Exclusión del EIGRP, del OSPF y de los mensajes BGP del examen de la intrusión de FirePOWER

Contenido

Introducción

Los Routing Protocol envían los mensajes Hello Messages y el Keepalives para intercambiar la información de ruteo y para asegurarse de que los vecinos son todavía accesibles. Bajo carga pesada, un dispositivo de Cisco FirePOWER puede retrasar un mensaje de keepalive (sin la caída de él) bastante tiempo para que un router declare a su vecino abajo. El documento le proporciona los pasos para crear una regla de la confianza para excluir el Keepalives y para controlar el tráfico del plano de un Routing Protocol. Permite a los dispositivos o a los servicios de FirePOWER para conmutar los paquetes del ingreso a la interfaz de egreso, sin el retardo del examen.

Prerequisites

Componentes Utilizados

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

- Centro de administración de FireSIGHT (FMC)
- Dispositivo de FirePOWER: 7000 Series, modelos de las 8000 Series

Note: La información sobre este documento fue creada de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier

comando.

Diagrama de la red

- El router A y el router B son capa 2 adyacente, y están inconscientes del dispositivo en línea de FirePOWER (etiquetado como IPS).
- Router A - 10.0.0.1/24
- Router B - 10.0.0.2/24

- Para cada protocolo Interior Gateway Protocols probado (EIGRP y OSPF), el Routing Protocol fue habilitado en la red 10.0.0.0/24.
- Cuando el BGP de prueba, e-BGP fue utilizado y las interfaces físicas directamente conectadas fueron utilizadas como la fuente de la actualización para los peeringes.

Configuración

Ejemplo del EIGRP

En el router

Router A:

