Использование команды tcpdump в программном обеспечении ACNS

Содержание

Введение

Cisco сетевой ПО приложений и контента (ACNS) 4.2.1 представил **команду tcpdump**. Эта команда позволяет вам собрать отслеживание средств прослушивания на Модуле контента, Маршрутизаторе контента или Менеджере распределения контента в целях устранения проблем, когда спросили собрать данные технической поддержкой Cisco. Эта утилита подобна **команде tcpdump** Linux/Unix.

Предварительные условия

Требования

Читатели данного документа должны обладать знаниями по следующим темам:

- Ftp
- ACNS
- Интерфейс командной строки (CLI) ACNS

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения и оборудования:

- Программное обеспечение ACNS 4.2.1 и позже
- Все платформы, которые выполняют ACNS 4.2. X и выше

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.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Получение пакетов

CLI на ACNS теперь позволяет администратору (должно быть администрирование пользователя) перехватывать пакеты от Ethernet. На Модуле контента серии 500 имена интерфейсов являются eth0 и eth1. На всех платформах ACNS рекомендуется задать путь/имя файла в каталоге local1.

Можно сделать прямой дамп заголовка пакета на экран при запуске **команды tcpdump** на CLI. Нажмите **Ctrl-C** для остановки дампа.

Опции

Команда tcpdump имеет эти опции:

- **- w *имя файла*** — Пишет необработанные выходные данные захвата пакета в файл.
- **- s *количество*** — Перехватывает первые байты <count> каждого пакета.
- **- я *взаимодействую*** — Позволяет вам задавать определенный интерфейс для использования для получения пакетов.
- **- c *количество*** — Ограничивает перехват для *подсчета* пакетов.

Это - эталонная команда:

tcpdump-w/local1/dump.pcap-i eth0-s 1500-c 10000

Эта команда перехватывает первые 1500 байтов следующих 10,000 пакетов от interface Ethernet 0 и помещает выходные данные в файл, названный **dump.pcap** в каталоге local1 на Модуле контента.

Примечание: Гарантируйте определение опции **–s** для установки длины SNAP пакета. Значение по умолчанию перехватывает только 64 байта, и это сохраняет только заголовки пакета в перехват файла. Для устранения проблем перенаправленных пакетов или высокоуровневого трафика (HTTP, аутентификация, и т.д), необходима копия полных пакетов.

Можно также выполнить **tcpdump** и фильтр на определенном IP - адресе:

- Добавьте **хост 10.255.1.34** до конца линии **tcpdump**. **Примечание:** Замените **10.255.1.34** IP-адресом, который использует клиент.
- Кроме того, используйте 1600 в качестве размера для ловли недопустимых пакетов, которые могут быть больше, чем 1500 байтов.

Например:

```
tcpdump -w /local/mydump -s 1600 -c10000 host 10.255.2.34
```

Ftp

После того, как дамп TCP был собран, необходимо переместить файл от Модуля контента до ПК так, чтобы это могло быть просмотрено средством декодирования анализатора трафика.

```
ftp <ip address of the CE>
 !--- Log in with the admin username and password. cd local1 bin hash get <name of the file> !--
- Using the previous example, it is dump.pcap.

     bye
```

Эфирный

Эфирный рекомендуемое программное приложение для чтения дампа TCP, должного вплоть до его функций и их использования с сетями передачи контента, включая способность декодировать пакеты, которые инкапсулируются в Туннель GRE, используемый перенаправлением WCCP. См. веб-сайт Wireshark для получения дополнительной информации.

Примечание: В большинстве случаев перенаправленные пакеты, перехваченные **средством дампа TCP**, доступным с CLI ACNS, отличаются от данных, полученных на интерфейсе. Из-за внутренней реализации и обработки перенаправленных пакетов, IP - адрес назначения и номер порта TCP модифицируются для отражения IP-адреса устройства и номера порта 8999.

Дополнительные сведения

- Поддержка программного обеспечения Cisco сетевого ПО приложений и контента (ACNS)
- Cisco Systems – техническая поддержка и документация