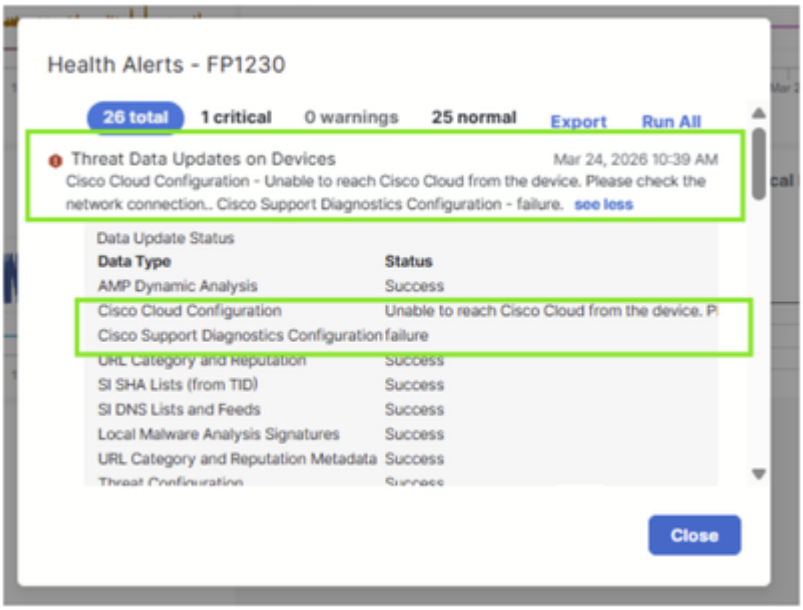
Fehlerbehebung: FTD kann Cisco Cloud nicht erreichen, um Aktualisierungen der Bedrohungsdaten zu erhalten

Inhalt

Problem

Eine neu bereitgestellte Cisco Secure Firewall (CSF) 1230-Appliance kann die Cisco Cloud nicht erreichen und verhindert, dass Threat Defence-Updates heruntergeladen werden. Folgende Fehlermeldungen werden im System angezeigt:

- "Threat Data Updates on Devices - Cisco Cloud Configuration - Vom Gerät aus kann keine Cisco Cloud erreicht werden. Bitte überprüfen Sie die Netzwerkverbindung."
- "Cisco Support Diagnostics Configuration - failure."



Die Firewalls scheinen in allen anderen Aspekten ordnungsgemäß zu funktionieren, aber der Ausfall der Cloud-Verbindung verhindert, dass die Geräte wichtige Threat-Intelligence-Updates von den Cloud-basierten Services von Cisco erhalten.

Umwelt

- FTD-Softwareversion: 7.7.11. Andere Softwareversionen können ebenfalls betroffen sein.
- HW: CSF1230. Andere Plattformen können ebenfalls betroffen sein.

Auflösung

Referenz (häufigste Ursachen)

Die häufigsten Ursachen für dieses Warnpaar bei FTD sind:

- DNS-Auflösung (Domain Name System) für Cisco Cloud-Endpunkt schlägt fehl.
- Ausgehende Verbindungen von der Verwaltungsebene werden blockiert.
- Der Proxy greift ein.
- Die Verwaltungsschnittstelle erreicht das Internet über NAT, aber die NAT-Konfiguration ist falsch.

In diesem Fall wurde das Problem durch die Konfiguration der erforderlichen Übersetzungsregeln für die neu bereitgestellten FTD-Appliances behoben.

Diese Schritte wurden unternommen, um die Cloud-Anbindung wiederherzustellen:

Schritt 1: Identifizieren fehlender NAT-Regeln

Die Untersuchung ergab, dass das Fehlen geeigneter NAT-Regeln die Firewalls daran hinderte, Verbindungen zu den Cisco Cloud-Services herzustellen. Diese NAT-Regeln sind von entscheidender Bedeutung, damit die Firewalls den Datenverkehr korrekt an die Cloud-basierten Services von Cisco zur Erkennung von Sicherheitsrisiken weiterleiten können.

Schritt 2: Übersetzungsregeln konfigurieren

Die erforderlichen NAT-Regeln wurden der Netzwerkkonfiguration des Kunden hinzugefügt, um die Cloud-Konnektivitätsanforderungen der neuen Firewalls zu unterstützen. Mithilfe dieser Regeln können die Firewall-Geräte bei Aktualisierungen von Bedrohungsdaten erfolgreich mit der Cloud-Infrastruktur von Cisco kommunizieren.

Schritt 3: Überprüfen der Cloud-Konnektivität

Nach der Implementierung der NAT-Regeln konnten die Firewalls erfolgreich eine Verbindung zur Cisco Cloud herstellen. Die zuvor angezeigten Fehlermeldungen wurden gelöscht, und die Geräte erhielten wie erwartet Updates mit Bedrohungsinformationen.

Die Lösung wurde durch Konfigurationsänderungen in der Netzwerkinfrastruktur des Kunden erreicht, nicht durch Änderungen an den Firewall-Geräten selbst. So wurde sichergestellt, dass die Cloud-Konnektivitätsanforderungen für die neuen Firewalls ordnungsgemäß erfüllt wurden.

Ursache

Die Ursache des Verbindungsproblems war das Fehlen erforderlicher NAT-Regeln in der Netzwerkkonfiguration des Kunden.

Verwandte Inhalte

- 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
- 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.