Internettoegang mislukt wanneer de Secure Client Umbrella SWG Agent-service actief is

Inhoud

uitgeven

Wanneer de Cisco Secure Client – Umbrella SWG Agent-service wordt uitgevoerd op een Windows Dell-laptop, hebben gebruikers geen toegang tot websites. Zodra de Umbrella SWG Agent-service is gestopt, wordt de normale webtoegang hersteld. Het probleem doet zich voor bij Cisco Secure Client versie 5.1.14.145, die zowel AnyConnect VPN- als Umbrella-modules bevat. Het bestand OrgInfo.json is aanwezig in de verwachte directory en het Cisco Secure Access Root CA-certificaat is geïnstalleerd in de vertrouwde rootcertificaatopslag.

milieu

- Product: Cisco Secure Client (AnyConnect VPN- en Umbrella-modules)
- Softwareversie: 5.1.14.145
- Besturingssysteem: Windows (Dell-laptop)
- Umbrella SWG Agent-service ingeschakeld/uitgeschakeld
- OrgInfo.json aanwezig in `%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json`
- Cisco Secure Access Root CA geïnstalleerd in Trusted Root Certification Authorities-archief
- DNS/webbeveiliging ingeschakeld in dashboard voor beveiligde toegang
- Toegewezen beveiligingsprofiel met decodering ingeschakeld

resolutie

Het probleem is opgelost door een NTP-synchronisatiefout op het clientapparaat te identificeren en te corrigeren. De onmogelijkheid om de tijd te synchroniseren verhinderde veilige communicatie vereist door de Umbrella SWG Agent voor proxying webverkeer, resulterend in TCP reset (RST) pakketten en verlies van toegang tot het web. Nadat de NTP-synchronisatie was hersteld, functioneerde de webtoegang normaal met de SWG Agent actief.

Volg deze uitgebreide workflow voor probleemoplossing.

Stap 1: Configuratie en vereisten controleren

- Zorg ervoor dat `OrgInfo.json` zich bevindt in `%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json`.
- Bevestig dat Cisco Secure Access Root CA aanwezig is in het archief van Trusted Root Certification Authorities.

- Controleer of DNS/Web Security is ingeschakeld in het dashboard voor beveiligde toegang.
- Controleer of decodering is ingeschakeld voor het toegewezen beveiligingsprofiel.

Stap 2: Netwerkverkeer vastleggen en analyseren

Verkrijgen van een pakketopname van clientverkeer dat is gericht op de SWG-proxy om abnormaal gedrag te identificeren, zoals onverwachte TCP-resetpakketten.

Beschrijving van het pakketafvangprobleem:

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

Stap 4: Regels voor de firewall van de perimeter valideren

- Inspecteer de firewallregels van de perimeter om ervoor te zorgen dat verkeer van en naar SWG-servers is toegestaan op de ingangsinterface.

Stap 5: Systeem- en protocoldiagnose uitvoeren

Voer deze opdracht uit op de client om te controleren op NTP-synchronisatiefouten:

```
curl ipinfo.io
```

Beschrijving van het diagnostische resultaat:

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

Oorzaak

De hoofdoorzaak was een fout in de NTP-synchronisatie (Network Time Protocol) op het clientapparaat. Dit timingprobleem voorkwam veilige communicatie tussen de client en de Umbrella SWG-proxyservice, wat resulteerde in TCP-resetpakketten en verlies van webtoegang wanneer de SWG Agent-service actief was. Door het NTP-synchronisatieprobleem op te lossen, werd de juiste werking van de Umbrella SWG Agent hersteld, waardoor webverkeer veilig kan worden benaderd.

Verwante inhoud

- 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.