Fehlerbehebung: Verbindungsprobleme bei der Sicherheits-Cloud-Integration auf FMC

Problem

Cisco Firewall Management Center (FMC) kann keine Verbindung zur Cisco Security Cloud für die Integration herstellen.

Umwelt

- Cisco Secure FMC für VMware (für alle Modelle)
- Software-Version: 7.6.2.1 (gilt für alle Versionen)
- Netzwerkumgebung mit Upstream-Sicherheitskontrollen/Firewall-Richtlinien

Auflösung

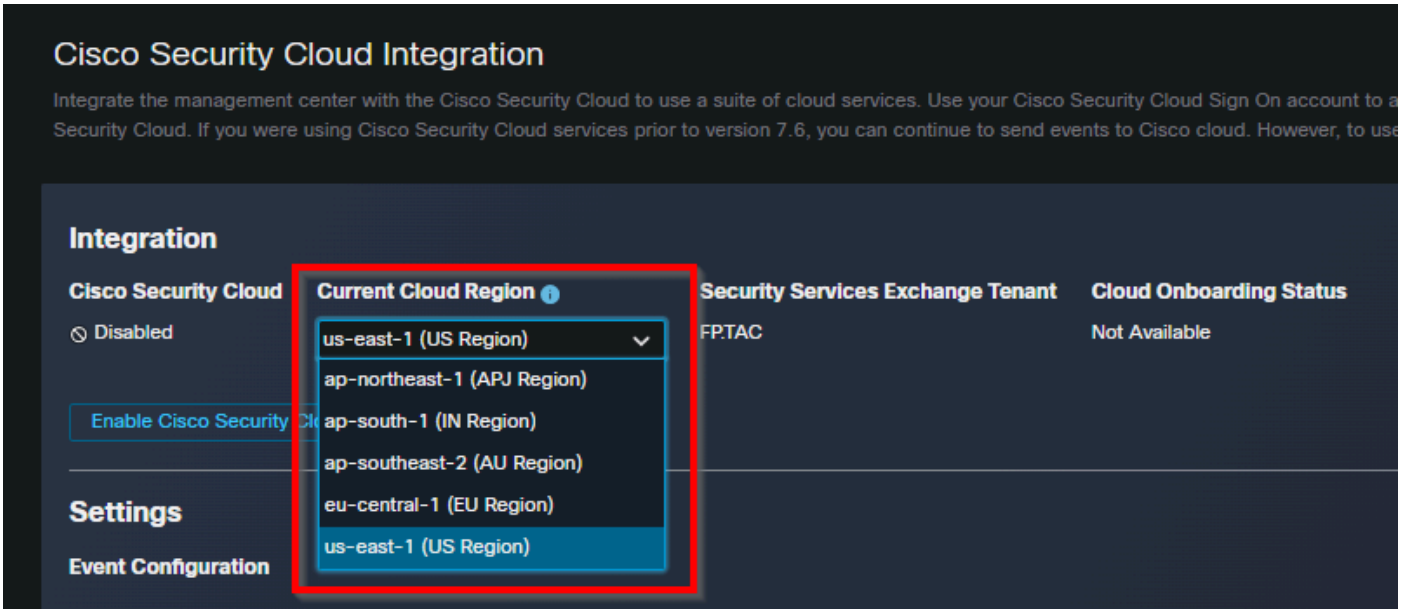
Um das Verbindungsproblem bei der Cisco Security Cloud-Integration zu beheben, befolgen Sie die folgenden Schritte zur Fehlerbehebung und -behebung:

1: Testen Sie die Verbindung zu den erforderlichen Cisco Security Cloud-URLs mithilfe der folgenden Befehle des FMC als Root-Benutzer:

```
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: Wenn die Verbindungstests Verbindungsverweigerungen oder verbotene Antworten zeigen, aktualisieren Sie die Upstream-Netzwerksicherheitsrichtlinien, um ausgehenden HTTPS-Zugriff des FMC auf alle erforderlichen Cisco Security Cloud-URLs für die Region "us-east-1" zuzulassen, falls diese Region verwendet wird. Stellen Sie sicher, dass diese URLs über den TCP-Port 443 vom FMC über zwischengeschaltete Firewalls, Proxys oder Sicherheitskontrollen zum Internet zugelassen werden.



inline_image_0,png

- www.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: Wiederholen Sie nach der Aktualisierung der Netzwerksicherheitsrichtlinien die Cisco Security Cloud-Integration über die FMC-Schnittstelle und die curl/telnet-Befehle. Die Integration wird nun erfolgreich abgeschlossen, und es wird der ordnungsgemäße Zugriff auf alle erforderlichen Cloud-

Endgeräte gewährleistet.

Ursache

Das FMC konnte die Cisco Security Cloud-Backend-Services nicht erreichen, da die erforderlichen Cisco Cloud-URLs für die ausgewählte Region (us-east-1) nicht von den Netzwerksicherheitskontrollen zugelassen wurden. Dies führte zu HTTPS-Verbindungsfehlern während des Integrationsprozesses.

Verwandte Inhalte

- Management des standortbasierten FMC mit Cloud-Sicherheitssteuerung
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.