Problemen met connectiviteit voor cloudintegratie oplossen op FMC

uitgeven

Cisco Firewall Management Center (FMC) kan geen connectiviteit tot stand brengen met Cisco Security Cloud voor integratie.

milieu

- Cisco Secure FMC voor VMware (toepasbaar op alle modellen)
- Softwareversie: 7.6.2.1 (van toepassing op alle versies)
- Netwerkomgeving met upstream beveiligingsmaatregelen/firewallbeleid

resolutie

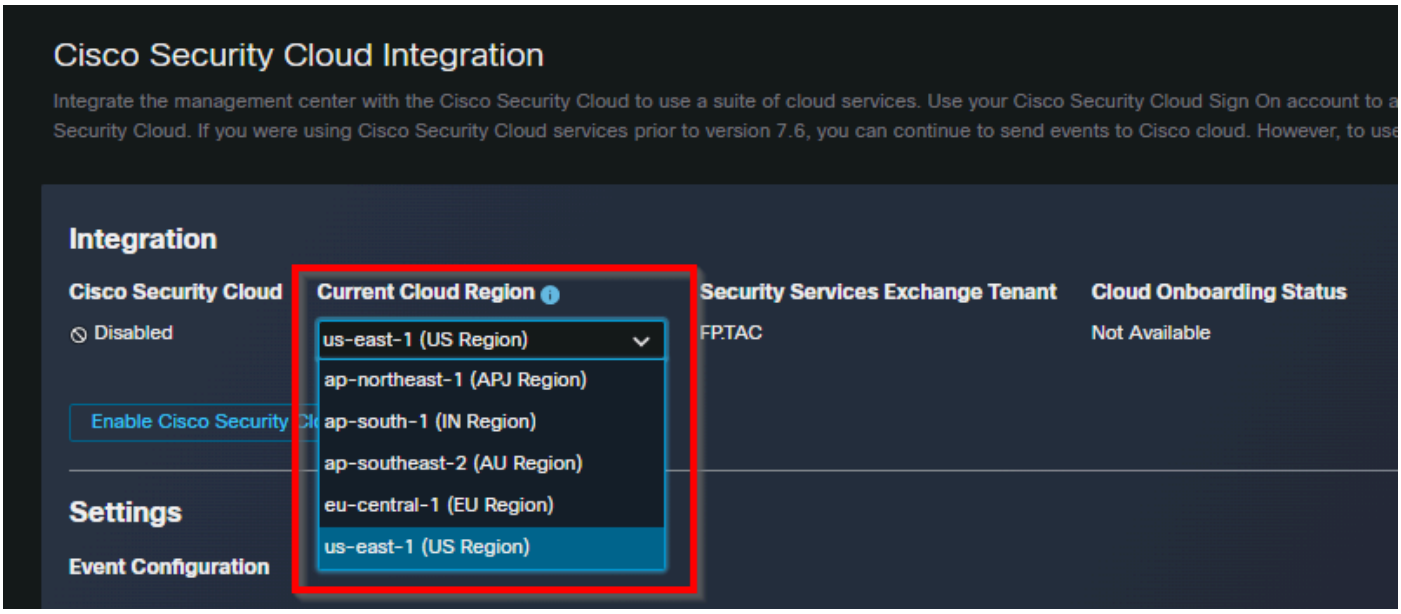
Om het probleem met de connectiviteit van de Cisco Security Cloud-integratie op te lossen, volgt u de volgende stappen voor probleemoplossing en -oplossing:

1: Test de connectiviteit met de vereiste Cisco Security Cloud-URL's met behulp van deze opdrachten van de FMC als hoofdgebruiker:

```
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: Als uit de connectiviteitstests blijkt dat een verbinding wordt geweigerd of verboden, werkt u het upstream netwerkbeveiligingsbeleid bij zodat FMC uitgaande HTTPS-toegang heeft tot alle vereiste Cisco Security Cloud-URL's voor de regio us-east-1, als dat de regio is die wordt gebruikt. Zorg ervoor dat deze URL's zijn toegestaan via TCP-poort 443 van de FMC naar het internet via tussenliggende firewalls, proxies of beveiligingscontroles.



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: Nadat u het beveiligingsbeleid voor het netwerk hebt bijgewerkt, probeert u de Cisco Security Cloud-integratie opnieuw vanuit de FMC-interface en de curl/telnet-opdrachten. De integratie wordt nu succesvol afgerond met de juiste toegang tot alle vereiste cloud-eindpunten.

Oorzaak

De FMC kon de Cisco Security Cloud-backendservices niet bereiken omdat de vereiste Cisco cloud-URL's voor de geselecteerde regio (us-east-1) niet waren toegestaan via de beveiligingscontroles van het netwerk, wat resulteerde in HTTPS-verbindingsfouten tijdens het integratieproces.

Verwante inhoud

- On-Prem FMC beheren met Cloud Security Control
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.