Risolvi avviso VA "è in uno stato di attenzione"

Sommario

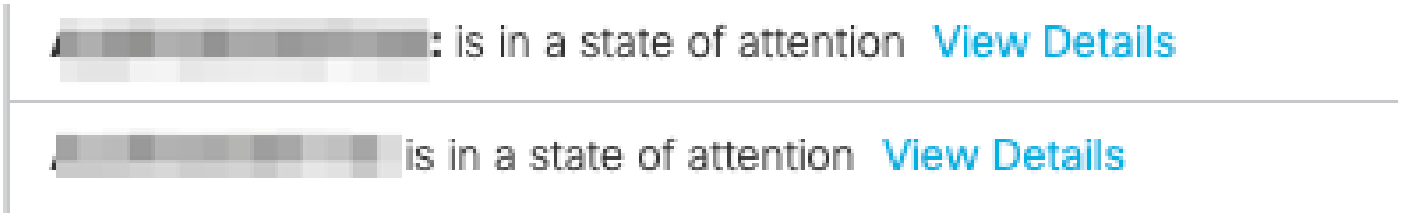
Introduzione

In questo documento viene descritto come risolvere l'avviso VA in cui viene indicato che il VA è in uno stato di attenzione relativo all'attivazione di DNSCrypt.

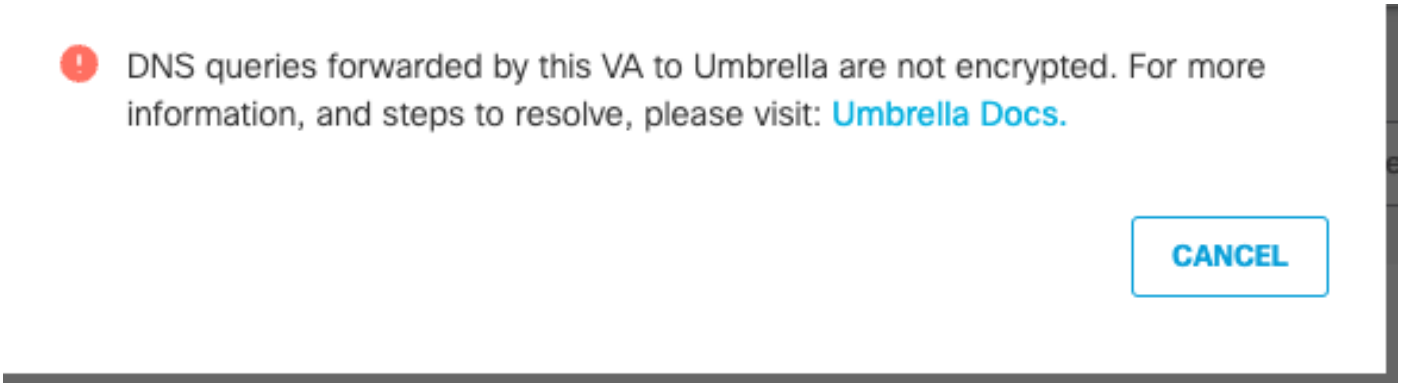
Panoramica

Virtual Appliance (VA) supporta la crittografia DNSCrypt tra se stessa e i resolver DNS (Domain Name System) pubblici OpenDNS. DNSCrypt crittografa i pacchetti DNS inoltrati dal VSA, impedendo l'intercettazione di informazioni riservate. DNSCrypt è abilitato per impostazione predefinita per una protezione ottimale, ma è possibile riscontrare problemi se un firewall blocca il traffico crittografato tra il VA e i resolver DNS pubblici.

Il traffico DNS non crittografato rappresenta un rischio per la sicurezza che è necessario affrontare. Quando non è possibile stabilire la crittografia tra VA e OpenDNS, il dashboard Umbrella visualizza un avviso che indica che l'appliance virtuale interessata "è in uno stato di attenzione" per garantire la migliore protezione possibile.



Se si fa clic su Visualizza dettagli, viene visualizzato un messaggio che indica che le query DNS inoltrate da questa VA a OpenDNS non sono crittografate.

