セキュアFTDでSnort 3レートフィルタを使用したレートベースの攻撃防御の設定

お問い合わせ内容

特にSYNフラッド攻撃防止のコンテキストにおいて、複数のサブネットをカバーするルールを構築する方法、実装のベストプラクティスを理解する方法、およびアラートまたはブロック用の適切なしきい値（1秒あたりのカウント）を決定する方法に重点を置きます。

環境

- FTD 7.4.2.4が稼働しているCisco Secure Firewall Firepower
- Firepower 2110ハードウェアプラットフォーム
- Firepower Management Center(FMC)7.6.2.1で管理
- Snort 3侵入防御システム（rate_filter inspectorが有効化されている場合）
- SYNフラッドからの保護を必要とする複数の内部サブネット
- アクティブな障害は存在しません。予防的防御のための設定ガイダンス

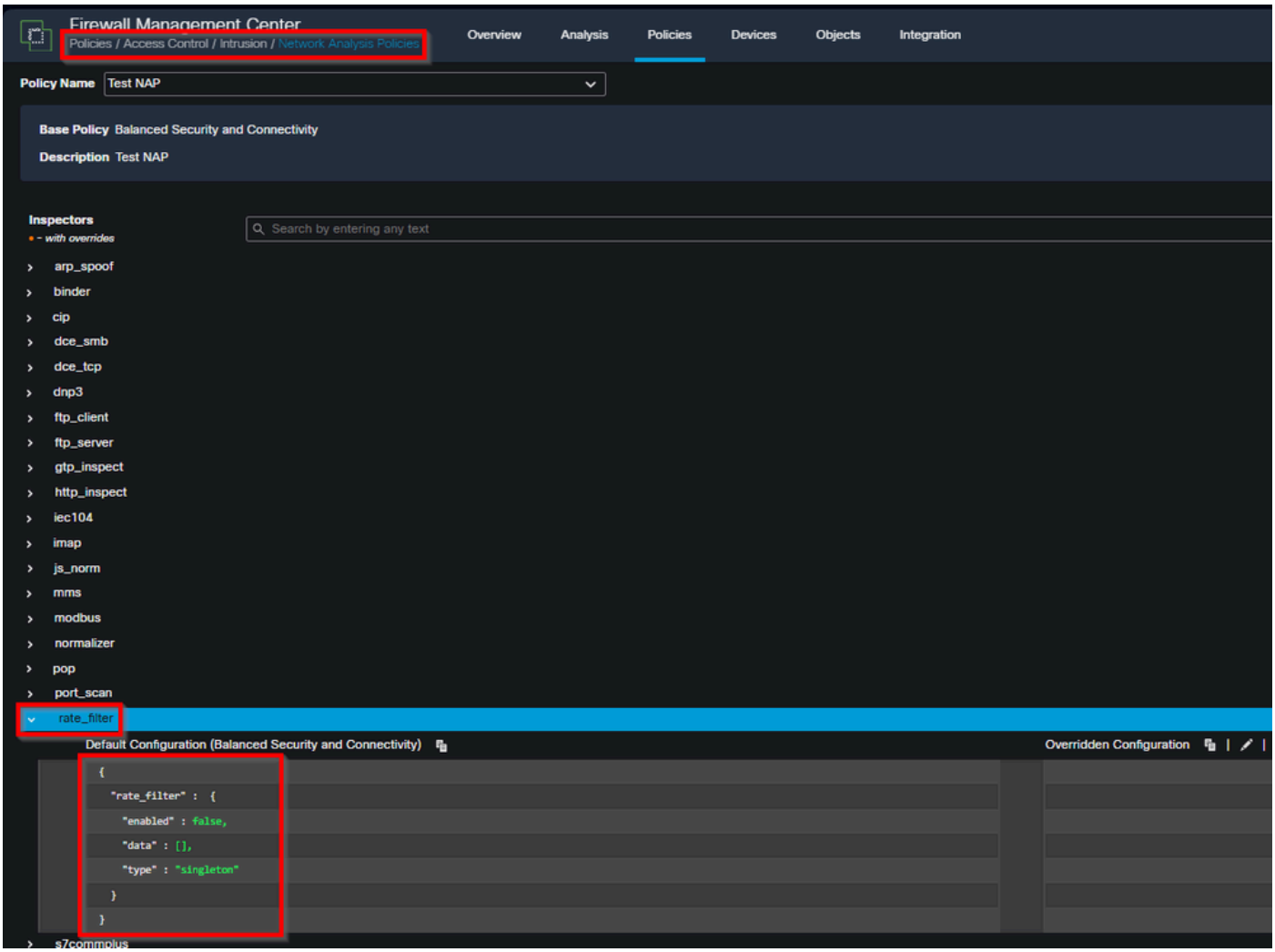
解決策

次の手順では、Cisco Secure Firewall FTDでSnort 3 rate_filterインスペクタを使用してレートベースの攻撃防御を設定および実装する方法を詳しく説明します。複数のサブネットのルール構造の説明、ベストプラクティスの推奨事項などが含まれます。 これらのアクションの目的は、通常のトラフィックのベースラインを確立し、SYNフラッド攻撃を効果的に検出またはブロックできるようにすることです。

注:TACの作業範囲内で、これらのルールフィルタに固有の値を提案または推奨することはできません。 環境はそれぞれ異なり、これらのフィルタの最適値を決定するには、トラフィックパターンとネットワーク設計の詳細な分析が必要です。

1:Snort 3 rate_filterに移動します。

これらのフィルタは、NAPポリシーのSnort 3バージョンをクリックし、左側のパネルから rate_filter ドロップダウンをクリックすることにより、Policies > Access Control: Intrusion > Network Analysis Policies の下で設定されます。



inline_image_0.png (インラインイメージ_0.png)

2: Snort 3レートフィルタルールの構造について

Snort 3のrate_filterインスペクタでは、特定タイプのトラフィック (SYNパケットなど) を監視し、定義済みのしきい値を超えたときにアクション (アラートまたはドロップ) を実行するルールを定義できます。 これらのルールは、複数のサブネットを対象にすることができます。

複数のサブネットに対するrate_filterの設定例 :

```
{
  "rate_filter": {
```

```
    "data": [
      {
