

MacOS Internet Access problemen na het importeren van Secure Access Certificate

Inhoud

uitgifte

MacOS-gebruikers hebben geen toegang tot internetbronnen via Cisco Secure Access nadat ze het internetcertificaat van het portaal hebben geïmporteerd.

De getroffen diensten omvatten:

- Microsoft Outlook (functionaliteit verzenden en ontvangen)
- Google.com
- AI-websites
- Andere webbestemmingen

Windows-gebruikers met dezelfde configuratie worden niet beïnvloed en blijven normaal functioneren. Het probleem is specifiek van invloed op de toegang van MacOS-clients tot e-mail en algemene internetmogelijkheden na de import van certificaten.

milieu

- Cisco Secure Access met Unified Policy-configuratie
- MacOS-clients met geïmporteerd internetcertificaat van Cisco Secure Access-portal
- Windows-clients met dezelfde configuratie (niet beïnvloed)
- Internetbeleid, privébeleid, DLP-beleid, RBI en beveiligingsprofielen in gebruik
- Gemengde besturingssysteemomgeving met differentieel gedrag tussen MacOS en Windows

resolutie

De oplossing omvat het toevoegen van specifieke Microsoft Outlook-eindpunten en -toepassingen aan de lijst Niet decoderen (DND) om SSL-inspectie voor deze services te omzeilen.

Stap 1: Outlook-eindpunten toevoegen aan de DND-lijst

Voeg de eindpunten of toepassingen die in de volgende secties worden beschreven toe aan de DND-configuratie (Do Not Decrypt) om de problemen met Outlook-toegang op te lossen.

outlook.cloud.microsoft
outlook.office.com
outlook.office365.com
smtp.office365.com

Stap 2: Resolutie valideren

Controleer na het toevoegen van de Outlook-gerelateerde eindpunten aan de DND-lijst of de getroffen MacOS-clients nu toegang hebben tot:

- Microsoft Outlook-functionaliteit voor verzenden en ontvangen
- Andere eerder getroffen internetbronnen

De gebruiker bevestigde dat na het implementeren van deze DND-vermeldingen de Outlook-toepassingen normaal blijven functioneren op MacOS-apparaten.

Oorzaak

Het probleem werd veroorzaakt door SSL / TLS-encryptie-inspectie die het vermogen van MacOS-clients om veilige verbindingen met internetbronnen tot stand te brengen, met name Microsoft Outlook-services, belemmert. Het encryptie-inspectieproces verhinderde de juiste

certificaatvalidatie of het tot stand brengen van verbindingen, specifiek op MacOS-platforms, terwijl Windows-clients niet werden beïnvloed door hetzelfde inspectiebeleid. Door de betreffende eindpunten toe te voegen aan de lijst Niet decoderen wordt de inspectie voor deze specifieke services omzeild, waardoor de normale connectiviteit kan worden hervat.

Gerelateerde 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.