解決警告VA "；處於注意"；狀態

目錄

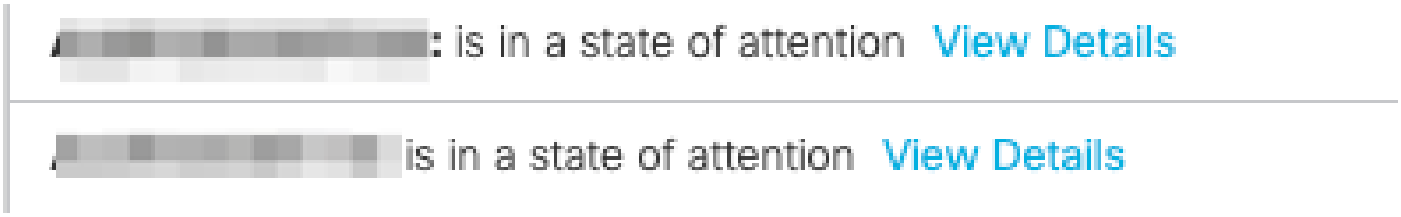
簡介

本文檔介紹如何解決有關啟用DNSCrypt的VA「處於注意狀態」的VA警告。

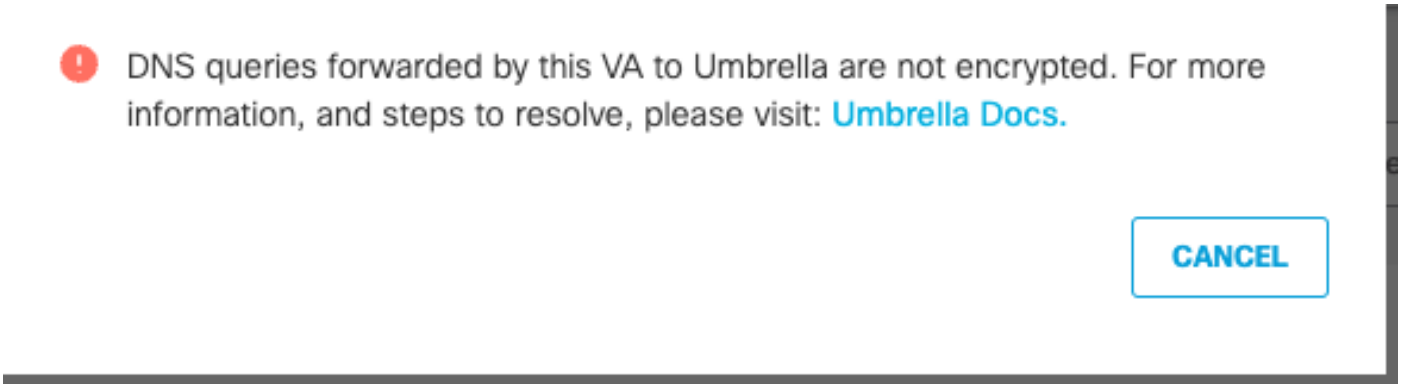
概觀

虛擬裝置(VA)支援自身和OpenDNS公共域名系統(DNS)解析器之間的DNSCrypt加密。DNSCrypt會加密VA轉發的DNS資料包，防止攔截敏感資訊。預設情況下啟用DNSCrypt以獲得最佳保護，但是如果防火牆阻止VA和公共DNS解析器之間的加密流量，則可能會遇到問題。

未加密的DNS流量是一種必須解決的安全風險。當VA和OpenDNS之間無法建立加密時，Umbrella控制面板會顯示一條警告，說明受影響的虛擬裝置「處於注意狀態」，以確保您保持儘可能最好的保護。



