Defense Center の SNORT_BPF 変数の設定

目次

概要

Defense Center での検査対象からホストまたはネットワークを除外するには、Berkeley パケット フィルタ（BPF）を使用できます。 Snort では、**Snort_BPF** 変数を使用して、侵入ポリシーの適用対象からトラフィックを除外します。 このドキュメントでは、さまざまなシナリオで **Snort_BPF** 変数を使用する方法を説明します。

> **ヒント**： 検査対象とするトラフィックと検査対象としないトラフィックを決定するには、侵入ポリシーの BPE ではなく、アクセス コントロール ポリシーの信頼ルールを使用することを強く推奨します。 ソフトウェア バージョン 5.2 では **Snort_BPF** 変数を使用できますが、ソフトウェア バージョン 5.3 以降では、この変数は非推奨となっています。

前提条件

要件

Defense Center、侵入ポリシー、Berkeley パケット フィルタ、Snort ルールに関する知識があることを推奨します。

使用するコンポーネント

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

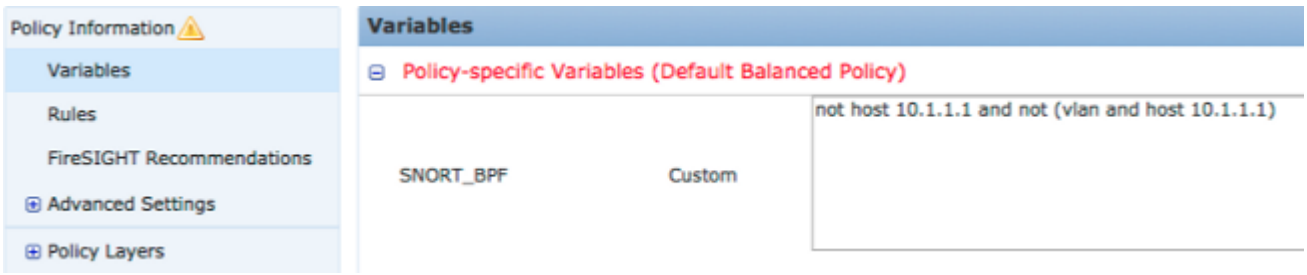
- Defense Center
- ソフトウェア バージョン 5.2

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定手順

Snort_BPF 変数を設定するには、次の手順に従います。

1. Defense Center の Web ユーザ インターフェイスにアクセスします。
2. [Policies] > [Intrusion] > [Intrusion Policy] に移動します。
3. *鉛筆アイコンをクリックし、侵入ポリシーを編集します。*
4. 左側のメニューで、[Variables] をクリックします。
5. 変数を設定したら、変更を保存します。変更を適用するには、侵入ポリシーを再適用する必要があります。



図： Snort_BPF 変数設定ページのスクリーンショット

設定例

参考のために、以下に基本的な例を記載します。

シナリオ 1： 脆弱性スキャナとの間で送受信されるすべてのトラフィックを無視する

1. 脆弱性スキャナは IP アドレス 10.1.1.1 にあります。
2. スキャナとの間で送受信されるすべてのトラフィックを無視します。
3. トラフィックに 802.1q（VLAN）タグが付いているかどうかは問いません。

SNORT_BPF の設定は次のとおりです。

```
not host 10.1.1.1 and not (vlan and host 10.1.1.1)
```

COMPARISON: traffic *is not* VLAN-tagged, but points 1 and 2 remain true would be:

```
not host 10.1.1.1
```

つまり、この設定では、エンドポイントのいずれかが 10.1.1.1（スキャナ）となっているトラフィックが無視されます。

シナリオ 2： 2 つの脆弱性スキャナとの間で送受信されるすべてのトラフィックを無視する

1. 脆弱性スキャナは IP アドレス 10.1.1.1 にあります。
2. 2 つ目の脆弱性スキャナは IP アドレス 10.2.1.1 にあります。
3. スキャナとの間で送受信されるすべてのトラフィックを無視します。
4. トラフィックに 802.11 (VLAN) タグが付いているかどうかは問いません。

