Защита ядра: Списки управления доступом для защиты инфраструктуры

Содержание

Введение

В настоящем документе представлены инструкции и рекомендованные техники разворачивания списков управления доступом защиты инфраструктуры. Списки ACL для инфраструктуры применяются для минимизации рисков и эффективности прямых атак на инфраструктуру путем явного разрешения только авторизованного трафика на оборудование инфраструктуры и запрета всего остального транзитного трафика.

Защита инфраструктуры

Общие сведения

С целью защиты маршрутизаторов от различных рисков – случайных и злонамеренных – списки ACL для защиты инфраструктуры необходимо определять на точках входа в сеть. Списки управления доступом IPv4 и IPv6 отказывают в доступе от внешних источников на все адреса инфраструктуры, например, интерфейсы маршрутизаторов. В то же время, списки ACL разрешают непрерывный поток транзитного трафика и предоставляют основные RFC 1918 , RFC 3330 , а также фильтрацию ложных IP-пакетов.

Данные, принимаемые маршрутизатором, можно разделить на две обширные категории:

- трафик, который проходит через маршрутизатор по пути пересылки
- трафик, предназначенный для маршрутизатора через путь приема, для обработки его

процессором маршрутизации

При нормальной работе, основная часть трафика проходит через маршрутизатор по пути к конечному пункту назначения.

Однако процессору маршрутизации (RP) необходимо обрабатывать определенные типы данных напрямую, наиболее часто - протоколы маршрутизации, удаленный доступ к маршрутизаторам (например Secure Shell [SSH]) и трафик управления сетью, например, простой протокол управления сетью (SNMP). Кроме того, для протоколов, например, протокола управляющих сообщений Интернета (ICMP) и IP-параметров, необходима обработка с помощью RP. Наиболее часто прямой доступ к маршрутизаторам инфраструктуры необходим только из внутренних источников. Несколько заметных исключений включают внешний обмен трафиком по протоколу пограничных шлюзов (BGP), протоколы, которые завершаются на данном маршрутизаторе (например, общей инкапсуляцией маршрутов [GRE] или IPv6 через туннели IPv4), а также потенциально ограниченные пакеты ICMP для проверки соединения, например, сообщения эхо-запроса, ограничения ICMP и истекшего времени жизни (TTL) для трассировки.

Примечание: Помните, что ICMP часто используется для простых атак атаки Denial of Service (DoS) и должен только быть разрешен от внешних источников при необходимости.

У всех RP есть ограничения по производительности, в пределах которых они работают. Избыточный трафик, предназначенный для RP, может переполнить маршрутизатор. Это приведет к высокой загрузке CPU и, следовательно, к потерям пакетов и сбоям протокола маршрутизации, что вызовет отказ в обслуживании. С помощью фильтрации доступа к маршрутизаторам инфраструктуры из внешних источников снижается количество внешних рисков, связанных с прямой атакой на маршрутизатор. Внешние атаки не могут больше достигать оборудования инфраструктуры. Атака отбрасывается на входных интерфейсах автономной системы (AS).

Технологии фильтрации, описанные в этом документе, предназначены для фильтрации данных, предназначенных для оборудования сетевой инфраструктуры. Следует различать фильтрацию инфраструктуры и общую фильтрацию. Единственной целью списков ACL для защиты инфраструктуры является ограничение на гранулярном уровне протоколов и источников, которые могут получить доступ к оборудованию инфраструктуры.

Оборудование сетевой инфраструктуры охватывает следующие области:

- Все адреса для управления маршрутизаторами и коммутаторами, включая интерфейсы обратной связи
- Все адреса внутренних соединений: соединения маршрутизатор-маршрутизатор (доступ точка-точка и множественный)
- Внутренние серверы или службы, к которым необходимо ограничить доступ из внешних источников

В данном документе трафик, не предназначенный для инфраструктуры, часто называется транзитным трафиком.

Способы

Существует несколько способов защиты инфраструктуры:

- **Получение ACL (rACLs)**Платформы Cisco 12000 и 7500 поддерживают rACL, которые

фильтруют весь трафик, предназначенный для RP, и не влияют на транзитный трафик. Необходимо явно разрешить авторизированный трафик и применять rACL на каждом маршрутизаторе. Дополнительные сведения см. в разделе GSR: Получение списков управления доступом.

