

AI-03158 pfsense and NordVPN Deployment

Owner	Ⓜ Rigel Arcayan
Tags	Project
Created time	@November 12, 2025 11:10 AM

Integrate pfsense and NordVPN. List hardware and software requirements. Create a step by step deployment of pfsense and NordVPN to provide vpn aware Wireless LAN connections.

Quick Answer:

To integrate pfSense with NordVPN, you'll need a dedicated pfSense router (physical or virtual), an active NordVPN subscription, and configuration via OpenVPN. The deployment involves setting up pfSense, importing NordVPN's OpenVPN configuration, creating firewall rules, and binding your Wireless LAN interface to route traffic through the VPN vpnAlert +2.

Hardware Requirements

- Dedicated pfSense device (options):
 - Small form-factor PC (Intel/AMD CPU, 2+ cores recommended)
 - Network appliance (e.g., Netgate SG-1100/SG-2100/SG-3100)
 - Virtual machine (VMware, Proxmox, Hyper-V, etc.)
- Minimum specs:
 - CPU: 1 GHz+ (AES-NI support recommended for VPN performance)
 - RAM: 2 GB (4 GB+ preferred for multiple services)
 - Storage: 8 GB SSD/HDD
 - NICs: At least 2 (WAN + LAN); add more if segmenting WLAN separately
- Wireless Access Point (AP):
 - Standalone AP or router in AP mode connected to pfSense LAN/WLAN interface

Software Requirements

- pfSense OS (latest stable release, e.g., 2.5.x or newer)
 - NordVPN subscription
 - OpenVPN client (built into pfSense)
 - Certificates & configuration files from NordVPN (downloadable from NordVPN site)
 - Optional: pfSense packages for monitoring (e.g., openvpn-client-export, status_openvpn)
-

Step-by-Step Deployment

1. Install pfSense

- Deploy pfSense on hardware or VM.
 - Configure WAN (internet) and LAN (internal network).
 - Ensure internet connectivity from LAN clients.

1. Prepare NordVPN Configuration

- Log into NordVPN dashboard.
 - Download OpenVPN configuration files (.ovpn) for your chosen server.
 - Obtain username/password (service credentials, not account login).

1. Configure OpenVPN Client in pfSense

- Navigate: VPN → OpenVPN → Clients → Add.
 - Set:
 - Server mode: Peer-to-peer (SSL/TLS)
 - Protocol: UDP (recommended) or TCP
 - Server host/IP: NordVPN server address
 - Port: 1194 (UDP default)
 - Authentication: Username/Password
 - TLS/CA certificate: Import from NordVPN .ovpn file
- Save and apply.

1. Create Interface for VPN

- Go to Interfaces → Assignments.
 - Add new interface for the OpenVPN client (e.g., OPT1).
 - Enable and name it VPN_Nord.

1. Firewall & NAT Rules

- Navigate: Firewall → NAT → Outbound.
 - Switch to Manual Outbound NAT.
 - Add rules mapping LAN/WLAN traffic to VPN_Nord interface.
 - Ensure DNS traffic is also routed through VPN (or use NordVPN DNS servers).

1. WLAN Integration

- Connect your Wireless Access Point to pfSense LAN port or a dedicated WLAN interface.
 - Create firewall rules:
 - Source: WLAN subnet
 - Destination: Any
 - Gateway: VPN_Nord
- This ensures all WLAN traffic is forced through NordVPN.

1. Test Connectivity

- Connect a device to WLAN.
 - Visit <https://nordvpn.com/what-is-my-ip> to confirm VPN IP.
 - Verify DNS leak protection.

1. Optional Enhancements

- Kill switch: Block WAN access if VPN disconnects.
 - Policy-based routing: Route specific devices/subnets through VPN, others direct.
 - Monitoring: Use pfSense dashboard to track VPN status.

Outcome

With this setup, all WLAN clients automatically use NordVPN, ensuring privacy and security without individual device configuration. pfSense acts as the central VPN-aware router/firewall, enforcing consistent VPN usage across your wireless network vpnAlert +2.

Follow-up:

Would you like me to create a protocol checklist (like a reproducible deployment matrix) so you can archive this setup alongside your DockerLab documentation? That way, you'll have a structured reference for future VPN-aware network builds.

Sources: vpnAlert +2