Практическая работа №7

ИСПОЛЬЗОВАНИЕ СПИСКОВ ДОСТУПА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНЫХ СЕТЯХ

Цель работы. Изучить способы защиты сетей и устройств от нежелательных соединений путем фильтрации траффика.

Краткие сведения из теории

Access-lists, **Access-control-lists** (**ACL**) – списки контроля доступа. Существует несколько разновидностей ACL, применяемых на маршрутизаторах и коммутаторах Cisco. ACL используются для фильтрации трафика или для определения классов трафика при применении политик. Список доступа представляет собой набор строк вида условие-действие. Строка ACL называется access-control-entry (ACE). Условием может быть соответствие пакета определенному протоколу или набору параметров. Действием может быть разрешение пакета (permit), либо запрещение (deny). Для списков доступа справедливы следующие правила:

1) Созданный список доступа не действует, пока он не применен к конкретному интерфейсу.
2) Список доступа применяется на интерфейсе в конкретном направлении – для исходящего, либо входящего трафика (inbound/outbound).
3) К интерфейсу можно применить только по одному ACL на протокол (IP), на направление (in/out).
4) Список доступа проверяется строка за строкой до первого совпадения. Оставшиеся строки игнорируются.
5) В конце любого IP ACL подразумевается запрещающее правило (implicit deny). Пакет, не попавший ни под одно условие в списке, отбрасывается, в соответствии с правилом implicit deny.
6) Рекомендуется более специфические правила указывать в начале ACL, а более общие – в конце.
7) Новые строки по умолчанию дописываются в конец списка.
8) Отдельную строку можно удалить из именованного ACL, другие ACL удаляются лишь целиком.
9) Список доступа должен иметь по крайней мере один permit, иначе он будет блокировать весь трафик.
10) Интерфейс, которому назначен несуществующий ACL не фильтрует трафик.
11) Расширенные ACL применяются как можно ближе к источнику трафика.

По способу создания списки доступа делятся на:

- стандартные;
- расширенные;
- именованные.

Стандартный ACL фильтрует трафик только по IP-адресу источника. Номер такого ACL должен быть в диапазоне от 1 до 99.

Запретить IP-адрес источника:

access-list 10 deny host 172.16.30.2

Разрешить всё:

access-list 10 permit any

Расширенный ACL фильтрует трафик по адресам источника и получателя для протоколов 3 и 4 уровня модели OSI. Номер такого ACL должен быть в диапазоне от 100 до 199.

Запретить TCP от всех на хост с портом 22:

access-list 110 deny tcp any host 172.16.30.2 eq 22

Запретить IP от сети по шаблону на всех:

access-list 110 deny ip 192.168.160.0 0.0.31.255 any

Разрешить всё:

access-list 110 permit ip any any

Именованный расширенный ACL фильтрует трафик по адресам источника и получателя для протоколов 3 и 4 уровня модели OSI, он должен иметь имя и имеется возможность удалять из него отдельные строки.

Создать список с именем INET и заполнить его тремя условиями:

Router(config)# ip access-list extended INET
Router(config-ext-nacl)#deny tcp any host 172.16.30.2 eq 22
Router(config-ext-nacl)#deny ip 192.168.160.0 0.0.31.255 any
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#end

Строки именованных списков доступа нумеруются с шагом 10 по умолчанию. Есть возможность перенумеровать ACL с другим шагом. Также можно добавлять строки с указанием их номера, тогда они попадут в указанное место, по нумерации.

