Exclusão de mensagens EIGRP, OSPF e BGP da inspeção de intrusão do Firepower

Contents

Introduction

Os protocolos de roteamento enviam mensagens hello e keepalives para trocar informações de roteamento e garantir que os vizinhos ainda estejam acessíveis. Sob carga pesada, um dispositivo Cisco Firepower pode retardar uma mensagem de keepalive (sem descartá-la) por tempo suficiente para que um roteador declare seu vizinho inativo. O documento fornece as etapas para criar uma regra de Confiança para excluir keepalives e tráfego de plano de controle de um protocolo de roteamento. Ele permite que os dispositivos ou serviços Firepower comutem pacotes da interface de entrada para a interface de saída, sem o atraso da inspeção.

Prerequisites

Componentes Utilizados

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

- FireSIGHT Management Center (FMC)
- Dispositivo Firepower: Série 7000, modelos 8000

> **Note**: As informações neste documento foram criadas a partir dos dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagrama de Rede

- Os roteadores A e B são adjacentes à camada 2 e não conhecem o dispositivo Firepower em linha (rotulado como ips).
- Roteador A - 10.0.0.1/24
- Roteador B - 10.0.0.2/24

- Para cada Interior Gateway Protocol testado (EIGRP e OSPF), o protocolo de roteamento foi ativado na rede 10.0.0.0/24.
- Ao testar o BGP, o e-BGP foi usado e as interfaces físicas diretamente conectadas foram utilizadas como a fonte de atualização para os peerings.

Configuração

Exemplo de EIGRP

No roteador

Router A:

