

SenPos VPN Gateway

Hướng dẫn thao tác từng bước cho quản trị viên, Operator và người dùng VPN.

Phiên bản 1.0 · Cập nhật 09/10/2026 · Gateway [IP]

Ảnh web lấy từ giao diện gateway, qua bản hiển thị chỉ đọc để tránh thao tác nhầm trên production. Số đỏ trên ảnh tương ứng với các bước hoặc vị trí được giải thích ngay bên dưới. Không có mật khẩu, private key hay nội dung profile trong tài liệu.

/guide/

Mục lục

01. Tổng quan và chuẩn bị
02. Đăng nhập web
03. Quyền Admin và Operator
04. Dashboard, trạng thái client và traffic
05. Tạo client VPN mới
06. Tải profile và revoke client
07. Cài và kết nối OpenVPN trên Windows
08. Cài và kết nối OpenVPN trên iPhone
09. Kiểm tra kết nối tới mạng nội bộ
10. Quản lý route trên Linux
11. Quản lý NAT và xem firewall
12. Bổ sung một mạng nội bộ mới
13. Restart dịch vụ OpenVPN
14. Tạo tài khoản Operator
15. Đổi mật khẩu đăng nhập web
16. Backup cấu hình
17. Restore cấu hình từ backup
18. Tra cứu lịch sử audit
19. Xử lý lỗi thường gặp

01. Tổng quan và chuẩn bị

Hệ thống gồm Linux chạy OpenVPN và định tuyến/NAT, web .NET để quản trị, Nginx trong Docker cung cấp HTTPS, và ứng dụng OpenVPN Connect trên thiết bị người dùng.
VPN client Linux gateway Các mạng nội bộ

Thông tin	Giá trị hiện tại
Web quản trị và tài liệu	https://[IP] và /guide/
Địa chỉ VPN từ bên ngoài	[IP] : 1194, giao thức UDP
IP cấp cho VPN client	[IP]; gateway tunnel [IP]
Gateway LAN / interface	[IP] / enx68e43b3088bf
Internet của client	Giữ đường đi Wi-Fi/4G/5G hiện tại; chỉ các mạng nội bộ được push qua VPN.
Xác thực VPN hiện tại	Certificate và private key riêng, được đóng gói trong file .ovpn.

1. Quản trị viên chuẩn bị tài khoản web phù hợp; người dùng VPN nhận file .ovpn riêng qua kênh an toàn.
2. Người dùng ở ngoài công ty lấy profile và tài liệu trước. IP web [IP] chỉ truy cập được khi đang ở LAN phù hợp hoặc sau khi VPN đã kết nối.
3. Kiểm tra router phía công ty chuyển tiếp **UDP 1194** từ IP public về [IP]. Không mở trực tiếp backend port 5080 ra Internet.
4. Khi trình duyệt báo chứng chỉ HTTPS không tin cậy, xác minh đúng gateway với Admin và dùng chứng chỉ/CA được đơn vị tin cậy. Không bỏ qua cảnh báo trên địa chỉ không rõ nguồn gốc.

Hai loại tài khoản không phải một
Admin/Operator dùng đăng nhập web. Hiện VPN dùng certificate trong profile, không dùng mật khẩu Admin/Operator. Xác thực VPN bằng username/password chỉ mới được thảo luận, chưa triển khai. File MSI là bộ cài Windows, không cài lên iPhone.

02. Đăng nhập web

Admin / Operator

SenPos VPN Gateway

Đăng nhập quản trị

Tài khoản

1

Mật khẩu

2

Đăng nhập

3

4

OpenVPN Connect 3.9.0
Windows · Bộ cài MSI

Hướng dẫn sử dụng
Quản trị gateway · Kết nối VPN

Hình 1. Trang login. Vị trí 1-3 là đăng nhập; vị trí 4 là tải bộ cài Windows, không cần đăng nhập.

1. Mở [https://\[IP\]/Account/Login](https://[IP]/Account/Login), nhập **Tài khoản** được Admin cấp tại vị trí 1.
2. Nhập **Mật khẩu** của tài khoản web tại vị trí 2. Không có mật khẩu mặc định công khai trong tài liệu này.
3. Bấm **Đăng nhập** tại vị trí 3. Thành công sẽ vào Dashboard; sai thông tin sẽ có thông báo ngay trên form.
4. Để cài client Windows, bấm **OpenVPN Connect 3.9.0** tại vị trí 4. Để đọc tài liệu này, bấm **Hướng dẫn sử dụng** bên dưới link bộ cài.

Kết quả đúng

Thanh trên cùng hiển thị role Admin hoặc Operator. Khi dùng xong, bấm biểu tượng đăng xuất trên thanh này.

