Лабораторная работа №5. Работа с протоколом TelNet и SSH в Cisco Packet Tracer.

Цель работы: построить схему сети с протоколом TelNet и SSH в Cisco Packet Tracer.

Теоретический материал:

Списки доступа позволяют создавать правила управления трафиком, по которым будет происходить межсетевое взаимодействие как в локальных, так и в корпоративных сетях.Существует шестнадцать типов списков доступа, но наиболее часто используются два типа: **standart** – стандартные (номера с 1 по 99) и **extended** – расширенные (номера с 100 по 199 или с 2000 по 2699). Различия между этими двумя списками заключаются в возможности фильтровать пакеты не только по IP – адресу, но и по другим различным параметрам. Стандартные списки обрабатывают только входящие IP адреса источников, т.е. ищут соответствие только по IP адресу отправителя. Расширенные списки работают со всеми адресами корпоративной сети и дополнительно могут фильтровать трафик по портам и протоколам. Работа списка доступа напрямую зависит от порядка следования строк в этом списке, где в каждой строке записано правило обработки трафика. Просматриваются все правила списка с первого до последнего по порядку, но просмотр завершается, как только было найдено первое соответствие, т.е. для пришедшего пакета было найдено правило, под которое он подпадает. После этого остальные правила списка игнорируются. Если пакет не подпал ни под одно из правил, то включается правило по умолчанию: **access-list номер_списка deny any** которое запрещает весь трафик по тому интерфейсу сетевого устройства, к которому данный список был применен.
Для того, чтобы начать использовать список доступа, необходимо выполнить следующие три этапа:

1 – создать список;
2 – наполнить список правилами обработки трафика;
3 – применить список доступа к интерфейсу устройства на вход или на выход этого интерфейса.

Этап первый – создание списка доступа:
Стандартный список:
Switch3(config)#**ip access-list standart 10**
(создается стандартный список доступа под номером 10, в данном случае создается на коммутаторе)
Расширенный список:
Router1(config)#**ip access-list extended 100**
89 (создается расширенный список доступа под номером 100, в данном случае создается на маршрутизаторе).

Этап второй – ввод правил в список доступа:
Каждое, правило в списке доступа сдержит три важных элемента:
1 - число, идентифицирующее список при обращении к нему в других частях конфигурации маршрутизатора или коммутатора третьего уровня;

2 - инструкцию **deny** (запретить) или **permit** (разрешить);
3 - идентификатор пакета, который задается по одному из трех вариантов:
- адрес сети (например 192.168.2.0 0.0.0.255) – где вместо маски подсети указывается шаблон маски подсети;
- адрес хоста (host 192.168.2.1);
- любой IP адрес (**any**).
Пример стандартного списка доступа №10:
access-list 10 deny host 11.0.0.5
access-list 10 deny 12.0.0.0 0.255.255.255
access-list 10 permit any
В этом списке:
- запрещен весь трафик хосту с IP адресом 11.0.0.5;
- запрещен весь трафик в сети 12.0.0.0/8 (в правиле указывается не реальная маска подсети, а ее шаблон);
- весь остальной трафик разрешен.

В расширенных списках доступа вслед за указанием действия ключами permit или deny должен находиться параметр с обозначением протокола (возможны протоколы IP, TCP, UDP, ICMP), который указывает, должна ли выполняться проверка всех пакетов IP или только пакетов с заголовками ICMP, TCP или UDP. Если проверке подлежат номера портов TCP или UDP, то должен быть указан протокол TCP или UDP (службы FTP и WEB используют протокол TCP).

При создании расширенных списков в правилах доступа можно включатьфильтрацию трафика по протоколам и портам. Для указания портов в правиле доступа указываются следующие обозначения (таблица 10.1):

Таблица 10.1.

обозначение	действие
lt n	Все номера портов, меньшие n.
gt n	Все номера портов, большие n.
eq n	Порт n
neq n	Все порты, за исключением n.
range n m	Все порты от n до m включительно.