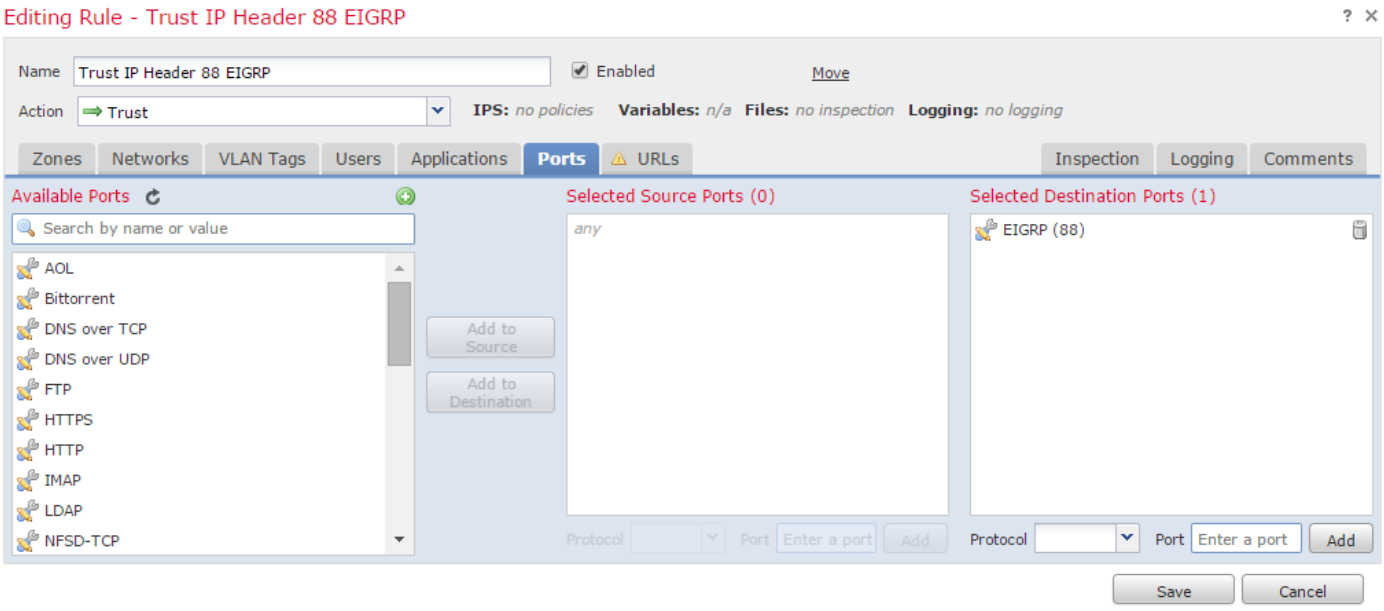
```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

Router B:

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

No FireSIGHT Management Center

1. Selecione a Política de controle de acesso aplicada ao Firepower appliance.
2. Crie uma regra de Controle de Acesso com uma ação de **Confiança.**
3. Na guia **Portas**, selecione **EIGRP** no protocolo 88.
4. Clique em **Adicionar** para adicionar a porta à porta de destino.
5. Salve a regra de controle de acesso.



Exemplo de OSPF

No roteador

Router A:

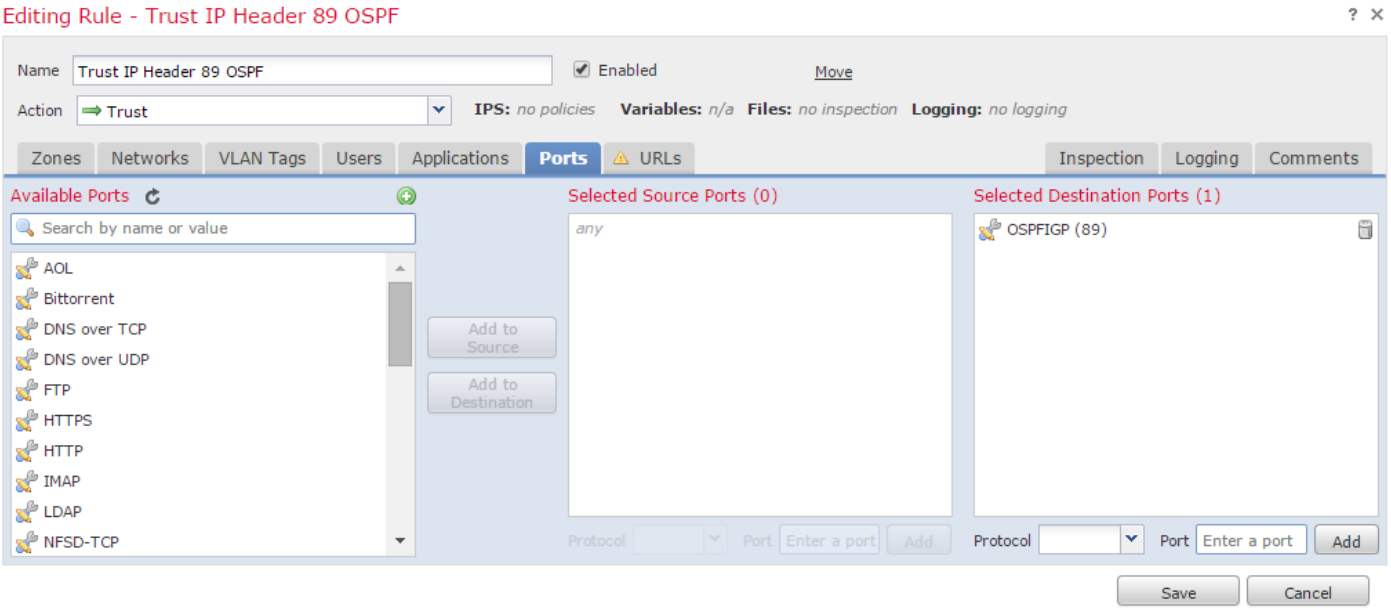
```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

Router B:

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

No FireSIGHT Management Center

1. Selecione a Política de controle de acesso aplicada ao Firepower appliance.
2. Crie uma regra de Controle de Acesso com uma ação de **Confiança.**
3. Na guia **Portas**, selecione OSPF no protocolo 89.
4. Clique em **Adicionar** para adicionar a porta à porta de destino.
5. Salve a regra de controle de acesso.



