Configurazione degli intervalli IP e del firewall per l'integrazione di Secure Access Webhook

Problema

Le integrazioni di terze parti vengono caricate correttamente nel dashboard SSE (Cisco Secure Access), ma gli eventi di sicurezza basati su webhook non vengono ricevuti nel connettore HTTP locale per l'integrazione SIEM. L'organizzazione richiede chiarimenti sugli intervalli IP di origine SSE di Cisco, inclusi gli IP specifici dell'area geografica, per configurare correttamente le regole del firewall e abilitare la consegna degli eventi webhook.

Ambiente

- Prodotto: SSE (Cisco Secure Access)
- Tecnologia: Supporto per la soluzione - Creazione di rapporti e registrazione ad accesso sicuro
- Tipo di integrazione: Integrazione di terze parti basata su Webhook
- Connettore di destinazione: Server connettore HTTP locale

Risoluzione

Per risolvere i problemi di recapito dei webhook con le integrazioni di Cisco Secure Access, configurare le regole del firewall in modo da consentire il traffico HTTPS in entrata dagli intervalli IP di origine SSE specificati al connettore locale.

Cisco SSE Source IP Range

Configurare il firewall in modo da consentire le connessioni HTTPS in entrata da questi intervalli IP di origine SSE Cisco:

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

Passaggi di configurazione del firewall

Passaggio 1: Verifica dello stato di integrazione di terze parti

Passare a Amministrazione > Integrazioni di terze parti nel pannello di controllo SSE e verificare che le integrazioni vengano caricate correttamente per l'organizzazione.

Passaggio 2: Configura regole firewall

Creare regole firewall per consentire il traffico HTTPS in entrata (porta 443) dagli intervalli IP di origine SSE al server del connettore locale. Verificare che le regole vengano applicate sia al firewall di rete che a tutti i firewall che si trovano tra Internet e il server di connessione.

Passaggio 3: Convalida recapito eventi Webhook

Dopo aver implementato le modifiche del firewall, monitorare il connettore HTTP locale per verificare che gli eventi webhook vengano ricevuti da Cisco SSE.

Informazioni IP regionali

Cisco SSE utilizza intervalli IP condivisi solo da regioni dell'UE e degli Stati Uniti. Gli intervalli IP forniti coprono entrambe le distribuzioni regionali e devono essere configurati indipendentemente dall'area primaria dell'organizzazione.

Causa

Gli eventi Webhook da Cisco Secure Access vengono bloccati da regole del firewall che non consentono connessioni HTTPS in entrata dagli indirizzi IP di origine SSE al server del connettore HTTP locale. Mentre il dashboard SSE mostra un caricamento di integrazione riuscito, il recapito effettivo del webhook richiede una configurazione specifica del firewall per consentire al traffico

proveniente dall'infrastruttura Cisco di raggiungere l'endpoint del connettore utente.

Contenuto correlato

- Documentazione di Cisco Secure Access
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).