Списки управления транзитным доступом: фильтрация граничного уровня

Содержание

Введение

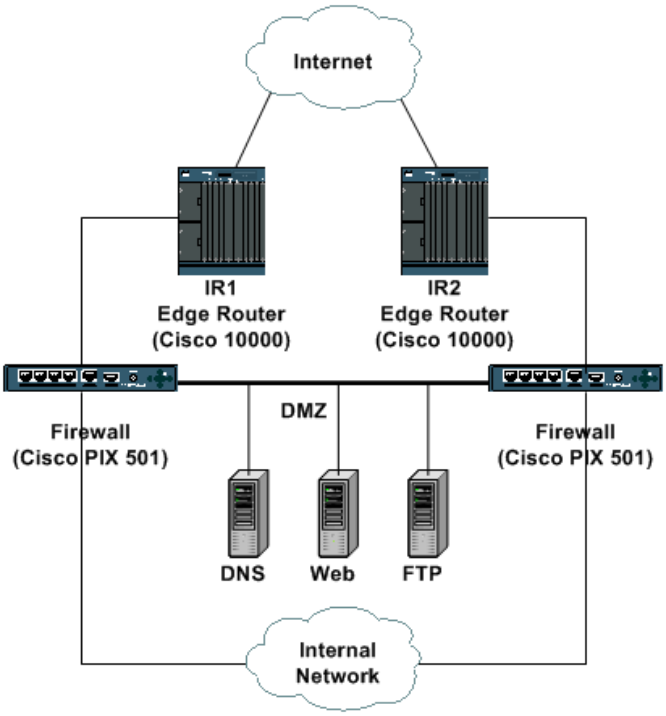
Данный документ содержит указания и рекомендуемые методы развертывания для фильтрации транзитного и граничного трафика на точках входа в сеть. Списки управления транзитным доступом (ACL) используются для увеличения безопасности сети, разрешая только требуемый трафик в сети.

Фильтры передачи

Обычная настройка

В большинстве граничных сетевых сред, таких как точки выхода в корпоративные Интернет-сети, фильтрация входа должна использоваться для перемещения трафика от незарегистрированных пользователей на границу сети. В некоторых развертываниях поставщиков услуг такая форма фильтрации трафика граничного уровня или транзитного трафика также может эффективно использоваться для ограничения входящего и исходящего транзитного трафика с помощью специально разрешенных протоколов. Основной темой этого документа является модель развертывания сети предприятия.

На рисунке изображена схема типичного Интернет-соединения предприятия. Два граничных маршрутизатора – IR1 и IR2 – обеспечивают прямой доступ к Интернету. Помимо этих маршрутизаторов, два брандмауэра (на этой схеме Cisco PIX) обеспечивают проверку трафика "потоком" и доступ как к внутренней сети, так и к демилитаризованной зоне (DMZ). DMZ включает в себя внешние услуги, такие как DNS и Интернет; это единственная сеть, доступная непосредственно при коллективном доступе в Интернет. Прямой Интернет-доступ к внутренней сети должен отсутствовать, в то время как для исходящего трафика внутренней сети должна быть возможность выхода на Интернет-сайты.



Граничные маршрутизаторы должны быть настроены таким образом, чтобы обеспечивать первый уровень безопасности с помощью списков ACL для входящего трафика. Списки ACL допускают в DMZ только специально разрешенный трафик, а также открывают пользователям внутренней сети, имеющим выход в Интернет, доступ к ответному трафику. Весь незарегистрированный трафик должен быть отправлен во входящие интерфейсы.

Разделы списков ACL для транзитного трафика

Как правило список управления транзитным доступом состоит из четырех разделов.

- Специальный адрес и анти-спуфинговые записи, которые запрещают незаконным источникам и пакетам с адресами отправителей, принадлежащими вашей сети, доступ в сеть с внешнего источника.