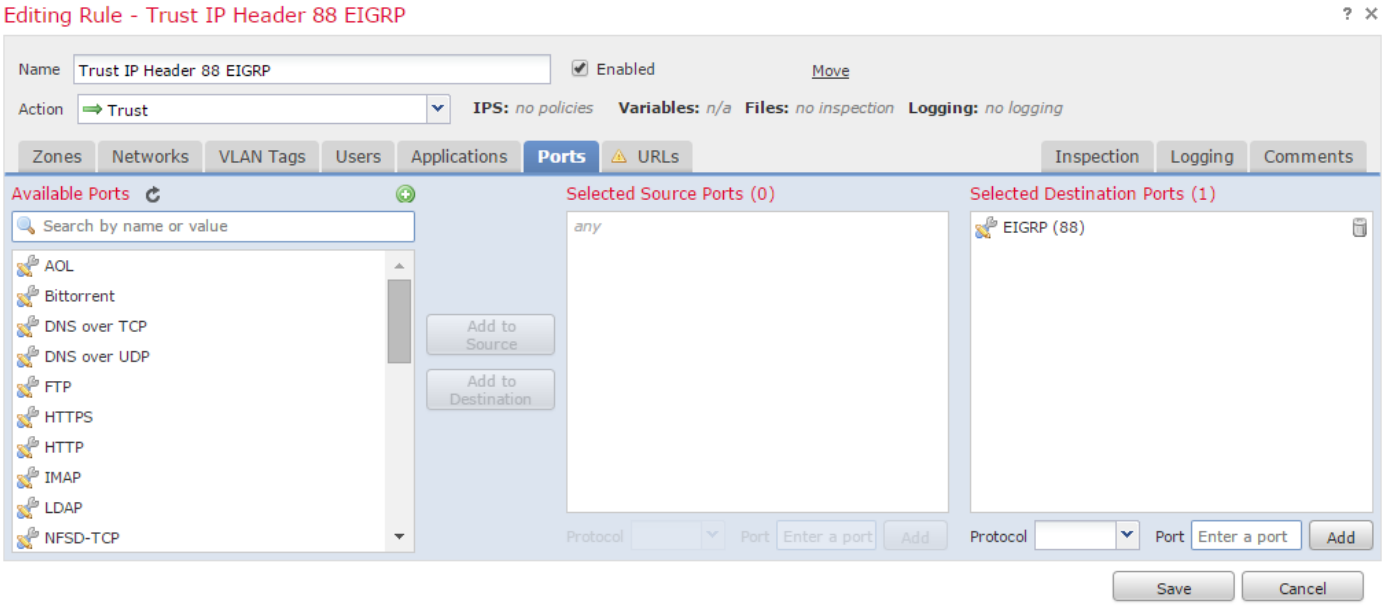
```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

Router B:

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

En el centro de administración de FireSIGHT

1. Seleccione la directiva del control de acceso aplicada al dispositivo de FirePOWER.
2. Cree una regla del control de acceso con una acción de la **confianza.**
3. Bajo los **puertos** tabule, seleccione el **EIGRP** bajo protocolo 88.
4. El tecleo **agrega** para agregar el puerto al puerto destino.
5. Salve la regla del control de acceso.



Ejemplo OSPF

En el router

Router A:

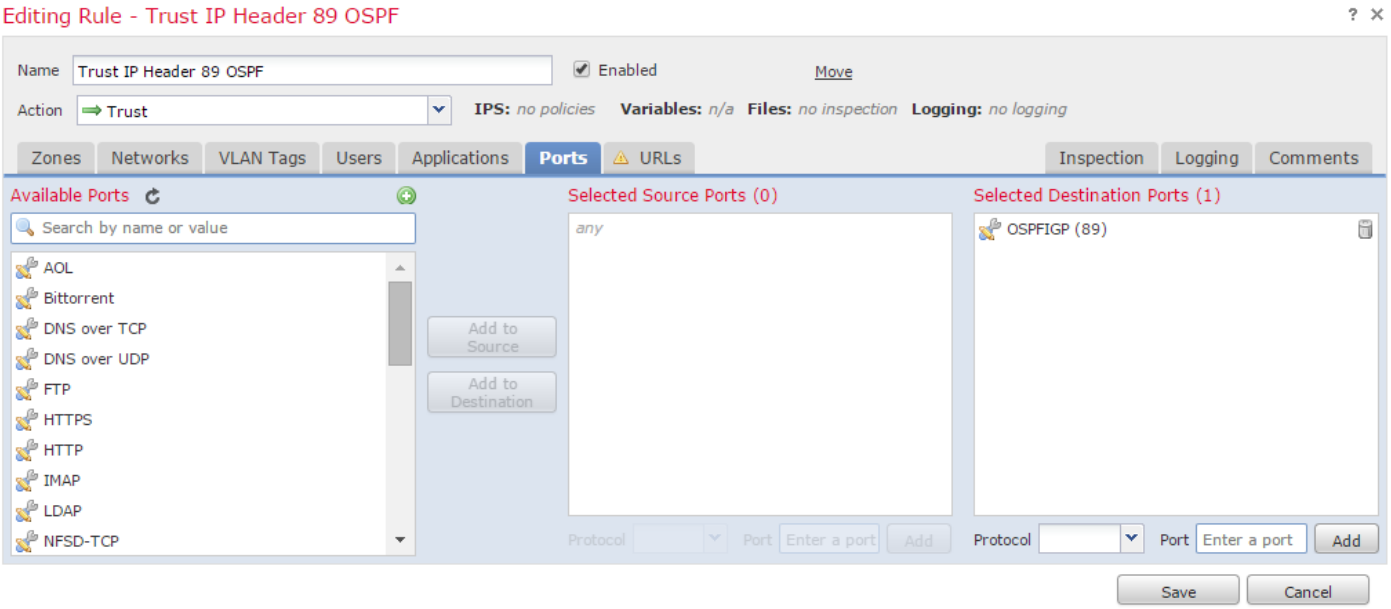
```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

Router B:

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

En el centro de administración de FireSIGHT

1. Seleccione la directiva del control de acceso aplicada al dispositivo de FirePOWER.
2. Cree una regla del control de acceso con una acción de la **confianza.**
3. Bajo los **puertos** tabule, seleccione el OSPF bajo protocolo 89.
4. El tecleo **agrega** para agregar el puerto al puerto destino.
5. Salve la regla del 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 el centro de administración de FireSIGHT

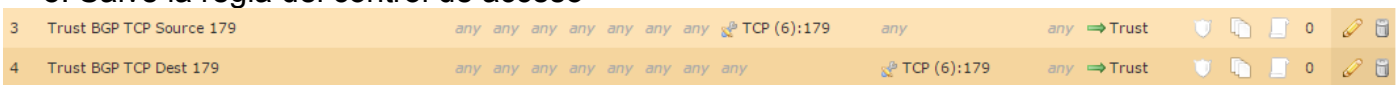
> **Note**: Usted debe crear dos entradas de control de acceso, pues el puerto 179 puede ser el puerto de origen o de destino dependiendo del cual el TCP del BGP de conversación SYN establece la sesión primero.

