

Secure Client Umbrella Module SSL/TLS-vertrouwensfout tijdens apparaatregistratie

Inhoud

uitgeven

Tijdens de uitrol van Cisco Secure Client met de Umbrella-module stopten apparaten met synchroniseren met het Dashboard en rapporteerden ze als "Inactief". De getroffen clients kregen te maken met SSL/TLS-vertrouwensfouten bij hun poging om zich te registreren op `devices.api.sse.cisco.com`, waardoor registratie en bescherming van apparaten niet succesvol waren.

De gebruikersinterface toonde Umbrella als inactief met deze statusberichten:

- De paraplu is inactief.
- U bent momenteel niet beschermd door een beveiligde webgateway.
- De beveiligde webgateway heeft geen licentie / is uitgeschakeld.

Uit de diagnostische bevindingen bleek een consistente SSL/TLS-vertrouwensfout tijdens de registratie met deze foutmelding in de logboeken van de beveiligde client:

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

milieu

- Cisco Secure Client met Umbrella-module-implementatie op meer dan 2.000 eindpunten
- SD-WAN-infrastructuur met routebeleid
- Legacy paraplu tunnels op zijn plaats

- Netwerkconfiguratie die alle vereiste bestemmingen per Cisco-documentatie mogelijk maakt
- Geen SSL-decodering actief voor Cisco-bestemmingen op perimeter

resolutie

De oplossing betrof het identificeren en corrigeren van een probleem met de routeringsconfiguratie waardoor het apparaatregistratieverkeer verkeerd werd geleid door oudere paraplutunnels.

identificatie van de hoofdoorzaak

Analyse van pakketregistratiegegevens toonde aan dat het TLS-certificaat dat werd gepresenteerd voor de API-verbinding een Cisco Umbrella-certificaat was in plaats van het verwachte Cisco Secure Access/Let's Encrypt-certificaat. Identificeer het IP-adres voor `devices.api.sse.cisco.com`.

Verder onderzoek wees uit dat er een SD-WAN-routebeleid was dat overeenkwam met het subnet `146.112.0.0/16`, waardoor het verkeer naar `devices.api.sse.cisco.com` werd geleid naar bestaande paraplutunnels in plaats van de beoogde bestemming.

Configuratiwijzigingen

Deze stappen zijn genomen om het probleem op te lossen:

- Stap 1: Verwijder de problematische statische routes. Statische routes die `146.112.0.0/16` naar de oude Umbrella-tunnels wezen, werden verwijderd uit de SD-WAN-configuratie.
- Stap 2: connectiviteit valideren. Nadat de statische routes waren verwijderd, werden de getroffen klanten getest om ervoor te zorgen dat ze met succes verbinding konden maken en zich konden registreren op `devices.api.sse.cisco.com`.

Verificatie

De verwachte certificaatketen voor devices.api.sse.cisco.com moet worden weergegeven als volgt:

```
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
```

Nadat de configuratiewijzigingen zijn geïmplementeerd, hebben de getroffen clients verbinding gemaakt en geregistreerd en is de implementatie met succes voltooid.

Oorzaak

De hoofdoorzaak was een SD-WAN-routebeleid dat overeenkwam met het subnet 146.112.0.0/16, waardoor het apparaatregistratieverkeer dat bestemd was voor devices.api.sse.cisco.com (146.112.59.104) onjuist werd gerouteerd via oudere Umbrella-tunnels. Dit resulteerde in de presentatie van een onjuist TLS-certificaat (Cisco Umbrella-certificaat in plaats van het verwachte Cisco Secure Access/Let's Encrypt-certificaat), wat leidde tot SSL/TLS-vertrouwensfouten tijdens het apparaatregistratieproces.

Verwante inhoud

- [Documentatie vereisten Cisco Secure Client Network](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.