Содержание

Введение

Этот документ описывает, как выполнить захваты пакета на устройствах Безопасности содержания Cisco.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Email Security Appliance (ESA)
- Cisco Web Security Appliance (WSA)
- Устройство менеджмента Cisco Security (SMA)
- AsyncOS

Используемые компоненты

Сведения в этом документе являются ядром на всех версиях AsyncOS.

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.

Как вы выполняете захват пакета на устройстве Безопасности содержания Cisco?

Выполните эти шаги для выполнения захвата пакета **(команда tcpdump)** с GUI:

1. Перейдите, чтобы **Помочь и Поддержать> Захват пакета** на GUI.

2. Отредактируйте параметры настройки захвата пакета как требуется, такие как сетевой интерфейс, на котором выполняется захват пакета. Можно использовать один из предопределенных фильтров, или можно создать пользовательский фильтр с использованием любого синтаксиса, который поддерживается **командой tcpdump** Unix.

3. Нажмите **Start Capture** для начала перехвата.

4. Нажмите **Stop Capture** для окончания перехвата.

5. Загрузите захват пакета.

Выполните эти шаги для выполнения захвата пакета **(команда tcpdump)** с CLI:

1. Введите эту команду в CLI:

```
wsa.run> packetcapture

Status: No capture running


Current Settings:

 Max file size:     200 MB

 Capture Limit:     None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:    (tcp port 80 or tcp port 3128)
```

2. Выберите операцию, которую вы хотите выполнить:

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> setup
```

3. Введите максимальный допустимый размер для перехвата файла (в МБ):

```
[200]> 200

Do you want to stop the capture when the file size is reached? (If not, a new
 file will be started and the older capture data will be discarded.)

[N]> n

The following interfaces are configured:

1. Management

2. T1

3. T2
```

4. Введите имя или количество одного или более интерфейсов, от которых можно перехватить пакеты, разделенные запятыми:

```
[1]> 1
```

5. Введите фильтр, который вы хотите использовать для перехвата. Введите слово, **ЯСНОЕ**, чтобы очистить фильтр и перехватить все пакеты на выбранных интерфейсах.

```
[(tcp port 80 or tcp port 3128)]> host 10.10.10.10 && port 80


Status: No capture running


Current Settings:

 Max file size:     200 MB

 Capture Limit:     None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:    host 10.10.10.10 && port 80
```

6. Выберите операцию **запуска** для начала перехвата:

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> start


Status: Capture in progress (Duration: 0s)

File Name: S650-00137262569A-8RVFDB1-20080919-174302.cap (Size: 0K)


Current Settings:

 Max file size:     200 MB

 Capture Limit:     None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:    host 10.10.10.10 && port 80
```

7. Выберите операцию **остановки** для окончания перехвата:

```
- STOP - Stop packet capture.

- STATUS - Display current capture status.

- SETUP - Change packet capture settings.

[]> stop


Status: No capture running (Capture stopped by user)


Current Settings:

 Max file size:     200 MB

 Capture Limit:     None (Run Indefinitely)
```

```
Capture Interfaces: Management

Capture Filter:    host 10.10.10.10 && port 80
```