如果按一下View Details，您會看到一條消息，指出此VA向OpenDNS轉發的DNS查詢未加密。

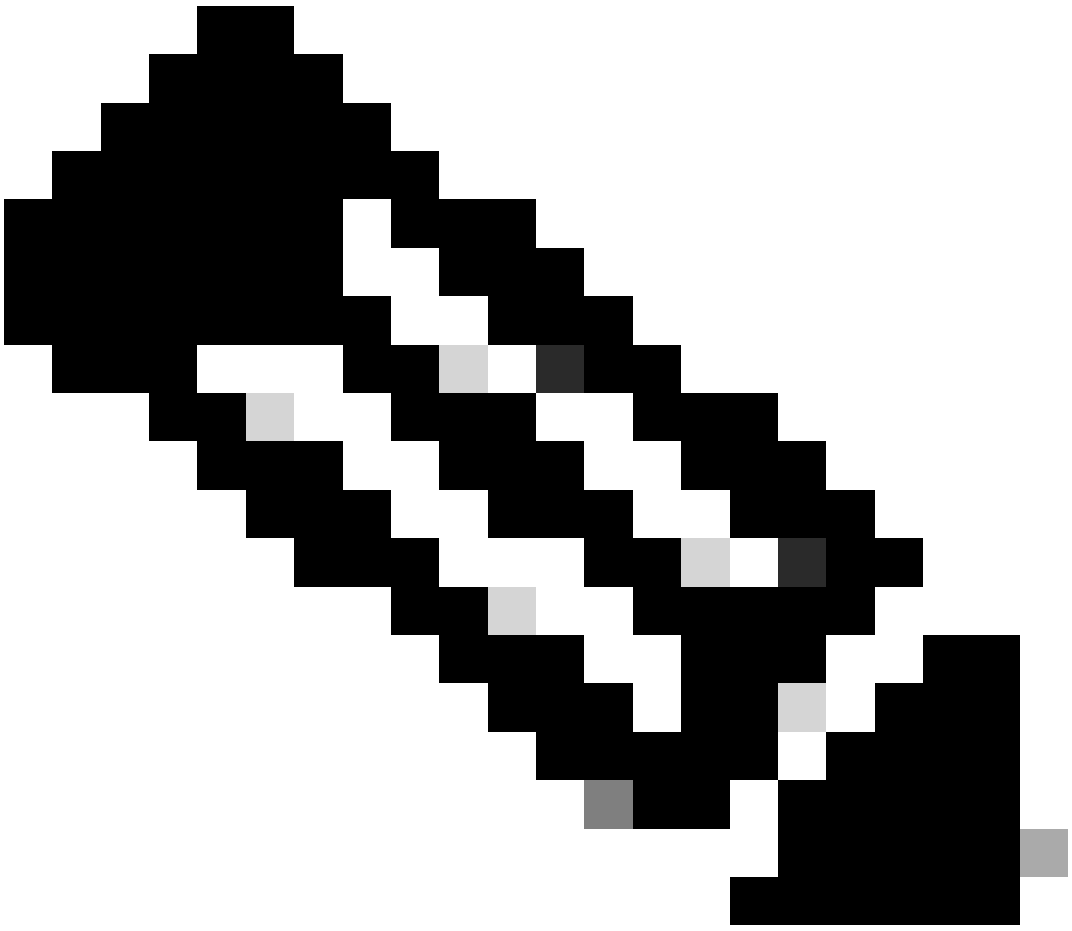


附註：DNSCrypt僅在運行1.5.x或更高版本的虛擬裝置中可用。如果您只有一個VA且它尚未升級，則還會出現此消息。

解決DNSCrypt警告

要解決警告並恢復DNSCrypt保護：

1. 檢查您的防火牆或入侵防禦系統(IPS)/入侵檢測系統(IDS)配置。
2. 確保您的防火牆或IPS/IDS允許針對VA的加密DNSCrypt流量。
3. 允許連線埠53(UDP/TCP)上的傳出和傳入流量到達以下OpenDNS IP位址：
    - 208.67.220.220
    - 208.67.222.222
    - 208.67.222.220
    - 208.67.220.222
4. 如果使用防火牆或IPS/IDS進行深度資料包檢測，請確認其不會阻止或干擾加密的DNSCrypt資料包。如果某些裝置只期望在埠53上獲得標準DNS流量，則它們可以阻止這些資料包。
5. 確認加密的流量可以在您的網路與路徑中所有裝置的OpenDNS解析器之間同時進行出站和入站流量。



附註：如果您的防火牆或IPS/IDS阻止DNSCrypt流量，則VA後面的使用者的DNS解析可能會失敗。

如果您認為防火牆已允許此流量，但警告仍然存在，請開啟支援案例以獲得進一步協助。

有關Cisco ASA防火牆行為以及與深度資料包檢測和DNSCrypt相關的可能錯誤消息的詳細資訊，請參閱：為什麼Cisco ASA防火牆阻止來自Umbrella虛擬裝置的DNSCrypt功能？

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。