

Ausschluss von EIGRP-, OSPF- und BGP-Nachrichten aus der FirePOWER Intrusion Inspection

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm](#)

[Konfiguration](#)

[EIGRP-Beispiel](#)

[OSPF-Beispiel](#)

[BGP-Beispiel](#)

[Überprüfung](#)

[EIGRP](#)

[OSPF](#)

[BGP](#)

[Fehlerbehebung](#)

Einführung

Routingprotokolle senden Hello-Nachrichten und Keepalives, um Routing-Informationen auszutauschen und sicherzustellen, dass Nachbarn immer noch erreichbar sind. Bei starker Auslastung verzögert eine Cisco FirePOWER-Appliance möglicherweise eine Keepalive-Nachricht (ohne diese zu verwerfen), sodass ein Router den Nachbarn als ausgefallen deklarieren kann. In diesem Dokument werden die Schritte zum Erstellen einer Vertrauensregel beschrieben, um Keepalives und Kontrollebenen-Datenverkehr eines Routing-Protokolls auszuschließen. Sie ermöglicht den FirePOWER-Appliances oder -Services, Pakete ohne Verzögerung von der Eingangs- zur Ausgangsschnittstelle zu übertragen.

Voraussetzungen

Verwendete Komponenten

Bei den Änderungen der Zugriffskontrollrichtlinien für dieses Dokument werden die folgenden Hardwareplattformen verwendet:

- FireSIGHT Management Center (FMC)
- FirePOWER-Appliance: Modelle der Serie 7000 und 8000

Hinweis: Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

- Router A und Router B sind an Layer 2 angrenzend und kennen die Inline-FirePOWER-Appliance (als IP bezeichnet) nicht.
- Router A - 10.0.0.1/24
- Router B - 10.0.0.2/24



- Für jedes getestete Interior Gateway Protocol (EIGRP und OSPF) wurde das Routing-Protokoll im Netzwerk 10.0.0.0/24 aktiviert.
- Beim BGP-Test wurden e-BGP und die direkt verbundenen physischen Schnittstellen als Aktualisierungsquelle für die Peerings verwendet.

Konfiguration

EIGRP-Beispiel

Router

Router A:

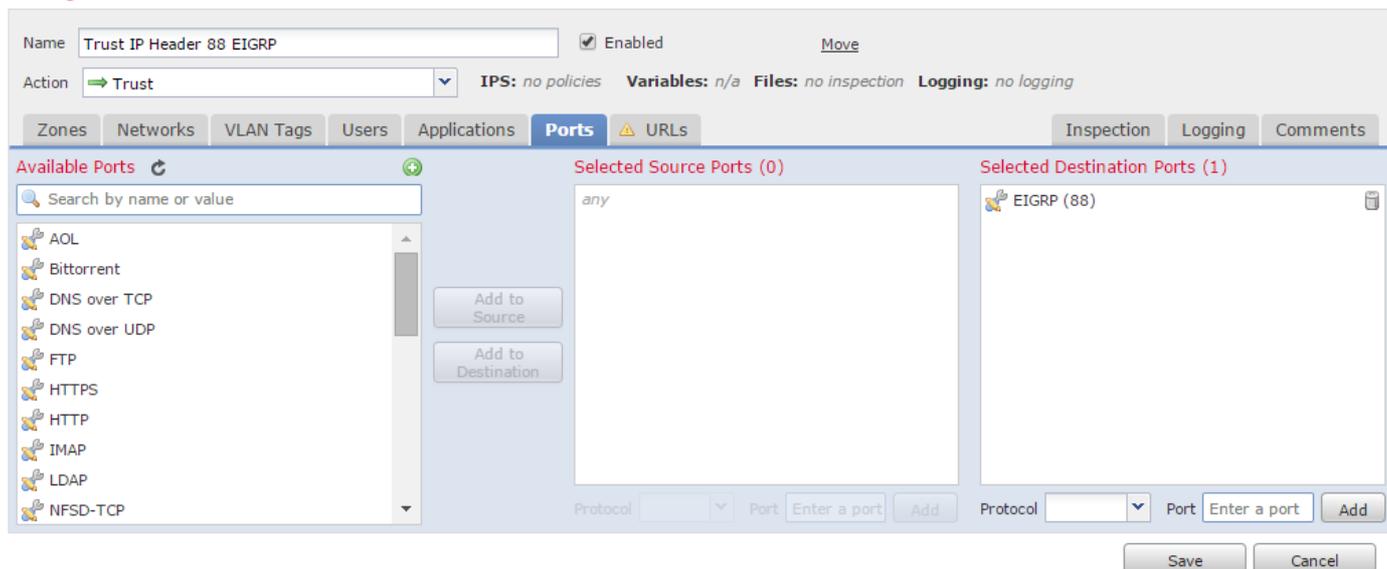
```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

Router B:

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

Im FireSIGHT Management Center

1. Wählen Sie die auf die FirePOWER-Appliance angewendete Zugriffskontrollrichtlinie aus.
2. Erstellen Sie eine Zugriffskontrollregel mit einer Aktion von **Trust**.
3. Wählen Sie auf der Registerkarte **Ports** unter Protokoll 88 **EIGRP** aus.
4. Klicken Sie auf **Hinzufügen**, um den Port dem Zielport hinzuzufügen.
5. Speichern Sie die Zugriffskontrollregel.



OSPF-Beispiel

Router

Router A:

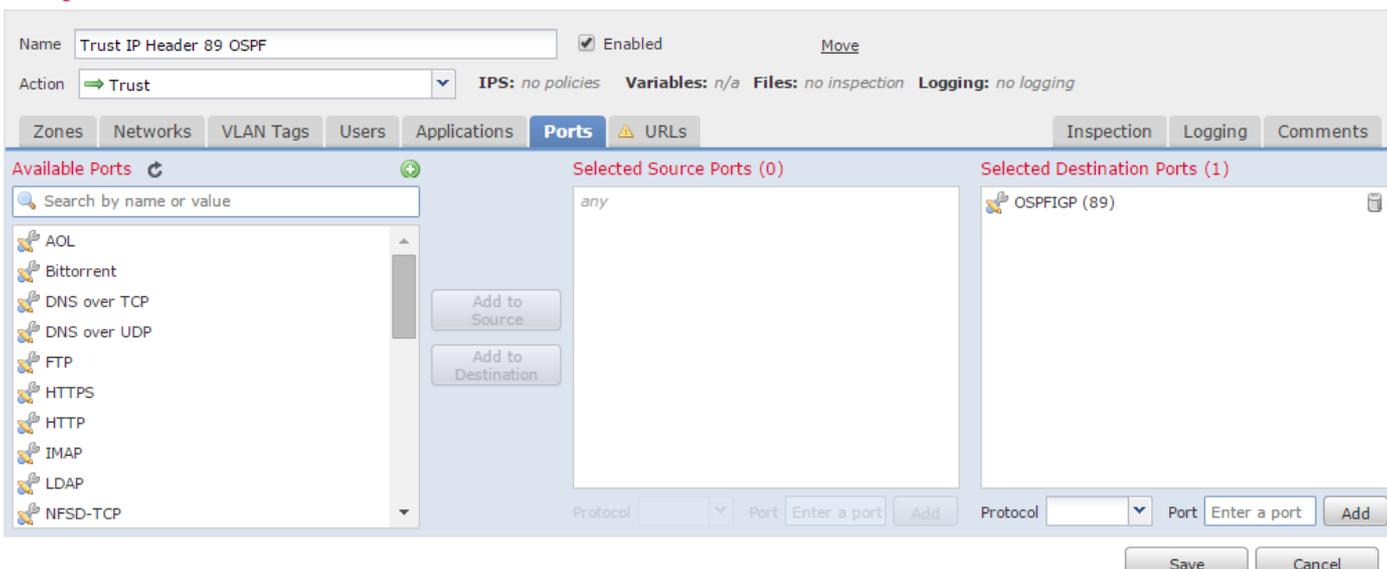
```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

Router B:

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

Im FireSIGHT Management Center

1. Wählen Sie die auf die FirePOWER-Appliance angewendete Zugriffskontrollrichtlinie aus.
2. Erstellen Sie eine Zugriffskontrollregel mit einer Aktion von **Trust**.
3. Wählen Sie auf der Registerkarte **Ports** unter Protokoll 89 die Option OSPF aus.
4. Klicken Sie auf **Hinzufügen**, um den Port dem Zielport hinzuzufügen.
5. Speichern Sie die Zugriffskontrollregel.



