CSF CLIでのトラフィック問題のトラブルシューティング

内容

概要

このドキュメントでは、Cisco Secure Firewall CLIを使用して、ルーティング、パケットフロー、およびSnortの動作を検証し、トラフィックの問題をトラブルシューティングする方法について説明します。

前提条件

このドキュメントに特有の要件はありません。

要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Center(FMC)のポリシーとオブジェクトの設定

- Cisco Secure Firewall(CSF)ルーティングおよびインターフェイスロジック
- パケットインスペクションとファイアウォールトラブルシューティングの概念

使用するコンポーネント

このドキュメントは、CSFの特定のソフトウェアおよびハードウェアのバージョンに限定されるものではありません。このドキュメントで使用されているデバイスは、コード7.6.5を実行しています。

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、初期（デフォルト）設定の状態から起動しています。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。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- セキュアファイアウォール管理センター(FMC)
- Cisco Secure Firewall(CSF)
- Firepower Threat Defense(FTD)CLIツール

重要な情報

デバイスのCPU、メモリ、またはI/O使用率が上昇している場合、トラブルシューティングコマンドを実行すると、パフォーマンスの低下が悪化する可能性があります。最初にリソース枯渇状態を調査して解決してから、トラフィック問題の診断に進むことをお勧めします。診断コマンドは追加のシステムリソースを消費するため、アベイラビリティがさらに低下し、回復時間が長くなる可能性があります。

背景説明

CSFでのトラフィックのトラブルシューティングは、多くの場合、パケットがファイアウォールを通過する必要のある論理パスを確認することから始まります。ルートとインターフェイスのマッピングを理解したら、次の手順は、予想されるパスと実際のパケットフローを比較することです。これは、ルートルックアップ、パケットトレーサシミュレーション、パケットキャプチャ、およびSnort工ンジントレースを使用して実行できます。

各ツールは、異なる可視性レイヤを提供します。

- show routeは、パケットのルーティングパスとインターフェイスidを確認します。
- packet-tracerはトラフィックフローをシミュレートし、ACL、NAT、およびインターフェイスの決定を特定します。
- パケットキャプチャは、ファイアウォールを通過するライブトラフィックを検査します。
- システムサポートトレースにより、ポリシー関連のブロックまたはインスペクションイベントに関するSnortの意思決定が公開されます。

ヒント：トラフィックをキャプチャする前に、ルーティングとパケットトレーサの検証を開始します。これにより、ライブトラフィックを分析する前に、予測されるパスとアクセスコントロールの決定が正しいかどうかを確認できます。

問題

トラフィックフローが期待どおりに動作しておらず、管理者はパケットが正しいパスを使用しているかどうか、ファイアウォールが接続を許可しているか拒否しているか、およびSnortまたはポリシーインスペクションがトラフィックをブロックしているかどうかを確認する必要があります。

ステップ1：ルートの検索

ルーティングパスを特定し、送信元と宛先のIPアドレスに関連付けられた論理インターフェイス名を特定します。論理インターフェイス名は、ほとんどのトラブルシューティングコマンドで必要とされるため、トラブルシューティングワークフローの最初の手順として使用する必要があります。

送信元と宛先のIPアドレスに対して、次のコマンドを実行します。

```
show route <IP>
```

デフォルトルートに依存するインターネット宛トラフィックでは、論理出力インターフェイスの識別が必要です。論理インターフェイス名は、次の手順を実行して判別できます。

```
show route 0.0.0.0
```

出力例：

```
FTD1# show route 192.168.0.11


Routing entry for 192.168.0.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:

    directly connected, via Inside
    Route metric is 0, traffic share count is 1
```

```
FTD1# show route 0.0.0.0

Routing entry for 0.0.0.0 0.0.0.0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:

    128.107.0.1, via Outside
    Route metric is 0, traffic share count is 1
```

この例では、論理入力インターフェイスは「Inside」で、出力インターフェイスは「Outside」です。

注意：ネットワークアドレス変換(NAT)は、NATポリシーがトラフィックフローと一致する場合に、ルーティングテーブルに示されているインターフェイスとは異なるインターフェイスを介してトラフィックをリダイレクトできます。接続のトラブルシューティングを行う際には、NATの設定が予想されるトラフィックパスと一致していることを確認します。

ヒント：論理インターフェイス名は、CLIのトラブルシューティングコマンドで使用します。後で参照できるように、論理名をメモしておいてください。

ステップ2：パケットトレーサを実行します。

パケットトレーサを使用して、ファイアウォールが特定のトラフィックフローを評価する方法をシミュレートします。このツールは、使用されているインターフェイス、NATポリシーが適用されているかどうか、およびACLがトラフィックを許可するか拒否するかを確認するのに役立ちます。

次のコマンド構文を使用します。

```
packet-tracer input <source interface> <protocol> <source IP> <source port> <destination IP> <destinati
```

