

从Firepower入侵检测排除EIGRP、OSPF和BGP消息

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](#)

[确认](#)

[EIGRP](#)

[OSPF](#)

[调试输出中显示“BGP](#)

[故障排除](#)

简介

路由协议发送hello消息和keepalive来交换路由信息并确保邻居仍然可到达。在负载较重时，Cisco Firepower设备可能会延迟保持连接消息（不丢弃该消息）足够长，以便路由器声明其邻居关闭。本文档提供创建信任规则以排除路由协议的keepalive和控制平面流量的步骤。它使Firepower设备或服务能够将数据包从入口交换到出口接口，而无需延迟检查。

先决条件

使用的组件

本文档中的访问控制策略更改使用以下硬件平台：

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

注意：本文档中的信息是从特定实验环境中的设备创建的。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是第2层邻接的，不知道内联Firepower设备（标记为ips）。
- 路由器A - 10.0.0.1/24
- 路由器B - 10.0.0.2/24



- 对于测试的每个内部网关协议（EIGRP和OSPF），路由协议在10.0.0.0/24网络上启用。
- 在测试BGP时，使用e-BGP，并且直接连接的物理接口用作对等体的更新源。

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
```

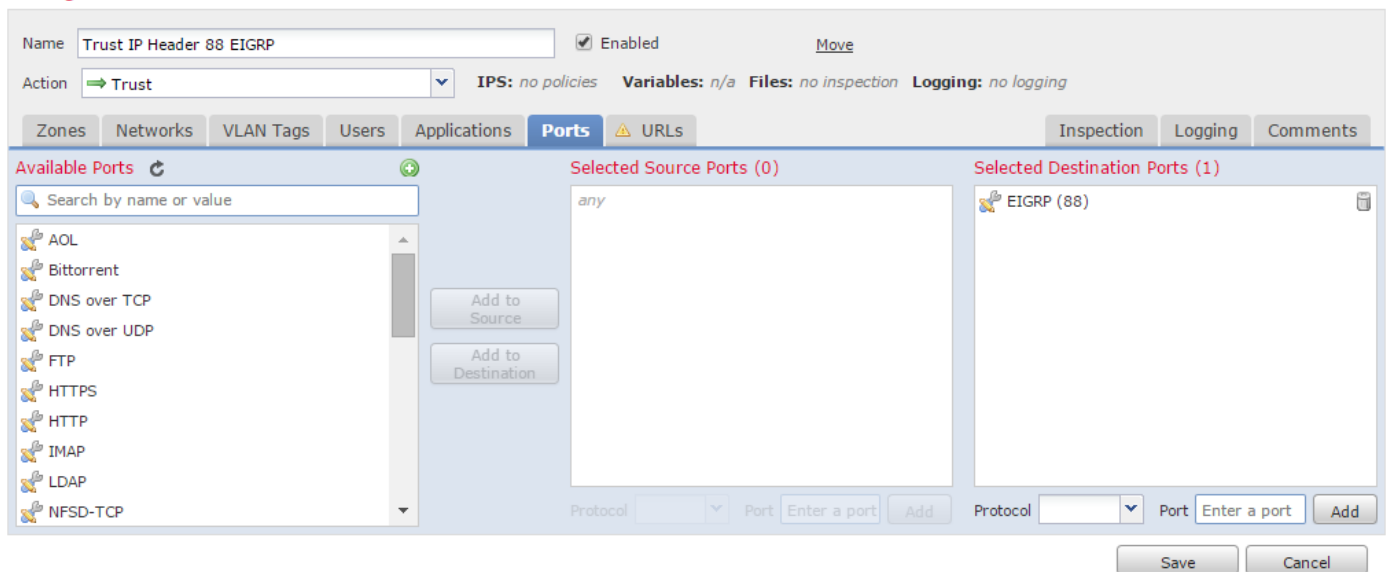
路由器 B:

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

在FireSIGHT管理中心

1. 选择应用于Firepower设备的访问控制策略。
2. 使用Trust操作创建访问控制规则。
3. 在“端口”选项卡下，在协议88下选择EIGRP。
4. 单击Add将端口添加到目标端口。
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. 选择应用于Firepower设备的访问控制策略。
2. 使用Trust操作创建访问控制规则。
3. 在Ports选项卡下，选择协议89下的OSPF。
4. 单击Add将端口添加到目标端口。
5. 保存访问控制规则。

Editing Rule - Trust IP Header 89 OSPF

The screenshot shows the 'Editing Rule' window for 'Trust IP Header 89 OSPF'. The rule is enabled and has an action of 'Trust'. The configuration is set for the 'Ports' tab. The 'Selected Source Ports' list is empty, showing 'any'. The 'Selected Destination Ports' list contains 'OSPF (89)'. The 'Available Ports' list on the left includes various protocols such as AOL, Bittorrent, DNS over TCP, DNS over UDP, FTP, HTTPS, HTTP, IMAP, LDAP, and NFS-D-TCP. The interface also features buttons for 'Add to Source', 'Add to Destination', 'Save', and 'Cancel'.

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

注意：您必须创建两个访问控制条目，因为端口179可能是源或目标端口，具体取决于哪个BGP发言者的TCP SYN首先建立会话。

规则 1 :

1. 选择应用于Firepower设备的访问控制策略。
2. 使用Trust操作创建访问控制规则。
3. 在“端口”选项卡下，选择TCP(6)并输入端口179。
4. 单击Add将端口添加到源端口。
5. 保存访问控制规则。

规则 2 :

1. 选择应用于Firepower设备的访问控制策略。
2. 使用Trust操作创建访问控制规则。
3. 在“端口”选项卡下，选择TCP(6)并输入端口179。
4. 单击Add将端口添加到目标端口。
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: Search by name or value

- 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: Search by name or value

- 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

确认

要验证信任规则是否按预期运行，请在Firepower设备上捕获数据包。如果您在数据包捕获中注意到EIGRP、OSPF或BGP流量，则该流量不会按预期受信任。

提示： 请阅读，了解如何捕获Firepower设备上的流量。

例如：

EIGRP

如果信任规则按预期运行，则不应看到以下流量：

```
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

如果信任规则按预期运行，则不应看到以下流量：

```
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
```

调试输出中显示“BGP

如果信任规则按预期运行，则不应看到以下流量：

```
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
```

注意： BGP在TCP上访问，keepalive的频率不如IGP。假设没有要更新或撤消的前缀，您可能需要等待更长的时间来验证您没有看到端口TCP/179上的流量。

故障排除

如果您仍然看到路由协议流量，请执行以下任务：

1. 验证访问控制策略已成功从FireSIGHT管理中心应用到Firepower设备。为此，请导航至“系统”>“**监控**”>“**任务状态**”页。
2. 验证规则操作是“**信任**”而不是“**允许**”。
3. 验证是否未在信任规则上启用日志。