Problemen met volledige clientconnectiviteit door beveiligde toegang

Inhoud

uitgeven

De volledige Omnissa-client kan geen virtuele desktops laden wanneer deze is verbonden via Cisco Secure Access. Gebruikers ondervinden verbindingsfouten wanneer ze proberen verbindingen tot stand te brengen met virtuele omgevingen met behulp van de volledige clienttoepassing. Toegang via de HTML/webclient blijft echter normaal werken, wat aangeeft dat de onderliggende virtuele desktopinfrastructuur functioneel is, maar er is een specifiek probleem dat van invloed is op de volledige mogelijkheid van de client om verbindingen tot stand te brengen via de Cisco Secure Access-oplossing.

milieu

- Technologie: oplossingsondersteuning (SSPT - contract vereist)
- Subtechnologie: Cisco Secure Access
- Productfamilie: SECACS
- Softwareversie: alle betrokken versies
- Clienttoepassing: Omnissa volledige cliënt
- Virtuele desktopomgeving: Omnissa virtuele desktops
- Netwerkinfrastructuur: IPsec-tunnels en FTD (Firepower Threat Defense)

resolutie

De oplossing omvat het implementeren van specifieke wijzigingen in de netwerkconfiguratie om de juiste routering voor de volledige Omnissa-client via Cisco Secure Access mogelijk te maken. Deze stappen zijn genomen om het connectiviteitsprobleem op te lossen:

- Gesplitste tunnelinstellingen configureren. Voeg gesplitste tunnelconfiguraties toe zodat de volledige Omnissa-client directe verbindingen met de vereiste bestemmingshosts kan maken. Deze configuratie zorgt ervoor dat het verkeer dat bestemd is voor specifieke virtuele-desktopclients op de juiste manier wordt geleid via de juiste netwerkpaden.
- Implementeer statische routeconfiguraties. Configureer statische routes voor de specifieke clients die verbindingen met virtuele desktops moeten maken. De belangrijkste vereiste is om routes te configureren, niet alleen naar de aggregatieserver downstream, maar rechtstreeks naar de bestemmingshsts die de virtuele desktopclients moeten bereiken.
- IPsec-tunnels wissen. Na het implementeren van de configuratiewijzigingen, moet u de IPsec-tunnels op de FTD wissen om ervoor te zorgen dat de nieuwe routeringsconfiguraties correct worden uitgevoerd.
- Connectiviteit valideren. Test de volledige clientconnectiviteit van Omnissa na het implementeren van de wijzigingen om te bevestigen dat virtuele desktopverbindingen met succes tot stand kunnen worden gebracht via Cisco Secure Access.

implementatieschema

De configuratiewijzigingen moeten tijdens een gepland onderhoudsvenster worden geïmplementeerd om de gevolgen voor gebruikers tot een minimum te beperken. Na de implementatie moet zowel de bereikbaarheid als de volledige connectiviteit van Omnissa worden gevalideerd om ervoor te zorgen dat de oplossing succesvol is.

Oorzaak

Het connectiviteitsprobleem werd veroorzaakt door onvoldoende routeringsconfiguraties in de Cisco Secure Access-omgeving. Concreet werd het netwerk geconfigureerd met alleen routes naar de aggregatieserver stroomafwaarts, maar ontbrak het aan de nodige split-tunnel- en statische routeconfiguraties voor de specifieke clients waar de Omnissa volledige client verbindingen mee moest maken. Door deze routeringskloof kon de volledige client de virtuele desktophosts niet goed bereiken, terwijl de HTML-/webclient nog steeds kon functioneren omdat deze verschillende verbindingspaden gebruikte die correct waren geconfigureerd.

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.