Лабораторная работа №7

Списки управления доступом ACL

Цель

- Создать список контроля доступа (ACL) для фильтрации трафика в целях безопасности и управления трафиком.

Задачи

- Настроить и применить списки управления доступом (ACL), основанные на требованиях к фильтрации сетевого трафика
- Настроить и применить списки управления доступом (ACL) для ограничения доступа по проколам telnet и SSH к маршрутизатору.
- Проверить и контролировать списки управления доступом в сетевой среде.

Исходные данные

В данной лабораторной работе учащиеся должны учитывать необходимость контроля трафика данных и фильтрации в сети, а также выработать политику для достижения данной цели.

Политика обеспечения безопасности трафика будет применена к модельной сети с использованием списков контроля доступа.

Источник	Получатель	Разрешить	Запретить	Протокол
Левая подсеть PC-PT XPC1	Правая подсеть	X		Все
Левая подсеть VLAN10	Правая подсеть		X	Все
Верхняя подсеть	Правая подсеть	X		Все
Правая подсеть	Верхняя подсеть	X		Только HTTP
Правая подсеть	Все подсети		X	ICMP
Левая подсеть VLAN10	Верхняя подсеть Server-PT 30WebServer3		X	DNS
Левая подсеть VLAN10	Верхняя подсеть Server-PT 30WebServer3	X		FTP HTTP
Левая подсеть VLAN20	Верхняя подсеть Server-PT 30WebServer3	X		DNS HTTP
Левая подсеть VLAN20	Верхняя подсеть Server-PT 30WebServer3		X	FTP
Верхняя подсеть	Все подсети	X		Все

Задание 1. Создание схемы сети и тестирование сетевых сервисов без списков контроля доступа.

Постройте схему в программе Packet Tracer согласно примеру и данных вашего варианта задания.

1. Откройте сохраненный проект с итоговой схемой предыдущей лабораторной работы.

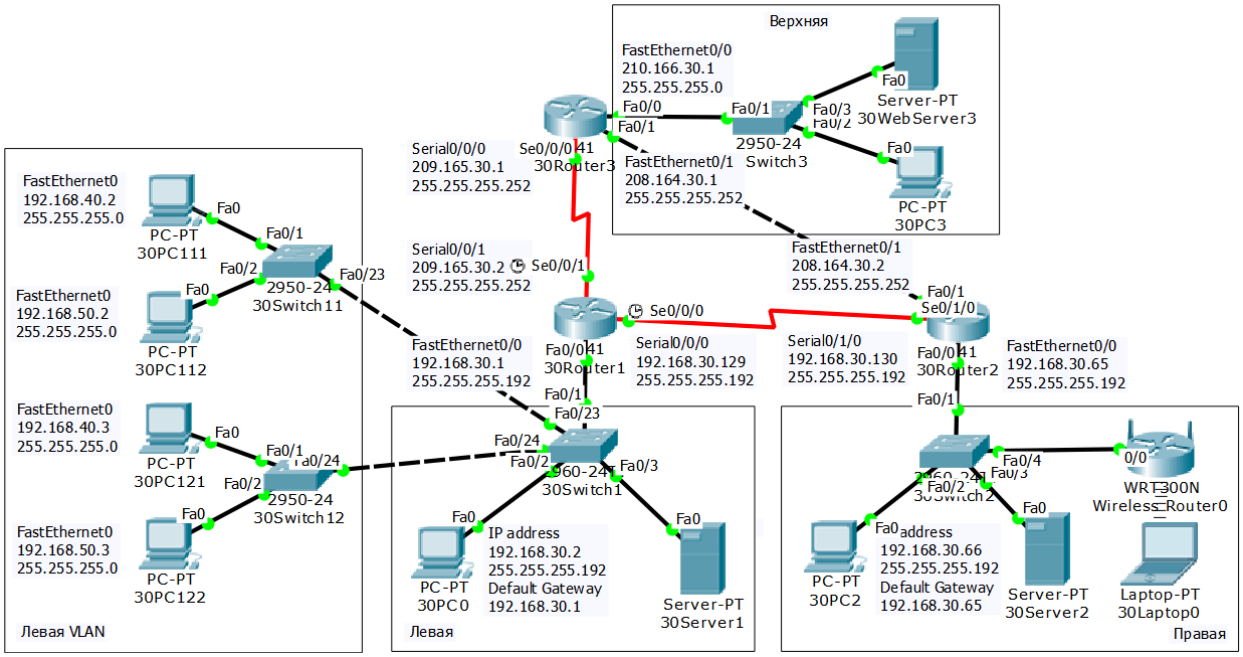
2. Настройте сервер XWebServer3 в качестве HTTP, DNS, FTP сервера.

