8.7. Настройка трансляции сетевых адресов

Цель задания - настройка трансляции сетевых адресов (NAT), а точнее, PAT[6].

В командном интерпретаторе vipnet shell выполнить команду:

```
firewall nat add 1 src @myhosts dst @any change src 89.175.27.2
```

Выполнить аналогичную настройку и на Server2

Проверить доступность незащищенных узлов Linux1 ↔ Linux2 - выяснить, сработала ли настройка PAT, повлияло ли это на трафик 4 (рис. 8.2 стр. 316).

Если трафик 4 перестал ходить, то для выяснения причин его отсутствия следует обратиться к журналу ip-пакетов и получить ответы на следующие вопросы:

- На каком координаторе блокируются пакеты трафика 4?
- На каком интерфейсе координатора блокируются пакеты тра-фика 4?
- Какое направление движения трафика на интерфейсе координатора, где блокируется трафик 4?
- Какие именно ip-пакеты блокируются?
- Какое событие (event) описывает в журнале блокировку пакетов трафика 4?

На основании анализа ответов на вышеперечисленные пункты сле-дует ответить на главный вопрос:

В какое правило какого фильтра следует внести изменения для возобновления трафика 4?

---

6 См. «Понятие NAT», стр. 167

8.8. Фильтрация защищенного трафика

Цель задания - демонстрация некоторых возможностей рабо-ты драйвера iplir по фильтрации т. н. «защищенного» трафика 3 (рис. 8.2 стр. 316) между ViPNet-узлами, которыми в лабора-торной схеме на данном этапе являются координаторы Server1 и Server2.

Для выполнения задания потребуется:

- Сменить на координаторах имена узлов (hostname).
- Проверить, включен ли автозапуск службы ssh-сервера на координаторах при старте ОС Linux, включить её и запустить.

Подготовка ОС Linux - смена имени компьютера

Сменить на Координаторах имена компьютеров (hostname):

На СМ1 - Server1;

На СМ2 - Server2.

Образец команд для смены имени (в режиме root):

hostname Server1 – задание нового hostname;

exit – выход из оболочки root;

su – вход в оболочку root.

После чего в этом конкретном окне терминала в приглашении командной строки имя хоста сменится на Server1[7].

Подготовка ОС Linux - включение и запуск ssh-сервера

Для того, чтобы заходить по ssh на Координаторы, необходимо на Server1 и Server2 выполнить следующие процедуры [8]:

su - (su пробел минус) – вход в режим root;
chkconfig −−list |grep sshd – проверка включения автозагруз-ки сервера ssh;
chkconfig sshd on – включение ssh-сервера ;
service sshd start – запуск ssh-сервера и генерация ключей .

Внимание! Проверка работы связи по ssh (Server2 → Server1) должна происходить в режиме пользователя.

ssh student@89.175.27.2

[7]Смена имени узла данным способом будет действовать только в определенном окне терминал, имя узла не сохранится после перезагрузки ОС.

[8]В том случае, если в ОС Linux работает SystemV – способ начальной инициализа-ции системы.

Проверка доступности при помощи icmp (ping) Server1 → Server2 iplir view

Требуется разрешить координатору Server2 удаленно «заходить» по ssh на координатор Server1. При этом Server1 не должен иметь возможность заходить на Server2 посредством ssh. Любой другой защищенный трафик между этими СУ также разрешается.

Для этого в командном интерпретаторе vipnet shell :

```
firewall vpn add src [ID Server2] dst @local tcp dport 22 pass
```

firewall vpn show – проверка создания правила фильтрации защищенного трафика.

Проверить работу этого правила можно командой, запущенной с соседнего координатора Server2, чей ssh-трафик был разрешен выше:

ssh student@89.175.27.2

После этого следует проконтролировать прохождение пакетов ssh с помощью журнала ip-пакетов – iplir view.

Примечание. В том случае, если с Server2 по-прежнему не получается зайти на Server1 по протоколу ssh, следует изучить показания журналов ip-пакетов (iplir view) обо-их координаторов, отследив прохождение пакетов, начиная с Server2. Необходимо выяснить причину и ответить на вопрос
– что еще потребуется сделать для успешного выполнения этого задания?

СОВЕТ. Необходимо вспомнить результаты, полученные в практической работе по изучению правил фильтрации по умолчанию в firewall Координатора Linux 4 (см. стр. 316).

Дополнительное задание

1. Добавить новые виртуальные машины WinXP1 и WinXP2.

   Для этого проследить, чтобы сетевые интерфейсы соответствовали нужным значениям виртуальных сетей эмулятора (vmnet,

vboxnet, виртуальный адаптер хоста) согласно новой схеме лабораторной сети (рис. 8.3).

2. Изменить на Win1 и Win2 сетевые настройки и добавить шлюз по умолчанию.
3. Включить новые незащищенные узлы Win1 и Win2 во все существующие правила фильтрации незащищенного трафика на коор-динаторах (группа команд firewall).