Распространенные приложения и соответствующие им стандартные номера портов приведены в следующей таблице 10.2:

Таблица 10.2.

Номер порта	Протокол	Приложение	Ключевое слово в команде access_list
20	TCP	FTP	data ftp_data
21	TCP	Управление сервером FTP	ftp
22	TCP	SSH	
23	TCP	Telnet	telnet
25	TCP	SMTP	Smtp
53	UDP, TCP	DNS	Domain
67, 68	UDP	DHCP	nameserver
69	UDP	TFTP	Tftp
80	TCP	HTTP (WWW)	www
110	TCP	POP3	pop3
161	UDP	SNMP	Snmp

Пример расширенного списка доступа №111:

! Запретить трафик на порту 80 (www-трафик)
ip access-list 111 deny tcp any any eq 80
ip access-list 111 deny ip host 10.0.0.15 host 12.0.0.5
ip access-list 111 permit ip any any
interface ethernetO
! Применить список доступа 111 к исходящему трафику
ip access-group 111 out

В этом списке внешние узлы не смогут обращаться на сайты внутренней сети, т.к. список доступа был применен на выход (для внешних узлов) интерфейса, а так же узлу 10.0.0.15 запрещен доступ к узлу 12.0.0.5. Остальной трафик разрешен.
Этап третий – применение списка доступа.
Списки доступа могут быть использованы для двух типов устройств:
1 – на маршрутизаторе;
2 - на коммутаторе третьего уровня.
На каждом интерфейсе может быть включено два списка доступа: только один список доступа для входящих пакетов и только один список для исходящих пакетов.

Каждый список работает только с тем интерфейсом, на который он был применен и не действует на остальные интерфейсы устройства, если он там не применялся. Однако один список доступа может быть применен к разным интерфейсам. Применение списка доступа к устройству осуществляется следующими командами:

interface ethernet0/0/0
ip access-group 1 in
ip access-group 2 out

В данном случае к интерфейсу ethernet0/0/0 применили два списка доступа:
список доступа №1 – на вход интерфейса (т.е. для внутренних адресов);
список доступа №2 – на выход интерфейса (применение к внешней сети).
Чтобы просмотреть все созданные списки доступа и применение их к интерфейсам устройства используйте следующие команды:
Команда просмотра списков доступа:
Router# **Sh access-list**
Просмотр текущей конфигурации устройства и привязки списков к интерфейсам:
Router# **Show running-config**
Просмотр сохраненной конфигурации:
Router# **Show configuration**
Сохранение текущей конфигурации:
Router# **write memory**
Или
Router# **copy run start**
Команда удаления списка доступа:
interface ethernet0/0/0 - выбор нужного интерфейса
no access-list номер_списка – удаление списка в выбранном интерфейсе

Практическая часть:

Создайте схему сети, как показано на рис.1.

