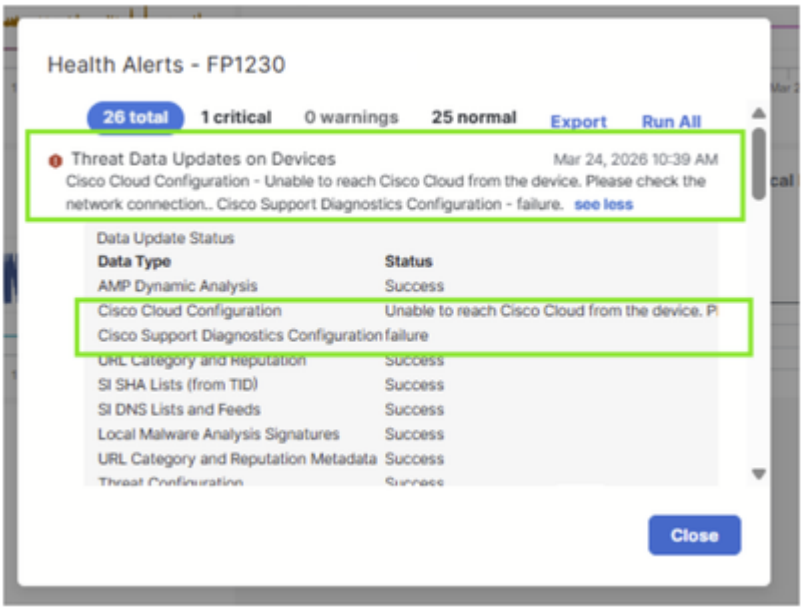
排除FTD无法到达思科云以获取威胁数据更新的故障

目录

问题

新部署的思科安全防火墙(CSF)1230设备无法到达思科云，导致无法下载威胁防御更新。以下错误消息显示在系统中：

- “设备上的威胁数据更新 — 思科云配置 — 无法从设备访问思科云。请检查网络连接。"
- "Cisco支持诊断配置 — 故障。"



防火墙在所有其他方面似乎都运行正常，但云连接故障使设备无法接收来自思科基于云的服务的重要威胁情报更新。

环境

- FTD软件版本：7.7.11.其他软件版本也可能会受到影响。
- 硬件：CSF1230。其他平台也可能受到影响。

分辨率

参考（最常见原因）

对于FTD上的此警报对，最常见的原因包括：

- 思科云终端的域名系统(DNS)解析失败。
- 来自管理平面的出站连接被阻止。
- 代理正在干扰。
- 管理接口通过NAT到达Internet，但NAT配置不正确。

在这种情况下，通过配置新部署的FTD设备所需的转换规则，问题得以解决。

恢复云连接采取以下步骤：

步骤1.识别缺失的NAT规则

调查发现，缺乏适当的NAT规则阻止防火墙建立与思科云服务的连接。这些NAT规则对于防火墙将流量正确路由到思科基于云的威胁情报服务至关重要。

步骤2.配置转换规则

所需的NAT规则已添加到客户的网络配置中，以支持新防火墙的云连接要求。这些规则使防火墙设备能够成功与思科的云基础设施通信，以进行威胁数据更新。

步骤3.检验云连接

实施NAT规则后，防火墙成功连接到思科云。之前显示的错误消息被清除，设备开始按预期接收威胁情报更新。

解决方案是通过更改客户的网络基础设施配置（而不是修改防火墙设备本身）实现的，从而确保正确满足新防火墙的云连接要求。

原因

连接问题的根本原因是客户的网络配置中缺乏所需的NAT规则。

相关内容

- 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
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。