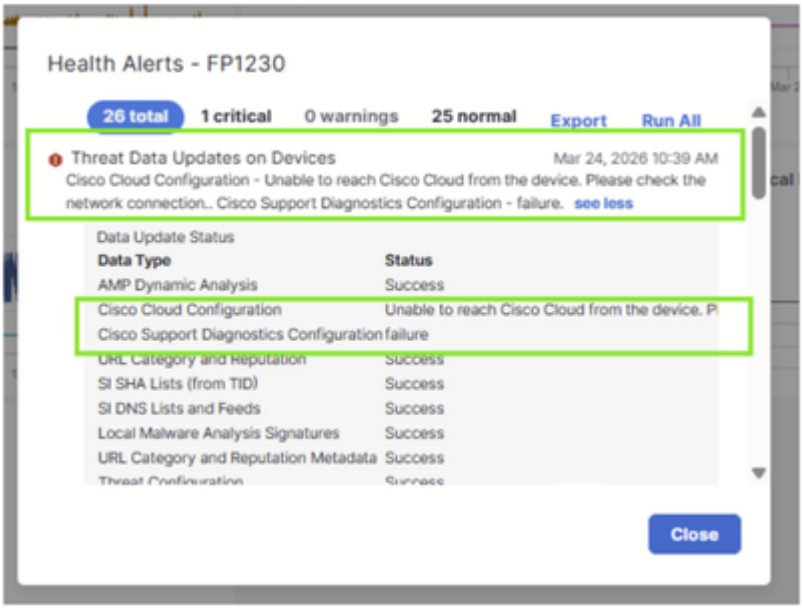
Resolución de problemas FTD no puede alcanzar la nube de Cisco para actualizaciones de datos de amenazas

Contenido

Problema

Un dispositivo Cisco Secure Firewall (CSF) 1230 recién implementado no puede acceder a la nube de Cisco, lo que impide que se descarguen las actualizaciones de Threat Defence. Estos mensajes de error se muestran en el sistema:

- "Actualizaciones de datos de amenazas en dispositivos: configuración de la nube de Cisco; no se puede acceder a la nube de Cisco desde el dispositivo. Compruebe la conexión de red."
- "Configuración de diagnóstico de soporte de Cisco: error".



Los firewalls parecen funcionar correctamente en todos los demás aspectos, pero el fallo de conectividad de la nube impide que los dispositivos reciban actualizaciones de inteligencia de amenazas críticas de los servicios basados en la nube de Cisco.

Entorno

- Versión del software FTD: 7.7.11. Otras versiones de software también pueden verse afectadas.
- HW: CSF1230. Otras plataformas también pueden verse afectadas.

Resolución

Referencia (causas más comunes)

Para este par de alertas en FTD, las causas más comunes son:

- La resolución del sistema de nombres de dominio (DNS) para el terminal en la nube de Cisco falla.
- La conectividad saliente desde el plano de administración está bloqueada.
- El proxy está interfiriendo.
- La interfaz de administración llega a Internet a través de NAT, pero la configuración de NAT es incorrecta.

En este caso, el problema se resolvió configurando las reglas de conversión necesarias para los dispositivos FTD implementados recientemente.

Para restaurar la conectividad de la nube, se han tomado las siguientes medidas:

Paso 1. Identificar las reglas NAT que faltan

La investigación reveló que la ausencia de reglas NAT adecuadas estaba impidiendo que los firewalls establecieran conectividad con los servicios en la nube de Cisco. Estas reglas NAT son esenciales para que los firewalls enruten correctamente el tráfico a los servicios de inteligencia de amenazas basados en la nube de Cisco.

Paso 2. Configurar reglas de traducción

Las reglas NAT necesarias se agregaron a la configuración de red del cliente para cumplir los requisitos de conectividad en la nube de los nuevos firewalls. Estas reglas permiten que los dispositivos de firewall se comuniquen correctamente con la infraestructura de nube de Cisco para las actualizaciones de datos de amenazas.

Paso 3. Verificar la conectividad de la nube

Después de implementar las reglas NAT, los firewalls pudieron conectarse correctamente a la nube de Cisco. Se eliminaron los mensajes de error mostrados anteriormente y los dispositivos comenzaron a recibir actualizaciones de inteligencia de amenazas según lo previsto.

La resolución se logró mediante cambios de configuración en la infraestructura de red del cliente en lugar de modificaciones en los dispositivos de firewall, lo que garantiza que se cumplieron correctamente los requisitos de conectividad en la nube para los nuevos firewalls.

Causa

La causa raíz del problema de conectividad fue la ausencia de reglas NAT requeridas en la configuración de red del cliente.

Contenido relacionado

- 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
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).