        "apply_to": ["10.1.2.0/24", "10.1.3.0/24"],
        "count": 5,
        "gid": 135,
        "sid": 1,
        "new_action": "alert",
        "seconds": 10,
        "timeout": 15,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

パラメータの説明：

- apply_to：フィルタが適用される（複数のサブネットをサポートする）IPアドレスまたはサブネットのリスト。
- count + seconds：イベントのしきい値（たとえば、10秒以内に5つのSYNパケット）。
- gid / sid:Snortイベント（SID 135、SYNフラッド検出のSID 1など）を示します。
- new_action：しきい値を超えたときに実行するアクション(alert、dropなど)。
- timeout：同じ条件に対して新しいアラートまたはアクションがトリガーされるまでの時間。
- track：トラッキングモード(たとえば、送信元IPごとのby_src、宛先IPごとのby_dst)。

3：しきい値の調整とポリシー導入のベストプラクティス

- アラートモードで開始：new_actionをalertに設定し、保守的なしきい値(countやsecondsの値が高いなど)を使用して誤検出を回避します。
- ベースラインネットワークトラフィック：生成されたイベントを監視して、環境やサブネットの「通常の」SYNレートを把握します。
- パラメータを繰り返し調整する：観察されたトラフィックパターンと運用ニーズに基づいて、カウント、秒、およびタイムアウトを調整します。
- ブロッキングへの移行：しきい値が異常な動作を正確に反映していると確信できたら、new_actionをalertからdrop、またはアクティブに攻撃をブロックする権限に相当するように変更します。
- 必要に応じてフィルタを分離する：トラフィックパターンが異なる場合は、異なるセグメン

トまたはロール（たとえば、サーバとユーザサブネット）に対して異なるレート制限を検討します。

- 継続的なモニタリング： rate_filterイベントに対するアラートとモニタリングを維持し、チューニングの問題やアクティブな脅威をすばやく特定します。

原因

ありません。 この設定は、以前のSYNフラッドインシデントによる予防的なセキュリティとガイダンスを目的として要求されたものです。

関連コンテンツ

- Snort 3インスペクタリファレンス：レートフィルタ
- Cisco Secure Firewall Management Centerデバイスコンフィギュレーションガイド7.4：レートベースの攻撃防御
- 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。