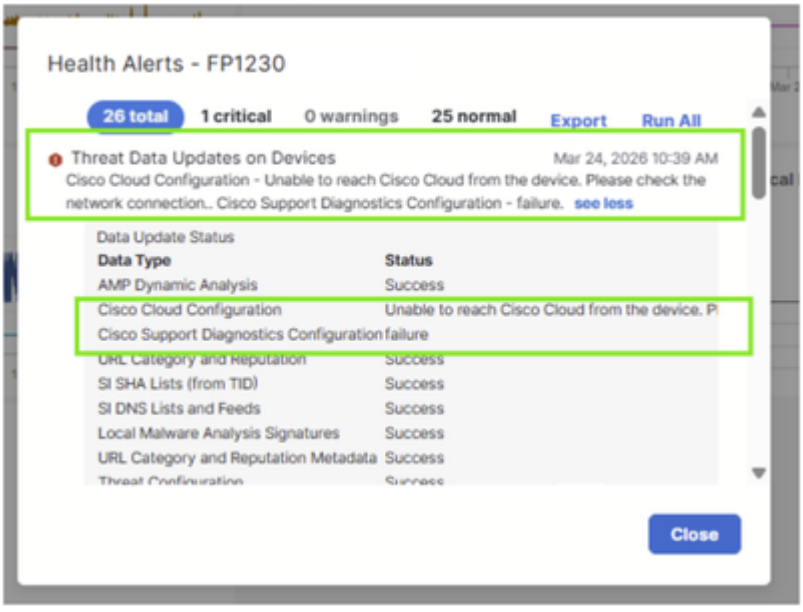
Troubleshooting de FTD Incapaz de Alcançar o Cisco Cloud para Atualizações de Dados de Ameaças

Contents

Problema

Um dispositivo Cisco Secure Firewall (CSF) 1230 recém-implantado não consegue acessar a nuvem da Cisco, impedindo o download de atualizações do Threat Defense. Estas mensagens de erro são exibidas no sistema:

- "Atualizações de dados de ameaças em dispositivos - Configuração de nuvem da Cisco - Não é possível acessar a nuvem da Cisco a partir do dispositivo. Verifique a conexão de rede."
- "Configuração do Cisco Support Diagnostics - falha."



Os firewalls parecem estar funcionando corretamente em todos os outros aspectos, mas a falha de conectividade de nuvem está impedindo que os dispositivos recebam atualizações de inteligência de ameaças críticas dos serviços baseados em nuvem da Cisco.

Ambiente

- Versão do software FTD: 7.7.11. Outras versões de software também podem ser afetadas.
- HW CSF1230. Outras plataformas também podem ser afetadas.

Resolução

Referência (causas mais comuns)

Para esse par de alertas no FTD, as causas mais comuns são:

- Falha na resolução do Sistema de Nomes de Domínio (DNS) para o endpoint de nuvem da Cisco.
- A conectividade de saída do plano de gerenciamento está bloqueada.
- O proxy está interferindo.
- A interface de gerenciamento alcança a Internet através do NAT, mas a configuração do NAT está incorreta.

Nesse caso, o problema foi resolvido com a configuração das regras de conversão necessárias para os dispositivos FTD recém-implantados.

Estas etapas foram executadas para restaurar a conectividade de nuvem:

Etapa 1. Identificar as regras de NAT ausentes

A investigação revelou que a ausência de regras de NAT adequadas estava impedindo que os firewalls estabelecessem conectividade com os serviços de nuvem da Cisco. Essas regras de NAT são essenciais para que os firewalls roteiem adequadamente o tráfego para os serviços de inteligência contra ameaças baseados em nuvem da Cisco.

Etapa 2. Configurar Regras de Conversão

As regras de NAT necessárias foram adicionadas à configuração de rede do cliente para suportar os requisitos de conectividade de nuvem dos novos firewalls. Essas regras permitem que os dispositivos de firewall se comuniquem com êxito com a infraestrutura de nuvem da Cisco para atualizações de dados de ameaças.

Etapa 3. Verificar a conectividade da nuvem

Após a implementação das regras de NAT, os firewalls conseguiram se conectar com êxito ao Cisco Cloud. As mensagens de erro exibidas anteriormente foram apagadas e os dispositivos começaram a receber atualizações de inteligência de ameaças como esperado.

A resolução foi obtida por meio de alterações de configuração na infraestrutura de rede do cliente, em vez de modificações nos próprios dispositivos de firewall, garantindo que os requisitos de conectividade de nuvem para os novos firewalls fossem tratados adequadamente.

Causa

A causa principal do problema de conectividade foi a ausência das regras de NAT necessárias na configuração de rede do cliente.

Conteúdo 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
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.