МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

СПИСКИ УПРАВЛЕНИЯ ДОТУПОМ

Методические рекомендации по выполнению лабораторной работы №4
для студентов направления подготовки бакалавриата
10.03.01«Информационная безопасность»

Курск 2017

УДК 621.(076.1)

Составитель: А.Г. Спеваков

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» И.В. Калуцкий

Списки управления доступом [Текст] : методические рекомендации по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: А.Г. Спеваков. – Курск, 2017. – 13 с.: ил. 1. – Библиогр.: с. 13.

Содержат сведения по вопросам работы в программном продукте Cisco Packet Tracer. Указывается порядок выполнения лабораторной работы, правила содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 10.03.01 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл.печ. л. 0,76. Уч.-изд. л. 0,68. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

1 Стандартные списки доступа

Списки доступа (access lists) представляют собой общие критерии отбора, которые можно впоследствии применять при фильтрации дейтаграмм, для отбора маршрутов, определения приоритетного трафика и в других задачах.

Списки доступа, производящие отбор по IP-адресам, создаются командами access-list в режиме глобальной конфигурации, каждый список определяется номером – числом в диапазоне 0 ÷ 99 [11].

Каждая такая команда добавляет новый критерий отбора в список: router(config)#access-list <номер_списка><{deny|permit}> <IP-адрес> [маска_шаблона].

IP-адрес и маска шаблона записываются в десятично-точечной нотации, при этом в маске шаблона устанавливаются биты, значение которых в адресе следует игнорировать, остальные биты сбрасываются. При этом сетевая маска (netmask) и маска шаблона (wildcard) – это разные вещи. Например, чтобы строка списка сработала для всех узлов с адресами 1.16.124.xxx, адрес должен быть 1.16.124.0, а маска – 0.0.0.255, поскольку значения первых 24 бит жестко заданы, а значения последних 8 бит могут быть любыми. Как видно в этом случае маска шаблона является инверсией соответствующей сетевой маски. Однако маска шаблона в общем случае не связана с сетевой маской и даже может быть разрывной (содержать чередования нулей и единиц). Например, строка списка должна сработать для всех нечетных адресов в сети 1.2.3.0/24. Соответствующая комбинация адреса и маски шаблона: 1.2.3.1 0.0.0.254.

Комбинация «адрес – маска шаблона» вида 0.0.0.0 255.255.255.255 (то есть соответствующая всем возможным адресам) может быть записана в виде одного ключевого слова any. Если маска отсутствует, то речь идет об IP-адресе одного узла.

Операторы permit и deny определяют, соответственно, положительное (принять, пропустить, отправить, отобрать) или отрицательное (отбросить, отказать, игнорировать) будет принято решение при срабатывании данного критерия отбора. Например, если список используется при фильтрации дейтаграмм по адресу

источника, то эти операторы определяют, пропустить или отбросить дейтаграмму, адрес источника которой удовлетворяет комбинации «адрес – маска шаблона». Если же список применяется для идентификации какой-либо категории трафика, то оператор allow отбирает трафик в эту категорию, а deny – нет.

Список доступа представляет собой последовательность из одного и более критериев отбора, имеющих одинаковый номер списка. Последовательность критериев имеет значение: маршрутизатор просматривает их по порядку; срабатывает первый критерий, в котором обнаружено соответствие образцу; оставшаяся часть списка игнорируется. Любые новые критерии добавляются только в конец списка. Удалить критерий нельзя, можно удалить только весь список. В конце списка неявно подразумевается критерий «отказать в любом случае» (deny any) – он срабатывает, если ни одного соответствия обнаружено не было.

Для аннулирования списка доступа следует ввести команду: router(config)#no access-list <номер_списка>.

Чтобы применить список доступа для фильтрации пакетов, проходящих через определенный интерфейс, нужно в режиме конфигурации этого интерфейса ввести команду:

router(config-if)#ip access-group <номер_списка><{in|out}>.

