Setting Up NordVPN Onion Over VPN with Threat Protection on TP-Link Omada

Description: This guide details how to configure a dedicated "Secure Network" VLAN on a TP-Link Omada router (ER8411/OC300) that routes all traffic through NordVPN's Onion network. It includes specific steps to enable malware blocking (Threat Protection) and to prevent location leaks via IPv6 and WebRTC/QUIC.

Last Updated: January 2026

Prerequisites: NordVPN Account, Omada SDN Controller, Omada Router

---

Phase 1: Obtain Configuration & Credentials

Do not use your regular NordVPN email and password.

1. Log in to the NordVPN Dashboard and navigate to **NordVPN > Manual setup**.
2. **Get Credentials:**
   - Click the **Service credentials** tab.
   - Copy the Username and Password (these are long alphanumeric strings).
3. **Download Onion Config:**
   - Go to the **Server recommendation** tab.
   - Change the Country to Switzerland or The Netherlands.
   - In the **Server type** dropdown, select **Onion Over VPN**.
   - Click **Get setup configuration** and download the UDP .ovpn file.
4. **Extract Server IP:**
   - Open the downloaded .ovpn file with a text editor (Notepad).
   - Locate the line starting with `remote`.
   - Copy the IP Address found on that line (e.g., 37.120.137.172).

Phase 2: Configure Omada VPN Client

This sets up the tunnel interface.

1. In Omada Controller, go to **Settings > VPN > VPN > OpenVPN Client**.
2. Click **Create** and configure:
   - **VPN Type:** VPN Client - OpenVPN
   - **Username/Password:** Paste the Service Credentials obtained in Phase 1.
   - **Configuration:** Upload the .ovpn file you downloaded.
3. **CRITICAL FIX (IP Mismatch):**
   - Check the **Remote Server** field. If it does not match the IP address inside your text file, delete it.
   - Manually enter the correct IP address you found in the text file (e.g., 37.120.137.172).
   - Ensure the port is set to **1194**.
4. **Local Networks:** Select your specific VLAN (e.g., "SecureLAN").
5. Click **Create/Apply**.
6. Check **VPN > Client status** to confirm it says "Connected".

Phase 3: Enable Malware Protection (DNS)

This replaces standard DNS with NordVPN's Threat Protection filtering.

1. Go to **Settings > Wired Networks > LAN**.
2. Edit your **Secure Network VLAN**.
3. Scroll to **DNS Server** and select **Manual**.

Primary DNS: 103.86.96.96 Secondary DNS: 103.86.99.99

5. Click **Save**.

Phase 4: "Leak Plug" Configuration

These steps prevent Google and other services from bypassing the VPN.

Step A: Disable IPv6

1. In the same VLAN Edit menu (Settings > Wired Networks > LAN), scroll to **Configure IPv6**.
2. Uncheck the **Status** box (or set interface type to "None") to disable IPv6 entirely for this VLAN.
3. Click **Save**.

Step B: Block QUIC (UDP 443)

Omada cannot use "0.0.0.0/0" for groups, so we use the "Split Subnet" method.

1. **Create Port Group:**
   - Go to **Settings > Profiles > Groups**.
   - Create a new IP-Port Group named **QUIC_Ports**.
   - **Port:** 443
   - **Subnets:** Add these two entries to cover all IPs:

Entry 1: 1.0.0.0/1 Entry 2: 128.0.0.0/1

2. **Create ACL Rule:**
   - Go to **Settings > Network Security > ACL > Gateway ACL**.
   - Create a new rule:
     - **Description:** Block_QUIC_Google
     - **Direction:** LAN > WAN
     - **Policy:** Deny
     - **Protocol:** UDP
     - **Source:** Your Secure VLAN (Network).
     - **Destination:** IP-Port Group > QUIC_Ports.
   - Click **Create**.

Phase 5: Verification

Perform these tests to confirm security.

- **BrowserLeaks Test:** Visit https://browserleaks.com/ip.
  - **Success:** IP Location shows Europe (Netherlands/Switzerland).
  - **Success:** WebRTC Leak shows European IP or "Disabled".
  - **Success:** IPv6 Test says "Not Reachable".
- **Latency Check:**
  - Run a speed test (e.g., fast.com).
  - **Success:** Latency should be high (>100ms), confirming traffic is routing through the Tor network.

Troubleshooting Notes

- **Connection Failed:** If the VPN refuses to connect, re-open the .ovpn file in a text editor and verify the "Remote Server" IP in Omada matches the file exactly.
- **Google Speed Test 5ms:** If you see low ping on Google, the QUIC block is not active. Verify the ACL rule is set to UDP (not TCP) and the destination group covers all IPs.

Revision #3
Created 2026-03-16 03:06:46 UTC by Francis
Updated 2026-03-28 21:51:46 UTC by Francis