

# Esclusione dei messaggi EIGRP, OSPF e BGP dalla funzione Firepower Intrusion Inspection

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Configurazione](#)

[Esempio di EIGRP](#)

[Esempio OSPF](#)

[Esempio di BGP](#)

[Verifica](#)

[EIGRP](#)

[OSPF](#)

[BGP](#)

[Risoluzione dei problemi](#)

## Introduzione

I protocolli di routing inviano messaggi di saluto e pacchetti keepalive per scambiare informazioni di routing e garantire che i vicini siano ancora raggiungibili. In condizioni di carico elevato, un accessorio Cisco Firepower può ritardare un messaggio keepalive (senza lasciarlo cadere) per un tempo sufficiente a consentire al router di dichiarare il proprio router adiacente come non attivo. Nel documento viene descritto come creare una regola di trust per escludere i pacchetti keepalive e controllare il traffico del piano di routing. Consente alle appliance o ai servizi Firepower di commutare i pacchetti dall'interfaccia in entrata all'interfaccia in uscita, senza ritardi nell'ispezione.

## Prerequisiti

### Componenti usati

Le modifiche apportate ai criteri di controllo di accesso in questo documento utilizzano le seguenti piattaforme hardware:

- Centro di gestione FireSIGHT (FMC)
- Appliance Firepower: serie 7000, modelli serie 8000

**Nota:** Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Esempio di rete

- Il router A e il router B sono adiacenti al layer 2 e non sono a conoscenza dell'appliance Firepower in linea (etichettata come ips).
- Router A - 10.0.0.1/24
- Router B - 10.0.0.2/24



- Per ciascun protocollo gateway interno testato (EIGRP e OSPF), il protocollo di routing è stato abilitato sulla rete 10.0.0.0/24.
- Durante il test di BGP, è stato utilizzato e-BGP e le interfacce fisiche direttamente connesse sono state utilizzate come origine di aggiornamento per i peer.

## Configurazione

### Esempio di EIGRP

#### Su 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
```

#### Su FireSIGHT Management Center

1. Selezionare i criteri di controllo dell'accesso applicati all'accessorio Firepower.
2. Creare una regola di controllo d'accesso con un'azione **Attendibile**.
3. Nella scheda **Porte**, selezionare **EIGRP** sotto il protocollo 88.
4. Fare clic su **Add** (Aggiungi) per aggiungere la porta alla porta di destinazione.
5. Salvare la regola di controllo d'accesso.

Editing Rule - Trust IP Header 88 EIGRP

The screenshot shows the 'Editing Rule' interface for a rule named 'Trust IP Header 88 EIGRP'. The rule is enabled and has an action of 'Trust'. The 'Ports' tab is selected, showing a list of available ports on the left and two selected destination ports on the right: 'EIGRP (88)'. The interface includes tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', and 'URLs'. At the bottom, there are 'Save' and 'Cancel' buttons.

## Esempio OSPF

### Su 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
```

### Su FireSIGHT Management Center

1. Selezionare i criteri di controllo dell'accesso applicati all'accessorio Firepower.
2. Creare una regola di controllo d'accesso con un'azione **Attendibile**.
3. Nella scheda **Porte**, selezionare OSPF sotto il protocollo 89.
4. Fare clic su **Add** (Aggiungi) per aggiungere la porta alla porta di destinazione.
5. Salvare la regola di controllo d'accesso.

Editing Rule - Trust IP Header 89 OSPF

The screenshot shows the 'Editing Rule' interface for a rule named 'Trust IP Header 89 OSPF'. The rule is enabled and has an action of 'Trust'. The 'Ports' tab is selected, showing 'Available Ports' on the left, 'Selected Source Ports (0)' in the middle, and 'Selected Destination Ports (1)' on the right. The destination port is 'OSPF (89)'. The interface includes search bars, 'Add to Source' and 'Add to Destination' buttons, and 'Save' and 'Cancel' buttons at the bottom.

## Esempio di BGP

### Su 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
```

### Su FireSIGHT Management Center

**Nota:** È necessario creare due voci di controllo dell'accesso, poiché la porta 179 può essere la porta di origine o di destinazione, a seconda della porta TCP SYN dell'altoparlante BGP che stabilisce per prima la sessione.

## Regola 1:

1. Selezionare i criteri di controllo dell'accesso applicati all'accessorio Firepower.
2. Creare una regola di controllo d'accesso con un'azione **Trust**.
3. Nella scheda **Porte**, selezionare **TCP(6)** e immettere la **porta 179**.
4. Fare clic su **Add** (Aggiungi) per aggiungere la porta alla **porta di origine**.
5. Salvare la regola di controllo d'accesso.

## Regola 2:

1. Selezionare i criteri di controllo dell'accesso applicati all'accessorio Firepower.
2. Creare una regola di controllo d'accesso con un'azione **Trust**.
3. Nella scheda **Porte**, **selezionare TCP(6)** e immettere la **porta 179**.
4. Fare clic su **Add** (Aggiungi) per aggiungere la porta alla **porta di destinazione**.
5. Salva la regola di controllo di accesso

|   |                          |                                 |             |             |     |       |  |  |   |  |
|---|--------------------------|---------------------------------|-------------|-------------|-----|-------|--|--|---|--|
| 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 |  |

### Editing Rule - Trust BGP TCP Source 179

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  Search by name or value

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

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

## Verifica

Per verificare che una regola **Trust** funzioni come previsto, acquisire i pacchetti sull'accessorio Firepower. Se si nota il traffico EIGRP, OSPF o BGP nell'acquisizione del pacchetto, il traffico non viene considerato attendibile come previsto.

**Suggerimento:** Leggere la procedura per acquisire il traffico sugli accessori Firepower.

Seguono alcuni esempi:

### EIGRP

Se la regola di attendibilità funziona come previsto, il traffico seguente non dovrebbe essere visualizzato:

```
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

Se la regola di attendibilità funziona come previsto, il traffico seguente non dovrebbe essere visualizzato:

```
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

Se la regola di attendibilità funziona come previsto, il traffico seguente non dovrebbe essere visualizzato:

```
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:** Le corse BGP su TCP e keepalive non sono così frequenti come le IGP. Supponendo che non vi siano prefissi da aggiornare o ritirare, potrebbe essere necessario attendere un periodo di tempo più lungo per verificare che il traffico sulla porta TCP/179 non sia visibile.

## Risoluzione dei problemi

Se il traffico del protocollo di routing è ancora visibile, eseguire i task seguenti:

1. Verificare che i criteri di controllo dell'accesso siano stati applicati correttamente dal centro di gestione FireSIGHT all'accessorio Firepower. A tale scopo, passare alla pagina **Sistema > Monitoraggio > Stato task**.
2. Verificare che l'azione della regola sia **Trust** e non **Allow** (Consenti).
3. Verificare che la registrazione non sia abilitata nella regola **Trust**.