03. Quyền Admin và Operator

Chức năng	Admin	Operator	Người dùng VPN thông thường
Xem Dashboard, route/NAT, client, audit	Có	Có	Không cần tài khoản web
Tạo client mới	Có	Có, không nhận lại client đã tồn tại	Nhờ Admin/Operator cấp
Tải profile	Client certificate còn hợp lệ	Chỉ client do mình tạo, theo cấu hình hiện tại	Nhận file riêng từ người cấp
Revoke client, sửa route/NAT, restart OpenVPN	Có	Không	Không
Web Users, Backup/Restore	Có	Không	Không
Đổi mật khẩu web của chính mình	Có	Có	Không áp dụng

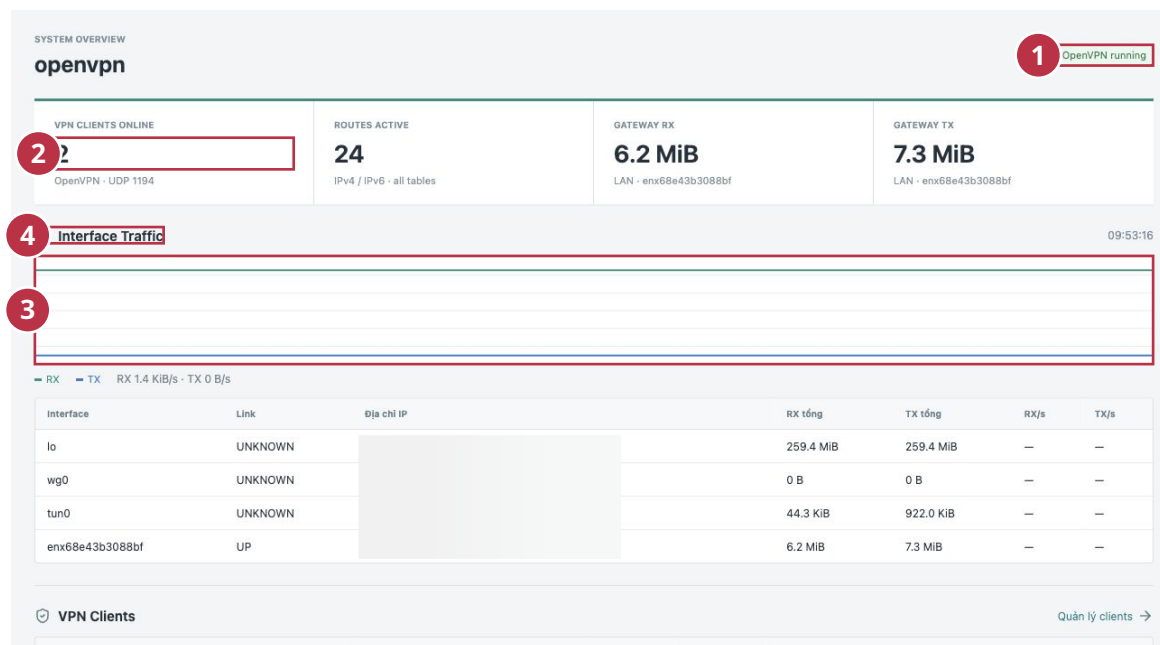
Operator không thấy menu Web Users/Backup hoặc các nút thao tác quản trị. Gọi trực tiếp URL/API bị hạn chế vẫn trả HTTP 403. Công tắc route bị khóa không phải lỗi giao diện.

Thiết bị và profile riêng

Mỗi thiết bị nên có client riêng, ví dụ office-laptop01 và iphone-hai. Không dùng một profile cho nhiều người hoặc nhiều thiết bị cùng lúc.

04. Dashboard, trạng thái client và traffic

Admin / Operator



Hình 2. Các số đánh dấu trạng thái dịch vụ, số client online, traffic và danh sách client.

Phiên tên UNDEF hoặc chưa có VPN IP có thể đang chờ hoàn tất xác thực, chưa chứng minh client kết nối thành công. Chỉ xác nhận khi OpenVPN Connect báo Connected và client có IP [IP]; tiếp tục thử dịch vụ nội bộ thật.

1. Mở **Dashboard**. Tại vị trí 1, kiểm tra **OpenVPN running**; Stopped nghĩa là dịch vụ chưa chạy.
2. Tại vị trí 2, đọc số **VPN CLIENTS ONLINE**. Có certificate không đồng nghĩa với đang online.
3. Tại vị trí 3, xem Interface Traffic, RX/TX tổng và tốc độ theo giây. RX/TX được tính từ phía Linux server.
4. Tại vị trí 4, xem tên client, trạng thái certificate, IP VPN, địa chỉ ngoài và RX/TX của phiên. Dữ liệu tự cập nhật khoảng mỗi 3 giây; bấm nút làm mới khi cần.

Đọc đúng trạng thái

Online/Offline mô tả phiên kết nối; valid/revoked mô tả certificate. Sau reconnect, counter phiên client có thể bắt đầu lại. Khi có cảnh báo stale, không coi số liệu cũ là trạng thái hiện tại.

05. Tạo client VPN mới

Admin / Operator

VPN ACCESS

OpenVPN Clients

OpenVPN running

ONLINE	CERTIFICATES	ENDPOINT
2	8	UDP

Client mới

09:53:16

Client name

1 office-laptop01

Tạo client

2

Hình 3. Nhập tên tại vị trí 1 và tạo tại vị trí 2. Các ví dụ trong ảnh chỉ được điền để minh họa, không tạo thêm client production.

