Resolver advertencia " de VA se encuentra en un estado de atención"

Contenido

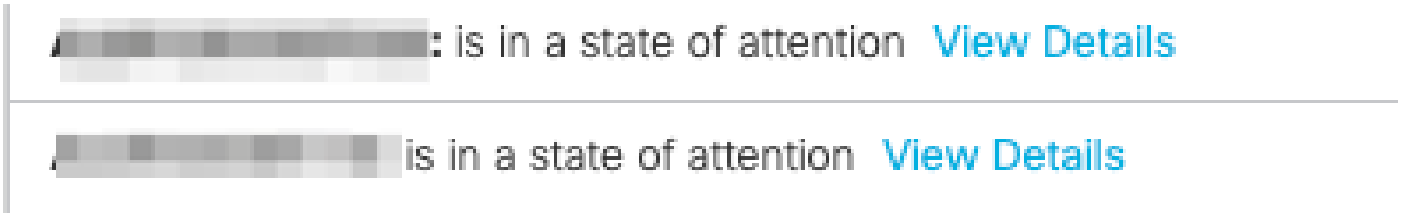
Introducción

Este documento describe cómo resolver la advertencia de VA indicando que su VA "está en un estado de atención" relacionado con la habilitación de DNSCrypt.

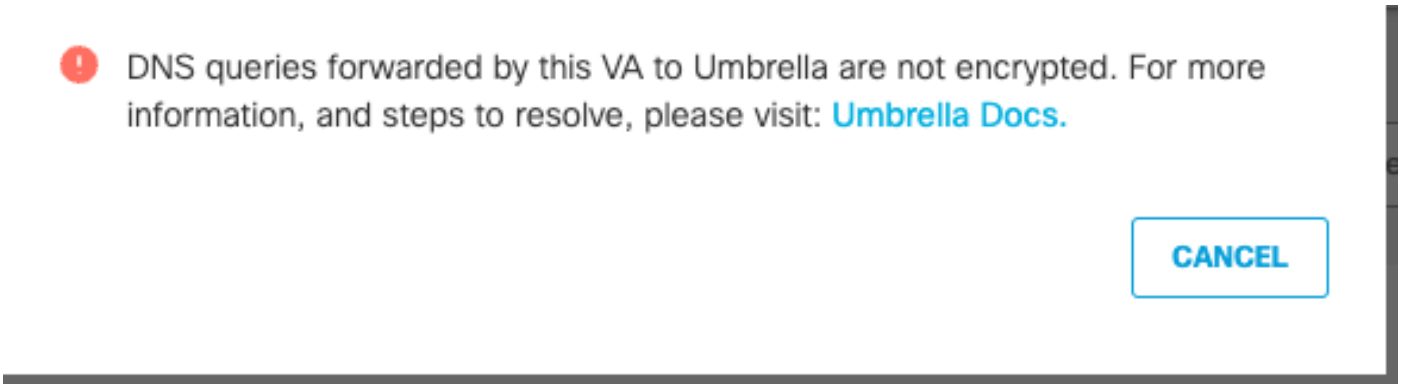
Overview

El dispositivo virtual (VA) admite el cifrado DNSCrypt entre sí y los resolvers del sistema de nombres de dominio (DNS) público OpenDNS. DNSCrypt cifra los paquetes DNS que el VA reenvía, lo que evita la intercepción de información confidencial. DNSCrypt está habilitado de forma predeterminada para una protección óptima, pero puede encontrar problemas si un firewall bloquea el tráfico cifrado entre su VA y los resolvers de DNS públicos.

El tráfico DNS no cifrado supone un riesgo de seguridad que debe abordar. Cuando no se puede establecer el cifrado entre el VA y OpenDNS, el panel de Umbrella muestra una advertencia de que el dispositivo virtual afectado "está en un estado de atención" para garantizar que se mantiene la mejor protección posible.



Si hace clic en Ver detalles, verá un mensaje que indica que las consultas DNS reenviadas por este VA a OpenDNS no están cifradas.

