### Стандартные списки доступа

Списки доступа (access lists) представляют собой общие кри- терии отбора, которые можно впоследствии применять при филь- трации дейтаграмм, для отбора маршрутов, определения приори- тетного трафика и в других задачах.

Списки доступа, производящие отбор по IP-адресам, создают- ся командами access-list в режиме глобальной конфигурации, каж- дый 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, значе- ние которых в адресе следует игнорировать, остальные биты сбра- сываются. При этом сетевая маска (netmask) и маска шаблона (wildcard) – это разные вещи. Например, чтобы строка списка сра- ботала для всех узлов с адресами 1.16.124.ххх, 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 соот- ветствующей сетевой маски. Однако маска шаблона в общем слу- чае не связана с сетевой маской и даже может быть разрывной (со- держать чередования нулей и единиц). Например, строка списка должна сработать для всех нечетных адресов в сети 1.2.3.0/24. Со- ответствующая 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 отсутству- ет, то речь идет об IP-адресе одного узла.

Операторы permit и deny определяют, соответственно, поло- жительное (принять, пропустить, отправить, отобрать) или отрица- тельное (отбросить, отказать, игнорировать) будет принято реше-

ние при срабатывании данного критерия отбора. Например, если список используется при фильтрации дейтаграмм по адресу источ- ника, то эти операторы определяют, пропустить или отбросить дей- таграмму, адрес источника которой удовлетворяет комбинации

«адрес – маска шаблона». Если же список применяется для иденти- фикации 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: маршрути- затор 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 «от- казать 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 кон- фигурации этого интерфейса ввести команду:

# router(config-if)#ip access-group <номер\_списка>

**<{in|out}>.**

Ключевое слово in или out определяет, будет ли список при- меняться 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 кон- кретном интерфейсе для фильтрации входящих пакетов, и один – для исходящих. Соответственно, все необходимые критерии филь- трации 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.**

1. Применить созданный стандартный список доступа на вход одного из интерфейсов маршрутизатора.
2. С помощью команды **ping** проверить доступность компьютеров из сетей 192.168.20.1/24 и 10.0.0.1/24.
3. Аннулировать созданный стандартный список доступа.

### Расширенные списки доступа

Кроме стандартных (standard) списков доступа существуют также расширенные (extended), имеющие большее количество па- раметров и предлагающие более богатые возможности для форми- рования 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 ко- манды 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 опре- деляются так же, как и в стандартных списках.

Оператор при значении порта должен иметь одно из следую- щих 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, комби- нация оператор-порт, которая следует сразу же за адресом получа- теля, относится к портам узла-получателя. Применение этих ком- бинаций 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 входя- щих 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 про- токолы». Отметим, что в конце каждого списка доступа подразуме- вается deny ip any any, поэтому в предыдущем примере мы указали permit ip any any для разрешения произвольных пакетов, не попав- ших под предшествующие критерии.

Расширенный список с протоколом ip позволяет также произ- водить отбор произвольных пакетов по адресу отправителя и по ад- ресу получателя (в стандартных списках отбор производится толь- ко по адресу отравителя).

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

## ВЫПОЛНИТЬ!

1. 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.
2. Применить созданный расширенный список доступа на вход одного из интерфейсов маршрутизатора.
3. 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 по- мощью 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 опреде- ляют 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 парамет- ры, специфичные для данного протокола.

В конце команды **access-list** (расширенный) можно ука- зать 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 сраба- тывания, дальше сообщения посылаются каждые 5 минут с указа- нием числа срабатываний за отчетный период.

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

# router#show access-lists.

## ВЫПОЛНИТЬ!

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

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

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

## ВЫПОЛНИТЬ!

1. Включить учет случаев нарушения списка доступа.

Просмотр накопленной статистики (с указанием адресов от- правителей и получателей пакетов):

# router#show ip accounting access-violations.

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

## ВЫПОЛНИТЬ!

1. Выполнить несколько запросов к Web-серверам.
2. Просмотреть результаты работы команды **ping**.
3. Вывести на консоль накопленную статистику по учету случаев нарушений.
4. Аннулировать созданный расширенный список доступа.

### Динамические обратные списки доступа

Недостатком списков доступа, применяемых для фильтрации трафика, является то, что они формируются администратором ста- тически до начала работы. В итоге администратор вынужден закла- дывать 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 во- вторых, для пропуска сегментов в обратном направлении необхо-