1. Mở **OpenVPN Clients**. Nhập tên thiết bị vào **Client name** tại vị trí 1, ví dụ office-laptop01. Tên có 3-64 ký tự: chữ, số, gạch ngang hoặc gạch dưới; không có dấu tiếng Việt hay khoảng trắng.
2. Bấm **Tạo client** tại vị trí 2 một lần, chờ thông báo hoàn tất. Không reload hoặc bấm liên tục trong lúc tạo certificate.
3. Kiểm tra dòng client mới xuất hiện với certificate **valid**. Trạng thái Offline là bình thường khi chưa kết nối.
4. Bấm biểu tượng tải profile của dòng đó, nhận file office-laptop01.ovpn, rồi chuyển riêng cho đúng người/thiết bị. Operator chỉ tải được profile do mình tạo.

Giữ kín profile

File .ovpn hiện chứa certificate và private key, tương đương thông tin truy cập VPN. Không chụp nội dung file, không gửi vào nhóm chung và không đăng lên thư mục công khai.

06. Tải profile và revoke client

Tải: Admin / Operator phù hợp · Revoke: chỉ Admin

Certificates & Sessions								RX/TX từ phía server	
Client	Trạng thái	VPN IP	Remote IP	RX / phiên	TX / phiên	Kết nối từ	Hết hạn	Thao tác	
1 client01	Offline	—	—	0 B	0 B	—	10/01/2029	2	3

Hình 4. Vị trí 1 xác định đúng client; 2 tải profile; 3 thu hồi certificate bằng biểu tượng user-x.

Tải profile

1. Tìm đúng tên client ở vị trí 1, kiểm tra certificate valid.
2. Bấm biểu tượng tải xuống ở vị trí 2 và lưu file .ovpn. Không sửa địa chỉ remote hoặc các block certificate/key nếu chưa có chỉ dẫn của Admin.
3. Chuyển profile qua kênh được phép. Nếu mất file hoặc nghi bị lộ, báo Admin để revoke và tạo client mới.

Thu hồi quyền VPN

1. Admin xác định đúng client cần thu hồi ở vị trí 1.
2. Bấm biểu tượng **Thu hồi client** tại vị trí 3 và đọc xác nhận ngắt kết nối/thu hồi certificate.
3. Xác nhận thao tác. Kiểm tra trạng thái đổi sang **revoked** và client online bị ngắt. Profile revoked không còn tải được.

Revoke không phải công tắc bật/tắt

Không có nút un-revoke trên web. Khi cần cấp lại, tạo client mới với tên mới. Tài liệu không hướng dẫn restore bản cũ để mở lại certificate vì có thể khôi phục cả cấu hình không mong muốn.

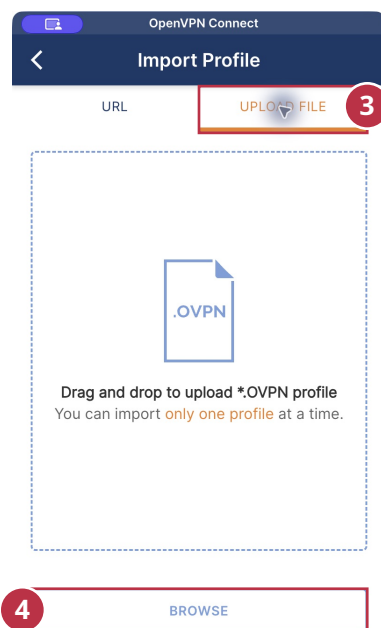
07. Cài và kết nối OpenVPN trên Windows

Người dùng VPN

A. Cài phần mềm

1. Trên máy Windows, mở trang login khi đang trong LAN/VPN phù hợp, bấm link **OpenVPN Connect 3.9.0**; hoặc nhận bộ cài từ Admin. File là `openvpn-connect-3.9.0.5008_signed.msi`.
2. Mở file MSI vừa tải, kiểm tra đúng nhà phát hành OpenVPN. Trong trình cài đặt, bấm Next, đọc điều khoản và chỉ chấp nhận khi bạn đồng ý.
3. Bấm Install; khi Windows yêu cầu quyền quản trị/UAC, dùng tài khoản được đơn vị cho phép hoặc nhờ IT cài đặt. Sau khi xong, bấm Finish và mở OpenVPN Connect.

B. Import profile và kết nối



Hình 5. Ảnh thật OpenVPN Connect 3.7.1 trên macOS để minh họa luồng desktop. Windows 3.9.0 có thể khác bố cục; dùng các mục Upload File/FILE và Browse/Upload File tương ứng.

1. Nhận file `office-laptop01.ovpn` riêng từ Admin/Operator và lưu vào Downloads hoặc thư mục dễ tìm. Bộ cài MSI không chứa profile của bạn.
2. Mở OpenVPN Connect. Nếu đã có profile, dùng nút + hoặc **Menu My Profiles Add** để mở Import Profile.

3. Chọn **UPLOAD FILE / FILE** tại vị trí 3 trong ảnh. Không nhập URL web quản trị vào ô Server Address/Cloud ID.
4. Bấm **BROWSE / Upload File** tại vị trí 4, chọn file .ovpn rồi xác nhận Open. Có thể kéo thả file vào ứng dụng hoặc mở đúp file .ovpn nếu Windows đã liên kết với OpenVPN Connect.
5. Trong màn hình xác nhận Imported Profile, kiểm tra đúng profile do IT cấp, bấm **Add / OK / Import** tùy phiên bản. Chỉ nhập mật khẩu private key nếu IT thông báo profile có mã hóa key; profile do web hiện tạo không yêu cầu mật khẩu đó.
6. Bật công tắc của profile để kết nối. Nếu ứng dụng báo **CONNECTED** và có IP VPN [IP], chuyển sang mục kiểm tra mạng nội bộ. Để ngắt, tắt công tắc.