3. Укажите на всех узлах в качестве DNS сервера XWebServer3.

4. Убедитесь, что все функционирует верно, и эхо-запросы проходят между всеми устройствами из различных сетей.

5. Убедитесь, что со всех компьютеров возможен доступ к веб-серверу по доменному имени www.cisco.com, со всех узлов возможно подключение к серверу XWebServer3 по протоколу ftp, а также со всех узлов возможен доступ к маршрутизаторам по протоколу telnet.

Если какое-либо соединений было неудачным, выполните диагностику неисправностей сети и настроек и установите каждый тип соединения с каждого узла.



Задание 2. Разработка и создание списка контроля доступа.

1. Проверьте и примените рекомендуемые правила списков контроля доступа.

   - Перед внедрением всегда тщательно планируйте.
   - Последовательность утверждений очень важна. Поместите более конкретные утверждения в начало, а более общие в конец.
   - Утверждения добавляются в конец списка контроля доступа по мере их написания.
   - Создайте и измените списки контроля доступа с помощью текстового редактора, затем сохраните файл.
   - По возможности используйте именованные списки контроля доступа.

- Используйте комментарии (параметр remark) в списках контроля доступа, для документирования цели утверждений.
- Чтобы списки контроля доступа вступили в силу, их необходимо применить к интерфейсу.
- Интерфейс может иметь один список контроля доступа на каждый протокол сетевого уровня, в каждом направлении.
- Несмотря на то, что в конце каждого списка контроля доступа содержится неявное утверждение deny any, рекомендуется настроить это утверждение в явном виде. Это не позволит вам забыть о том, что утверждение действует, и позволит использовать функцию регистрации соответствий данному утверждению.
- Списки контроля доступа со многими утверждениями обрабатываются дольше, что может повлиять на производительность маршрутизатора.
- Размещение списков контроля доступа:
    - Стандартный: ближе всего к пункту назначения (при наличии административного доступа на данном маршрутизаторе).
    - Расширенный: ближе всего к источнику (при наличии административного доступа на данном маршрутизаторе).

2. Рассмотрите два подхода к написанию списков контроля доступа:

    - Сначала разрешить специальный трафик, затем заблокировать общий трафик.
    - Сначала заблокировать специальный трафик, затем разрешить общий трафик.

3. Выберите один подход и запишите утверждения списка контроля доступа, удовлетворяющие требованиям данной лабораторной работы.

    После написания и применения списка контроля доступа к интерфейсу полезным будет узнать, оказали ли утверждения списка контроля доступа желаемый эффект. Количество пакетов, удовлетворяющих условиям каждого списка контроля доступа, может быть зарегистрировано посредством добавления параметра log в конце каждого утверждения.

Задание 3. Создание стандартного списка доступа для ограничения доступа к VTY.

1. Выберите маршрутизатор XRouter2.
2. Настройте линии vty 0–4 для входа в систему. В качестве пароля должно быть задано значение "ciscoX".
3. Создайте стандартный список доступа, предоставляющий доступ через Telnet только клиенту XPC3 верхней подсети. Номер списка доступа – номер варианта.
4. Примените список доступа к линиям vty с 0 по 4.
5. Проверьте на маршрутизаторе правильность настройки доступа через Telnet.
6. Сохраните конфигурацию.

Задание 4. Создание стандартных именованных списков контроля доступа

1. Выберите маршрутизатор XRouter2.
2. Создайте стандартный именованный список с именем inXRouter2.
3. Разрешите исходящий трафик только от узла XPC0 .

4. Запретите исходящий трафик из VLAN10.
5. Весь остальной трафик разрешите.

Задание 5. Создание расширенных списков контроля доступа.

