IP-bereiken en firewall configureren voor integratie van beveiligde webhook-toegang

uitgeven

Integraties van derden worden succesvol geladen in het Cisco Secure Access (SSE)-dashboard, maar webhook-gebaseerde beveiligingsgebeurtenissen worden niet ontvangen in de on-premises HTTP-connector voor SIEM-integratie. De organisatie heeft verduidelijking nodig over Cisco SSE-bron-IP-bereiken, inclusief regiospecifieke IP's, om firewallregels correct te configureren en levering van webhook-gebeurtenissen mogelijk te maken.

milieu

- Cisco Secure Access (SSE)
- Technologie: Oplossingsondersteuning - Veilige toegangsrapportage en -registratie
- Integratietype: integratie van derden via webhook
- Doelconnector: on-premises HTTP-connectorserver

resolutie

Om problemen met de levering van webhook met Cisco Secure Access-integraties op te lossen, configureert u firewallregels om inkomende HTTPS-verkeer van de opgegeven SSE-bron IP-bereiken naar uw on-premises connector toe te staan.

Cisco SSE Source IP Ranges

Configureer uw firewall om inkomende HTTPS-verbindingen vanuit deze Cisco SSE-bron-IP-bereiken toe te staan:

```
146.112.161.0/24
146.112.163.0/24
146.112.165.0/24
146.112.167.0/24
```

Stappen voor firewallconfiguratie

Stap 1: Integratiestatus van derden controleren

Navigeer naar Beheer > Integraties van derden in het SSE-dashboard en bevestig dat integraties correct worden geladen voor uw organisatie.

Stap 2: Firewallregels configureren

Maak firewallregels om inkomend HTTPS-verkeer (poort 443) van de SSE-bron IP-bereiken naar uw on-premises connectorserver mogelijk te maken. Zorg ervoor dat de regels worden toegepast op zowel uw netwerkfirewall als eventuele tussenliggende firewalls tussen het internet en uw connectorserver.

Stap 3: Webhook Event Delivery valideren

Nadat u de firewallwijzigingen hebt geïmplementeerd, controleert u uw on-premises HTTP-connector om te bevestigen dat webhook-gebeurtenissen worden ontvangen van Cisco SSE.

Regionale IP-informatie

Cisco SSE maakt alleen gebruik van gedeelde IP-bereiken uit regio's in de EU en de VS. De geleverde IP-bereiken bestrijken zowel regionale implementaties als moeten worden geconfigureerd, ongeacht in welke primaire regio uw organisatie zich bevindt.

Oorzaak

Webhook-gebeurtenissen van Cisco Secure Access worden geblokkeerd door firewallregels die inkomende HTTPS-verbindingen van SSE-bron-IP-adressen naar de on-premises HTTP-connectorserver niet toestaan. Terwijl het SSE-dashboard een succesvolle integratie laat zien, vereist de daadwerkelijke levering van de webhook een specifieke firewallconfiguratie zodat

verkeer vanuit de Cisco-infrastructuur het eindpunt van de gebruikersconnector kan bereiken.

Verwante inhoud

- Cisco Secure Access-documentatie
- 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.