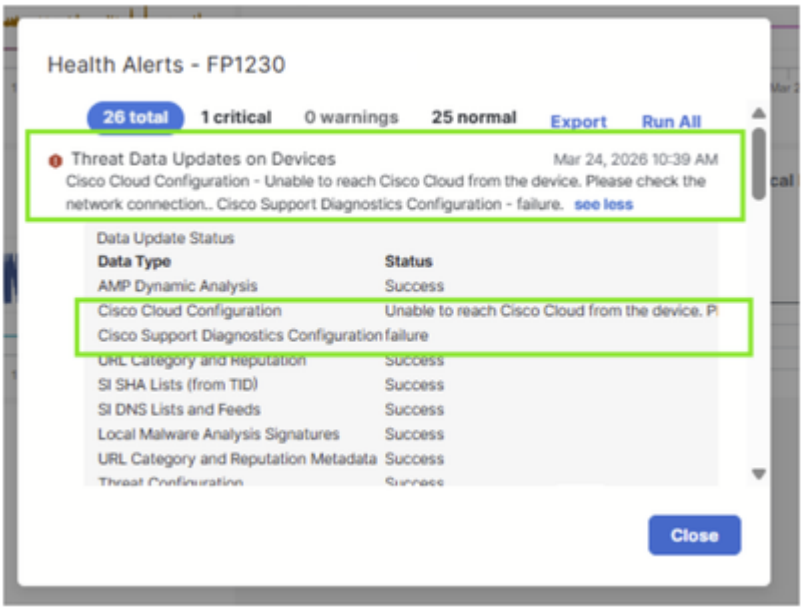
Risoluzione dei problemi relativi a FTD non in grado di raggiungere Cisco Cloud per gli aggiornamenti dei dati sulle minacce

Sommario

Problema

Un accessorio Cisco Secure Firewall (CSF) 1230 di nuova implementazione non è in grado di raggiungere il cloud Cisco, impedendo il download degli aggiornamenti di Threat Defense. Nel sistema vengono visualizzati i seguenti messaggi di errore:

- "Threat Data Updates on Devices - Cisco Cloud Configuration - Impossibile raggiungere Cisco Cloud dal dispositivo. Controllare la connessione di rete."
- "Configurazione di Cisco Support Diagnostics - errore".



I firewall sembrano funzionare correttamente in tutti gli altri aspetti, ma l'errore di connettività del cloud impedisce ai dispositivi di ricevere gli aggiornamenti di critical threat intelligence dai servizi basati su cloud Cisco.

Ambiente

- Versione software FTD: 7.7.11. Possono essere interessate anche altre versioni del software.
- HARDWARE: CSF1230. Possono essere interessate anche altre piattaforme.

Risoluzione

Riferimento (cause più comuni)

Per questa coppia di avvisi su FTD, le cause più comuni sono:

- Risoluzione DNS (Domain Name System) per l'endpoint cloud Cisco non riuscita.
- La connettività in uscita dal piano di gestione è bloccata.
- Il proxy sta interferendo.
- L'interfaccia di gestione raggiunge Internet tramite NAT, ma la configurazione NAT non è corretta.

In questo caso, il problema è stato risolto configurando le regole di conversione necessarie per i nuovi accessori FTD implementati.

Per ripristinare la connettività cloud, sono stati eseguiti i seguenti passaggi:

Passaggio 1. Identificazione delle regole NAT mancanti

L'indagine ha rivelato che la mancanza di adeguate norme NAT impediva ai firewall di stabilire la connettività ai servizi cloud Cisco. Queste regole NAT sono essenziali per i firewall in modo da indirizzare correttamente il traffico ai servizi Cisco basati su cloud Threat Intelligence.

Passaggio 2. Configurare le regole di conversione

Le regole NAT richieste sono state aggiunte alla configurazione di rete del cliente per supportare i requisiti di connettività cloud dei nuovi firewall. Queste regole consentono ai dispositivi firewall di comunicare con successo con l'infrastruttura cloud di Cisco per gli aggiornamenti dei dati relativi alle minacce.

Passaggio 3. Verifica della connettività del cloud

Dopo aver implementato le regole NAT, i firewall sono stati in grado di connettersi con successo al Cisco Cloud. I messaggi di errore visualizzati in precedenza sono stati cancellati e i dispositivi hanno iniziato a ricevere gli aggiornamenti relativi alle minacce come previsto.

La risoluzione è stata raggiunta tramite modifiche alla configurazione dell'infrastruttura di rete del cliente anziché modifiche ai dispositivi firewall stessi, garantendo che i requisiti di connettività cloud per i nuovi firewall fossero adeguatamente soddisfatti.

Causa

La causa principale del problema di connettività è stata l'assenza delle regole NAT richieste nella configurazione di rete del cliente.

Contenuto correlato

- 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
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).