Передать списки управления доступом: Фильтрация граничного уровня

Содержание

Введение

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

Фильтры передачи

Типичная установка

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 на предприятии.

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. Внутренняя сеть никогда не должна быть доступна напрямую из Интернета, в то время как трафик, исходящий из внутренней сети, должен иметь возможность выхода на Интернет-сайты.

Граничный концентратор должен быть настроен таким образом, чтобы обеспечивать первый уровень безопасности, используя списки контроля входящего доступа ACLs. 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.

Транзитный раздел ACL

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, которое не является допустимым источником адресов в Интернете. RFC 3330 определяет специальные адреса, для которых может потребоваться фильтрация. RFC 2827 предоставляет анти-спуфинговые рекомендации.
- Четко определенный ответный трафик для внутреннего соединения с Интернетом
- Четко определенный внешний трафик, предназначенный для защиты внутренних адресов
- **Явный оператор denyПримечание:** Несмотря на то, что все ACL содержат неявную **инструкцию deny**, Cisco рекомендует, чтобы использование явного **запретило** statemen, например, **запретите ip любой любой**. **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 / политики службы.**Политика локальных узлов должна помогать в предоставлении базы разрешенных и запрещенных служб.
- **Обзор/аудит конфигурации межсетевого экрана.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:** Самонастраивающийся межсетевой экран обычно не имеет явных правил для возврата трафика авторизованным соединениям. Поскольку списки управления доступом (ACL) к маршрутизатору не изменяют свое состояние, ответный трафик должен быть явно разрешен.
- **Проанализируйте свои 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.
- **Используйте 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.**
- **Используйте функцию 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 услугПротоколы маршрутизацииIPSec VPN, если граничный маршрутизатор используется в качестве граничного устройства
- **Четко определенный ответный трафик для внутреннего соединения с**

ИнтернетомКонкретные виды трафика ICMP (протокола управляющих сообщений Интернета)Ответы на запрос системы исходящих имен доступа (DNS)Установка TCPОтветный трафик пользовательского протокола данных (UDP)Информационные соединения FTPИнформационные соединения TFTPМультимедийные соединения

- **Четко определенный внешний трафик, предназначенный для защиты внутренних адресов**Трафик VPNАссоциация межсетевой безопасности и протокол управления ключами (ISAKMP)Просмотр трансляции сетевых адресов (протокол NAT)Собственный механизм инкапсуляцииИнкапсуляция защищенной полезной нагрузки (протокол ESP)Протокол аутентификации заголовка (AH)HTTP для веб-серверовПротокол безопасных соединений (SSL) для веб-серверовFTP для FTP-серверовВходящие информационные соединения FTP**Входящие пассивные информационные соединения FTP (pasv)**Простой протокол электронной почты (SMTP)Другие приложения и серверыВходящий запрос DNSЗонный 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.

```
!--- Add anti-spoofing entries. !--- Deny special-use address sources. !--- Refer to RFC 3330
for additional special use addresses. 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 !--- The deny statement should not be
configured !--- on Dynamic Host Configuration Protocol (DHCP) relays. access-list 110 deny ip
host 0.0.0.0 any !--- Filter RFC 1918 space. 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 !--- Permit Border Gateway Protocol (BGP) to the edge router. 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 !--- Deny your space as source (as noted in RFC 2827). access-list
110 deny ip your Internet-routable subnet any !--- Explicitly permit return traffic. !--- Allow
specific ICMP types. 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 !--- These are outgoing DNS queries. access-list 110 permit udp any eq 53 host primary
DNS server gt 1023 !--- Permit older DNS queries and replies to primary DNS server. access-list
110 permit udp any eq 53 host primary DNS server eq 53 !--- Permit legitimate business traffic.
access-list 110 permit tcp any Internet-routable subnet established access-list 110 permit udp
any range 1 1023 Internet-routable subnet gt 1023 !--- Allow ftp data connections. access-list
110 permit tcp any eq 20 Internet-routable subnet gt 1023 !--- Allow tftp data and multimedia
connections. access-list 110 permit udp any gt 1023 Internet-routable subnet gt 1023 !---
Explicitly permit externally sourced traffic. !--- These are incoming DNS queries. access-list
110 permit udp any gt 1023 host <primary DNS server> eq 53 !-- These are zone transfer DNS
queries to primary DNS server. access-list 110 permit tcp host secondary DNS server gt 1023 host
```

```
primary DNS server eq 53 !--- Permit older DNS zone transfers. access-list 110 permit tcp host
secondary DNS server eq 53 host primary DNS server eq 53 !--- Deny all other DNS traffic.
access-list 110 deny udp any any eq 53 access-list 110 deny tcp any any eq 53 !--- Allow IPSec
VPN traffic. access-list 110 permit udp any host IPSec headend device eq 500 access-list 110
permit udp any host IPSec headend device eq 4500 access-list 110 permit 50 any host IPSec
headend device access-list 110 permit 51 any host IPSec headend device access-list 110 deny ip
any host IPSec headend device !--- These are Internet-sourced connections to !--- publicly
accessible servers. access-list 110 permit tcp any host public web server eq 80 access-list 110
permit tcp any host public web server eq 443 access-list 110 permit tcp any host public FTP
server eq 21 !--- Data connections to the FTP server are allowed !--- by the permit established
ACE. !--- Allow PASV data connections to the FTP server. access-list 110 permit tcp any gt 1023
host public FTP server gt 1023 access-list 110 permit tcp any host public SMTP server eq 25 !---
Explicitly deny all other traffic. access-list 101 deny ip any any
```

