

Secure Client Umbrella Module Becomes Inactive Due to Codex Application DNS Storm

Contents

Issue

Multiple users on macOS experience the Cisco Secure Client Umbrella roaming module intermittently transitioning to an inactive (fail-open) state. During these periods, DNS requests, including terminal-initiated **nslookup** commands, fail to reach the network layer, impacting users' ability to resolve domains and access internet-based resources.

The issue manifests with repeated probe failures in Umbrella logs, showing messages such as:

```
Transparent probe failed
Encrypted probe failed
Switching to basic probe
DNS probe failed by timeout - going open
```

Analysis revealed that the acsock driver crashes during the same failure window when Umbrella becomes inactive. The issue is most frequently observed while users are actively using Codex and AI Assistant applications, with a high volume of connection attempts to chatgpt.com immediately after commands sent to CODEX.

Environment

- Cisco Secure Client versions 5.1.13, 5.1.16, 5.1.17
- macOS (multiple versions observed)
- Umbrella Roaming Module enabled
- ZTNA/Secure Internet Access (SIA) module enabled
- Codex application in use
- Users working from various networks (home, office, different ISPs)

Resolution

The issue was resolved by implementing domain bypass configurations to prevent DNS request duplication. The approaches described in the next sections were validated.

Primary Resolution: Domain Bypass

- Step 1: Add chatgpt.com to the bypass list in the Cisco Secure Access configuration. This prevents the Secure Client from duplicating DNS requests generated by the Codex application, eliminating the DNS storm that causes driver instability.
- Step 2: Verify the bypass configuration. Test Codex functionality to confirm that the issue no longer reproduces with the bypass in place.

Alternative Resolution: Codex Configuration Workaround

Apply the Codex configuration changes referenced in the GitHub issue to reduce the volume of DNS requests generated by the application. <https://github.com/openai/codex/issues/21218>

Advanced Troubleshooting Steps Used

These diagnostic steps were performed to identify the root cause.

1.- Enable verbose acsock logging:

```
sudo /opt/cisco/secureclient/kdf/bin/acsocktool -sdf 0x830801F2
```

2.- Reproduce the issue and collect DART bundle immediately after failure.

3.- Disable verbose logging:

```
sudo /opt/cisco/secureclient/kdf/bin/acsocktool -cdf
```

4.- Enable maximum debug logging for SWG. Create SWGConfigOverride.json file with content:

```
{"logLevel": "1"}
```

Save to /opt/cisco/secureclient/umbrella/swg/SWGConfigOverride.json.

5.- Enable RSM trace logs for DNS. Create force_log_level.plist file with content:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>logLevel</key>
<string>trace</string>
</dict>
</plist>
```

Save to /opt/cisco/secureclient/umbrella/data.

Cause

The core issue is related to Codex application behavior, which generates a very high volume of DNS requests. When chatgpt.com is not bypassed, these requests are effectively duplicated by the Cisco Secure Client, creating a DNS storm that leads to high CPU usage and acsock kernel driver instability.

The problem occurs because:

- Codex generates numerous DNS queries to chatgpt.com during operation.
- Without bypass configuration, Secure Client intercepts and duplicates these requests.
- The high volume of duplicated DNS requests causes the acsock driver to crash.
- Driver instability results in Umbrella probe failures and transition to fail-open state.

When chatgpt.com is bypassed or the Codex workaround is applied, this duplication does not occur and the issue no longer reproduces. The issue affects both Umbrella-only and ZTNA SIA configurations, indicating the problem lies within the traffic handling mechanism rather than a specific module.

Related Content

- [Troubleshoot Secure Access Roaming Module](#)
- [Troubleshoot and Collect Basic Information](#)
- [Cisco Technical Support & Downloads](#)