Процедуры захвата пакета на устройстве огневой мощи Cisco

Содержание

Введение

Этот документ описывает, как использовать **команду tcpdump** для получения пакетов, которые замечены сетевым интерфейсом устройства Огневой мощи. Это использует синтаксис Фильтра пакета Беркли (BPF).

Предварительные условия

Требования

Cisco рекомендует ознакомиться с устройством Огневой мощи Cisco и моделями виртуального устройства.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

> **% Warning:** При выполнении **`команды tcpdump`** на производственной системе она может повлиять на производительность сети.

Шагает для получения пакетов

Войдите к CLI вашего устройства Огневой мощи.

В версиях 6.1 и позже, введите **трафик перехвата**. Пример,

```
> capture-traffic

Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set (Interfaces s2p1, s2p2)
```

В версиях 6.0. x. x и ранее, введите **трафик перехвата поддержки системы**. Пример,

```
> system support capture-traffic

Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set (Interfaces s2p1, s2p2)
```

После того, как вы сделаете выбор, вам предложат для опций:

```
> system support capture-traffic

Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set (Interfaces s2p1, s2p2)
```

Для получения достаточных данных от пакетов необходимо использовать`-s` опцию для установки snaplength правильно. snaplength должен быть установлен в значение, которое совпадает с блоком передачи настраиваемого максимального значения (MTU) значение Интерфейсной конфигурации Набора, который настройки по умолчанию к 1518.

> **% Warning:** Начиная с получения трафика на экран может ухудшить производительность системы и сети, Cisco рекомендует использовать`-w` опцию `<filename>` с `командой tcpdump`. Это перехватывает пакеты к файлу. Если вы выполняете команду без`-w` опции, нажмите сочетание клавиш **Ctrl-C** для выхода.

Пример`-w` опции `<filename>`:

```
-w capture.pcap -s 1518
```

> **Внимание. :** Не используйте элементы пути при определении захвата пакета (pcap) имя файла. Необходимо задать только pcap имя файла, которое будет создано в устройстве.

Если выбираемо перехватить ограниченное число пакетов, можно использовать`-c` флаг `<packets>` для определения количества пакетов для получения. Например, для получения точно 5000 пакетов:

```
-w capture.pcap -s 1518 -c 5000
```

Кроме того, фильтр BPF может быть добавлен в конце команды для ограничения, какие пакеты перехвачены. Например, для ограничения захвата пакета 5000 пакетов с источником или IP - адресом назначения 192.0.2.1, вы могли использовать эти опции:

```
-w capture.pcap -s 1518 -c 5000 host 192.0.2.1
```

Когда вы перехватываете трафик, который является теговой виртуальной локальной сетью (VLAN), необходимо задать VLAN с синтаксисом BPF. В противном случае pcap не содержит ни одного из маркированных тегами пакетов VLAN. Например, данный пример ограничивает перехват для трафика, который является VLAN, помеченной от 192.0.2.1:

```
-w capture.pcap -s 1518 -c 5000 vlan and host 192.0.2.1
```

Если вы не уверены, если трафик является теговой VLAN, этот синтаксис мог бы

использоваться для получения трафика от 192.0.2.1, который является и не является теговой VLAN:

```
-w capture.pcap -s 1518 -c 5000 'host 192.0.2.1 or (vlan and host 192.0.2.1)'
```

> **Примечание:** В предыдущем примере необходимы круглые скобки так, чтобы `'или'` не только применился к `'vlan'`. Одинарные кавычки тогда необходимы для предотвращения любого возможного неверного истолкования круглых скобок оболочкой.

Спецификация тега VLAN перехватывает весь трафик виртуальной локальной сети (VLAN), который совпадает с остатком вашего BPF. Однако, если бы вы хотите перехватить определенный тег VLAN, можно задать, как какой тег VLAN требуется перехватить так:

```
-w capture.pcap -s 1518 -c 5000 vlan 1 and host 192.0.2.1
```

После того, как вы зададите желаемые опции и нажмете **Enter**, tcpdump начинает перехватывать трафик.

> **Совет:** Если `-c` опция не использовалась, нажмите сочетание клавиш **Ctrl-C** для остановки перехвата.

Как только вы останавливаете перехват, вы получите подтверждение. Пример:

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -w capture.pcap -s 1518 -c 5000 host 192.0.2.1
Cleaning up.
Done.
```

Скопируйте файл Pcap

Для копирования pcap файла от устройства FirePOWER до другой системы, которая принимает входящие SSH - подключения, используйте эту команду:

```
> system file secure-copy hostname username destination_directory pcap_file
```

После нажатия **Enter** вам предложат для пароля к удаленной системе. Файл будет скопирован по сети.

> **Примечание:** В данном примере **имя хоста** обращается к названию или IP-адресу целевого удаленного хоста, **имя пользователя** задает имя пользователя на удаленном хосте, **destination_directory** задает путь назначения на удаленном хосте, и **pcap_file** задает локальный pcap файл для передачи.