Uitsluiting van EHBO-, OSPF- en BGP-berichten van de Inbraakinspectie van vuurkracht

Inhoud

Inleiding

Routing protocols verzenden hallo-berichten en keepalives om routing informatie uit te wisselen en om te verzekeren dat buren nog steeds bereikbaar zijn. Onder zware lading kan een Cisco FirePOWER-apparaat een blijvende bericht (zonder het te laten vallen) lang genoeg vertragen voor een router om zijn buurman te verklaren. Het document biedt u de stappen om een trustregel te maken om keepalives en het controle vliegtuigverkeer van een routeringsprotocol uit te sluiten. Hiermee kunnen de FirePOWER-apparaten of -diensten de pakketten van de ingangen naar de spanning-interface overschakelen zonder dat de inspectie wordt uitgesteld.

Voorwaarden

Gebruikte componenten

Bij de wijzigingen in het toegangscontrolebeleid voor dit document worden de volgende hardwareplatforms gebruikt:

- FireSIGHT Management Center (FMC)
- FirePOWER-apparaat: 7000 Series, 8000 Series modellen

> Opmerking: De informatie over dit document is gemaakt van de apparatuur in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdiagram

- De router A en router B zijn laag-2 naast elkaar en zijn niet op de hoogte van het inline Firepower apparaat (aangeduid als IPS).
- router A - 10.0.0.1/24
- router B - 10.0.0.2/24

- Voor elk getest Protocol van de Gateway van Binnenlandse Zaken (OSPF en OSPF) werd het routerprotocol op het 10.0.0.0/24 netwerk geactiveerd.
- Bij het testen van BGP werd e-BGP gebruikt en werden de direct aangesloten fysieke interfaces gebruikt als de update bron voor de peeringen.

Configuratie

DHCP-voorbeeld

Op router

router A:

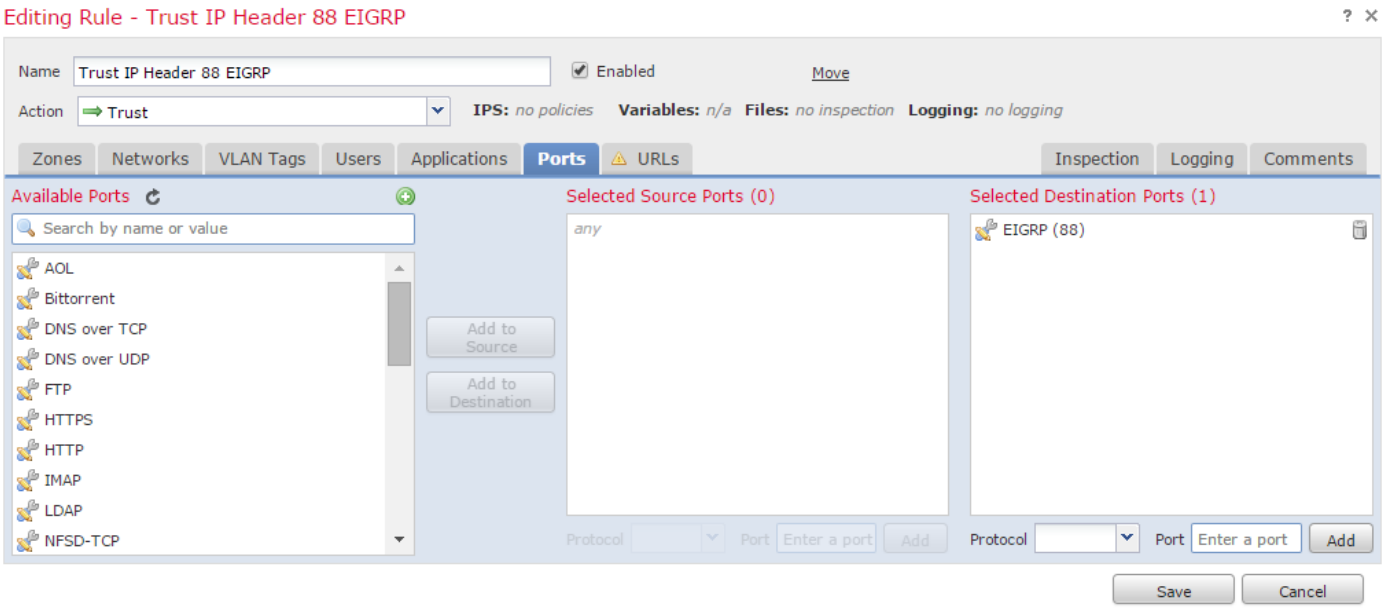
```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

router B:

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

Op FireSIGHT Management Center

1. Selecteer het Access Control Policy dat van toepassing is op het FirePOWER-apparaat.
2. Maak een toegangscontroleregel met een actie van **vertrouwen.**
3. Selecteer onder het tabblad **Ports** de optie **Ecu** onder protocol 88.
4. Klik op **Add** om de poort aan de doelpoort toe te voegen.
5. Bewaar de toegangscontroleregel.



OSPF-voorbeeld

Op router

router A:

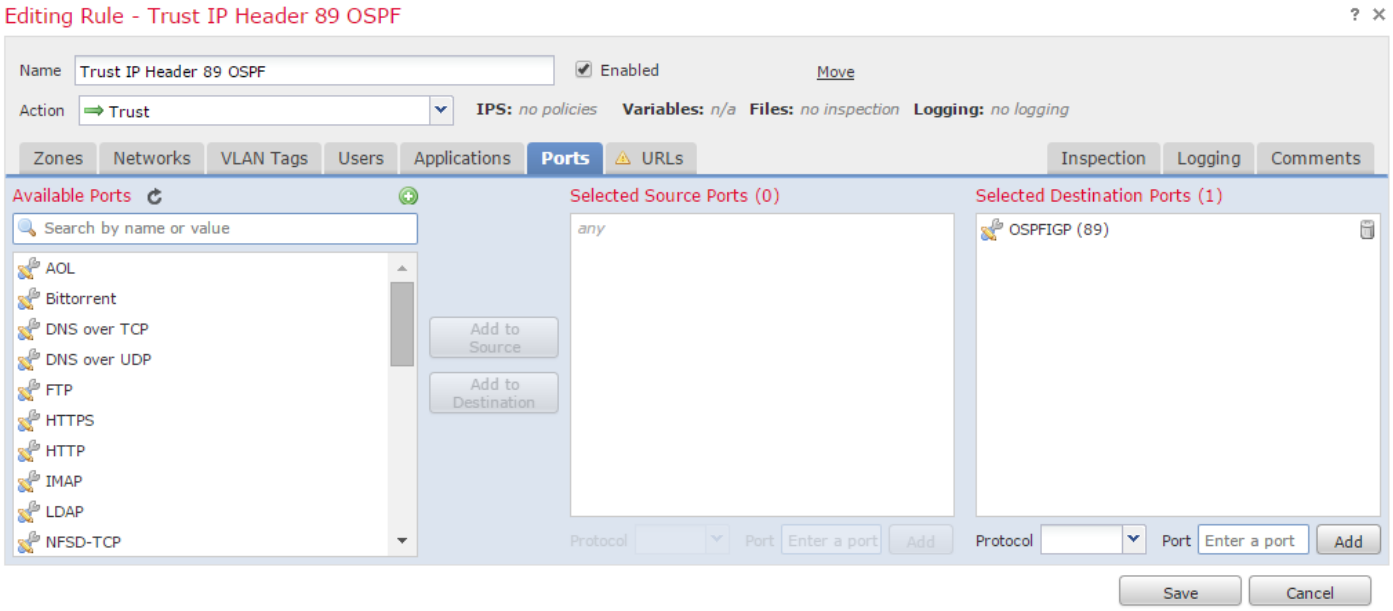
```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

router B:

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

Op FireSIGHT Management Center

1. Selecteer het Access Control Policy dat van toepassing is op het FirePOWER-apparaat.
2. Maak een toegangscontroleregel met een actie van **vertrouwen.**
3. Selecteer onder het tabblad **Ports** de optie OSPF onder protocol 89.
4. Klik op **Add** om de poort aan de doelpoort toe te voegen.
5. Bewaar de toegangscontroleregel.