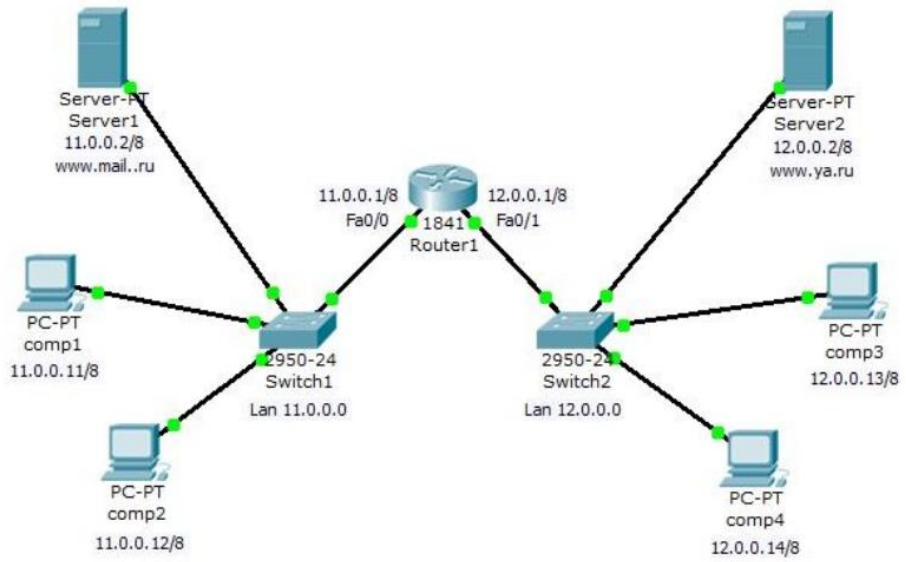

Рис.1. Схема корпоративной сети.

Задача:
1 - Компьютеры comp1 и comp2 должны открывать все сайты, но им запрещено
входить на компьютеры comp3 и comp4.
2 - Компьютеры comp3 и comp4 доступны друг для друга и должны открывать
только сайт своей сети, сеть 11.0.0.0 для них недоступна.
Создадим стандартный список доступа, где укажем правила блокировки на хосты comp3 и comp4 и применим этот список на выход интерфейса Fa0/0.
Включите привилегированный режим и войдите в конфигурацию роутера:

```
Router1>en
Router1#conf t
```

Создадим стандартный список доступа и введем правила доступа:

```
Router1(config)#ip access-list standard 10
Router1(config-std-nacl)#deny host 12.0.0.13
Router1(config-std-nacl)#deny host 12.0.0.14
Router1(config-std-nacl)#permit any
```


Здесь мы разрешили весь трафик, за исключением двух адресов: 12.0.0.13 и 12.0.0.14.
Просмотрим созданный список доступа в настройках роутера. Для этого надо выйти из режима конфигурации роутера и ввести команду просмотра списков
на устройстве `sh access-list`:

```
Router1#sh access-list
Standard IP access list 10
deny host 12.0.0.13
deny host 12.0.0.14
permit any
Router1#
```

Применим созданный список на выход интерфейса Fa0/0:

```
Router1#
Router1#conf t
Router1(config)#interface fa0/0
Router1(config-if)#ip access-group 10 out
```

В результете того, что список доступа был применен к выходу интерфейса сети
11.0.0.0 мы получили следующую политику доступа:

1 – пакеты, входящие на роутер из сети 11.0.0.0 получают блокировку на два внешних адреса – 12.0.0.13 и 12.0.0.14;
2 – всем внешним пакетам, входящим из роутера в сеть 11.0.0.0 разрешается все, кроме двух адресов - 12.0.0.13 и 12.0.0.14 (этим адресам запрещен вход в сеть 11.0.0.0)
Просмотрим привязку списка доступа к интерфейсу Fa0/0 в конфигурации роутера:

```
Router1(config-if)#exit
Router1(config)#exit
Router1#
Router1#sh running-config
```

Используя данную команду, вы увидите полную конфигурацию роутера, в том
числе и привязку списка доступа к конкретному интерфейсу (в данном случае
на выход интрфейса):

```
interface FastEthernet0/0
ip address 11.0.0.1 255.0.0.0
ip access-group 10 out
duplex auto
```



```
speed auto
!
```

Проверьте созданную политику доступа к ресурсам сети. Должны выполняться
следующие правила:
1 - компьютеры comp3 и comp4 доступны друг для друга и должны открывать
только сайт своей сети, вход в сеть 11.0.0.0 им заблокирован;
2 – сервера Server2 доступен всем ресурсам сети;
3 - компьютерам comp1 и comp2 доступны все ресурсы, кроме адресов 12.0.0.13
и 12.0.0.14.

Контрольные вопросы:

1. Какой командой можно посмотреть текущие настройки роутера?
2. Какими командами настраивается сетевой интерфейс роутера.
3. Как просмотреть конфигурационные настройки коммутатора?
4. Как определить распределение вилланов по портам коммутатора?