Exclusion des messages EIGRP, OSPF et BGP de l'inspection d'intrusion de FirePOWER

Contenu

Introduction

Les protocoles de routage envoient des messages Hello et le Keepalives pour permuter les informations de routage et pour s'assurer que les voisins sont encore accessibles. Sous la charge lourde, une appliance de Cisco FirePOWER peut retarder un message de keepalive (sans le relâcher) assez longtemps pour qu'un routeur déclare son voisin vers le bas. Le document te fournit les étapes pour créer une règle de confiance d'exclure le Keepalives et de contrôler le trafic plat d'un protocole de routage. Il permet aux appliances ou à des services de FirePOWER de commuter des paquets d'entrée à l'interface de sortie, sans retard d'inspection.

Conditions préalables

Composants utilisés

Les changements de politique de contrôle d'accès sur ce document utilisent les plates-formes matérielles suivantes :

- Centre de Gestion de FireSIGHT (FMC)
- Appliance de FirePOWER : Gamme 7000, modèles de gamme 8000

Note: Les informations sur ce document ont été créées des périphériques dans un environnement de travaux pratiques spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Diagramme du réseau

- Le routeur A et le routeur B sont layer-2 adjacent, et sont inconscients de l'appliance intégrée de FirePOWER (étiquetée comme IPS).
- Routeur A - 10.0.0.1/24
- Routeur B - 10.0.0.2/24

- Pour chaque Interior Gateway Protocol testé (EIGRP et OSPF), le protocole de routage a été activé sur le réseau 10.0.0.0/24.
- Quand le BGP de test, e-BGP a été utilisé et les interfaces physiques directement connectées ser de la source de mise à jour pour les peerings.

Configuration

Exemple EIGRP

Sur le routeur

Routeur A :

