Internet Access Fails When Secure Client Umbrella SWG Agent Service Is Active

Contents

Issue

When the Cisco Secure Client – Umbrella SWG Agent service is running on a Windows Dell laptop, users are unable to access any websites. Once the Umbrella SWG Agent service is stopped, normal web access is restored. The issue occurs with Cisco Secure Client version 5.1.14.145, which includes both AnyConnect VPN and Umbrella modules. The OrgInfo.json file is present in the expected directory and the Cisco Secure Access Root CA certificate is installed in the trusted root certificate store.

Environment

- Product: Cisco Secure Client (AnyConnect VPN and Umbrella modules)
- Software Version: 5.1.14.145
- Operating System: Windows (Dell laptop)
- Umbrella SWG Agent service enabled/disabled
- OrgInfo.json present in `%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json`
- Cisco Secure Access Root CA installed in Trusted Root Certification Authorities store
- DNS/Web Security enabled in Secure Access dashboard
- Assigned Security Profile with Decryption enabled

Resolution

The issue was resolved by identifying and correcting a Network Time Protocol (NTP) synchronization failure on the

Follow this comprehensive troubleshooting workflow.

Step 1: Verify Configuration and Prerequisites

- Ensure `OrgInfo.json` is located in `%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json`.
- Confirm Cisco Secure Access Root CA is present in the Trusted Root Certification Authorities store.
- Check that DNS/Web Security is enabled in the Secure Access dashboard.
- Verify the assigned Security Profile has Decryption enabled.

Step 2: Capture and Analyze Network Traffic

Obtain a packet capture of client traffic directed to the SWG proxy to identify abnormal behaviors, such as unexpect

Description of the packet capture showing issue:

```
The packet capture revealed that TCP reset (RST) packets were being sent to the client, disrupting the
```

Step 4: Validate Perimeter Firewall Rules

- Inspect perimeter firewall rules to ensure traffic to and from SWG servers is permitted on the ingress interface

Step 5: Run System and Protocol Diagnostics

Execute this command on the client to check for NTP synchronization errors:

```
curl ipinfo.io
```

Description of the diagnostic result:

```
The output indicated NTP timing was out of sync on the client device.
```

Cause

The root cause was a failure in NTP (Network Time Protocol) synchronization on the client device. This timing issue prevented secure communication between the client and the Umbrella SWG proxy service, resulting in TCP reset packets and loss of web access when the SWG Agent service was active. Resolving the NTP synchronization issue restored proper operation of the Umbrella SWG Agent, allowing web traffic to be proxied securely.

Related Content

- Cisco Technical Support & Downloads