tunnel hoạt động. Ở `split` mode: chỉ các subnet đã khai báo reply được; ping Internet (`8.8.8.8`) vẫn đi đường bình thường. Ở `full` mode: cả `8.8.8.8` cũng đi qua tunnel.

Ngắt kết nối:

```
sudo <vpn_gateway_name> down
```

Khắc phục sau reboot nếu tunnel không tự up:

Daemon `charon` thường không auto-start kèm tunnel. Sau reboot, chạy:

```
sudo <vpn_gateway_name> start     # đảm bảo daemon chạy + reload config
sudo <vpn_gateway_name> up        # bật tunnel
```

Đổi username/password không cần chạy lại script (khi quản trị viên cấp lại thông tin đăng nhập):

```
sudo <vpn_gateway_name> rotate
# Wizard hỏi username + password mới, tự cập nhật /etc/ipsec.secrets + conf
# Nếu tunnel đang UP thì down + up lại để áp dụng:
sudo <vpn_gateway_name> down && sudo <vpn_gateway_name> up
```

Xem trợ giúp (tất cả sub-command):

```
sudo <vpn_gateway_name> -h
```

Bảng tổng hợp sub-command:

Lệnh	Tác dụng
`sudo <gw>`	mặc định = `up`
`sudo <gw> up`	kết nối tunnel lên
`sudo <gw> down`	ngắt tunnel
`sudo <gw> status`	xem trạng thái kết nối
`sudo <gw> start`	start daemon + reload config (không up tunnel), dùng sau reboot hoặc khi chỉnh tay
`sudo <gw> rotate`	đổi username/password qua wizard, không cần chạy lại file .sh
`sudo <gw> -h`	hiển thị trợ giúp

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

```
sudo rm /etc/ipsec.d/<vpn_gateway_name>.conf /etc/ipsec.d/cacerts/<vpn_gateway_name>.crt
        /usr/local/bin/<vpn_gateway_name>
sudo sed -i '/^<username> *:/d' /etc/ipsec.secrets
sudo ipsec rereadall && sudo ipsec reload
```

---

3. Hướng dẫn sử dụng trên Windows 10 / 11

Windows có sẵn IKEv2 VPN client native, bạn không cần cài thêm phần mềm VPN bên thứ 3. Cần 2 thứ từ Portal: **file CA cert** `.crt` và thông tin `username` / `password` / `vpn_server_endpoint`.

3.1 Yêu cầu

- Windows 10 (build 1903+) hoặc Windows 11.
- Quyền Administrator để import CA và tạo VPN profile.
- Đã tải từ Portal: `<vpn_gateway_name>.crt` (CA Certificate) và ghi nhớ `username`, `password`, `vpn_server_endpoint` (vd `100.72.253.70`).

3.2 Cài đặt

Bước 1. Import CA Certificate vào Trusted Root (để Windows xác minh server cert):

1. Nhấp đúp vào file `<vpn_gateway_name>.crt` để mở hộp thoại Certificate.
2. Bấm **Install Certificate...**.
3. Chọn **Local Machine** (UAC prompt xuất hiện, bấm cho phép).
4. Bấm Next, chọn **"Place all certificates in the following store"**, bấm **Browse...**.
5. Chọn **Trusted Root Certification Authorities**, bấm OK, Next, **Finish**.
6. Hộp thoại "The import was successful" xuất hiện là CA đã cài.

> Cách nhanh hơn: chạy `certutil -addstore -f "Root" "<vpn_gateway_name>.crt"` trong PowerShell (Administrator).

Bước 2. Tạo VPN profile:

1. Mở **Settings** (`Win + I`).
2. Chọn **Network & Internet** > **VPN** (menu bên trái).
3. Bấm **"Add a VPN connection"** (nút + ở đầu trang).
4. Điền các trường như sau:

Trường	Giá trị điền
VPN provider	`Windows (built-in)`
Connection name	tên dễ nhớ, vd `FPT Cloud VPN C2S gw-58f160f9`
Server name or address	`vpn_server_endpoint` Portal cấp (vd `100.72.253.70`)
VPN type	`IKEv2`
Type of sign-in info	`User name and password`
User name (optional)	`username` Portal cấp (vd `vpnuser01`)
Password (optional)	`password` Portal cấp
Remember my sign-in info	`On` (tích)

5. Bấm **Save**.

3.3 Kiểm tra cài đặt thành công

1. Mở **Settings** > **Network & Internet** > **VPN**.
2. Thấy VPN `FPT Cloud VPN C2S gw-58f160f9` xuất hiện trong danh sách là OK.

