Veilige toegang VPN - geen toegang tot Jabber

Inhoud

uitgeven

Gebruikers van Secure Client hadden geen toegang tot interne en privétoepassingen zoals Jabber en Epic via de VPN-tunnel voor beveiligde toegang bij gebruik van een beleid voor privétoegang. Gebruikers ondervonden connectiviteitsfouten bij het bereiken van deze kritieke bedrijfstoepassingen via de VPN-verbinding. Tijdens het oplossen van problemen werd unidirectioneel verkeer waargenomen voor Epic-bronnen waarbij ping- en TCP SYN-verkeer de Secure Access VPN-tunnel verliep, maar problemen met de validatie van het retourverkeer werden geïdentificeerd op de Palo Alto-firewall. Daarnaast werden Jabber-bereikbaarheidsproblemen gedocumenteerd waarbij CUCM FQDN's via interne DNS werden opgelost terwijl verkeerssturing werd geconfigureerd voor IP-gebaseerde routering, waardoor een mismatch in de verkeersstroom ontstond.

milieu

- Cisco Secure Access met VPN-tunnelconfiguratie
- Veilige client voor VPN-connectiviteit
- Implementatie van het toegangsbeleid voor particulieren
- Cisco Unified Communications Manager (CUCM) voor Jabber-services
- Bronnen voor Epic-toepassingen
- Palo Alto firewall voor netwerkbeveiliging
- Interne DNS-resolutie voor CUCM FQDN's

resolutie

De oplossing omvatte meerdere configuratiewijzigingen en stappen voor het oplossen van problemen om de connectiviteit met interne toepassingen te herstellen via de VPN-tunnel voor beveiligde toegang:

Subnetconfiguratie en tunnelwijzigingen

Stap 1: Voeg extra subnetten toe aan VPN-tunnel

Extra subnetten werden toegevoegd aan de VPN-tunnelconfiguratie voor de getroffen bronnen. Na het doorvoeren van deze wijziging zijn de bronnen die voorheen ontoegankelijk waren, met succes geladen.

CUCM IP Address Steering Configuration

Stap 2: CUCM IP-besturing configureren

Om het probleem met de Jabber-connectiviteit op te lossen waarbij CUCM-FQDN's via interne DNS werden opgelost terwijl de verkeersbesturing op IP was gebaseerd, werden de CUCM IP-adressen in Secure Client gestuurd. Deze configuratiewijziging heeft de DNS-resolutie afgestemd op het verkeersstuurmechanisme.

Stap 3: regel toegangsbeleid maken

Er is een regel voor toegangsbeleid gemaakt om bereikbaarheid van de CUCM IP-adressen mogelijk te maken. Deze regel herstelde de juiste connectiviteit met de CUCM-infrastructuur, waardoor Jabber-functionaliteit via de VPN-tunnel mogelijk werd.

Statische routingconfiguratie

Stap 4: Statische routering voor CUCM-subnet configureren

Zorg ervoor dat CUCM IP-adressen en het totale CUCM-subnet zijn opgenomen in de statische routeringstabel voor de netwerktunnel. Deze configuratie zorgt voor een goede routering van het verkeer tussen de Secure Client-gebruikersgroep en de CUCM-infrastructuur.

Terugkeerverkeersvalidatie

Stap 5: Packet Flow en retourverkeer valideren

Valideer de pakketstroomconfiguratie om te bevestigen dat het retourverkeer de Secure Client-gebruikersgroep kan bereiken. Dit omvat het herzien van de Palo Alto firewall configuratie om een goede terugkeer-pad validatie voor alle interne bronnen te garanderen, met name voor Epic

connectiviteit waar unidirectioneel verkeer werd waargenomen.

Oorzaak

De connectiviteitsproblemen werden veroorzaakt door meerdere configuratiekloven in de Secure Access VPN-implementatie:

- Ontbrekende subnetconfiguraties in de VPN-tunnel voorkwamen een goede routering naar interne toepassingsbronnen
- Mismatch tussen DNS-resolutie (op basis van FQDN) en configuratie van verkeerssturing (op basis van IP) voor CUCM-services veroorzaakte connectiviteitsfouten van Jabber
- Onvolledige regels voor toegangsbeleid die geen verkeer naar CUCM-IP-adressen toestaan
- Ontbrekende statische routeringsitems voor CUCM-subnetten in de netwerktunnelconfiguratie
- Problemen met de validatie van het retourverkeerspad op de firewall van Palo Alto die van invloed zijn op bidirectionele communicatie

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.