Configure Cisco ASA Shun Feature to Exempt Virtual Appliance

Contents

[Introduction](#)

[Threat Detection 'Shun' Feature](#)

[Exempt the Virtual Appliance](#)

[Determine if the Appliance has been 'Shunned'](#)

Introduction

This document describes how to configure the Cisco ASA to exempt the Virtual Appliance from the threat detection component. The Cisco ASA threat detection compontent performs packet inspection on DNS and other protocols. Umbrella support recommends these ASA configuration changes to prevent this feature from conflicting with our Virtual Appliance:

- Exempt the Virtual Appliance from the Threat Detection 'shun' feature as described in this article.
- Exempt the Virtual Appliance from DNS packet inspection to allow our DNS encryption (DNScrypt) which is covered in this article: Cisco ASA Firewall blocks DNScrypt.

Threat Detection 'Shun' Feature

When the 'Shun' feature is enabled the ASA can completely block a source IP address address that triggers threat detection rules. More details are in the Cisco article: ASA Threat Detection Functionality and Configuration.

The Virtual Appliance normally sends a very high number of DNS queries to Umbrella DNS resolvers. In cases where there is a local problem connecting to the resolvers (such as a temporary network outage/latency) these queries can fail. Due to the sheer volume of queries that are sent, even a small percentage failing causes the ASA to shun the Virtual Appliance; which leads to a complete DNS outage for a period of time.

Exempt the Virtual Appliance

Note: The commands in this article are noted for guidance only and it is recommended to consult a Cisco expert before you make any changes to a production environment.

Via CLI:

- To exempt the Appliance IP from being shunned, run this command: **no shun <src_ip>**

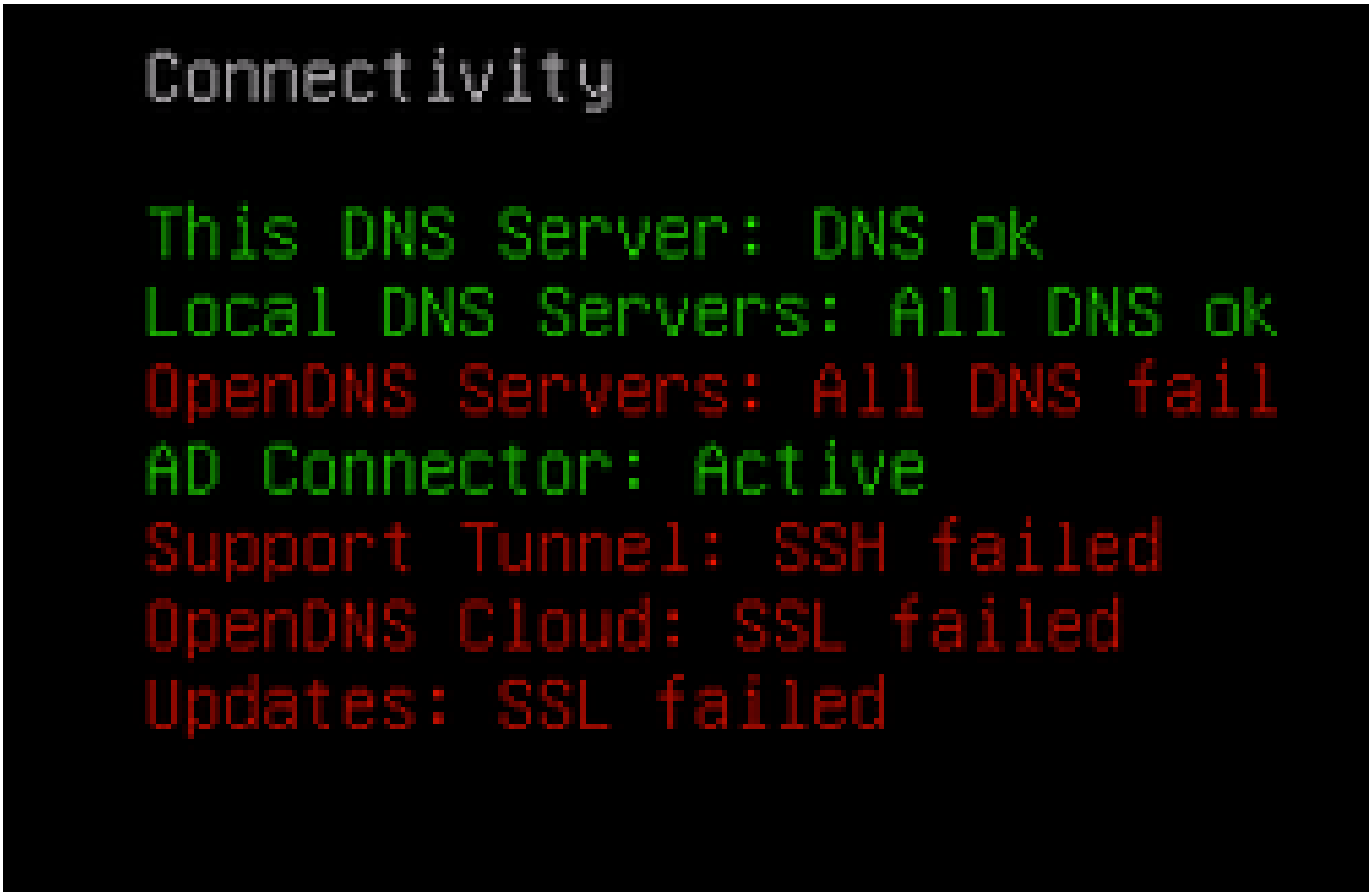
Via ASDM interface:

- Choose the *Configuration > Firewall > Threat Detection* pane.
- To exempt the Appliance IP address from being shunned, enter an address in the *'Networks excluded from shun'* field. You can enter multiple addresses or subnets separated by commas.

Determine if the Appliance has been 'Shunned'

If these steps have not been followed the appliance could become 'shunned' in some circumstances, which leads to a DNS outage.

When the Virtual Appliance has no external connectivity, the console appears as follows:



The Cisco ASA logs the event as follows:

4|Jun 06 2014 14:00:42|401004: Shunned packet: 192.168.1.3 ==> 208.67.222.222 on interface inside
4|Jun 06 2014 14:00:42|401004: Shunned packet: 192.168.1.3 ==> 208.67.222.222 on interface inside

To see a list of currently shunned IP addresses, run this command on the ASA: **show shun**

To immediately clear the currently shunned IP addresses, run this command on the ASA: **clear shun**