Hoặc qua PowerShell:

```
Get-VpnConnection -Name "FPT Cloud VPN C2S gw-58f160f9"
# In ra Name, ServerAddress, TunnelType=IKEv2, ... → đã có profile
```

3.4 Cách dùng

Kết nối:

- Cách 1. Click chuột: **Settings** > **VPN** > click VPN vừa tạo > bấm **Connect**.
- Cách 2. System tray: click icon mạng góc dưới phải > click VPN > chọn VPN > bấm **Connect**.
- Cách 3. Rasphone: `Win + R` > `rasphone` > chọn VPN > **Connect**.
- Cách 4. PowerShell (Administrator):

  ```
  rasdial "FPT Cloud VPN C2S gw-58f160f9" <username> <password>
  ```

Kiểm tra kết nối thành công:

```
Get-VpnConnection -Name "FPT Cloud VPN C2S gw-58f160f9"
# ConnectionStatus phải là "Connected"
ipconfig | findstr "IKEv2"
# Thấy adapter "IKEv2 FPT Cloud VPN C2S ..." + có IP cấp từ VPN pool (vd 10.100.0.x)
```

Hoặc ping thử máy chủ nội bộ VPC:

```
ping 192.168.45.1
```

Có reply là tunnel OK.

Ngắt kết nối:

- Click chuột: Settings > VPN > chọn VPN > **Disconnect**.
- PowerShell: `rasdial "FPT Cloud VPN C2S gw-58f160f9" /disconnect`

Đổi password (khi quản trị viên cấp lại thông tin đăng nhập):

- Settings > VPN > chọn VPN > **Advanced options** > **Edit** > nhập lại username/password mới > Save.

- Hoặc đơn giản nhất: sửa lại password trong form ở Bước 3.2.

Gỡ VPN profile:

- Settings > VPN > chọn VPN > **Remove** > confirm.
- PowerShell: `Remove-VpnConnection -Name "FPT Cloud VPN C2S gw-58f160f9" -Force`

Gỡ CA cert (khi quản trị viên deprovision gateway):

```
# Tìm CA theo CN trong Trusted Root:
Get-ChildItem Cert:\LocalMachine\Root | Where-Object { $_.Subject -like "*FSP*OSP*vpn_ca*" }
# Gỡ:
Get-ChildItem Cert:\LocalMachine\Root | Where-Object { $_.Subject -like "*<subject CA>" } |
        Remove-Item
```

---

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 IPsec sẽ tự quyết định Traffic Selector khi thiết lập kết nối.

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 `sudo <gw> status`): **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 Xem Traffic Selector (TSr) trên Ubuntu/Debian

```
sudo <vpn_gateway_name> status
# Hoặc:
sudo ipsec status vpn-client-to-site_<vpn_gateway_name>
```

Tìm dòng `TS=` trong phần CHILD_SA:

- `TSr={ 0.0.0.0/0 ... }`: **full mode** (server báo catch-all).
- `TSr={ <danh sách CIDR subnet nội bộ> }` (vd `192.168.45.0/24 172.16.10.0/24`): **split mode** (server chỉ cho phép các subnet đó).

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 tự áp dụng chế độ mới. Phía bạn cần **`sudo <gw> down`** **rồi** **`sudo <gw> up`** (hoặc đợi IKE_SA rekey tự nhiên khoảng 1h) để CHILD_SA mới được thiết lập với TSr mới. Sau khi up 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 TSr mới từ server.

---

5. FAQ: Các câu hỏi thường gặp

Q1: Làm sao xác nhận gateway của tôi là IPsec?

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

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

- **Ubuntu/Debian**: không tự up. Cần `sudo <gw> start && sudo <gw> up`.
- **Windows**: VPN profile không auto-connect mặc định. Settings > VPN > chọn VPN > "Advanced options" > bật "Connect automatically".

Q4: Quên password hoặc muốn đổi password?

- Ubuntu/Debian: chạy `sudo <gw> rotate`, wizard hỏi username + password mới rồi tự cập nhật và reload.
- Windows: sửa password trong form Settings > VPN.
- Trường hợp mất/lộ mật khẩu: nhờ quản trị viên cấp lại thông tin đăng nhập trên Portal, rồi bạn nhập lại.

Q5: Log Ubuntu báo "TS_UNACCEPTABLE"

CA và server endpoint có thể đã đúng nhưng chế độ chưa khớp. Hãy thử `sudo <gw> rotate` để nhập lại thông tin đăng nhập, hoặc liên hệ quản trị viên kiểm tra chế độ tunnel đang cấu hình.

Q6: Dùng nhiều VPN gateway song song trên cùng một máy?

Mỗi gateway có `vpn_gateway_name` riêng nên script cài lệnh riêng tại `/usr/local/bin/<gw_name>`. Về lý thuyết chạy được nhiều tunnel song song, nhưng **không khuyến nghị** vì dễ xung đột route.

Q7: Gỡ hoàn toàn sau khi quản trị viên deprovision gateway

Tham khảo phần "Gỡ profile VPN" (Ubuntu, §2.4) và "Gỡ VPN profile / Gỡ CA cert" (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 cài lại, hãy liên hệ quản trị viên hệ thống kèm theo:

- `vpn_gateway_name`, `vpn_server_endpoint`, hệ điều hành và phiên bản.
- Output `sudo <gw> status` (Ubuntu) hoặc `Get-VpnConnection` (Windows).
- Lần cuối kết nối thành công, và các thay đổi gần đây trên hệ thống (firewall, antivirus, mạng công ty...).