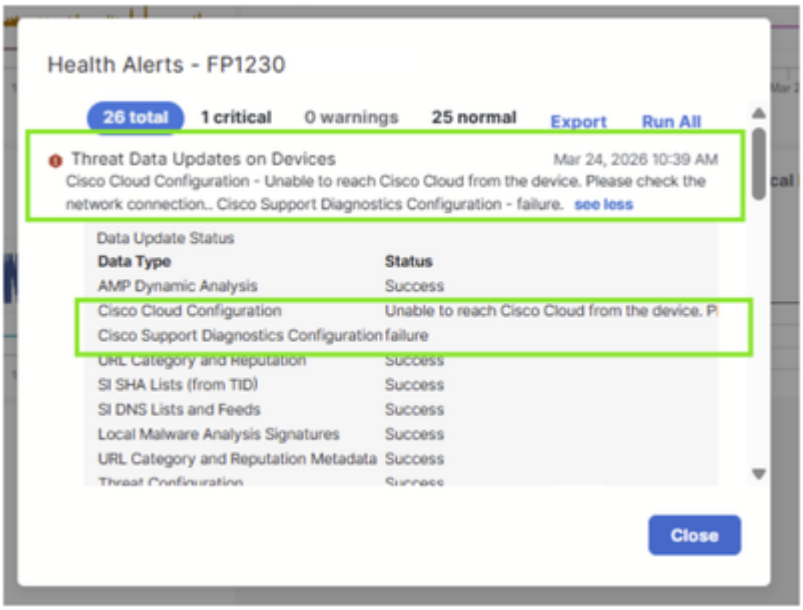
Troubleshoot FTD Unable to Reach Cisco Cloud for Threat Data Updates

Contents

Issue

A newly deployed Cisco Secure Firewall (CSF) 1230 appliance is unable to reach the Cisco Cloud, preventing Threat Defense updates from being downloaded. These error messages are displayed in the system:

- "Threat Data Updates on Devices - Cisco Cloud Configuration - Unable to reach Cisco Cloud from the device. Please check the network connection."
- "Cisco Support Diagnostics Configuration - failure."



The firewalls appear to be functioning properly in all other aspects, but the cloud connectivity failure is preventing the devices from receiving critical threat intelligence updates from Cisco's cloud-based services.

Environment

- FTD Software Version: 7.7.11. Other software versions can be also affected.
- HW: CSF1230. Other platforms can be also affected.

Resolution

Reference (most common causes)

For this alert pair on FTD, the most common causes are:

- Domain Name System (DNS) resolution for the Cisco cloud endpoint fails.
- Outbound connectivity from the management plane is blocked.
- Proxy is interfering.
- The management interface reaches the Internet through NAT but the NAT configuration is incorrect.

In this case, the issue was resolved by configuring the required translation rules for the newly deployed FTD appliances.

These steps were taken to restore cloud connectivity:

Step 1. Identify Missing NAT Rules

The investigation revealed that the absence of proper NAT rules was preventing the firewalls from establishing connectivity to the Cisco Cloud services. These NAT rules are essential for the firewalls to properly route traffic to Cisco's cloud-based threat intelligence services.

Step 2. Configure Translation Rules

The required NAT rules were added to the customer's network configuration to support the new firewalls' cloud connectivity requirements. These rules enable the firewall devices to successfully communicate with Cisco's cloud infrastructure for threat data updates.

Step 3. Verify Cloud Connectivity

After implementing the NAT rules, the firewalls were able to successfully connect to the Cisco Cloud. The previously displayed error messages were cleared, and the devices began receiving threat intelligence updates as expected.

The resolution was achieved through configuration changes on the customer's network infrastructure rather than modifications to the firewall devices themselves, ensuring that the cloud connectivity requirements for the new firewalls were properly addressed.

Cause

The root cause of the connectivity issue was the absence of required NAT rules in the customer's network configuration.

Related Content

- 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 & Downloads