Secure Client Umbrella Module - SSL/TLS-Vertrauensfehler während der Geräteregistrierung

Inhalt

Problem

Während der Einführung des Cisco Secure Client mithilfe des Umbrella-Moduls wurde die Synchronisierung der Geräte mit dem Dashboard gestoppt und als "Inaktiv" gemeldet. Bei den betroffenen Clients traten SSL/TLS-Vertrauensstellungsfehler auf, als versucht wurde, sich bei devices.api.sse.cisco.com zu registrieren. Dies verhinderte eine erfolgreiche Geräteregistrierung und die Schutzabdeckung.

Umbrella wurde mit den folgenden Statusmeldungen als inaktiv angezeigt:

- Regenschirm ist inaktiv.
- Sie sind derzeit nicht durch ein sicheres Web-Gateway geschützt.
- Das sichere Web-Gateway ist nicht lizenziert/deaktiviert.

Die Diagnoseergebnisse zeigten einen konsistenten SSL/TLS-Vertrauensfehler während der Registrierung. Diese Fehlermeldung wurde in den Protokollen des sicheren Clients angezeigt:

```
[ERROR] < 10> Device Registration: Registration failed against https://devices.api.sse.cisco.com/deploy
```

Umwelt

- Cisco Secure Client mit Umbrella-Modul für mehr als 2.000 Endgeräte
- SD-WAN-Infrastruktur mit Routing-Richtlinien

- Legacy-Umbrella-Tunnel installiert
- Netzwerkkonfiguration, die alle erforderlichen Ziele gemäß Cisco Dokumentation zulässt
- Keine SSL-Entschlüsselung aktiv für Cisco Ziele im Perimeter

Auflösung

Die Lösung bestand in der Identifizierung und Behebung eines Routing-Konfigurationsproblems, das dazu führte, dass der Geräteregistrierungsverkehr durch ältere Umbrella-Tunnel fehlgeleitet wurde.

Ursachenidentifizierung

Die Analyse der Paketerfassungsdaten ergab, dass es sich bei dem für die API-Verbindung bereitgestellten TLS-Zertifikat um ein Cisco Umbrella-Zertifikat handelte und nicht um das erwartete Cisco Secure Access-/Let's Encrypt-Zertifikat. Geben Sie die IP-Adresse für devices.api.sse.cisco.com an.

Eine weitere Untersuchung ergab eine SD-WAN-Routenrichtlinie, die mit dem Subnetz 146.112.0.0/16 übereinstimmte, was dazu führte, dass der Datenverkehr an devices.api.sse.cisco.com in ältere Umbrella-Tunnel und nicht an das beabsichtigte Ziel geleitet wurde.

Konfigurationsänderungen

Die folgenden Schritte wurden zur Behebung des Problems unternommen:

- Schritt 1: Entfernen Sie die problematischen statischen Routen. Statische Routen, die auf 146.112.0.0/16 zu den älteren Umbrella-Tunneln verweisen, wurden aus der SD-WAN-Konfiguration entfernt.
- Phase 2: Überprüfen der Verbindung Nach dem Entfernen der statischen Routen wurden die betroffenen Clients getestet, um sicherzustellen, dass sie sich erfolgreich mit devices.api.sse.cisco.com verbinden und registrieren können.

Verifizierung

Die erwartete Zertifikatskette für devices.api.sse.cisco.com sollte wie folgt angezeigt werden:

```
openssl s_client -connect devices.api.sse.cisco.com:443
CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R13
verify return:1
depth=0 CN = api.sse.cisco.com
verify return:1
---
Certificate chain
 0 s:CN = api.sse.cisco.com
   i:C = US, O = Let's Encrypt, CN = R13
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar  5 14:13:56 2026 GMT; NotAfter: Jun  3 14:13:55 2026 GMT
 1 s:C = US, O = Let's Encrypt, CN = R13
   i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT
```

Nach der Implementierung der Konfigurationsänderungen wurden die betroffenen Clients erfolgreich verbunden und registriert, und die Bereitstellung wurde erfolgreich abgeschlossen.

Ursache

Die Ursache dafür war eine SD-WAN-Routenrichtlinie, die dem Subnetz 146.112.0.0/16 entsprach, sodass der für devices.api.sse.cisco.com (146.112.59.104) bestimmte Geräteregistrierungsverkehr fälschlicherweise durch ältere Umbrella-Tunnel geleitet wurde. Dies führte zur Anzeige eines falschen TLS-Zertifikats (Cisco Umbrella-Zertifikat anstelle des erwarteten Cisco Secure Access/Let's Encrypt-Zertifikats), was zu SSL/TLS-Vertrauensfehlern während des Registrierungsvorgangs des Geräts führte.

Verwandte Inhalte

- Dokumentation der Netzwerkanforderungen für Cisco Secure Client

- 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.