解决警告VA "；处于关注状态"

目录

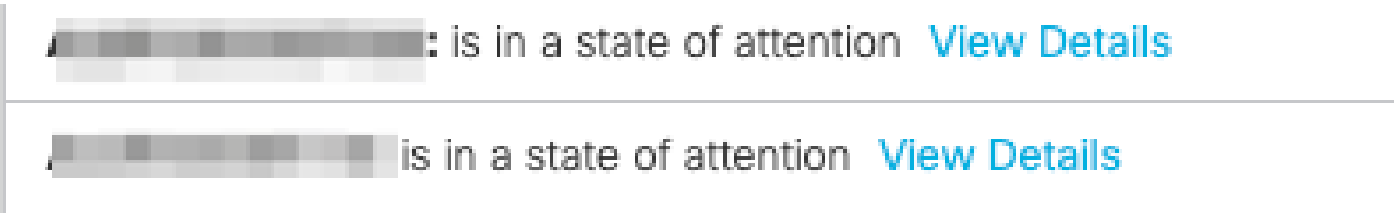
简介

本文档介绍如何解决有关启用DNSCrypt的VA“处于注意状态”的VA警告。

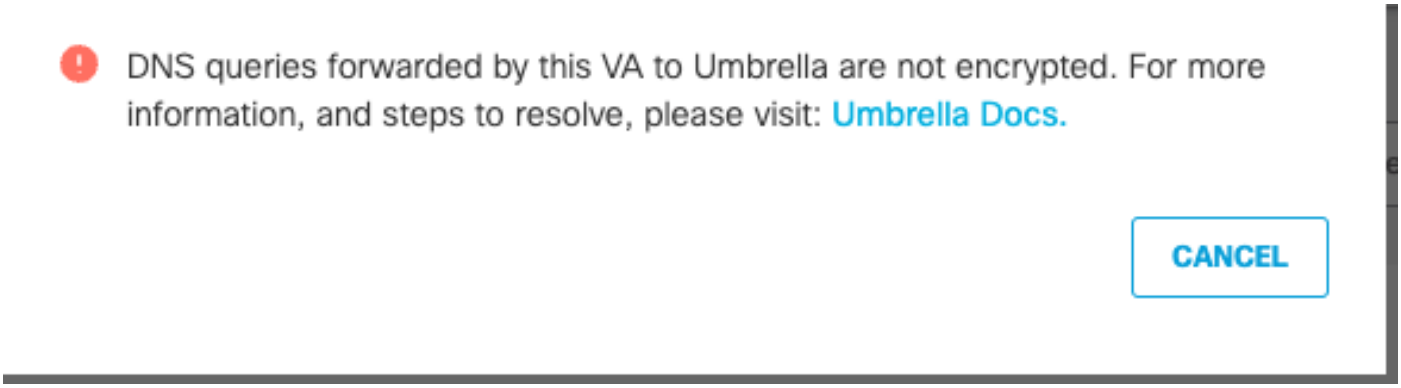
概述

虚拟设备(VA)在其自身和OpenDNS公共域名系统(DNS)解析器之间支持DNSCrypt加密。DNSCrypt加密VA转发的DNS数据包，防止拦截敏感信息。默认情况下启用DNSCrypt以实现最佳保护，但是如果防火墙阻止VA和公共DNS解析器之间的加密流量，则可能会遇到问题。

未加密的DNS流量是您必须应对的安全风险。当VA和OpenDNS之间无法建立加密时，Umbrella控制面板会显示一条警告，指示受影响的虚拟设备“处于注意状态”，以确保您保持尽可能最好的保护。



