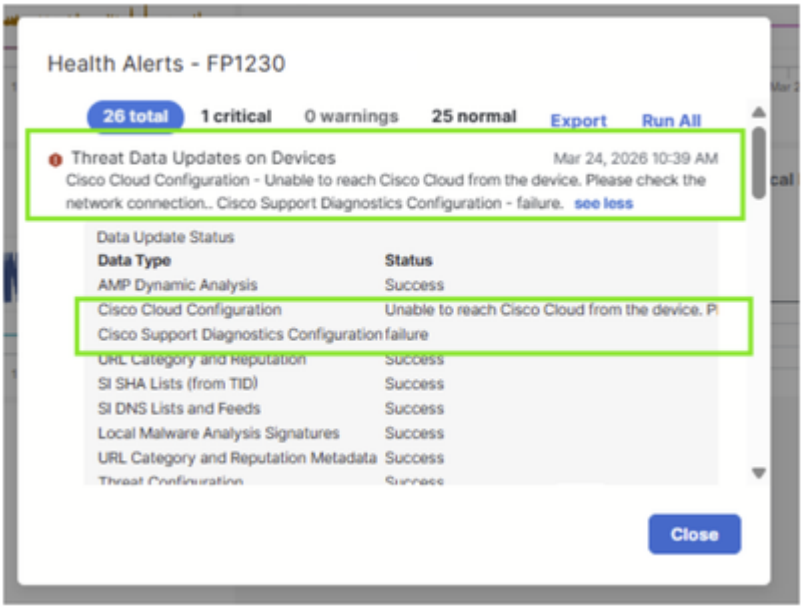
Dépannage du FTD incapable d'atteindre le cloud Cisco pour les mises à jour des données sur les menaces

Table des matières

Problème

Une appliance Cisco Secure Firewall (CSF) 1230 nouvellement déployée ne parvient pas à atteindre le cloud Cisco, ce qui empêche le téléchargement des mises à jour Threat Defense. Les messages d'erreur suivants s'affichent dans le système :

- « Mises à jour des données de menace sur les périphériques - Configuration du cloud Cisco - Impossible d'atteindre le cloud Cisco à partir du périphérique. Vérifiez la connexion réseau."
- "Configuration des diagnostics du support technique Cisco - échec."



Les pare-feu semblent fonctionner correctement dans tous les autres aspects, mais la défaillance de la connectivité cloud empêche les périphériques de recevoir des mises à jour critiques des informations sur les menaces provenant des services cloud de Cisco.

Environnement

- Version du logiciel FTD : 7.7.11. D’autres versions logicielles peuvent également être affectées.
- MATÉRIEL : CSF1230. D’autres plates-formes peuvent également être affectées.

Résolution

Référence (causes les plus courantes)

Pour cette paire d'alertes sur FTD, les causes les plus courantes sont :

- La résolution DNS (Domain Name System) du point de terminaison cloud Cisco échoue.
- La connectivité sortante du plan de gestion est bloquée.
- Le proxy interfère.
- L’interface de gestion atteint Internet via la fonction NAT, mais la configuration de cette fonction est incorrecte.

Dans ce cas, le problème a été résolu en configurant les règles de traduction requises pour les appliances FTD nouvellement déployées.

Les étapes suivantes ont été suivies pour restaurer la connectivité du cloud :

Étape 1 : identification des règles NAT manquantes

L'enquête a révélé que l'absence de règles NAT appropriées empêchait les pare-feu d'établir une connectivité aux services cloud Cisco. Ces règles NAT sont essentielles pour que les pare-feu acheminent correctement le trafic vers les services cloud de renseignements sur les menaces de Cisco.

Étape 2 : configuration des règles de traduction

Les règles NAT requises ont été ajoutées à la configuration réseau du client pour prendre en charge les exigences de connectivité cloud des nouveaux pare-feu. Ces règles permettent aux périphériques pare-feu de communiquer avec l'infrastructure cloud de Cisco pour les mises à jour des données sur les menaces.

Étape 3. Vérification de la connectivité du cloud

Une fois les règles NAT implémentées, les pare-feu ont pu se connecter au cloud Cisco. Les messages d'erreur précédemment affichés ont été effacés et les périphériques ont commencé à recevoir les mises à jour de renseignements sur les menaces comme prévu.

La résolution a été obtenue par des modifications de configuration sur l'infrastructure réseau du client plutôt que par des modifications sur les périphériques pare-feu eux-mêmes, garantissant que les exigences de connectivité cloud pour les nouveaux pare-feu ont été correctement traitées.

Motif

La cause principale du problème de connectivité était l'absence de règles NAT requises dans la configuration réseau du client.

Autres informations utiles

- 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
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.