Setting Up OpenVPN on pfSense: A Step-by-Step Guide

TechRounder PDF Edition

Live article: https://www.techrounder.com/how-to/setting-up-openvpn-on-pfsense-a-step-by-step-guide/

By Vipin PG | Published September 12, 2024 | Updated January 4, 2026 | Format: Guide | 5 min read

Quick answer

Setting up OpenVPN on pfSense involves creating a Certificate Authority and server certificate, configuring the OpenVPN server with your chosen tunnel network and encryption settings, adding firewall rules for WAN and OpenVPN interfaces, creating user accounts, and exporting client configurations for remote devices.

OpenVPN is a powerful tool for creating secure connections between remote devices and your home or office network. When combined with pfSense, a robust open-source firewall and router platform, you can create a flexible and secure remote access solution. This article will walk you through the process of setting up OpenVPN on pfSense, allowing you to access your network resources from anywhere in the world.

Why Use OpenVPN with pfSense?

Before we dive into the setup process, let's look at some reasons why you might want to use OpenVPN with pfSense:

1. Secure remote access to your network
2. Ability to use your home internet connection while away
3. Protection from unsecured public Wi-Fi networks
4. Access to region-restricted content

Prerequisites

Before starting, make sure you have:

1. A working pfSense installation
2. Admin access to your pfSense router
3. A basic understanding of networking concepts

Step 1: Planning Your VPN Setup

Before configuring OpenVPN, it's important to plan your network layout. You'll need to choose:

1. An IP range for your VPN clients
2. The port your VPN server will use (default is 1194)
3. The protocol (UDP or TCP)

For this guide, we'll use:

- VPN Client IP range: 10.3.201.0/24
- Port: 1194
- Protocol: UDP

Step 2: Creating a Certificate Authority (CA)

OpenVPN uses certificates for authentication. To create these, we first need a Certificate Authority:

1. Go to System > Cert Manager
2. Click "Add" under the "CAs" tab
3. Fill in the following:
    - Descriptive Name: OpenVPN-CA
    - Method: Create an internal Certificate Authority
    - Key length: 2048
    - Lifetime: 3650
    - Common Name: Your-CA-Name
4. Click "Save"

Step 3: Creating a Server Certificate

Now, create a certificate for your OpenVPN server:

1. Go to System > Cert Manager
2. Click "Add" under the "Certificates" tab
3. Fill in:
    - Descriptive Name: OpenVPN-Server-Cert
    - Method: Create an internal Certificate
    - Certificate Authority: Select the CA you just created
    - Key length: 2048
    - Lifetime: 3650
    - Common Name: Your-Server-Name
4. Click "Save"

Step 4: Setting Up the OpenVPN Server

Now we'll configure the OpenVPN server:

1. Go to VPN > OpenVPN
2. Click "Add" under the "Servers" tab
3. Fill in these key settings:
    - Server mode: Remote Access (SSL/TLS + User Auth)
    - Protocol: UDP on IPv4 only
    - Device mode: tun
    - Interface: WAN
    - Local port: 1194
    - Description: OpenVPN Server
    - TLS Authentication: Enable authentication of TLS packets
    - Peer Certificate Authority: Select your CA
    - Server Certificate: Select your server certificate
    - DH Parameters Length: 2048 bit
    - Encryption Algorithm: AES-256-GCM
    - Auth Digest Algorithm: SHA256

- Tunnel Network: 10.3.201.0/24
- Redirect Gateway: Force all client-generated traffic through the tunnel
- Local Network: Your LAN subnet (e.g., 192.168.1.0/24)
- Concurrent Connections: Set a limit if desired
- Compression: Disable compression (legacy)
- Push "redirect-gateway def1": Checked
- Push "block-outside-dns": Checked
- DNS Server 1: Your preferred DNS server
- DNS Server 2: A backup DNS server
- Inter-client communication: Allow clients to communicate with each other
- Duplicate Connections: Allow multiple connections from clients with the same common name

4. Click "Save"

Step 5: Creating Firewall Rules

To allow traffic through your VPN, you need to create firewall rules:

1. Go to Firewall > Rules
2. Click "Add" on the WAN tab
3. Set:
   - Action: Pass
   - Interface: WAN
   - Protocol: UDP
   - Source: Any
   - Destination: WAN Address
   - Destination Port Range: 1194
4. Click "Save"

Now, create a rule for the OpenVPN interface:

1. Go to the OpenVPN tab
2. Click "Add"
3. Set:
   - Action: Pass
   - Interface: OpenVPN
   - Protocol: Any
   - Source: Any
   - Destination: Any
4. Click "Save"

Don’t forget to apply your changes after creating these rules.

Step 6: Creating User Accounts

If you’re using local authentication, you’ll need to create user accounts:

1. Go to System > User Manager
2. Click "Add"
3. Fill in:
   - Username: Choose a username

- Password: Set a strong password
- Full name: User’s full name

4. Under "Certificate", click "Add"
5. Fill in:
   - Descriptive name: User’s name
   - Certificate authority: Your OpenVPN CA
6. Click "Save"

Repeat this process for each user who needs VPN access.

Step 7: Installing the OpenVPN Client Export Package

To easily generate client configurations, install the OpenVPN Client Export package:

1. Go to System > Package Manager
2. Click "Available Packages"
3. Find "openvpn-client-export"
4. Click "Install" and confirm

Step 8: Exporting Client Configurations

Now you can export client configurations:

1. Go to VPN > OpenVPN
2. Click the "Client Export" tab
3. Select your OpenVPN server in the "Remote Access Server" dropdown
4. Scroll down to see various export options for different devices

For most clients, the "Most Clients" option works well. For Windows users, the installer can be convenient.

Step 9: Connecting Clients

The process for connecting clients varies depending on the device and operating system. Generally, you’ll need to:

1. Install an OpenVPN client on the device
2. Import the configuration file you exported
3. Connect using the username and password you set up

Troubleshooting Tips

If you encounter issues, try these steps:

1. Check firewall rules: Ensure your rules are correctly configured
2. Verify server settings: Double-check your OpenVPN server configuration
3. Check client logs: Most OpenVPN clients provide logs that can help identify issues
4. Test connectivity: Make sure the client can reach the server’s IP and port
5. Verify certificates: Ensure client certificates are valid and not expired

Advanced Configuration Options

Once you have a basic setup working, you might want to explore more advanced options:

1. Two-factor authentication: Add an extra layer of security

2. Split tunneling: Allow certain traffic to bypass the VPN
3. Traffic shaping: Prioritize certain types of VPN traffic
4. Multiple VPN servers: Set up different servers for different purposes
5. Site-to-site VPNs: Connect entire networks together

Maintaining Your VPN

To keep your VPN running smoothly and securely:

1. Regularly update pfSense and the OpenVPN package
2. Monitor server logs for unusual activity
3. Periodically review and update firewall rules
4. Rotate certificates and keys on a schedule
5. Keep track of user accounts and revoke access when no longer needed

Conclusion

Setting up OpenVPN on pfSense provides a powerful and flexible VPN solution. While the initial setup process might seem complex, it offers robust security and a wide range of configuration options. By following this guide, you should now have a functioning OpenVPN server on your pfSense router, allowing secure remote access to your network.

Remember, network security is an ongoing process. Regularly review and update your VPN configuration to ensure it continues to meet your needs and security requirements. With proper setup and maintenance, your pfSense OpenVPN server will provide a reliable and secure way to access your network resources from anywhere in the world.