- **Списки ACL последовательно соединенных маршрутизаторов**Маршрутизаторы также можно защищать с помощью определения списков ACL, которые разрешают только авторизированный трафик на интерфейсы маршрутизатора, отклоняя весь остальной, кроме транзитного трафика, который должен быть явно разрешен. Данный ACL логически похож на rACL, но не влияет на транзитный трафик. Таким образом, он может оказывать негативное влияние на производительность с точки зрения скорости передачи маршрутизатора.
- **Граничная фильтрация с помощью списков ACL инфраструктуры**ACL можно применять на границе сети. Для поставщика услуг (SP) - это граница AS. Данный ACL явно фильтрует трафик, предназначенный для адресного пространства инфраструктуры. Для развертывания списков ACL граничной инфраструктуры необходимо четко определить пространство инфраструктуры и требуемые/авторизованные протоколы, которые получают доступ к данному пространству. ACL применяется при входе в сеть на всех внешних подключениях, например, одноранговых соединениях, подключениях пользователей и т.д.В настоящем документе описывается разработка и развертывание защиты оконечной инфраструктуры списков управления доступом.

Примеры ACL

Списки доступов IPv4 и IPv6 представляют собой простые, но реальные примеры типичных записей, необходимых при защите ACL. Эти базовые ACL необходимо настраивать с учетом элементов конфигурации конкретной площадки. В двойных средах IPv4 и IPv6 применяются два списка доступа.

Пример IPv4

```
!--- Anti-spoofing entries are shown here. !--- Deny special-use address sources. !--- Refer to RFC 3330 for additional special use addresses. access-list 110 deny ip host 0.0.0.0 any 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 !--- 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 !--- Deny your space as source from entering your AS. !--- Deploy only at the AS edge. access-list 110 deny ip YOUR_CIDR_BLOCK any !--- Permit BGP. access-list 110 permit tcp host bgp_peer host router_ip eq bgp access-list 110 permit tcp host bgp_peer eq bgp host router_ip !--- Deny access to internal infrastructure addresses. access-list 110 deny ip any INTERNAL_INFRASTRUCTURE_ADDRESSES !--- Permit transit traffic. access-list 110 permit ip any any
```

Пример IPv6

Список доступа IPv6 необходимо применять в качестве расширенного именованного списка доступа.

```
!--- Configure the access-list. ipv6 access-list iacl !--- Deny your space as source from entering your AS. !--- Deploy only at the AS edge. deny ipv6 YOUR_CIDR_BLOCK_IPV6 any !--- Permit multiprotocol BGP. permit tcp host bgp_peer_ipv6 host router_ipv6 eq bgp permit tcp host bgp_peer_ipv6 eq bgp host router_ipv6 !--- Deny access to internal infrastructure addresses. deny ipv6 any INTERNAL_INFRASTRUCTURE_ADDRESSES_IPV6 !--- Permit transit traffic. permit ipv6
```

```
any any
```

Примечание: Ключевое слово log можно использовать для предоставления дополнительных сведений об источнике и пунктах назначения для данного протокола. Хотя данное ключевое слово предоставляет подробные сведения обращений ACL, чрезмерные обращения к записи ACL, которая использует ключевое слово log, увеличивают использование CPU. Влияние регистрации на производительность системы зависит от платформы. Также использование ключевого слова log выключает коммутацию Cisco Express Forwarding (CEF) для пакетов, которые совпадают с записью в списке доступа. Вместо этого пакеты быстро переключаются.

Разработка защиты ACL

В целом, список ACL инфраструктуры состоит из четырех разделов:

- Специальный адрес и записи для аутентификации адресов, которые запрещают неавторизованным источникам и пакетам с исходными адресами на сервере доступа доступ к серверу с внешнего источника**Примечание:** В RFC 3330 определены адреса протокола IPv4 для специального использования которые могут требовать фильтрации. RFC 1918 определяет зарезервированное адресное пространство, которому не могут принадлежать адреса источников в Интернете. RFC 3513 определяет архитектуру адресации IPv6. В RFC 2827 представлены указания по входящей фильтрации.
- Явно разрешенный трафик от внешних источников, направляемый на адреса инфраструктуры
- **выражения deny для всего другого внешнего трафика на адреса инфраструктуры**
- **выражения permit для другого трафика для обычного магистрального трафика на пути к пунктам назначения вне инфраструктуры**

Последняя строка в списке ACL инфраструктуры разрешает транзитный трафик: **permit ip any any для IPv4 и permit ipv6 any any для IPv6.** Эта запись гарантирует, что всем IP-протоколам разрешено передавать данные через ядро, а клиенты могут запускать приложения без затруднений.

