

# EIGRP、OSPF和BGP消息排除从Firepower入侵检查的

## 目录

[简介](#)

[先决条件](#)

[使用的组件](#)

[网络图](#)

[配置](#)

[EIGRP示例](#)

[OSPF示例](#)

[BGP示例](#)

[验证](#)

[EIGRP](#)

[OSPF](#)

[BGP](#)

[排除故障](#)

## 简介

路由协议发送hello消息和Keepalive交换路由信息和保证邻居可及的。在重载下，思科Firepower设备可能延迟一个保活信息(没有丢弃它)太久路由器的能宣称其邻居下来。本文提供您步骤创建托拉斯规则排除Keepalive和路由协议的控制层面流量。它使Firepower设备或服务转换数据包从入口到出口接口，不用检查延迟。

## [先决条件](#)

### 使用的组件

在本文的访问控制策略变更使用以下硬件平台：

- FireSIGHT管理中心(FMC)
- Firepower设备：7000系列，8000系列型号

**Note:**关于本文的信息从在特定实验室环境的设备创建。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 网络图

- 路由器A和路由器B是相邻的第2层，并且对轴向Firepower设备是没有察觉的(被标记作为ips)。
- 路由器A - 10.0.0.1/24
- 路由器B - 10.0.0.2/24



- 对于测试的每内部网关协议(EIGRP和OSPF)，路由协议在10.0.0.0/24网络启用。
- 当测试BGP时，使用了e-BGP，并且直接地连接的物理接口为对等互连使用，当更新来源。

## 配置

### EIGRP示例

在路由器上

路由器A：

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

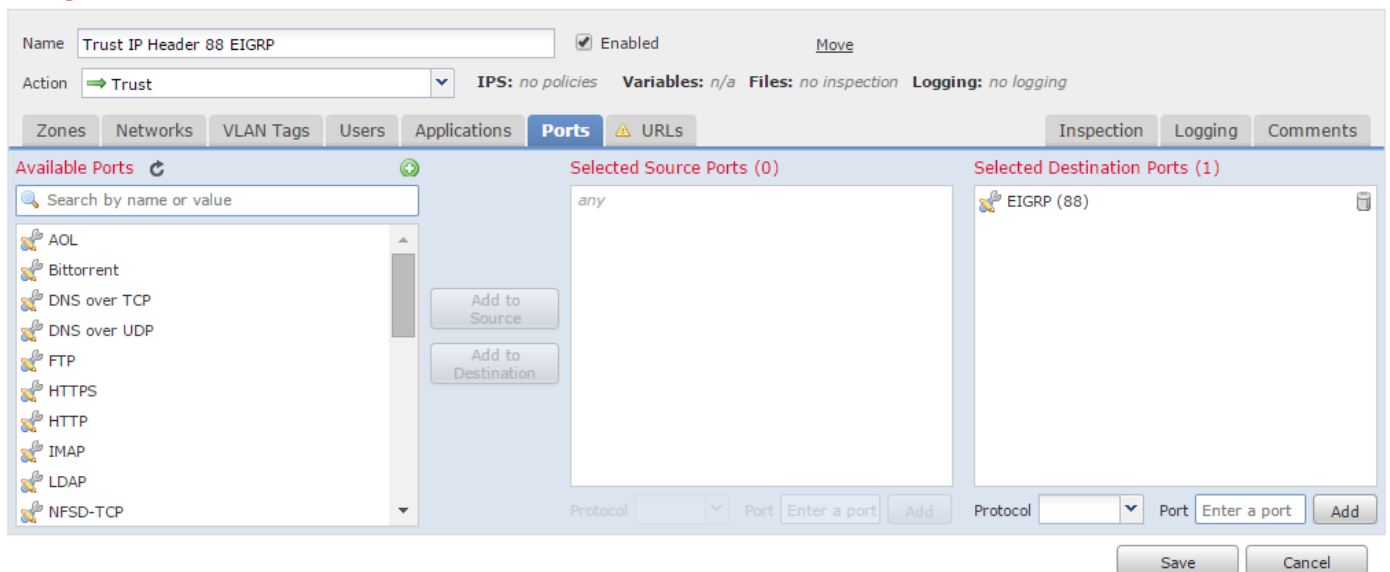
路由器B：

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

在FireSIGHT管理中心

1. 选择访问控制策略应用对Firepower设备。
2. 创建与托拉斯的操作的访问控制规则。
3. 在端口下请选中，选择EIGRP在协议88下。
4. 单击添加添加端口到目的地端口。
5. 保存访问控制规则。

Editing Rule - Trust IP Header 88 EIGRP



### 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
```

### 在FireSIGHT管理中心

1. 选择访问控制策略应用对Firepower设备。
2. 创建与托拉斯的操作的访问控制规则。
3. 在端口下请选中，选择OSPF在协议89下。
4. 单击添加添加端口到目的地端口。
5. 保存访问控制规则。

#### Editing Rule - Trust IP Header 89 OSPF

The screenshot shows the 'Editing Rule' interface for 'Trust IP Header 89 OSPF'. The rule is enabled and has an action of 'Trust'. The 'Ports' tab is selected, showing 'Available Ports' on the left, 'Selected Source Ports (0)' in the middle, and 'Selected Destination Ports (1)' on the right. The destination port is 'OSPF(89)'. There are 'Add to Source' and 'Add to Destination' buttons, and 'Save' and 'Cancel' buttons at the bottom.

## BGP示例

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
```

### 在FireSIGHT管理中心

**Note:** 您必须创建两访问控制条目，因为端口179可能是BGP扬声器的TCP SYN首先建立会话的源或目的地端口。

## 规则 1 :

1. 选择访问控制策略应用对Firepower设备。
2. 创建与托拉斯的操作的访问控制规则。
3. 在端口下请选中，挑选TCP(6)和回车端口179。
4. 单击添加添加端口到源端口。
5. 保存访问控制规则。

## 规则 2 :

1. 选择访问控制策略应用对Firepower设备。
2. 创建与托拉斯的操作的访问控制规则。
3. 在端口下请选中，挑选TCP(6)和回车端口179。
4. 单击添加添加端口到目的地端口。
5. 保存访问控制规则。

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

## 验证

为了验证**托拉斯**规则操作正如所料，请获取在Firepower设备的数据包。如果注意在数据包捕获的EIGRP、OSPF或者BGP流量，则流量没有被信任正如所料。

**提示：**读查找关于怎样的步骤捕获在Firepower设备的流量。

例如：

## EIGRP

如果托拉斯规则运行正如所料，您不应该看到以下流量：

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

## OSPF

如果托拉斯规则是运行正如所料，您不应该看到以下流量：

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

## BGP

如果托拉斯规则是运行正如所料，您不应该看到以下流量：

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

**Note:**在TCP顶部的BGP乘驾和Keepalive不是一样常见象IGP。假设那里没有将更新的前缀或让步，您可能需要等待长时间验证您看不到在端口TCP/179的流量。

## 排除故障

如果仍然看到路由协议流量，请执行以下任务：

1. 验证访问控制策略从FireSIGHT管理中心顺利地应用到Firepower设备。为了执行那，请导航对的系统> **Status**页**Monitoring**>的任务。
2. 验证规则操作是**托拉斯**和**不准许**。
3. 验证记录在**托拉斯**规则没有启用。