Исключение EIGRP, OSPF и BGP - сообщений от контроля проникновения огневой мощи

Содержание

Введение

Протоколы маршрутизации передают приветственные сообщения и пакеты Keepalive, чтобы обмениваться сведениями о маршрутизации и гарантировать, что соседние узлы все еще достижимы. Под нагрузкой большая устройство Огневой мощи Cisco может задержать сообщение поддержки активности (не отбрасывая его) достаточно долго для маршрутизатора для объявления его соседнего узла вниз. Документ предоставляет вас шаги для создания Трастового правила исключить пакеты Keepalive и трафик уровня управления протокола маршрутизации. Это позволяет устройствам Огневой мощи или сервисам коммутировать пакеты от входа до исходящего интерфейса без задержки контроля.

Предварительные условия

Используемые компоненты

Изменения Политики контроля доступа на этом документе используют следующие аппаратные платформы:

- Центр управления FireSIGHT (FMC)
- Устройство огневой мощи: модели серии 8000, серии 7000

Примечание: Информация об этом документе была создана от устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

Схема сети

- Маршрутизатор A и маршрутизатор B являются смежным уровнем 2, и не знают о встроенном устройстве Огневой мощи (маркированный как ips).
- Маршрутизатор A - 10.0.0.1/24
- Маршрутизатор B - 10.0.0.2/24

- Для каждого протестированного Протокола внутреннего шлюза (EIGRP и OSPF), протокол маршрутизации был включен в 10.0.0.0/24 сети.
- При тестировании BGP использовался eBGP, и непосредственно связанные физические интерфейсы использовались как источник обновления для равноправных информационных обменов.

!--- конфигурацию

Пример EIGRP

На маршрутизаторе

Маршрутизатор A:

