

# Exclusão do EIGRP, do OSPF e dos mensagens BGP da inspeção da intrusão de FirePOWER

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Configuração](#)

[Exemplo EIGRP](#)

[Exemplo OSPF](#)

[Exemplo de BGP](#)

[Verificação](#)

[EIGRP](#)

[OSPF](#)

[BGP](#)

[Troubleshooting](#)

## Introdução

Os protocolos de roteamento enviam mensagens Hello Messages e Keepalives para trocar a informação de roteamento e para assegurar-se de que os vizinhos sejam ainda alcançáveis. Sob a carga pesada, um dispositivo de Cisco FirePOWER pode atrasar um mensagem de keepalive (sem o deixar cair) o suficiente para que um roteador declare seu vizinho para baixo. O documento fornece-lhe as etapas para criar uma regra da confiança para excluir o Keepalives e controlar o tráfego plano de um protocolo de roteamento. Permite os dispositivos ou os serviços de FirePOWER de comutar pacotes do ingresso à interface de saída, sem o atraso da inspeção.

## Pré-requisitos

### [Componentes Utilizados](#)

As alterações de política do controle de acesso neste documento usam as seguintes plataformas de hardware:

- Centro de gerenciamento de FireSIGHT (FMC)
- Dispositivo de FirePOWER: 7000 Series, modelos do 8000 Series

**Note:** A informação neste documento foi criada dos dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Diagrama de Rede

- O roteador A e o roteador B são camada 2 adjacente, e são inconscientes do dispositivo inline de FirePOWER (etiquetado como IP).
- Roteador A - 10.0.0.1/24
- Roteador B - 10.0.0.2/24



- Para cada protocolo Interior Gateway Protocols testado (EIGRP e OSPF), o protocolo de roteamento foi permitido na rede 10.0.0.0/24.
- Quando o BGP de teste, e-BGP foi usado e as interfaces física diretamente conectadas foram utilizadas como a fonte da atualização para os peerings.

## Configuração

### Exemplo EIGRP

#### No roteador

Roteador A:

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

Roteador B:

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

#### No centro de gerenciamento de FireSIGHT

1. Selecione a política do controle de acesso aplicada ao dispositivo de FirePOWER.
2. Crie uma regra do controle de acesso com uma ação da **confiança**.
3. Sob as **portas** catalogue, selecione o **EIGRP** sob o protocolo 88.
4. O clique **adiciona** para adicionar a porta à porta do destino.
5. Salvar a regra do controle de acesso.

Editing Rule - Trust IP Header 88 EIGRP

## Exemplo OSPF

No roteador

Roteador A:

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

Roteador B:

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

## No centro de gerenciamento de FireSIGHT

1. Selecione a política do controle de acesso aplicada ao dispositivo de FirePOWER.
2. Crie uma regra do controle de acesso com uma ação da **confiança**.
3. Sob as **portas** catalogue, selecione o OSPF sob o protocolo 89.
4. O clique **adiciona** para adicionar a porta à porta do destino.
5. Salvar a regra do controle de acesso.

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 'Selected Destination Ports' list contains 'OSPF (89)'. The interface includes search bars, 'Add to Source' and 'Add to Destination' buttons, and 'Save' and 'Cancel' buttons at the bottom.

## Exemplo de BGP

No roteador

Roteador A:

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

Roteador B:

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

## No centro de gerenciamento de FireSIGHT

**Note:** Você deve criar duas entradas de controle de acesso, porque a porta 179 pode ser a porta de origem ou destino segundo que o TCP do auto-falante de BGP SYN estabelece a sessão primeiramente.

### Regra 1:

1. Selecione a política do controle de acesso aplicada ao dispositivo de FirePOWER.
2. Crie uma regra do controle de acesso com uma ação da **confiança**.
3. Sob as **portas** catalogue, selecione **TCP(6)** e entre na **porta 179**.
4. O clique **adiciona** para adicionar a porta à **porta de origem**.
5. Salvar a regra do controle de acesso.

### Regra 2:

1. Selecione a política do controle de acesso aplicada ao dispositivo de FirePOWER.
2. Crie uma regra do controle de acesso com uma ação da **confiança**.
3. Sob as **portas** catalogue, **selecione TCP(6)** e entre na **porta 179**.
4. O clique **adiciona** para adicionar a porta à **porta do destino**.
5. Salvar a regra do controle de acesso

|   |                          |                                 |             |             |     |       |  |  |   |  |
|---|--------------------------|---------------------------------|-------------|-------------|-----|-------|--|--|---|--|
| 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 | 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

Add to Source Add to Destination

Selected Destination Ports (0)

any

Protocol TCP (6) Port Enter a port Add Protocol TCP (6) Port Enter a port Add

Save Cancel

The screenshot shows the configuration page for a rule named "Trust BGP TCP Dest 179". The rule is enabled. The action is set to "Trust". The configuration tabs include "Zones", "Networks", "VLAN Tags", "Users", "Applications", "Ports", "URLs", "Inspection", "Logging", and "Comments". The "Ports" tab is active, showing a list of available ports on the left, including AOL, Bittorrent, DNS over TCP, DNS over UDP, FTP, HTTPS, HTTP, IMAP, LDAP, and NFS-D-TCP. The "Selected Source Ports" list is empty, and the "Selected Destination Ports" list contains "TCP (6):179". There are "Add to Source" and "Add to Destination" buttons between the lists. At the bottom, there are input fields for "Protocol" (set to TCP (6)) and "Port" (set to Enter a port), with "Add" buttons. "Save" and "Cancel" buttons are at the bottom right.

## Verificação

A fim verificar que uma regra da **confiança** se está operando como esperado, capture pacotes no dispositivo de FirePOWER. Se você observa o tráfego EIGRP, OSPF ou BGP na captura de pacote de informação, a seguir o tráfego não está sendo confiado como esperado.

**Tip:** Lido para encontrar as etapas em como capturar o tráfego nos dispositivos de FirePOWER.

Aqui estão alguns exemplos:

### EIGRP

Se a regra da confiança se opera como esperado, você não deve ver o seguinte tráfego:

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

### OSPF

Se a regra da confiança for se opera como esperado, você considera o seguinte tráfego:

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

### BGP

Se a regra da confiança for se opera como esperado, você considera o seguinte tráfego:

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

**Note:** Os passeios BGP sobre o TCP e o Keepalives não são tão frequentes quanto os IGP.

Não estão supondo lá nenhum prefixo a ser atualizado ou retirado, você pode precisar de esperar um período de tempo mais longo para verificar que você não está vendo o tráfego na porta TCP/179.

## Troubleshooting

Se você ainda vê o tráfego do protocolo de roteamento, execute por favor as seguintes tarefas:

1. Verifique que a política do controle de acesso esteve aplicada com sucesso do centro de gerenciamento de FireSIGHT ao dispositivo de FirePOWER. A fim fazer isso, navegue à página do **estado do sistema > da monitoração > da tarefa**.
2. Verifique que a ação da regra é **confiança** e **para não reservar**.
3. Verifique que registrar não está permitido na regra da **confiança**.