  Примечание. RFC 1918 определяет зарезервированное адресное пространство, которому не могут принадлежать адреса источников в Интернете. RFC 3330 определяет адреса для специального пользования, которым может потребоваться фильтрация. RFC 2827 предоставляет анти-спуфинговые рекомендации.

- Четко определенный ответный трафик для внутреннего подключения к Интернету
- Четко определенный внешний трафик, предназначенный для защиты внутренних адресов
- Явный оператор **deny**

  Примечание. Кроме этого, все списки ACL содержат неявный оператор **deny**, Cisco рекомендует использовать явный оператор **deny**, например, **deny ip any any**. На большинстве платформ такие операторы выполняют расчет числа запрещенных пакетов, которые могут быть отображены с помощью команды **show access-list**.

Создание списка ACL для транзитного трафика

Первым этапом в создании списка ACL для транзитного трафика является определение протоколов, требуемых в пределах ваших сетей. Кроме того, каждый узел имеет специфические требования, которые широко применяются и подразумевают использование разрешенных протоколов и приложений. Например, если сегмент DMZ обеспечивает связь с общедоступным веб-сервером, требуется TCP из Интернета на адрес(а) сервера DMZ в порт 80. Таким же образом, при внутреннем соединении с Интернетом требуется, чтобы ACL разрешил установленный ответный график TCP, имеющий установленный бит подтверждения (ACK).

Определение требуемых протоколов

Разработка данного списка протоколов может быть весьма сложной задачей, но существует ряд методик для определения требуемого

трафика.

- **Просмотрите настройки локальной политики безопасности/стратегии обслуживания.**

  Политика локальных сетевых узлов должна помогать в предоставлении базы разрешенных и запрещенных служб.

- **Проведите проверку конфигурации брандмауэра.**

  Текущие конфигурации брандмаура должны содержать явный оператор **permit** для разрешенных служб. В большинстве случаев возможно преобразовывать эти конфигурации в формат списка ACL и использовать их для создания большого числа записей ACL.

  Примечание. Как правило, брандмауэр с контролем состояния соединений не имеет определенных правил для авторизированного соединения возвратного трафика. Поскольку списки управления доступом (ACL) к маршрутизатору не изменяют свое состояние, ответный трафик должен быть явно разрешен.

- **Просмотрите приложения.**

  Те приложения, которые расположены в DMZ или используются внутри, могут помочь определить требования фильтрации. Просмотрите требования к приложениям для получения необходимой информации о структуре фильтра.

- **Использование списка ACL в формате классификации.**

  Список ACL в формате классификации состоит из операторов **permit** для различных протоколов, которые могут быть предназначены для внутренней сети. (См. Приложение A для списка наиболее часто используемых протоколов и приложений.) Используйте команду **show access-list** для отображения числа записей управления доступом (ACE) для определения требуемых протоколов. Изучите все сомнительные и неожиданные результаты перед созданием явного оператора **permit** для непредусмотренных протоколов.

- **Использование функции коммутации Netflow.**

  Netflow – это функция коммутации, которая в активированном состоянии предоставляет подробную информацию о технологическом процессе. Если функция Netflow активирована на ваших граничных маршрутизаторах, команда **show ip cache flow** выдает список протоколов, зарегистрированных с помощью функции Netflow. Функция Netflow не определяет все протоколы, поэтому эта методика должна применяться совместно с остальными.

Определение недопустимого трафика

Помимо направленной защиты список ACL для транзитного трафика также должен обеспечивать оперативную защиту от определенных типов недопустимых видов трафика в Интернете.

- Пространство Deny RFC 1918.
- Пакеты Deny, адрес источника которых входит в пространство адресов специального пользования, определяемых в RFC 3330.
- Использование анти-спуфинговых фильтров в соответствии с RFC 2827; ваше адресное пространство не должно быть источником пакетов, расположенных за пределами автономной системы (AS).

