Списки управления доступом (ACL) и IP - фрагменты

Содержание

[Введение](#)
[Типы записей ACL](#)
[Блок-схема правил ACL](#)
[Как происходит сопоставление пакетов с ACL](#)
[Пример 1](#)
[Пример 2](#)
[фрагментирует сценарии ключевых слов](#)
[Сценарий 1](#)
[Сценарий 2](#)
[Дополнительные сведения](#)

Введение

В этом Описании технологических решений объяснены различные виды записей списка управления доступом (ACL) и что происходит, когда различные виды пакетов встречаются с этими разнообразными записями. Списки ACL используются для блокирования пакетов IP от , пересылаемых маршрутизатором.

RFC 1858 покрывает учитываемые факторы безопасности для фильтрации IP - фрагмента и выделяет две атаки на хосты, которые включают IP - фрагменты пакетов TCP, Крошечной Атаки фрагментами и Перекрывающейся Атаки фрагментами. Желательно блокировать эти атаки, так как они могут скомпрометировать хост или ограничить все его внутренние ресурсы.

RFC 1858 также описывает 2 метода защиты от этих атак, прямой и косвенный. В прямом методе сбрасывают от начальных фрагментов, которые меньше, чем минимальная длина. Способ обхода заключается в сбросе второго фрагмента из набора фрагментов, если с него начинается 8 байт исходной IP-дейтаграммы. Дополнительную информацию см. в RFC 1858.

Традиционно, фильтры пакета как ACL применены к нефрагментам и начальному фрагменту пакета IP, потому что они содержат и Уровень 3 и 4 информации, против которой ACL могут совпасть для разрешения или запретить решение. Неначальный фрагменты традиционно позволены через ACL, потому что они могут быть заблокированы на основе информации сетевого уровня 3 в пакетах; однако, потому что эти пакеты не содержат информацию уровня 4, они не совпадают с информацией уровня 4 в записи ACL, если это существует. Разрешение неначальный фрагментов дейтаграммы IP через приемлемо, потому что хост, получающий фрагменты, не в состоянии повторно собрать исходную IP - датаграмму без начального фрагмента.

Межсетевые экраны могут также использоваться к блокировкам пакета путем поддержания таблицы фрагментов пакета, индексированных с разбивкой по источникам и IP - адрес назначения, протокол и ID IP. И Межсетевой экран Cisco PIX и Cisco, IOS® Firewall может фильтровать все фрагменты отдельного потока путем поддержания этой таблицы информации, но слишком дорого сделать это на функции списка прав доступа (ACL) маршрутизатора для основы. Исходное задание межсетевого экрана к блокировкам пакета, и его дополнительная роль к маршрутизированным пакетам; главная задача маршрутизатора – направлять пакеты, а его вторая задача – блокировать их.

Чтобы решить проблему безопасности с фрагментами TCP, два изменения было внесено в Cisco IOS Software Releases 12.1(2) и 12.0(11). Способ обхода, как описано в RFC 1858, был внедрен как часть стандартной санитарной проверки входящего пакета TCP/IP. Изменения были также внесены в функцию списка прав доступа (ACL) относительно неначальный фрагментов.

Типы записей ACL

Существует шесть различных типов строк ACL, и результаты каждой строки зависят от того, соответствует ей пакет или нет. В следующем списке FO = 0 указывает на нефрагмент или начальный фрагмент в потоке TCP, FO> 0 указывает, что пакет является неначальный фрагментом, L3 означает Уровень 3, и L4 означает Уровень 4.

Примечание: Когда сведения уровня 3 и уровня 4 будут в строке ACL и когда будет присутствовать ключевое слово "fragments", действие ACL будет традиционным и для действий разрешения и для действий запрещения. Действия являются консервативными во избежание случайного отказа от фрагментированного сегмента потока, поскольку фрагменты не содержат достаточной информации, соответствующей всем атрибутам фильтра. В запрещать случае, вместо того, чтобы запретить неначальный фрагмент, обработана следующая запись списка контроля доступа. В случае разрешения предполагается, что информация уровня 4 в пакете, при наличии, совпадает с информацией уровня 4 в строке ACL.

