



VPN SITE-TO-SITE (OPENVPN)

Guia Oficial iT Guys

Código: ITGENG 0025/26 | **Classificação:** RESTRITO

Responsável: João Pedro Toledo Gonçalves | **Data:** 25/01/2026

1. HISTÓRICO DE REVISÃO

Data	Versão	Descrição	Autor
25/01/2026	1.0	Criação Inicial	João Pedro Toledo Gonçalves

2. OBJETIVO

Interligar duas ou mais filiais (Matriz x Filial) de forma transparente, permitindo que servidores e computadores de ambas as redes se comuniquem como se estivessem no mesmo prédio, utilizando túneis OpenVPN (Shared Key ou SSL/TLS).

3. PRÉ-REQUISITOS

- [] IP Público (Fixo ou DynDNS) em **pelo menos uma** das pontas (Server).
- [] Faixas de IP de LAN **DIFERENTES** em cada ponta (ex: Matriz `192.168.1.0/24`, Filial `192.168.2.0/24`). **Se forem iguais, a VPN não roteia.**
- [] Shared Key gerada automaticamente pelo pfSense (Server).

4. PASSO A PASSO (EXECUÇÃO)

Cenário Exemplo

- * **Matriz (Server):** WAN IP `200.200.200.1`, LAN `192.168.1.0/24`.
- * **Filial (Client):** WAN IP (Dinâmico), LAN `192.168.2.0/24`.
- * **Tunnel Net:** `10.0.99.0/30` (Rede exclusiva pra comunicação VPN).

Etapa 1: Configurar a Matriz (Server)

1. Acesse `VPN > OpenVPN > Servers`. Clique **Add**.

2. **Server Mode:** `Peer to Peer (Shared Key)` . (Mais simples e robusto para 1:1).
3. **Protocol:** `UDP on IPv4`.
4. **Device Mode:** `tun` (Layer 3 Routing).
5. **Interface:** `WAN`.
6. **Local Port:** `1195` (Use uma porta diferente da Road Warrior 1194).
7. **Shared Key:** Marque `Automatically generate a shared key`.
8. **Cryptographic Settings:** AES-256-GCM (ou CBC com hardware support).
9. **Tunnel Settings:**
 - * **IPv4 Tunnel Network:** `10.0.99.0/30`
 - * **IPv4 Remote Network:** `192.168.2.0/24` (A LAN da Filial. O pfSense cria a rota sozinho).
10. Salve.
11. **IMPORTANTE:** Entre na edição novamente e COPIE a **Shared Key** gerada (o bloco de texto inteiro). Você vai colar na Filial.

Etapa 2: Configurar a Filial (Client)

1. Acesse `VPN > OpenVPN > Clients`. Clique **Add**.
2. **Server Mode:** `Peer to Peer (Shared Key)`.
3. **Interface:** `WAN`.
4. **Server Host or Address:** `200.200.200.1` (IP da Matriz).
5. **Server Port:** `1195`.
6. **Shared Key:** Desmarque a auto-geração e **COLE** a chave copiada da Matriz.
7. **Tunnel Settings:**
 - * **IPv4 Tunnel Network:** `10.0.99.0/30` (Igual à Matriz).
 - * **IPv4 Remote Network:** `192.168.1.0/24` (A LAN da Matriz).
8. Salve.

Etapa 3: Regras de Firewall e Interfaces

Faça isso em **AMBOS** (Matriz e Filial):

1. Acesse `Firewall > Rules > WAN`.
 - * Crie uma regra **Pass** para Protocolo **UDP**, Porta **1195** (Isso permite fechar o túnel).
2. Acesse `Firewall > Rules > OpenVPN`.
 - * Crie uma regra **Pass** (Protocolo Any) liberando o tráfego da rede remota.
 - * *Exemplo na Matriz:* Source `192.168.2.0/24`, Dest `LAN Net`.
 - * *Exemplo na Filial:* Source `192.168.1.0/24`, Dest `LAN Net`.

- * ***Dica:*** Para teste inicial, libere `Any` to `Any` na aba OpenVPN.

Etapa 4: Validação do Túnel

1. Acesse `Status > OpenVPN`.
2. O Status deve estar **UP** (Verde).
3. Verifique o IP Virtual (`10.0.99.1` e `10.0.99.2`).

5. SOLUÇÃO DE PROBLEMAS (TROUBLESHOOTING)

Problema 1: Status UP, mas não pinga a LAN remota

- * **Causa:** Bloqueio de Firewall (ICMP) nos Windows/Linux da ponta.
- * **Solução:** O Firewall do Windows bloqueia Pings de subnets "estranhas" por padrão. Tente pingar o **IP da Interface LAN do pfSense remoto** (ex: ping `192.168.1.1` da filial). Se responder, o túnel está OK e o problema é o firewall do host destino.
- * ***Teste:*** Desative o firewall do Windows temporariamente para validar.

Problema 2: Túnel fica "Reconnecting"

- * **Causa:** Shared Key errada, Porta fechada na WAN ou incompatibilidade de Crypto.
- * **Solução:**
- * Confira se a Shared Key é IDÊNTICA.
- * Confira se o algoritmo de criptografia (ex: AES-256-GCM) e o de Hash (SHA256) são iguais.
- * Verifique se a Regra de WAN libera a porta 1195 UDP.

Problema 3: Conflito de rotas

- * **Causa:** Tunnel Network conflitante ou LANs iguais.
- * **Solução:** Garanta que Tunnel Network (`10.0.99.0/30`) não exista em nenhum outro lugar da rede. E JAMAIS tente VPN se ambos os lados usam `192.168.1.0`.

6. DADOS TÉCNICOS

Campo	Valor	Descrição
Porta	1195+ UDP	Dica: Use portas separadas por túnel

Campo	Valor	Descrição
Modo	Shared Key	Para conexões Site-to-Site simples de 1:1
Rota	Estática	pfSense adiciona via Remote Network

7. VALIDAÇÃO FINAL (Definição de Pronto)

- ☐ Status OpenVPN mostra "Connected"?
- ☐ Ping da Matriz para Filial (`ping 192.168.2.1`) responde?
- ☐ Servidor de Arquivos da Matriz é acessível pela Filial (`\\192.168.1.10`)?