Exemplo de BGP

No roteador

Router A:

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

Router B:

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

No FireSIGHT Management Center

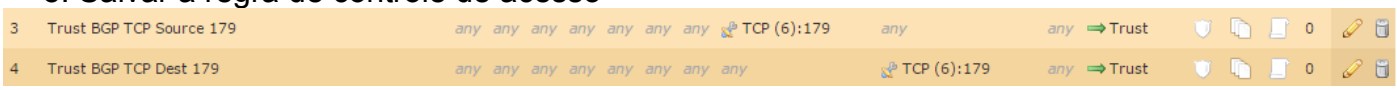
Note: Você deve criar duas entradas de controle de acesso, já que a porta 179 pode ser a porta de origem ou de destino dependendo de qual TCP SYN do alto-falante BGP estabelece a sessão primeiro.

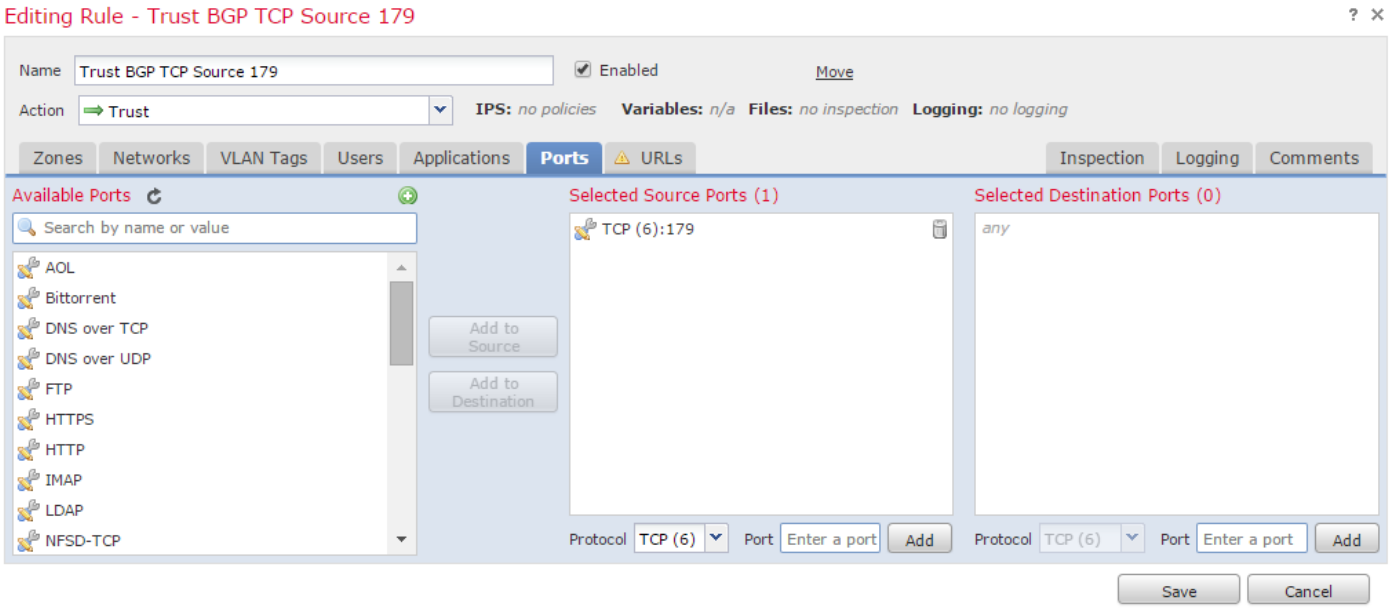
Regra 1:

