Problemen met de zichtbaarheid van clientidentiteit met MX75-netwerktunnel in beveiligde toegang

Inhoud

uitgeven

Wanneer eindpunten met Secure Client worden geïmplementeerd achter een MX75-netwerktunnel die verbinding maakt met Secure Access, zijn de identiteit van de roamende client en de gebruikersidentiteiten niet goed zichtbaar in het systeem. De volgende specifieke gedragingen worden waargenomen:

- Back-off-instellingen die zijn geconfigureerd om prioriteit te geven aan Secure Client boven netwerktunnelverbindingen, werken niet zoals verwacht wanneer eindpunten achter de MX75 liggen
- Regels voor verkeerssturing op basis van domeinen zijn niet van toepassing omdat het verkeer alleen wordt toegeschreven aan de identiteit van de netwerktunnel in plaats van aan de roamende client
- Activity Search geeft onvolledige bronlocatiegegevens weer, waarbij alleen de netwerktunnelidentiteit wordt weergegeven en gebruikers- en roamingclientidentiteiten worden weggelaten
- Op identiteit gebaseerde verkeerssturingsregels (zoals die op basis van Active Directory-gebruikers of de identiteit van roamende clients) zijn niet van toepassing op verkeer dat door de MX75-tunnel rijdt

Dit gedrag verhindert een goede identiteitsscheiding en beleidstoepassing voor eindpunten die via de netwerktunnelinfrastructuur verbinding maken.

milieu

- Cisco Secure Access-implementatie
- MX75-toestel met netwerktunnelconfiguratie voor beveiligde toegang

- Beveiligde clientagents geïnstalleerd op alle eindpunten
- Back-off-instellingen zijn uitgeschakeld op roamingclients om prioriteit te geven aan Secure Client boven netwerktunnelverbindingen
- Regels voor verkeerssturing geconfigureerd voor routering via een domein
- Op identiteit gebaseerd beleid geconfigureerd voor Active Directory-gebruikers en roamingclients

resolutie

Het probleem werd opgelost door een workaround-configuratie te implementeren met behulp van een aanpak voor een geregistreerd netwerk in plaats van te vertrouwen op zichtbaarheid van de roamingidentiteit via de MX75-netwerktunnel.

Implementatie van workaround

Stap 1: RSM (Roaming Security Module) configureren met geregistreerd netwerk

Vervang de bestaande netwerktunnelconfiguratie door een RSM-implementatie in combinatie met een geregistreerde netwerkconfiguratie. Deze configuratie maakt een juiste identiteitstoewijzing en beleidstoepassing mogelijk.

Stap 2: Zichtbaarheid van identiteit valideren

Controleer na het implementeren van de geregistreerde netwerkconfiguratie of:

- Gebruikersidentiteiten worden correct weergegeven in Activiteit zoeken
- De identiteit van de roamende client is zichtbaar en correct toegewezen
- Regels voor verkeerssturing op basis van de functie voor gebruikers- en cliëntidentiteit zoals verwacht

Stap 3: Test de verkeerssturingsfunctionaliteit

Bevestig dat de op het domein gebaseerde verkeerssturingsregels en het op identiteit gebaseerde beleid correct worden toegepast met de nieuwe configuratie.

alternatieve benadering

Voor omgevingen waar identiteitsscheiding over privénetwerken niet vereist is, kunt u overwegen om RSM - Internet-configuratie te implementeren. Deze aanpak stuurt RSM-verkeer rechtstreeks naar het internet in plaats van via de privénetwerktunnel, die een goede zichtbaarheid van de identiteit kan bieden met behoud van beveiligingscontroles.

technische analyse

Tijdens het oplossen van problemen werd diagnostische output verzameld met behulp van policy.test.sse.cisco.com om het gedrag van identiteitsattributie aan te tonen wanneer eindpunten zich achter de MX75-tunnel bevonden. De analyse bevestigde dat het routeren van roamingidentiteiten door een netwerktunnel weliswaar technisch mogelijk is, maar dat het geen aanbevolen of ondersteunde operationele stroom is voor dit specifieke implementatiescenario.

Oorzaak

De hoofdoorzaak is gerelateerd aan hoe Secure Access omgaat met identiteitsattributie wanneer verkeer door de netwerktunnelinfrastructuur gaat. Wanneer eindpunten verbinding maken via de MX75-netwerktunnel, kent het systeem al het verkeer toe aan de tunnelidentiteit in plaats van de individuele roamingclient en gebruikersidentiteiten te behouden. Dit gedrag is van ontwerp voor netwerktunnelverbindingen, maar is in strijd met de vereiste van zichtbaarheid van de individuele identiteit en beleidstoepassing.

Hoewel het technisch haalbaar is om roamingidentiteiten door netwerktunnels te routeren, wordt deze configuratie niet aanbevolen of ondersteund als een standaard operationele stroom vanwege de beperkingen voor identiteitstoekenning die hierboven zijn beschreven.

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.