Ключевое слово in или out определяет, будет ли список применяться к входящим или исходящим пакетам соответственно. Входящими считаются пакеты, поступающие к интерфейсу из сети.

Исходящие пакеты движутся в обратном направлении.

Только один список доступа может быть применен на конкретном интерфейсе для фильтрации входящих пакетов, и один – для исходящих. Соответственно, все необходимые критерии фильтрации должны быть сформулированы администратором внутри одного списка.

В стандартных списках доступа отбор пакетов производится по IP-адресу источника пакета.

ВЫПОЛНИТЬ!

1. Создать стандартный список доступа, разрешающий прохождения сетевых пакетов только для сетей 192.168.20.1/24 и 10.0.0.1/24. Для этого в глобальном контексте конфигурирования необходимо выполнить следующие команды:

router(config)#access-list 1 permit 192.168.20.1 0.0.0.255
router(config)#access-list 1 permit 10.0.0.1 0.0.0.255
router(config)#access-list 1 deny any any.

2. Применить созданный стандартный список доступа на вход одного из интерфейсов маршрутизатора.

3. С помощью команды ping проверить доступность компьютеров из сетей 192.168.20.1/24 и 10.0.0.1/24.

4. Аннулировать созданный стандартный список доступа.

2 Расширенные списки доступа

Кроме стандартных (standard) списков доступа существуют также расширенные (extended), имеющие большее количество параметров и предлагающие более богатые возможности для формирования критериев отбора.

Расширенные списки доступа создаются также с помощью команды access-list в режиме глобальной конфигурации, но номера этих списков лежат в диапазоне 100–199. Пример синтаксиса команды создания строки расширенного списка для контроля TCP-соединений:

router(config)#access-list<номер_списка><{deny| permit}> tcp <IP-адрес_источника> <маска_шаблона> [оператор порт[порт]]<IP-адрес_получателя> <маска_шаблона> [оператор порт[порт]] [established]

Маски шаблона для адреса источника и узла назначения определяются так же, как и в стандартных списках.

Оператор при значении порта должен иметь одно из следующих значений: lt (меньше), gt (больше), eq (равно), neq (не равно), range (диапазон включительно). После оператора следует номер порта (или два номера порта в случае оператора range), к которому этот оператор применяется.

Комбинация оператор-порт, следующая сразу же за адресом источника, относится к портам источника. Соответственно, комбинация оператор-порт, которая следует сразу же за адресом получателя, относится к портам узла-получателя. Применение этих комбинаций позволяет отбирать пакеты не только по адресам мест отправки и назначения, но и по номерам TCP- или UDP-портов.

Кроме того, ключевое слово established определяет сегменты TCP, передаваемые в состоянии установленного соединения. Это значит, что строке, в которую включен параметр established, будут соответствовать только сегменты с установленным флагом ACK (или RST).

Пример: «запретить установление соединений с помощью протокола Telnet со всеми узлами сети 22.22.22.0 netmask 255.255.255.0 со стороны всех узлов Интернета, причем в обратном направлении все соединения должны устанавливаться; остальные TCP-соединения разрешены». Фильтр устанавливается для входящих сегментов со стороны Интернета (предположим, к Интернету маршрутизатор подключен через интерфейс FastEthernet 1/0).

router(config)#access-list 101 permit tcp any 22.22.22.0 0.0.0.255 eq 23 established

router(config)#access-list 101 deny tcp any 22.22.22.0 0.0.0.255 eq 23

router(config)#access-list 101 permit ip any any

router(config)#interface FastEthernet 1/0 router(config-if)#ip access-group 101 in.

Указание ip вместо tcp в команде access-list означает «все протоколы». Отметим, что в конце каждого списка доступа подразумевается deny ip any any, поэтому в предыдущем примере мы указали permit ip any any для разрешения произвольных пакетов, не попавших под предшествующие критерии.

Расширенный список с протоколом ip позволяет также производить отбор произвольных пакетов по адресу отправителя и по адресу получателя (в стандартных списках отбор производится только по адресу отравителя).

