Contents

Introduction

Routing protocols send hello messages and keepalives to exchange routing information and ensure that neighbors are still reachable. Under heavy load, a Cisco Firepower appliance may delay a keepalive message (without dropping it) long enough for a router to declare its neighbor down. The document provides you the steps to create a Trust rule to exclude keepalives and control plane traffic of a routing protocol. It enables the Firepower appliances or services to switch packets from ingress to egress interface, without the delay of inspection.

Prerequisites

Components Used

The Access Control policy changes on this document use the following hardware platforms:

- FireSIGHT Management Center (FMC)
- Firepower appliance: 7000 series, 8000 series models

> **Note**: The information on this document was created from the devices in a specific lab environment. 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.

Network Diagram

- Router A and Router B are layer-2 adjacent, and are unaware of the inline Firepower appliance (labeled as ips).
- Router A - 10.0.0.1/24
- Router B - 10.0.0.2/24

- For each Interior Gateway Protocol tested (EIGRP and OSPF), the routing protocol was enabled on the 10.0.0.0/24 network.
- When testing BGP, e-BGP was used and the directly connected physical interfaces were utilized as the update source for the peerings.

Configuration

EIGRP Example

On Router

Router A:

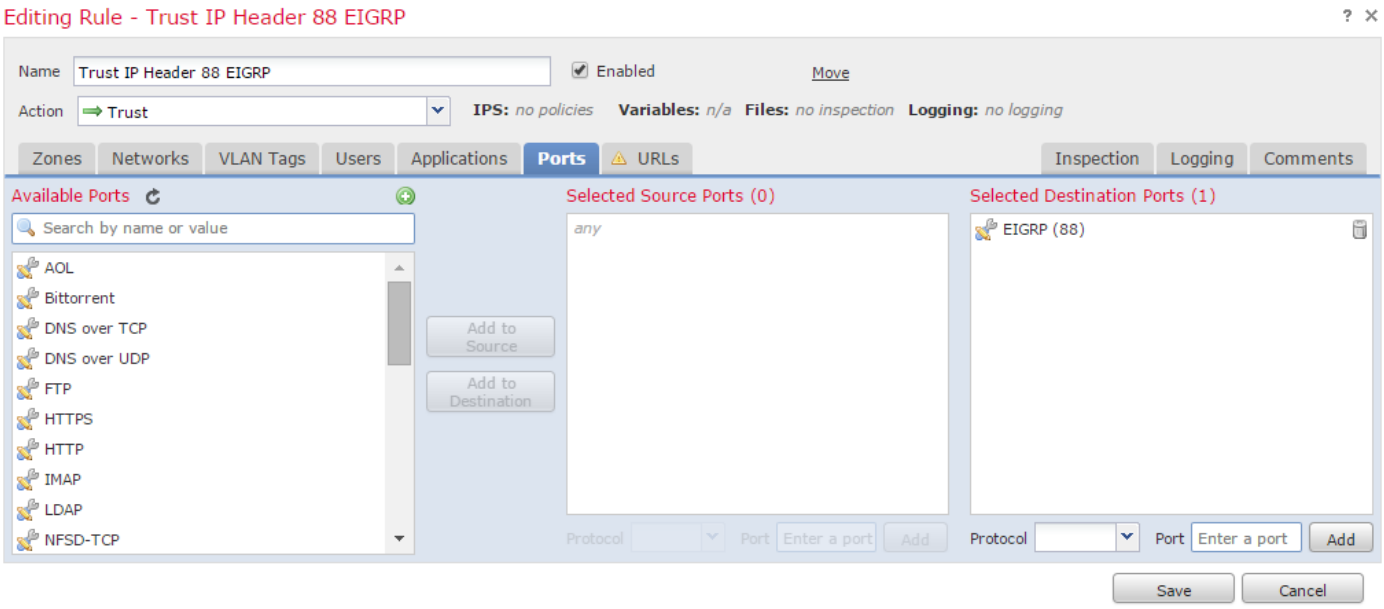
```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

Router B:

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

On FireSIGHT Management Center

1. Select the Access Control Policy applied to the Firepower appliance.
2. Create an Access Control rule with an action of **Trust.**
3. Under the **Ports** tab, select **EIGRP** under protocol 88.
4. Click **Add** to add the port to the destination port.
5. Save the access control rule.



OSPF Example

On Router

Router A:

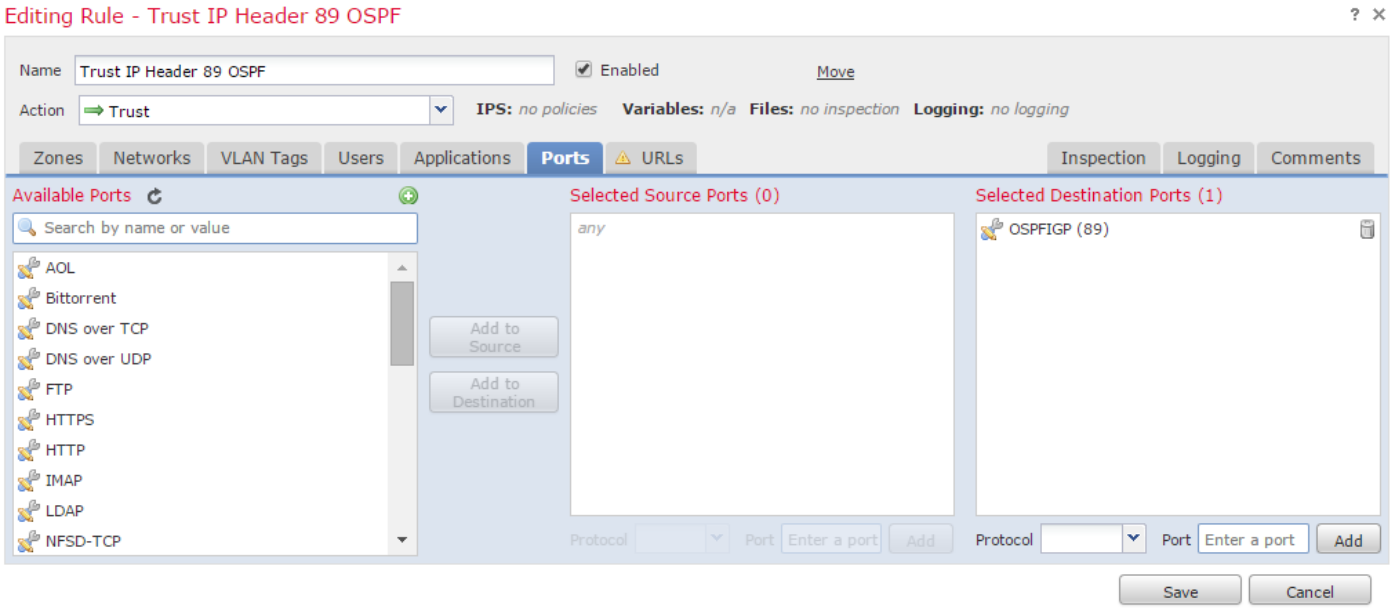
```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

