Анализ сетевого трафика с помощью утилиты Tcpdump

ViPNet xFirewall 5

Общая информация

Для диагностики и последующего решения проблем при использовании устройств в сетях ViPNet в ряде случаев необходимо анализировать трафик. Для этого вы можете использовать утилиту tcpdump, которая находится в составе продукта и используется из системной консоли.

tcpdump – это штатная утилита UNIX, которая позволяет перехватывать и анализировать сетевой трафик, проходящий через устройство и вне устройства (promisc mode), на котором запущена данная утилита. Основные функции tcpdump:

- Захват пакетов.
- Анализ проходящего трафика.
- Фильтрация захваченных пакетов по заданным критериям.
- Вывод захваченных пакетов в файл.

Утилита tcpdump имеет возможность анализировать и фильтровать не только пакеты TCP/IP, но и все протоколы семейства IP (icmp, esp, udp и др.), семейства протоколов Ethernet (ip, arp, rarp, lat, stp и др.), а также пакеты беспроводных сетей.

После завершения захвата пакетов утилита tcpdump выводит следующие данные:

- «Захваченных» пакетов – число пакетов, полученных и обработанных утилитой tcpdump.
- Пакетов, «полученных фильтром» – число пакетов, поступивших в фильтр (а не только прошедших через него). В это число входят пакеты, которые позднее были отброшены вследствие нехватки пространства в буфере.
- Пакетов, «отклоненных ядром» – число пакетов, отброшенных механизмом захвата пакетов вследствие нехватки пространства в буфере.

Примечание. promisc mode — «неразборчивый» режим, в котором tcpdump может захватывать все пакеты независимо от того, кому они адресованы.

Использование TCPDUMP для снятия дампа трафика

Данная утилита встроена в программно-аппаратный комплекс, поэтому ее установка не требуется.

Внимание! Запуск tcpdump приводит к значительному увеличению нагрузки на ЦП и, как следствие, к снижению производительности устройства. Например, при фильтрации трафика по одному конкретному интерфейсу или порту в любом случае возникает высокая нагрузка на ЦП.

Подключение к утилите tcpdump и снятие дампа трафика

Для снятия дампа трафика:

1. Подключитесь к командному интерпретатору (как подключаться к командному интерпретатору написано в руководстве по настройке с помощью CLI).
2. Выполните команду `enable` для перехода в режим администратора, введите пароль администратора.
3. Выполните команду `admin escape` для перехода в системную консоль.
4. Просмотрите список доступных сетевых интерфейсов:

   ```
   # tcpdump -D
   ```
5. Для начала захвата трафика запустите утилиту tcpdump с нужными параметрами:

   ```
   # tcpdump [опции] -i <сетевой интерфейс> [фильтры]
   ```
6. Для остановки захвата пакетов использовать комбинацию клавиш CTRL+C (Если не используются опции условия прекращения захвата пакетов).

Экспорт дампа трафика

Для экспорта полученного дампа на USB-накопитель:

1. Для экспорта файла дампа (При использовании опции `-w`) подключите USB-накопитель к ПАК.
2. Выделите список доступных разделов и определите номер раздела подключенного USB-накопителя (Как правило, это последний раздел в списке):

   ```
   # fdisk -l | grep sd
   ```
3. Смонтируйте раздел USB-накопителя:

   `# mkdir /mnt/usb && mount /dev/sdc1 /mnt/usb/` , где `</dev/sdc1>` – корректный номер раздела подключенного USB-накопителя.
4. Скопируйте файл дампа на USB-накопитель:

   ```
   # cp <путь к файлу дампа> /mnt/usb/
   ```
5. Отмонтируйте раздел USB-накопителя:

   ```
   # umount /mnt/usb/
   ```

Совет. Дамп трафика лучше сохранять на встроенный HDD компьютера, или на внешний подключаемый носитель. При сохранении дампа трафика по умолчанию в `/mnt/data/root/` может возникнуть ошибка сохранения, так как на `mnt` невелик объем памяти

[опции]:

- `-c` – остановить работу после перехвата некоторого количества пакетов;
- `-C` – чередование файлов при превышении указанного размера памяти (Mb). Работает в связке с опцией –w;
- `-w` – запись пакетов в файл без обработки. По-умолчанию, без указания полного пути, файл создается в каталоге /mnt/data/root/<имя файла дампа>. Далее полученный файл можно анализировать с помощью программы Wireshark;

- `-D` – отобразить список доступных сетевых интерфейсов для перехвата пакетов;
- `-e` – отобразить информацию об уровне соединения для каждого пакета (отображение MAC-адресов);
- `-f` – вывод доменных имён для ip-адресов;
- `-r` – прочитать пакеты из файла, созданного с помощью опции -w;
- `-n` – не отображать доменные имена (если отображаются по умолчанию);
- `-i` – задание сетевого интерфейса;
- `-q` – вывести краткую информацию;
- `-I` – переключить интерфейс в режим монитора для захвата всех проходящих пакетов;
- `-p` – Не переводит интерфейс в режим приема всех пакетов (promisc mode);
- `-v`, `-vv`, `-vvv` – при синтаксическом анализе и печати выводит подробный вывод, например, вывод общей длины и параметров ip-пакета. Также включает дополнительные проверки целостности пакетов (контрольные суммы заголовков IP и ICMP);
- -ttt – выводить разницу (в микросекундах) между текущей и предыдущей строками дампа;
- `-L` – вывести поддерживаемые протоколы подключения для интерфейса;
- `-F <файл>` – задает использование фильтров, содержащихся в указанном файле. В этом случае заданные в командной строке фильтры игнорируются;
- `-U` – Включить для выходных данных, сохраняемых с помощью опции -w, буферизацию по пакетам, т.е. записывать каждый пакет в файл сразу при сохранении пакета, а не при заполнении выходного буфера.

<сетевой интерфейс>

Параметр `<сетевой интерфейс>` задаёт имя интерфейса для перехвата пакетов. Для захвата пакетов со всех доступных интерфейсов использовать значение – **any**. Имя сетевого интерфейса соответствует имени интерфейса в ViPNet xFirewall (`eth0`, `eth1` и т.д).

При запуске tcpdump автоматически производит поиск сетевых интерфейсов и для анализа использует первый найденный. Поэтому нужно обращать внимание на вывод, чтобы удостовериться, что анализируется нужный интерфейс.

[фильтры]:

- `host` – ip-адрес;
- `net` – адрес сети или подсети;
- `port` - адрес порта назначения;
- `src` – параметр отправителя;
- `dst` – параметр получателя;
- `icmp`, `tcp`, `udp` – сетевые протоколы;
- `broadcast` – только широковещательные пакеты.

Совет. Фильтры можно объединить при помощи логических выражений `and`, `or` и `not`

Более подробно о работе с утилитой:

Справочник по утилитам UNIX,

Официальный сайт утилиты tcpdump

Примеры использования утилиты

Запись вывода данных по протоколу tcp на порт 22 в файл `sshtrace.tcpdump`, пример команды в коде ниже (Файл будет по-умолчанию создан или перезаписан в домашнем каталоге текущего пользователя.):

```
# tcpdump -w sshtrace.tcpdump tcp port 22
```

Вывод информации из файла `sshtrace.tcpdump`:

```
# tcpdump -r sshtrace.tcpdump
```

Выполнить захват всего трафика с интерфейса `eth1`:

```
# tcpdump -i eth1
```

Перехватить трафик с диапазона портов на интерфейсе `eth1`:

```
# tcpdump -i eth1 portrange 100-200
```

Перехватить и отобразить только широковещательные пакеты локальной сети:

```
# tcpdump ether broadcast
```

Выполнить анализ пакетов, отправленных на определённый IP 192.168.1.1:

```
# tcpdump src host 192.168.1.1
```

Выполнить перехват только arp пакетов:

```
# tcpdump -i eth0 -n -nn -ttt 'ip proto \arp'
```

Перехватить первые 100 tcp-пакетов:

```
# tcpdump -i eth1 -n -ttt 'ip proto \tcp' 100
```

АО «ИнфоТеКС», 127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

ФРКЕ.00234-01 91 04, версия продукта 5.6.1