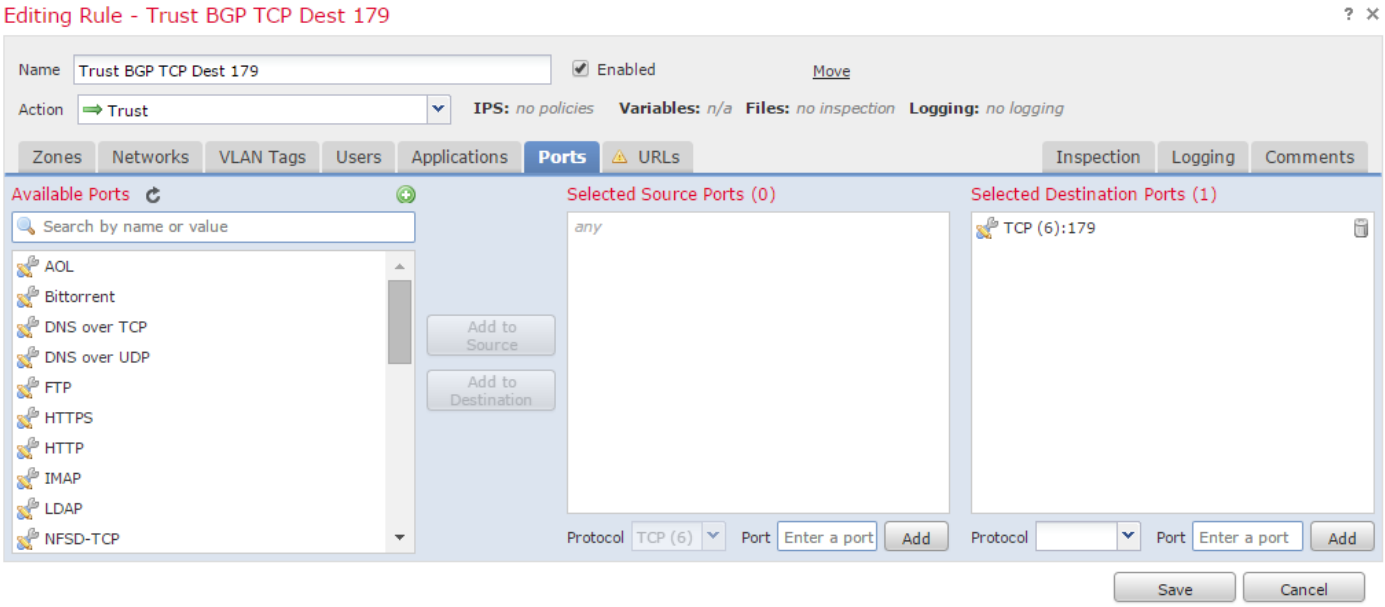
1. Selecione a Política de controle de acesso aplicada ao Firepower appliance.
2. Crie uma regra de Controle de Acesso com uma ação de **Confiança**.
3. Na guia **Portas**, selecione **TCP(6)** e insira a **porta 179**.
4. Clique em **Adicionar** para adicionar a porta à **porta de origem**.
5. Salve a regra de controle de acesso.

Regra 2:

1. Selecione a Política de controle de acesso aplicada ao Firepower appliance.
2. Crie uma regra de Controle de Acesso com uma ação de **Confiança**.
3. Na guia **Portas**, **selecione TCP(6)** e insira a **porta 179**.
4. Clique em **Adicionar** para adicionar a porta à **porta de destino**.
5. Salvar a regra de controle de acesso







Verificação

Para verificar se uma regra **Trust** está funcionando conforme esperado, capture pacotes no Firepower appliance. Se você observar o tráfego EIGRP, OSPF ou BGP na captura de pacotes, o tráfego não está sendo confiável como esperado.

> **Tip**: Leia para encontrar as etapas sobre como capturar tráfego nos dispositivos Firepower.

Aqui estão alguns exemplos:

EIGRP

Se a regra de Confiança funcionar como esperado, você não verá o seguinte tráfego:

```
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

Se a regra de Confiança estiver operando conforme esperado, você não deverá ver o seguinte tráfego:

```
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

Se a regra de Confiança estiver operando conforme esperado, você não deverá ver o seguinte tráfego:

```
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
```

Note: Os passeios de BGP sobre TCP e keepalives não são tão frequentes quanto os IGPs. Supondo que não haja prefixos a serem atualizados ou retirados, talvez seja necessário aguardar um período de tempo maior para verificar se você não está vendo tráfego na porta TCP/179.

Troubleshooting

Se você ainda vir o tráfego do protocolo de roteamento, execute as seguintes tarefas:

1. Verifique se a política de controle de acesso foi aplicada com êxito do FireSIGHT Management Center ao Firepower appliance. Para fazer isso, navegue até a página **Sistema > Monitoramento > Status da Tarefa**.

2. Verifique se a ação da regra é **Trust** e não **Allow**.

3. Verifique se o registro não está ativado na regra **Trust**.