Критерии для отбора UDP-сообщений составляются аналогично TCP, при этом вместо tcp следует указать udp, а параметр established, конечно, не применим.

ВЫПОЛНИТЬ!

5. Создать расширенный список доступа, запрещающий установление соединений с помощью протокола HTTP со всеми узлами сети 192.168.20.0 netmask 255.255.255.0 со стороны всех

узлов сети «Интернет», но разрешающий установление всех соединений в обратном направлении.

6. Применить созданный расширенный список доступа на вход одного из интерфейсов маршрутизатора.

7. Проверить работоспособность созданного расширенного списка, подключив к маршрутизатору две сети с Web-серверами и осуществив к ним поочередно запросы.

Контроль за ICMP-сообщениями может осуществляться с помощью критериев отбора типа:

router(config)#access-list<номер_списка> <{deny|permit}> icmp <IP-адрес_источника> <маска_шаблона> <IP-адрес_назначения> <маска_шаблона> [icmp-тип [icmp-код]].

Здесь icmp-тип и, если требуется уточнение, icmp-код определяют ICMP-сообщение.

Вообще, в расширенных списках можно работать с пакетами любого IP-протокола. Для этого после оператора deny/permit надо указать название протокола (ahp, esp, eigrp, gre, icmp, igmp, igrp, ipinip, ospf, tcp, udp) или его номер, которым он кодируется в поле Protocol заголовка пакета. Далее указываются адреса источника и узла назначения с масками и, возможно, дополнительные параметры, специфичные для данного протокола.

В конце команды **access-list** (расширенный) можно указать параметр log, тогда все случаи срабатывания данного критерия (то есть обнаружения пакета, соответствующего критерию), будут протоколироваться на консоль или как указано командой **logging**. После того, как протоколируется первый случай срабатывания, дальше сообщения посылаются каждые 5 минут с указанием числа срабатываний за отчетный период.

Просмотр имеющихся списков доступа (с указыванием числа срабатываний каждого критерия):

router#show access-lists.

ВЫПОЛНИТЬ!

8. Просмотреть число срабатываний каждого критерия из созданного списка доступа.

Более подробную статистику работы списков доступа можно получить, включив режим ip accounting. Режим включается в контексте конфигурирования интерфейса. Следующая команда включает режим учета случаев нарушения (то есть, пакетов, которые не были пропущены списком доступа на данном интерфейсе):

router(config-if)#ip accounting access-violations.

ВЫПОЛНИТЬ!

9. Включить учет случаев нарушения списка доступа.

Просмотр накопленной статистики (с указанием адресов отправителей и получателей пакетов):

router#show ip accounting access-violations.

При конфигурировании запрещающих фильтров (в конце которых подразумевается deny all) администратор должен не забыть оставить «дверь» для сообщений протоколов маршрутизации, если они используются на конфигурируемом интерфейсе.

ВЫПОЛНИТЬ!

10. Выполнить несколько запросов к Web-серверам.
11. Просмотреть результаты работы команды **ping**.
12. Вывести на консоль накопленную статистику по учету случаев нарушений.
13. Аннулировать созданный расширенный список доступа.

3 Динамические обратные списки доступа

Недостатком списков доступа, применяемых для фильтрации трафика, является то, что они формируются администратором статически до начала работы. В итоге администратор вынужден закладывать в них разрешения «на все случаи жизни». Например, чтобы позволить узлам внутренней сети соединяться по Telnet с узлами Интернета, необходимо разрешить, во-первых, движение TCP-сегментов с любого порта изнутри на порт 23 снаружи; а вовторых, для пропуска сегментов в обратном направлении необходимо разрешить движение сегментов с порта 23 наружных узлов на любой порт внутренних, так как заранее не известно,

какой клиентский порт будет использовать внутренний узел для открытия сеанса Telnet. Эти два списка доступа, для исходящих и входящих сегментов, никак не связаны друг с другом. В итоге злоумышленник, занявший порт 23 какого-либо внешнего узла, может отправлять сегменты на любой порт внутренних узлов, попадающих под список доступа. В случае с TCP проблема может быть частично решена установкой в списке доступа флага established, но для протокола UDP и это неприменимо.

