了解安全防火墙7.7.0中的DNS防护

目录

简介

本文档介绍安全防火墙7.7.0中的DNS防护功能，重点介绍其功能和故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解DNS协议和UDP会话
- 熟悉Snort 3及其会话管理

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全防火墙威胁防御(FTD)版本7.7.0
- Firepower管理中心(FMC)版本7.7.0
- Snort第3版

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

DNS是具有短期会话的基于UDP请求响应的协议。与Lina不同，Snort 3中的DNS会话不会在DNS响应后立即清除。相反，DNS会话会根据120秒或更长的流超时进行修剪。这会导致不必要的会话累积，否则可用于其他TCP或UDP连接。

与上一版本比较

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.

7.7中的新功能

新功能

- 此“DNS防护”功能可在接收和检查DNS响应数据包后立即清除UDP流量。
- 这是针对Snort 3当前设计和架构的协议特定增强功能。

基础知识：支持的平台，许可

FTD平台和管理器

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

支持的平台

其他支持方面

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

许可和兼容性

问题

在以前的版本（尤其是Secure Firewall 7.6及更低版本）中，DNS会话将保持为陈旧的Snort 3流，直到因UDP超时而被修剪为止。这会导致会话管理问题，并随着DNS会话不必要地累积，可能导致资源的低效使用。

重新创建问题的步骤

要观察问题，请执行Lina命令以从Lina端检查活动DNS连接：

```
show conn detail
```

在安全防火墙7.6及更低版本中，DNS会话保持活动状态，直到UDP超时，从而导致资源效率低下。

解决方案

Secure Firewall 7.7.0中的DNS防护功能可在接收和检查DNS响应数据包后立即清除UDP流量，从而解决此问题。此特定于协议的增强可确保立即释放Snort 3中的DNS会话，防止不必要的会话累积，并提高资源效率。

功能概述

DNS防护功能会在接收和检查DNS响应数据包后立即清除UDP流量。Snort流量无需等待，直到UDP超时发生。

- 当机箱上有足够的DNS流量时，由于及时清理相应的Snort流量，此功能会导致活动流量减少。
- 机箱可以处理更多的TCP/UDP连接，而无需删除活动连接，这提高了机箱的整体效能。

故障排除

要验证DNS防护功能的功能，请使用Lina命令确保在收到DNS响应时释放UDP会话：

<#root>

>

show snort counters | begin stream_udp

不具有DNS防护功能的输出示例：

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

<#root>

>

show snort counters | begin stream_udp

具有DNS防护功能的输出示例：

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

输出指示及时释放所有创建的会话，确认DNS防护功能的正确操作。

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。