Первым шагом в разработке ACL для защиты инфраструктуры является понимание, какие протоколы требуются. Хотя на каждой площадке есть свои особые требования, обычно разворачиваются определенные протоколы, которые необходимо освоить. Например, необходимо явно разрешить внешние BGP на внешних одноранговых узлах. Необходимо также явно разрешить другие протоколы, для которых требуется прямой доступ на маршрутизатор инфраструктуры. Например, если вы завершаете туннель GRE на маршрутизаторе основной инфраструктуры, вы должны явно разрешить протокол 47 (GRE). Аналогично, если вы завершаете IPv6 через туннель IPv4 на маршрутизаторе основной инфраструктуры, вы также должны явно разрешить протокол 41 (IPv6 over IPv4).

Классификацию ACL можно использовать для идентификации необходимых протоколов. **Классификация ACL состоит из выражений permit для различных протоколов, которые могут быть предназначены для маршрутизатора инфраструктуры.** Полный список см. в приложении поддерживаемые IP-протоколы в ПО Cisco IOS®. **Использование команды show access-list command для отображения счетчика обращений к элементам списка контроля доступа (ACE) определяет необходимые протоколы. Сомнительные или непредвиденные результаты должны быть проверены и изучены до создания выражений permit для неожидаемых протоколов.**

Например, IPv4 ACL определяет, необходимо ли разрешить GRE, IPsec (ESP) и туннелирование IPv6 (IP-протокол 41).

```
access-list 101 permit GRE any infrastructure_ips
access-list 101 permit ESP any infrastructure_ips
access-list 101 permit 41 any infrastructure_ips
access-list 101 permit ip any infrastructure_ips log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted. access-list 101 permit ip any any interface <int> ip access-group 101 in
```

IPv6 ACL можно использовать, чтобы определять, необходимо ли разрешать GRE и IPsec (ESP).

```
ipv6 access-list determine_protocols
 permit GRE any infrastructure_ips_ipv6
 permit ESP any infrastructure_ips_ipv6
 permit ipv6 any infrastructure_ips_ipv6 log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted. permit ipv6 any any interface <int> ipv6 traffic-filter determine_protocols in
```

Помимо требуемых протоколов, необходимо определить пространство для адресов инфраструктуры, так как ACL защищает данное пространство. Пространство для адресов инфраструктуры включает любые адреса, которые используются во внутренней сети, и к которым редко получают доступ внешние источники, например, интерфейсы маршрутизаторов, адресация соединений "точка-точка" и важнейшие службы инфраструктуры. Так как данные адреса используются для места назначения списка ACL инфраструктуры, правильные выводы являются особо важными. При любой возможности данные адреса должны быть сгруппированы в блоки бесклассовой междоменной маршрутизации (CIDR).

С помощью использования определенных протоколов и адресов можно создавать списки ACL инфраструктуры, чтобы разрешить протоколы и защитить адреса. Помимо прямой защиты, ACL также предоставляет первую линию защиты против определенных типов недопустимого трафика в сети Интернет.

- Пространство RFC 1918 необходимо запретить.
- Пакеты, адрес источника которых попадает в особое адресное пространство, как определено в RFC 3330, необходимо запретить.
- Необходимо применить фильтры защиты от ложных IP пакетов. (Ваше адресное пространство никогда не должно быть источником пакетов, приходящих извне в вашу AS.).)

Этот вновь созданный список ACL необходимо применять на входе на всех входящих интерфейсах. Дополнительные сведения см. в разделах инструкции по развертыванию и примеры развертывания.

Списки ACL и фрагментированные пакеты

Списки ACL имеют ключевое слово fragments, которое активирует специальный режим обработки фрагментированных пакетов. Без этого ключевого слова **фрагментов** на фрагменты неначальных, которые совпадают с операторами Уровня 3 (независимо от информации уровня 4) в ACL, влияют разрешение или инструкция deny записи, с которой совпадают. Однако путем добавления ключевого слова **фрагментов**, можно вынудить ACL или запретить или разрешить фрагменты неначальных с большим количеством глубины детализации. Это поведение является тем же и для IPv4 и для Ipv6 access-list, за исключением того, что, в то время как ACL IPv4 позволяют использование ключевого слова

фрагментов в операторах Уровня 3 и Уровня 4, ACL IPv6 только позволяют использование ключевого слова фрагментов в операторах Уровня 3.

