Cisco Secure Client VPN Connection Reset door Peer met Zscaler SSL/TLS-decoderingsinterferentie

Inhoud

uitgeven

Een gebruiker ervaart VPN-verbindingsfouten wanneer hij probeert een verbinding tot stand te brengen met behulp van Cisco Secure Client.

milieu

- Technologie: Cisco Secure Access - Veilige externe clienttoegang (VPN, houding, privébron)
- Productfamilie: SECACS
- Besturingssysteem: macOS (gebaseerd op logbestandspaden met /Users/admin/workspace/secure-client-macos_Raccoon_MR.15/)
- Software van derden: Zscaler geïnstalleerd op het clientsysteem
- VPN-protocol: CSTP (Cisco SSL Tunnel Protocol)
- TLS-versie: TLS 1.3 met codering TLS_AES_256_GCM_SHA384

resolutie

De oplossing omvat het identificeren en aanpakken van het conflict tussen Cisco Secure Client en de SSL/TLS-decoderingsfunctionaliteit van Zscaler.

Stap 1: Loganalyse en diagnose

Leg de DART-logs van de Cisco Secure Client vast en analyseer deze om het patroon van verbindingsfouten te identificeren. De logs tonen een succesvolle instelling van de TLS-sessie, gevolgd door een onmiddellijke reset van de verbinding.

Belangrijke diagnostische indicatoren in de logs:

- TLS 1.3-verbindingsinrichting met codering TLS_AES_256_GCM_SHA384
- MTU-berekening en HTTP-onderhandelingsprocedure normaal
- Verbindingsreset door peer-fout (Retourcode: 54) tijdens socketleesbewerking

De TLS 1.3-sessie wordt succesvol tot stand gebracht met behulp van het cijfer TLS_AES_256_GCM_SHA384, maar onmiddellijk na het instellen van de sessie wordt een resetpakket verzonden dat de verbinding beëindigt, waardoor de VPN-tunnel wordt afgebroken. De specifieke fout die in de logs wordt waargenomen, toont "Connection reset by peer" met retourcode 54 (0x00000036) tijdens de socketleesbewerking.

De volgende foutvolgorde treedt op tijdens verbindingspogingen:

```
2026-03-11 10 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] A TLS 1.3 conne
2026-03-11 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function: calculat
2026-03-11 17:01:48. vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function
2026-03-11 17:01:48.356 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Funct
```

Stap 2: Software-identificatie van derden

Onderzoek de aanwezigheid van beveiligingssoftware van derden die mogelijk SSL/TLS-inspectie of -decodering uitvoert op het clientsysteem. In dit geval werd Zscaler geïdentificeerd als de interfererende toepassing.

Stap 3: SSL/TLS-decodering conflictoplossing

Het conflict tussen Cisco Secure Client VPN-verkeer en de SSL/TLS-decoderingsfunctionaliteit van Zscaler oplossen. Het VPN-verkeer lijkt SSL/TLS-decodering door Zscaler te ondergaan, wat de VPN-tunnelinstelling verstoort en de verbinding reset.

Potentiële afwikkelingsbenaderingen omvatten:

- Zscaler configureren om Cisco Secure Client VPN-verkeer uit te sluiten van SSL/TLS-inspectie
- Bypass-regels maken in Zscaler voor de VPN-servereindpunten
- Schakel Zscaler tijdelijk uit tijdens het testen van de VPN-verbinding om het conflict te bevestigen
- Coördineren met het netwerkbeveiligingsteam om de juiste uitsluitingen vast te stellen

Oorzaak

De hoofdoorzaak van dit probleem is een conflict tussen Cisco Secure Client VPN-verkeer en de SSL/TLS-decoderingsfunctionaliteit van Zscaler. Wanneer Zscaler probeert het TLS-verkeer van de VPN te decoderen of te inspecteren, interfereert het met het beveiligde tunneloprichtingsproces. Deze interferentie manifesteert zich als een verbindingsreset onmiddellijk nadat de TLS-sessie is ingesteld, waardoor de VPN-tunnel de onderhandelingsfase niet kan voltooien. De timing van het resetpakket (direct na succesvolle TLS-instelling maar vóór tunnelvoltooiing) is kenmerkend voor SSL/TLS-inspectieinterferentie van beveiligingsapparaten of -software.

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.