Динамические обратные списки (reflexive access lists) предлагают способ решения проблемы. Они служат для автоматической фильтрации пакетов, следующих в обратном направлении относительно пакетов, пропущенных некоторым статическим списком. Динамические обратные списки открывают только те «двери», которые необходимо открыть для обслуживания данного конкретного сеанса обмена пакетами. В этом случае заранее формируется только один список, например список 120 «пропускать UDP-пакеты с любого порта внутри на порт 53 снаружи», а для пропуска пакетов в обратном направлении список 121 формируется динамически:

router(config)#access-list 120 permit udp any any eq 53 reflect DNS_REPLIES

router(config)#access-list 121 evaluate DNS_REPLIES

router(config)#interface FastEthernet 1/0

router(config-if)#ip access-group 120 out

router(config-if)#ip access-group 121 in

Приведенный выше пример работает следующим образом.

Когда внутренний узел A посылает сообщение с клиентского порта 3456 на порт 53 некоторого внешнего узла B, то соответствующий сегмент пропускается в узел B согласно списку 120. Кроме того, узел A ожидает, что и ответное сообщение от B с порта 53 на A порт 3456 будет пропущено маршрутизатором. Для этого маршрутизатор динамически создает (дополняет) список доступа 121 обратный к списку 120. Точнее, критерий отбора, содержащий указание evaluate DNS_REPLIES, будет обратным критерию отбора, содержащему указание reflect DNS_REPLIES с учетом параметров данного конкретного сеанса – адресов A и B и номера порта 3456.

Иными словами, список 121 будет выглядеть: «пропускать UDPпакеты с порта 53 узла B на порт 3456 узла A».

Динамически сформированный критерий отбора в списке 121 будет действовать до завершения сеанса между A и B. Завершение сеанса определяется таймером неактивности; кроме того, в TCPсеансах отслеживаются сегменты с флагами FIN и RST. Таймер неактивности для всех динамических обратных списков устанавливается командой:

router(config)#ip reflexive-list timeout <число_секунд>.

Кроме того, таймер для конкретного критерия может быть установлен с помощью параметра timeout:

router(config)#access-list 120 permit udp any any eq 53 reflect DNS_REPLIES timeout 120.

Если одновременно с сеансом A – B будет установлен сеанс между узлами C и D, то в список 121 будет добавлен еще один критерий отбора, учитывающий параметры этого нового сеанса – адреса C и D и клиентский порт на узле C.

Необходимо понимать, что использование динамических обратных списков доступа несовместимо с приложениями, которые изменяют номера портов в процессе своей работы.

В заключение обсуждения списков доступа необходимо отметить такой очевидный факт, что использование списков доступа замедляет работу маршрутизатора. Чем больше и сложнее списки, тем меньше производительность маршрутизатора. То же относится и к фиксации событий в журналах.

ВЫПОЛНИТЬ!

14. Создать динамический обратный список доступа, предложенный выше в качестве примера, и осуществить его проверку, отправляя запросы к DNS-серверу.

15. Аннулировать созданные списки доступа.

В качестве примера предлагается реализовать схему сети, представленную на рисунке 1.