Router B:

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

On FireSIGHT Management Center

1. Select the Access Control Policy applied to the Firepower appliance.
2. Create an Access Control rule with an action of **Trust.**
3. Under the **Ports** tab, select OSPF under protocol 89.
4. Click **Add** to add the port to the destination port.
5. Save the access control rule.



BGP Example

On 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
```

On FireSIGHT Management Center

> **Note**: You must create two access control entries, as port 179 may be the source or destination port depending on which BGP speaker's TCP SYN establishes the session first.

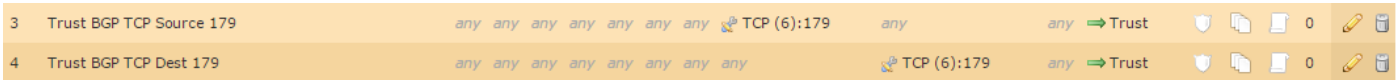
Rule 1:

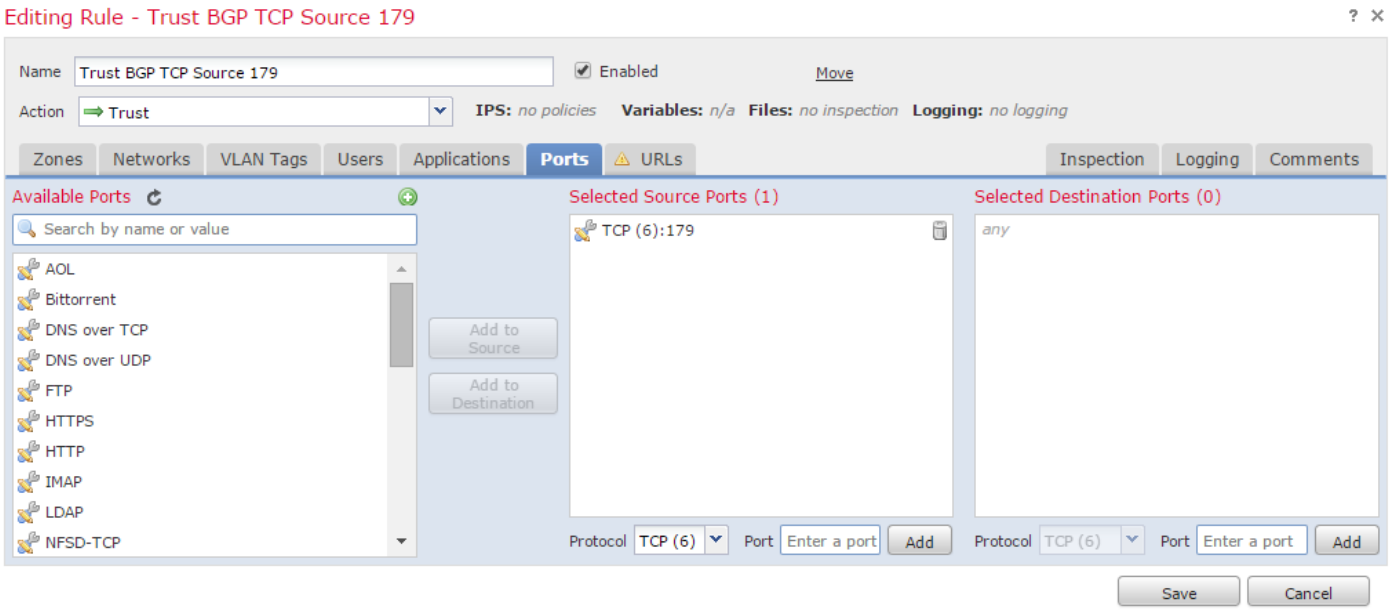
1. Select the Access Control Policy applied to the Firepower appliance.

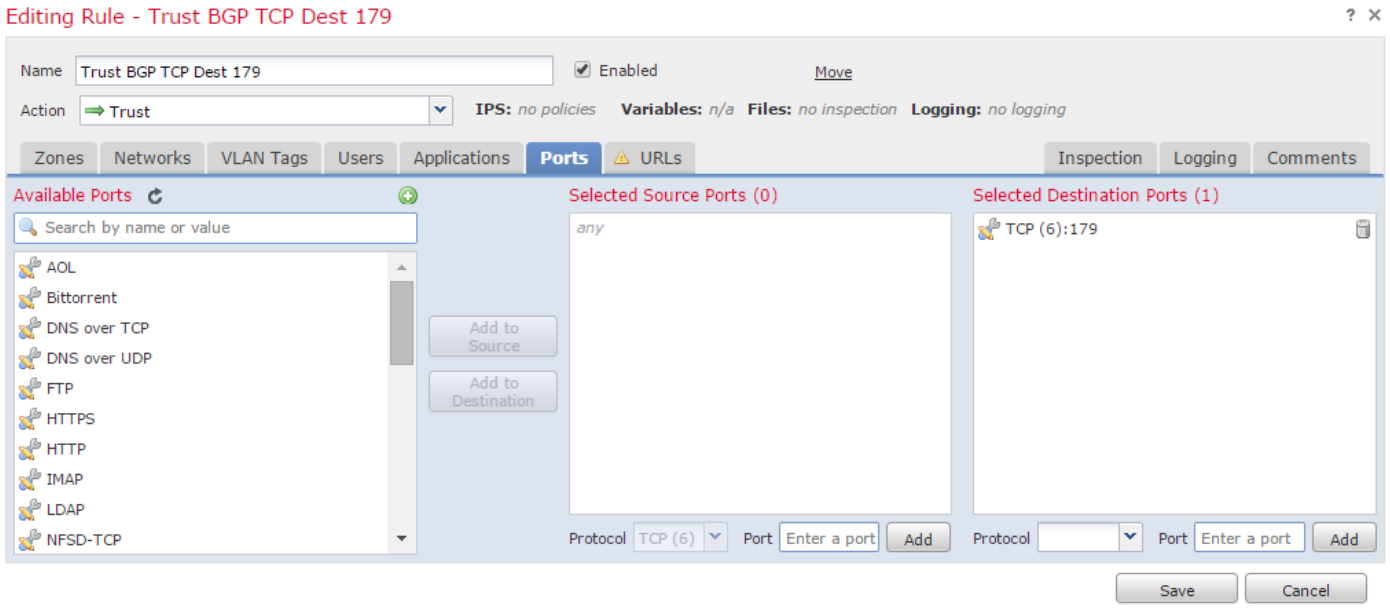
2. Create an Access Control rule with an action of **Trust**.
3. Under the **Ports** tab, select **TCP(6)** and enter **port 179**.
4. Click **Add** to add the port to the **source port**.
5. Save the access control rule.

Rule 2:

1. Select the Access Control Policy applied to the Firepower appliance.
2. Create an Access Control rule with an action of **Trust**.
3. Under the **Ports** tab, **select TCP(6)** and enter **port 179**.
4. Click **Add** to add the port to the **destination port**.
5. Save the access control rule







Verification

In order to verify that a **Trust** rule is operating as expected, capture packets on the Firepower appliance. If you notice the EIGRP, OSPF or BGP traffic in the packet capture, then the traffic is not being trusted as expected.

Tip: Read to find the steps on how to capture traffic on the Firepower appliances.

Here are some examples:

EIGRP

If the Trust rule operates as expected, you should not see the following traffic:

```
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

If the Trust rule is operates as expected, you should not see the following traffic:

```
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

If the Trust rule is operates as expected, you should not see the following traffic:

```
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**: BGP rides on top of TCP and keepalives are not as frequent as the IGPs. Assuming there are no prefixes to be updated or withdrawn, you may need to wait for a longer period of time to verify you are not seeing traffic on port TCP/179.

Troubleshooting

If you still see the routing protocol traffic, please perform the following tasks:

1. Verify that the Access Control Policy was successfully applied from the FireSIGHT Management Center to the Firepower appliance. In order to do that, navigate to the **System > Monitoring > Task Status** page.

2. Verify that the rule action is **Trust** and not **Allow**.

3. Verify that logging is not enabled on the **Trust** rule.