Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ Информатика и системы управления

КАФЕДРА Программное обеспечение ЭВМ и информационные технологии

Реферат
по курсу “Компьютерные сети”

Студент: Уласик Е.А.
Группа: ИУ7-71
Преподаватель: Рогозин Н. О.

2020 г.

Оглавление

Введение

Списки управления доступом (Access Control List, ACL) – одно из важнейших средств организации базовой безопасности составных и распределенных IP-сетей. Требование безопасности особенно актуально в локальных корпоративных сетях, когда они через пограничные маршрутизаторы связаны с открытой глобальной сетью Internet.

Списки доступа являются управляемыми фильтрами для проходящего трафика и при соответствующей настройке один трафик они могут беспрепятственно пропускать дальше, другой – блокировать (подавлять, отбрасывать). ACL устанавливаются на интерфейсах маршрутизаторов. Очевидным и естественным местом ACL являются интерфейсы пограничных маршрутизаторов. В результате эти маршрутизаторы становятся межсетевыми экранами или брандмаурами (firewall), подавляя непредусмотренный сетевой трафик из Internet в корпоративную сеть и наоборот и обеспечивая защиту периметра корпоративной сети.

Критерием для фильтрации могут быть значения IP-адреса отправителя и получателя проходящих пакетов сетевого уровня, имена протоколов более высокого уровня, номера TCP- и UDP-портов и др. параметры.

В целом, список доступа ACL представляет собой упорядоченный набор из одного или нескольких правил (шаблонов), используемых для сравнения с параметрами проходящих пакетов через данный интерфейс. Синтаксически отдельное правило – это одна строка. Для каждого пакета список ACL просматривается заново, последовательно, начиная с первого правила:

- если параметры пакета не совпадают с параметрами данного правила, то правило игнорируется и рассматривается следующее по порядку правило;
- если параметры пакета правилу удовлетворяют, то выполняется одно из запрограммированных в правиле действий – разрешить (ключевое слово **permit**) прохождение пакета дальше или блокировать (**deny**)

прохождение. При этом последующие правила в ACL для этого пакета уже не рассматриваются.

С целью большей безопасности в конце каждого списка ACL присутствует неотображаемое (скрытое) правило – “запретить все кроме того, что в ACL явно разрешено”.

Для идентификации конкретного ACL всем его правилам присваивается некоторый одинаковый числовой номер (так называемые “нумерованные” ACL) или символьное имя (“именованные” ACL). Номер или имя используются для ссылки на правила ACL как на единый объект. Далее рассматриваются только более распространенные нумерованные ACL.

Существует два вида списков доступа: стандартные (standard) ACL и расширенные (extended) ACL. Стандартные ACL более простые и содержат в правилах только адрес отправителя пакета, а расширенные – как адрес отправителя, так и адрес получателя, а также множество других контролируемых параметров.

Настройка списков доступа всегда состоит из двух этапов:

1. определения ACL, т.е. написания правил-шаблонов для сравнения;
2. активизации определенного ACL на заданном интерфейсе маршрутизатора. Пока второй шаг не выполнен, списки доступа никакого влияния на фильтрацию пакетов не оказывают.

1. Стандартные списки доступа

Список доступа – это список строк-правил. Каждое правило стандартного списка ACL фильтрации IP-пакетов для маршрутизаторов Cisco вводится по команде (в глобальном режиме!):

access-list *номер ACL* **deny | permit** *адрес отправителя спец. маска адреса*

где:

номер ACL – любой номер из диапазона **1…99** или **1300…1999**;

адрес отправителя – 32-битовый IP-адрес хоста или адрес подсети;

спец. маска адреса – 32-битовая маска специального для ACL вида. В этой маске цепочка нулей слева указывают на те биты *адреса отправителя*, которые должны обязательно проверяться на совпадение с этими же битами в адресе отправителя, а оставшиеся единицы маски указывают на те биты, для которых совпадение проверять не требуется.

Пара *адрес отправителя* и *спец.маска адреса* образуют адресный шаблон-правило для фильтрации проходящих пакетов через интерфейс. Если адрес отправителя пакета совпадает с адресным шаблоном, то выполняется указанное в команде действие – запретить или разрешить. Если не совпадает, то команда игнорируется и анализируется следующая по порядку команда из данного ACL. Введение специальной маски адреса позволяет гибко формировать адресный шаблон для фильтрации, как отдельных IP-адресов, так и сразу группы адресов хостов.

Команды определения списка доступа вводятся одна за другой, пока не будет сформирован весь ACL. Он может состоять и из одной команды. В конец ACL автоматически помещается неотображаемая команда:

access-list *номер ACL* **deny any**

Ранее введенные команды исправить невозможно; необходимо удалить весь ACL и ввести его заново.

Для активизации ACL его необходимо “присоединить” к желаемому интерфейсу маршрутизатора. Сначала надо войти в режим конфигурации этого интерфейса, затем выдать команду присоединения:

ip access-group *номер ACL* **in | out**

где: номер ACL - ссылка на номер активизируемого списка доступа;

in - требование фильтрации входящего (inbound) трафика;

out - фильтрация исходящего (outbound) от маршрутизатора трафика.

Для отмены фильтрации достаточно отменить команду присоединения, поставив перед ней ключевое слово **no**.