Không nhập mật khẩu web vào VPN

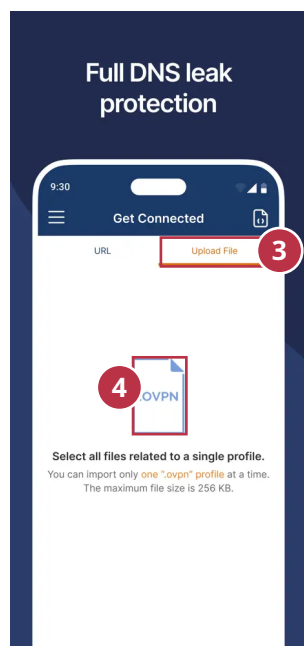
Profile hiện dùng certificate. Nếu ứng dụng bất ngờ yêu cầu username/password VPN, dừng và kiểm tra profile với Admin; không thử mật khẩu Admin/Operator.

Đối chiếu thao tác import theo [tài liệu OpenVPN Connect chính thức](#). Phần cài Windows thao tác theo bộ cài đã được cung cấp; máy làm tài liệu không chạy Windows nên không gắn nhãn ảnh macOS là ảnh cài Windows.

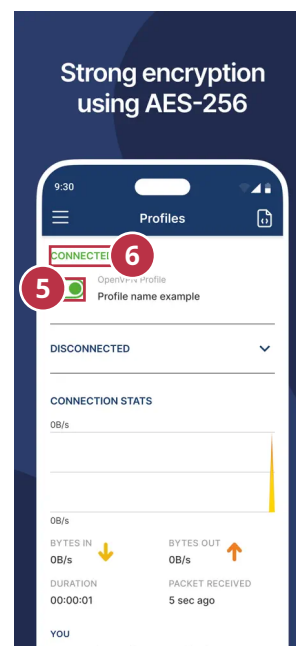
08. Cài và kết nối OpenVPN trên iPhone

Người dùng VPN

1. Trên iPhone, mở App Store, tìm **OpenVPN Connect** của **OpenVPN Inc.**, bấm Nhận/Get và cài. Có thể mở [trang ứng dụng chính thức](#). Không tải hoặc mở file MSI Windows trên iPhone.
2. Nhận profile riêng, ví dụ iphone-hai.ovpn, qua AirDrop hoặc kênh riêng được đơn vị cho phép. Lưu vào **Tệp/Files**; giữ đúng đuôi .ovpn, không thành .ovpn.txt.
3. Mở OpenVPN Connect, vào **Import Profile** bằng nút + nếu cần; chọn **UPLOAD FILE / FILE**, vị trí 3 trên hình 6.
4. Dùng Browse/Upload File để chọn file từ Files; xác nhận **Add / OK / Import**. Vị trí 4 minh họa loại file .ovpn cần nhập. Không chọn luồng Cloud ID/URL vì gateway này cấp file trực tiếp.
5. Bật công tắc của profile, vị trí 5 trên hình 7. Khi iOS hỏi cho phép thêm cấu hình VPN, bấm Allow nếu đúng ứng dụng và xác nhận Face ID/Touch ID/mật mã của chính bạn.
6. Kiểm tra trạng thái **CONNECTED**, vị trí 6. Mở Safari hoặc ứng dụng nghiệp vụ tới IP nội bộ cần dùng. Muốn ngắt VPN, tắt công tắc profile.



Hình 6. Chọn Upload File và nhập .ovpn. Ảnh minh họa do OpenVPN công bố trên App Store, không phải màn hình gateway SenPos.



Hình 7. Công tắc và trạng thái Connected; tên, IP và counter trong ảnh là dữ liệu mẫu của nhà phát hành.

Thử từ 4G/5G

Khi iPhone đang cùng LAN với server, router có thể không hỗ trợ NAT loopback tới IP public. Để kiểm tra truy cập từ bên ngoài, tắt Wi-Fi và dùng 4G/5G rồi kết nối lại. Internet thông thường vẫn dùng mạng của iPhone; chỉ các subnet nội bộ được định tuyến qua gateway.

Nguồn: cài [OpenVPN Connect trên iOS](#), chuyển file .ovpn sang iOS, ảnh từ [trang OpenVPN Inc. trên App Store](#).

09. Kiểm tra kết nối tới mạng nội bộ

Người dùng VPN / Admin

1. Đảm bảo ứng dụng báo Connected; Admin kiểm tra client Online và IP VPN [IP] trên OpenVPN Clients.
2. Chọn một IP máy đang hoạt động trong mạng đích và cổng dịch vụ được phép. Ví dụ mở `https://[IP]` nếu máy đó có web HTTPS, hoặc nhập IP vào ứng dụng nghiệp vụ/RDP phù hợp. Không truy cập địa chỉ mạng [IP] như một máy đích.
3. Trên Windows, có thể mở PowerShell và chạy các lệnh dưới đây. Thay IP ví dụ bằng máy thật, cổng 443 bằng cổng dịch vụ thực tế.
4. Nếu chỉ ping lỗi nhưng ứng dụng/TCP kết nối được, có thể máy đích chặn ICMP. Không kết luận mạng mất kết nối chỉ từ ping.

```
ipconfig
route print -4
ping [IP]
Test-NetConnection [IP] -Port 443
```

Kết quả mong đợi

VPN có IP [IP]; các route [IP], [IP], [IP] đi qua tunnel; dịch vụ trên máy đích trả lời. Internet không chuyển toàn bộ qua VPN.