如果单击View Details，则会看到一条消息，指示此VA转发到OpenDNS的DNS查询未加密。

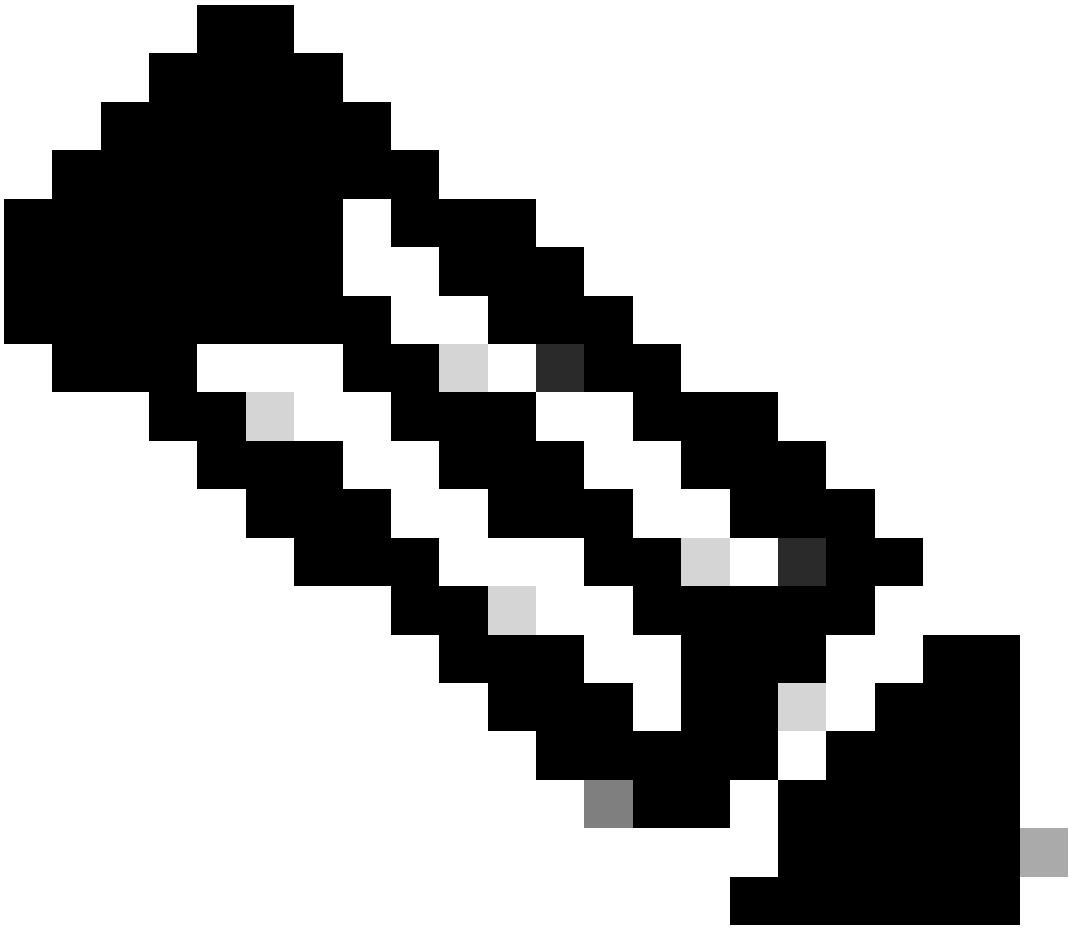


注意：DNSCrypt仅在运行版本1.5.x或更高版本的虚拟设备中可用。如果您只有一个VA且它尚未升级，则还会显示此消息。

解决DNSCrypt警告

要解决警告并恢复DNSCrypt保护，请执行以下操作：

1. 检查您的防火墙或入侵防御系统(IPS)/入侵检测系统(IDS)配置。
2. 确保您的防火墙或IPS/IDS允许VA的加密DNSCrypt流量。
3. 允许端口53(UDP/TCP)上的出站和入站流量流向以下OpenDNS IP地址：
    - 208.67.220.220
    - 208.67.222.222
    - 208.67.222.220
    - 208.67.220.222
4. 如果使用防火墙或IPS/IDS进行深度数据包检测，请确认其不会阻止或干扰加密的DNSCrypt数据包。如果某些设备只期望在端口53上获得标准DNS流量，则它们可以阻止这些数据包。
5. 确认加密流量可以在网络与路径中所有设备的OpenDNS解析器之间同时流经出站和入站。



注意：如果防火墙或IPS/IDS阻止DNSCrypt流量，VA后面的用户的DNS解析可能会失败。

如果您认为您的防火墙已允许此流量，但警告仍然存在，请打开支持案例以获得进一步帮助。

有关Cisco ASA防火墙行为以及与深度数据包检测和DNSCrypt相关的可能错误消息的详细信息，请参阅：为什么Cisco ASA防火墙会阻止Umbrella虚拟设备的DNSCrypt功能？

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。