

Der Internetzugriff schlägt fehl, wenn der SWG-Agent-Dienst des sicheren Clients aktiv ist.

Inhalt

Problem

Wenn der Cisco Secure Client - Umbrella SWG Agent-Dienst auf einem Windows Dell-Laptop ausgeführt wird, können Benutzer nicht auf Websites zugreifen. Sobald der Umbrella SWG Agent Dienst beendet ist, wird der normale Webzugriff wiederhergestellt. Das Problem tritt bei Cisco Secure Client Version 5.1.14.145 auf, die sowohl AnyConnect VPN- als auch Umbrella-Module enthält. Die Datei OrgInfo.json befindet sich im erwarteten Verzeichnis, und das Zertifikat der Cisco Secure Access-Stammzertifizierungsstelle wird im Speicher für vertrauenswürdige Stammzertifikate installiert.

Umwelt

- Produkt: Cisco Secure Client (AnyConnect VPN- und Umbrella-Module)
- Software-Version: 5.1.14.145
- Betriebssystem: Windows (Dell Notebook)
- Umbrella SWG Agent-Dienst aktiviert/deaktiviert
- OrgInfo.json vorhanden in %ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json
- Cisco Secure Access Root-Zertifizierungsstelle im Speicher vertrauenswürdiger Stammzertifizierungsstellen installiert
- DNS-/Websicherheit im Dashboard für sicheren Zugriff aktiviert
- Zugewiesenes Sicherheitsprofil mit aktivierter Entschlüsselung

Auflösung

Das Problem wurde behoben, indem ein NTP-Synchronisierungsfehler (Network Time Protocol) auf dem Clientgerät identifiziert und korrigiert wurde. Die fehlende Synchronisierung verhinderte eine sichere Kommunikation, die vom Umbrella SWG Agent für das Proxyen von Webdatenverkehr erforderlich war. Dies führte zu TCP-Reset-Paketen (RST) und dem Verlust des Webzugriffs. Nach der Wiederherstellung der NTP-Synchronisierung funktionierte der Webzugriff normal mit dem aktiven SWG Agent.

Befolgen Sie diesen umfassenden Workflow zur Fehlerbehebung.

Schritt 1: Überprüfen der Konfiguration und der Voraussetzungen

- Stellen Sie sicher, dass sich OrgInfo.json in

%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json befindet.

- Bestätigen Sie, dass die Cisco Secure Access Root-Zertifizierungsstelle im Speicher der vertrauenswürdigen Stammzertifizierungsstellen vorhanden ist.
- Überprüfen Sie, ob DNS/Web Security im Dashboard für sicheren Zugriff aktiviert ist.
- Überprüfen Sie, ob Entschlüsselung für das zugewiesene Sicherheitsprofil aktiviert ist.

Schritt 2: Erfassen und Analysieren des Netzwerkverkehrs

Abrufen einer Paketerfassung des Client-Datenverkehrs, der an den SWG-Proxy weitergeleitet wird, um ungewöhnliches Verhalten wie unerwartete TCP-Reset-Pakete zu identifizieren

Beschreibung der Paketerfassung mit dem Problem:

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

Schritt 4: Firewall-Regeln am Perimeter validieren

- Überprüfen Sie die Perimeter-Firewall-Regeln, um sicherzustellen, dass Datenverkehr zu und von SWG-Servern an der Eingangsschnittstelle zulässig ist.

Schritt 5: System- und Protokolldiagnose ausführen

Führen Sie diesen Befehl auf dem Client aus, um auf NTP-Synchronisierungsfehler zu überprüfen:

```
curl ipinfo.io
```

Beschreibung des Diagnoseergebnisses:

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

Ursache

Die Ursache war ein Fehler bei der NTP-Synchronisierung (Network Time Protocol) auf dem Client-Gerät. Dieses Zeitproblem verhinderte eine sichere Kommunikation zwischen dem Client und dem Umbrella SWG-Proxydienst, was zu TCP-Rücksetzpaketen und zum Verlust des Webzugriffs führte, als der SWG Agent-Dienst aktiv war. Durch die Behebung des NTP-Synchronisierungsproblems wurde der ordnungsgemäße Betrieb des Umbrella SWG Agents wiederhergestellt, sodass ein sicheres Proximieren des Webdatenverkehrs möglich war.

Verwandte Inhalte

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.