BGP-Beispiel

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
```

Im FireSIGHT Management Center

Hinweis: Sie müssen zwei Zugriffskontrolleinträge erstellen, da Port 179 der Quell- oder Zielport sein kann, je nachdem, welches TCP-SYN des BGP-Sprechers die Sitzung zuerst erstellt.

Regel 1:

1. Wählen Sie die auf die FirePOWER-Appliance angewendete Zugriffskontrollrichtlinie aus.
2. Erstellen Sie eine Zugriffskontrollregel mit einer Aktion von **Trust**.
3. Wählen Sie auf der Registerkarte **Ports** die Option **TCP(6)** aus, und geben Sie **Port 179 ein**.
4. Klicken Sie auf **Hinzufügen**, um den Port dem **Quellport** hinzuzufügen.
5. Speichern Sie die Zugriffskontrollregel.

Regel 2:

1. Wählen Sie die auf die FirePOWER-Appliance angewendete Zugriffskontrollrichtlinie aus.
2. Erstellen Sie eine Zugriffskontrollregel mit einer Aktion von **Trust**.
3. Wählen Sie auf der Registerkarte **Ports** **TCP(6)** aus, und geben Sie **Port 179 ein**.
4. Klicken Sie auf **Hinzufügen**, um den Port dem **Zielport** hinzuzufügen.
5. Speichern der Zugriffskontrollregel

3	Trust BGP TCP Source 179	any any any any any any any any	TCP (6):179	any	any → Trust	   0	 
4	Trust BGP TCP Dest 179	any any any any any any any any		TCP (6):179	any → Trust	   0	 

Name: Trust BGP TCP Source 179 Enabled [Move](#)

Action: Trust **IPS:** no policies **Variables:** n/a **Files:** no inspection **Logging:** no logging

Zones Networks VLAN Tags Users Applications **Ports** URLs Inspection Logging Comments

Available Ports

- AOL
- Bittorrent
- DNS over TCP
- DNS over UDP
- FTP
- HTTPS
- HTTP
- IMAP
- LDAP
- NFSD-TCP

Add to Source Add to Destination

Selected Source Ports (1): TCP (6):179

Selected Destination Ports (0): any

Protocol TCP (6) Port Enter a port Add Protocol TCP (6) Port Enter a port Add

Save Cancel

Name: Trust BGP TCP Dest 179 Enabled [Move](#)

Action: Trust **IPS:** no policies **Variables:** n/a **Files:** no inspection **Logging:** no logging

Zones Networks VLAN Tags Users Applications **Ports** URLs Inspection Logging Comments

Available Ports

- AOL
- Bittorrent
- DNS over TCP
- DNS over UDP
- FTP
- HTTPS
- HTTP
- IMAP
- LDAP
- NFSD-TCP

Add to Source Add to Destination

Selected Source Ports (0): any

Selected Destination Ports (1): TCP (6):179

Protocol TCP (6) Port Enter a port Add Protocol Port Enter a port Add

Save Cancel

Überprüfung

Um zu überprüfen, ob eine **Trust**-Regel wie erwartet funktioniert, erfassen Sie Pakete auf der FirePOWER-Appliance. Wenn Sie bei der Paketerfassung den EIGRP-, OSPF- oder BGP-Datenverkehr feststellen, wird der Datenverkehr nicht wie erwartet vertrauenswürdig.

Tipp: In diesem Dokument finden Sie die Schritte zur Erfassung des Datenverkehrs auf den FirePOWER-Appliances.

Hier einige Beispiele:

EIGRP

Wenn die Vertrauensregel wie erwartet funktioniert, sollte der folgende Datenverkehr nicht angezeigt werden:

```
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

Wenn die Vertrauensregel wie erwartet ausgeführt wird, sollte der folgende Datenverkehr nicht angezeigt werden:

```
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

Wenn die Vertrauensregel wie erwartet ausgeführt wird, sollte der folgende Datenverkehr nicht angezeigt werden:

```
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
```

Hinweis: BGP-Fahrten über TCP und Keepalives sind nicht so häufig wie IGP. Wenn keine Präfixe aktualisiert oder zurückgezogen werden müssen, müssen Sie möglicherweise eine längere Zeit warten, um sicherzustellen, dass Sie auf dem TCP/179 keinen Datenverkehr sehen.

Fehlerbehebung

Wenn der Routing-Protokoll-Datenverkehr weiterhin angezeigt wird, führen Sie die folgenden Schritte aus:

1. Überprüfen Sie, ob die Zugriffskontrollrichtlinie vom FireSIGHT Management Center erfolgreich auf die FirePOWER-Appliance angewendet wurde. Navigieren Sie dazu zur Seite **System > Monitoring > Task Status (System > Überwachung > Aufgabenstatus)**.
2. Stellen Sie sicher, dass die Regelaktion **vertrauenswürdig** und nicht **zugelassen** ist.
3. Vergewissern Sie sich, dass die Protokollierung für die **Trust**-Regel nicht aktiviert ist.