1. Выберите маршрутизатор XRouter2.
2. Создайте несколько правил для расширенного списка с номером 100.
3. Разрешите только HTTP трафик от всех компьютеров правой подсети в верхнюю подсеть.
4. Явно запретите ICMP трафик из правой подсети к любым другим подсетям.
5. Выберите маршрутизатор XRouter1.
6. Создайте несколько правил для расширенного списка с номером 110.
7. Запретите UDP трафик от компьютеров VLAN10 к серверу доменных имен XWebServer3.
8. Разрешите TCP трафик по протоколам FTP и HTTP от компьютеров VLAN10 к серверу XWebServer3.
9. Создайте несколько правил для расширенного списка с номером 120.
10. Разрешите доступ по протоколам DNS и HTTP от компьютеров VLAN20 к серверу XWebServer3.
11. Запретите TCP трафик по протоколу FTP от компьютеров VLAN20 к серверу XWebServer3.
12. Заблокируйте весь остальной трафик.

Задание 6. Создание расширенных именованных списков контроля доступа.

1. Выберите маршрутизатор XRouter3.
2. Создайте расширенный именованный список с именем outXRouter3.
3. Разрешите весь исходящий трафик из верхней подсети во все другие подсети.

Задание 7. Применение списков контроля доступа.

1. Примените все списки контроля доступа к соответствующим интерфейсам маршрутизаторов.
2. В привилегированном режиме EXEC введите команду show running-configuration и подтвердите, что списки контроля доступа были настроены и применялись по мере необходимости. В случае выявления ошибок выполните перенастройку.
3. Сохраните конфигурацию.

Задание 8. Тестирование сетевых сервисов со списками контроля доступа.

Убедитесь, что все функционирует верно, отправив эхо-запросы между устройствами из различных сетей.

1. Выполните эхо-тестирование PC2 с PC1.
2. Выполните эхо-тестирование сервера XWebServer3 с PC1.
3. Зайдите на сайт www.cisco.com с PC1.
4. Задайте в адресной строке браузера PC1 IP-адрес XWebServer3.
5. Попробуйте подключиться с узла PC1 к серверу XWebServer3 по протоколу ftp.
6. Повторите все приведенные шаги для тестирования соединений с узлов PC2, PC111, PC112, PC121, PC122.

Вопросы для самопроверки

- В какой момент лучше всего разрешить специальный трафик и заблокировать общий трафик?
- В какой момент лучше всего заблокировать специальный трафик и разрешить общий трафик?
- Почему важно знать, сколько раз блокируются пакеты, совпадающие с утверждением списка контроля доступа?
- Зачем необходимо тщательное планирование и тестирование списков управления доступом?
- Каково главное ограничение стандартных ACL-списков?
- Каким образом можно проконтролировать сетевой трафик с помощью ACL-списков?
- Какое выражение по умолчанию является последним в ACL-списке?
- Что означает "out" в конце строки оператора "ip access-group"?
- Чем отличаются команды добавления ACL к конкретному интерфейсу и к VTY?
- Какие сокращения чаще всего используются для указания состояния порта?

Дополнительная информация

Основные задачи

- необходимо сконфигурировать список управления доступом в режиме глобальной конфигурации маршрутизатора;
- следует назначить номер списку управления доступом в диапазоне от 1 до 99, если требуется создать стандартный список для протокола IP;
- следует назначить номер списку управления доступом в диапазоне от 100 до 199, если требуется создать расширенный список ACL для протокола IP;
- при создании списка ACL необходимо тщательно отбирать необходимые директивы и соблюдать их логическую последовательность. В списке должны быть

указаны разрешенные IP протоколы; все данные других протоколов должны быть запрещены;

- необходимо выбрать IP протоколы, которые следует проверять; все остальные протоколы проверяться не будут. В дальнейшем для большей точности можно будет также указать порт получателя;
- после того как будет создан необходимый список контроля доступа, его следует привязать к определенному интерфейсу.