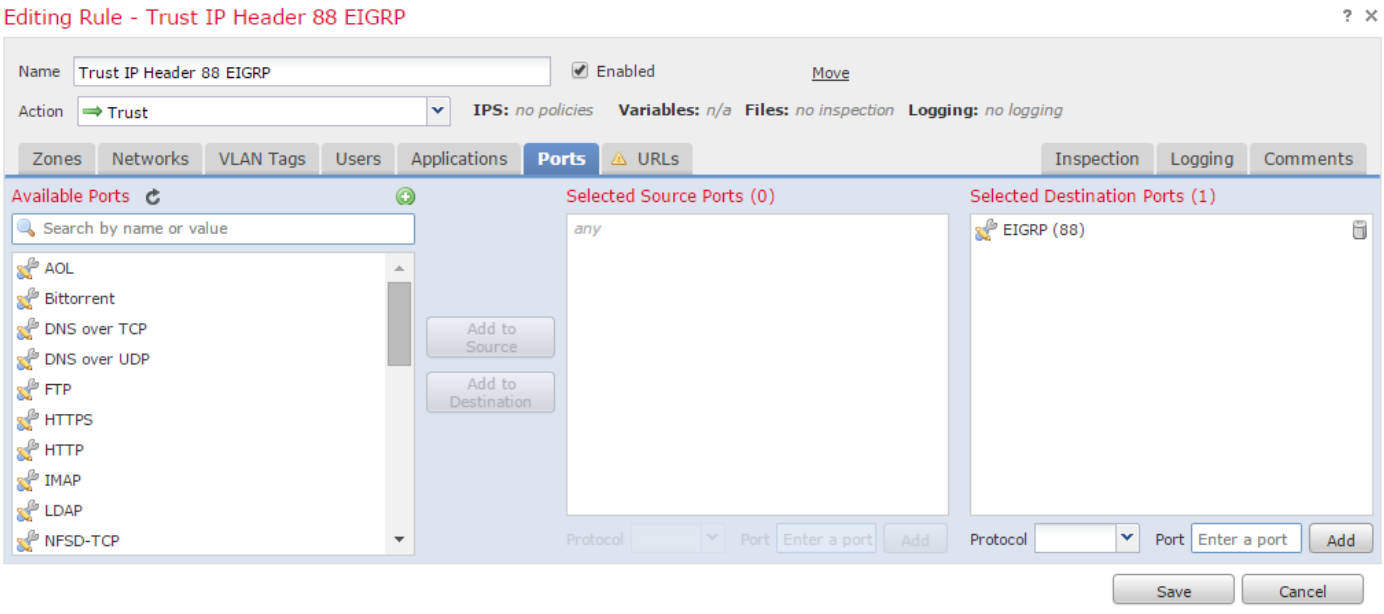
```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

Routeur B :

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

Au centre de Gestion de FireSIGHT

1. Sélectionnez la stratégie de contrôle d'accès appliquée à l'appliance de FirePOWER.
2. Créez une règle de contrôle d'accès avec une action de **confiance.**
3. Sous les **ports** tabulez, **EIGRP** choisi sous le protocole 88.
4. Cliquez sur Add pour ajouter le port à la destination port.
5. Sauvegardez la règle de contrôle d'accès.



Exemple OSPF

Sur le routeur

Routeur A :

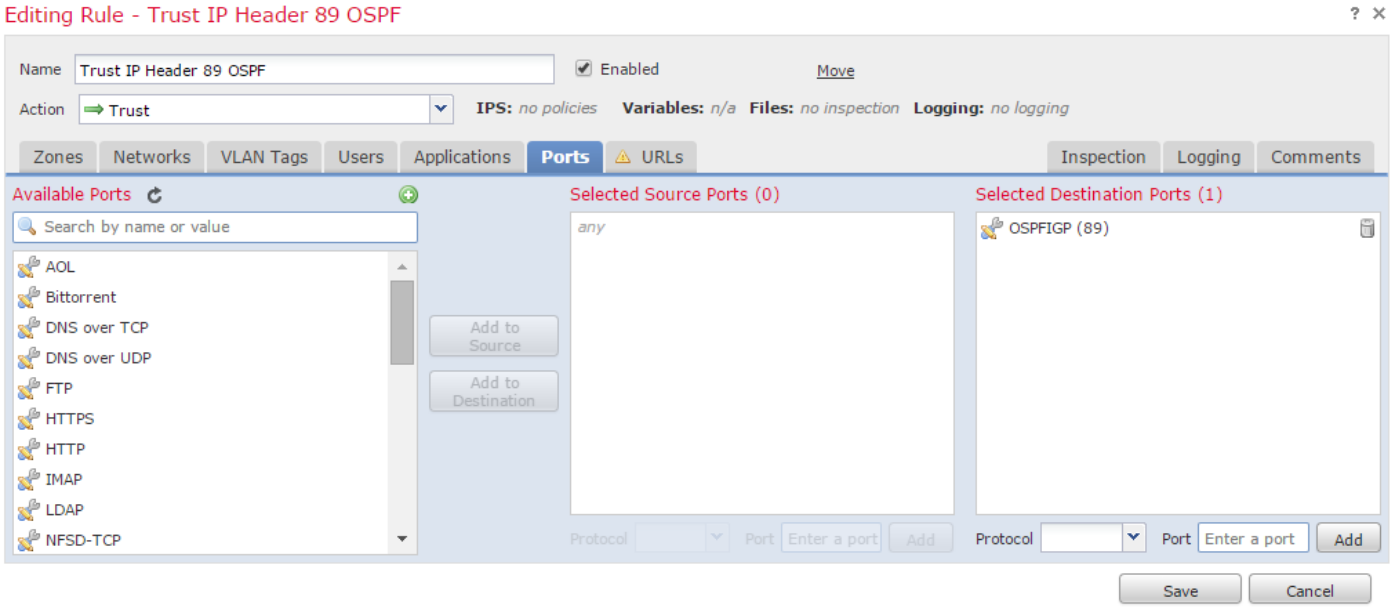
```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

Routeur B :

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

Au centre de Gestion de FireSIGHT

1. Sélectionnez la stratégie de contrôle d'accès appliquée à l'appliance de FirePOWER.
2. Créez une règle de contrôle d'accès avec une action de **confiance.**
3. Sous les **ports** tabulez, OSPF choisi sous le protocole 89.
4. Cliquez sur Add pour ajouter le port à la destination port.
5. Sauvegardez la règle de contrôle d'accès.



