

# 從Firepower入侵檢測排除EIGRP、OSPF和BGP消息

## 目錄

[簡介](#)

[必要條件](#)

[採用元件](#)

[網路圖表](#)

[組態](#)

[EIGRP示例](#)

[OSPF示例](#)

[BGP範例](#)

[驗證](#)

[EIGRP](#)

[OSPF](#)

[BGP](#)

[疑難排解](#)

## 簡介

路由協定傳送hello消息和keepalive以交換路由資訊並確保鄰居仍然可訪問。在重負載下，Cisco Firepower裝置可能會延遲keepalive消息（不丟棄），使路由器有足夠的時間宣告其鄰居已關閉。本文檔提供了建立信任規則以排除路由協定的keepalive和控制平面流量的步驟。它使Firepower裝置或服務能夠將資料包從入口切換到出口介面，而不會延遲檢查。

## 必要條件

### 採用元件

本文檔中的訪問控制策略更改使用以下硬體平台：

- FireSIGHT管理中心(FMC)
- Firepower裝置：7000系列、8000系列型號

**附註：**本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

。

## 網路圖表

- 路由器A和路由器B是第2層相鄰路由器，並不知道內聯Firepower裝置（標籤為ips）。
- 路由器A - 10.0.0.1/24
- 路由器B - 10.0.0.2/24



- 對於每個測試的內部網關協定（EIGRP和OSPF），路由協定在10.0.0.0/24網路上啟用。
- 測試BGP時，使用e-BGP，且直接連線的物理介面用作對等體的更新源。

## 組態

### EIGRP示例

在路由器上

路由器A:

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

路由器B:

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

### FireSIGHT管理中心

1. 選擇應用於Firepower裝置的訪問控制策略。
2. 建立具有「信任」操作的訪問控制規則。
3. 在Ports頁籤下，選擇協定88下的EIGRP。
4. 按一下「Add」，將連線埠新增到目的地連線埠。
5. 儲存訪問控制規則。

Editing Rule - Trust IP Header 88 EIGRP

The screenshot shows the 'Editing Rule - Trust IP Header 88 EIGRP' configuration window. The rule is enabled and has an action of 'Trust'. The 'Ports' tab is selected, showing 'Selected Source Ports (0)' as 'any' and 'Selected Destination Ports (1)' as 'EIGRP (88)'. The 'Available Ports' list includes various protocols like AOL, Bittorrent, DNS over TCP, etc.

### OSPF示例

在路由器上

路由器A:

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

路由器B:

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

### FireSIGHT管理中心

1. 選擇應用於Firepower裝置的訪問控制策略。
2. 建立具有「信任」操作的訪問控制規則。
3. 在Ports頁籤下，選擇協定89下的OSPF。
4. 按一下「Add」，將連線埠新增到目的地連線埠。
5. 儲存訪問控制規則。

Editing Rule - Trust IP Header 89 OSPF

The screenshot shows the 'Editing Rule' interface for a rule named 'Trust IP Header 89 OSPF'. The rule is enabled and has an action of 'Trust'. The 'Ports' tab is selected, showing a list of available ports on the left and selected source and destination ports on the right. The destination port is set to 'OSPF (89)'. The interface includes buttons for 'Add to Source', 'Add to Destination', 'Save', and 'Cancel'.

## BGP範例

在路由器上

路由器A:

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

路由器B:

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

### FireSIGHT管理中心

附註：您必須建立兩個存取控制專案，因為連線埠179可能是來源或目的地連線埠，取決於BGP發言者的TCP SYN首先建立作業階段。

## 規則1:

1. 選擇應用於Firepower裝置的訪問控制策略。
2. 使用Trust操作建立訪問控制規則。
3. 在Ports頁籤下，選擇TCP(6)，然後輸入port 179。
4. 按一下「Add」，將連線埠新增到來源連線埠。
5. 儲存訪問控制規則。

## 規則2:

1. 選擇應用於Firepower裝置的訪問控制策略。
2. 使用Trust操作建立訪問控制規則。
3. 在Ports索引標籤下，選擇TCP(6)，然後輸入port 179。
4. 按一下「Add」，將連線埠新增到目的地連線埠。
5. 儲存訪問控制規則。

3	Trust BGP TCP Source 179	any any any any any any any any	TCP (6):179	any	any	Trust			0	
4	Trust BGP TCP Dest 179	any any any any any any any any	TCP (6):179	any	any	Trust			0	

### Editing Rule - Trust BGP TCP Source 179

Name: Trust BGP TCP Source 179  Enabled [Move](#)

Action: Trust  IPS: no policies Variables: n/a Files: no inspection Logging: no logging

Zones Networks VLAN Tags Users Applications **Ports** URLs Inspection Logging Comments

Available Ports

- AOL
- Bittorrent
- DNS over TCP
- DNS over UDP
- FTP
- HTTPS
- HTTP
- IMAP
- LDAP
- NFSD-TCP

Selected Source Ports (1)

- TCP (6):179

Selected Destination Ports (0)

any

Protocol TCP (6) Port Enter a port Add

Protocol TCP (6) Port Enter a port Add

Save Cancel

### Editing Rule - Trust BGP TCP Dest 179

Name: Trust BGP TCP Dest 179  Enabled [Move](#)

Action: Trust  IPS: no policies Variables: n/a Files: no inspection Logging: no logging

Zones Networks VLAN Tags Users Applications **Ports** URLs Inspection Logging Comments

Available Ports

- AOL
- Bittorrent
- DNS over TCP
- DNS over UDP
- FTP
- HTTPS
- HTTP
- IMAP
- LDAP
- NFSD-TCP

Selected Source Ports (0)

any

Selected Destination Ports (1)

- TCP (6):179

Protocol TCP (6) Port Enter a port Add

Protocol Port Enter a port Add

Save Cancel

## 驗證

為了驗證信任規則是否按預期運行，請在Firepower裝置上捕獲資料包。如果您在資料包捕獲中注意到EIGRP、OSPF或BGP流量，則該流量未按預期受信任。

**提示：** 閱讀以找到有關如何在Firepower裝置上捕獲流量的步驟。

以下是一些範例：

## EIGRP

如果信任規則按預期運行，則不應看到以下流量：

```
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

如果信任規則按預期運行，則不應看到以下流量：

```
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

如果信任規則按預期運行，則不應看到以下流量：

```
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
```

**附註：** TCP和keepalive上的BGP訪問並不像IGP那樣頻繁。假設沒有要更新或撤銷的字首，您可能需要等待更長時間以驗證埠TCP/179上未看到流量。

## 疑難排解

如果仍然看到路由協定流量，請執行以下任務：

1. 驗證訪問控制策略是否已成功從FireSIGHT管理中心應用到Firepower裝置。為此，請導航到 **System > Monitoring > Task Status** 頁。
2. 驗證規則操作是否為**Trust**而不是**Allow**。
3. 驗證是否未在**Trust**規則上啟用日誌記錄。