Остальные типы рассматриваемых трафиков включают в себя:

- **Внешние протоколы и IP-адреса, необходимые для связи с граничным маршрутизатором**
  - ICMP из IP-адресов поставщиков услуг
  - Протоколы маршрутизации
  - IPSec VPN, если граничный маршрутизатор используется в качестве граничного устройства
- **Четко определенный ответный трафик для внутреннего соединения с Интернетом**
  - Специальные виды трафика ICMP (протокола управляющих сообщений Интернета)
  - Ответы на запрос системы исходящих имен доступа (DNS)

- Установленный протокол TCP
- Ответный трафик пользовательского протокола данных (UDP)
- Информационные соединения FTP
- Информационные соединения TFTP
- Мультимедийные соединения

- **Четко определенный внешний трафик, предназначенный для защиты внутренних адресов**
  - Трафик VPN
    - Ассоциация межсетевой безопасности и протокол управления ключами (ISAKMP)
    - Просмотр трансляции сетевых адресов (протокол NAT)
    - Собственный механизм инкапсуляции
    - Инкапсуляция защищенной полезной нагрузки (протокол ESP)
    - Протокол аутентификации заголовка (AH)
  - HTTP для веб-серверов
  - Протокол безопасных соединений (SSL) для веб-серверов
  - FTP для FTP-серверов
  - Входящие информационные соединения FTP
  - Входящие пассивные информационные соединения FTP (**pasv**)
  - Простой протокол передачи почты (SMTP)
  - Другие приложения и серверы
  - Входящий запрос DNS
  - Зонный перенос входящего DNS

Применение ACL

Вновь созданный список ACL следует применять к входящему трафику для интерфейсов со стороны Интернета в граничных маршрутизаторах. В примере, приведенном в разделе Обычная установка, ACL применяется в интерфейсах Интернет-сетей на IR1 и IR2.

Более подробную информацию см. в разделе указания к применению и пример развертывания.

Пример ACL

Данный список доступа обеспечивает простой и в тоже время вполне реальный пример обычных записей, требуемых в списке ACL для транзитного трафика. Эти базовые списки ACL необходимо сопоставлять с элементами локальных конфигураций, характерных для каждого из узлов.

```
!--- Добавьте анти-спуфинговые записи.
!--- Запретите источники адресов специального пользования.
!--- О дополнительных адресах специального пользования см. RFC 3330.

access-list 110 deny ip 127.0.0.0 0.255.255.255 any
access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 31.255.255.255 any
access-list 110 deny ip host 255.255.255.255 any
```

```
!--- Оператор deny не должен быть настроен
!--- на ретрансляции протокола динамической конфигурации хоста (DHCP).

access-list 110 deny ip host 0.0.0.0 any
!--- Пространство фильтра RFC 1918.

access-list 110 deny ip 10.0.0.0 0.255.255.255 any
access-list 110 deny ip 172.16.0.0 0.15.255.255 any
access-list 110 deny ip 192.168.0.0 0.0.255.255 any
!--- Протокол разрешенного пограничного шлюза (BGP) в граничный маршрутизатор.

access-list 110 permit tcp host bgp_peer gt 1023 host router_ip eq bgp
access-list 110 permit tcp host bgp_peer eq bgp host router_ip gt 1023
!--- Не используйте свое пространство, как источник (как указано в RFC 2827).

access-list 110 deny ip ваша маршрутизируемая подсеть Интернет any


!--- Разрешите ответный трафик явным образом.
!--- Разрешите специальные типы ICMP.

access-list 110 permit icmp any any echo-reply
access-list 110 permit icmp any any unreachable
access-list 110 permit icmp any any time-exceeded
access-list 110 deny   icmp any any
!--- Это исходящие запросы DNS.

access-list 110 permit udp any eq 53  host первичный сервер DNS gt 1023
!--- Разрешите допуск первоначальных запросов DNS и ответов в первичный сервер DNS.

access-list 110 permit udp any eq 53  host первичный сервер DNS eq 53
!--- Разрешите законный бизнес-трафик.

access-list 110 permit tcp any маршрутизируемая подсеть Интернет established
access-list 110 permit udp any range 1 1023 маршрутизируемая подсеть Интернет gt 1023
!--- Разрешите информационные соединения ftp.

access-list 110 permit tcp any eq 20 маршрутизируемая подсеть Интернет gt 1023
!--- Разрешите информационные соединения tftp и мультимедийные соединения.

access-list 110 permit udp any gt 1023 маршрутизируемая подсеть Интернет gt 1023


!--- Разрешите трафик от внешнего источника явным образом.
!--- Это входящие запросы DNS.

access-list 110 permit udp any gt 1023 host <primary DNS server> eq 53
!-- Это запросы DNS зонного переноса в первичный сервер DNS.

access-list 110 permit tcp host вторичный сервер DNS gt 1023 host первичный сервер DNS eq 53
!--- Разрешить первоначальные зонные переносы DNS.

access-list 110 permit tcp host вторичный сервер DNS eq 53  host первичный сервер DNS eq 53
!--- Запретите весь остальной трафик DNS.

access-list 110 deny udp any any eq 53
access-list 110 deny tcp any any eq 53
!--- Разрешите трафик IPSec VPN.

access-list 110 permit udp any host Головной узел IPSec eq 500
access-list 110 permit udp any host Головной узел IPSec eq 4500
access-list 110 permit 50 any host Головной узел IPSec
access-list 110 permit 51 any host Головной узел IPSec
access-list 110 deny   ip any host Головной узел IPSec
!--- Это Интернет-подключения к
!--- к общедоступному серверу.

access-list 110 permit tcp any host общедоступный веб-сервер eq 80
access-list 110 permit tcp any host общедоступный веб-сервер eq 443
access-list 110 permit tcp any host общедоступный сервер FTP eq 21
!--- Разрешены информационные соединения с сервером FTP
!--- через ACE permit established.
!--- Разрешить информационные соединения PASV с сервером FTP.

access-list 110 permit tcp any gt 1023 host общедоступный сервер FTP gt 1023
access-list 110 permit tcp any host общедоступный сервер SMTP eq 25


!--- Запретите весь остальной трафик.


access-list 101 deny ip any any
```

