Secure Access ZTNA Configuration Sync Error with SSL Decryption and Network Tunnels

Contents

Issue

Cisco Secure Client Zero Trust Access (ZTA) successfully enrolls, but fails during configuration synchronization with HTTP 502 responses and "BadResponse" server connectivity state. The DART logs from the Windows 11 endpoint show successful enrollment but repeated configuration sync failures. The issue occurs only when the endpoint is connected to the corporate network path using Secure Access/Umbrella proxy with Meraki AutoVPN tunnels, while the same endpoint successfully completes configuration sync on a home network without proxy or tunnel infrastructure.

Environment

- Cisco Secure Client ZTA version 5.1.16.4434
- Windows 11 Enterprise endpoint
- Meraki MX appliances with AutoVPN integration
- Secure Access (SSE) with Network Tunnels Gateway (NTG)
- Umbrella DNS and Secure Access Web Security
- SSL decryption and HTTPS inspection enabled on corporate network path
- System Provided Do Not Decrypt List (DND) not initially configured

Resolution

The configuration sync failure was resolved by implementing proper SSL decryption bypasses for ZTA-related domains when using Network Tunnels with Secure Access.

Step 1: Identify SSL Decryption Impact

Verify that SSL decryption is causing the configuration sync failures by reviewing Activity Search logs in Secure Access for decryption events related to ZTA domains.

Step 2: Configure System Provided DND list

When using Network Tunnels Gateway (NTG) with Secure Access, the System Provided DND must be enabled to properly bypass ZTA-related traffic from SSL inspection.

Navigate to **Secure Access Dashboard > Secure > Do Not Decrypt Lists** and modify the System Provided Do Not Decrypt List.

Step 3: Create Security Profile for ZTA Domains

Add the required ZTA-related domains to a new Security Profile using the System Provided DND List:

- zpc.sse.cisco.com
- *.zpc.sse.cisco.com
- ztna.sse.cisco.com
- acme.sse.cisco.com
- devices.api.umbrella.com

Step 4: Apply Security Profile to Testing Rule

Assign the newly created Security Profile containing the ZTA domain bypasses to a testing rule to validate the configuration.

Step 5: Validate Configuration Sync

Test ZTA enrollment and configuration sync from the corporate network. The sync can now complete

successfully without HTTP 502 errors.

Step 6: Coordinate with Meraki Team

For comprehensive coverage, coordinate with Meraki support to validate official ZTA-related URLs and domains that can be bypassed from Secure Access inspection. Reference these Meraki documentation:

- Upstream Firewall Rules for Cloud Connectivity
- Meraki Dashboard URL Update - PCI Compliance

Cause

The configuration sync failure was caused by SSL decryption and proxying of Zero Trust Access traffic on the corporate network. When Network Tunnels Gateway (NTG) is used with Secure Access, ZTA-related domains must be bypassed using the System Provided Do Not Decrypt List (DND). Without this bypass configuration, SSL inspection modifies certificate chains and interferes with ZTA control plane communication, causing the client to receive HTTP 502 responses during configuration synchronization attempts.

Related Content

- Troubleshoot Secure Access Decryption and SSL Issues
- Secure Access Zero Trust Client-Based Enrollment Services
- ZTA Domain Requirements for Secure Access
- Troubleshoot Secure Access Error Enrollment Issues
- Secure Client Configuration Sync Error Troubleshooting
- Collect Detailed ZTNA Logs for Troubleshooting
- Cisco Technical Support & Downloads