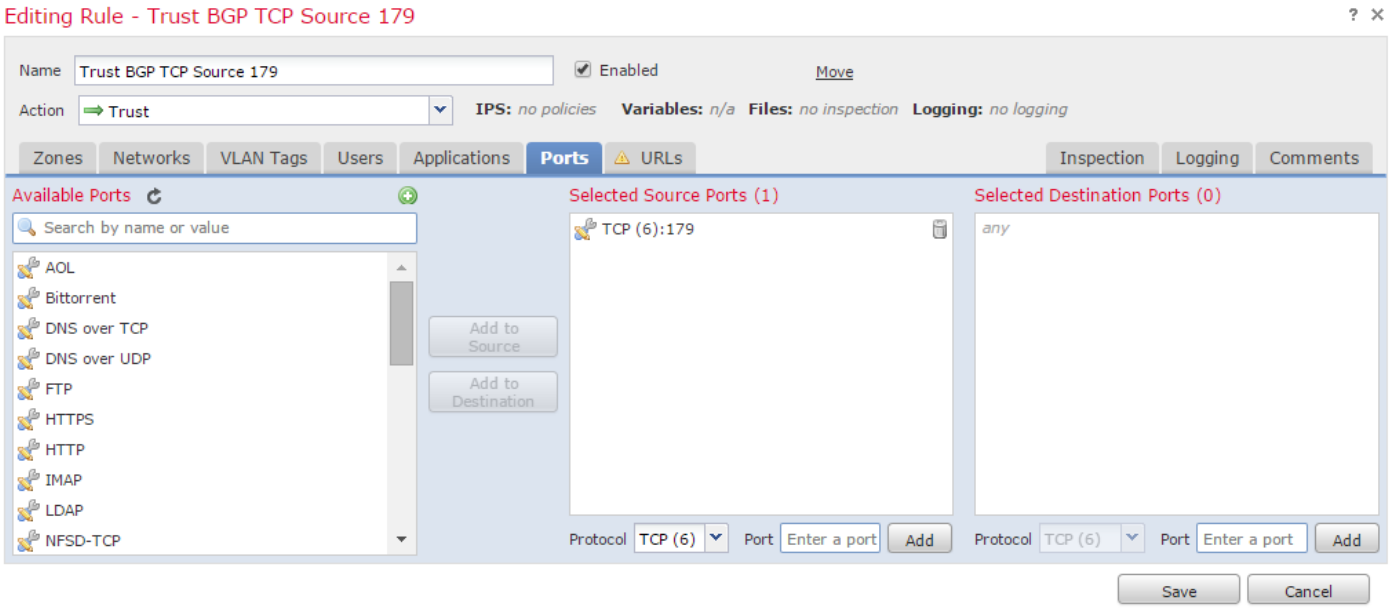
Regla 1:

