Secure Client ZTNA DNS Resolution and Connectivity Loss After macOS Hibernation

Contents

Issue

Cisco SecureClient ZTNA on macOS endpoints experiences DNS resolution failure and ZTA connectivity loss after the system resumes from sleep or hibernation mode. This issue affects both ZTNA IA (Identity Access) and ZTNA PA (Private Access) functionality. While basic IP connectivity remains functional (ICMP ping to external IP addresses like 8.8.8.8 and 208.67.222.222 works successfully), DNS name resolution fails completely, preventing access to both internet resources and private resources configured through ZTNA.

The specific symptoms observed include:

- DNS lookups fail using nslookup commands (like nslookup of www.cisco.com via 8.8.8.8 and 208.67.222.222 does not work).
- ZTNA IA and ZTNA PA connections become unavailable.
- Issue occurs consistently after endpoint hibernation and wake-up cycles.
- Issue can also occur randomly while the device is in active use.
- Killing the ZTNA process results in immediate restart, but the connectivity issue typically persists.
- Only a complete system reboot restores full DNS resolution and ZTNA connectivity.

Environment

- Operating System: macOS (version 26.3 documented in case)
- Cisco SecureClient: Version 5.1.14.x (affected versions prior to 5.1.16)
- ZTNA Module: Active with both Identity Access (IA) and Private Access (PA) configurations
- Network Monitoring: Can include third-party security solutions like Sentinel One
- Additional Security Software: Can include Cisco Secure Endpoint

- DNS Servers: External DNS servers (8.8.8.8, 208.67.222.222) accessible via ICMP but DNS resolution fails
- UMB Module: Not in use

Resolution

The issue was resolved through a software fix provided by Cisco Engineering. The resolution process involved the steps described in the next sections.

Step 1: Issue Identification and Bug Tracking

Cisco Engineering identified this as a known defect and logged it under Cisco bug ID CSCwt24392 with the description "macOS: DNS stops working with ZTA SIA-all and NVM active".

Step 2: Diagnostic Data Collection

This diagnostic information was collected to support the engineering analysis:

- DART (Diagnostic and Reporting Tool) bundles from affected endpoints.
- Packet capture files (ZTNA Issue1.pcapng).
- Screenshots demonstrating the connectivity failure.
- Screen recordings showing the issue reproduction.
- Process interaction logs showing com.cisco.secureclient.zta.app.service and system extension process behavior.

Step 3: Engineering Fix Development

Cisco Engineering developed a targeted fix for CSCwt24392 and included it in SecureClient release version 5.1.16. The fix specifically addresses the DNS resolution failure that occurs when ZTA SIA-all and NVM are active on macOS systems after sleep/hibernation cycles.

Step 4: Software Update Installation

Install Cisco SecureClient version 5.1.16 or later on affected macOS endpoints. This version contains the fix for the DNS resolution and ZTA connectivity issues.

Step 5: Validation Testing

After installing SecureClient 5.1.16, perform these validation steps:

1.- Allow the macOS endpoint to enter sleep or hibernation mode.

2.- Wake the system from sleep or hibernation.

3.- Test DNS resolution using nslookup commands.

4.- Verify ZTNA IA and ZTNA PA connectivity to configured resources.

5.- Confirm that both internet access and private resource access function properly without requiring a system reboot.

Workaround for Earlier Versions

For environments where immediate upgrade to SecureClient 5.1.16 is not possible, this temporary workaround can be used:

- Perform a complete system reboot after each sleep/hibernation cycle to restore DNS resolution and ZTNA connectivity.
- Consider unenrolling from ZTNA temporarily if the sleep/hibernation issue significantly impacts productivity (note that this removes ZTNA protection).

Cause

The root cause of this issue is a software defect in Cisco SecureClient versions prior to 5.1.16, specifically tracked as Cisco bug ID CSCwt24392. The defect occurs when the ZTA (Zero Trust Access) SIA-all

(Secure Internet Access) and NVM (Network Visibility Module) components are active on macOS systems. During the sleep or hibernation and wake cycle, these components fail to properly restore DNS resolution functionality, while maintaining basic IP connectivity. This creates a state where ICMP traffic (ping) functions normally, but DNS queries fail, effectively blocking access to internet resources and ZTNA-protected private resources. The issue involves improper interaction between the com.cisco.secureclient.zta.app.service process and the system extension process during system state transitions.

Related Content

- Cisco Bug ID CSCwt24392 - macOS: DNS stops working with ZTA SIA-all and NVM active
- Cisco Technical Support & Downloads