Разрешить каналу ACL передачу только данных третьего уровня (L3)

1. Если информация о L3 пакета совпадает с информацией о L3 в строке ACL, это разрешено.
2. Если сведения третьего уровня пакета не совпадают со сведениями третьего уровня в строке ACL, обрабатывается следующая запись этого списка.

Строка ACL отвергается только с информацией с 3 уровня

1. Если данные пакета L3 совпадают с данными L3 в строке списка ACL, то он отбрасывается.
2. Если сведения третьего уровня пакета не совпадают со сведениями третьего уровня в строке ACL, обрабатывается следующая запись этого списка.

Строка ACL разрешения с информацией о L3 только и ключевое слово фрагментов присутствуют

Если информация о L3 пакета совпадает с информацией о L3 в строке ACL, смещение фрагмента пакета проверено.

1. Если значение FO пакета >0, прием пакета допускается.
2. Если у пакета FO = 0, будет обрабатываться следующая запись ACL.

Запретите строку ACL с информацией о L3 только, и ключевое слово фрагментов присутствует

Если информация о L3 пакета действительно совпадает с информацией о L3 в строке ACL, смещение фрагмента пакета проверено.

1. Если FO пакета больше 0, пакет запрещается.
2. Если значение пакета FO = 0, обрабатывается следующая строка списка ACL.

Разрешить канал ACL со сведениями L3 и L4

1. Если информация о L3 и L4 пакета совпадает со строкой ACL и FO = 0, пакет разрешен.
2. Если сведения третьего уровня пакета совпадают со сведениями третьего уровня в строке списка управления доступом, а FO > 0, пакет разрешен.

Запрет строки ACL с информацией L3 и L4

1. Если информация о L3 и L4 пакета совпадает с записью ACL и FO = 0, пакет запрещен.
2. Если информация о L3 пакета совпадает со строкой ACL и FO> 0, следующая запись списка контроля доступа обработана.

Блок-схема правил ACL

На приведенной ниже блок-схеме описывается порядок применения правил ACL при проверке пакетов, являющихся начальными фрагментами, не фрагментами или не начальными фрагментами, по списку ACL.

Примечание: Сами непервичные фрагменты содержат только сведения уровня 3 и никогда уровня 4, хотя ACL может содержать сведения как уровня 3, так и уровня 4.

Как происходит сопоставление пакетов с ACL

Пример 1

Следующие пять возможных сценариев включают различные типы пакетов, встречающихся с ACL 100. См. таблицу и блок-схему, поскольку вы придерживаетесь того, что происходит в каждой ситуации. IP-адрес веб-узла — 171.16.23.1.

```
access-list 100 permit tcp any host 171.16.23.1 eq 80 access-list 100 deny ip any any
```

Пакет является начальным фрагментом или не фрагментом, предназначенным для сервера

на порту 80:

Первая линия ACL содержит сведения об уровнях 3 и 4, которые совпадают со Сведениями об уровнях 3 и 4 в пакете, таким образом, разрешен пакет.

Пакет – начальный фрагмент или не фрагмент, предназначенный для сервера на порт 21:

1. Первая линия ACL содержит сведения об уровнях 3 и 4, но информация уровня 4 в ACL не совпадает с пакетом, таким образом, обработана следующая строка ACL.
2. Вторая строка ACL запрещает все пакеты, поэтому пакет запрещен.

Пакет – неначальный фрагмент сервера в порте 80 потока:

Первая строка ACL содержит сведения уровня 3 и уровня 4, сведения уровня 3 в ACL соответствуют пакету, и действие ACL – разрешить, следовательно, пакет разрешается.

Этот пакет не является начальным фрагментом потока к серверу по порту 21:

Первая строка списка управления доступом содержит сведения третьего и четвертого уровней модели OSI. Информация третьего уровня в ACL соответствует пакету. В пакете отсутствует информация четвертого уровня, и действием ACL должно быть разрешение, поэтому данный пакет разрешен.

Этот пакет является начальным фрагментом, не фрагментом или не начальным фрагментом к другому узлу в подсети сервера:

1. Первая строка ACL содержит информацию уровня 3, которая не совпадает с информацией третьего уровня в пакете (конечного адреса), поэтому обрабатывается следующая строка ACL.
2. Вторая строка ACL запрещает все пакеты, поэтому пакет запрещен.