Giới hạn kiểm thử đã thực hiện

Client VPN thử đã nhận ba route và ping router LAN [IP] thành công. IP [IP] không trả lời ping từ Linux trong lần kiểm tra trước; cần IP/cổng máy đích thật để xác nhận toàn tuyến [IP].

10. Quản lý route trên Linux

Sửa: chỉ Admin · Xem/lookup: Admin / Operator

NETWORK

Routing Table

24 route

Route tĩnh mới

Destination / CIDR: Gateway: Interface: Metric: + Thêm route

Tất cả IPv4 IPv6 Web managed

Bật	Destination	Gateway	Interface	Table	Metric	Nguồn	Trạng thái	Thao tác
☒			enx68e43b3088bf	main	100	Web unicast	Active	

Hình 8. Destination, gateway, interface, metric, nút thêm và ô tìm kiếm. Công tắc chỉ hoạt động với route do web quản lý.

Thêm route tĩnh

1. Mở **Routing**. Tìm destination trước để tránh thêm trùng. Ví dụ [IP] hiện đã có route quản lý, không thêm lại.
2. Trong form Route tĩnh mới, nhập **Destination/CIDR** tại vị trí 1; **Gateway** tại vị trí 2; chọn **Interface** tại vị trí 3; nhập **Metric** tại vị trí 4. Với next-hop LAN hiện tại, gateway là [IP], interface enx68e43b3088bf, metric ví dụ 100.
3. Bấm **Thêm route** tại vị trí 5. Kiểm tra dòng mới có nguồn Web, trạng thái Active và gateway/interface đúng.

Tra cứu, import, bật/tắt và xóa

1. Dùng ô tìm kiếm ở vị trí 6 hoặc các bộ lọc IPv4/IPv6/Web managed để tìm route.
2. Với route tĩnh có sẵn ngoài web và không được bảo vệ, bấm biểu tượng circle-plus **Đưa vào quản lý web**. Import chỉ đưa route vào cấu hình lưu, không đổi đường đi đang chạy.

3. Bật/tắt công tắc ở đầu dòng route Web. Active là route đang tồn tại; Disabled là đã tắt; Missing nghĩa là cấu hình bật nhưng route chưa thấy trong kernel, cần kiểm tra.
4. Bấm biểu tượng thùng rác và xác nhận nếu cần xóa route đã quản lý. Dùng Route Lookup phía dưới: nhập IP máy đích và bấm Tra cứu để kiểm tra next-hop.

Route Linux khác route client

Thêm route trên web không tự push route xuống VPN client. Default, route connected/kernel, IPv6 và bảng ngoài main được bảo vệ/chỉ xem. Không xóa đường đi phục vụ SSH hoặc web đang dùng.

11. Quản lý NAT và xem firewall

Sửa: chỉ Admin · Xem: Admin / Operator

NETWORK SECURITY

NAT & Firewall

MASQUERADE mới

Source / CIDR Destination / CIDR Output interface

1 2 3 enx68e43b3088bf 4 + Thêm NAT

Web Managed NAT

Source	Destination	Interface	Action	Thao tác
		enx68e43b3088bf	MASQUERADE	
		enx68e43b3088bf	MASQUERADE	
		enx68e43b3088bf	MASQUERADE	

Hình 9. Điền ba tham số rồi thêm NAT; bảng dưới hiển thị rule do web lưu.

1. Mở **NAT & Firewall**. Trong MASQUERADE mới, nhập **Source/CIDR** tại vị trí 1, thường là [IP].
2. Nhập **Destination/CIDR** tại vị trí 2, ví dụ [IP]; nhập **Output interface** tại vị trí 3 là enx68e43b3088bf. Không thêm trùng ba rule nội bộ đã có.
3. Bấm **Thêm NAT** tại vị trí 4. Kiểm tra bảng Web Managed NAT có đúng source, destination, interface và action MASQUERADE.
4. Khi cần xóa, Admin bấm thùng rác của đúng dòng và xác nhận. Mở các mục System Rules để đọc iptables/nftables; các rule hệ thống không có chức năng sửa tổng quát trên web.

Vì sao có NAT?

Máy đích thấy traffic đến từ IP LAN [IP], nên không cần return route về [IP]. NAT không tự mở cổng dịch vụ trên máy đích. Những lệnh iptables FORWARD/POSTROUTING là firewall/NAT, không phải dòng route trong bảng định tuyến.

12. Bổ sung một mạng nội bộ mới

Admin + quản trị Linux/router

Ví dụ dưới đây dùng [IP] để minh họa, không khẳng định mạng đó tồn tại. Thay bằng subnet thật được đơn vị cho phép. Trước khi đổi, backup cấu hình và chọn thời điểm có thể ngắt VPN ngăn.

