

Eventos de segurança baseados em webhook are not Received at the On-prem HTTP Connector for SIEM Integration

Contents

Problema

Os eventos de segurança baseados em webhook não estão sendo recebidos no conector HTTP local para integração do SIEM.

Ambiente

- Produto: Cisco Secure Access (SSE)
- Tecnologia: suporte à solução - Secure Access Reporting and Logging
- Tipo de integração: integração de terceiros baseada em Webhook
- Conector de Destino: Conector HTTP Local
- Status do Pannel: Integrações de terceiros são carregadas com êxito em Admin > Integrações de terceiros

Resolução

Para resolver problemas de entrega de webhook com integrações de terceiros do Cisco Secure Access, configure as regras de firewall para permitir o tráfego HTTPS de entrada desses intervalos de IP de origem do Cisco SSE.

Configuração de firewall necessária

Permitir tráfego HTTPS de entrada destes intervalos de IP de origem Cisco SSE para o conector local:

146.112.161.0/24

146.112.163.0/24

146.112.165.0/24

146.112.167.0/24

Esses intervalos de IP representam os endereços IP compartilhados usados pelo Cisco SSE das regiões da UE e dos EUA para a entrega de webhook.

Etapas de verificação

Etapa 1: Verifique o status da integração de terceiros no painel SSE.

Navegue até Admin > Integrações de terceiros no painel SSE e confirme se as integrações estão sendo carregadas corretamente para sua organização.

Etapa 2: configurar regras de firewall.

Atualize seu firewall de rede e todos os firewalls intermediários para permitir conexões HTTPS de entrada dos intervalos IP SSE fornecidos para seu servidor de conectores local.

Etapa 3: Monitore a entrega de eventos webhook.

Após implementar as alterações de firewall, monitore seu conector HTTP local para verificar se os eventos de webhook estão sendo recebidos do Cisco SSE.

Troubleshooting Adicional

Se os eventos de webhook ainda não forem recebidos após a configuração das regras de firewall:

- Verifique se o conector local está configurado corretamente e ouvindo a porta esperada.
- Verifique a conectividade de rede entre os IPs de origem SSE e o endpoint do conector.
- Reveja a configuração de integração de webhook no painel SSE.
- Considere o agendamento de uma sessão de solução de problemas ao vivo para revisar a entrega do webhook em tempo real.

Causa

A falha de entrega do webhook ocorre quando os firewalls de rede bloqueiam conexões HTTPS de entrada de endereços IP de origem Cisco SSE para o conector HTTP local. O Cisco SSE usa faixas de IP específicas de infraestrutura compartilhada em regiões da UE e dos EUA para fornecer eventos de webhook, e estes devem ser permitidos explicitamente através de configurações de firewall para a entrega bem-sucedida de eventos.

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.