Фрагменты фильтрации добавляют дополнительный уровень защиты от Атаки типа отказ в обслуживании (DOS), которая использует фрагменты неначальных (т.е. FO> 0). **Использование выражения deny для неначальных фрагментов в начале списка ACL запрещает доступ к маршрутизатору для всех неначальных фрагментов. В редких случаях допустимая операция может потребовать фрагментации и, таким образом, будет отфильтрована при наличии в списке ACL оператора deny fragment.**

Например, рассмотрим частичный IPv4ACL:

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

С помощью добавления данных записей в начало ACL запрещается любой доступ неначальных фрагментов к основному маршрутизатору, тогда как нефрагментированные пакеты или начальные фрагменты переходят на следующие строки ACL, не испытывая влияния выражений deny fragment. Предшествующая команда ACL упрощает классификацию атаки, так как каждый протокол – универсальный протокол передачи данных (UDP), TCP и ICMP – увеличивает отдельные счетчики в ACL.

Это - сопоставимый пример для IPv6:

```
ipv6 access-list iacl deny ipv6 any infrastructure_IP fragments
```

Добавление этой записи в начало ACL IPv6 запрещает любой доступ фрагмента неначальных к центральным маршрутизаторам. Как ранее обращено внимание, Ipv6 access-list только позволяет использование ключевого слова фрагментов в операторах Уровня 3.

Так как многие атаки основаны на "затоплении" опорных маршрутизаторов фрагментированными пакетами, фильтрация входящих фрагментов в инфраструктуре опорной сети – дополнительное средство защиты, позволяющее с помощью простых правил сопоставления на уровне 3 в списках доступа для инфраструктуры предотвратить попытки злоумышленного внедрения фрагментов.

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

Оценка рисков

Рассмотрим две области ключевого риска во время разворачивания списков ACL для защиты инфраструктуры:

- **Убедитесь, что соответствующие выражения permit/deny находятся где нужно. Чтобы ACL был более эффективным, необходимо разрешить все требуемые протоколы и защитить правильное адресное пространство с помощью выражений deny.**
- Производительность ACL зависит от платформы. Ознакомьтесь с характеристиками производительности вашего ПО перед развертыванием списков ACL.

Как всегда, рекомендуется перед развертыванием проверить свою разработку в лаборатории.

Приложения

Поддерживаемые протоколы IP в Cisco IOS

Программное обеспечение Cisco IOS поддерживает следующие IP-протоколы:

- 1 – ICMP
- 2 – IGMP
- 3 – GGP
- 4 – IP в IP-инкапсуляции
- 6 (TCP)
- 8 – EGP
- 9 – IGRP
- 17 (UDP)
- 20 – HMP
- 27 – RDP
- 41 – IPv6 в туннелировании IPv4
- 46 – RSVP
- 47 – GRE
- 50 (ESP)
- 51 – AH
- 53 – SWIPE
- 54 – NARP
- 55 – IP-мобильность
- 63 – любая локальная сеть
- 77 – Sun ND
- 80 – ISO IP
- 88 – EIGRP
- 89 – OSPF
- 90 – Sprite RPC
- 91 – LARP
- 94 – KA9Q/NOS-совместимая IP через IP
- 103 – PIM
- 108 – IP-компрессия
- 112 – VRRP
- 113 – PGM
- 115 – L2TP
- 120 – UTI
- 132 – SCTP

Инструкции по развертыванию

Cisco рекомендует осторожные способы развертывания. Чтобы успешно развернуть списки ACL инфраструктуры, необходимо получить подробные сведения о требуемых протоколах и четко уяснить и определить адресное пространство. В данных инструкциях описан очень осторожный способ развертывания списков ACL для защиты с помощью итеративного подхода.