Router(config)#ip access-list extended INET
Router(config-ext-nacl)#5 permit ip host 10.10.10.10 any
Router(config-ext-nacl)#223 deny ip host 1.1.1.1 any

Router(config-ext-nacl)#end

Удалить отдельную строчку из листа можно по номеру, или по полному указанию строки с префиксом «no»:

Router(config)#ip access-list extended INET
Router(config-ext-nacl)#no permit ip host 10.10.10.10 any

или так:

Router(config-ext-nacl)#no 223

Полностью удалить список доступа можно указав соответствующую команду и «no»:

Router(config)#no ip access-list extended INET

Для того, чтобы применить ACL к конкретному интерфейсу необходимо выполнить следующие команды.
Переход в режим конфигурирования:

Router#configure terminal

Переход в конфигурацию интерфейса FastEthernet 0/0:

Router(config)#interface Fast Ethernet 0/0

Применить ACL 110 на вход интерфейса:

Router(config-in)#ip access-group 110 in

Применить ACL 120 на выход интерфейса:

Router(config-in)#ip access-group 120 out

Для того, чтобы применить ACL к линиям удаленного доступа необходимо выполнить следующие команды.
Переход в режим конфигурирования:

Router#configure terminal

Переход к линиям vty с 0 по 4:

Router(config)#line vty 0 4

Применить ACL 10 на вход интерфейса:

Router(config-line)#access-class 10 in

Для того, чтобы просмотреть созданные на сетевом устройстве ACL необходимо выполнить следующую команду.

Router#show access-lists

или для демонстрации конкретного ACL с номером 10:

Router#show access-lists 10

или именем INET:

Router#show access-lists INET

Порядок выполнения работы

1 В программе Cisco Packet Tracer собрать сеть, представленную на рисунке 1. Интерфейсам сетевых устройств задать IP-адреса в соответствии с подписями на рисунке 1.

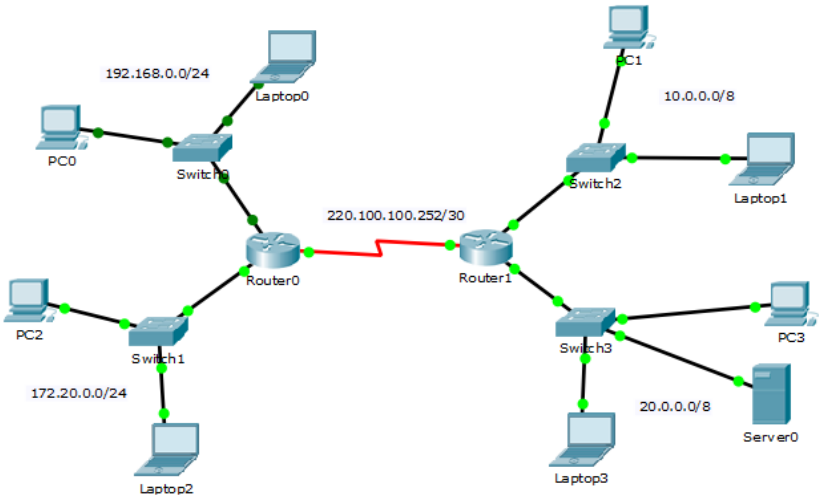

Рисунок 1 – Схема сети

2 Используя утилиту ping попарно проверить доступность всех сетей.

3 Создать на маршрутизаторах ACL и применить их к необходимым интерфейсам для следующих ситуаций:

– запретить доступ к сети 20.0.0.0/8 от компьютера с IP-адресом 192.168.0.2/24 (Laptop0 на рисунке 1);

– запретить доступ к сети 172.20.0.0/24 из сети 10.0.0.0/8 за исключением одного компьютера с IP-адресом 10.0.0.3/8 (PC1 на рисунке 1);

– запретить пересылку сообщений ICMP из сети 172.20.0.0/24.

4 Вывести ACL обоих маршрутизаторов командой **show access-lists**.

5 Используя утилиту ping проверить работу ACL.

Содержание отчета

1 Цель работы.

2 Схема сети.

3 Списки доступа обоих маршрутизаторов.

4 Результаты выполнения утилиты ping до и после применения ACL на интерфейсы маршрутизаторов.

5 Вывод по работе.

Контрольные вопросы

1 Что такое списки контроля доступа?

2 Какие правила необходимо использовать при создании ACL?

3 Классификация списков контроля доступа.

4 Как создаются стандартные ACL?

5 Как создаются расширенные ACL?

6 В чем особенности именованных ACL?