Uitdagingen bij de configuratie van beveiligde toegang met split-tunneling

Inhoud

uitgeven

Tijdens het configureren van de Cisco Secure Access (TIA)-functie voor split-tunnelverkeer zijn tijdens het configuratieproces meerdere complicaties opgetreden die een juiste implementatie hebben verhinderd:

- Uitdagingen bij verkeersidentificatie: bij het configureren van TIA voor split tunneling moet al het VPN-verkeer worden uitgesloten van internetbeveiligingsinspectie. Het identificeren van de vereiste verkeersstromen bleek moeilijk, en sommige redirect-URL's waren bijzonder uitdagend om te volgen en te categoriseren.
- Authenticatieverkeersbeperkingen: Bepaalde scenario's met gesplitste tunnels vereisten dat het verificatieverkeer van de proxy werd uitgesloten. Op basis van het bestaande beleid kon authenticatieverkeer echter niet worden omzeild van de proxy, wat tot beleidsconflicten leidde.
- Beveiligingsrisico's bij het verbreken van de VPN-verbinding: wanneer de VPN-verbinding wordt verbroken, wordt het gesplitste tunnelverkeer blootgesteld aan het open internet, wat resulteert in extra beveiligingsrisico's waarmee rekening moet worden gehouden tijdens de configuratie.

Tijdens het proces werden ook aanvullende configuratieproblemen waargenomen die verdere analyse en oplossing vereisten.

milieu

- Productfamilie: SECACS (Secure Access)
- Technologie: Cisco Secure Access (TIA) met split-tunneling

- Configuratie: verkeersscenario's in een gesplitste tunnel met bestaand beleid
- Verificatie: op proxy gebaseerde verwerking van verificatieverkeer
- Netwerkbeveiliging: vereisten voor internetbeveiligingsinspectie voor VPN-verkeer

resolutie

Op basis van de configuratie-uitdagingen die zijn geïdentificeerd met Cisco Secure Access split-tunneling, is een uitgebreid functieverzoek ingediend om de geïdentificeerde beperkingen en beleidsconflicten aan te pakken.

Indiening van aanvraag voor functie

Er is een aanvraag voor een functie (CSE-I-5636) geopend en ingediend voor beoordeling door het relevante engineeringteam om deze configuratie-uitdagingen aan te pakken:

- Verbeterde verkeersidentificatiemogelijkheden voor uitsluiting van VPN-verkeer van internetbeveiligingsinspectie
- Verbeterde afhandeling van omleidings-URL's die moeilijk te traceren en te categoriseren zijn
- Oplossing van beperkingen voor het omzeilen van verificatieverkeer met bestaand beleid
- Beperking van beveiligingsrisico's voor blootstelling aan split-tunnelverkeer tijdens het verbreken van de VPN-verbinding

Oorzaak

De configuratie-uitdagingen vloeien voort uit de huidige beperkingen in de split-tunneling-implementatie van Cisco Secure Access (TIA) die niet adequaat is afgestemd op complexe scenario's voor bedrijfsimplementatie. Concreet ontbreekt het systeem aan voldoende gedetailleerde controle voor verkeersidentificatie en -categorisatie, heeft het beperkingen bij het omzeilen van authenticatieverkeer wanneer er beleid is en biedt het geen adequate beveiligingsmaatregelen voor split-tunnelverkeer wanneer VPN-verbindingen worden

onderbroken.

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.