Understand DNS Guard in Secure Firewall 7.7.0

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Comparison to the Previous Release
- New Features

Basics: Supported Platforms, Licensing

- FTD Platforms and Managers
- Other Support Aspects

Problem

- Steps to Recreate the Problem

Solution

- Feature Overview
- Troubleshooting

Introduction

This document describes the DNS Guard feature in Secure Firewall 7.7.0, focusing on its functionality and troubleshooting.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Understanding of DNS protocol and UDP sessions
- Familiarity with Snort 3 and its session management

Components Used

The information in this document is based on these software and hardware versions:

- Secure Firewall Threat Defense (FTD) version 7.7.0
- Firepower Management Center (FMC) version 7.7.0
- Snort version 3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

DNS is a UDP request-response based protocol with short-lived sessions. Unlike Lina, the DNS sessions in Snort 3 are not cleared immediately after the DNS response. Instead, DNS sessions are pruned based on a flow timeout of 120 seconds or more. This leads to unnecessary session accumulation, which could otherwise be used for other TCP or UDP connections.

Comparison to the Previous Release

In Secure Firewall 7.6 and Below		New to Secure Firewall 7.7
• The DNS session remains as a stale Snort 3 flow until it is pruned by the UDP timeout.		• DNS sessions in Snort 3 are released immediately after the DNS Response is inspected and handled.

New Feature in 7.7

New Features

- This “DNS Guard” feature clears the UDP Flow immediately after receiving and inspecting the DNS Response packet.
- This is a protocol-specific enhancement over the current design and architecture of Snort 3.

Basics: Supported Platforms, Licensing

FTD Platforms and Managers

FTD Platforms	All
FMC on 7.7.0 FMC Rest API	Yes No
FTD Supported Versions *(lowest version FMC on 7.7.0 can manage is 7.2)*	7.7.0 only
Snort Support (Snort 3 is the only Snort version supported in 7.7)	Snort 3

Supported Platforms

Other Support Aspects

FTD	
Licenses Required	Essentials, URL, Threat, Malware
Works in Evaluation Mode	Yes
IP Addressing	IPv4 IPv6
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes
Other (only routed mode | transparent mode), etc.	No Special Notes

Licensing and Compatibility

Problem

In previous releases, specifically Secure Firewall 7.6 and below, the DNS session remains as a stale Snort 3 flow until it is pruned by the UDP timeout. This causes issues with session management and could lead to inefficient use of resources as DNS sessions accumulate unnecessarily.

Steps to Recreate the Problem

To observe the problem, execute the Lina command to check active DNS connections from the Lina side:

```
show conn detail
```

In Secure Firewall 7.6 and below, DNS sessions remain active until the UDP timeout, leading to resource inefficiency.

Solution

The DNS Guard feature in Secure Firewall 7.7.0 addresses this problem by immediately clearing the UDP flow after receiving and inspecting the DNS response packet. This protocol-specific enhancement ensures that DNS sessions in Snort 3 are released immediately, preventing unnecessary session accumulation and improving resource efficiency.

Feature Overview

The DNS Guard feature clears the UDP flow immediately after receiving and inspecting the DNS response packet. The Snort flow need not wait until the UDP timeout occurs.

- When there is sufficient DNS traffic on the box, this feature leads to fewer active flows due to timely cleanup of the corresponding Snort flows.
- More TCP/UDP connections can be handled by the box without pruning active connections, which

improves overall efficacy of the box.

Troubleshooting

To verify the functionality of the DNS Guard feature, use the Lina command to ensure that UDP sessions are released upon receiving a DNS response:

<#root>

>

show snort counters | begin stream_udp

Example output without DNS guard feature:

```
stream_udp sessions: 755
 max: 12
created: 755
released: 0
total_bytes: 124821
```

<#root>

>

show snort counters | begin stream_udp

Example output with DNS guard feature:

```
stream_udp sessions: 899
max: 14
created: 899
released: 899
total_bytes: 135671
```

The outputs indicate that all created sessions are released timely, confirming the correct operation of the DNS Guard feature.

Related Information

- Cisco Technical Support & Downloads