Глава 8.

Coordinator Linux 4

Примечание. Для успешного выполнения практической работы, а также полноценного изучения подробного описания утилит, конфигурационных файлов, команд запуска, примеров настроек и получения подробных инструкций по администрированию Координа-тора Linux и Координатора HW следует использовать справочные руководства для актуальных версий данных программ и устройств.

8.1. Описание лабораторной схемы

Простейшая первоначальная схема стенда практической работы состоит из трех сетей, правая и левая (по схеме) из которых представляют собой защищенные сегменты одной корпоративной ViPNet-сети, третья же сеть (центральная в схеме) олицетворяет собой очень упро-щенную имитацию пространства сети Интернет[1].

На начальном этапе в состав лабораторной ViPNet-сети входят сле-дующие сетевые узлы:

- Левая (по схеме) подсеть (192.168.120.0/28):
  - Незащищенный компьютер Linux1.
  - Координатор Server1 – на базе виртуальной машины CM1.
- Правая (по схеме) подсеть (192.168.80.0/29):
  - Незащищенный компьютер Linux2.
  - Координатор Server2 – на базе виртуальной машины CM2.
- Центральная (по схеме) сеть (89.175.27.0/25):

[1] С т. н. «белым» адресным пространством

– Координатор Server1 – на базе виртуальной машины СМ1.
– Координатор Server2 – на базе виртуальной машины СМ2.

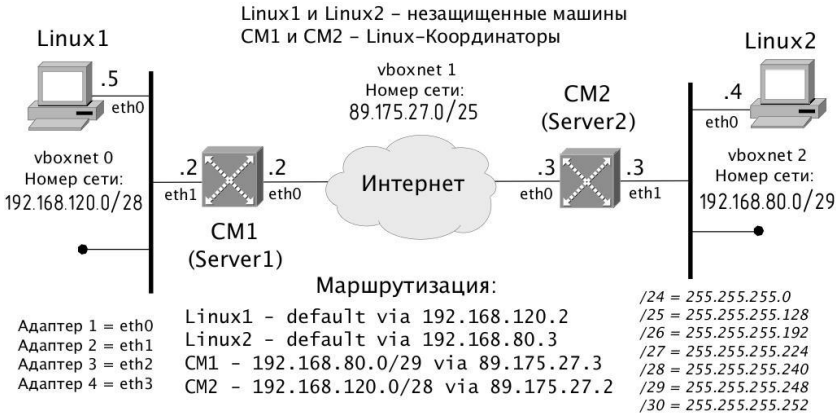

Рис. 8.1. Первоначальная схема лабораторного практикума

Примечание. Для удобства работы с схемами, встречающими-ся в описаниях практических работ, они продублированы дополнительно, в большем´ разрешении, в конце данного учебного пособия в разделе Приложения (стр. 349).

8.2. Подготовка виртуальных машин

1. В свойствах виртуальной машины (VirtualBox) добавить нужное количество сетевых интерфейсов с привязкой к определенной виртуальной сети эмулятора [2] согласно рис 8.1.
2. Включить виртуальную машину. Загрузится ОС Linux.

   В вирт. машинах Linux1 и Linux2 ОС Linux обладает графическим интерфейсом, в ОС Linux же вирт. машин СМ1 и СМ2 графический интерфейс отсутствует.

3. Настроить сетевые интерфейсы - назначение ip-адресов [3].
4. Проверить в терминале (в режиме root, su -) командой ifconfig или ip a наличие нужного количества сетевых интер-фейсов с правильно назначенными на них сетевыми адресами.

2 В ПО Virtualbox виртуальная сеть называется по-разному, для ОС Linux - vboxnet с определеным номером сети, для ОС Windows - Виртуальный адаптер хоста с определенным номером. На схеме 8.1 показано соответствие номеров виртуальных адаптеров хоста и номеров интерфейсов виртуальной машины ОС Linux на базе VirtualBox.

