Secure Access Network Tunnel Group Interne serverfout Primaire peer-IP terugzetten

Inhoud

uitgifte

Wanneer gebruikers proberen het externe peer-IP in een Network Tunnel Group (NTG) op Cisco Secure Access te wijzigen, kunnen ze een "Internal Server Error" in de gebruikersinterface tegenkomen wanneer ze proberen het primaire tunnel-IP terug te zetten naar een eerder geconfigureerde waarde. Het specifieke scenario omvat:

- Een NTG is aanvankelijk geconfigureerd met een primaire IP-tunnel en secundaire IP, waarbij beide tunnels met succes zijn ingesteld.
- Het primaire IP-adres van de tunnel wordt voor testdoeleinden gewijzigd in een ander IP-adres, dat zonder problemen wordt geaccepteerd.
- Wanneer u probeert het IP-adres van de primaire tunnel terug te zetten naar de oorspronkelijke waarde, slaat het systeem de configuratie niet op en retourneert het een "Internal Server Error" in de gebruikersinterface.
- Dit gedrag is consistent reproduceerbaar en verschijnt wanneer u een eerder geconfigureerd IP-adres probeert te hergebruiken.
- Het oorspronkelijke IP werkte eerder en er zijn geen conflicten met het secundaire IP-tunnelnetwerk.

milieu

- Cisco Secure Access (voorheen Cisco Umbrella for SSE)
- Netwerktunnelgroepconfiguratie voor privétoegang
- Dubbele tunnelconfiguratie met primaire en secundaire peer-IP's
- Webgebaseerde beheerinterface

resolutie

Dit probleem wordt veroorzaakt door een back-endvalidatie/statusprobleem waarbij het oorspronkelijke peer-IP gereserveerd blijft of vastzit in het back-endsysteem nadat de configuratie is gewijzigd. De stappen voor probleemoplossing en -oplossing die in de volgende sectie worden uitgelegd, moeten worden gevolgd:

Stap 1: Verzamel diagnostische informatie

Verzamel de volgende informatie voor backend-validatie:

- ID Beveiligde toegangsorganisatie
- Netwerktunnelgroepnaam
- Tunnel-ID voor de getroffen primaire tunnel
- Regio/datacenter geselecteerd voor de NTG
- Exacte tijdstempel van een mislukte opslagpoging, inclusief tijdzone
- Bevestiging of het oorspronkelijke IP wordt weergegeven in een andere NTG, huidige of vorige
- Browser HAR-opname van de mislukte opslagpoging

Stap 2: HAR-bestand van browser vastleggen

Diagnostische gegevens verzamelen voor de mislukte opslagpoging:

- Open browser Developer Tools
- Ga naar het tabblad Netwerk
- Logboek behouden inschakelen
- De opslagfout reproduceren
- Exporteer het HAR-bestand en voeg het toe aan de ondersteuningscase

Opmerking: Reinig/verwijder sessietokens of cookies voordat u het HAR-bestand uploadt.

Stap 3: Backend-validatie en -opruiming

Dit probleem vereist backend-interventie en kan niet worden opgelost vanuit de gebruikersinterface alleen. De volgende acties moeten worden uitgevoerd door Cisco Technical Support:

- Het Secure Access-backend/SSE-platformteam inschakelen
- Valideren voor stabiele peer-IP-reservering
- Controleren op verweesde tunnelobjecten
- Dubbele back-endsleutels identificeren die zijn gekoppeld aan de specifieke NTG-configuratie
- Duidelijke stabiele tunnelpeer-referentie voor het oorspronkelijke IP
- Back-endhersynchronisatie van NTG-objecten forceren indien nodig
- Peer-IP-toewijzing vrijgeven gekoppeld aan de NTG UUID

Stap 4: Alternatieve resolutiemethode

Als back-end opruimen niet onmiddellijk beschikbaar is, probeer dan deze procedure:

- De primaire configuratie van de Netwerktunnelgroep verwijderen
- Wacht 5 minuten
- Voeg de NTG opnieuw toe met het vereiste IP-adres

Let op: mogelijk. De hier genoemde details lijken procedures of opdrachten te bevatten die aanzienlijke gevolgen kunnen hebben als ze worden uitgevoerd. Controleer of de bovenstaande procedures of opdrachten door een kmo of bedrijfseenheid zijn geëvalueerd voordat u ze uitvoert of aanbeveelt.

Stap 5: Tijdelijke workaround

Als de NTG in productie is en niet kan worden verwijderd:

- Doorgaan met het gebruik van de secundaire tunnel voor connectiviteit
- Vraag een alternatief openbaar IP-adres aan bij uw leverancier/partner
- Update de primaire NTG om het alternatieve IP te gebruiken
- Erken verminderde redundantie totdat het backend-probleem is opgelost

Oorzaak

Dit probleem wordt veroorzaakt door een softwarefout in het Cisco Secure Access-backendsysteem. Wanneer een primaire peer-IP wordt gewijzigd en teruggebracht naar de oorspronkelijke waarde, behandelt het backend-validatiesysteem het oorspronkelijke IP ten onrechte als nog steeds toegewezen of gereserveerd, zelfs als het beschikbaar zou moeten zijn voor hergebruik. Dit resulteert in een backend-validatiefout die door de gebruikersinterface wordt gemaskeerd als een algemene "Internal Server Error." Het back-endsysteem kan de IP-reservering niet goed opschonen of vrijgeven tijdens het configuratiewijzigingsproces, waardoor een probleem met de status persistent wordt dat voorkomt dat het IP opnieuw wordt gebruikt in dezelfde NTG.

Gerelateerde inhoud

- Problemen oplossen en basisinformatie verzamelen voor Cisco Secure Access
- 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.