Konfiguration von IP-Bereichen und Firewall für Webhook-Integration mit sicherem Zugriff

Problem

Integrationen von Drittanbietern werden erfolgreich in das Cisco Secure Access (SSE) Dashboard geladen. Am lokalen HTTP-Connector werden jedoch keine webbasierten Sicherheitsereignisse für die SIEM-Integration empfangen. Zur korrekten Konfiguration der Firewall-Regeln und zur Bereitstellung von Webhook-Ereignissen muss der Kunde die Quell-IP-Bereiche von Cisco SSE einschließlich der regionsspezifischen IP-Adressen klären.

Umwelt

- Produkt: Cisco Secure Access (SSE)
- Technologie: Lösungssupport - Reporting und Protokollierung für sicheren Zugriff
- Integrationstyp: Webhook-basierte Drittanbieterintegration
- Zielanschluss: Lokaler HTTP-Connector-Server

Auflösung

Zur Behebung von Problemen bei der Zustellung über Webhook mit Cisco Secure Access-Integrationen müssen Sie Firewall-Regeln so konfigurieren, dass eingehender HTTPS-Datenverkehr von den angegebenen SSE-Quell-IP-Bereichen zu Ihrem Connector vor Ort zugelassen wird.

Cisco SSE IP-Quellbereiche

Konfigurieren Sie Ihre Firewall so, dass eingehende HTTPS-Verbindungen aus den folgenden Cisco SSE-Quell-IP-Bereichen zugelassen werden:

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

Schritte zur Firewall-Konfiguration

Schritt 1: Überprüfen des Status der Drittanbieter-Integration

Navigieren Sie im SSE Dashboard zu Admin > Third Party Integrations (Admin > Integration von Drittanbietern), und vergewissern Sie sich, dass die Integrationen für Ihr Unternehmen korrekt geladen werden.

Phase 2: Firewall-Regeln konfigurieren

Erstellen Sie Firewall-Regeln, um eingehenden HTTPS-Datenverkehr (Port 443) von den SSE-Quell-IP-Bereichen zum Connector-Server vor Ort zuzulassen. Stellen Sie sicher, dass die Regeln sowohl auf Ihre Netzwerk-Firewall als auch auf alle dazwischen liegenden Firewalls zwischen dem Internet und dem Connector-Server angewendet werden.

Schritt 3: Zustellung von Webhook-Ereignissen überprüfen

Nachdem Sie die Änderungen an der Firewall implementiert haben, überwachen Sie den lokalen HTTP-Connector, um sicherzustellen, dass Web-Hook-Ereignisse von Cisco SSE empfangen werden.

Regionale IP-Informationen

Cisco SSE verwendet gemeinsame IP-Bereiche nur aus der EU und den USA. Die bereitgestellten IP-Bereiche decken beide regionalen Bereitstellungen ab und müssen unabhängig von der primären Region konfiguriert werden, in der sich Ihr Unternehmen befindet.

Ursache

Webhook-Ereignisse von Cisco Secure Access werden durch Firewall-Regeln blockiert, die

eingehende HTTPS-Verbindungen von SSE-Quell-IP-Adressen zum lokalen HTTP-Connector-Server nicht zulassen. Während das SSE-Dashboard zeigt, dass die Integration erfolgreich geladen wurde, ist für die tatsächliche Webhook-Bereitstellung eine spezielle Firewall-Konfiguration erforderlich, damit der Datenverkehr von der Cisco Infrastruktur den Endpunkt des Benutzerkonnektors erreichen kann.

Verwandte Inhalte

- Cisco Secure Access-Dokumentation
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.