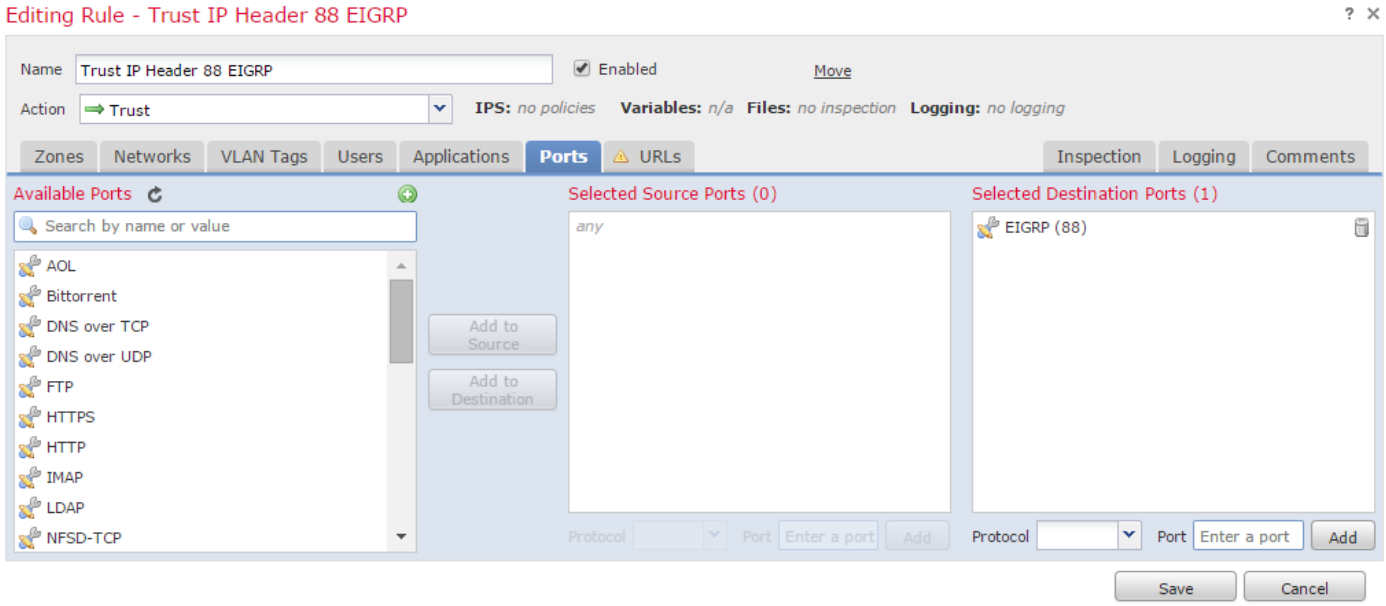
```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

Маршрутизатор B:

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

На центре управления FireSIGHT

1. Выберите Access Control Policy, применился к устройству Огневой мощи.
2. Создайте правило Управления доступом с действием **Доверия.**
3. Под вкладкой **Ports** выберите **EIGRP** в соответствии с протоколом 88.
4. **Нажмите Add**, чтобы добавить порт к порту назначения.
5. Сохраните правило управления доступом.



Пример OSPF

На маршрутизаторе

Маршрутизатор A:

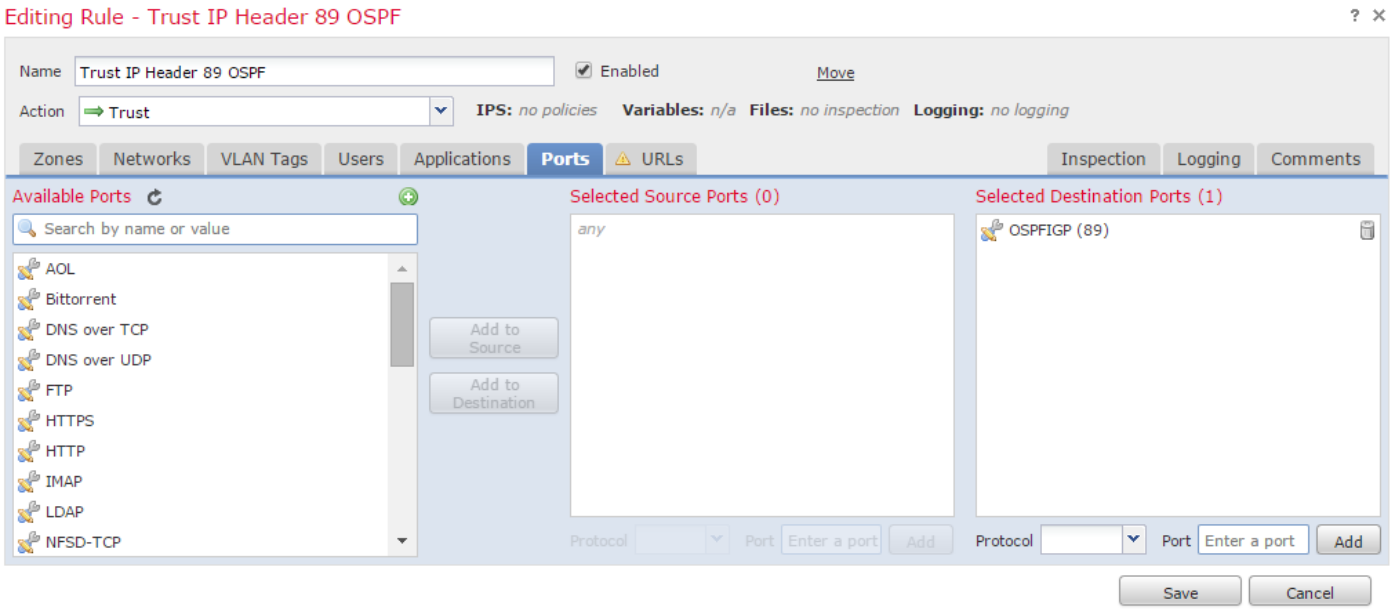
```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

Маршрутизатор B:

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

На центре управления FireSIGHT

1. Выберите Access Control Policy, применился к устройству Огневой мощи.
2. Создайте правило Управления доступом с действием **Доверия.**
3. Под вкладкой **Ports** выберите OSPF в соответствии с протоколом 89.
4. **Нажмите Add**, чтобы добавить порт к порту назначения.
5. Сохраните правило управления доступом.



