Secure Access Intermittent Disconnects behind Corporate Firewalls with IdleTimeout Errors

Contents

- Issue
- Environment
- Resolution
  - Step 1: Implement MX TTL Buffer Configuration
  - Step 2: Configure Required Domain Exclusions
  - Step 3: Verify Port and Protocol Allowances
  - Step 4: Monitor and Validate Resolution
- Cause
- Related Content

Issue

Cisco Secure Access clients experience intermittent disconnects and immediate reconnects when endpoints are connected to the corporate network. The disconnections occur randomly, with the client reconnecting automatically after approximately 5 seconds. This behavior is observed when internet traffic is proxied via Zero Trust Access (ZTA) to Secure Access from endpoints positioned behind Cisco FirePower and Meraki MX devices.

The Windows event log captures specific "idleTimeout" errors during these disconnect events. The disconnection pattern does not occur when users connect from home internet connections, indicating the issue is specifically related to the corporate network infrastructure.

The symptom creates business disruption to secure remote access connectivity for users operating within the corporate network environment, while remote users remain unaffected by this connectivity issue.

Environment

- Cisco Secure Access - Advantage deployment
- Cisco Secure Internet Access (SIA) client software
- Corporate network infrastructure with Cisco FirePower security appliances
- Meraki MX security appliances in the network path
- Zero Trust Access (ZTA) configuration proxying internet traffic to Secure Access
- Windows endpoints with event logging capability
- Mixed connectivity scenarios: corporate network (affected) and home internet connections (unaffected)

Resolution

The resolution involved implementing configuration changes on the Meraki MX device and ensuring proper domain exclusions and port allowances for Secure Access integration.

Step 1: Implement MX TTL Buffer Configuration

Configure an MX TTL buffer on the Meraki MX device to address the DNS TTL caching behavior that was contributing to the intermittent disconnect issues. This configuration change resolves the timing conflicts between DNS resolution caching and the Secure Access client connectivity expectations.

Step 2: Configure Required Domain Exclusions

Ensure these domains are properly excluded from interception and added to non-decrypt lists on both Cisco FirePower and Meraki MX devices:

- ztna.sse.cisco.com
- zpc.sse.cisco.com
- Additional Secure Access service domains as identified in the policy configuration

Step 3: Verify Port and Protocol Allowances

Configure the corporate firewall infrastructure to allow required Secure Access ports and protocols through both FirePower and Meraki MX devices. Ensure that traffic to port 443 for Secure Access service endpoints is properly handled without interference from security inspection that could cause timeout conditions.

Step 4: Monitor and Validate Resolution

After implementing the MX TTL buffer configuration, monitor the Secure Access client behavior for several days to confirm that the intermittent disconnect and reconnect pattern has ceased.

Cause

The intermittent disconnects were caused by DNS TTL (Time To Live) caching behavior conflicts between the corporate network infrastructure and Secure Access service expectations. The Cisco engineering analysis revealed that DNS TTL values vary due to resolver caching behavior, and alternating IP addresses are expected behavior due to load balancing mechanisms in the Secure Access service architecture.

When corporate network devices (Cisco FirePower and Meraki MX) processed DNS responses for Secure Access endpoints, the caching and TTL handling created timing mismatches that resulted in "idleTimeout" conditions. This timing conflict caused the Secure Access client to interpret the connection as idle and initiate disconnect/reconnect cycles.

The issue was specific to corporate network environments because home internet connections typically do not implement the same level of DNS caching and traffic inspection that can interfere with Secure Access client connection state management.

Related Content

- Cisco Technical Support & Downloads