8.9. Туннелирование незащищенных узлов

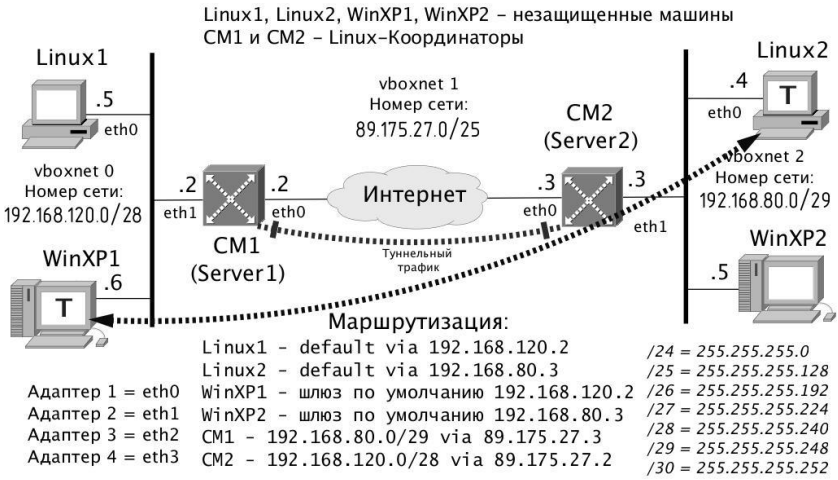

Рис. 8.3. Схема туннельных соединений

Цель задания - создать защищенное туннельное соединение на участке центральной сети («Интернет») (Server1 ⟷ Server2, см. рис. 8.3) между незащищенными узлами WinXP1 и Linux2. Трафик между двумя другими незащищенными компьютерами пока оста-нется незашифрованным на всем протяжении пути от Linux1 ⟷ WinXP2.

Следует проверить, существует ли по умолчанию правило фильтра-ции, разрешающее весь туннельный трафик:

```
firewall tunnel show
```

Настройки туннелируемых ресурсов WinXP1 и Linux2 будут выглядеть следующим образом:

В файле iplir.conf (Server 1)

```
[id] - своя секция, первая
tunnel= 192.168.120.6-192.168.120.6 to 192.168.120.6-192.168.120.6

[id] - секция для соседнего Server 2
tunnel= 192.168.80.4-192.168.80.4 to 192.168.80.4-192.168.80.4
```

В файле iplir.conf (Server 2)

```
[id] - своя секция, первая
```

```
tunnel= 192.168.80.4-192.168.80.4 to 192.168.80.4-192.168.80.4

[id] - секция для соседнего Server 1
tunnel= 192.168.120.6-192.168.120.6 to 192.168.120.6-192.168.120.6
```

Проверка правильности выполнения задания осуществляется при помощи icmp (ping) между WinXP1 ←→ Linux2 (туннельный защищенный трафик).

Одновременно с этим следует проверить доступность узлов Linux1 ↔ WinXP2 (незащищенный трафик).

Анализировать трафик в журнале ip-пакетов iplir view и по вы-воду команды iplir info.

Убедиться, что на участке между координаторами проходят оба ти-па трафика одновременно.

Проверить доступность узлов Linux2 ↔ Linux1, а также Win XP1 ↔ WinXP2. Туннелируемый узел будет «пинговать» незащи-щенную машину, а та, в свою очередь, туннелируемую - нет.

8.10. Фильтрация туннельного трафика

Цель задания - выполнить фильтрацию туннельного трафика таким образом, чтобы работало только защищенное соединение с узла Linux2 на WinXP1 по протоколу rdp (Удаленный Рабочий стол, tcp:3389). Любое другое взаимодействие между этими туннелируемыми ресурсами должно быть запрещено.

