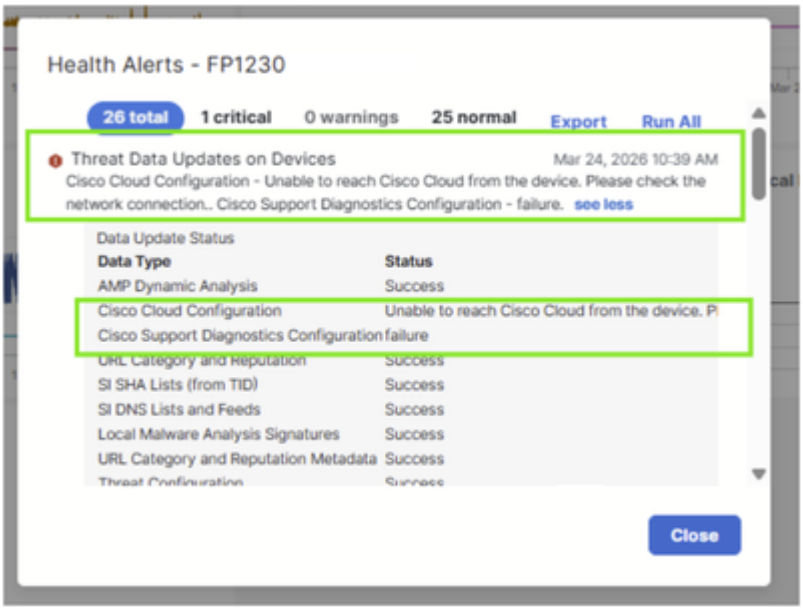
Problemen oplossen FTD kan Cisco Cloud niet bereiken voor updates van bedreigingsgegevens

Inhoud

uitgeven

Een nieuw geïmplementeerd Cisco Secure Firewall (CSF) 1230-apparaat kan de Cisco Cloud niet bereiken, waardoor updates voor Threat Defense niet kunnen worden gedownload. Deze foutmeldingen worden weergegeven in het systeem:

- "Threat Data Updates on Devices - Cisco Cloud Configuration - Kan Cisco Cloud niet bereiken vanaf het apparaat. Controleer de netwerkverbinding."
- "Cisco Support Diagnostics Configuration - failure."



De firewalls lijken goed te functioneren in alle andere aspecten, maar de cloud-connectiviteitsfout voorkomt dat de apparaten kritieke dreigingsinformatie-updates ontvangen van de cloudgebaseerde services van Cisco.

milieu

- FTD-softwareversie: 7.7.11. Ook andere softwareversies kunnen worden beïnvloed.
- HW: CSF1230. Ook andere platformen kunnen getroffen worden.

resolutie

Referentie (meest voorkomende oorzaken)

Voor dit waarschuwingspaar op FTD zijn de meest voorkomende oorzaken:

- De DNS-resolutie (Domain Name System) voor het Cisco-cloudeindpunt mislukt.
- De uitgaande connectiviteit vanuit het beheervlak is geblokkeerd.
- De proxy stoort zich.
- De beheerinterface bereikt het internet via NAT, maar de NAT-configuratie is onjuist.

In dit geval werd het probleem opgelost door de vereiste vertaalregels voor de nieuw geïmplementeerde FTD-apparaten te configureren.

Deze stappen zijn genomen om de connectiviteit in de cloud te herstellen:

Stap 1. Ontbrekende NAT-regels identificeren

Uit het onderzoek bleek dat het ontbreken van goede NAT-regels de firewalls verhinderde om connectiviteit met de Cisco Cloud-services tot stand te brengen. Deze NAT-regels zijn essentieel voor de firewalls om verkeer naar de cloudgebaseerde bedreigingsinlichtingendiensten van Cisco te routeren.

Stap 2. Vertaalregels configureren

De vereiste NAT-regels werden toegevoegd aan de netwerkconfiguratie van de klant om de vereisten voor de cloudconnectiviteit van de nieuwe firewalls te ondersteunen. Deze regels stellen de firewall-apparaten in staat om succesvol te communiceren met de cloudinfrastructuur van Cisco voor updates van bedreigingsgegevens.

Stap 3. Cloudconnectiviteit verifiëren

Na het implementeren van de NAT-regels konden de firewalls met succes verbinding maken met de Cisco Cloud. De eerder weergegeven foutmeldingen werden gewist en de apparaten begonnen zoals verwacht dreigingsinformatie-updates te ontvangen.

De oplossing werd bereikt door configuratiewijzigingen in de netwerkinfrastructuur van de klant in plaats van wijzigingen in de firewallapparaten zelf, waardoor werd gewaarborgd dat de vereisten voor de cloudconnectiviteit voor de nieuwe firewalls naar behoren werden aangepakt.

Oorzaak

De hoofdoorzaak van het connectiviteitsprobleem was het ontbreken van de vereiste NAT-regels in de netwerkconfiguratie van de klant.

Verwante inhoud

- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/217616-troubleshoot-cisco-cloud-configuration.html
- https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/740/management-center-admin-74/reference-ports.html
- 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.