FirePOWER 侵入試験からの EIGRP、OSPF、および BGP メッセージの除外

内容

概要

ルーティング プロトコルは、ルーティング情報を交換、helloメッセージとキープアライブを送信し、ネイバーが到達可能であることを確認します。負荷で、Cisco FirePOWERアプライアンスはネイバーのダウンを宣言するルータのキープアライブ メッセージの入ったカバン低下なし）十分長く延びる可能性があります。ドキュメントはキープアライブを除外し、ルーティング プロトコルのコントロール プレーン トラフィックを信頼するルールを作成する手順を示します。これは、FirePOWERアプライアンスを使用すると、入力インターフェイスから出力にパケットをスイッチング サービスは試験の遅延なし上のインターフェイス。

前提条件

使用するコンポーネント

このドキュメントのアクセス制御ポリシーの変更は次のハードウェア プラットフォームを使用します:

- Firepower Management Center（FMC）
- Firepower アプライアンス：7000 シリーズ、8000 シリーズ モデル

注：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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

- ルータAとルータBがレイヤ2に隣接してインラインFirePOWERアプライアンスを認識しない（ipsとして分類される）。
- ルータ A - 10.0.0.1/24
- ルータ B - 10.0.0.2/24

- テストされた各Interior Gateway Protocol（EIGRP）、およびOSPFルーティング プロトコルは10.0.0.0/24ネットワークで提供されています。
- テスト、e BGPとBGPが使用されたときには直接接続された物理インターフェイスはpeeringsでupdate-sourceとして使用されました。

コンフィギュレーション

EIGRPの例

ルータ

ルータ A：

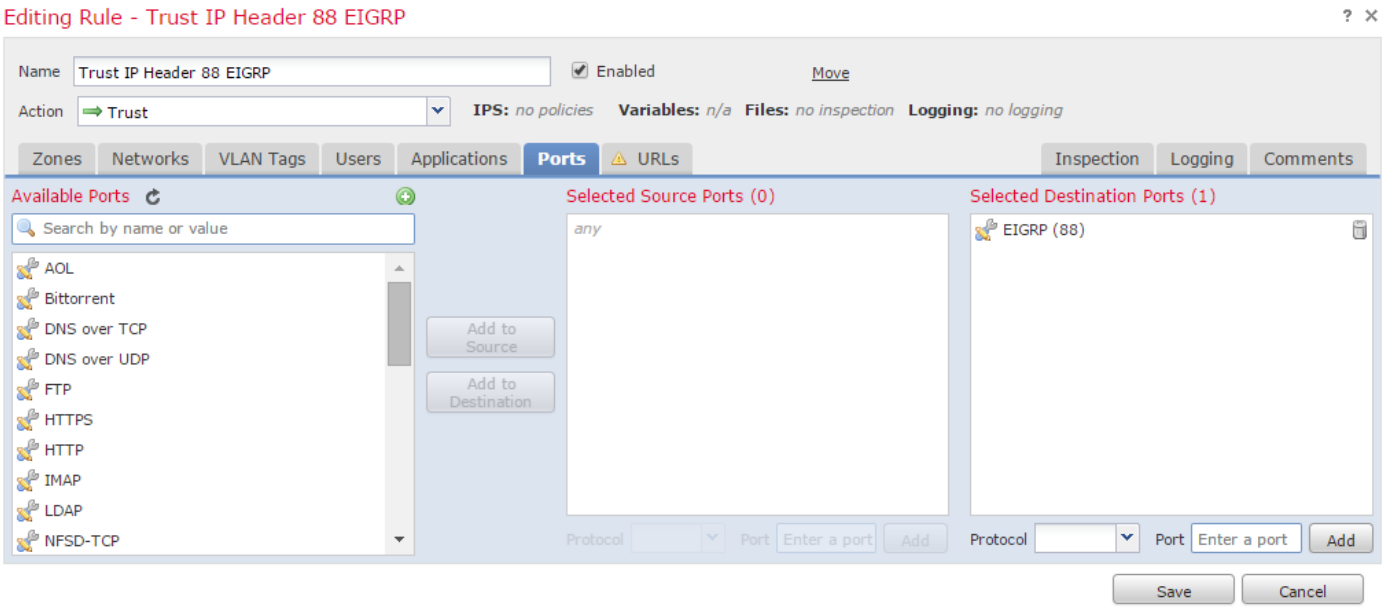
```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

ルータ B：