Примечание. Не забывайте об этих советах при использовании списка ACL для транзитного трафика

- Ключевое слово **log** может быть использовано для получения дополнительной информации об источниках и назначениях для данного протокола. Кроме того, данное ключевое слово предоставляет подробное объяснение использования списка управления доступом, успешный выход к записям в списке ACL, который использует ключевое слово **log** для повышения коэффициента использования CPU. Влияние регистрации на производительность системы зависит от платформы.

- Сообщения о недоступности ICMP генерируются для пакетов, которые в административном порядке запрещены списком ACL. Это может повлиять на производительность маршрутизатора и канала. Используйте команду **no ip unreachables** для отключения сообщений IP-недоступности в интерфейсе, где развернут транзитный (граничный) список ACL.

- Этот ACL может быть внутренне развернут с помощью всех операторов **permit** для проверки того, что законный бизнес-трафика не отклоняется. Как только законный бизнес-трафик определен и рассчитан, могут быть настроены специальные элементы **deny**.

Списки ACL и фрагментированные пакеты

Списки ACL имеют ключевое слово **fragments**, которое активирует специальный режим обработки фрагментированных пакетов. В общем случае, на неначальные фрагменты, совпадающие с операторами уровня 3 (протокол, адрес источника и адрес назначения) – независимо от информации уровня 4 в списке управления доступом – оказывают влияние оператор **permit** или **deny** совпадающих записей. Обратите внимание на то, что использование ключевого слова **fragments** может привести к большей степени структурированности запрещенных или разрешенных неначальных фрагментов.