SNORT_BPF の設定は次のとおりです。

```
not (host 10.1.1.1 or host 10.2.1.1) and not (vlan and (host 10.1.1.1 or host 10.2.1.1))
```

Comparison: Traffic *is not* VLAN-tagged, but points 1 and 2 remain true would be:

```
not (host 10.1.1.1 or host 10.2.1.1)
```

つまり、この設定では、エンドポイントのいずれかが 10.1.1.1 または 10.2.1.1 となっているトラフィックが無視されます。

> **注:** 重要な点として、ほとんどの場合、VLAN タグは特定の BPF で 1 回だけ出現することに注意してください。 2 回以上出現するのは、ネットワークが入れ子構造の VLAN タギング（「QinQ」と呼ばれることもあります）を使用している場合のみです。

シナリオ 3： 2 つの脆弱性スキャナとの間で送受信される VLAN タグ付きトラフィックを無視する

1. 脆弱性スキャナは IP アドレス 10.1.1.1 にあります。
2. 2 つ目の脆弱性スキャナは IP アドレス 10.2.1.1 にあります。
3. スキャナとの間で送受信されるすべてのトラフィックを無視します。
4. トラフィックには 802.11 (VLAN) タグが付いています。VLAN 101 では特定の (VLAN) タグが使用されるようにします。

SNORT_BPF の設定は次のとおりです。

```
not (host 10.1.1.1 or host 10.2.1.1) and not (vlan 101 and (10.1.1.1 or host 10.2.1.1))
```

シナリオ 4： バックアップ サーバからのトラフィックを無視する

1. ネットワーク バックアップ サーバは IP アドレス 10.1.1.1 にあります。
2. ネットワーク上のコンピュータは、ポート 8080 でこのサーバに接続して夜間バックアップを実行します。

3. 暗号化されて膨大な量になるこのバックアップ トラフィックを無視します。

SNORT_BPF の設定は次のとおりです。

```
not (dst host 10.1.1.1 and dst port 8080) and not (vlan and (dst host 10.1.1.1
and dst port 8080))
```

Comparison: Traffic *is not* VLAN-tagged, but points 1 and 2 remain true would be:

```
not (dst host 10.1.1.1 and dst port 8080)
```

つまり、この設定では、ポート 8080（リスニング ポート）上の 10.1.1.1（架空のバックアップ サーバ）へのトラフィックは IPS 検出エンジンで検査されません。

host の代わりに net を使用して、単一のホストではなくネットワーク ブロックを指定することもできます。 次に、例を示します。

```
not net 10.1.1.0/24
```

一般に、BPF はできる限り明示的に指定することが推奨されます。 そうすることで、検査対象から除外する必要のあるトラフィックは除外される一方、それとは関係のない、不正利用の試みが含まれている可能性のあるトラフィックは除外されなくなります。

シナリオ 5： 個々のホストではなくネットワーク範囲を使用する場合

BPF 変数にホストではなくネットワーク範囲を指定することで、この変数の長さを短くすることができます。 その場合は、host の代わりに net キーワードを使用して CIDR の範囲を指定します。 次に例を示します。

```
not (dst net 10.8.0.0/16 and dst port 8080) and not (vlan and (dst net 10.8.0.0/16
and dst port 8080))
```

> **注:** ネットワーク アドレスは、CIDR 表記と CIDR ブロック アドレス スペース内の使用可能なアドレスを使用して入力してください。 たとえば、net 10.8.2.16/16 ではなく net 10.8.0.0/16 を使用します。

SNORT_BPF 変数は、特定のトラフィックが IPS 検出エンジンで検査されないようにするために使用されます。 これが使用されるのは、通常、パフォーマンス上の理由からです。 この変数は、標準の Berkeley パケット フィルタ（BPF）形式を使用します。 SNORT_BPF 変数と一致するトラフィックは検査対象となります。 一方、SNORT_BPF 変数と一致しないトラフィックは、IPS 検出エンジンで検査されません。