Exclusión de Mensajes EIGRP, OSPF y BGP de la Inspección de Intrusión de Firepower

Contenido

Introducción

Los protocolos de ruteo envían mensajes de saludo y señales de mantenimiento para intercambiar información de ruteo y asegurarse de que los vecinos aún estén accesibles. Bajo una carga pesada, un dispositivo Cisco Firepower puede retrasar un mensaje de keepalive (sin descartarlo) lo suficiente como para que un router declare su vecino inactivo. El documento proporciona los pasos para crear una regla de confianza para excluir keepalives y el tráfico del plano de control de un protocolo de ruteo. Habilita los dispositivos o servicios Firepower para conmutar paquetes de la interfaz de entrada a la de salida, sin el retraso de la inspección.

Prerequisites

Componentes Utilizados

Los cambios de política de control de acceso en este documento utilizan las siguientes plataformas de hardware:

- FireSIGHT Management Center (FMC)
- Dispositivo FirePOWER: 7000 Series, modelos 8000 Series

Nota: La información de este documento se creó a partir de los dispositivos en un entorno de laboratorio 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 la red

- El router A y el router B son adyacentes a la capa 2 y no conocen el dispositivo Firepower en línea (etiquetado como ips).
- Router A - 10.0.0.1/24
- Router B - 10.0.0.2/24

- Para cada protocolo de gateway interior probado (EIGRP y OSPF), el protocolo de routing se habilitó en la red 10.0.0.0/24.
- Al probar BGP, se utilizó e-BGP y se utilizaron las interfaces físicas directamente conectadas como fuente de actualización para los peerings.

Configuración

Ejemplo de EIGRP

En el router

Router A:

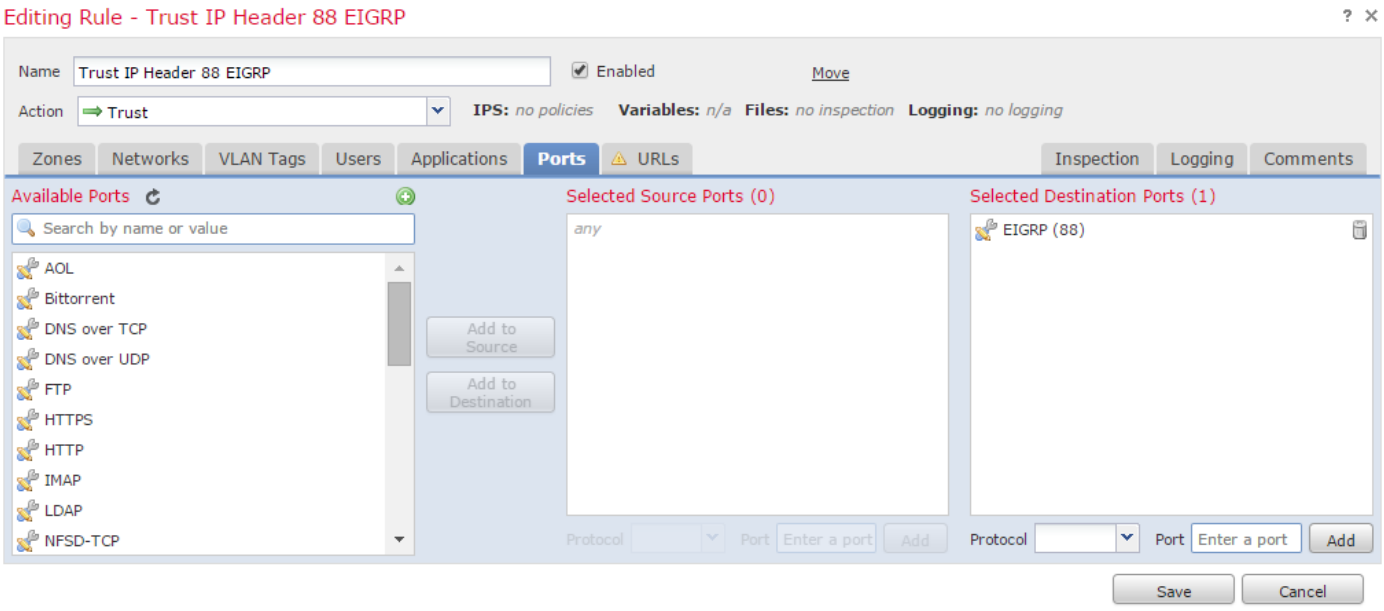
```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

Router B:

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

En FireSIGHT Management Center

1. Seleccione la política de control de acceso aplicada al dispositivo Firepower.
2. Cree una regla de control de acceso con una acción de **Confianza.**
3. Bajo la pestaña **Ports**, seleccione **EIGRP** en el protocolo 88.
4. Haga clic en **Agregar** para agregar el puerto al puerto de destino.
5. Guarde la regla de control de acceso.



Ejemplo de OSPF

En el router

Router A:

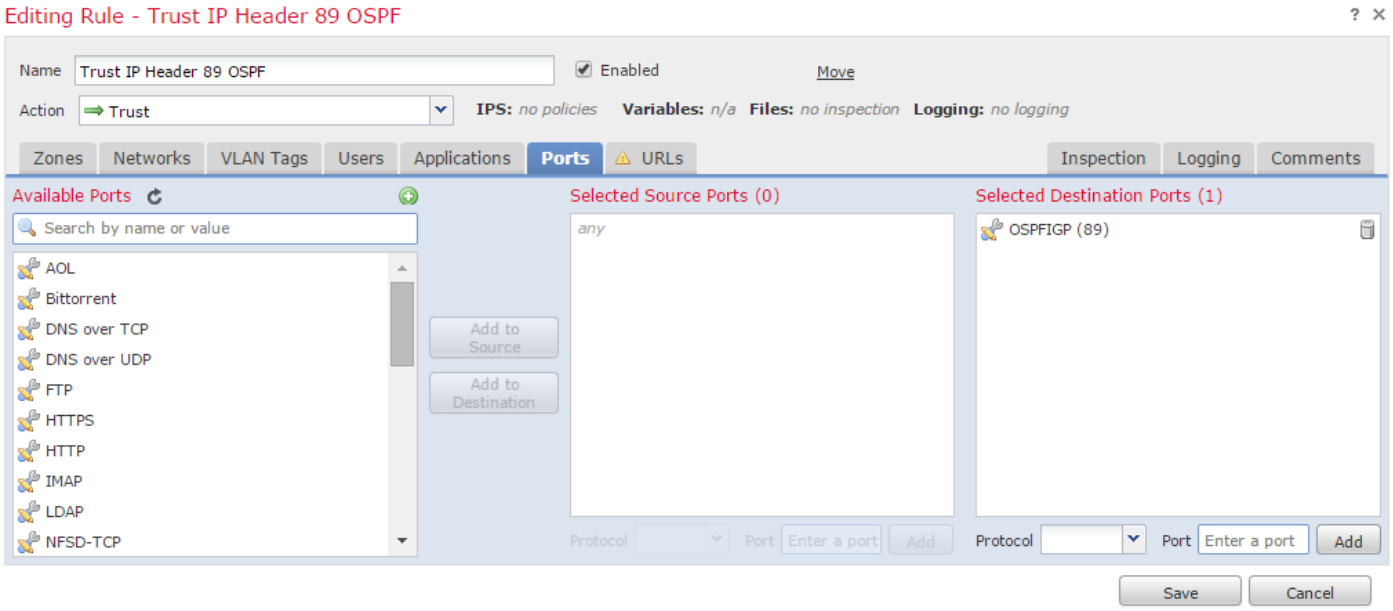
```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

Router B:

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

En FireSIGHT Management Center

1. Seleccione la política de control de acceso aplicada al dispositivo Firepower.
2. Cree una regla de control de acceso con una acción de **Confianza.**
3. En la pestaña **Ports**, seleccione OSPF en el protocolo 89.
4. Haga clic en **Agregar** para agregar el puerto al puerto de destino.
5. Guarde la regla de control de acceso.