Пример BGP

На маршрутизаторе

Маршрутизатор A:

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

Маршрутизатор B:

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

На центре управления FireSIGHT

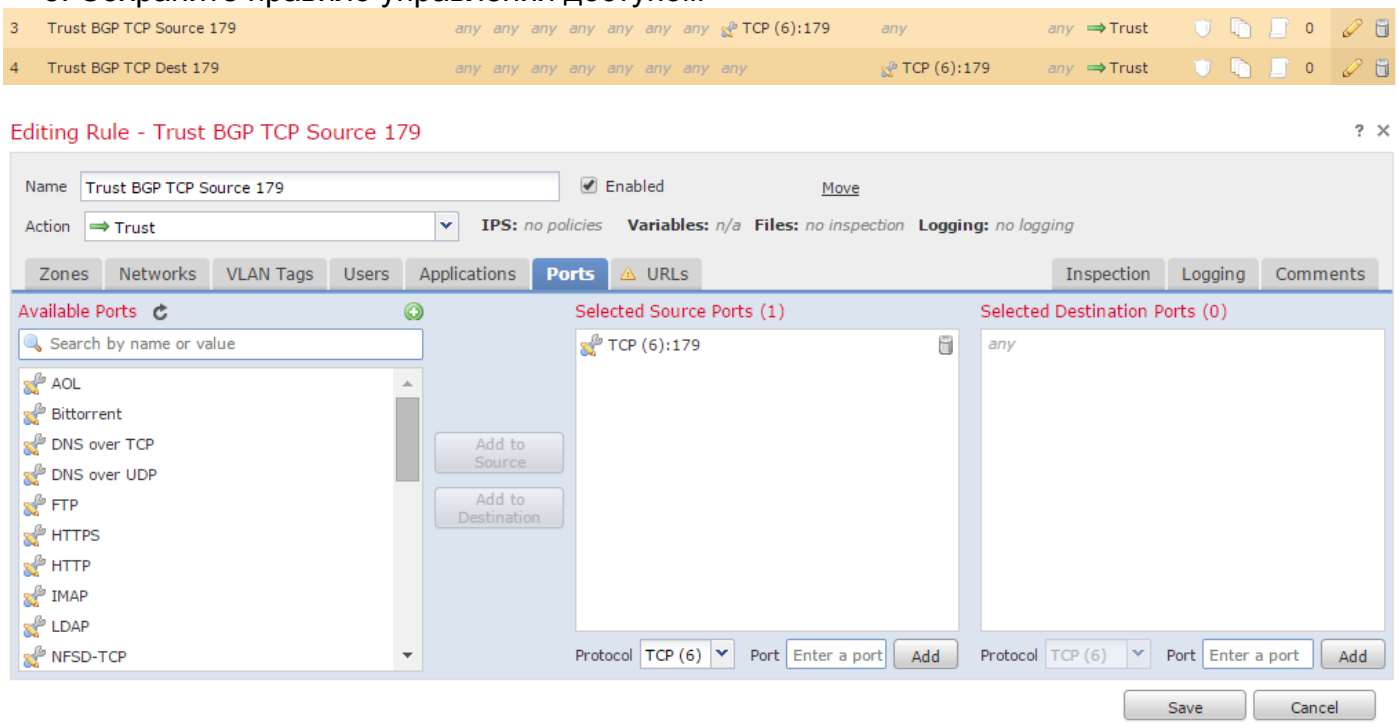
> **Примечание:** Необходимо создать две записи управления доступом, поскольку порт 179 может быть портом источника или назначения, в зависимости от которого SYN TCP динамика BGP устанавливает сеанс сначала.

