セキュアファイアウォールのFTD展開の失敗

お問い合わせ内容

Cisco Firewall Firepower Threat Defense(FTD)では、ネットワークの中断や停止が発生しています。 繰り返し発生するインシデントにより、SNMP通信を含むトラフィックが拒否され、根本原因を特定してさらなる影響を軽減するために、デバイスの再起動と継続的なモニタリングが必要になりました。

環境

- Cisco Secure Firewall Firepower 1140アプライアンス（すべてのFTDモデルに影響）
- FTDソフトウェアバージョン：7.4.2.4（他のバージョンにも影響）
- 動的なオブジェクトベースのアクセスコントロールポリシー(ACP)
- 頻繁なポリシー導入

解決策

Cisco Secure Firewall FTDデバイスで繰り返し発生するフェールオーバーとポリシー展開の問題に対処するには、包括的なトラブルシューティングと修復の手順に従う必要があります。 リストされているワークフローは、モニタリング、データ収集、診断、アップグレードガイダンスなど、各ステップを明確に分離して説明できるように構成されています。

1：パケットトレーサを使用して、目的のトラフィックのルーティングとアクセスを確認します。

```
firepower# packet-tracer input INPUTNAMEIF tcp SRCIP 54321 DSTIP 443
firepower# packet-tracer input INPUTNAMEIF icmp SRCIP 8 0 DSTIP
```

2:FTDでキャプチャを使用し、トラフィックに対して有効なルールとルートが存在するにもかかわらず、「設定済みのルールに従って」エントリでパケットがドロップされるかどうかを確認します。

```
firepower# capture 1 interface INPUTIFNAME trace detail trace-count 1000 match ip host SRCIP host DSTIP
firepower# capture x type asp-drop all match ip host SRCIP host DSTIP
firepower# show capture
capture 1 type raw-data trace detail trace-count 1000 interface inside [Capturing - 31565 bytes]
  match ip 10.1.1.0 255.255.255.0 any
capture x type asp-drop all [Capturing - 31565 bytes]
  match ip 10.1.1.0 255.255.255.0 any
```

3:FTDメッセージログで不具合CSCwo78475の証拠を確認します。

```
> expert
admin@FTD-1:~$ sudo su
Password:
root@FTD-1:/Volume/home/admin# cat /ngfw/var/log/messages | grep -E "New inspector|did not finish|swappe
Feb 10 18:35:03 FTD-device SF-IMS[28366]: New inspector is not initializing Identity API because it's a
Feb 10 18:35:03 FTD-device SF-IMS[28366]: New inspector has different policy groups or ABP name to ID ma
Feb 10 18:35:10 FTD-device SF-IMS[28366]: Reading the muster data snapshot did not finish in time: 4 se
Feb 10 18:36:22 FTD-device SF-IMS[28366]: Identity API state swapped
```

4：これらのログのタイムスタンプを、FTDの導入ログのタイムスタンプと一致させてください。

```
Feb 10 18:34:45 FTD-device policy_apply.pl[18923]: INFO  Deployment type is NORMAL_DEPLOYMENT and devic
Feb 10 18:37:03 FTD-device policy_apply.pl[30894]: INFO  finalizeDeviceDeployment - sandbox = /var/cisc
```

5:FTDがHAの場合は、スタンバイFTDにフェールオーバーし、後でトラフィックの回復を確認するために同じことを確認します。

6：一致するログと条件がFTDで見つかった場合、デバイスは不具合の影響を受け、7.4.3にアップグレードできます。 その間、トラフィックへの影響を減らすために、展開を営業時間外に制限できます。

原因

確認されたトラフィックへの影響とポリシー導入の問題の根本的な原因は、FTDソフトウェアに

影響を与える既知の不具合に起因します。具体的には次のような原因が考えられます。

- Cisco Bug ID CSCwo78475：トラフィックが、ダイナミックオブジェクトを持つFTDデバイスでのポリシー展開中に、不正なアクセスコントロールポリシー(ACP)ルールにヒットする。 これにより、実行コンフィギュレーションに適切なルールが存在する場合でも、正規のトラフィックが拒否される可能性があります。 バージョン7.4.3で修正されています。

関連コンテンツ

- Cisco Bug ID CSCwo78475:ダイナミックオブジェクトを使用したFTDでのポリシー展開中に、トラフィックが誤ったACPルールにヒットする
- シスコテクニカルサポートおよびダウンロード：シスコテクニカルサポートおよびダウンロード

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。