Примечание: Помните эти предложения при применении транзитного ACL.

- **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 Internet routable subnet fragments access-list 110 deny udp any
Internet routable subnet fragments access-list 110 deny icmp any Internet routable subnet
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.

Сведения о подробном обсуждении данных параметров см. в разделе ACL и IP-фрагменты.

Оценка рисков

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

- **Убедитесь, что соответствующие выражения permit/deny находятся где нужно.** Для эффективного функционирования списка ACL необходимо разрешить все требуемые протоколы.
- Производительность ACL зависит 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	вход в систему
cmd	lpd
дневное время	nntp
сброс	pim
domain	pop2
эхо	pop3

exec	smtp
finger	sun RPC
ftp	системный журнал
fTP-данные	tacacstalk
gopher	telnet
host name	время
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
сброс	snmp
dnsix	сообщение SNMP
domain	sun RPC
эхо	системный журнал
isakmp	tacacs
mobile IP	разговор
имя сервера	tftp
netbios-dgm	время
netbios-ns	кто
netbios-ss	xdmcp

Инструкции по развертыванию

Cisco рекомендует осторожные способы 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. **Определите протоколы, которые используются в сети с классификацией ACL.**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: Хотя ключевое слово log предоставляет подробные сведения об обращениях к ACL, чрезмерные обращения к записи ACL, которая использует данное ключевое слово, могут послужить появлению большого количества записей log и высокой загрузке ЦП. 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.**Определив и пересмотрев пакеты, отфильтрованные списком ACL на первом этапе, обновите ACL классификации для учетной записи для заново 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.Диапазон адресов для сети с Интернет-маршрутизацией составляет от 192.168.201.0 до 255.255.255.0.Головной узел VPN - 192.168.201.100.Веб-сервер – 192.168.201.101.Адрес сервера FTP составляет 192.168.201.102.Адрес сервера 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
!--- Phase 1 – Add anti-spoofing entries. !--- Deny special-use address sources. !--- See RFC
3330 for additional special-use addresses. 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 !--- This deny statement should not be
configured !--- on Dynamic Host Configuration Protocol (DHCP) relays. access-list 110 deny ip
host 0.0.0.0 any !--- Filter RFC 1918 space. 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 !--- Permit BGP to the edge router. 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
!--- Deny your space as source (as noted in RFC 2827). access-list 110 deny ip 192.168.201.0
0.0.0.255 any !--- Phase 2 – Explicitly permit return traffic. !--- Allow specific ICMP types.
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 !--- These
are outgoing DNS queries. access-list 110 permit udp any eq domain host 192.168.201.104 gt 1023
!--- Permit older DNS queries and replies to primary DNS server. access-list 110 permit udp any
eq domain host 192.168.201.104 eq domain !--- Permit legitimate business traffic. 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 !--- Allow FTP data connections. access-list 110 permit tcp
any eq ftp-data 192.168.201.0 0.0.0.255 gt 1023 !--- Allow TFTP data and multimedia connections.
access-list 110 permit udp any gt 1023 192.168.201.0 0.0.0.255 gt 1023 !--- Phase 3 – Explicitly
permit externally sourced traffic. !--- These are incoming DNS queries. access-list 110 permit
udp any gt 1023 host 192.168.201.104 eq domain !--- Zone transfer DNS queries to primary DNS
server. access-list 110 permit tcp host 172.16.201.50 gt 1023 host 192.168.201.104 eq domain !--
- Permit older DNS zone transfers. access-list 110 permit tcp host 172.16.201.50 eq domain host
192.168.201.104 eq domain !--- Deny all other DNS traffic. access-list 110 deny udp any any eq
domain access-list 110 deny tcp any any eq domain !--- Allow IPSec VPN traffic. 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 !---
These are Internet-sourced connections to !--- publicly accessible servers. 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 !--- Data connections to the
FTP server are allowed !--- by the permit established ACE in Phase 3. !--- Allow PASV data
connections to the FTP server. 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 !--- Phase 4 – Add explicit
deny statement. 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