1. Trên Linux, kiểm tra route và truy cập tới máy đích thật bằng `ip -4 route get <IP-máy>` và công cụ kiểm tra dịch vụ. Nếu Linux chưa tới được, xử lý router/upstream trước.
2. Trên web Routing, thêm route cho subnet mới qua next-hop đúng nếu cần. Không sao chép gateway ví dụ nếu hạ tầng thực tế khác.
3. Trên NAT & Firewall, thêm MASQUERADE nguồn [IP] tới subnet mới, trên interface LAN đúng.
4. Qua SSH được cấp quyền, mở file push route bằng `sudoedit`; giữ các dòng cũ và thêm một dòng cho subnet mới như ví dụ dưới.
5. Kiểm tra IP forwarding và rule FORWARD của Linux. Nếu firewall có chính sách chặn, cần cho phép tunnel tới subnet đó và traffic trả lời established/related; web chỉ hiển thị rule hệ thống, không tự tạo mọi luật firewall.
6. Trên OpenVPN Clients, Admin restart OpenVPN theo mục 13; các client reconnect để nhận route mới. Kiểm tra từ client tới IP/cổng máy đích.

```
sudoedit /etc/openvpn/senpos-internal-routes.conf
```

```
# Dòng ví dụ cho mạng mới; không xóa các push route hiện có:
push "route [IP] [IP]"
```

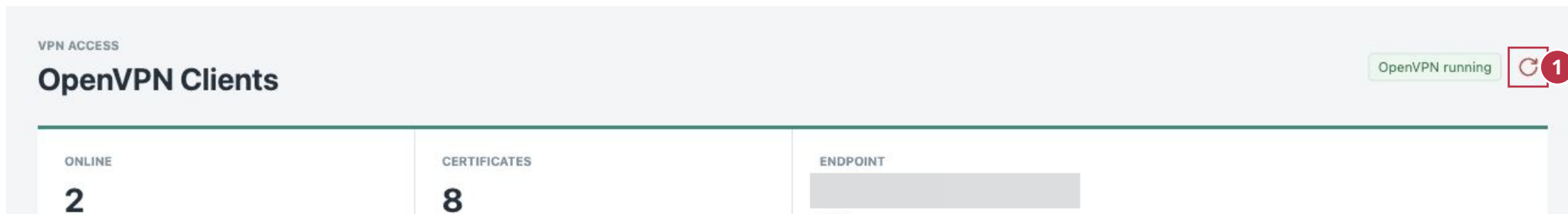
```
# Kiểm tra trước/sau thay đổi:
ip -4 route get [IP]
sysctl net.ipv4.ip_forward
sudo nft list table ip vpnadmin_nat
```

Không đổi thành full tunnel ngoài yêu cầu

Không thêm push redirect-gateway chỉ để truy cập một mạng nội bộ. Luôn kiểm tra đủ route server, push route client, forwarding/NAT và firewall của máy đích.

13. Restart dịch vụ OpenVPN

Chỉ Admin



Hình 10. Biểu tượng rotate-cw tại vị trí 1 khởi động lại dịch vụ VPN, không phải nút refresh ở thanh trên cùng.

1. Thông báo cho người đang sử dụng VPN và mở **OpenVPN Clients**. Bấm biểu tượng đồ **Khởi động lại OpenVPN** cạnh trạng thái dịch vụ ở vị trí 1.
2. Đọc hộp xác nhận: mọi client sẽ bị ngắt tạm thời. Chọn Hủy nếu chưa đến thời điểm phù hợp; chọn OK để thực hiện.
3. Chờ thông báo hoàn tất và trạng thái Running; reconnect client nếu chưa tự kết nối lại. Kiểm tra client Online và audit của thao tác.

Phạm vi thao tác

Chỉ restart unit OpenVPN đã cấu hình. Không xóa certificate, profile hay route/NAT. Operator không có nút và không thể gọi trực tiếp API restart.

14. Tạo tài khoản Operator

Chỉ Admin

ADMINISTRATION

Web Users

Tài khoản Operator mới

Tên đăng nhập Mật khẩu ban đầu Role

1 ops-branch01 2 3 Tạo tài khoản

Tên đăng nhập	Role
admin	Admin
operator	Operator

Hình 11. Form chỉ tạo Operator, không tạo Admin mới; các ô mật khẩu trong ảnh được để trống.

1. Mở **Web Users**. Nhập tên đăng nhập tại vị trí 1: 3-32 ký tự chữ/số/gạch ngang/gạch dưới, ví dụ ops-branch01.
2. Nhập mật khẩu ban đầu tại vị trí 2, dài 12-128 ký tự. Dùng mật khẩu riêng và chuyển trực tiếp qua kênh an toàn; role luôn là Operator.
3. Bấm **Tạo tài khoản** tại vị trí 3. Kiểm tra tên và role xuất hiện trong bảng tài khoản.
4. Người được cấp đăng nhập web, đổi mật khẩu của mình, rồi chỉ dùng chức năng tạo client và xem thông tin theo quyền.

Giới hạn hiện tại

Web chưa có chức năng xóa/khóa/reset mật khẩu Operator bởi Admin. Khi cần các thao tác đó, liên hệ người vận hành; không sửa hash JSON thủ công nếu chưa có quy trình kiểm soát.

