Configuration des plages IP et du pare-feu pour l'intégration Webhook d'accès sécurisé

Problème

Les intégrations tierces se chargent correctement dans le tableau de bord Cisco Secure Access (SSE), mais les événements de sécurité basés sur un webhook ne sont pas reçus sur le connecteur HTTP local pour l'intégration SIEM. L'entreprise a besoin de précisions sur les plages d'adresses IP source Cisco SSE, y compris les adresses IP spécifiques à une région, pour configurer correctement les règles de pare-feu et activer la livraison d'événements webhook.

Environnement

- Produit : Accès sécurisé Cisco (SSE)
- Technologie : Assistance pour les solutions - Reporting et consignation d'accès sécurisé
- Type d'intégration : Intégration tierce basée sur Webhook
- Connecteur cible : Serveur de connecteurs HTTP sur site

Résolution

Pour résoudre les problèmes de remise de webhook avec les intégrations Cisco Secure Access, configurez les règles de pare-feu pour autoriser le trafic HTTPS entrant des plages IP source SSE spécifiées vers votre connecteur local.

Plages IP source Cisco SSE

Configurez votre pare-feu pour autoriser les connexions HTTPS entrantes à partir des plages IP source Cisco SSE suivantes :

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

Étapes de configuration du pare-feu

Étape 1: Vérification de l'état de l'intégration tierce

Accédez à Admin > Third Party Integrations dans le tableau de bord SSE et vérifiez que les intégrations se chargent correctement pour votre organisation.

Étape 2: Configurer les règles de pare-feu

Créez des règles de pare-feu pour autoriser le trafic HTTPS entrant (port 443) des plages IP source SSE vers votre serveur de connecteurs local. Assurez-vous que les règles sont appliquées à la fois à votre pare-feu réseau et à tous les pare-feu intermédiaires entre Internet et votre serveur de connecteurs.

Étape 3: Valider la remise des événements Webhook

Après avoir implémenté les modifications du pare-feu, surveillez votre connecteur HTTP local pour confirmer que des événements webhook sont reçus de Cisco SSE.

Informations IP régionales

Cisco SSE utilise uniquement des plages IP partagées dans les régions de l'UE et des États-Unis. Les plages IP fournies couvrent les deux déploiements régionaux et doivent être configurées quelle que soit la région principale dans laquelle se trouve votre entreprise.

Motif

Les événements Webhook de Cisco Secure Access sont bloqués par des règles de pare-feu qui n'autorisent pas les connexions HTTPS entrantes des adresses IP source SSE au serveur de connecteur HTTP local. Bien que le tableau de bord SSE indique un chargement d'intégration réussi, la livraison du webhook nécessite une configuration de pare-feu spécifique pour permettre

au trafic provenant de l'infrastructure Cisco d'atteindre le point d'extrémité du connecteur utilisateur.

Autres informations utiles

- Documentation sur Cisco Secure Access
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.