Beheben Warnung VA "hat einen Aufmerksamkeitsstatus"

Inhalt

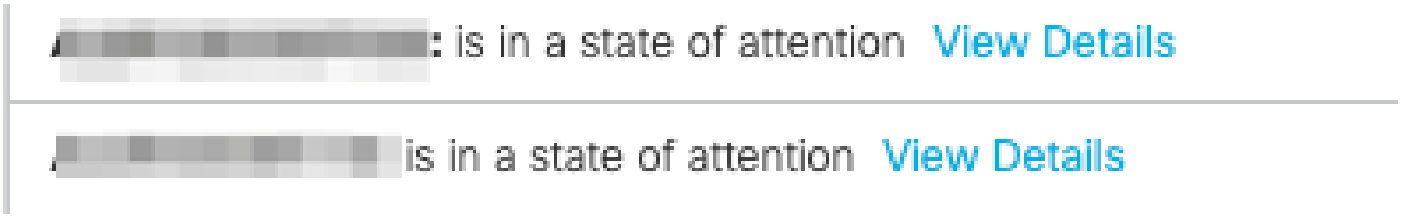
Einleitung

In diesem Dokument wird beschrieben, wie Sie die VA-Warnung beheben, die besagt, dass Ihre VA "sich im Aufmerksamkeitsstatus befindet", wenn Sie DNSCrypt aktivieren.

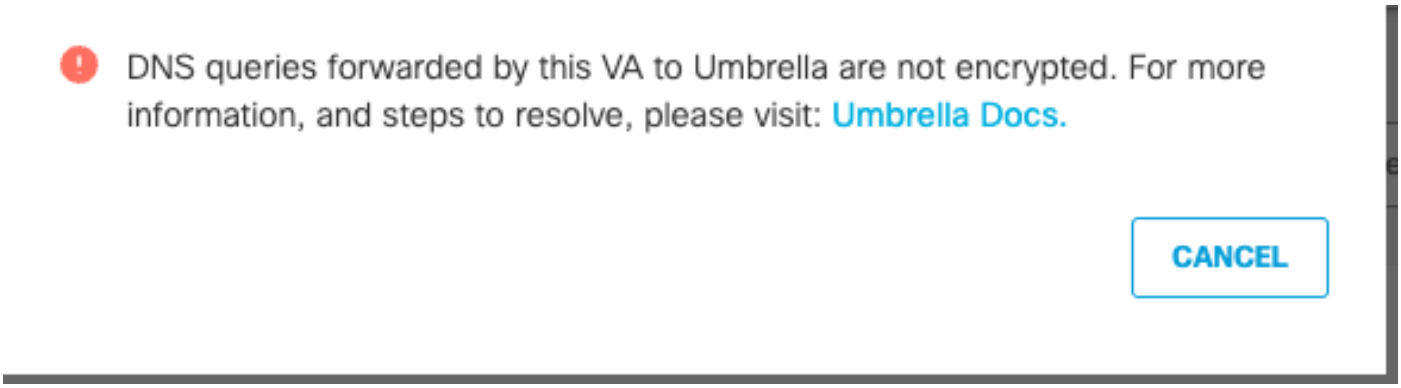
Überblick

Virtual Appliance (VA) unterstützt die DNSCrypt-Verschlüsselung zwischen sich selbst und den OpenDNS-DNS-Resolvern (Public Domain Name System). DNSCrypt verschlüsselt die von der VA weitergeleiteten DNS-Pakete und verhindert so das Abfangen vertraulicher Informationen. DNSCrypt ist standardmäßig für einen optimalen Schutz aktiviert, es können jedoch Probleme auftreten, wenn eine Firewall den verschlüsselten Datenverkehr zwischen der VA und den öffentlichen DNS-Resolvern blockiert.

Unverschlüsselter DNS-Datenverkehr ist ein Sicherheitsrisiko, das behoben werden muss. Wenn keine Verschlüsselung zwischen Ihrer VA und OpenDNS hergestellt werden kann, zeigt Ihr Umbrella Dashboard eine Warnung an, dass die betroffene virtuelle Appliance "in einem Aufmerksamkeitsstatus" ist, um den bestmöglichen Schutz zu gewährleisten.



Wenn Sie auf Details anzeigen klicken, wird eine Meldung angezeigt, die besagt, dass DNS-Abfragen, die von dieser VA an OpenDNS weitergeleitet werden, nicht verschlüsselt sind.