BGP-voorbeeld

Op 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
```

Op FireSIGHT Management Center

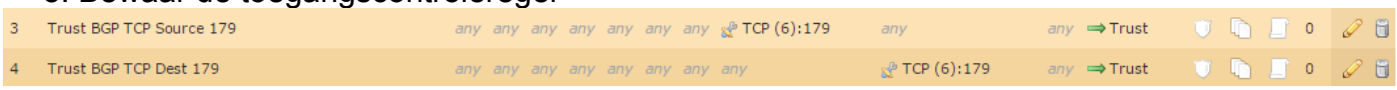
Opmerking: U moet twee toegangscontrole-ingangen maken, aangezien poort 179 de bron of de doelpoort kan zijn afhankelijk van welke TCP SYN van de spreker van BGP de sessie eerst vaststelt.

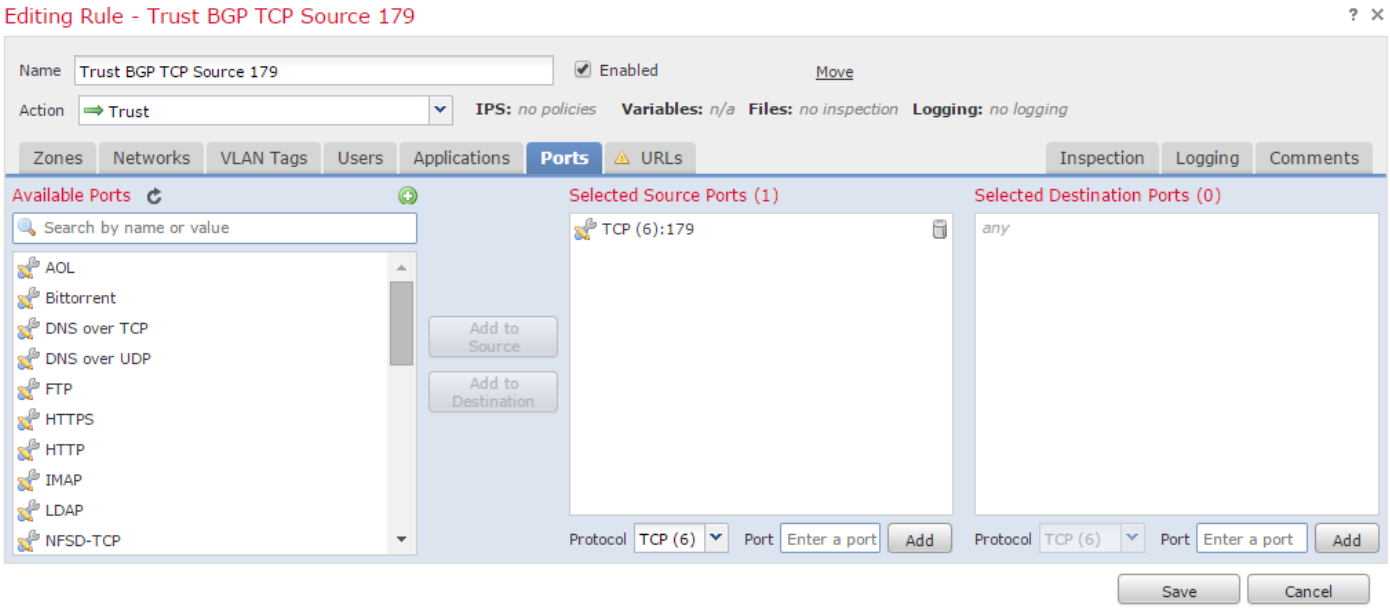
Regel 1:

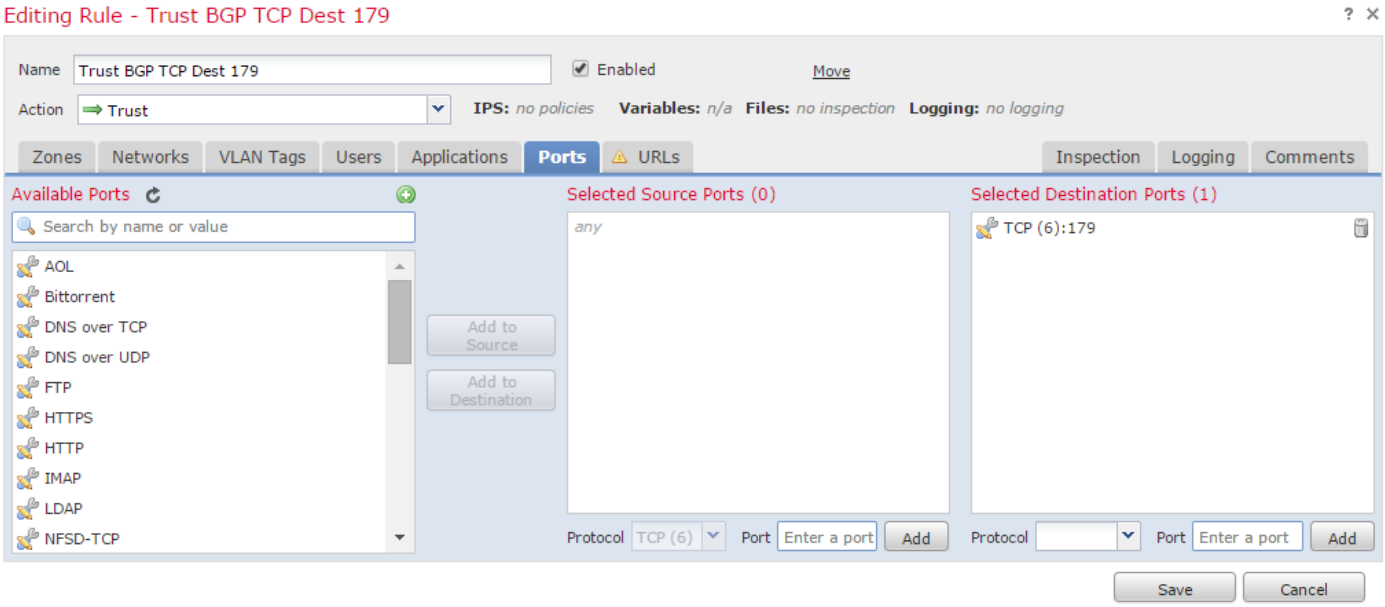
1. Selecteer het Access Control Policy dat van toepassing is op het FirePOWER-apparaat.
2. Maak een toegangscontroleregel met een actie van **vertrouwen**.
3. Selecteer onder het tabblad **Port** TCP(6) en voer **poort 179 in**.
4. Klik op **Add** om de poort aan de **bronpoort** toe te voegen.
5. Bewaar de toegangscontroleregel.

Artikel 2:

1. Selecteer het Access Control Policy dat van toepassing is op het FirePOWER-apparaat.
2. Maak een toegangscontroleregel met een actie van **vertrouwen**.
3. Onder het tabblad **Port** selecteert u **TCP(6)** en voert u **poort 179 in**.
4. Klik op **Add** om de poort aan de **doelpoort** toe te voegen.
5. Bewaar de toegangscontroleregel







Verificatie

Om te controleren of een **vertrouwensregel** volgens de verwachtingen werkt, neemt u pakketten op het FirePOWER-apparaat op. Als u het verkeer DHCP, OSPF of BGP in de pakketvastlegging opmerkt, dan wordt het verkeer niet vertrouwd zoals verwacht.

