Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Общие сведения](#)
[Захваты пакета на версиях AsyncOS 7.x и позже](#)
[Запустите или остановите захват пакета](#)
[Функциональность захвата пакета](#)
[Захваты пакета на версиях AsyncOS 6.x и ранее](#)
[Запустите или остановите захват пакета](#)
[Фильтры захвата пакета](#)

Введение

Этот документ описывает, как выполнить захваты пакета на Cisco Email Security Appliance (ESA).

Предварительные условия

Требования

Cisco рекомендует ознакомиться с ESA Cisco.

Используемые компоненты

Сведения в этом документе основываются на ESA Cisco, который выполняет любую версию AsyncOS.

Общие сведения

При контакте со Службой поддержки пользователей IronPort с проблемой вас можно было бы попросить предоставить понимание исходящей и входящей активности сети ESA. Устройство предоставляет способность перехватить и отобразить TCP, IP и другие пакеты, которые переданы или получены по сети, к которой подключено устройство. Вы могли бы хотеть выполнить захват пакета для отладки сетевой установки и для проверки сетевого трафика, который достигает или оставляет устройство.

Примечание: Этот документ ссылается на программное обеспечение, которое не

поддерживается или поддерживается IronPort. Информация предоставлена как любезность для вашего удобства. Для дальнейшей поддержки свяжитесь с поставщиком программного обеспечения.

Следует отметить, что ранее используемая команда CLI **tcpdump** заменена новой **packetcapture** командой в Версиях AsyncOS 7.0 и позже. Эта команда предлагает функциональность, подобную **команде tcpdump**, и это также доступно для использования на GUI.

При выполнении Версии 6.x AsyncOS или ранее обратитесь к инструкциям по тому, как использовать **команду tcpdump** в **Захватах пакета на Версиях AsyncOS 6.x и Более ранний** раздел этого документа. Кроме того, параметры фильтрации, которые описаны в разделе **Фильтров Захвата пакета**, допустимы для новой **packetcapture** команды также.

Захваты пакета на версиях AsyncOS 7.x и позже

В этом разделе описываются процесс захвата пакета на Версиях AsyncOS 7.x и позже.

Запустите или остановите захват пакета

Для начала захвата пакета с GUI перейдите к Поддержке и Меню справки, выберите **Packet Capture**, и затем нажмите **Start Capture**. Для остановки процесса захвата пакета нажмите **Stop Capture**.

Примечание: Перехват, который начинается в GUI, сохранен между сеансами.

Для начала захвата пакета с CLI войдите**, packetcapture> запускают** команду. Для остановки процесса захвата пакета войдите**, packetcapture> останавливают** команду, и ESA останавливает захват пакета, когда заканчивается сеанс.

Функциональность захвата пакета

Вот список полезных сведений, которые можно использовать для управления захватами пакета:

- ESA сохраняет действие захваченного пакета в файл и хранит файл локально. Можно настроить размер перехвата файла MAXIMUM PACKET, промежуток времени, в течение которого захват пакета выполняется, и на котором сетевом интерфейсе выполняется перехват. Можно также использовать фильтр для ограничения захвата пакета трафиком через определенный порт или трафиком от определенного клиента или IP-адреса сервера.

- Перейдите, чтобы **Поддержать и Помочь> Захват пакета** от GUI для просмотра полного списка файлов захвата пакета, которые хранятся на жестком диске. Когда захват пакета выполняется, отображения страницы Захвата пакета, статус происходящего перехвата

с текущей статистикой, такие как размер файла и время истек.

- Нажмите кнопку **Download File** для загрузки файла захвата пакета. Можно передать его на электронной почте к Службе поддержки пользователей IronPort, чтобы отладить и решить любые проблемы.
- Для удаления файла захвата пакета выберите один или несколько файлов и нажмите **Delete Selected Files**.
- Для редактирования параметров настройки захвата пакета с GUI выберите **Packet Capture** от Поддержки и Меню справки и нажмите **Edit Settings**.
- Для редактирования параметров настройки захвата пакета с CLI введите **packetcapture>** команда **настройки**.

Примечание: GUI только отображает захваты пакета, которые начинаются в GUI, не тех, которые начинают с CLI. Точно так же CLI только отображает статус перехвата текущего пакета, который начался в CLI. Только один перехват может работать за один раз.

Совет: Для дополнительных сведений об опциях захвата пакета и параметрах настройки фильтра, обратитесь к разделу **Фильтров Захвата пакета** этого документа. Для доступа к AsyncOS Онлайновая Справка от GUI, перейдите, чтобы **Помочь и Поддержать> Онлайновая Справка> Индекс> P> Захват пакета**.

Захваты пакета на версиях AsyncOS 6.x и ранее

В этом разделе описываются процесс захвата пакета на Версиях AsyncOS 6.x и ранее.

Запустите или остановите захват пакета

Можно использовать **команду tcpdump** для получения TCP/IP и других пакетов, которые переданы или получены по сети, к которой подключен ESA.

Выполните эти шаги, чтобы запустить или остановить захват пакета:

1. Введите **диагностику> сеть> команда tcpdump** в CLI ESA. Ниже представлен пример выходных данных:

```
example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
```

```
[]> network

Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> tcpdump

- START - Start packet capture
- STOP - Stop packet capture
- STATUS - Status capture
- FILTER - Set packet capture filter
- INTERFACE - Set packet capture interface
- CLEAR - Remove previous packet captures
[]>
```

2. Установите интерфейс (Данные 1, Данные 2, или менеджмент) и фильтр.

   Примечание: Фильтр использует тот же формат в качестве **команды tcpdump** Unix.
3. Выберите **START**, чтобы начать перехват и **ОСТАНОВИТЬСЯ** для окончания его.

   Примечание: Не выходите из меню tcpdump, в то время как перехват происходит. Необходимо использовать второе окно CLI для выполнения любых других команд. Как только процесс перехвата завершен, необходимо использовать протокол SCP или Протокол FTP от локального рабочего стола для загрузки файлов из каталога под названием Диагностика (обратитесь к разделу **Фильтров Захвата пакета** для подробных данных). Файлы используют Захват пакета (PCAP) формат и могут быть рассмотрены с программой такой как Эфирные или Wireshark.

Фильтры захвата пакета

Диагностика> СЕТЕВАЯ команда CLI использует стандартный синтаксис фильтра tcpdump. Этот раздел предоставляет сведения в отношении перехвата tcpdump, фильтрует и предоставляет некоторые примеры.

Это стандартные фильтры, которые используются:

- **ip -** Фильтрует для всего трафика Протокола "IP"
- **tCP /*-** Фильтры для всего трафика протокола TCP
- **ip host** - Фильтры для определенного источника IP-адреса или назначения

Вот некоторые примеры фильтров в использовании:

- **ip host 10.1.1.1** - Этот фильтр перехватывает любой трафик, который включает 10.1.1.1 как источник или назначение.
- **ip host 10.1.1.1 или ip host 10.1.1.2** - Этот фильтр перехватывает трафик, который содержит или 10.1.1.1 или 10.1.1.2 как источник или назначение.

Для извлечения перехваченного файла перейдите к **вару> журнал> диагностика** или **данные> паб> диагностика** для достижения каталога Diagnostic.

Примечание: Когда эта команда используется, она может заставить ваше дисковое

пространство ESA заполняться и может также вызвать снижение производительности. Cisco рекомендует только использовать эту команду с помощью Инженера службы поддержки Cisco IronPort.