

Exclusion des messages EIGRP, OSPF et BGP de l'inspection des intrusions Firepower

Contenu

[Introduction](#)

[Conditions préalables](#)

[Components Used](#)

[Diagramme du réseau](#)

[Configuration](#)

[Exemple EIGRP](#)

[Exemple OSPF](#)

[Exemple BGP](#)

[Vérification](#)

[EIGRP](#)

[OSPF](#)

[BGP](#)

[Dépannage](#)

Introduction

Les protocoles de routage envoient des messages Hello et des messages de test d'activité pour échanger des informations de routage et s'assurer que les voisins sont toujours accessibles. Sous charge élevée, un appareil Cisco Firepower peut retarder un message keepalive (sans le supprimer) suffisamment longtemps pour qu'un routeur déclare son voisin hors service. Le document vous indique les étapes à suivre pour créer une règle d'approbation afin d'exclure les keepalives et le trafic du plan de contrôle d'un protocole de routage. Il permet aux appliances ou services Firepower de commuter les paquets d'une interface d'entrée à une interface de sortie, sans délai d'inspection.

Conditions préalables

Components Used

Les modifications apportées à la stratégie de contrôle d'accès sur ce document utilisent les plateformes matérielles suivantes :

- FireSIGHT Management Center (FMC)
- Appareil Firepower : Modèles des gammes 7000 et 8000

Note: Les informations de ce document ont été créées à partir des périphériques d'un environnement de travaux pratiques spécifique. 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.

Diagramme du réseau

- Les routeurs A et B sont adjacents à la couche 2 et ne connaissent pas l'appareil Firepower en ligne (désigné comme ips).
- Routeur A - 10.0.0.1/24
- Routeur B - 10.0.0.2/24



- Pour chaque protocole IGP testé (EIGRP et OSPF), le protocole de routage a été activé sur le réseau 10.0.0.0/24.
- Lors du test de BGP, e-BGP a été utilisé et les interfaces physiques directement connectées ont été utilisées comme source de mise à jour pour les homologues.

Configuration

Exemple EIGRP

Sur le routeur

Routeur A :

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

Routeur B :

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

Sur FireSIGHT Management Center

1. Sélectionnez la stratégie de contrôle d'accès appliquée au périphérique Firepower.
2. Créez une règle de contrôle d'accès avec une action de **confiance**.
3. Sous l'onglet **Ports**, sélectionnez **EIGRP** sous protocole 88.
4. Cliquez sur **Add** pour ajouter le port au port de destination.
5. Enregistrez la règle de contrôle d'accès.

Editing Rule - Trust IP Header 88 EIGRP

Name: Trust IP Header 88 EIGRP 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) EIGRP (88)

Protocol Add Protocol Add

Save Cancel

Exemple OSPF

Sur le routeur

Routeur A :

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

Routeur B :

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

Sur FireSIGHT Management Center

1. Sélectionnez la stratégie de contrôle d'accès appliquée au périphérique Firepower.
2. Créez une règle de contrôle d'accès avec une action de **confiance**.
3. Sous l'onglet **Ports**, sélectionnez OSPF sous protocole 89.
4. Cliquez sur **Add** pour ajouter le port au port de destination.
5. Enregistrez la règle de contrôle d'accès.

Editing Rule - Trust IP Header 89 OSPF

Name: Trust IP Header 89 OSPF 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) OSPF (89)

Protocol Add Protocol Add

Save Cancel

Exemple BGP

Sur le routeur

Routeur A :

```
router bgp 65001
neighbor 10.0.0.2 remote-as 65002
```

Routeur B :

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

Sur FireSIGHT Management Center









Note: Vous devez créer deux entrées de contrôle d'accès, car le port 179 peut être le port source ou le port de destination en fonction du TCP SYN du haut-parleur BGP qui établit la session en premier.

Règle 1 :

1. Sélectionnez la stratégie de contrôle d'accès appliquée au périphérique Firepower.
2. Créez une règle de contrôle d'accès avec une action de **confiance**.
3. Sous l'onglet **Ports**, sélectionnez **TCP(6)** et entrez **port 179**.
4. Cliquez sur **Add** pour ajouter le port au **port source**.
5. Enregistrez la règle de contrôle d'accès.

Règle 2 :

1. Sélectionnez la stratégie de contrôle d'accès appliquée au périphérique Firepower.
2. Créez une règle de contrôle d'accès avec une action de **confiance**.
3. Sous l'onglet **Ports**, sélectionnez **TCP(6)** et entrez **port 179**.
4. Cliquez sur **Add** pour ajouter le port au **port de destination**.
5. Enregistrer la règle de contrôle d'accès

3	Trust BGP TCP Source 179	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		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

Vérification

Afin de vérifier qu'une règle **Trust** fonctionne comme prévu, capturez les paquets sur le dispositif Firepower. Si vous remarquez le trafic EIGRP, OSPF ou BGP dans la capture de paquets, alors le trafic n'est pas approuvé comme prévu.

Astuce : Lisez la section pour connaître les étapes de capture du trafic sur les appliances Firepower.

Voici quelques exemples :

EIGRP

Si la règle Trust fonctionne comme prévu, le trafic suivant ne doit pas s'afficher :

```
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

Si la règle d'approbation fonctionne comme prévu, le trafic suivant ne doit pas s'afficher :

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

Si la règle d'approbation fonctionne comme prévu, le trafic suivant ne doit pas s'afficher :

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: Les trajets BGP en haut de TCP et les keepalives ne sont pas aussi fréquents que les IGP. En supposant qu'il n'y ait aucune préfixe à mettre à jour ou à retirer, vous devrez peut-être attendre plus longtemps pour vérifier que vous ne voyez pas de trafic sur le port TCP/179.

Dépannage

Si le trafic du protocole de routage apparaît toujours, procédez comme suit :

1. Vérifiez que la stratégie de contrôle d'accès a bien été appliquée de FireSIGHT Management Center à l'apppliance Firepower. Pour ce faire, accédez à la page **System > Monitoring > Task Status**.
2. Vérifiez que l'action de règle est **Trust** et non **Allow**.
3. Vérifiez que la journalisation n'est pas activée sur la règle **d'approbation**.