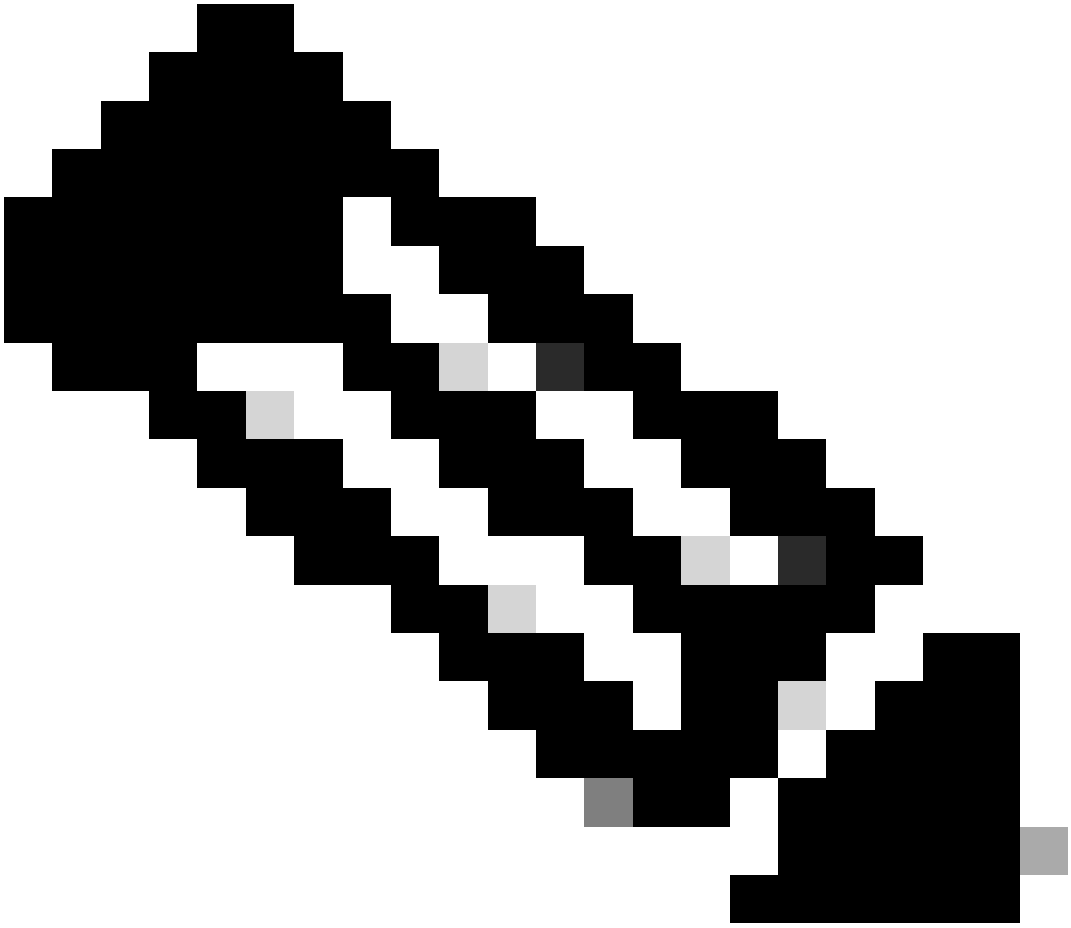


Anmerkung: DNSCrypt ist nur auf virtuellen Appliances mit Version 1.5.x oder höher verfügbar. Wenn Sie nur über eine VA verfügen und diese nicht aktualisiert wurde, wird diese Meldung ebenfalls angezeigt.

DNSCrypt-Warnung auflösen

So beheben Sie die Warnung und stellen den DNSCrypt-Schutz wieder her:

1. Überprüfen Sie Ihre Konfiguration für die Firewall oder das Intrusion Prevention System (IPS)/das Intrusion Detection System (IDS).
2. Stellen Sie sicher, dass Ihre Firewall oder IPS/IDS verschlüsselten DNSCrypt-Datenverkehr für die VA zulässt.
3. Ausgehenden und eingehenden Datenverkehr auf Port 53 (UDP/TCP) an diese OpenDNS IP-Adressen zulassen:
    - 208.67.220.220
    - 208.67.222.222
    - 208.67.222.220
    - 208.67.220.222
4. Wenn Sie eine Firewall oder IPS/IDS mit Deep Packet Inspection verwenden, stellen Sie sicher, dass diese keine verschlüsselten DNSCrypt-Pakete blockiert oder stört. Einige Geräte können diese Pakete blockieren, wenn sie nur Standard-DNS-Datenverkehr auf Port 53 erwarten.
5. Vergewissern Sie sich, dass der verschlüsselte Datenverkehr auf allen Geräten im Pfad zwischen Ihrem Netzwerk und den OpenDNS-Resolvern hin- und herfließen kann.



Anmerkung: Wenn Ihre Firewall oder IPS/IDS den DNSCrypt-Datenverkehr blockiert, kann die DNS-Auflösung für Benutzer hinter der VA fehlschlagen.

Wenn Sie glauben, dass Ihre Firewall diesen Datenverkehr bereits zulässt, die Warnung jedoch weiterhin besteht, öffnen Sie ein Support-Ticket, um weitere Unterstützung zu erhalten.

Weitere Informationen zum Verhalten der Cisco ASA-Firewall und mögliche Fehlermeldungen im Zusammenhang mit Deep Packet Inspection und DNSCrypt finden Sie unter: Warum blockiert die Cisco ASA Firewall die DNSCrypt-Funktion von der Umbrella Virtual Appliance?

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.