コマンド例：

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443
```

出力を見直して、パケットが期待されるパスに従っていること、およびシミュレーション中に許可されていることを確認します。これは、ライブパケット分析を行う前に、問題がルーティング、NAT、またはポリシーマッチングに関連しているかどうかを判断する必要がある場合に役立ちます。

packet-tracerのtransmitキーワードにより、シミュレートされたパケットが入力インターフェイスで注入され、シミュレーションとしてではなく、すべてのファイアウォール処理フェーズを通過できるようになります。

コマンド例：

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443 transmit
```

ステップ3：キャプチャの実行

パケットキャプチャを使用して、ファイアウォールを通過するライブトラフィックを検査します。パケットキャプチャは実際のトラフィックをキャプチャするため、パケットトレーサとは異なり、キャプチャがアクティブなときにファイアウォールを通過する実際のフローと一致する必要があります。パケットキャプチャは双方向で、接続の両側を文書化します。

ほとんどのトラフィックのトラブルシューティングシナリオでは、次のキャプチャを設定します。

- 入力キャプチャ：ソース側インターフェイスに到着するトラフィックをキャプチャします
- 出力キャプチャ：宛先側インターフェイスから発信されるトラフィックをキャプチャします
- ASPドロップキャプチャ：ファイアウォールによってドロップされ、設定された基準に一致するパケットをキャプチャします

一般的なキャプチャ構文：

```
capture <name> interface <interface name> trace match ip host <source IP> host <destination IP>
```

入力キャプチャの例：

```
FTD1# capture in interface trace Inside match ip host 192.168.0.11 host 72.163.4.161
```

出力キャプチャの例：

```
FTD1# capture out interface trace Outside match ip host 128.107.0.22 host 72.163.4.161
```

ASPドロップキャプチャの例：

```
FTD1# cap asp type asp-drop match ip host 192.168.0.11 host 72.163.4.161
```

パケットキャプチャは双方向です。つまり、定義された一致基準に基づいてフォワードトラフィックとリターントラフィックの両方をキャプチャできます。トレース機能を使用すると、ファイアウォールが実際のトラフィックに対して行う決定を視覚化できます。

⚠ 注意: NATが実行されている場合、ポストNATトラフィックを正しくキャプチャするには、出力キャプチャで、元の送信元IPではなく、変換された送信元IPを使用する必要があります。

ステップ4：システムサポートトレースの実行

システムサポートトレースを使用して、特定のトラフィックフローに関するリアルタイムのSnortインスペクションプロセスを表示します。これは、トラフィックがACLの許可ルールに一致しているものの、引き続きポリシー検査によってブロックされている場合に特に役立ちます。標準的なパケットキャプチャでは、パケットがブロックされたことが示されますが、システムサポートトレースでは、パケットがそのように処理された理由が表示されます。システムサポートトレースは双方向です。つまり、トラフィックを両側から受信します。つまり、ツールにIPが追加される順序は重要ではありません。

次のコマンドを実行し、プロンプトに応答します。

```
> system support trace


Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 72.163.4.161
Please specify a server port: 443
```

このツールは、環境でアプリケーションまたはURLルール、アイデンティティベースのルール、ファイルポリシー、または侵入ポリシーを使用している場合に特に役立ちます。これらの機能はACLが一致した後に評価されるため、アクセスコントロールポリシーでパケットを許可しながら、Snortインスペクションでブロックできます。

注：正確な送信元ポートが不明な場合は、クライアントポートを空白のままにすることができます。

確認

ルートルックアップ、パケットトレーサシミュレーション、パケットキャプチャ、およびシステムサポートトレースの出力を一緒に使用して、トラフィックフローの動作を確認します。目標は、パケットが正しいパスを使用しているかどうか、ファイアウォールがそれを許可しているか拒否しているか、およびより詳細なインスペクションに基づいてSnortがパケットをブロックしているかを判別することです。

通常、完全なトラブルシューティングフローで次の点を確認します。

- ルートルックアップは、論理的な入力インターフェイスと出力インターフェイスを示します。
- パケットトレーサは、目的の転送パスとポリシー評価を確認します。
- パケットキャプチャにより、トラフィックが期待どおりに発着信しているかどうかが確認されます。
- システムサポートトレースにより、Snortまたはポリシーインスペクションがブロックの原因であるかどうかを確認します。

トラブルシューティング

トラフィックの問題が続く場合は、次の領域を確認してください。

- ルートルックアップが、予期される送信元インターフェイスと宛先インターフェイスに一致するかどうかを確認します。
- パケットトレーサの出力で、ACLまたはNAT段階で拒否されているトラフィックが示されているかどうかを確認します。
- 入力パケットキャプチャと出力パケットキャプチャを確認して、トラフィックがファイアウォールに到達して正しいインターフェイスから送出されていることを確認します。
- ASPドロップキャプチャを使用して、ファイアウォールが内部でトラフィックをドロップしているかどうかを確認します。
- システムサポートトレースを使用して、ACLの許可決定後にSnortがトラフィックをブロックしているかどうかを確認します。

関連情報

- ネットワークの問題をトラブルシューティングするためのFirepowerファイアウォールキャプチャの分析
- Firepower Threat Defense(FTD)のキャプチャとパケットトレーサを使用する

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。