Errore di trust SSL/TLS del modulo Secure Client Umbrella durante la registrazione del dispositivo

Sommario

Problema

Durante il rollout di Cisco Secure Client con il modulo Umbrella, i dispositivi hanno smesso di sincronizzarsi con il dashboard e sono stati segnalati come "Inattivi". I client interessati hanno riscontrato errori di attendibilità SSL/TLS durante il tentativo di registrazione su devices.api.sse.cisco.com, impedendo la corretta registrazione del dispositivo e la copertura di protezione.

L'interfaccia utente ha mostrato Umbrella come inattiva con questi messaggi di stato:

- Umbrella è inattiva.
- Al momento non si è protetti da un gateway Web sicuro.
- Il gateway Web protetto non è concesso in licenza / è disabilitato.

I risultati della diagnostica hanno rilevato un errore di trust SSL/TLS coerente durante la registrazione con questo messaggio di errore nei log di Secure Client:

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

Ambiente

- Cisco Secure Client con implementazione del modulo Umbrella su oltre 2.000 endpoint
- Infrastruttura SD-WAN con policy di routing
- Tunnel Umbrella legacy installati

- Configurazione della rete che consente di specificare tutte le destinazioni richieste in base alla documentazione Cisco
- Nessuna decrittografia SSL attiva per le destinazioni Cisco sul perimetro

Risoluzione

La risoluzione ha comportato l'identificazione e la correzione di un problema di configurazione del routing che stava causando un errato indirizzamento del traffico di registrazione dei dispositivi attraverso i tunnel Umbrella legacy.

Identificazione della root cause

L'analisi dei dati di acquisizione dei pacchetti ha rivelato che il certificato TLS presentato per la connessione API era un certificato Cisco Umbrella anziché il certificato Cisco Secure Access/Let's Encrypt previsto. Identificare l'indirizzo IP per devices.api.sse.cisco.com.

Un'ulteriore indagine ha identificato un criterio di route SD-WAN corrispondente alla subnet 146.112.0.0/16, che causa il routing del traffico verso devices.api.sse.cisco.com nei tunnel Umbrella legacy anziché alla destinazione prevista.

Modifiche alla configurazione

Per risolvere il problema sono state adottate le seguenti misure:

- Passaggio 1: Rimuovere le route statiche con problemi. Le route statiche che puntano a 146.112.0.0/16 verso i tunnel Umbrella legacy sono state rimosse dalla configurazione SD-WAN.
- Passaggio 2: Convalida connettività. Dopo aver rimosso le route statiche, i client interessati sono stati sottoposti a test per garantire la corretta connessione e registrazione a devices.api.sse.cisco.com.

Verifica

La catena di certificati prevista per devices.api.sse.cisco.com dovrebbe essere visualizzata come indicato:

```
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
```

Dopo l'implementazione delle modifiche alla configurazione, i client interessati si sono connessi e registrati correttamente e la distribuzione è stata completata correttamente.

Causa

La causa principale è stata una policy di route SD-WAN corrispondente alla subnet 146.112.0.0/16, che ha causato il routing errato del traffico di registrazione del dispositivo destinato a devices.api.sse.cisco.com (146.112.59.104) tramite tunnel Umbrella legacy. Di conseguenza, è stato presentato un certificato TLS errato (certificato Cisco Umbrella anziché il certificato Cisco Secure Access/Let's Encrypt previsto), che ha causato errori di attendibilità SSL/TLS durante il processo di registrazione del dispositivo.

Contenuto correlato

- Documentazione sui requisiti di rete per Cisco Secure Client
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).