セキュアファイアウォール7.7.0のDNSガードについて

内容

はじめに

このドキュメントでは、Secure Firewall 7.7.0のDNSガード機能について、その機能とトラブルシューティングを中心に説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- DNSプロトコルとUDPセッションの理解
- Snort 3およびそのセッション管理に精通していること。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- セキュアファイアウォール脅威対策(FTD)バージョン7.7.0
- Firepower Management Center（FMC）バージョン 7.7.0
- Snortバージョン3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

DNSは、UDP要求/応答ベースのプロトコルであり、短時間のセッションで使用されます。Linaとは異なり、Snort 3のDNSセッションは、DNS応答の直後にはクリアされません。代わりに、DNSセッションは120秒以上のフロータイムアウトに基づいてプルーニングされます。これにより、不必要なセッションの蓄積が発生し、他のTCPまたはUDP接続に使用される可能性があります。

旧リリースとの比較

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の新機能

新しい機能

- この「DNSガード」機能は、DNS応答パケットを受信して検査した直後にUDPフローをクリアします。
- これは、Snort 3の現在の設計とアーキテクチャに対する、プロトコル固有の機能拡張です。

基本：サポートされるプラットフォーム、ライセンス

FTDプラットフォームおよびマネージャ

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

対応プラットフォーム

その他のサポート面

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

ライセンスと互換性

問題

以前のリリース、特にSecure Firewall 7.6以前では、DNSセッションは、UDPタイムアウトによってプルーニングされるまで、古いSnort 3フローのままになっています。これにより、セッション管理に問題が発生し、DNSセッションが不必要に蓄積されて、リソースの非効率的な使用につながる可能性があります。

問題を再現する手順

問題を確認するには、Linaコマンドを実行して、Lina側からのアクティブなDNS接続を確認します。

```
show conn detail
```

Secure Firewall 7.6以前では、DNSセッションはUDPタイムアウトまでアクティブのままになり、リソースの非効率性が発生します。

解決方法

セキュアファイアウォール7.7.0のDNSガード機能は、DNS応答パケットを受信して検査した後すぐにUDPフローをクリアすることで、この問題に対処しています。このプロトコル固有の機能拡張により、Snort 3のDNSセッションが即時に解放され、不要なセッションの蓄積が防止され、リソース効率が向上します。

機能の概要

DNSガード機能は、DNS応答パケットを受信して検査した直後にUDPフローをクリアします。Snortフローは、UDPタイムアウトが発生するまで待機する必要はありません。

- ボックスに十分なDNSトラフィックがある場合、対応するSnortフローがタイムリーにクリーンアップされるため、この機能によってアクティブなフローが減少します。
- アクティブな接続をプルーニングすることなく、より多くのTCP/UDP接続をボックスで処理できるため、ボックス全体の有効性が向上します。

トラブルシューティング

DNSガード機能の機能を確認するには、Linaコマンドを使用して、DNS応答の受信時にUDPセッションが解放されることを確認します。

<#root>

>

show snort counters | begin stream_udp

DNSガード機能なしの出力例：

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

<#root>

>

show snort counters | begin stream_udp

DNSガード機能を使用した出力例は次のとおりです。

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

出力は、作成されたすべてのセッションがタイムリーにリリースされ、DNSガード機能が正しく動作していることを示しています。

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。