Gebruikers met externe toegang kunnen geen interne services bereiken via RAVPN

Inhoud

uitgeven

Gebruikers van Remote Access die Secure Access gebruikten, konden geen toegang krijgen tot interne services, waaronder de Domain Controller op het hoofdkantoor, terwijl de internettoegang normaal bleef werken. Gebruikers konden met succes op internet surfen, maar hadden geen toegang tot interne bronnen zoals de Domain Controller via RAVPN (Remote Access VPN).

milieu

- Cisco Secure Access - beveiligde externe clienttoegang (VPN, houding, privébron)
- RAVPN (Remote Access VPN) tunnels gemeld als up en gezond
- SD-WAN-infrastructuur in gebruik
- Interne DNS-servers op het hoofdkantoor
- Domeincontrollerservices op de locatie van het hoofdkantoor
- Meerdere vertakte netwerken verbonden via de infrastructuur

resolutie

De volgende stappen voor het oplossen van problemen en het oplossen van problemen zijn uitgevoerd om het probleem met de connectiviteit via externe toegang aan te pakken:

Stap 1: Analyse van pakketafvang

Verzamel simultane pakketopname van de client en uw Edge-apparaat (bidirectioneel) om verkeersstroompatronen te analyseren.

Stroom:

RA VPN-client ----------Cisco Secure Access ---------Ipsec tunnel ---------- Edge-apparaat ---------- Privé-bron

- Bevestig of DNS-query's van clients Edge Device hebben bereikt en naar de DNS-server zijn verzonden.
- Controleer of er geen DNS-antwoorden zijn waargenomen bij het retourneren van de lokale DNS-server naar de clients
- De lokale DNS-server stuurde een antwoord, maar die antwoorden kwamen nooit terug naar de tunnelinterface.

Stap 2: Identificatie van de hoofdoorzaak

Op basis van de analyse van de pakketopname werd het probleem geïdentificeerd als een routeringsprobleem met het retourpad. De verkeersanalyse gaf aan dat terwijl DNS-query's de lokale DNS-server bereikten via de Cisco Secure Access-infrastructuur, het retourverkeer met DNS-antwoorden de Remote Access-clients niet bereikte vanwege routerings- of configuratieproblemen op uw infrastructuur.

Stap 3: Configuratie controleren en herstellen

De interne netwerkconfiguratie en interne netwerkconfiguratie controleren en corrigeren, waarbij de nadruk ligt op:

- DNS-configuratie en routering van retourverkeer
- Intern routeringsbeleid voor terugkeerverkeer van VPN
- Configuratie van interne netwerkroutering

- Ontbrekende configuratie-elementen aan de kant van Edge Device

Stap 4: Verificatie van serviceherstel

Na de configuratiebeoordeling en correcties werd de functionaliteit voor beveiligde toegang grotendeels hersteld. De meeste gebruikers van Remote Access kregen weer toegang tot interne services, waaronder de Domain Controller op het hoofdkantoor.

Oorzaak

De hoofdoorzaak werd geïdentificeerd als een probleem met routering van het retourpad binnen de interne netwerkinfrastructuur. Terwijl DNS-query's van Remote Access-clients de lokale DNS-server bereikten via de Cisco Secure Access Infrastructure, werd het retourverkeer met DNS-antwoorden niet correct naar de clients gerouteerd. Dit werd veroorzaakt door ontbrekende of onjuiste configuratie aan de kant van de interne netwerkinfrastructuur waardoor DNS-antwoorden en TCP-antwoorden de Remote Access-clients via de VPN-verbinding niet konden bereiken.

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.