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
```

Au centre de Gestion de FireSIGHT

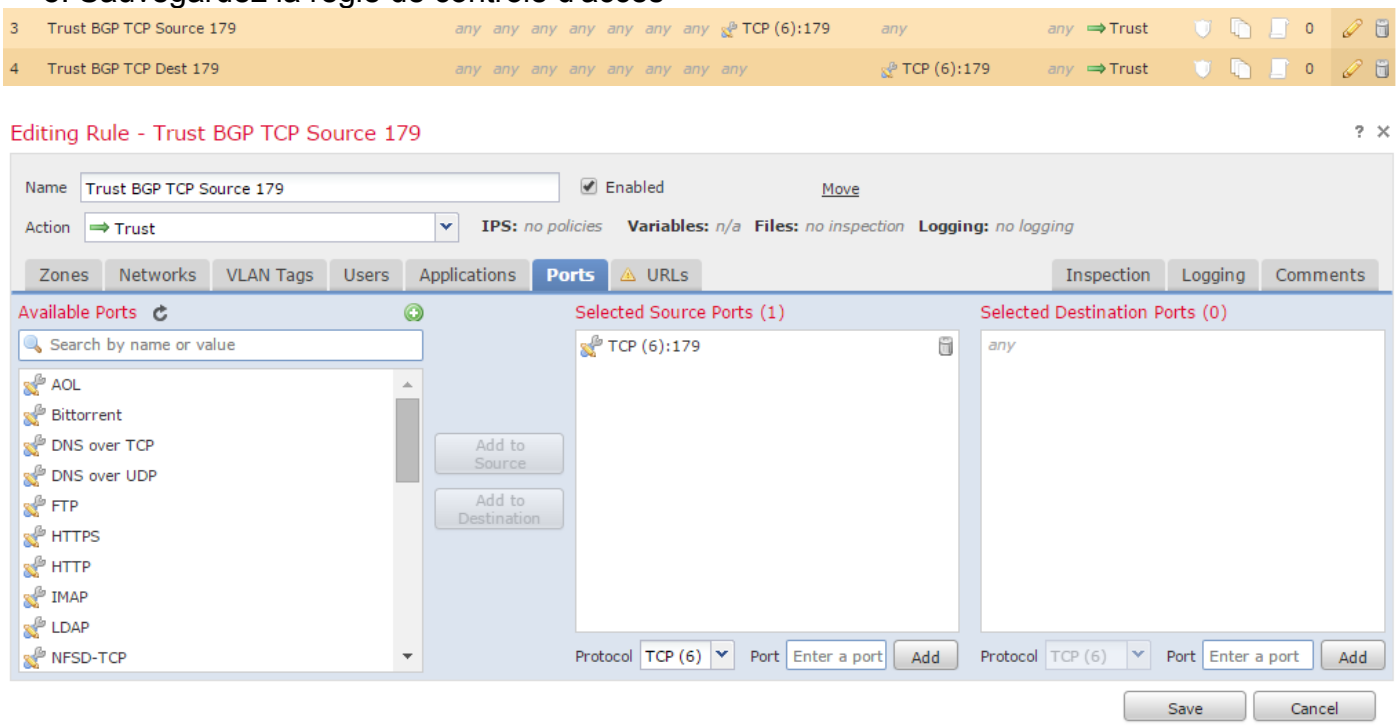
Note: Vous devez créer deux entrées de contrôle d'accès, car le port 179 peut être la source ou la destination port selon lesquelles la synchronisation du TCP du speaker BGP établit la session d'abord.

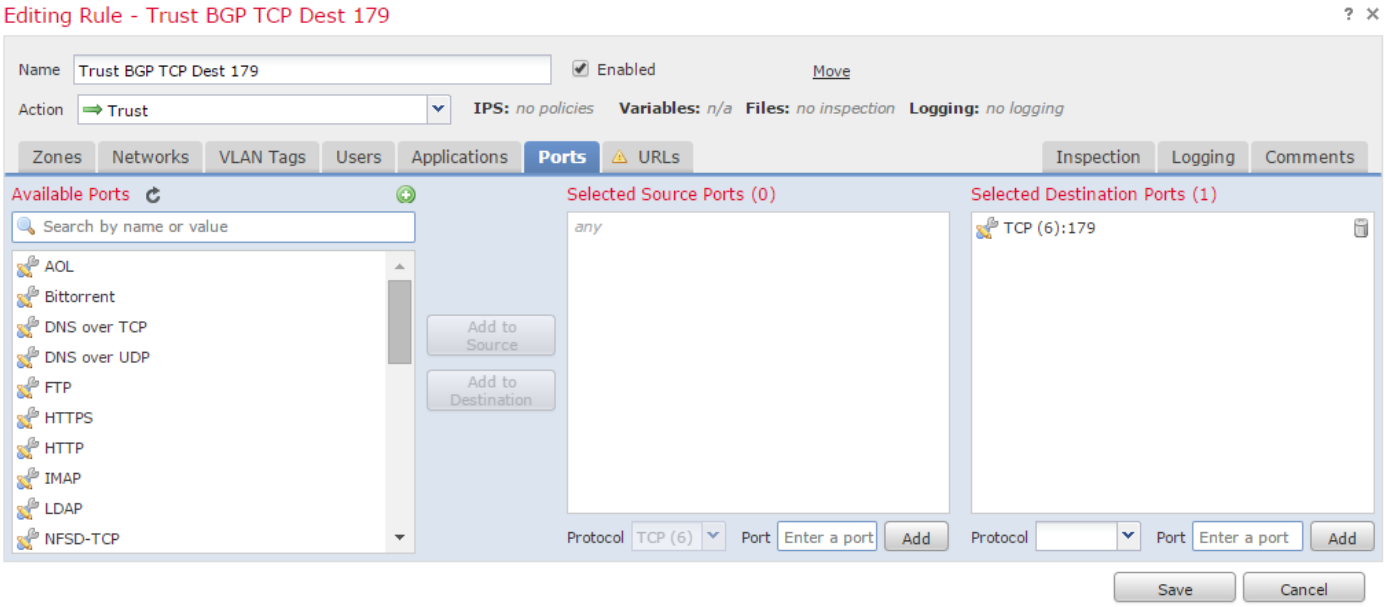
Règle 1 :

1. Sélectionnez la stratégie de contrôle d'accès appliquée à l'appliance de FirePOWER.
2. Créez une règle de contrôle d'accès avec une action de **confiance**.
3. Sous les **ports** tabulez, sélectionnez **TCP(6)** et entrez dans le **port 179**.
4. Cliquez sur Add pour ajouter le port au **port de source**.
5. Sauvegardez la règle de contrôle d'accès.

Règle 2 :

1. Sélectionnez la stratégie de contrôle d'accès appliquée à l'appliance de FirePOWER.
2. Créez une règle de contrôle d'accès avec une action de **confiance**.
3. Sous les **ports** tabulez, **sélectionnez TCP(6)** et entrez dans le **port 179**.
4. Cliquez sur Add pour ajouter le port à la **destination port**.
5. Sauvegardez la règle de contrôle d'accès





Vérification

Afin de vérifier qu'une règle de **confiance** fonctionne comme prévu, capturez les paquets sur l'appliance de FirePOWER. Si vous notez le trafic EIGRP, OSPF ou BGP dans la capture de paquet, alors le trafic n'est de confiance pas comme prévu.

