# 瞭解安全防火牆7.7.0中的DNS防護

## 目錄



## 簡介

本檔案介紹安全防火牆7.7.0中的DNS防護功能，重點介紹其功能和疑難排解。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 瞭解DNS通訊協定和UDP作業階段
- 熟悉Snort 3及其會話管理

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 安全防火牆威脅防禦(FTD)版本7.7.0
- Firepower管理中心(FMC)版本7.7.0
- Snort版本3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

# 背景資訊

DNS是一種基於UDP請求響應的協定，具有短期會話。與Lina不同，Snort 3中的DNS作業階段不會在DNS回應後立即清除。相反，DNS會話將基於流超時120秒或更長的時間進行修剪。這會導致不必要的會話累積，否則可用於其他TCP或UDP連線。

## 與先前版本的比較

| 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

- 在接收和檢查DNS響應資料包後，此「DNS防護」功能立即清除UDP流。
- 這是對Snort 3的當前設計和架構進行的協定特定增強。

# 基礎知識：支援的平台，許可

## FTD平台和管理員

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

支援的平台

## 其他支援方面

| FTD | |
|---|---|
| Licenses Required | Essentials, URL, Threat, Malware |
| Works in Evaluation Mode | Yes |
| IP Addressing | IPv4<br>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 |

許可和相容性

# 問題

在以前的版本（尤其是Secure Firewall 7.6及更低版本）中，DNS會話會保持為陳舊的Snort 3流，直到因UDP超時而被修剪為止。這會導致會話管理問題，並可能導致DNS會話不必要地累積，導致資源的低效使用。

## 重新建立問題的步驟

若要觀察問題，請執行Lina命令以從Lina端檢查作用中DNS連線：

```
show conn detail
```

在Secure Firewall 7.6及更低版本中，DNS會話將保持活動狀態，直到UDP超時，從而導致資源效率低下。

# 解決方案

Secure Firewall 7.7.0中的DNS防護功能通過在接收和檢查DNS響應資料包後立即清除UDP資料流來解決此問題。此特定於協定的增強功能可確保立即釋放Snort 3中的DNS會話，防止不必要的會話累積，並提高資源效率。

## 功能概述

收到並檢查DNS響應資料包後，DNS防護功能會立即清除UDP流量。Snort流無需等待，直到UDP超時。

- 當機箱上有足夠的DNS流量時，由於及時清除對應的Snort流量，此功能會導致活動流量減少。
- 該框可以處理更多的TCP/UDP連線，而無需修剪活動連線，這提高了框的整體效能。

### 疑難排解

要驗證DNS防護功能的功能，請使用Lina命令確保在收到DNS響應時釋放UDP會話：

```
<#root>

>

show snort counters | begin stream_udp
```

不具DNS防護功能的輸出範例：

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

```
<#root>

>

show snort counters | begin stream_udp
```

使用DNS防護功能的輸出示例：

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

輸出指示所有建立的會話都及時釋放，從而確認DNS防護功能的正確操作。

## 相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。