```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

FireSIGHT Management Center

1. FirePOWERアプライアンスに適用されるアクセス コントロール ポリシーを選択します。
2. 信頼の動作とアクセス コントロール ルールを**作成します。**
3. ポート**で、プロトコル88でEIGRPを選択して選択します。**
4. [宛先ポートにポートを追加ます。
5. アクセス コントロール ルールを保存します。



OSPF の例

ルータ

ルータ A：

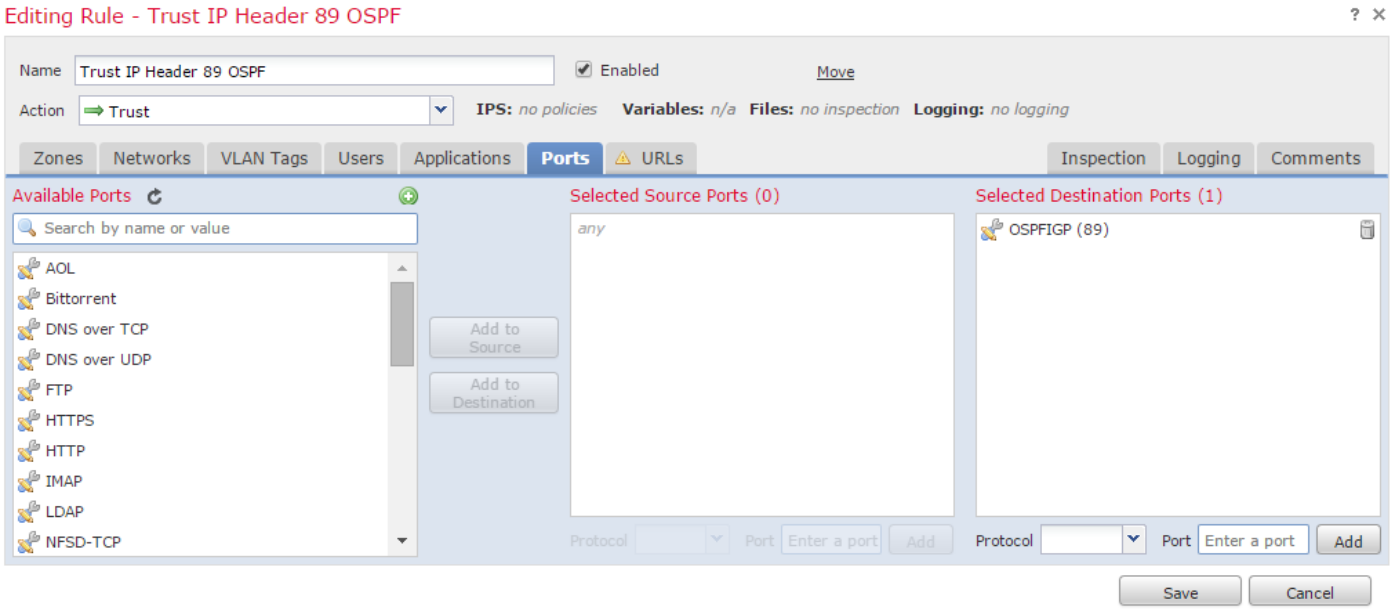
```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

ルータ B：

```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

FireSIGHT Management Center

1. FirePOWERアプライアンスに適用されるアクセス コントロール ポリシーを選択します。
2. 信頼の動作とアクセス コントロール ルールを作成します。
3. ポートで、プロトコル89でOSPFを選択して選択します。
4. [宛先ポートにポートを追加ます。
5. アクセス コントロール ルールを保存します。



BGP の例

ルータ

ルータ A：

```
router bgp 65001
neighbor 10.0.0.2 remote-as 65002
```

ルータ B：

```
router bgp 65002
neighbor 10.0.0.1 remote-as 65001
```

FireSIGHT Management Center

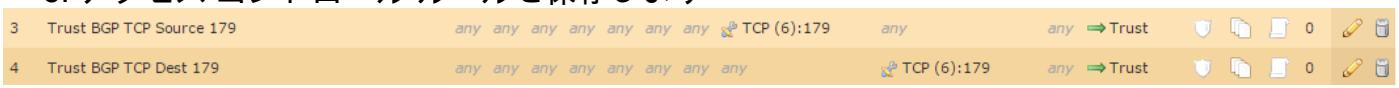
注：ポート179がBGPスピーカのTCP SYNがセッションを設定する発信元または宛先ポートなので、2つのアクセス コントロール エントリを作成します。