2. Расширенные списки доступа

Расширенные списки в принципе подобны стандартным, только содержат больше контролируемых параметров. Правило фильтрации IP-пакета для расширенного списка определяется следующим общим выражением:

access-list *номер ACL* **deny** | **permit** *протокол адр.шаблон отправ. адр.шаблон получат.* [*дополнит.спецификации протокола верхн.уровня*]

где: *номер ACL* – любой номер из диапазона **100…199** или **2000…2699**;

протокол – один из протоколов **tcp** (**6**), **udp** (**17**), **icmp** (**1**), **ospf** (**89**), **ip** (**0**) и некоторые другие Internet-протоколы. Можно указывать или имя протокола или его числовой код (приведен в скобках). Если правило относится к любому протоколу, то указывается протокол **ip**.

адр.шаблон отправ. и *адр.шаблон получат.* – это пары *<адрес отправителя спец. маска адреса>* и *<адрес получателя спец.маска адреса>*.

дополнительные спецификации – зависят от конкретного протокола, указанного в поле *протокол*. Для **tcp**, **udp**, **icmp** эти спецификации приведены ниже.

Проходящий пакет проверяется на совпадение со всеми параметрами, указанными в текущем правиле. При полном совпадении выполняется, как обычно, предписанное в правиле действие. Если совпадения нет хотя бы с одним параметром, то данное правило игнорируется и рассматривается следующее.

В конец ACL автоматически так же помещается неотображаемая команда:

access-list *номер ACL* **deny ip any any**

Активизация расширенного списка производится такой же командой, какой активизируется стандартный ACL.

3. Проверка списков управления доступом

Команда ***show ip interface*** отображает информацию об интерфейсах и показывает, установлены ли на них списки управления доступом.

Команда ***show access-lists*** отображает содержимое всех списков управления доступом. Если после двух указанных ключевых слов ввести имя или номер списка управления доступом в качестве параметра, то будет отображено содержимое конкретного списка ACL.

4. Практическая часть

На рисунке 1 представлена смоделированная сеть, состоящая из двух подсетей:

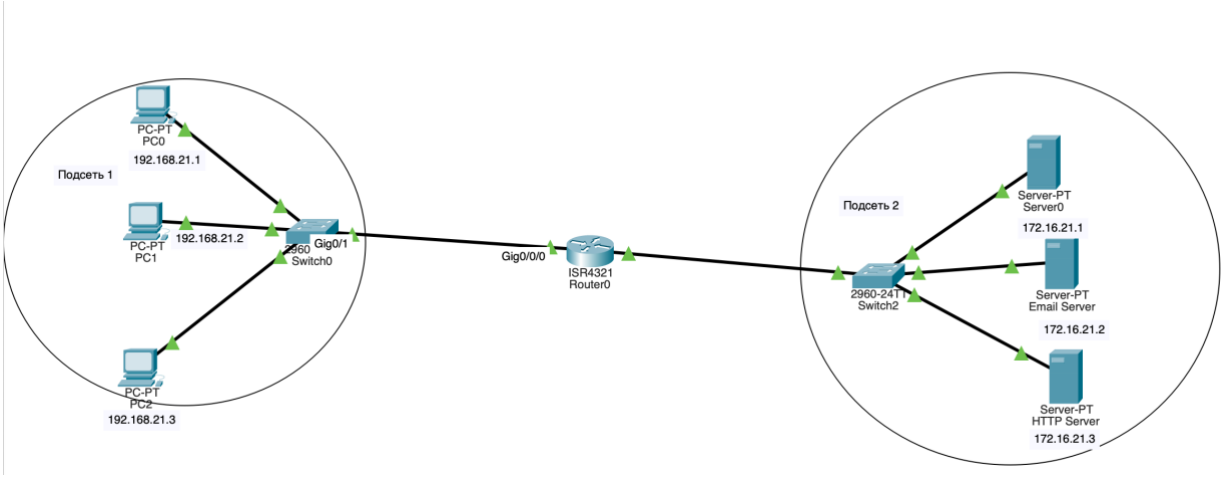

Рисунок 1. Смоделированная сеть

Пример стандартного нумерованного ACL, который запрещает хосту 192.168.21.1 доступ в сегмент сервера, но разрешает всем остальным:

```
Router(config)#access-list 1 deny 192.168.21.1
Router(config)#
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip access-group 1 in
Router(config-if)#ip access-group 1 out
Router(config-if)#exit
Router(config)#access-list 1 permit any
Router(config)#
```

Рисунок 2. Установка ACL правила

Теперь доступ во вторую подсеть с 192.168.21.1 ограничен. Остальные компьютеры доступ в другую подсеть имеют.

Пример расширенного правила ACL, которое запрещает хосту 192.168.21.2 отправлять http запросы в подсеть 2:

```
Router(config)#access-list 100 deny tcp host 192.168.21.2 any eq 80
Router(config)#access-list 100 permit ip 192.168.21.0 0.0.0.255 any
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip access-group 100 in
```

Рисунок 3. Пример расширенного ACL правила

Заключение

Таким образом, были рассмотрены списки управления доступом ACL, даны их определения и принцип работы. В практической части были приведены два примера использования списков управления.

Литература

1. Cisco // Настройка распространённых ACL IP URL: https://www.cisco.com/c/ru_ru/support/docs/ip/access-lists/26448-ACLsamples.html (дата обращения: 23.12.2020).