Configuring NordVPN on a Specific VLAN (TP-Link Omada)

This guide explains how to route a specific **VLAN** through a **NordVPN OpenVPN** tunnel on a TP-Link Omada network. This configuration ensures that only devices on a designated secure network are encrypted, while the rest of the network remains on the standard ISP connection.

1. Prerequisites

Before beginning, log in to your NordVPN dashboard to collect the following essential data:

- **Service Credentials:** Your manual username and password (found under *Services* > *NordVPN* > *Manual Setup*). **Note:** These are different from your email login.
- **OpenVPN Configuration File:** Download the `.ovpn` file for your desired server. UDP is recommended for better performance.
- **Server IP:** Note the **Direct IP address** of the NordVPN server (e.g., `89.187.183.182`).
- **NordVPN DNS:** Use `103.86.96.100` for a secure, leak-proof setup.

---

2. Configuration Steps

Phase A: Create the Secure VLAN

1. Navigate to **Settings → Wired Networks → LAN**.
2. Click **+ Create New LAN**.
3. **VLAN ID:** Assign a unique ID (e.g., `100`).
4. **Gateway/Subnet:** Define your desired local range (e.g., `192.168.x.1/24`).
5. **DNS Server:** Select **Manual** and enter the NordVPN DNS: `103.86.96.100`.

Phase B: The MTU Fix (Critical for Web Browsing)

To prevent "fragmentation," where some sites, like Google, load while others, like Amazon or Netflix, fail to load, you must manually adjust the packet size in the configuration file.

1. Open your downloaded `.ovpn` file in a text editor (like Notepad).
2. Add the following command to the **very top** of the file:

```
mssfix 1300
```

[Image showing the mssfix command placed at the start of an OpenVPN config file]

Phase C: Set up the VPN Client

1. Go to **Settings → VPN → VPN Client → OpenVPN**.
2. **Remote Server:** Enter the NordVPN Server IP (e.g., `89.187.183.182`) and Port (`1194` for UDP).
3. **Username/Password:** Use your NordVPN **Service Credentials**.
4. **Local Networks:** Select only your **Secure VLAN**.
5. **Configuration:** Upload your edited `.ovpn` file.
6. Click **Apply**.

---

3. Security & Isolation (Gateway ACLs)

To keep the Secure VLAN isolated from your primary network while still allowing management access, configure **Gateway ACLs**.

Rule Name	Policy	Source	Destination
Allow Management	Permit	Main Network	Secure VLAN
Isolate Secure VLAN	Deny	Secure VLAN	All Local Networks

---

4. Troubleshooting

- **No Internet:** Ensure the device (phone/laptop) does not have a native VPN app active. Double-encryption (VPN-in-VPN) often causes packet drops and connection failures.

- **Remote Desktop (RDP) Fails:** Ensure the target machine's network profile is set to **Private** in Windows settings. If connecting by hostname fails, use the specific **Reserved IP** address.
- **DNS Leaks:** Verify your setup by visiting `dnsleaktest.com` from a device on the Secure VLAN. The results should show NordVPN servers, not your ISP.

Revision #1
Created 2026-03-21 22:17:57 UTC by Francis
Updated 2026-03-27 17:32:29 UTC by Francis