Resolve Warning VA "is in a state of attention"

Contents

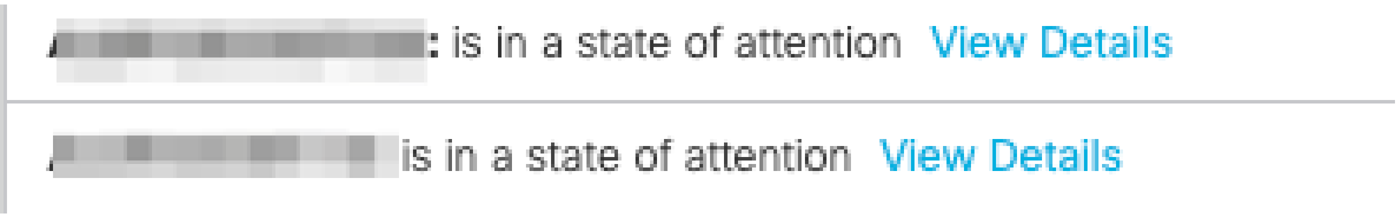
Introduction

This document describes how to resolve the VA warning stating your VA "is in a state of attention" related to enabling DNSCrypt.

Overview

Virtual Appliance (VA) supports DNSCrypt encryption between itself and OpenDNS public Domain Name System (DNS) resolvers. DNSCrypt encrypts DNS packets that the VA forwards, preventing interception of sensitive information. DNSCrypt is enabled by default for optimal protection, but you can encounter issues if a firewall blocks the encrypted traffic between your VA and the public DNS resolvers.

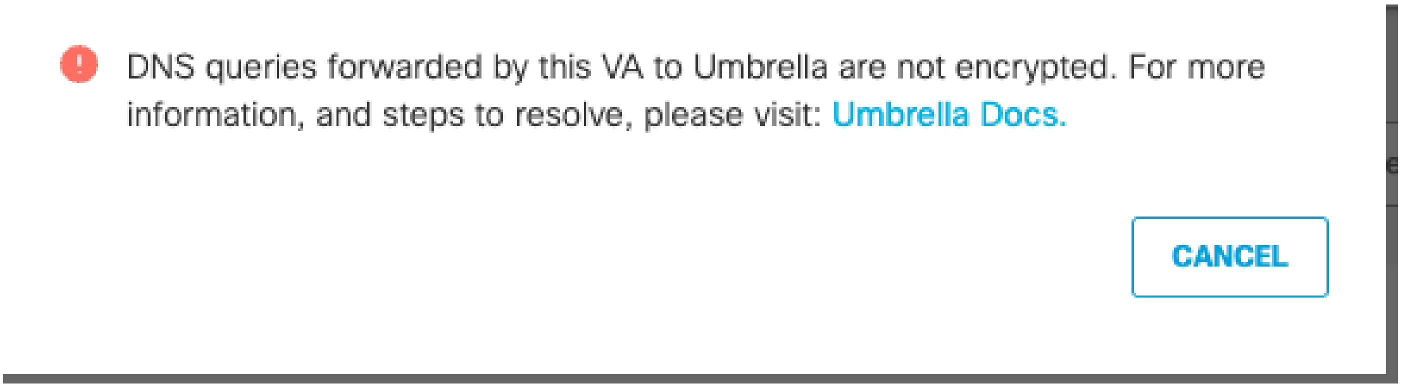
Unencrypted DNS traffic is a security risk that you must address. When encryption cannot be established between your VA and OpenDNS, your Umbrella dashboard displays a warning that the affected Virtual Appliance "is in a state of attention" to ensure you maintain the best possible protection.



[redacted]: is in a state of attention View Details

[redacted] is in a state of attention View Details

If you click **View Details**, you see a message indicating that DNS queries forwarded by this VA to OpenDNS are not encrypted.



DNS queries forwarded by this VA to Umbrella are not encrypted. For more information, and steps to resolve, please visit: Umbrella Docs.

Note: DNSCrypt is available only in Virtual Appliances running version 1.5.x or higher. If you have only one VA and it has not been upgraded, this message also appears.

Resolve the DNSCrypt Warning

To resolve the warning and restore DNSCrypt protection:

1. Review your firewall or Intrusion Prevention System (IPS)/Intrusion Detection System (IDS) configuration.
2. Ensure that your firewall or IPS/IDS allows encrypted DNSCrypt traffic for the VA.
3. Allow outbound and inbound traffic on port 53 (UDP/TCP) to these OpenDNS IP addresses:
    - 208.67.220.220
    - 208.67.222.222
    - 208.67.222.220
    - 208.67.220.222
4. If you use a firewall or IPS/IDS with deep packet inspection, verify that it does not block or interfere with encrypted DNSCrypt packets. Some devices can block these packets if they expect only standard DNS traffic on port 53.
5. Confirm that encrypted traffic can flow both outbound and inbound between your network and OpenDNS resolvers on all devices in the path.

Note: If your firewall or IPS/IDS blocks DNSCrypt traffic, DNS resolution can fail for users behind the VA.

If you believe your firewall already allows this traffic but the warning persists, open a support case for further assistance.

For more information about Cisco ASA firewall behavior and possible error messages related to deep packet inspection and DNSCrypt, see: Why is Cisco ASA Firewall blocking DNSCrypt functionality from the Umbrella Virtual Appliance?