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.

Revision #1
Created 2026-03-28 21:40:39 UTC by Francis
Updated 2026-03-28 21:41:32 UTC by Francis