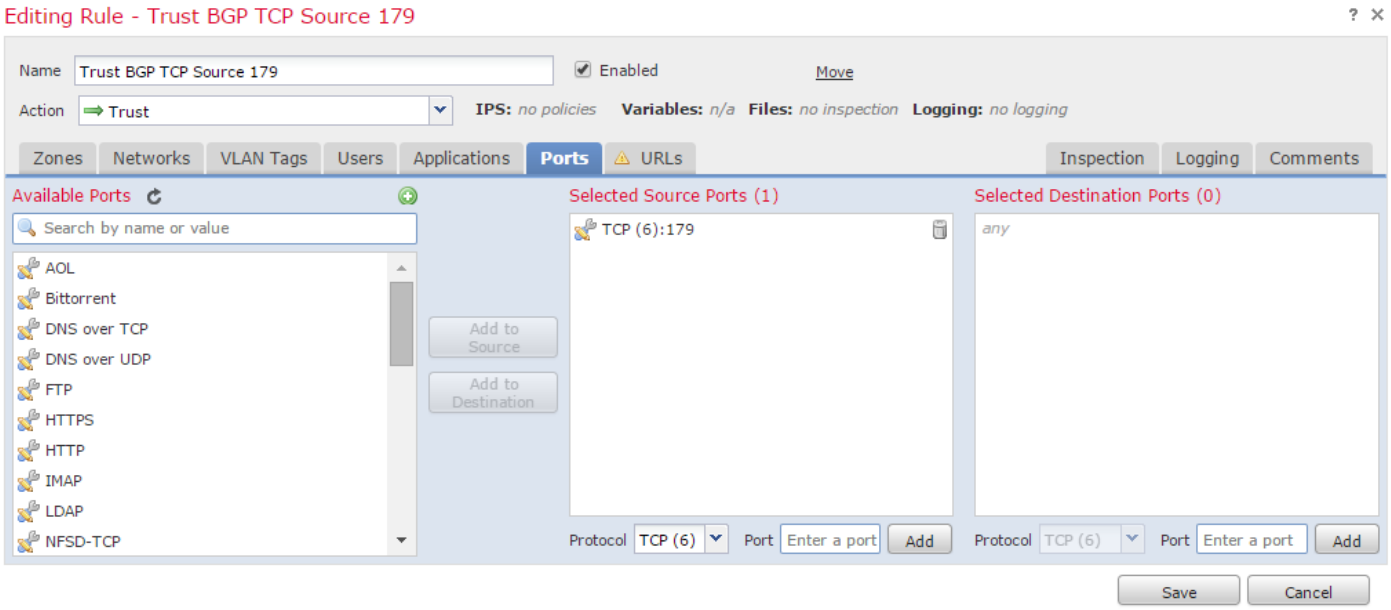
ルール 1：

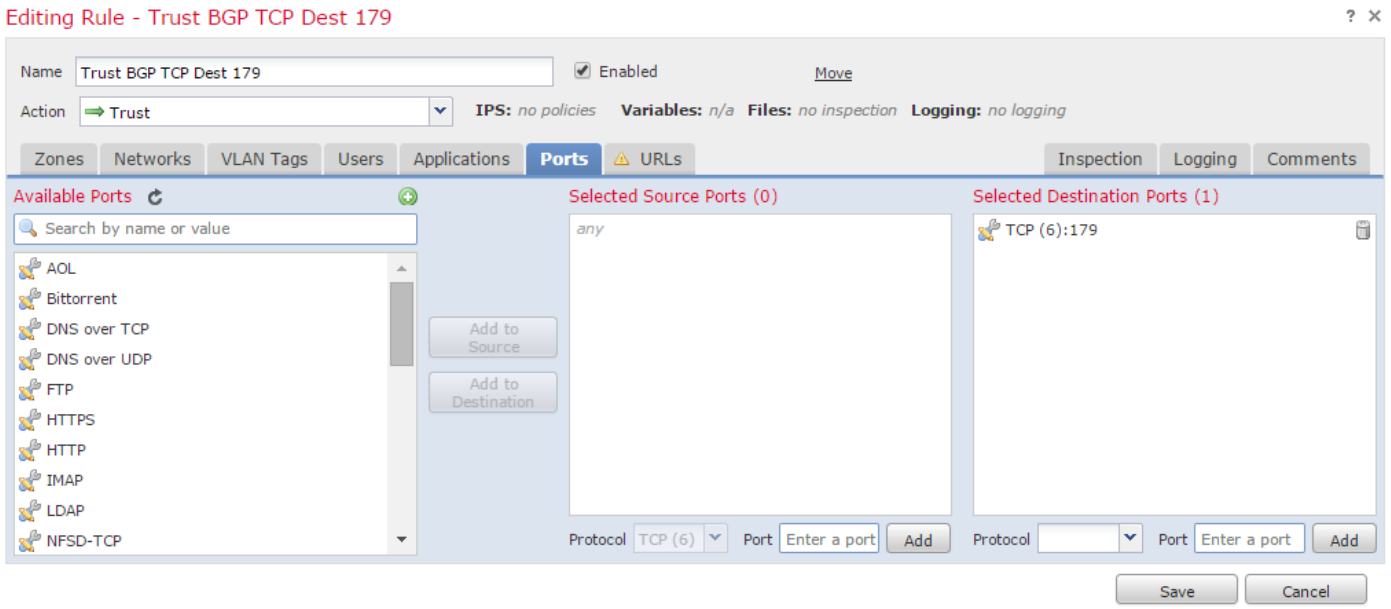
1. FirePOWERアプライアンスに適用されるアクセス コントロール ポリシーを選択します。
2. 信頼の動作とアクセス コントロール ルールを**作成します。**
3. ポート**で、TCPを記録する[(6) とポート179を入力します。**
4. [送信元ポートにポートを追加ます。
5. アクセス コントロール ルールを保存します。

ルール 2：

1. FirePOWERアプライアンスに適用されるアクセス コントロール ポリシーを選択します。
2. 信頼の動作とアクセス コントロール ルールを**作成します。**
3. ポート**で、TCPを記録する[(6) とポート179を入力します。**
4. [宛先ポートにポートを追加ます。
5. アクセス コントロール ルールを保存します







確認

信頼のルールが正しく動作することを確認するには、FirePOWERアプライアンスのパケットをキャプチャします。EIGRP、OSPF、パケット キャプチャのBGPトラフィックの方、トラフィックが期待どおりに信頼されていません。

> **ヒント**：FirePOWERアプライアンスのトラフィックをキャプチャする方法の手順について説明します。

次に例を示します。

EIGRP

信頼のルールが期待どおりに動作すると、次のトラフィックをドロップ":

```
16:46:51.568618 IP 10.0.0.1 > 224.0.0.10: EIGRP Hello, length: 40
16:46:51.964832 IP 10.0.0.2 > 224.0.0.10: EIGRP Hello, length: 40
```

OSPF