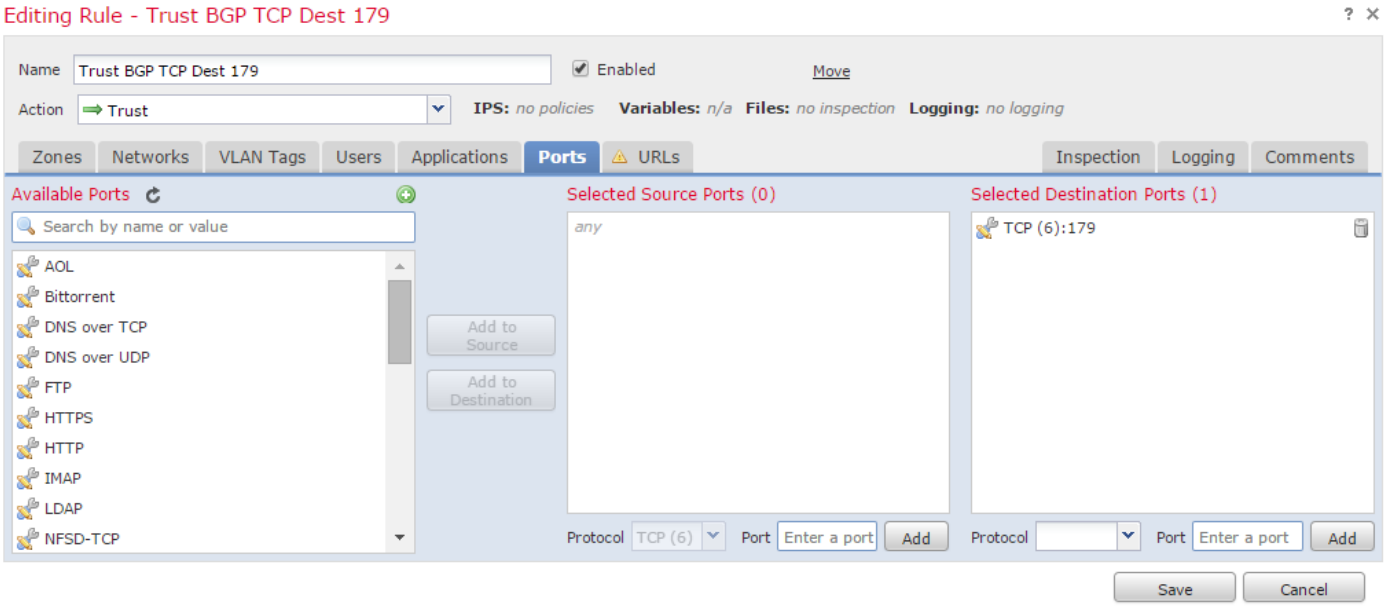
Правило 1:

1. Выберите Access Control Policy, применился к устройству Огневой мощи.
2. Создайте правило Управления доступом с действием **Доверия**.
3. Под вкладкой **Ports** выберите **TCP (6)** и введите **порт 179**.
4. **Нажмите Add** для добавления порта к **исходному порту**.
5. Сохраните правило управления доступом.

Правило 2:

1. Выберите Access Control Policy, применился к устройству Огневой мощи.
2. Создайте правило Управления доступом с действием **Доверия**.
3. Под вкладкой **Ports выберите TCP (6)** и введите **порт 179**.
4. **Нажмите Add**, чтобы добавить порт к **порту назначения**.
5. Сохраните правило управления доступом





Проверка

Чтобы проверить, что **Трастовое** правило работает как ожидалось, пакеты перехвата на устройстве Огневой мощи. Если вы замечаете EIGRP, OSPF или трафик BGP в захвате пакета, то трафику не доверяют как ожидалось.

> **Совет:** Читайте для обнаружения шагов в то, как перехватить трафик на устройствах Огневой мощи.

Приведем несколько примеров:

EIGRP

Если Трастовое правило работает как ожидалось, вы не должны видеть следующий трафик:

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

OSPF

Если Трастовое правило, работает как ожидалось, вы не должны видеть следующий трафик:

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

BGP

Если Трастовое правило, работает как ожидалось, вы не должны видеть следующий трафик:

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

> **Примечание:** Поездки BGP поверх TCP и пакетов Keepalive не являются столь же частыми как IGPs. Принятие там не является никакими префиксами, которые будут

обновлены или забраны, вы, возможно, должны ждать более длинного периода времени, чтобы проверить, что вы не видите трафик на TCP/179 порта.

Устранение неисправностей

Если вы все еще видите трафик протокола маршрутизации, выполните следующие задачи:

1. Проверьте, что Политика контроля доступа была успешно применена от Центра управления FireSIGHT до устройства Огневой мощи. Чтобы сделать это, перейдите к странице **System> Monitoring> Task Status**.

2. Проверьте, что действие правила является **Трастовым**, и не **Позволяют**.

3. Проверьте, что регистрация не включена на **Трастовом** правиле.