Тема: Списки доступа. Access Control List

# Этап 1 Познакомьтесь с представленными материалами

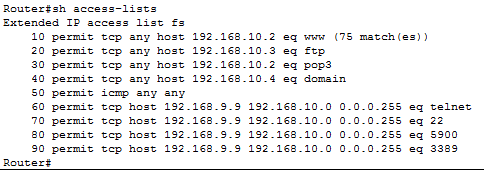
В организации ОАО “Леса Карелии” вы занимаете должность “Сетевой инженер”. Руководитель отдела информационных технологий поручил вам выбрать модель маршрутизатора удовлетворяющего новым требованиям политики безопасности. Вы выбрали модель CISCO 1941-SEC/K9. Организация приобрела маршрутизатор. Вы его установили, дополнительно сегментировали сеть. Для реализации политики безопасности принятой в организации, руководитель отдела информационных технологий поручил вам настроить списки доступа на новом оборудовании.

# Этап 2 Постановка проблемы

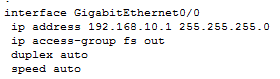
**Постановка проблемы:** в организации обновлено сетевое оборудование, но на нем не реализована политика безопасности

**Задание:** разработать списки доступа удовлетворяющие предъявленным требованиям политики безопасности:

* Разрешить доступ к web-серверу
* Разрешить доступ к ftp-серверу
* Разрешить доступ к почтовому серверу
* Разрешить доступ к dns-серверу
* Разрешить прохождение пакетов ICMP в сеть серверов
* Разрешить доступ по протоколу telnet, ssh, rdp и через программу vnc ко всем серверам с компьютера системного администратора (pc-admin).



access list fs



Применение access list fs на порту

# Теория

Источники:

[Ссылка на статью 1 (cisco.com)](http://www.cisco.com/cisco/web/support/RU/9/92/92035_confaccesslists.html#turbo)

[Ссылка на статью 2 (habr.ru)](http://habrahabr.ru/post/121806/)

ACL (Access Control List) — это набор текстовых выражений, которые что-то разрешают, либо что-то запрещают. Обычно ACL разрешает или запрещает IP-пакеты, но помимо всего прочего он может заглядывать внутрь IP-пакета, просматривать тип пакета, TCP и UDP порты. Также ACL существует для различных сетевых протоколов (IP, IPX, AppleTalk и так далее). В основном применение списков доступа рассматривают с точки зрения пакетной фильтрации, то есть пакетная фильтрация необходима в тех ситуациях, когда у вас стоит оборудование на границе Интернет и вашей частной сети и нужно отфильтровать ненужный трафик.

Вы размещаете ACL на входящем направлении и блокируете избыточные виды трафика.

ACL разделяются на два типа:

* Стандартные (Standard): могут проверять только адреса источников
* Расширенные (Extended): могут проверять адреса источников, а также адреса получателей, в случае IP ещё тип протокола и TCP/UDP порты

Стандартный список доступа

Router(config)#access-list <номер списка от 1 до 99> {permit | deny | remark} {address | any | host} [source-wildcard] [log]

* permit: *разрешить*
* deny: *запретить*
* remark: *комментарий о списке доступа*
* address: *запрещаем или разрешаем сеть*
* any: *разрешаем или запрещаем всё*
* host: *разрешаем или запрещаем хосту*
* source-wildcard: *WildCard маска сети*
* log: *включаем логгирование пакеты проходящие через данную запись ACL*

Расширенный список доступа

Router(config)#access-list <номер списка от 100 до 199> {permit | deny | remark} protocol source [source-wildcard] [operator operand] [port <порт или название протокола> [established]

* protocol source: *какой протокол будем разрешать или закрывать (ICMP, TCP, UDP, IP, OSPF и т.д)*
* deny: *запретить*
* operator:
* *A.B.C.D — адрес получателя*
* *any — любой конечный хост*
* *eq — только пакеты на этом порте*
* *gt — только пакеты с большим номером порта*
* *host — единственный конечный хост*
* *lt — только пакеты с более низким номером порта*
* *neq — только пакеты не на данном номере порта*
* *range — диапазон портов*
* port: *номер порта (TCP или UDP), можно указать имя*
* established: *разрешаем прохождение TCP-сегментов, которые являются частью уже созданной TCP-сессии*

Прикрепляем к интерфейсу

Router(config-if)#ip access-group <номер списка или имя ACL> {in | out}

* in: *входящее направление*
* out: *исходящее направление*

Именованные списки доступа

Router(config)#ip access-list {standard | extended} {<номер ACL> | <имя ACL>}

Router(config-ext-nacl)# {default | deny | exit | no | permit | remark}

* standard: *стандартный ACL*
* extended: *расширенный ACL*
* default: *установить команду в значение по умолчанию*

Схема сети организации

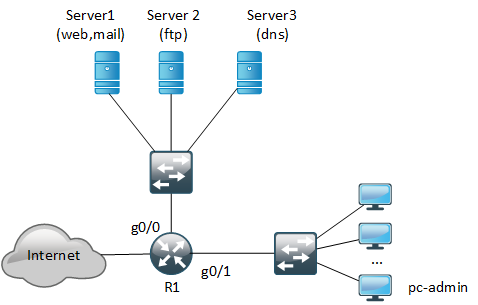


Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | Интерфейс | IP адрес | Маска | Шлюз по умолчанию |
| R1 | g0/0 | 192.168.10.1 | 255.255.255.0 | - |
| g0/1 | 192.168.9.1 | 255.255.255.0 | - |
| Server 1 | fa0 | 192.168.10.2 | 255.255.255.0 | 192.168.10.1 |
| Server 2 | fa0 | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| Server 3 | fa0 | 192.168.10.4 | 255.255.255.0 | 192.168.10.1 |
| pc-admin | fa0 | 192.168.9.9 | 255.255.255.0 | 192.168.9.1 |

# Этап 3 Резюме: обмен мнениями и принятие решения

Для того чтобы оценить разработанные списки доступа, выполните следующее:

* в программе Cisco Packet Tracer постройте сеть
* настройте основные сервисы (ftp, dns, web)
* на маршрутизаторе настройте разработанные списки доступа
* проверьте правильность списков доступа, выполняя различные действия по “обходу” списков доступа
* оцените списки доступа разработанные вашими товарищами
* по итогу работы примите решение - достаточно ли списков доступа которые вы создали, для защиты критически важных сервисов организации ОАО “Леса Карелии”.