Azure-gehoste FQDN-connectiviteitsproblemen via beveiligde toegang met Meraki-integratie

Inhoud

uitgifte

Specifieke Azure-gehoste FQDN's worden onbereikbaar wanneer gebruikersverkeer via Meraki naar Cisco Secure Access wordt gerouteerd, ondanks Secure Access-logboeken die het verkeer als "toegestaan" weergeven. Het probleem heeft voornamelijk betrekking op RDP-connectiviteit met behulp van niet-standaard poorten naar deze FQDN's.

Wanneer u logs zoekt op FQDN in het Secure Access-portaal, worden alleen DNS-beveiligingslogs weergegeven met de status "toegestaan". De RDP-connectiviteit naar dezelfde bestemmingen op niet-standaard poorten mislukt echter. Wanneer het FQDN is opgelost naar een IP-adres en Activity Search het bestemmings-IP gebruikt, worden Cloud Firewall-logs onthuld die het verkeer hadden geblokkeerd.

milieu

- Cisco Secure Access (SSE) met Meraki-integratie
- Meraki Dashboard met lokale breakout mogelijkheden
- Azure-gehoste ontwikkelingsbronnen waarvoor RDP-toegang op niet-standaard poorten vereist is
- Verkeersroute door Meraki-tunnel naar Secure Access

resolutie

Onmiddellijke workaround

Voeg de getroffen FQDN's toe aan Meraki lokale breakout-regels om Secure Access te omzeilen voor de specifieke bestemmingen die in de volgende secties worden beschreven.

Stap 1: Toegang tot Meraki Dashboard

Navigeer naar het Meraki Dashboard en zoek de lokale breakout configuratie sectie.

Stap 2: Configureer de lokale regels voor de uitbraak

Voeg de problematische FQDN's toe aan de lokale breakout-regels om Secure Access-routering te omzeilen. Deze configuratiewijziging herstelt onmiddellijk de toegang voor de getroffen gebruikers door het verkeer rechtstreeks van Meraki naar het internet te routeren, waarbij de Secure Access-tunnel wordt omzeild.

Problemen oplossen en analyseren

Stap 1: Loganalyse door FQDN

Zoeken in logboeken voor beveiligde toegangsactiviteiten met behulp van het FQDN. Dit toont voornamelijk DNS-beveiligingslogs en kan de "toegestane" status voor webverkeer op poort 443 weergeven.

Stap 2: Loganalyse op bestemming IP

Los het FQDN op naar zijn IP-adres en zoek Activiteitenlogboeken met behulp van het bestemmings-IP in plaats van het FQDN. Dit onthult Cloud Firewall-logs die geblokkeerd verkeer

weergeven en de werkelijke verkeersbeschikbaarheid bieden.

Stap 3: Verifieer de verkeersstroom

Bevestig dat het probleem alleen optreedt wanneer het verkeer het pad volgt: Gebruiker → Meraki → Tunnel → Secure Access → Internet. Test die bypass via lokale breakout lost het connectiviteitsprobleem op.

langetermijnresolutie

Het waargenomen gedrag is geïdentificeerd als verwachte functionaliteit binnen de huidige Secure Access-implementatie. Er is een aanvraag voor kenmerken (FR CSE-I-5543) geopend om de zichtbaarheid en functionele problemen met betrekking tot:

- Verschil tussen FQDN-gebaseerde en IP-gebaseerde logzoekopdrachten
- Rapportage over inconsistente verplaatsing van verkeer tussen DNS Security- en Cloud Firewall-logs
- Verbeterde zichtbaarheid voor RDP-verkeer op niet-standaard poorten

Oorzaak

Het probleem komt voort uit een discrepantie in de manier waarop Secure Access verkeer voor Azure-gehoste FQDN's verwerkt en rapporteert wanneer deze via RDP worden benaderd op niet-standaard poorten. Bij het zoeken naar logs door FQDN, geeft het systeem voornamelijk DNS-beveiligingslogs weer met de status "toegestaan" voor webverkeer (meestal poort 443). Het werkelijke RDP-verkeer op niet-standaard poorten wordt echter verwerkt door Cloud Firewall-regels, die alleen zichtbaar zijn bij het zoeken op het IP-adres van de opgeloste bestemming in plaats van het FQDN.

Dit creëert een zichtbaarheidskloof waarbij beheerders "toegestaan" verkeer zien in op FQDN gebaseerde zoekopdrachten terwijl de werkelijke RDP-verbindingen worden geblokkeerd door firewallbeleid dat alleen zichtbaar is in IP-gebaseerde logzoekopdrachten. Het gedrag wordt momenteel als verwachte functionaliteit beschouwd, maar er is een verzoek om functies ingediend

om de zichtbaarheid en consistentie van verkeersrapportage over verschillende zoekmethoden te verbeteren.

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.