Snortでのアクティブなフローの表示

内容

はじめに

このドキュメントでは、show snort flowsコマンドを使用してSnortのアクティブなフローを表示する方法について説明します。

今回のリリースとの違い

In Secure Firewall 7.4 and Below		New to Secure Firewall 7.6
• No way to look at active flows in Snort		• New CLI `show snort flows` can be used to view active flows in Snort

機能の概要

- 新しいCLIのshow snort flowsコマンドを使用すると、Snort 3フローキャッシュ内のアクティブなフローが表示されます。
- これにより、Snort 3プロセス実行中のアクティブフローの詳細が提供されます。
- 出力には、Snortフローの状態、送信元および宛先のIPとポートが示されます。
- 実稼働環境での問題の特定とデバッグに役立ちます。

スポイラー（参照用に強調表示）

注：この機能が導入され、アクティブなSnortフローとクライアント、フローのサーバ状態、タイムアウトなどを確認できるようになりました。

注：この機能が導入され、アクティブなSnortフローとクライアント、フローのサーバ状態、タイムアウトなどを確認できるようになりました。

最低限のソフトウェアおよびハードウェアプラットフォーム

Manager(s) and Version (s)	Application (FTD) and Minimum Version of Application	Supported Platforms
• (CLI only)	FTD 7.6.0	All platforms running FTD and Snort 3

Snort 3、IPv6、マルチインスタンス、およびHA/クラスタリングのサポート

- IPv4とIPv6の両方で動作します。
- Snort 3を検出エンジンにする必要がある

FTD	
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes

サポートのその他の側面

Platforms	
FTD	
Licenses Required	Essentials
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

機能説明とウォークスルー

この項では、フロータイムアウトなどのウォークスルーと、その他の機能の詳細について説明します。

新しいShow Snort Flows CLI

<#root>

```
> show snort flows
```

```
TCP 0: x1.x1.x1.2/38148 x1.x1.x1.1/22 pkts/bytes client 9/2323 server 6/2105 idle 7s, uptime 7s, timeout
ICMP 0: x1.x1.x1.2 type 8 x1.x1.x1.1 pkts/bytes client 1/98 server 1/98 idle 0s, uptime 0s, timeout 3m0
UDP 0: x1.x1.x1.1/40101 x1.x1.x1.1/12345 pkts/bytes client 3/141 server 0/0 idle 19s, uptime 58s, timeo
```

この例では、TCP、ICMP、およびUDPの3つのフローを示します。

TCPフローの場合、値は次のとおりです。

- プロトコル：TCP/ICMP/UDP/IP
- アドレス空間ID – インターフェイスのVRF ID
- 送信元IP/ポート：x1.x1.x1.2/38148
- 宛先IP/ポート：x1.x1.x1.1/22
- クライアントのパケット/バイト：9/2323
- サーバパケット/バイト：6/2105
- Idle：最後のパケットがフローしてからの時間
- 稼働時間 – フローが設定されてからの時間
- Timeout：フロータイムアウト
- クライアントの状態（TCPフローのみ） - EST

- サーバの状態（TCPフローのみ）:EST

クライアントとサーバのフロー状態

- 出力のClient StateおよびServer Stateは、プロトコルがTCPの場合にのみ表示されます。
- 各状態の可能な値と、各略語の意味を次に示します。

State Acronym	Description
LST	Listen
SYS	SYN Sent
SYR	SYN received
EST	Established
MDS	Midstream Sent
MDR	Midstream Received
FW1	Final Wait 1
FW2	Final Wait 2
CLW	Close Wait
CLG	Closing
LAK	Last ACK
TWT	Time wait
CLD	Closed

フィルタ オプション

show snort flowsコマンドでは、フィルタに一致するフローだけを出力するフィルタリングオプションがサポートされています。 構文は次のとおりです

show snort flows <filterオプション> <値>

フィルタオプションは次のとおりです。

- proto -TCP/UDP/IP/ICMP
- src_ip：送信元ipでフローをフィルタリングする

- dst_ip：宛先ipでフローをフィルタする
- src_port：送信元ポートでフローをフィルタリングする
- dst_port：宛先ポートでフローをフィルタリングする

> show snort flows proto TCPコマンドでは、TCPフローのみがリストされます。

```
TCP 0: x1.x1.x1.2/45508 x1.x1.x1.1/22 pkts/bytes client 10/2389 server 7/2171 idle
30s, uptime 150s, timeout 59m30s state client CLW server FW2
```

スポイラー（参照用に強調表示）

注：コマンドで複数のフィルタを使用することもできます。 たとえば、

> show snort flows proto TCP src_ip x1.x1.x1.2：送信元がip x1.x1.x1.2のTCPフローを出力します。

注：コマンドで複数のフィルタを使用することもできます。 たとえば、> show snort flows proto TCP src_ip x1.x1.x1.2：送信元がip x1.x1.x1.2であるTCPフローを出力します。

潜在的なエラー応答

- CLIユーザに「unable to process the command, please try again later」という応答が返される場合があります。
- これは、たとえば、Snort 3がダウンしている場合、Snort 3がビジーの場合、またはSnort 3が制御ソケットコマンド（スタック状態のスレッドなど）を処理していない場合に発生します。
- CLIが正常に実行される条件：
  - Snort 3は実行中です。
  - Snort 3は、UNIXドメインソケット経由で制御コマンドに応答しています。

CLI/出力の停止

- 他のCLIコマンドと同様に、Ctrl + Cを押すとコマンドプロンプトが表示されますが、コマンドはすべてのパケットスレッドにすでに渡されており、Snortで補完まで実行されます。
- コマンドは、両方の条件が当てはまる場合に完了します。
  - フローキャッシュ内のすべてのフローが表示されました
  - CLIコマンドのフィルタに一致するすべてのフローは、CLIで出力するコマンドの入力として機能するファイルに書き込まれています。

パフォーマンスへの影響

- これはデバッグCLIです。通過するパケットごとに、フローテーブルから約100のフローを確認し、条件に一致するフローを印刷します。
- show snort flowsを実行すると、パフォーマンスに影響します。

参考資料

FAQ

Q:「show snort flows」では複数のフィルタを使用できますか。

A：はい。CLIは複数のフィルタを同時に提供することをサポートし、両方のフィルタに一致するフローを出力します。

Q：どのプロトコルがサポートされていますか。

A:IP/TCP/UDP/ICMP

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。