信頼のルールが期待どおりに動作すると、表示される次のトラフィックが表示されます:

```
16:46:52.316814 IP 10.0.0.2 > 224.0.0.5: OSPFv2, Hello, length 60
16:46:53.236611 IP 10.0.0.1 > 224.0.0.5: OSPFv2, Hello, length 60
```

BGP

信頼のルールが期待どおりに動作すると、表示される次のトラフィックが表示されます:

```
17:10:26.871858 IP 10.0.0.1.179 > 10.0.0.2.32158: Flags [S.], seq 1060979691, ack 3418042121,
win 16384, options [mss 1460], length 0
17:10:26.872584 IP 10.0.0.2.32158 > 10.0.0.1.179: Flags [.], ack 1, win 16384, length 0
```

> **注**：TCPキープアライブとのBGPライドはIGPほど頻繁ではありません。そこで更新するプレフィックス想定しない、または廃止、ポートTCP/179トラフィックを検知していないことを確認する長期を待つ必要があります。

トラブルシューティング

まだルーティング プロトコル トラフィックが表示されたら、次のタスクを実行:

1. アクセス制御ポリシーがFireSIGHT Management CenterからFirePOWERアプライアンスに正しく適用されていることを確認します。そのために、システム>**モニタリング>タスク ステータス ページに移動します。**
2. ルール アクションが不安定であることを確認し、許可しないことを**確かめます。**

3. ロギングが信頼ルールで有効**になっていないことを確認します。**