[3]Способ назначения сетевых адресов на интерфейсы зависит от того или иного дис-трибутива Linux, выбранного для лабораторного практикума.

5. Задать маршруты - на Linux1 и Linux2 - маршруты по умолчанию, а на будущих координаторах СМ1 и СМ2 - конкретные статические маршруты до удаленных сетей друг друга. Проверить в терминале из-под root (su -) командами route или ip r наличие вновь созданных маршрутов.

6. Проверить доступность удаленных друг от друга сетей при помо-щи ping (Linux1 ←→ Linux2).

7. На СМ1 и СМ2 в домашнем каталоге пользователя student проверить наличие каталога ViPNet Linux Install с необходимыми для практикума файлами - дистрибутивом Координатора Linux и готовыми ключевыми дистрибутивами (т. н. dst-файлами).

8. Установить Координатор Linux на СМ1 (dst-файл Server1) и СМ2 (dst-файл Server2) (см. «Установка Координатора» на стр. 254).

Внимание! Встречающиеся далее в схемах и примерах иден-тификаторы СУ могут не совпадать с реальными.

Для ALT Linux порядок настройки сетевых параметров (ip-адресов и маршрутов) в СМ1(2) может происходить следующим образом:

su - «su пробел минус» – вход в полноценный режим root.

Запуск mc (Midnight Commander)

Переход в каталог /etc/net/ifaces/eth0 (eth1)

Создание в этих каталогах пустого файла для ip-адреса с названием ipv4address и, там, где это нужно, файла для маршрута ipv4route:

Shift+F4 - создание пустого файла в mc сочетанием клавиш.

Вписать в созданный файл ip-адрес или маршрут, например:

192.168.120.2/28 (ipv4address)

192.168.80.0/29 via 89.175.27.3 (ipv4route)

или маршрут по умолчанию:

default via 89.175.27.3 (ipv4route)

F2 - сохранение и последующий ввод названия созданных файлов – ipv4address и ipv4route соответственно.

Сохранение/применение сетевых настроек:

service network restart

Проверка ip-адресов:

ifconfig либо ip a

Просмотр таблицы маршрутизации:

route либо ip r

8.3. Firewall. Фильтры по умолчанию

Целью данного задания является изучение особенностей прохождения сетевого трафика с умолчательными правилами фильтрации на Координаторах Linux.

Выяснить, какие виды трафика по умолчанию разрешены в схеме.

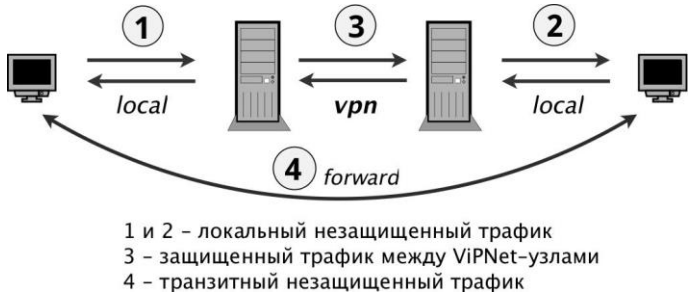

Рис. 8.2. Виды трафика в лабораторной схеме.

Внимание! В Координаторах 4.* понятие режима безопасности и его настройка в явном виде отсутствуют.

Примечание. Все действия по запуску команд управления и редактированию конфигурационных файлов Координатора следует производить в режиме root.
Все изменения настроек в режиме vipnet shell производят-ся в режиме администратора узла ViPNet или администрато-ра сети ViPNet. Для этого потребуется ввод соответству-ющего пароля после входа в vipnet shell и выполнения ко-манды enable (подробнее об этом см. на стр. 268).

Остановка службы iplir:

```
iplir stop
```

В файле /etc/vipnet/user/iplir.conf-eth* (для всех интерфейсов обоих координаторов) изменить следующие параметры:

```
registerall=on [4]
```

После чего следует запустить службу iplir:

```
iplir start
```

После этого следует проверить доступность узлов сети (трафики 1-4 на рис. 8.2 стр. 316) с помощью отправки пакетов icmp (ping) с последующим разбором ситуации с помощью журнала ip-пакетов.

