Problemen met MS Teams oplossen met de configuratie van het toegangsprofiel zonder vertrouwen

Inhoud

uitgifte

Gebruikers die zijn ingeschreven in een Zero Trust Access (ZTA)-profiel voor beveiligde internettoegang hebben problemen met de connectiviteit van Microsoft Teams. Wanneer gebruikers worden toegevoegd aan het ZTA-profiel, worden oproepen van Microsoft Teams onverwacht verbroken en kunnen andere gebruikers geen oproepen naar de betreffende gebruiker initiëren. Oproepen maken echter succesvol verbinding wanneer de getroffen gebruiker het gesprek van zijn kant initieert.

Het probleem is geïsoleerd voor gebruikers aan boord van het ZTA-profiel, wat aangeeft dat ZTA-beleid of routeringsconfiguraties van invloed zijn op de aanroepconnectiviteit van Teams. Verkeerslogs tonen aan dat Microsoft Teams-verkeer van processen zoals ms-teams.exe naar IP-adressen in vereiste bereiken (zoals 52.115.245.30:3480, dat deel uitmaakt van 52.112.0.0/14) wordt onderschept door de ZTA-client in plaats van rechtstreeks naar het internet te gaan.

milieu

- Cisco Secure Access met Zero Trust Access (ZTA)-profielconfiguratie
- ZTA-profiel geconfigureerd met "ZTA gebruiken om alle internetbestemmingen te beveiligen"
- Microsoft Teams-toepassing
- Cisco Secure Client met ZTA-mogelijkheden
- Gebruikers die zijn ingeschreven in het ZTA-profiel voor beveiligde internettoegang

resolutie

Om het probleem op te lossen, voegt u Microsoft Teams-verkeersuitzonderingen toe aan de configuratie van het ZTA-profiel, zodat Teams-verkeer de ZTA-tunnel kan omzeilen en rechtstreeks verbinding kan maken met internet:

1. Navigeer naar Dashboard > Eindgebruikersconnectiviteit > Zero Trust Access en zoek het betreffende ZTA-profiel.

2. Selecteer het ZTA-profiel en kies Bewerken > Veilige internettoegang.

3. Voeg deze IP-bereiken en FQDN's toe aan de uitzonderingenlijst volgens de officiële documentatie van Microsoft:

IP-bereiken:

```
52.112.0.0/14
52.122.0.0/15
2603:1063::/38
2603:1027::/48
2603:1037::/48
2603:1047::/48
2603:1057::/48
2620:1ec:6::/48
2620:1ec:40::/42
```

FQDN's:

```
*.lync.com
*.teams.cloud.microsoft
*.teams.microsoft.com
teams.cloud.microsoft
teams.microsoft.com
*.keydelivery.mediaservices.windows.net
*.streaming.mediaservices.windows.net
aka.ms
```

4. Voeg een beschrijving toe voor de uitzonderingen, zoals:

```
MS Teams exception as per: https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-addre
```

5. Sla de configuratiewijzigingen op. Wacht een paar minuten om de wijzigingen toe te passen.

6. Zorg ervoor dat het ZTA-clientbeleid opnieuw wordt gesynchroniseerd op de betreffende eindpunten. Hiervoor kan het nodig zijn de Zero Trust Access Agent Service opnieuw op te starten of het clientapparaat opnieuw op te starten.

7. Functionaliteit van de oproep van de testteams om te bevestigen dat:

- Inkomende oproepen aan getroffen gebruikers maken nu verbinding
- Teams bellen niet langer onverwacht
- Verkeersteams omzeilen de ZTA-tunnel en maken rechtstreeks verbinding met internet

---



Opmerking: na het implementeren van de uitzonderingen wordt het Teams-verkeer niet weergegeven in de activiteitenlogboeken voor beveiligde toegang, omdat het de ZTA-tunnel volledig omzeilt.

Oorzaak

Het probleem wordt veroorzaakt doordat Microsoft Teams-verkeer via de ZTA Secure Internet Access-tunnel wordt geleid in plaats van rechtstreeks verbinding te maken met internet. Wanneer het ZTA-profiel is geconfigureerd met de optie "Alle internetbestemmingen beveiligen", wordt het mediaverkeer van Teams onderschept, inclusief UDP-stromen die nodig zijn voor realtime communicatie. Dit veroorzaakt connectiviteitsproblemen, met name voor inkomende oproepen en mediastreams.

Microsoft raadt aan om het Microsoft Teams-verkeer van proxyservers en SSL-inspectie te omzeilen voor optimale prestaties en gesprekskwaliteit. Wanneer de ZTA-configuratie de noodzakelijke uitzonderingen voor Teams-verkeer mist, wordt de mediastroom van de toepassing verwerkt via de ZTA-client in plaats van het directe pad te nemen dat nodig is voor realtime communicatie.

Gerelateerde inhoud

- Microsoft 365 URL's en IP-adresbereiken - Microsoft Teams
- Aanbevelingen voor Microsoft Teams-proxyservers
- Problemen oplossen en basisinformatie verzamelen voor Cisco Secure Access
- 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.