

Beveiligde toegangsdoeladressen voor configuratie van gesplitste routing

Inhoud

uitgifte

Bij de implementatie van Cisco Secure Access (CSA) met Cisco Secure Client (CSC) op Windows-eindpunten in een Hub-Spoke-netwerkarchitectuur moeten organisaties hoogstwaarschijnlijk gesplitste routing configureren om Spoke-siteverkeer rechtstreeks met CSA via het lokale Spoke-internetcircuit te laten verbinden in plaats van via de Hub te hairpinnen. Deze configuratie vereist kennis van alle Cisco-bestemmingsadressen die worden gebruikt bij het opzetten van de CSA-tunnel, zodat routeringsuitzonderingen (breakout/split routing) kunnen worden gedefinieerd op netwerkapparaten zoals Fortigate-firewalls.

De specifieke vereiste is om alle bestemmingsinformatie (IP-adressen of URL's) te identificeren voor CSA-eindpunten die door CSC worden gebruikt bij het opzetten van TLS/DTLS-tunnels, waardoor een juiste configuratie van routeringsbeleid mogelijk wordt dat de Hub-Spoke VPN-tunnel voor CSA-verkeer omzeilt.

milieu

- Cisco Secure Access (CSA)-implementatie
- Cisco Secure Client (CSC) op Windows-eindpunten
- Hub-Spoke netwerktopologie met Fortigate-firewalls
- TLS/DTLS-tunnelconnectiviteit met CSA

resolutie

Als u gesplitste routing voor Cisco Secure Access-verbindingen wilt configureren, moet de in de volgende secties beschreven bestemmingsinformatie op het Fortigate-apparaat worden geconfigureerd om directe verbinding met CSA-eindpunten mogelijk te maken.

CSA-bestemmingsdomein en -poorten

Primair domein

`*.vpn.sse.cisco.com`

Vereiste poorten en protocollen

- TCP/UDP 443: Gebruikt voor TLS/DTLS-tunnelinstallatie
- UDP 500/4500: Gebruikt voor IPsec-tunnelinrichting
- TCP 80: Gebruikt voor VPN-certificaatherroepingscontroles

Fortigate Configuration-benadering

Configureer het routeringsbeleid op het Fortigate-apparaat om verkeer dat bestemd is voor het CSA-domein (`*.vpn.sse.cisco.com`) en de opgegeven poorten via het lokale Spoke-internetcircuit te leiden in plaats van via de Hub-Spoke VPN-tunnel. Dit maakt de verkeersstroom mogelijk die wordt beschreven in de volgende codefragmenten.

Gewenste verkeersstroom

Spoke Site → CSA Tunnel Connection → CSA-mediated Internet Communication

In plaats van de doorstroming van het verkeer via de Hub-site

Spoke Site → Hub Site → CSA Tunnel Connection → CSA-mediated Internet Communication

Belangrijke overwegingen

De CSA-verbindingsbestemmingen worden dynamisch bepaald tijdens runtime, wat betekent dat specifieke IP-adressen niet vooraf kunnen worden bepaald voor statische routeringsconfiguratie. De domeingebaseerde aanpak met *.vpn.sse.cisco.com biedt de meest betrouwbare methode voor het configureren van gesplitste routeringsbeleid.

Raadpleeg de officiële Cisco Secure Access-documentatie voor de meest recente bestemmings- en poortvereisten, omdat deze hoogstwaarschijnlijk worden bijgewerkt met nieuwe softwarereleases.

Oorzaak

In Hub-Spoke-netwerktopologieën wordt al het internetgebonden verkeer van Spoke-sites standaard door de Hub-site geleid. Wanneer CSA met CSC wordt geïmplementeerd, zorgt dit standaardrouteringsgedrag ervoor dat het CSA-tunnelverkeer door de Hub-site wordt gehairpin voordat de CSA-eindpunten worden bereikt, waardoor mogelijk latentie- en bandbreedteinefficiënties worden geïntroduceerd. De dynamische aard van de selectie van CSA-eindpunten vereist een op domeinen gebaseerd routeringsbeleid in plaats van statische op IP gebaseerde regels om de juiste functionaliteit voor gesplitste routing te garanderen.

Gerelateerde inhoud

- [Cisco Secure Access-documentatie - Verbindingsvereisten](#)
- [Cisco Secure Access-documentatie - netwerkconfiguratie](#)

- [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.