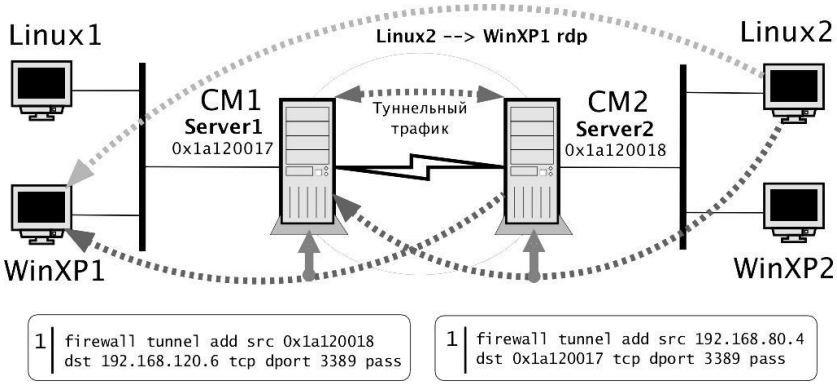

Рис. 8.4. Принцип создания правил фильтрации туннельного трафика между Linux2 ↔ WinXP1

Linux2 → WinXP1 по rdp (tcp:3389)

Для этого достаточно создать правила фильтрации на обоих коор-динаторах Server1 и Server2.

Правила фильтрации туннельного трафика по умолчанию в секции firewall tunnel удалить! Это можно сделать либо командой:

firewall tunnel delete [номер правила]

либо (предпочтительнее) временно отключить эти правила с помощью веб-интерфейса Координатора.

На Server 2:

```
firewall tunnel add src 192.168.80.4 dst 0x1a120017 tcp dport 3389 pass
```

На Server 1:

```
firewall tunnel add src 0x1a120018 dst 192.168.120.6 tcp dport 3389 pass
```

В том случае, если помимо частного правила фильтрации не будет указано глобальное правило, указывающее, что делать с пакетами, не подходящими под параметры частного правила – такие пакеты будут «отброшены», запрещены.

> Иными словами, что явно не разрешено конкретными правилами – будет запрещено

В WinXP1 разрешить удаленный доступ к рабочему столу (Мой Компьютер → Свойства → Удаленные сеансы)

В Linux2 в терминале выполнить команду из-под пользователя:

```
rdesktop -k en-us 192.168.120.6 &
```

Проверить доступность:

Linux2 −→ WinXP1 по rdp
Linux2 ←−→ WinXP1 ping
WinXP1 ←−→ WinXP2 ping,rdp
Linux1 ←−→ Linux2 ping
Linux1 ←−→ WinXP2 ping

С помощью журнала ip-пакетов iplir view убедиться в том, что запрещен любой туннельный трафик кроме соединения туннелируемых ресурсов Linux2 с WinXP1 по прикладному протоколу rdp.

> В качестве дополнительного задания рекомендуется заменить правила фильтрации туннельного трафика на новые, с использованием групп объектов @tunneledip и @RDP.

По итогам работы сделать соответствующие выводы.

Дополнительное задание

Сделать оставшиеся незащищенные машины туннелируемыми ресурсами (Linux1 и WinXP2).

1. Правила в секции firewall tunnel , оставшиеся с предыдущей работы отключить в веб-интерфейсах обоих координаторов.

2. Вернуть правило фильтрации по умолчанию:

firewall tunnel add src @any dst @any pass

либо активировать их посредством веб-интерфейса.

С помощью ping и журнала ip-пакетов iplir view убедиться в том, что теперь любой трафик, проходящий на центральном участке схемы (между Координаторами), является зашифрованным.

Сделать выводы.

Самостоятельное задание

1. Linux2 → Linux1 - ssh
2. WinXP1 → WinXP2 - rdp
3. Linux1 9 Server2 - ssh
4. Linux1 → Server1 - ssh
5. Linux2 → Server2 - ssh
6. ping разрешить там, где это возможно (локальный и туннельный трафики).

