Configure IP Ranges and Firewall for Secure Access Webhook Integration

Issue

Third-party integrations load successfully in the Cisco Secure Access (SSE) dashboard, but webhook-based security events are not being received at the on-premises HTTP connector for SIEM integration. The organization requires clarification on Cisco SSE source IP ranges, including region-specific IPs, to configure firewall rules properly and enable webhook event delivery.

Environment

- Product: Cisco Secure Access (SSE)
- Technology: Solution Support - Secure Access Reporting and Logging
- Integration Type: Webhook-based third-party integration
- Target Connector: On-premises HTTP connector server

Resolution

To resolve webhook delivery issues with Cisco Secure Access integrations, configure firewall rules to allow inbound HTTPS traffic from the specified SSE source IP ranges to your on-premises connector.

Cisco SSE Source IP Ranges

Configure your firewall to allow inbound HTTPS connections from these Cisco SSE source IP ranges:

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

Firewall Configuration Steps

Step 1: Verify Third-Party Integration Status

Navigate to Admin > Third Party Integrations in the SSE dashboard and confirm that integrations are loading correctly for your organization.

Step 2: Configure Firewall Rules

Create firewall rules to allow inbound HTTPS traffic (port 443) from the SSE source IP ranges to your on-premises connector server. Ensure rules are applied to both your network firewall and any intervening firewalls between the internet and your connector server.

Step 3: Validate Webhook Event Delivery

After implementing the firewall changes, monitor your on-premises HTTP connector to confirm that webhook events are being received from Cisco SSE.

Regional IP Information

Cisco SSE uses shared IP ranges from EU and US regions only. The provided IP ranges cover both regional deployments and must be configured regardless of which primary region your organization is in.

Cause

Webhook events from Cisco Secure Access are blocked by firewall rules that do not permit inbound HTTPS connections from SSE source IP addresses to the on-premises HTTP connector server. While the SSE dashboard shows successful integration loading, the actual webhook delivery requires specific firewall configuration to allow traffic from the Cisco infrastructure to reach the user connector endpoint.

Related Content

- Cisco Secure Access Documentation
- Cisco Technical Support & Downloads