> **Tip**: Lees ook de stappen om verkeer op de FirePOWER-apparatuur op te nemen.

Hier zijn een paar voorbeelden:

EINDTIJD

Als de vertrouwensregel naar verwachting functioneert, dan ziet u het volgende verkeer niet:

```
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

Als de vertrouwensregel naar verwachting functioneert, dan ziet u het volgende verkeer niet:

```
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

Als de vertrouwensregel naar verwachting functioneert, dan ziet u het volgende verkeer niet:

```
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
```

> Opmerking: BGP-ritten boven TCP en keepalives zijn niet zo vaak als IGP's. Aangenomen

dat er geen prefixes zijn die moeten worden bijgewerkt of ingetrokken, kunt u een langere tijd moeten wachten om te controleren of u geen verkeer ziet op port TCP/179.

Probleemoplossing

Als u nog steeds het routingprotocol verkeer ziet, voert u de volgende taken uit:

1. Controleer of het toegangscontrolbeleid is toegepast via FireSIGHT Management Center op het FireSIGHT Management Center. Om dat te doen, navigeer dan naar het **System > Monitoring > Task Status-**pagina.

2. Controleer dat de regel actie **vertrouwen** is en niet **toestaan**.

3. Controleer dat houtkap niet op de regel **Vertrouwen** is ingeschakeld.