Пример 2

Следующие те же пять возможных сценариев включают различные типы пакетов, встречающихся с ACL 101. Снова, см. таблицу и блок-схему, поскольку вы придерживаетесь того, что происходит в каждой ситуации. IP-адрес веб-узла — 171.16.23.1.

```
access-list 101 deny ip any host 171.16.23.1 fragments access-list 101 permit tcp any host 171.16.23.1 eq 80 access-list 101 deny ip any any
```

Пакет является начальным фрагментом или нефрагментом, предназначенным для сервера на порту 80:

1. Первая строка ACL содержит сведения слоя 3, соответствующие сведениям слоя 3 пакета. Действие списка прав доступа (ACL) должно запретить, но потому что ключевое слово **фрагментов** присутствует, следующая запись списка контроля доступа обработана.
2. Вторая строка ACL содержит сведения третьего и четвертого уровня, которые

соответствуют пакету, поэтому пакет разрешается.

Пакет является начальным фрагментом или нефрагментом, предназначенным для сервера на порту 21:

1. Первая линия ACL содержит информацию сетевого уровня 3, которая совпадает с пакетом, но запись ACL также имеет ключевое слово **фрагментов**, которое не совпадает с пакетом, потому что FO = 0, таким образом, следующая запись списка контроля доступа обработана.
2. Вторая строка ACL содержит сведения третьего и четвертого уровней модели OSI. В этом случае информация уровня 4 не совпадает, таким образом, обработана следующая запись списка контроля доступа.
3. Третья строка ACL запрещает все пакеты, поэтому пакет запрещен

Пакет – неначальный фрагмент сервера в порте 80 потока:

Первая строка ACL содержит сведения слоя 3, соответствующие сведениям слоя 3 пакета. Следует помнить, что даже если это часть потока порта 80, информация уровня 4 отсутствует в неначальном фрагменте. Пакет запрещен, потому что совпадает информация сетевого уровня 3.

Этот пакет не является начальным фрагментом потока к серверу по порту 21:

Первая строка ACL содержит только данные уровня 3, соответствующие информации в пакете, поэтому пакет отклоняется.

Этот пакет является начальным фрагментом, не фрагментом или не начальным фрагментом к другому узлу в подсети сервера:

1. Первая строка списка ACL содержит только данные уровня 3 и не соответствует пакету. Поэтому обрабатывается следующая строка ACL.
2. Вторая строка ACL содержит сведения третьего и четвертого уровней модели OSI. Уровень 4 и информация сетевого уровня 3 в пакете не совпадают с уровнем 4 ACL, таким образом, обработана следующая строка ACL.
3. Третья линия ACL запрещает этот пакет

фрагментирует сценарии ключевых слов

Сценарий 1

Подключения маршрутизатора B к Web-серверу и администратор сети не хотят позволять любым фрагментам достигать сервера. Этот сценарий показывает то, что происходит, если администратор сети внедряет ACL 100 по сравнению с ACL 101. ACL применен входящий на Serial0 маршрутизаторов (s0) интерфейс и должен позволить только нефрагментированным пакетам достигать Web-сервера. Обратите внимание на структурную схему "Правила ACL2" и раздел "Как сопоставлять пакеты с ACL" по мере выполнения сценария.

Результат использования ключевого слова "fragments"

Ниже представлен ACL 100:

```
access-list 100 permit tcp any host 171.16.23.1 eq 80 access-list 100 deny ip any any
```

Первая линия ACL 100 разрешает доступ к серверу только по протоколу HTTP, а также позволяет пересылку неначальных фрагментов к любому TCP-порту сервера. Это разрешает эти пакеты, потому что неначальный фрагменты не содержат информацию уровня 4, и логика ACL предполагает что, если бы информация сетевого уровня 3 совпадает, то информация уровня 4 также совпала бы, если бы это было доступно. Вторая линия является неявной и отклоняет весь другой трафик.