Для того, чтобы заходить по ssh на узел с ОС Linux, необходимо на этом узле выполнить следующие процедуры по активации ssh-сервера:

su - вход в режим root
chkconfig sshd on - включение ssh-сервера
service sshd start - старт ssh-сервера и генерация ключей chkconfig –list |grep sshd - проверка состояния ssh-сервера

ssh X.X.X.X - вход по ssh на устройство с адресом X.X.X.X

rdp = tcp:3389
ssh = tcp:22
ping = icmp
proto = any, tcp, udp, icmp

Вход по rdp (Удаленный рабочий стол) на устройство с адресом X.X.X.X осуществляется командой

rdesktop -k en-us X.X.X.X &

8.11. Настройка полутуннеля

Цель задания - установка защищенных соединений между подсетями сети ViPNet[9], в одной из которых находятся ViPNet-клиент WinXP1 и туннелируемый узел Linux1, в другой - туннелируемый узел Linux2 и ViPNet-клиент WinXP2.

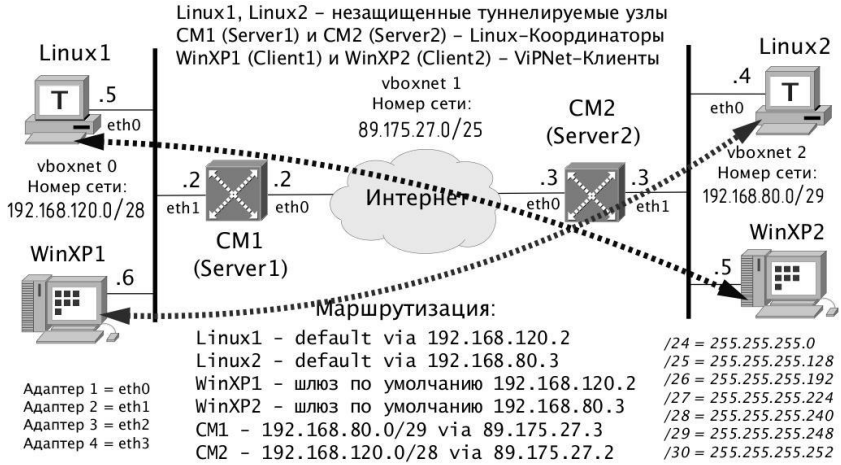

Рис. 8.5. Схема полутуннеля между Клиентами WinXP1(2) и туннелируемыми ресурсами Linux1(2)

1. Восстановить туннельные фильтры по умолчанию в секции firewall tunnel .
2. Исключить из настроек туннелируемых ресурсов (параметр tunnel в iplir.conf) ip-адреса узлов WinXP1 и WinXP2.
3. На WinXP1(2) установить ViPNet Client 3.2 или 4.3.2 .
4. Произвести для ViPNet Client на WinXP1 и WinXP2 первичную инициализацию с dst-файлами Client1 и Client2.
5. В Client Monitor WinXP1 в списке защищенной сети выде-лить Координатор Server2 и двойным щелчком запустить его настройки. Во вкладке Туннель прописываем адрес туннелируемого ресурса Linux2.
6. В Client Monitor WinXP2 в списке защищенной сети выде-лить Координатор Server1 и двойным щелчком запустить его

[9] На участке сети, имитирующем Интернет.

настройки. Во вкладке Туннель прописываем адрес туннелируе-мого ресурса Linux1.

7. Внимание! Этот пункт только для Клиентов 3.2. Первона-чально в свойствах клиентов (раздел Сервис → Настройки → Защищенная сеть) выставить Автономный режим работы (без координатора) (отключить настройку « Межсетевой экран»). В дальнейшем можно попробовать настройку « Межсетевой экран» тип Координатор.

8. Проверка[10] доступности vpn-узлов каждому из Клиентов.

9. Запустить icmp-трафик между WinXP1 и Linux2.

10. Запустить icmp-трафик между WinXP2 и Linux1.

11. Изучить выводы журнала ip-пакетов iplir view на обоих коор-динаторах (результаты отфильтровать по интерфейсу eth0). Убе-диться в работоспособности полутуннелей лабораторной схемы.

12. Отправка-получение файлов по Файловому обмену и одновре-менный просмотр на Координаторах очереди mftp-пакетов с по-мощью команды mftp info.