Фильтрация фрагментов добавляет дополнительный уровень защиты от атаки DoS (отказ от обслуживания), которая использует только неначальные фрагменты (когда FO > 0). Использование оператора **deny** для неначальных фрагментов в начале ACL закрывает доступ в маршрутизатор всем неначальным фрагментам. В редких случаях допустимая операция может потребовать фрагментации и, таким образом, будет отфильтрована при наличии в списке ACL оператора **deny fragment**. К условиям, вызывающим фрагментацию, можно отнести использование аутентификации цифровых сертификатов для ISAKMP, а также просмотр IPSec NAT.

В качестве примера рассмотрим неполный список ACL.

```
access-list 110 deny tcp any маршрутизируемая подсеть Интернет fragments
access-list 110 deny udp any маршрутизируемая подсеть Интернет fragments
access-list 110 deny icmp any маршрутизируемая подсеть Интернет fragments
<rest of ACL>
```

Добавление этих записей в начало списка управления доступом закрывает доступ в сеть всем неначальным фрагментам, в то время как нефрагментированные пакеты или исходные фрагменты передаются в следующие строки списка ACL (оператор **deny fragment** на них не действует). Предыдущий фрагмент списка ACL также способствует классификации атаки, поскольку каждый протокол – UDP, TCP и ICMP – увеличивает отдельные счетчики в ACL.

Поскольку большинство атак основано на волновом распространении фрагментированных пакетов, фильтрация входящих фрагментов во внутреннюю сеть обеспечивает дополнительные защитные меры и помогает удостовериться в том, что атака не может внедриться во фрагмент простым совпадением правил уровня 3 в списке ACL.

Более подробно параметры рассмотрены в документе Списки управления доступом и IP-фрагменты.

Оценка риска

Когда вы разворачиваете защиту транзитного трафика ACL, рассматривается две ключевые зоны риска.

- Проверьте правильность размещения соответствующих операторов **permit**/**deny**. Для эффективного функционирования списка ACL необходимо разрешить все требуемые протоколы.

- Производительность списка ACL изменяется в зависимости от платформы. Прежде чем развернуть списки ACL, изучите технические характеристики имеющегося оборудования.

Компания Cisco рекомендует перед развертыванием протестировать устройство в лаборатории.

Приложения

Часто используемые протоколы и приложения

Имена портов TCP

Этот список имен портов TCP может применяться вместо номеров портов при задании конфигураций списка ACL в ПО Cisco IOS®. Справочная информация по этим протоколам находится в RFC текущего назначенного номера. Номера портов, соответствующих данным протоколам, могут также быть определены во время настройки списка ACL при вводе **?** вместо номера порта.

bgp	kshell
chargen	login
cmd	lpd
daytime	nntp
discard	pim
domain	pop2
echo	pop3
exec	smtp
finger	sunrpc
ftp	syslog
ftp-data	tacacstalk
gopher	telnet
hostname	time
ident	uucp
irc	whois
klogin	www

Имена портов UDP

Этот список имен портов UDP может применяться вместо номеров портов при задании конфигураций списка ACL в ПО Cisco IOS. Справочная информация по этим протоколам находится в RFC текущего назначенного номера. Номера портов, соответствующих данным протоколам, могут также быть определены во время настройки списка ACL при вводе **?** вместо номера порта.

biff	ntp
bootpc	pim-auto-rp
bootps	rip
discard	snmp
dnsix	snmptrap
domain	sunrpc
echo	syslog
isakmp	tacacs
mobile-ip	talk
nameserver	tftp
netbios-dgm	time
netbios-ns	who
netbios-ss	xdmcp

Указания к развертыванию

Компания Cisco рекомендует традиционные методы развертывания. Необходимо иметь четкое представление о требуемых протоколах для того, чтобы развернуть списки ACL для транзитного трафика. В настоящем руководстве описан традиционный метод развертывания защитных списков ACL с использованием итеративного метода.

1. **Идентификация используемых в сети протоколов с помощью списка ACL в формате классификации.**

   Разверните список ACL, который разрешает все известные протоколы, используемые в сети. Это список ACL, предназначенный для обнаружения (или классификации) должен иметь адрес источника **any** и назначение IP-адреса или полную Интернет-маршрутизированную IP-подсеть. Задайте конфигурацию последней записи, которая разрешает **ip any any log**, для идентификации дополнительных протоколов, которые требуется разрешить.