Следует отметить, что, с Cisco IOS Software Release 12.1 (2) и 12.0 (11), новый код ACL отбрасывает фрагменты, которые не совпадают ни с какой другой линией в ACL. Более ранние релизы позволяют неначальный фрагменты через, если они не совпадают ни с какой другой линией ACL.

Далее следует ACL 101:

```
access-list 101 deny ip any host 171.16.23.1 fragments access-list 101 permit tcp any host 171.16.23.1 eq 80 access-list 101 deny ip any any
```

ACL 101 не позволяет неначальный фрагменты через серверу из-за первой линии. Неначальный фрагмент к серверу запрещен, когда это встречается с первой строкой списка контроля доступа, потому что информация сетевого уровня 3 в пакете совпадает с информацией сетевого уровня 3 в строке ACL.

Начальная буква или нефрагменты к порту 80 на сервере также совпадают с первой линией ACL для получения информации сетевого уровня 3, но потому что ключевое слово фрагментов присутствует, следующая запись списка контроля доступа (вторая линия) обработана. Вторая строка ACL разрешает исходные фрагменты или не-фрагменты, поскольку они соответствуют строке ACL для сведений третьего и четвертого уровней.

Неначальный фрагменты, предназначенные к портам TCP других хостов в 171.16.23.0 сетях, заблокированы этим ACL. Информация уровня 3 в этих пакетах не совпадает с информацией уровня 3 в первой линии ACL, так что следующая линия ACL обработана. Данные уровня 3, содержащиеся в этих пакетах, не соответствуют данным уровня 3, содержащимся и во второй строке ACL, поэтому обрабатывается третья строка ACL. Третья линия неявна и запрещает весь трафик.

В этом сценарии сетевой администратор решает реализовать ACL 101, так как при этом допускаются только нефрагментированные потоки HTTP на сервер.

Сценарий 2

У клиента есть интернет-соединение на двух других узлах, и между этими двумя узлами существует также закулисное соединение. Политика администратора сети должна позволить Группе в Узле 1 обращаться к серверу HTTP на Узле 2. Маршрутизаторы на обоих узлах используют частные адреса (RFC 1918) и Технология NAT для перевода пакетов, которые маршрутизируются через Интернет.

Администратор сети на Узле 1 является маршрутизацией в соответствии с политикой

частные адреса, назначенные на Группу A, так, чтобы они использовали черный ход через Serial0 A маршрутизатора (s0) при доступе к серверу HTTP на Узле 2. Маршрутизатор на Узле 2 имеет статический маршрут к 172.16.10.0, так, чтобы ответный трафик Группе A также маршрутизировался через черный ход. Весь другой трафик обрабатывается NAT и маршрутизируется через Интернет. В этом сценарии администратор сети должен решить, какое приложение или поток будет работать в случае фрагментирования пакетов. Не возможно сделать и HTTP и потоки Протокола FTP, работают в то же время потому что один или другие разрывы.

Обратите внимание на структурную схему "Правила ACL2" и раздел "Как сопоставлять пакеты с ACL" по мере выполнения сценария.

Пояснение опций администратора сети

В следующем примере Карта маршрутизации под названием FOO на маршрутизаторе A передает пакеты, которые совпадают с ACL 100 через к маршрутизатору B через s0. Все пакеты, которые не совпадают, обработаны NAT и берут маршрут по умолчанию через Интернет.

Примечание: Если пакет падает с нижней части ACL или запрещен им, то это не маршрутизируется политикой.

Ниже приводится частичная конфигурация маршрутизатора A, показывая, что route-map политики под названием FOO применен к интерфейсу e0, где трафик от Группы A вводит маршрутизатор:

```
hostname Router_A int e0 ip policy route-map FOO route-map FOO permit 10 match ip address 100
set ip next-hop 10.1.1.2 access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq
80 access-list 100 deny ip any any
```

ACL 100 позволяет маршрутизацию в соответствии с политикой и на начальной букве, нефрагментах и на неначальный фрагментах потоков HTTP к серверу. Начальная буква и нефрагменты потоков HTTP к серверу разрешены ACL и политикой, маршрутизировавшей, потому что они совпадают со Сведениями об уровнях 3 и 4 в первой строке списка контроля доступа. Неначальный фрагменты разрешены ACL и политикой, маршрутизировавшей, потому что информация сетевого уровня 3 в пакете также совпадает с первой строкой списка контроля доступа; логика ACL предполагает, что информация уровня 4 в пакете также совпала бы, если бы это было доступно.