[4] Регистрация всех типов пакетов в журнале ip-пакетов на данном интерфейсе.

8.4. Фильтрация незащищенного локального трафика

Цель задания - разрешение прохождения в обоих направлениях локального незащищенного трафика между компьютерами (незащищенными узлами) и координаторами Linux (трафики 1 и 2).

vipnet shell

На Server1 в командном интерпретаторе выполнить

команду enable для входа в режим администратора (см. стр. 268) и далее:

```
firewall local add src 192.168.120.5 dst 192.168.120.2 tcp dport 22 pass
```

или

```
firewall local add src 192.168.120.5 dst 192.168.120.2 service @SSH pass firewall local add src 192.168.120.5 dst @local tcp dport 8080 pass
```

Внимание! tcp dport 22 = service @SSH [5]

192.168.120.2 (локальный ip-адрес Server1) = @local

Выполнить аналогичную настройку и на Server2

После вышеуказанных настроек следует проверить прохождение трафиков 1 и 2 (рис. 8.2 стр. 316):

Проверить доступность Linux1 ↔ Server1 и Linux2 ↔ Server2 с помощью ping, с помощью ssh.

Попробовать подсоединиться к Координатору по веб-интерфейсу для изучения последнего. Для этого на Linux1/Linux2 в адресной строке браузера Firefox следует ввести ip-адрес Координатора и порт 8080:

```
192.168.120.2:8080
```

Проверить также доступность друг другу узлов Linux1 ↔ Linux2.

Просмотр пакетов в журнале ip-пакетов – iplir view

Сделать выводы.

> СОВЕТ. Если какое-либо правило разрешения|запрета соединения не срабатывает, то следует выяснить номера пользовательского и умолчательного правил. Затем переместить созданное правило вы-ше умолчательного.

Переместить созданное правило выше умолчательного можно спе-циальной командой, например:

```
firewall vpn move rule 20 to 13
```

[5] См. список сервисов firewall.

8.5. Фильтрация незащищенного транзитного трафика

Цель задания - разрешение прохождения в обоих направлениях транзитного незащищенного трафика между удаленными компьютерами (незащищенными узлами) Linux1 и Linux2 (трафик 4).

Проверить доступность удаленных друг от друга сетей (транзитный трафик).

В командном интерпретаторе vipnet shell :

firewall forward show - просмотр умолчательных правил тран-зитного трафика.

Создание собственных ip-объектов для своих и удаленных незащи-щенных узлов:

```
firewall ip-object add name @myhosts 192.168.120.5 firewall ip-object add
name @others 192.168.80.4
```

firewall ip-object show - просмотр созданных объектов

Разрешить незащищенный транзитный трафик:

```
firewall forward add src @myhosts dst @any pass firewall forward add src
@others dst @myhosts pass
```

firewall forward show - просмотр созданных правил транзитного незащищенного трафика.

Выполнить аналогичную настройку и на Server2

Проверить доступность Linux1 и Linux2 (ping)

С помощью журнала ip-пакетов iplir view следует убедиться, что между незащищенными узлами Linux1 и Linux2 действительно разрешен именно транзитный незащищенный трафик.

Выяснить, каким флагом пакета обозначается этот тип трафика в журнале ip-пакетов.

8.6. Настройка антиспуфинга

Цель задания - включение и проверка фильтра антиспуфинга (о том, что такое антиспуфинг – см. стр. 166).

В командном интерпретаторе vipnet shell :

iplir option get antispoofing - просмотр умолчательного состояния антиспуфинга.

iplir option set antispoofing on - включение.
iplir option get antispoofing - проверка.

Выполнить аналогичную настройку и на Server2

Проверить доступность Linux1 ↔ Linux2 (трафик 4, рис. 8.2 стр. 316).
Проанализировать данные журнала ip-пакетов:
iplir view.

Сделать выводы.