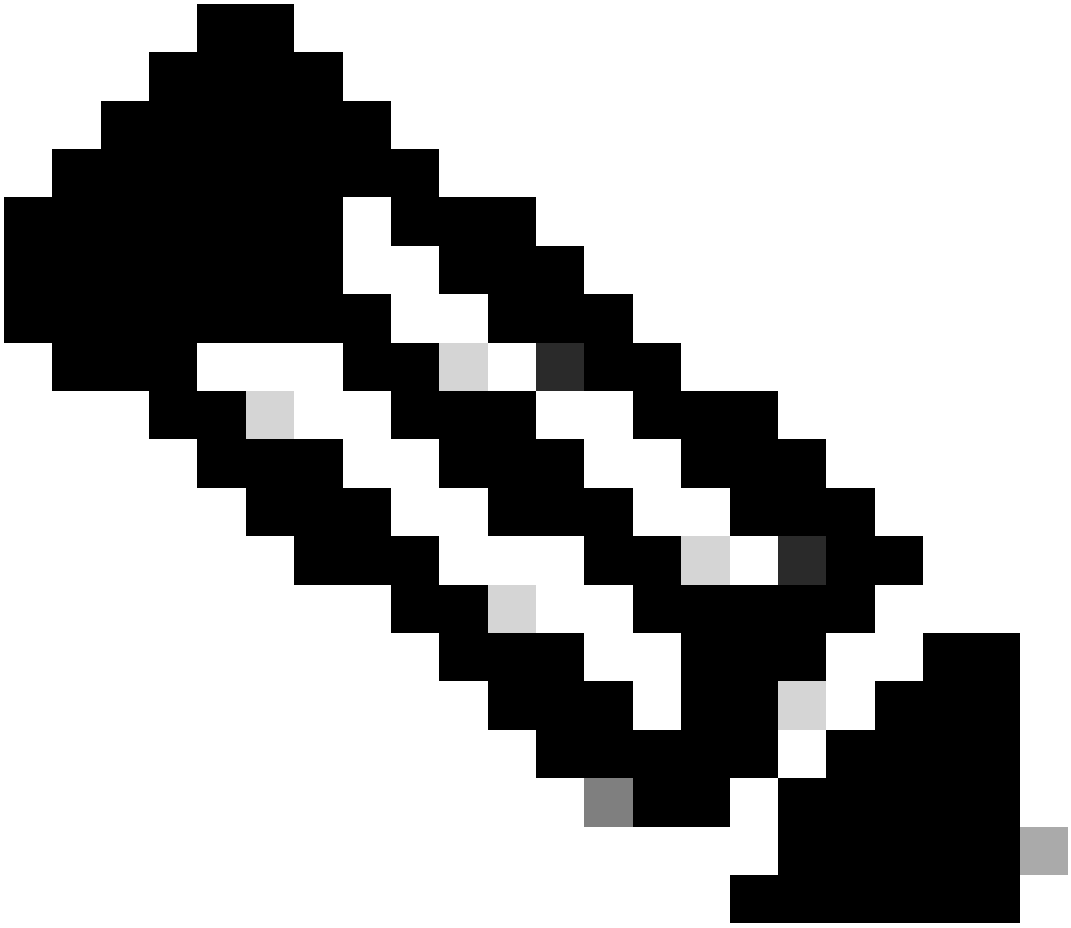


Nota: DNSCrypt solo está disponible en dispositivos virtuales que ejecutan la versión 1.5.x o superior. Si sólo tiene un dispositivo virtual y no se ha actualizado, también aparecerá este mensaje.

Resolver la advertencia de DNSCrypt

Para resolver la advertencia y restaurar la protección DNSCrypt:

1. Revise la configuración de su firewall o sistema de prevención de intrusiones (IPS)/sistema de detección de intrusiones (IDS).
2. Asegúrese de que su firewall o IPS/IDS permite el tráfico DNSCrypt cifrado para el dispositivo virtual.
3. Permitir el tráfico saliente y entrante en el puerto 53 (UDP/TCP) a estas direcciones IP de OpenDNS:
    - 208.67.220.220
    - 208.67.222.222
    - 208.67.222.220
    - 208.67.220.222
4. Si utiliza un firewall o IPS/IDS con inspección profunda de paquetes, compruebe que no bloquea ni interfiere con los paquetes DNSCrypt cifrados. Algunos dispositivos pueden bloquear estos paquetes si solo esperan tráfico DNS estándar en el puerto 53.
5. Confirme que el tráfico cifrado pueda fluir tanto saliente como entrante entre su red y los resolvers OpenDNS en todos los dispositivos de la ruta.



Nota: Si su firewall o IPS/IDS bloquean el tráfico DNSCrypt, la resolución de DNS puede fallar para los usuarios detrás del VA.

Si cree que su firewall ya permite este tráfico pero la advertencia persiste, abra un caso de soporte para obtener más ayuda.

Para obtener más información sobre el comportamiento del firewall Cisco ASA y los posibles mensajes de error relacionados con la inspección profunda de paquetes y DNSCrypt, consulte: ¿Por qué el firewall Cisco ASA bloquea la funcionalidad DNSCrypt del dispositivo virtual Umbrella?

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).