Использование шаблонов

Например, вместо использования строки

Router(config)# **accesslist 1 permit 0.0.0.0 255.255.255.255**

можно просто набрать

Router(config)# **accesslist 1 permit any**

Например, вместо строки

Router(config)# **access-list 1 permit 172.30.16.29 0.0.0.0**

можно записать

Router(config)# **access-list 1 permit host 172.30.16.29**

Синтаксис директивы стандартного списка ACL

Router(config)# **access-list** *access-list-number* {**permit** | **deny** | **remark**} **source** [*source-wildcard*] [**log**]

number	Номер списка управления доступом. Представляет собой целое десятичное число в диапазоне от 1 до 99 или от 1300 до 1999
deny	Пакету будет отказано в доступе, если он соответствует этой записи
permit	Пакету будет разрешен доступ, если он соответствует этой записи
source	Номер сети или адрес узла, с которого отправлен пакет. Устройство-отправитель можно указать двумя способами: ■ использовать 32-битовую величину в точечно-десятичном формате, состоящем из четырех частей; ■ использовать ключевое слово **any** для обозначения отправителя вместо записи `0.0.0.0 255.255.255.255`
source-wilcard	(Необязательный параметр) Инвертированная маска отправителя. Инвертированную маску устройства-отправителя можно указать двумя способами: ■ использовать 32-битовую величину в точечно-десятичном формате, состоящем из четырех частей; если какие-либо биты нужно игнорировать, в них следует записать единицы; ■ использовать ключевое слово **any** для обозначения отправителя вместо записи `0.0.0.0 255.255.255.255`

Формат команды access-list для расширенного списка ACL

Router(config)# **access-list** *access-list-number* {**permit** | **deny**} *protocol source* [*source-wildcard destination destination-wildcard*] [*operator* [*port*]]

access-list-number	Номер списка доступа. Представляет собой десятичное число в диапазоне от 100 до 199 или от 2000 до 2699

deny	Запрещает доступ, если условие выполнено
permit	Разрешает доступ, если условие выполнено
protocol	Имя или номер протокола сети Internet. В качестве параметра может использоваться одно из ключевых слов: **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **pim**, **tcp**, **udp** или целое число в диапазоне от 0 до 255, соответствующее номеру Internet-протокола. Для проверки любых Internet-протоколов (включая ICMP, TCP и UDP) следует использовать ключевое слово **ip**. Некоторые протоколы позволяют добавить уточняющие параметры в список
source	Номер сети или адрес узла, с которого отправлен пакет. Устройство-отправитель можно указать тремя способами: ■ использовать 32-битовую величину в точечно-десятичном формате, состоящем из четырех частей; ■ использовать ключевое слово **any** для обозначения любого отправителя вместо записи `0.0.0.0 255.255.255.255`;использовать ключевое слово **host** для обозначения единственного адреса отправителя вместо записи инвертированной маски в виде `0.0.0.0`
source-wildcard	Инвертированная маска отправителя. Если в какой-либо позиции маски стоит бит, равный нулю, то соответствующий бит адреса должен быть проверен; если же в какой-либо позиции бит равен единице, то соответствующий бит адреса должен быть проигнорирован. Инвертированную маску устройства-отправителя можно указать тремя способами: ■ использовать 32-битовую величину в точечно-десятичном формате, состоящем из четырех частей; биты адреса, которым соответствуют единичные биты в маске, не будут проверяться; ■ использовать ключевое слово **any** для обозначения любого отправителя вместо записи `0.0.0.0 255.255.255.255`; ■ использовать ключевое слово **host** для обозначения единственного адреса отправителя вместо записи инвертированной маски в виде `0.0.0.0`.

Port (Необязательный параметр) задает в десятичном формате номера или символьные имена TCP или UDP портов. Порт это номер в диапазоне от 0 до 65535. Символьное имя TCP порта может быть использовано только при фильтрации протокола из стека TCP. Символьное имя UDP порта может использоваться только при фильтрации UDP протоколов.

Использование именованных списков ACL

Синтаксис именованных списков управления доступом выглядит следующим образом:

ip access-list {**extended** | **standard**} *name*

Такая команда переведет устройство в режим конфигурирования именованного

списка ACL: Router(config-std-nacl)# или Router(config-ext-nacl)#

При конфигурировании именованного списка доступны следующие опции:

Router(config-std-nacl)#**permit** | **deny** {*source* [*source-wildcard*]| **any** [**log**]

или

Router(config-ext-nacl)#**permit** | **deny** *protocol source sourcewildcard* [*operator* [*port*]] *destination destinationwildcard* [*operator* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**timerange** *timerangename*]

Привязка созданного списка управления доступом к интерфейсу

Router(config)# **ip access-group** *номер списка* {**in** | **out**}

Для vty каналов используется команда **access-class** *номер списка* {**in** | **out**}