Dépannage des problèmes de connectivité d'intégration cloud de sécurité sur FMC

Table des matières

Problème

Cisco Firewall Management Center (FMC) ne peut pas établir de connectivité avec Cisco Security Cloud pour l'intégration.

Environnement

- Cisco Secure FMC pour VMware (applicable à tous les modèles)
- Version du logiciel: 7.6.2.1 (applicable à toutes les versions)
- Environnement réseau avec contrôles de sécurité/politiques de pare-feu en amont

Résolution

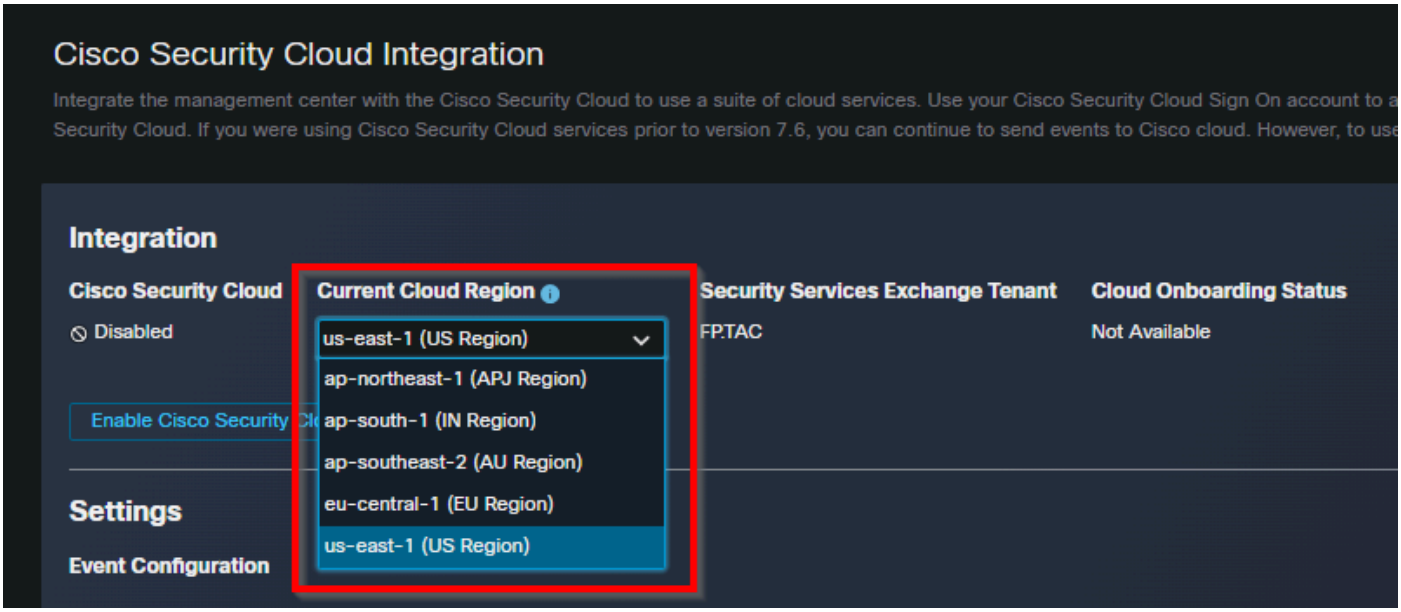
Pour résoudre le problème de connectivité lié à l'intégration de Cisco Security Cloud, procédez comme suit :

1: Testez la connectivité aux URL Cisco Security Cloud requises à l'aide des commandes suivantes du FMC en tant qu'utilisateur racine :

```
curl -v -k https://www.defenseorchestrator.com
nslookup www.defenseorchestrator.com
telnet www.defenseorchestrator.com 443
curl -v -k https://admin.sse.itd.cisco.com
nslookup admin.sse.itd.cisco.com
telnet admin.sse.itd.cisco.com 443
```

```
curl -v -k https://securex.us.security.cisco.com
nslookup securex.us.security.cisco.com
telnet securex.us.security.cisco.com 443
curl -v -k https://api-services.us.sse.itd.cisco.com
nslookup api-services.us.sse.itd.cisco.com
telnet api-services.us.sse.itd.cisco.com 443
curl -v -k https://api-sse.cisco.com
nslookup api-sse.cisco.com
telnet api-sse.cisco.com 443
curl -v -k https://registration.us.sse.itd.cisco.com
nslookup registration.us.sse.itd.cisco.com
telnet registration.us.sse.itd.cisco.com 443
```

2: Si les tests de connectivité indiquent des refus de connexion ou des réponses interdites, mettez à jour les stratégies de sécurité du réseau en amont pour autoriser l'accès HTTPS sortant FMC à toutes les URL de cloud de sécurité Cisco requises pour la région us-east-1, si c'est la région utilisée. Assurez-vous que ces URL sont autorisées sur le port TCP 443 du FMC vers Internet via des pare-feu intermédiaires, des proxys ou des contrôles de sécurité.



image_en_ligne_0.png

- defenseorchestrator.com
- admin.sse.itd.cisco.com
- securex.us.security.cisco.com
- api-services.us.sse.itd.cisco.com
- api-sse.cisco.com
- registration.us.sse.itd.cisco.com

3: Après avoir mis à jour les stratégies de sécurité réseau, recommencez l'intégration de Cisco Security Cloud à partir de l'interface FMC et des commandes curl/telnet. L'intégration se termine maintenant avec succès avec un accès approprié à tous les terminaux cloud requis.

Motif

Le FMC n'a pas pu accéder aux services de back-end du cloud de sécurité Cisco, car les URL du cloud Cisco requises pour la région sélectionnée (us-east-1) n'étaient pas autorisées via les contrôles de sécurité du réseau, ce qui a entraîné des échecs de connexion HTTPS au cours du processus d'intégration.

Autres informations utiles

- Gestion du centre de gestion des pare-feu sur site avec Security Cloud Control
- 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.