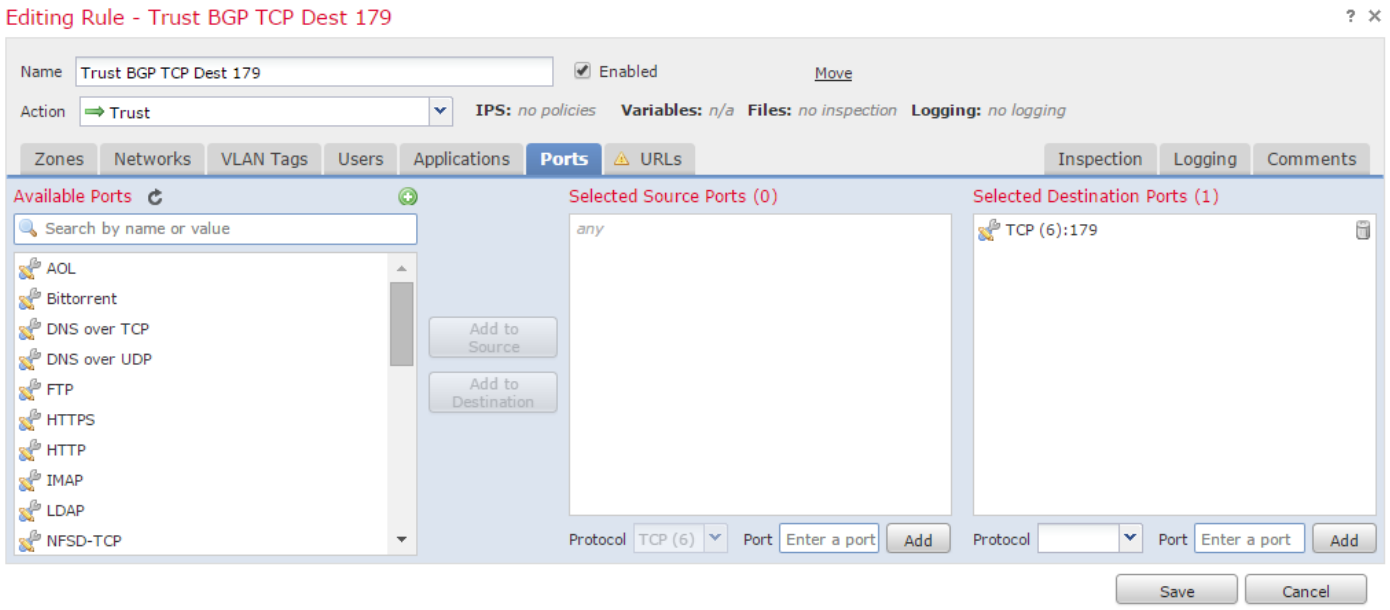
1. Seleccione la directiva del control de acceso aplicada al dispositivo de FirePOWER.
2. Cree una regla del control de acceso con una acción de la **confianza**.
3. Bajo los **puertos** tabule, seleccione **TCP(6)** y ingrese el **puerto 179**.
4. El tecleo **agrega** para agregar el puerto al **puerto de origen**.
5. Salve la regla del control de acceso.

Regla 2:

1. Seleccione la directiva del control de acceso aplicada al dispositivo de FirePOWER.
2. Cree una regla del control de acceso con una acción de la **confianza**.
3. Bajo los **puertos** tabule, **seleccione TCP(6)** y ingrese el **puerto 179**.
4. El tecleo **agrega** para agregar el puerto al **puerto destino**.
5. Salve la regla del control de acceso







Verificación

Para verificar que una regla de la **confianza** esté actuando como se esperaba, capture los paquetes en el dispositivo de FirePOWER. Si usted nota el tráfico del EIGRP, OSPF o BGP en la captura de paquetes, después el tráfico no se está confiando en como se esperaba.

> **Tip**: Leído para encontrar los pasos en cómo capturar el tráfico en los dispositivos de FirePOWER.

A continuación, se incluyen algunos ejemplos:

EIGRP

Si la regla de la confianza actúa como se esperaba, usted no debe ver el tráfico siguiente:

```
router bgp 65002
```

```
neighbor 10.0.0.1 remote-as 65001
```

OSPF

Si es la regla de la confianza actúa como se esperaba, usted considera el tráfico siguiente:

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

BGP

Si es la regla de la confianza actúa como se esperaba, usted considera el tráfico siguiente:

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

> **Note**: Los paseos BGP encima del TCP y el Keepalives no son tan frecuentes como los IGP. Están asumiendo allí ningún prefijo que se pondrá al día o retirado, usted puede necesitar esperar un período de tiempo más largo para verificarle no está viendo el tráfico en el puerto TCP/179.

Resolución de problemas

Si usted todavía ve el tráfico del Routing Protocol, realice por favor las tareas siguientes:

1. Verifique que la directiva del control de acceso fuera aplicada con éxito del centro de administración de FireSIGHT al dispositivo de FirePOWER. Para hacer eso, navegue a la página del **estatus del sistema > de la supervisión > de la tarea**.

2. Verifique que la acción de la regla sea **confianza** y **no permitir**.

3. Verifique que la registración no esté habilitada en la regla de la **confianza**.