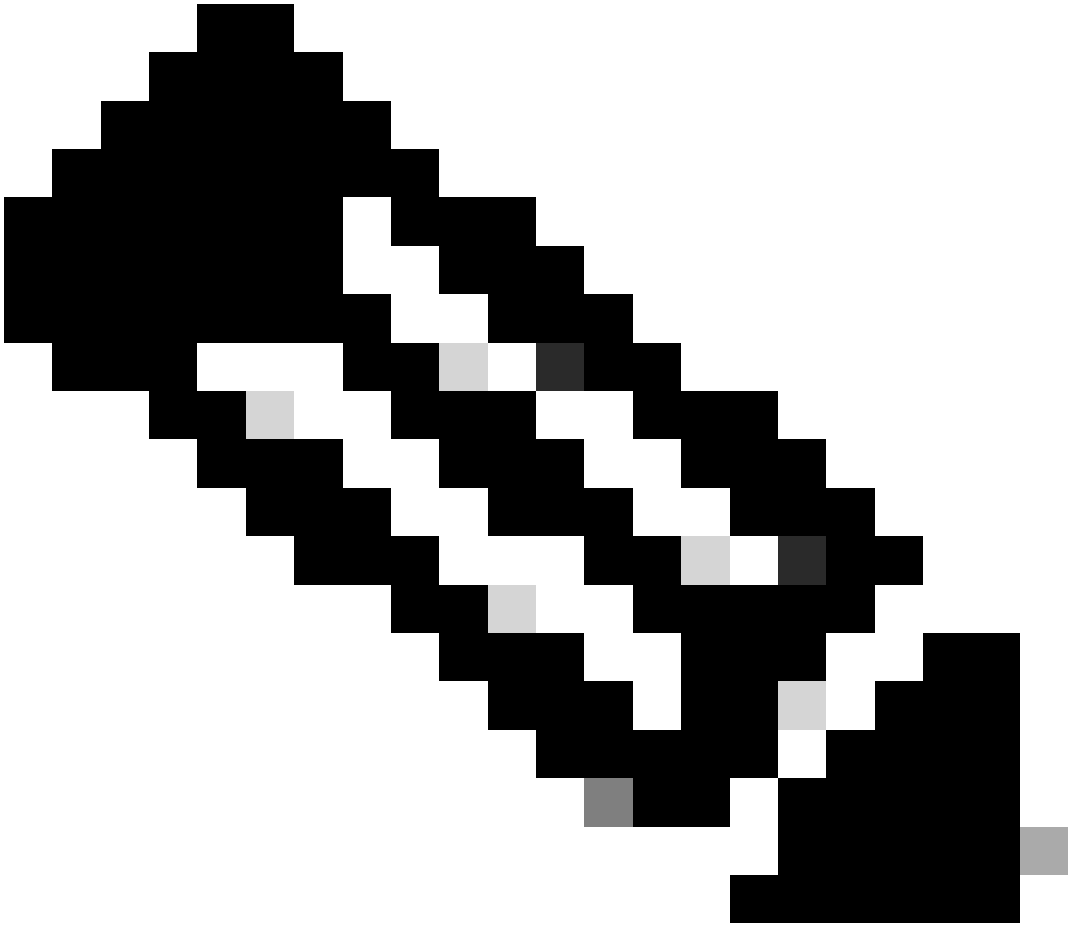


Nota: DNSCrypt è disponibile solo nelle appliance virtuali che eseguono la versione 1.5.x o successive. Se si dispone di un solo VA e non è stato aggiornato, viene visualizzato anche questo messaggio.

Risolvi l'avviso DNSCrypt

Per risolvere l'avviso e ripristinare la protezione DNSCrypt:

1. Esaminare la configurazione del firewall o del sistema di prevenzione delle intrusioni (IPS) o del sistema di rilevamento delle intrusioni (IDS).
2. Verificare che il firewall o IPS/IDS consenta il traffico DNSCrypt crittografato per VA.
3. Consenti traffico in entrata e in uscita sulla porta 53 (UDP/TCP) verso i seguenti indirizzi IP OpenDNS:
    - 208.67.220.220
    - 208.67.222.222
    - 208.67.222.220
    - 208.67.220.222
4. Se si utilizza un firewall o un protocollo IPS/IDS con ispezione approfondita dei pacchetti, verificare che non blocchi o interferisca con i pacchetti DNSCrypt crittografati. Alcuni dispositivi possono bloccare questi pacchetti se si aspettano solo il traffico DNS standard sulla porta 53.
5. Confermare che il traffico crittografato possa passare sia in entrata che in uscita tra la rete e i resolver OpenDNS su tutti i dispositivi nel percorso.



Nota: Se il firewall o IPS/IDS blocca il traffico DNSCrypt, la risoluzione DNS può avere esito negativo per gli utenti dietro la VA.

Se si ritiene che il firewall consenta già questo traffico ma l'avviso persiste, aprire una richiesta di assistenza per ricevere ulteriore assistenza.

Per ulteriori informazioni sul comportamento del firewall Cisco ASA e i possibili messaggi di errore relativi a DNSCrypt e a Deep Packet Inspection, vedere: Perché Cisco ASA Firewall blocca la funzionalità DNSCrypt di Umbrella Virtual Appliance?

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).