Цель – определить все требуемые протоколы, используемые в сети. Используйте регистрацию данных для определения элементов, которые могут быть связаны с маршрутизатором.

Примечание. Кроме того, ключевое слово **log** обеспечивает подробное объяснение использования списка ACL, успешный выход к записям в списке ACL, при этом использование данного ключевого слова может привести к большому числу записей в журнале и более высокому коэффициенту использования ЦП маршрутизатора. Используйте ключевое слово **log** для коротких периодов времени или для упрощения классифицирования трафика.

Обратите внимание, что существует риск атаки на сеть, поскольку действующий список ACL состоит целиком из всех операторов **permit**. Выполните процесс классификации как можно быстрее, чтобы обеспечить соответствующее управление доступом.

2. **Просмотр идентифицированных пакетов и начало фильтрации доступа во внутреннюю сеть.**

   После определения и просмотра пакетов, отфильтрованных списком ACL на первом этапе, обновите ACL классификации для вычисления новых определенных протоколов и IP-адресов. Добавьте анти-спуфинговые записи в список ACL. В соответствии с указаниями, в ACL классификации замените отдельные записи **deny** на операторы **permit**. Вы можете использовать команду **show access-list** для контроля отдельных записей **deny** и числа случаев выполнения функции. Это предоставляет информацию о запрещенных попытках доступа в сеть без включенных записей регистрации ACL. Последняя строка в списке ACL должна иметь вид **deny ip any any**. Снова число случаев выполнения функции для этой последней записи может предоставить информацию о запрещенных попытках доступа.

3. **Контроль и обновление списка ACL.**

   Просмотрите заполненный список ACL для того, чтобы проверить, что новые введенные требуемые протоколы добавлены в соответствии со списком управления. Контроль списка управления доступом также дает возможность получить информацию о запрещенных попытках доступа в сеть, что в свою очередь приводит к получению сведений о предстоящей атаке.

Пример развертывания

В данном примере представлен список управления транзитным доступом, защищающий сеть, основанную на данной адресации.

- IP-адрес маршрутизатора ISP – 10.1.1.1.

  IP-адрес граничного маршрутизатора Интернета – 10.1.1.2.

  Сеть с Интернет-маршрутизацией – 192.168.201.0 255.255.255.0.

  Головной узел VPN – 192.168.201.100.

  Веб-сервер – 192.168.201.101.

  Сервер FTP – 192.168.201.102.

  Сервер SMTP – 192.168.201.103.

  Первичный сервер DNS – 192.168.201.104.

  Вторичный сервер DNS – 172.16.201.50.