15. Đổi mật khẩu đăng nhập web

Admin / Operator, cho chính tài khoản đang đăng nhập

Đổi mật khẩu

Mật khẩu hiện tại

1

Mật khẩu mới

2

Nhập lại mật khẩu mới

3

Đổi mật khẩu 4

Hình 12. Các vị trí 1-4 lần lượt là mật khẩu hiện tại, mật khẩu mới, nhập lại và nút cập nhật.

1. Chọn **Đổi mật khẩu** ở menu; nhập mật khẩu web hiện tại tại vị trí 1.
2. Nhập mật khẩu mới tại vị trí 2, dài 12-128 ký tự và khác mật khẩu hiện tại.
3. Nhập lại đúng mật khẩu mới tại vị trí 3; bấm **Đổi mật khẩu** tại vị trí 4.
4. Sau thành công, ứng dụng đăng xuất tài khoản. Đăng nhập lại bằng mật khẩu mới; các phiên cũ của tài khoản đó hết hiệu lực, tài khoản khác không bị đổi mật khẩu.

Không phải mật khẩu VPN

Thao tác này chỉ đổi mật khẩu web. Không làm thay đổi certificate, profile hay xác thực VPN hiện tại.

16. Backup cấu hình

Chỉ Admin

ADMINISTRATION

Backup & Restore

Gateway hiện tại

Backup cấu hình

Phạm vi

Mật khẩu mã hóa

Xác nhận mật khẩu

Tải backup

1

VPN, certificate, tài khoản web, route/NAT

2

3

4

Hình 13. Chọn phạm vi 1, đặt mật khẩu 2, xác nhận 3 và tải backup 4.

1. Mở **Backup & Restore**, chọn phạm vi tại vị trí 1: **VPN, certificate, tài khoản web, route/NAT** hoặc **Chỉ route/NAT**.
2. Đặt mật khẩu mã hóa ở vị trí 2, dài 12-128 ký tự; nhập lại ở vị trí 3. Đây là mật khẩu bảo vệ file backup, không phải mật khẩu web/VPN.
3. Bấm **Tải backup** tại vị trí 4. Kiểm tra trình duyệt đã tải file senpos - full - . . .vpnbackup hoặc senpos - network - . . .vpnbackup, dung lượng lớn hơn 0.
4. Lưu file và mật khẩu ở các nơi an toàn, tách biệt. Đặt thêm ghi chú ngày, người tạo và lý do backup. Nên backup trước thay đổi mạng, revoke hàng loạt hoặc restore.

Phạm vi	Bao gồm	Không bao gồm
Đầy đủ VPN	OpenVPN, CA/PKI/certificate/private key, profile, tài khoản web/quyền sở hữu client, route/NAT, IP forwarding, cấu hình môi trường web.	MSI/ứng dụng, OS/packages, Netplan/SSH, Nginx/Docker, cookie session và lịch sử audit.
Chỉ route/NAT	Route/NAT do web quản lý.	Certificate/tài khoản, route hệ thống và push route OpenVPN.

Chuẩn bị cho sự cố mất máy

File được mã hóa; quên mật khẩu thì không giải mã được. Chữ ký gắn với gateway hiện tại. Cài lại OS/chuyển máy cần root giữ riêng khóa /var/lib/vpn-gateway-backups/config-signing.key ngoài máy, bảo vệ như khóa riêng và khôi phục đúng layout. File .vpnbackup một mình không phải bản sao toàn bộ máy chủ.

17. Restore cấu hình từ backup

Chỉ Admin

Hình 14. Chọn file 1, mật khẩu 2, xác nhận 3 và thực hiện 4.

1. Backup trạng thái hiện tại trước. Xác minh đúng gateway, đúng thời điểm cần khôi phục và có mật khẩu web nằm trong bản backup nếu chọn bản đầy đủ. Thông báo thời gian bảo trì.
2. Trong phần Restore, bấm chọn file tại vị trí 1 và chọn .vpnbackup của gateway này, tối đa 32 MB.
3. Nhập mật khẩu mã hóa đã dùng khi tạo file tại vị trí 2. Tích **Xác nhận thay thế cấu hình** ở vị trí 3.
4. Bấm **Restore** tại vị trí 4, đọc hộp cảnh báo rồi xác nhận. Sai mật khẩu/file bị sửa/chữ ký khác gateway bị từ chối trước khi áp dụng.
5. Với bản route/NAT: chờ thành công và kiểm tra lại Routing/NAT; OpenVPN không bị restart. Với bản đầy đủ: OpenVPN restart, web restart sau khoảng 10 giây; đợi rồi đăng nhập bằng tài khoản/mật khẩu trong backup.
6. Kiểm tra client/certificate, route/NAT, khả năng truy cập máy đích và Audit Log. Reconnect các thiết bị VPN; revoke lại các certificate cần thu hồi nếu trạng thái backup quá cũ.

Restore đầy đủ có thể mở lại certificate đã revoke

Trạng thái tài khoản, quyền và PKI quay về thời điểm backup. Các POST mới tạm bị chặn 503 trong khi restore/chờ web restart. Audit hiện tại không bị ghi đè.