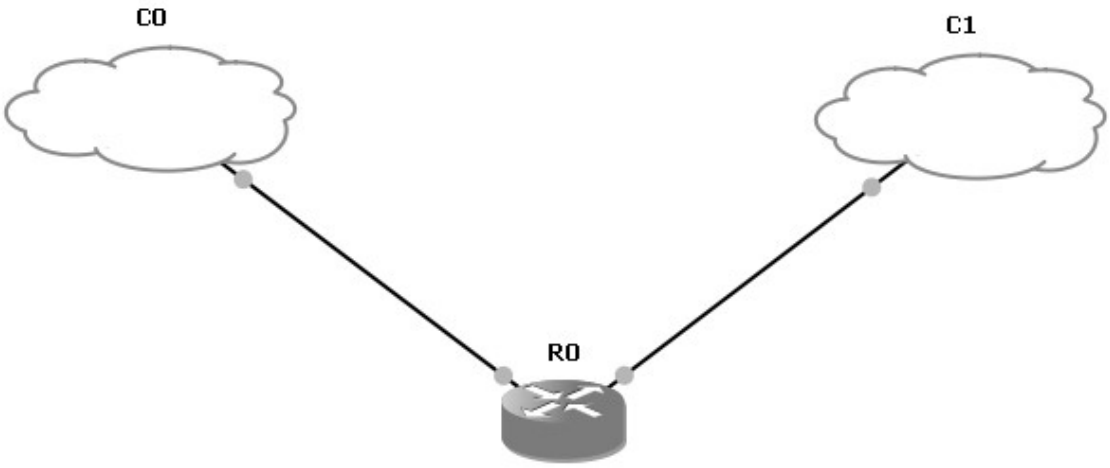

Рисунок 1 - Схема сети для примера использования расширенного списка доступа

Входные данные: C0 – сеть с диапазоном адресов 192.168.20.0/24; C1– сеть с диапазоном адресов 10.0.0.0/8. Необходимо настроить маршрутизатор R0 таким образом, чтобы весь трафик из сети C0 в сеть C1 был запрещен, за исключением трафика функционирования WEB-сервера, имеющего IP-адрес 10.0.0.5.

Реализовать данную схему можно с помощью следующих команд:

Router>enable

Router#

!Переход в контекст администратора. По умолчанию пароль не установлен.

Router#configuration terminal

!Переход в глобальный контекст конфигурирования.

Router(config)#access-list 101 permit tcp 192.168.20.0 0.0.0.255 10.0.0.5 eq 80

!Задание расширенного списка доступа № 101, разрешающего прохождение IP-трафика со всех адресов сети 192.168.20.0/24 на порт 80 IP-адреса 10.0.0.5.

Router(config)#access-list 101 deny ip any any

!Запрет всего остального трафика.

Router(config)#interface FastEthernet 1/1

!Переход в контекст конфигурирования интерфейса FastEthernet 1/1, подключенного к сети C0.

Router(config-if)#ip address 192.168.20.2 255.255.255.0

!Установка IP-адреса и маски сети.

Router(config-if)#ip access-group 101 in

Router(config-if)#no shutdown

!Включение интерфейса.

Router(config-if)#exit

!Выход из контекста конфигурирования интерфейса FastEthernet 1/1, подключенного к сети C0.

Router(config)#interface FastEthernet 1/0

!Переход в контекст конфигурирования интерфейса FastEthernet 1/0.

Router(config-if)#ip address 10.0.0.2 255.255.255.0

!Установка IP-адреса и маски сети.

Router(config-if)#no shutdown

!Включение интерфейса.

Router(config-if)#exit

ВЫПОЛНИТЬ!

16. Реализовать и проверить работоспособность приведенной схемы.

Библиографический список

1. Защита информации в компьютерных сетях. Практический курс : учеб. пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский [и др.] ; под ред. Н. И. Синадского. – Екатеринбург : УГТУ-УПИ, 2008. – 248 с.

2. Americas Headquarters Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x. – USA : Cisco Systems, 2009. – 136 p.

3. Gary Hallen, G. Kellogg Security Monitoring with Cisco Security MARS. – USA : Cisco Press, 2007. – 335 p.

4. James Burton, Ido Dubrawsky, Vitaly Osipov Cisco Security Professional's Guide to Secure Intrusion Detection Systems. – USA : Syngress Publishing, 2003. – 673 p.

5. Installation Guide for the Cisco Secure PIX Firewall Version 5.2. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

6. Install and Setup Guide for Cisco Security Monitoring Analysis and Response System. Release 4.3.x., 2008. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

7. Стивенс У. Р. Протоколы TCP/IP. Практическое руководство / пер. с англ. – СПб. : БХВ-Петербург, 2003. – 672 с.

8. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб. : Питер, 2001. – 320 с.