димо разрешить движение сегментов с порта 23 наружных узлов на любой порт внутренних, так как заранее не известно, какой клиент- ский порт будет использовать внутренний узел для открытия сеанса Telnet. Эти два списка доступа, для исходящих и входящих сегмен- тов, никак не связаны друг с другом. В итоге злоумышленник, за- нявший порт 23 какого-либо внешнего узла, может отправлять сег- менты 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) предла- гают способ решения проблемы. Они служат для автоматической фильтрации пакетов, следующих в обратном направлении относи- тельно пакетов, пропущенных некоторым статическим списком. Динамические обратные списки открывают только те «двери», ко- торые необходимо открыть для обслуживания данного конкретного сеанса обмена пакетами. В этом случае заранее формируется только один список, например список 120 «пропускать UDP-пакеты с лю- бого 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 А посылает сообщение с клиентского порта 3456 на порт 53 некоторого внешнего узла В, то соответствующий сегмент пропускается в узел В согласно списку 120. Кроме того, узел А ожидает, что и ответное сообщение от В с порта 53 на А порт 3456 будет пропущено маршрутизатором. Для этого марш- рутизатор динамически создает (дополняет) список доступа 121 об- ратный к списку 120. Точнее, критерий отбора, содержащий указа- ние evaluate DNS\_REPLIES, будет обратным критерию отбора, содержащему указание reflect DNS\_REPLIES с учетом параметров данного конкретного сеанса – адресов А и В и номера порта 3456.

Иными словами, список 121 будет выглядеть: «пропускать UDP-

пакеты с порта 53 узла В на порт 3456 узла А».

Динамически сформированный критерий отбора в списке 121 будет действовать до завершения сеанса между А и В. Завершение сеанса определяется таймером неактивности; кроме того, в TCP- сеансах отслеживаются сегменты с флагами FIN и RST. Таймер не- активности для всех динамических обратных списков устанавлива- ется командой:

# router(config)#ip reflexive-list timeout

**<число\_секунд>.**

Кроме того, таймер для конкретного критерия может быть установлен с помощью параметра timеout: **router(config)#access-list 120 permit udp any**

# any eq 53 reflect DNS\_REPLIES timeout 120.

Если одновременно с сеансом А – В будет установлен сеанс между узлами С и D, то в список 121 будет добавлен еще один кри- терий отбора, учитывающий параметры этого нового сеанса – ад- реса С и D и клиентский порт на узле С.

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

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

## ВЫПОЛНИТЬ!

1. Создать динамический обратный список доступа, предложенный выше в качестве примера, и осуществить его проверку, отправляя запросы к DNS-серверу.
2. Аннулировать созданные списки доступа.

В качестве примера предлагается реализовать схему сети, представленную на рис. 3.1.



Рис. 3.1. Схема сети для примера использования расширенного списка доступа

Входные данные: С0 – сеть с диапазоном адресов 192.168.20.0/24; С1– сеть с диапазоном адресов 10.0.0.0/8. Необхо- димо настроить маршрутизатор R0 таким образом, чтобы весь тра- фик из сети С0 в сеть С1 был запрещен, за исключением трафика функционирования WEB-сервера, имеющего IP-адрес 10.0.0.5.

Реализовать данную схему можно с помощью следующих ко- манд:

# 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 про- хождение 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 С0.

# 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 С0.

# 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!

1. Реализовать и проверить работоспособность приведенной схемы.

# Настройка Zone-Based Policy Firewall

Начиная с версии IOS 12.4, в маршрутизаторах появилась функция Zone-Based Policy Firewall, позволяющая производить настройку правил межсетевого экрана. Эта функция позволяет назначить интерфейсам маршрутизатора зоны безопасности и уста- новить правила взаимодействия между ними.

Конфигурирование Zone-Based Policy Firewall заключается в выполнение следующих шагов:

1. назначить зоны межсетевого экрана;
2. определить возможность прохождения сетевого трафика между зонами;
3. включить существующие сетевые интерфейсы в созданные зоны;
4. определить классы, к которым будут применяться полити- ки для пересечения пары зон;
5. определить политики для пар зон, регламентирующие про- изводимые действия над проходящим сетевым трафиком;
6. применить политики для выбранных пар зон.

Рассмотрим настройку Zone-Based Policy Firewall для случая, представленного на рис. 3.2. В демилитаризованной зоне (ДМЗ) с адресом 172.16.0.0/16 расположены: Web-сервер (172.16.0.4); поч- товый сервер (172.16.0.5); FTP-сервер (172.16.0.6). Адрес внутрен- ней сети (пользователи) 192.168.20.0/24. Внешний IP-адрес маршрути- затора 10.0.0.2, маска сети 255.0.0.0, внутренний – 192.168.20.2.



## ВЫПОЛНИТЬ!

Рис. 3.2. Схема сети

1. Создать в GNS3 топологию сети, представленную выше (на рис. 3.2).
2. В режиме глобального конфигурирования определить зоны безопасности. Для пользователей задать зону с именем inside, для Интернета – outside, для ДМЗ – DMZ.

# Gateway(config)#zone security outside Gateway(config-sec-zone)#description internet Gateway(config-sec-zone)#exit Gateway(config)#zone security inside Gateway(config-sec-zone)# description intranet Gateway(config-sec-zone)#exit Gateway(config)#zone security dmz

**Gateway(config-sec-zone)#description DMZ Gateway(config-sec-zone)#exit.**

1. Назначить интерфейсы в зоны. По умолчанию прохождения трафика между зонами запрещено.