> **Conseil** : Lu pour trouver les étapes sur la façon dont capturer le trafic sur les appliances de FirePOWER.

Voici quelques exemples :

EIGRP

Si la règle de confiance fonctionne comme prévu, vous ne devriez pas voir le trafic suivant :

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

OSPF

Si la règle de confiance est fonctionne comme prévu, vous ne devriez pas voir le trafic suivant :

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

BGP

Si la règle de confiance est fonctionne comme prévu, vous ne devriez pas voir le trafic suivant :

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

> **Note**: Les tours BGP sur le TCP et le Keepalives ne sont pas aussi fréquents que les IGP.

Supposent là aucun préfixe à mettre à jour ou retiré, vous pouvez devoir attendre une plus longue période pour vous vérifier ne voyez pas le trafic sur le port TCP/179.

Dépannage

Si vous voyez toujours le trafic de protocole de routage, effectuez s'il vous plaît les tâches suivantes :

1. Vérifiez que la stratégie de contrôle d'accès a été avec succès appliquée à partir du centre de Gestion de FireSIGHT à l'appliance de FirePOWER. Afin de faire cela, naviguez vers la page d'**état de système > de surveillance > de tâche**.

2. Vérifiez que l'action de règle est **confiance** et **ne pas laisser**.

3. Vérifiez cela qui se connecte n'est pas activé sur la règle de **confiance**.