Secure Client TND Manual VPN Connection Behavior and URL Blocking Considerations

Contents

Issue

When using a VPN profile with the Trusted Network Detection (TND) feature configured with the Trusted Network setting set to **Disconnect**, endpoints located within the Trusted Network can still successfully establish a VPN connection when users manually initiate connections using Cisco Secure Client.

This behavior occurs despite the TND configuration being set to disconnect VPN sessions when the endpoint is detected on a trusted network.

The specific concerns identified include:

- Manual VPN connections from Trusted Network endpoints cannot be controlled or blocked through standard TND configuration
- Uncertainty about whether Cisco Secure Access (CSA) settings can block manual VPN connections from Trusted Network endpoints
- Questions about the stability of the VPN profile connection URL (xxxx.vpn.sse.cisco.com) and whether it changes periodically, which could affect firewall-based blocking strategies

Environment

- Cisco Secure Access (CSA) deployment
- Cisco Secure Client with VPN profile configuration
- Trusted Network Detection (TND) feature enabled
- TND Trusted Network setting configured as **Disconnect**
- Endpoints located within configured Trusted Network
- Firewall infrastructure for network access control

Resolution

Understand TND Behavior with Manual VPN Connections

The observed behavior is consistent with documented Cisco Secure Client functionality. According to Cisco documentation, TND does not disconnect or prevent a VPN session that a user manually starts while on a Trusted Network. This is the expected behavior regardless of the TND configuration settings.

The key technical facts are:

- TND automatic disconnect functionality applies only to automatically established VPN connections.
- Manual VPN connections initiated by users bypass the TND disconnect behavior.
- No CSA configuration setting exists to block manual VPN connections from Trusted Network endpoints.

Operational Mitigation Strategy

The primary method for controlling manual VPN conections from Trusted Network endpoints is through network-level controls:

Step 1: Implement Firewall URL Blocking: Configure the Trusted Network firewall to block access to the VPN profile connection URL (xxxx.vpn.sse.cisco.com). This prevents endpoints on the Trusted Network from reaching the VPN service endpoint.

Step 2: Verify URL Stability: The VPN Profile URL identifier (the **xxxx** portion) is tenant-specific and is not expected to change periodically. This provides a stable target for firewall blocking rules.

Validation and Testing

Testing has confirmed that blocking the VPN profile connection URL at the Trusted Network firewall successfully prevents endpoints from establishing VPN connections, even when users attempt manual connections through Cisco Secure Client.

Cause

This behavior is by design in Cisco Secure Client TND implementation. The TND feature is specifically designed to manage automatic VPN connections based on network trust status, but it intentionally does not interfere with user-initiated manual VPN connections. This design allows users to override automatic behavior when necessary while still providing automated network detection and connection management for typical use cases.

Related Content

- Cisco Secure Client Administrator Guide - TND Configuration
- Cisco Technical Support & Downloads