Список ACL транзитной защиты создан на основе данной информации. Список ACL открывает доступ одноранговых узлов eBGP в маршрутизатор ISP, предоставляет анти-спуфинговые фильтры, предоставляет специальный ответный и входной трафики и отклоняет все остальные виды трафика явным образом.

```
no access-list 110
!--- Этап 1 – Добавьте анти-спуфинговые записи.
!--- Запретите источники адресов специального пользования.
!--- О дополнительных адресах специального пользования см. RFC 3330.

access-list 110 deny   ip 127.0.0.0 0.255.255.255 any
access-list 110 deny   ip 192.0.2.0 0.0.0.255 any
access-list 110 deny   ip 224.0.0.0 31.255.255.255 any
access-list 110 deny   ip host 255.255.255.255 any
!--- Оператор deny не должен быть настроен
```

```
!--- на ретрансляции протокола динамической конфигурации хоста (DHCP).

access-list 110 deny   ip host 0.0.0.0 any
!--- Пространство фильтра RFC 1918.

access-list 110 deny   ip 10.0.0.0 0.255.255.255 any
access-list 110 deny   ip 172.16.0.0 0.15.255.255 any
access-list 110 deny   ip 192.168.0.0 0.0.255.255 any
!--- Разрешите протокол BGP в граничный маршрутизатор.

access-list 110 permit tcp host 10.1.1.1 gt 1023 host 10.1.1.2 eq bgp
access-list 110 permit tcp host 10.1.1.1 eq bgp host 10.1.1.2 gt 1023
!--- Не используйте свое пространство, как источник (как указано в RFC 2827).

access-list 110 deny   ip 192.168.201.0 0.0.0.255 any


!--- Этап 2 – Разрешите ответный трафик явным образом.
!--- Разрешите специальные типы ICMP.

access-list 110 permit icmp any any echo-reply
access-list 110 permit icmp any any unreachable
access-list 110 permit icmp any any time-exceeded
access-list 110 deny   icmp any any
!--- Это исходящие запросы DNS.

access-list 110 permit udp any eq domain host 192.168.201.104 gt 1023
!--- Разрешите допуск первоначальных запросов DNS и ответов в первичный сервер DNS.

access-list 110 permit udp any eq domain host 192.168.201.104 eq domain
!--- Разрешите законный бизнес-трафик.

access-list 110 permit tcp any 192.168.201.0 0.0.0.255 established
access-list 110 permit udp any range 1 1023 192.168.201.0 0.0.0.255 gt 1023
!--- Разрешите информационные соединения ftp.

access-list 110 permit tcp any eq ftp-data 192.168.201.0 0.0.0.255 gt 1023
!--- Разрешите информационные соединения tftp и мультимедийные соединения.

access-list 110 permit udp any gt 1023 192.168.201.0 0.0.0.255 gt 1023


!--- Этап 3 – Разрешите ответный трафик явным образом.
!--- Это входящие запросы DNS.

access-list 110 permit udp any gt 1023 host 192.168.201.104 eq domain
!-- Это запросы DNS зонного переноса в первичный сервер DNS.

access-list 110 permit tcp host 172.16.201.50 gt 1023 host 192.168.201.104 eq domain
!--- Разрешите первоначальные зонные переносы DNS.

access-list 110 permit tcp host 172.16.201.50 eq domain host 192.168.201.104 eq domain
!--- Запретите весь остальной трафик DNS.

access-list 110 deny   udp any any eq domain
access-list 110 deny   tcp any any eq domain
!--- Разрешите трафик IPSec VPN.

access-list 110 permit udp any host 192.168.201.100 eq isakmp
access-list 110 permit udp any host 192.168.201.100 eq non500-isakmp
access-list 110 permit esp any host 192.168.201.100
access-list 110 permit ahp any host 192.168.201.100
access-list 110 deny   ip any host 192.168.201.100
!--- Это Интернет-подключения к
!--- к общедоступному серверу.

access-list 110 permit tcp any host 192.168.201.101 eq www
access-list 110 permit tcp any host 192.168.201.101 eq 443
access-list 110 permit tcp any host 192.168.201.102 eq ftp
!--- Разрешены информационные соединения с сервером FTP
!--- через ACE permit established на этапе 3.
!--- Разрешить информационные соединения PASV с сервером FTP.

access-list 110 permit tcp any gt 1023 host 192.168.201.102 gt 1023
access-list 110 permit tcp any host 192.168.201.103 eq smtp


!--- Этап 4 – Добавьте явный оператор deny.


access-list 110 deny   ip any any

Edge-router(config)#interface serial 2/0
Edge-router(config-if)#ip access-group 110 in
```

Дополнительные сведения

- **Страница поддержки списков доступа**
- **Справочник команд коммутации услуг Cisco IOS, версия 12.2 – команды: access-list rate-limit through ip cef**
- **Запросы комментариев (RFC)**
- **Cisco Systems – техническая поддержка и документация**

Дата генерации PDF файла: Jan 05, 2010

---

http://www.cisco.com/support/RU/customer/content/10/107547/tacl.shtml

---