Nếu restore lỗi

Backend lưu snapshot trước thay đổi ở `/var/lib/vpn-gateway-backups/pre-restore-*/configuration.json` và rollback nếu áp dụng lỗi. Nếu rollback cũng lỗi, dừng thao tác lặp lại và nhờ root phục hồi snapshot; chỉ xử lý cờ restore-in-progress sau khi kiểm tra hệ thống.

18. Tra cứu lịch sử audit

Admin / Operator

ADMINISTRATION

Audit Log

16 bản ghi

1 /Backup

2 Tìm kiếm

Thời gian	User	IP	Thao tác	Đối tượng	Kết quả
09/10/2026 09:38:47	operator		/Backup/Restore		3 forbidden
09/10/2026 09:38:47	operator		/Backup/Create		forbidden
09/10/2026 09:38:47	operator		/Backup		forbidden
09/10/2026 09:38:47	admin		/Backup/Restore		success
09/10/2026 09:38:47	admin		/Backup/Create		success
09/10/2026 09:38:46	admin		/Backup/Restore		failed

Hình 15. Tìm theo user, IP, thao tác; kiểm tra kết quả success/failed/forbidden.

1. Mở **Audit Log**, nhập từ khóa ở vị trí 1, ví dụ tên client, username, /OpenVpn/Restart hoặc /Backup.

2. Bấm **Tìm kiếm** tại vị trí 2.

3. Đối chiếu thời gian UTC+7, User, IP, Thao tác, Đối tượng và Kết quả ở vị trí 3. success là thành công; failed là lỗi; forbidden là bị chặn quyền; started là đã ghi nhận ý định và chưa có kết quả cuối tương ứng.

Audit ứng dụng khác log OpenVPN

Audit ghi các thao tác web/profile download, không phải toàn bộ log kết nối của daemon. Không ghi mật khẩu hoặc nội dung private key. Khi chẩn đoán tunnel, Admin có thể cần journal OpenVPN qua SSH.

19. Xử lý lỗi thường gặp

Hiện tượng	Kiểm tra theo thứ tự
Không mở được web từ 4G/Internet	IP web là IP nội bộ. Lấy profile trước, kết nối VPN rồi mở web; không dùng IP public VPN như một URL cấp profile tự động.
Connection timeout / không kết nối VPN	1. Dùng đúng profile. 2. Thử 4G/5G để tránh NAT loopback. 3. Admin kiểm tra Running. 4. Kiểm tra UDP 1194 port forwarding/firewall và IP public. Ping public không chứng minh cổng UDP đang mở.
Connected nhưng không vào được mạng nội bộ	1. Reconnect để nhận push route. 2. Kiểm tra route client và trùng subnet Wi-Fi. 3. Linux phải tới được máy đích. 4. Kiểm tra route server, forwarding/NAT và cổng/firewall máy đích. Không thêm redirect-gateway tùy tiện.
iPhone không thấy file .ovpn	Lưu vào Files, kiểm tra đuôi không thành .txt, mở Upload File/Browse trong OpenVPN Connect và chọn đúng vị trí lưu. Không nhập file MSI.
Certificate revoked / verification failed	Admin kiểm tra certificate còn valid, ngày giờ thiết bị đúng và profile đúng gateway. Certificate revoked cần cấp client mới; không tắt kiểm tra certificate.
Ứng dụng yêu cầu VPN username/password bất ngờ	Hệ thống hiện dùng certificate. Kiểm tra nguồn profile với Admin, không nhập mật khẩu đăng nhập web và không bỏ qua xác thực.
Operator không thấy nút tải profile hoặc bị 403	Chỉ tải profile chính mình tạo, certificate còn valid. Các chức năng quản trị/Backup/Web Users/revoke/restart bị chặn theo quyền, không phải lỗi.
Route Missing hoặc công tắc bị khóa	Missing: Admin kiểm tra interface/gateway và cấu hình Linux. Công tắc khóa: route hệ thống được bảo vệ hoặc user chỉ xem. Import chỉ áp dụng với route tĩnh được phép.
Restore sai mật khẩu / signature invalid	Dùng đúng mật khẩu mã hóa và backup từ gateway này. Không sửa file. Nếu đổi máy/cài lại OS, cần khóa ký gốc và đúng layout; nhờ root xử lý.
HTTP 413 / upload restore quá lớn	Giới hạn file là 32 MB; kiểm tra cấu hình Nginx đã cho request multipart 34 MB. Không tắt giới hạn hoặc tăng tùy tiện để nhận file không rõ nguồn.

Hiện tượng	Kiểm tra theo thứ tự
HTTP 503 sau restore đầy đủ	Đợi web restart khoảng 10 giây rồi thử lại. Nếu kéo dài, Admin kiểm tra service/journal và cờ restore-in-progress; không tự xóa cờ trước khi biết restore/rollback đã kết thúc.
MSI không cài được / cần quyền Admin Windows	Dùng bộ cài đúng Windows và từ nguồn đã xác minh. Nhờ IT cấp quyền cài; ghi lại thông báo lỗi, phiên bản OS và gửi qua kênh hỗ trợ. Không tắt antivirus để thử.

Khi gửi yêu cầu hỗ trợ, cung cấp thời gian, tên client, IP/cổng máy đích, thông báo lỗi và ảnh trạng thái. Không gửi mật khẩu, khóa riêng, file backup hoặc nội dung .ovpn vào nhóm công khai.