Для зоны outside: **Gateway(config)#interface FastEthernet0/0 Gateway(config-if)#ip address 10.0.0.2**

**255.0.0.0**

**Gateway(config-if)#no shutdown**

**Gateway(config-if)#zone-member security outside Gateway(config-if)#description outside Gateway(config-if)#exit.**

Для зоны inside:

**Gateway(config)#interface FastEthernet0/1 Gateway(config-if)#ip address 192.168.20.2**

**255.255.255.0**

**Gateway(config-if)#no shutdown**

**Gateway(config-if)#zone-member security inside Gateway(config-if)#description inside Gateway(config-if)#exit.**

Для зоны DMZ:

**Gateway(config)#interface FastEthernet1/0 Gateway(config-if)#ip address 172.16.0.2**

**255.255.255.0**

**Gateway(config-if)#no shutdown Gateway(config-if)#zone-member security dmz Gateway(config-if)#description DMZ Gateway(config-if)#exit.**

1. Определить протоколы, по которым пользователям разрешено выходить в Интернет (http, ftp, smtp, pop3, dns, icmp).

# Gateway(config)#class-map type inspect match-any cm\_http-ftp-dns-smtp-pop3-icmp

**Gateway(config-cmap)#match protocol http Gateway(config-cmap)#match protocol ftp**

|  |  |  |
| --- | --- | --- |
| **Gateway(config-cmap)#match** | **protocol** | **pop3** |
| **Gateway(config-cmap)#match** | **protocol** | **smtp** |
| **Gateway(config-cmap)#match** | **protocol** | **dns** |
| **Gateway(config-cmap)#match** | **protocol** | **icmp** |
| **Gateway(config-cmap)#exit.** |  |  |

1. Определить политики:

**Gateway(config)#policy-map type inspect in-out Gateway(config-pmap)#class type inspect cm\_http-**

**ftp-dns-smtp-pop3-icmp**

**Gateway(config-pmap-c)#inspect Gateway(config-pmap-c)#exit Gateway(config-pmap)#exit.**

1. Создать цепочку из пары зон inside → outside:

**Gateway(config)#zone-pair security inside- outside source inside destination outside**

**Gateway(config-sec-zone-pair)#service-policy type inspect in-out**

**Gateway(config-sec-zone-pair)#exit.**

1. Создать списки доступа для публичных серверов:

**Gateway(config)#access-list 101 remark web- server**

**Gateway(config)#access-list 101 permit ip any host 172.16.0.4**

**Gateway(config)#access-list 102 remark mail- server**

**Gateway(config)#access-list 102 permit ip any host 172.16.0.5**

**Gateway(config)#access-list 103 remark ftp- server**

**Gateway(config)#access-list 103 permit ip any host 172.16.0.6.**

1. Определить протоколы для доступа к серверам из внешней сети:

**Gateway(config)#class-map type inspect match-all web**

**Gateway(config-cmap)#match access-group 101**

**Gateway(config-cmap)#match protocol http Gateway(config-cmap)#exit**

**Gateway(config)#class-map type inspect match-all mail**

**Gateway(config-cmap)#match access-group 102 Gateway(config-cmap)#match protocol smtp Gateway(config-cmap)#match protocol pop3 Gateway(config-cmap)#exit**

**Gateway(config)#class-map type inspect match-all ftp**

|  |  |  |
| --- | --- | --- |
| **Gateway(config-cmap)#match** | **access-group** | **103** |
| **Gateway(config-cmap)#match** | **protocol ftp** |  |
| **Gateway(config-cmap)#exit.** |  |  |
| 9. Задать политики для ДМЗ: |  |  |
| **Gateway(config)#policy-map mail-ftp-dmz** | **type** | **inspect** | **web-** |
| **Gateway(config-pmap)#class** | **type** | **inspect** | **web** |
| **Gateway(config-pmap-c)#inspect** |  |  |
| **Gateway(config-pmap-c)#exit** |  |  |
| **Gateway(config-pmap)#class type** | **inspect** | **mail** |
| **Gateway(config-pmap-c)#inspect** |  |  |
| **Gateway(config-pmap-c)#exit** |  |  |
| **Gateway(config-pmap)#class type** | **inspect** | **ftp** |
| **Gateway(config-pmap-c)#inspect** |  |  |
| **Gateway(config-pmap-c)#exit** |  |  |
| **Gateway(config-pmap)#exit.** |  |  |

1. Создать цепочку из пары зон outside → dmz:

**Gateway(config)#zone-pair security out-dmz source outside destination dmz**

**Gateway(config-sec-zone-pair)#service-policy type inspect web-mail-ftp-dmz**

**Gateway(config-sec-zone-pair)#exit.**

1. Проверить работоспособность созданной конфигурации.