Network

- TP-Link Omada
  - Setting Up NordVPN Onion Over VPN with Threat Protection on TP-Link Omada
  - Configuring NordVPN on a Specific VLAN (TP-Link Omada)
  - Cross-VLAN Media Casting (TP-Link Omada SDN)
  - Configuring an IoT VLAN on TP-Link Omada SDN (Wi-Fi 7 Environment)
  - Configuring NordVPN Kill Switch & Strict VLAN Isolation

TP-Link Omada

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.

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.

TP-Link Omada

Cross-VLAN Media Casting (TP-Link Omada SDN)

Target Hardware: TP-Link Omada Gateways (ER8411, ER707-M2, etc.)
Controller: Omada Software/Hardware Controller (OC300/OC200)

---

1. Defining Custom Bonjour Services

By default, the Omada SDN does not include pre-defined entries for several modern streaming protocols. You must manually add these before they can be used in an mDNS rule.

1. Navigate to **Settings > Services > Bonjour Service**.
2. Click **+ Create New Bonjour Service** for each of the following:

Service Name	Service Type	Protocol
Spotify Connect	`_spotify-connect._tcp.local`	TCP
Google Cast	`_googlecast._tcp.local`	TCP
Apple Music / AirPlay	`_airplay._tcp.local`	TCP
Apple Music (RAOP)	`_raop._tcp.local`	TCP

---

2. Enabling the mDNS Forwarder

The mDNS (Multicast DNS) service allows discovery traffic to "jump" between isolated VLANs.

1. Go to **Settings > Services > mDNS**.
2. Click **Create New Rule**.
3. **Rule Name:** `Cross_VLAN_Discovery`
4. **Device Type:** Select **Gateway**.
5. **Bonjour Service:** Select the custom services created in Step 1 (Spotify, Google Cast, AirPlay, RAOP).
6. **Services Network:** Select the VLAN where the **Speakers/TVs** live (e.g., Media Network).

7. **Client Network:** Select the VLAN where your **Phones/Tablets** live (e.g., Main Network).
8. Click **Apply**.

---

3. Configuring the Gateway ACL (Stateful Connection)

The **ER8411** is a stateful gateway, meaning it remembers which connections you started. You only need to permit traffic from the trusted network to the media network.

1. Navigate to **Settings > Network Security > ACL > Gateway ACL**.
2. Click **Create New Rule**:
   - **Description:** `Permit_Main_to_Media_Casting`
   - **Direction:** LAN -> LAN
   - **Policy:** Permit
   - **Protocols:** All
   - **Source:** Network -> **Main Network**
   - **Destination:** Network -> **Media Network**
3. **Important:** Ensure this rule is positioned **above** any "Block IoT to Main" or "Deny All" rules in the list.

---

4. Troubleshooting

IGMP Snooping

If devices still do not appear, ensure **IGMP Snooping** is enabled on your switches for the involved VLANs:

`Settings > Wired Networks > LAN > [Edit VLAN] > IGMP Snooping`

Connection Stability

If the stream drops after a few seconds, verify that no "Block Media to Main" ACL is interfering with the return handshake. On stateful gateways like the ER8411, the rule in Step 3 is typically sufficient.

```
Config applied: Cross-VLAN mDNS & Gateway ACL
Status: Active
```

```
Environment: TP-Link Omada SDN
```

TP-Link Omada

Configuring an IoT VLAN on TP-Link Omada SDN (Wi-Fi 7 Environment)

Isolating Internet of Things (IoT) devices on a dedicated VLAN is a fundamental network security practice. Smart home devices, sensors, and appliances often utilize weaker security protocols and receive infrequent firmware updates, making them vulnerable if breached.

This guide details the best-practice setup for an IoT VLAN using the TP-Link Omada Software-Defined Networking (SDN) platform, specifically tailored for environments utilizing tri-band Wi-Fi 7 Access Points.

Prerequisites

- An Omada Software or Hardware Controller (v5.9 or newer recommended).
- An Omada-compatible Router/Gateway and Switch.
- Tri-band Wi-Fi 7 Omada Access Points (e.g., EAP773, EAP783, EAP789).

Step 1: Create the IoT Local Area Network (LAN)

First, establish a logical network foundation to assign IP addresses that are entirely separate from those of your trusted personal devices.

1. Navigate to **Settings** > **Wired Networks** > **LAN**.
2. Click **Create New LAN**.
3. Configure the following settings:
   - **Purpose:** VLAN
   - **Name:** `IoT_VLAN`
   - **VLAN ID:** Choose a unique ID (e.g., `40`).
   - **Gateway/Subnet:** Enter a dedicated subnet (e.g., `10.0.40.1/24`).
   - **DHCP Server: Enable**. Ensure the DHCP range does not overlap with your main LAN.

4. Click **Save**.

Step 2: Create the Dedicated IoT Wireless Network

IoT devices are notoriously sensitive to modern Wi-Fi standards. The cutting-edge features of your Wi-Fi 7 APs must be carefully managed for this specific SSID to ensure compatibility and network stability.