Примечание: ACL 100 ломает другие типы фрагментированных потоков TCP между Группой A и сервером, потому что начальная буква и неначальный фрагменты добираются до сервера через другие пути; начальные фрагменты обрабатываются NAT и маршрутизируются через Интернет, но неначальный фрагменты того же потока являются маршрутизировавшей политикой.

Фрагментированный поток FTP помогает иллюстрировать проблему в этом сценарии. Начальные фрагменты FTP-потока соответствуют информации уровня 3 первой строки ACL, и не соответствуют данным уровня 4. Впоследствии они запрещаются второй строкой. Эти пакеты обрабатываются NAT и маршрутизируются по Интернету.

Неначальный фрагменты потока FTP совпадают с информацией сетевого уровня 3 в первой строке списка контроля доступа, и логика ACL принимает положительное совпадение на информации уровня 4. Эти пакеты маршрутизируются политикой, а узел, повторно

собирающий эти пакеты, не распознает начальные фрагменты как часть одного и того же потока, что и маршрутизируемые политикой неначальные фрагменты, поскольку NAT изменила адрес источника начальных фрагментов.

ACL 100 в конфигурации приведенной внизу решает проблему FTP. Первая линия ACL 100 запрещает и начальную букву и фрагменты FTP неначальных от Группы к серверу.

```
hostname Router_A int e0 ip policy route-map FOO route-map FOO permit 10 match ip address 100
set ip next-hop 10.1.1.2 access-list 100 deny tcp 172.16.10.0 0.0.0.255 host 192.168.10.1
fragments access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq 80 access-list
100 deny ip any any
```

Соответствие начальных фрагментов на информации сетевого уровня 3 в первой строке списка контроля доступа, но присутствие ключевого слова **фрагментов** заставляет следующую строку ACL быть обработанной. Начальный фрагмент не совпадает со второй строкой ACL для получения информации уровня 4, и таким образом, следующая неявная линия ACL обработана, который запрещает пакет. Неначальный фрагменты совпадают с информацией сетевого уровня 3 в первой линии ACL, таким образом, они запрещены. И начальная буква и неначальный фрагменты обрабатываются NAT и маршрутизируются через Интернет, таким образом, сервер не имеет никакой проблемы с повторной сборкой.

Решение проблемы потоков FTP ломает фрагментированные потоки HTTP, потому что начальные фрагменты HTTP являются теперь маршрутизировавшей политикой, но неначальный фрагменты обрабатываются NAT и маршрутизируются через Интернет.

Когда начальный фрагмент HTTP-потока от группы Group A к серверу встречается с первой строкой ACL, он совпадает с информацией 3 уровня в этом списке управления доступом, но из-за наличия ключевых слов фрагмента обработка начинается со следующей строки ACL. Вторая строка ACL позволяет, а политика маршрутизирует пакет на сервер.

Когда непервичные фрагменты HTTP, отправляемые из группы A на сервер, встречаются с первой строкой ACL, сведения уровня 3 в пакете сопоставляются со строкой ACL и пакет отвергается. Эти пакеты обрабатываются NAT и передаются через Интернет на сервер.

Первый ACL в этом сценарии позволяет фрагментированные потоки HTTP, и разрывы фрагментировали потоки FTP. Второй список управления доступом разрешает фрагментацию потоков FTP и прерывает фрагментированные потоки HTTP. Потоки TCP прерываются во всех случаях, так как исходные и последующие фрагменты достигают сервера различными путями. Невозможно произвести повторную сборку, так как NAT изменила исходный адрес неначальных фрагментов.

Невозможно сконструировать список управления доступом, позволяющий обоим типам фрагментированных потоков попадать на сервер. Поэтому администратор должен выбрать, какой поток он предпочитает.

Дополнительные сведения

- Страница поддержки IP-маршрутизации
- Cisco Systems – техническая поддержка и документация