Ejemplo de BGP

En el router

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
```

En FireSIGHT Management Center

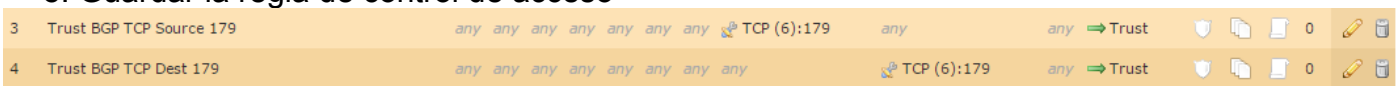
Nota: Debe crear dos entradas de control de acceso, ya que el puerto 179 puede ser el puerto de origen o de destino dependiendo del TCP SYN del altavoz BGP que establezca primero la sesión.

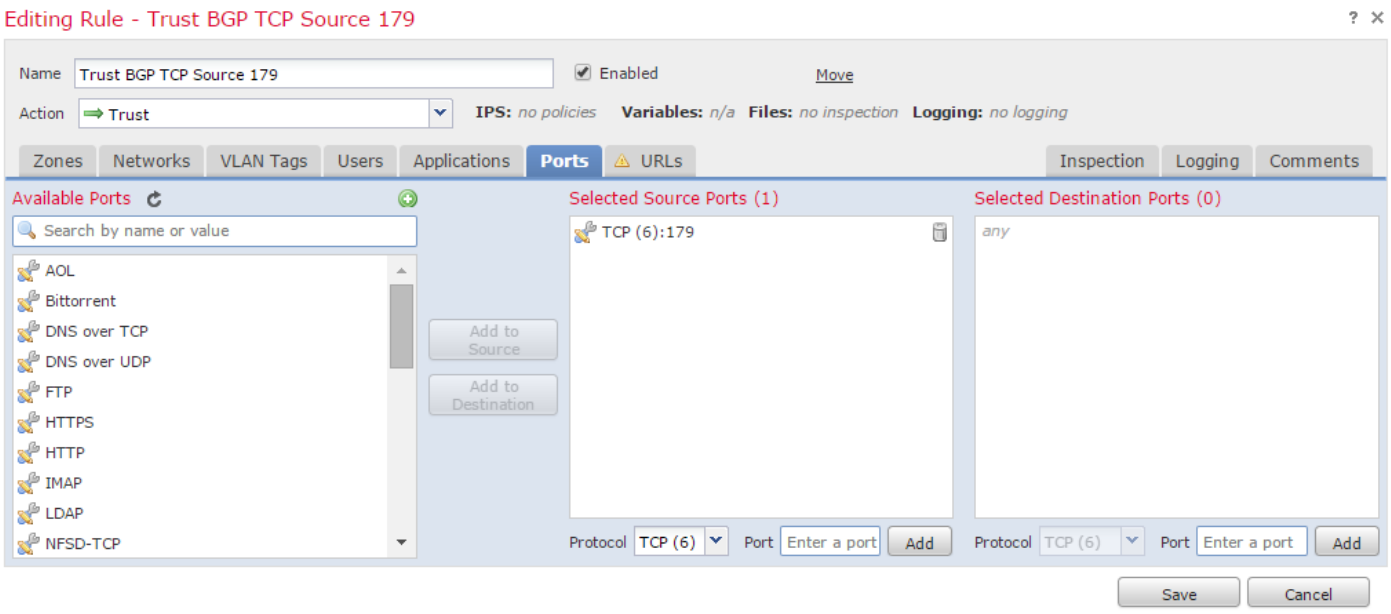
Regla 1:

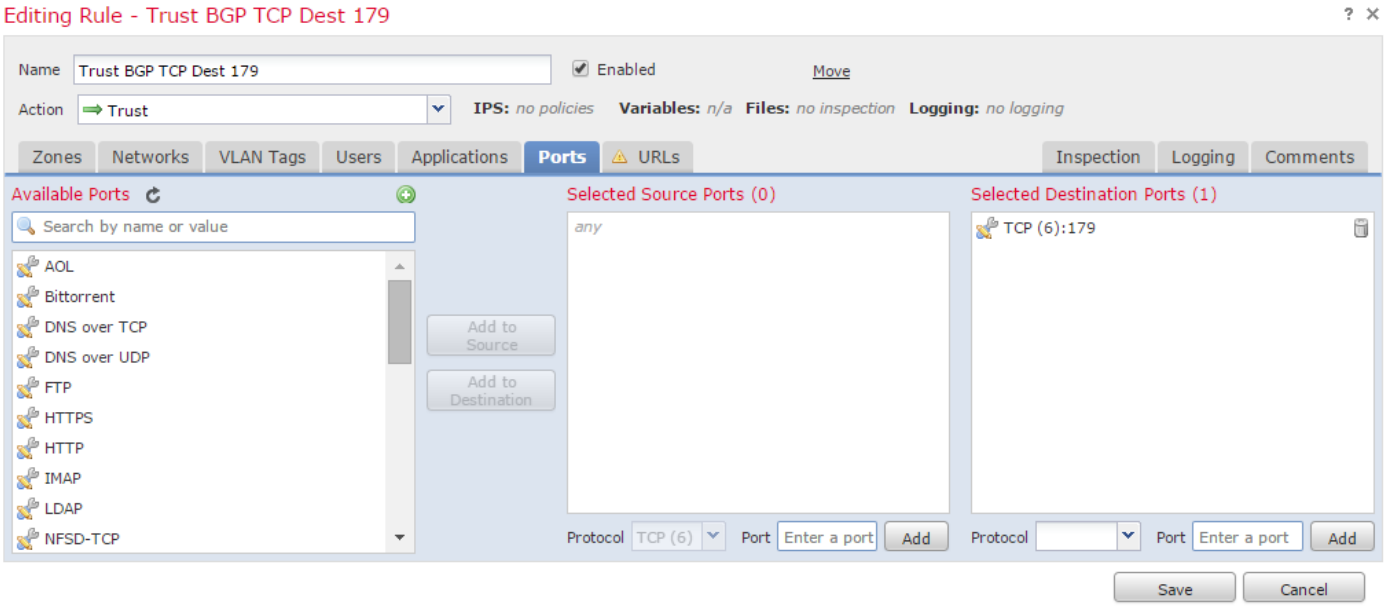
1. Seleccione la política de control de acceso aplicada al dispositivo Firepower.
2. Cree una regla de control de acceso con una acción de **Trust**.
3. Bajo la pestaña **Puertos**, seleccione **TCP(6)** e ingrese el **puerto 179**.
4. Haga clic en **Agregar** para agregar el puerto al **puerto de origen**.
5. Guarde la regla de control de acceso.

Regla 2:

1. Seleccione la política de control de acceso aplicada al dispositivo Firepower.
2. Cree una regla de control de acceso con una acción de **Trust**.
3. En la pestaña **Puertos**, **seleccione TCP(6)** e ingrese el **puerto 179**.
4. Haga clic en **Agregar** para agregar el puerto al **puerto de destino**.
5. Guardar la regla de control de acceso







Verificación

Para verificar que una regla **Trust** esté funcionando como se espera, capture los paquetes en el dispositivo Firepower. Si observa el tráfico EIGRP, OSPF o BGP en la captura de paquetes, entonces el tráfico no se confía como se esperaba.

> **Consejo:** Lea este documento para conocer los pasos para capturar el tráfico en los appliances Firepower.

A continuación, se incluyen algunos ejemplos:

EIGRP

Si la regla de confianza funciona como se espera, no debería ver el siguiente tráfico:

```
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

Si la regla de confianza funciona como se espera, no debería ver el siguiente tráfico:

```
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

Si la regla de confianza funciona como se espera, no debería ver el siguiente tráfico:

```
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
```

Nota: Los trayectos BGP sobre TCP y los keepalives no son tan frecuentes como los IGP. Suponiendo que no hay prefijos que actualizar o retirar, es posible que deba esperar un período de tiempo más largo para verificar que no está viendo tráfico en el puerto TCP/179.

Resolución de problemas

Si aún ve el tráfico del protocolo de ruteo, realice las siguientes tareas:

1. Verifique que la política de control de acceso se haya aplicado correctamente desde FireSIGHT Management Center al dispositivo Firepower. Para hacerlo, navegue a la página **System > Monitoring > Task Status**.

2. Verifique que la acción de regla sea **Trust** y no **Allow**.

3. Verifique que el registro no esté habilitado en la regla **Trust**.