1. Navigate to **Settings** > **Wireless Networks** > **WLAN**.
2. Click **Create New Wireless Network**.
3. Configure the following basic settings:
   - **Network Name (SSID):** `IoT-Network`
   - **Band:** Select **2.4 GHz** only. *(Note: You may enable 5 GHz if you have high-bandwidth devices like 4K video doorbells, but 2.4 GHz provides the widest compatibility for standard smart plugs and sensors.*
4. Configure Wi-Fi 7 and Security Settings:
   - **6 GHz: Leave unchecked.** Legacy IoT devices lack the hardware to see this spectrum, and enabling it can cause broadcasting overhead.
   - **MLO (Multi-Link Operation): Disable**. MLO allows devices to connect across multiple bands simultaneously. Cheaper IoT microcontrollers often fail to associate when MLO is broadcast on the SSID.
   - **Security: WPA2-Personal**. While WPA3 is the modern standard, many IoT devices will fail to connect to a WPA3 or WPA2/WPA3 transition network due to Protected Management Frame (PMF) requirements.
5. Expand **Advanced Settings**:
   - **VLAN:** Enable and enter the VLAN ID created in Step 1 (e.g., `40`).
6. Click **Save**.

Step 3: Implement Access Control Lists (ACLs)

By default, Omada routers allow inter-VLAN routing. To properly isolate the IoT devices, you must restrict traffic using Gateway ACLs.

Navigate to **Settings** > **Network Security** > **ACL** > **Gateway ACL**. Create the following rules in this exact top-to-bottom order:

1. **Permit Gateway Services (DNS/DHCP):**
   - **Direction:** LAN -> LAN
   - **Policy:** Permit
   - **Protocols:** UDP
   - **Source:** Network -> `IoT_VLAN`
   - **Destination:** IP Port Group -> Create a group for your Gateway IP (e.g., `10.0.40.1`) on Ports `53` (DNS) and `67` (DHCP).
2. **Deny Gateway Web UI Access:**
   - **Direction:** LAN -> LAN
   - **Policy:** Deny
   - **Protocols:** TCP
   - **Source:** Network -> `IoT_VLAN`
   - **Destination:** IP Port Group -> Gateway IP on Ports `80`, `443`, and `22`.
3. **Deny IoT to the Main LAN:**
   - **Direction:** LAN -> LAN
   - **Policy:** Deny
   - **Protocols:** All
   - **Source:** Network -> `IoT_VLAN`
   - **Destination:** Network -> `Main_LAN` (and any other trusted VLANs).
   - *Note: Omada's stateful firewall automatically allows return traffic for connections initiated by devices on your Main LAN, meaning you can still control your smart devices from your trusted network.*

Step 4: Configure mDNS Reflection (Optional)

If you have casting devices (Chromecast, Apple TV) or smart speakers (Sonos) on the IoT VLAN, devices on your Main LAN won't be able to discover them unless mDNS reflection is enabled.

1. Navigate to **Settings** > **Services** > **mDNS**.
2. **Enable** the mDNS service.
3. Select the **Bonjour** service.
4. Select both your `Main_LAN` and `IoT_VLAN` under the Client and Server networks.
5. Click **Save**.

Verification

You can verify that your WLAN configuration is correctly mapped to the appropriate VLAN and that Wi-Fi 7 features are properly disabled using the controller's CLI.

```
# Example output verifying WLAN to VLAN mapping and radio status
show wlan ssid "IoT-Network"

Status       : Active
VLAN ID      : 40
Security     : WPA2-PSK
Radios       : 2.4GHz
6GHz         : Disabled
MLO          : Disabled
```

TP-Link Omada

Configuring NordVPN Kill Switch & Strict VLAN Isolation

This article outlines the procedure to ensure that a specific VLAN (SecureLAN) remains permanently connected to NordVPN. The configuration prevents "IP leaks" by dropping all traffic when the VPN tunnel disconnects and by ensuring the network cannot communicate with any other local VLANs.

Hardware Note: These steps were verified on the TP-Link Omada ER8411 Gateway.

Step 1: Configure VPN Client Auto-Routing

First, ensure the VPN tunnel is established and that the specific network is routed through it.

Settings > VPN > VPN Client - Profile Name: NordOpenVPN - VPN Type: OpenVPN - Interface: SFP+ WAN1 - Local Network Type: Network - Local Networks: SecureLAN (Checked)

Step 2: Implement the VPN Kill Switch (Gateway ACL)

Because Omada evaluates virtual VPN interfaces separately from physical WAN interfaces, we can create a "Deny" rule for the physical WAN. This acts as a kill switch: if the VPN tunnel drops, the traffic attempts to hit the WAN directly and is immediately blocked.

Settings > Network Security > ACL > Gateway ACL - Name: KS_SecureLAN_Drop - Status: Enable - Direction: LAN -> WAN - Policy: Deny - Protocols: All - Source: Network -> SecureLAN - Destination: IP Group -> IPGroup_Any

Step 3: Enforce Strict VLAN Isolation

To ensure the SecureLAN cannot reach any other internal networks (Main, IoT, Media, etc.), a LAN-to-LAN restriction is required.

Settings > Network Security > ACL > Gateway ACL - Name: Block_SecureLAN_to_VLANs - Status: Enable - Direction: LAN -> LAN - Policy: Deny - Protocols: All - Source: Network -> SecureLAN - Destination: Network -> [Select: Main, IoT-Network, Media Network, Remote]

Verification & Testing

To verify the "Kill Switch" functionality:

1. Connect a device to the **SecureLAN**.
2. Confirm internet access and verify the public IP matches a NordVPN server.
3. Navigate to **VPN > VPN Client** and temporarily toggle the **Status** of the "NordOpenVPN" profile to **Off**.
4. Attempt to load a webpage on the client device. The connection should fail immediately (timed out), confirming the **KS_SecureLAN_Drop** ACL is working.