1. **Определите протоколы, которые используются в сети с классификацией ACL.**Разверните ACL, который разрешит все известные протоколы, у которых есть доступ к устройствам инфраструктуры. **В данном открытии ACL есть адрес источника any и место назначения, которое охватывает IP-пространство инфраструктуры. Регистрация используется для создания списка адресов источника, которые совпадают с выражениями permit протокола. Последняя строка, разрешающая ip any any (IPv4) или ipv6 any any (IPv6), необходима для разрешения потока трафика.**Цель состоит в том, чтобы определить, какие протоколы использует определенная сеть. Регистрация используется в анализе, чтобы определить, что еще может взаимодействовать 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. Также использование ключевого слова log выключает коммутацию Cisco Express Forwarding (CEF) для пакетов, которые совпадают с записью в списке доступа.** Вместо этого пакеты быстро переключаются. **Используйте ключевое слово log недолго, и только если необходимо классифицировать трафик.**
2. **Просмотрите идентифицированные пакеты и начните фильтровать доступ к процессору маршрутизации RP.Так как в шаге 1 пакеты, отфильтрованные с помощью ACL, были определены и просмотрены, разверните ACL с помощью permit any source для адресов инфраструктуры для разрешенных протоколов. Также как и в шаге 1, ключевое слово log предоставляет дополнительные сведения о пакетах, которые совпадают с записями permit. Использование deny any в конце помогает определить неожидаемые пакеты, предназначенные для маршрутизаторов. Последней строкой этого ACL должно быть выражение permit ip any any (IPv4) или permit ipv6 any any (IPv6) для разрешения потока транзитного трафика.** В ACL будет обеспечена основная защита, а сетевые инженеры смогут гарантировать, что весь необходимый трафик является разрешенным.
3. **Ограничьте адреса источников.**Получив четкое представление о том, какие протоколы должны быть разрешены, можно выполнить дополнительную фильтрацию с тем, чтобы доступ к таким протоколам был только у авторизованных источников. Например, можно разрешить внешних BGP-соседей или определенные адреса одноранговых узлов GRE.Этот шаг снижает риск без нарушения работы служб и позволяет применять гранулярный контроль к источникам, имеющим доступ к оборудованию инфраструктуры.
4. **Ограничьте в ACL адреса мест назначения.** ***Дополнительно***Некоторые провайдеры могут разрешать определенным протоколам использовать только конкретные адреса назначения на маршрутизаторе. Этот заключительный этап предназначен для ограничения диапазона адресов пунктов назначения, которые будут принимать трафик для протокола.

Примеры развертывания

Пример IPv4

В данном примере IPv4 изображен список ACL инфраструктуры, защищающий маршрутизатор на основе следующей адресации:

- Адресный блок ISP – 169.223.0.0/16.
- Блок инфраструктуры ISP – 169.223.252.0/22.
- Возвратная петля для маршрутизатора 169.223.253.1/32.
- Маршрутизатор является одноранговым и устанавливает связь с 169.254.254.1 (на адрес 169.223.252.1).

Показанный список ACL для защиты инфраструктуры разработан на основе предыдущих сведений. ACL разрешает внешний обмен трафика BGP с внешним одноранговым узлом, предоставляет фильтры защиты от ложных IP пакетов и защищает инфраструктуру от всякого внешнего доступа.

```
!
no access-list 110
!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 – Anti-spoofing Denies !--- These ACEs deny fragments, RFC 1918 space, !--- invalid source addresses, and spoofs of !--- internal space (space as an external source). ! !--- Deny fragments to the infrastructure block. access-list 110 deny tcp any 169.223.252.0 0.0.3.255 fragments access-list 110 deny udp any 169.223.252.0 0.0.3.255 fragments access-list 110 deny icmp any 169.223.252.0 0.0.3.255 fragments !--- Deny special-use address sources. !--- See RFC 3330 for additional special-use addresses. access-list 110 deny ip host 0.0.0.0 any 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 !--- 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 !--- Deny our internal space as an external source. !--- This is only deployed at the AS edge access-list 110 deny ip 169.223.0.0 0.0.255.255 any
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 – Explicit Permit !--- Permit only applications/protocols whose destination !--- address is part of the infrastructure IP block. !--- The source of the traffic should be known and authorized. ! !--- Note: This template must be tuned to the network's !--- specific source address environment. Variables in !--- the template need to be changed. !--- Permit external BGP. access-list 110 permit tcp host 169.254.254.1 host 169.223.252.1 eq bgp access-list 110 permit tcp host 169.254.254.1 eq bgp host 169.223.252.1 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 – Explicit Deny to Protect Infrastructure access-list 110 deny ip any 169.223.252.0 0.0.3.255 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 4 – Explicit Permit for Transit Traffic access-list 110 permit ip any any
```

Пример IPv6

В данном примере IPv6 изображен список ACL инфраструктуры, защищающий маршрутизатор на основе следующей адресации:

- Полный префиксный блок, выделенный интернет-провайдеру, 2001:0DB8::/32.
- Блок префикса IPv6, используемый интернет-провайдером для адресов инфраструктуры сети, 2001:0DB8:C18::/48.
- Существует маршрутизатор равноправного информационного обмена BGP с исходным адресом IPv6 2001:0DB8:C18:2:1:: 1, который взаимодействует к целевому адресу IPv6 2001:0DB8:C19:2:1:: _____ F.

Показанный список ACL для защиты инфраструктуры разработан на основе предыдущих сведений. ACL разрешает внешний обмен трафика мультипротокола BGP с внешним одноранговым узлом, предоставляет фильтры защиты от ложных IP пакетов и защищает инфраструктуру от внешнего доступа.

```
no ipv6 access-list iacl
ipv6 access-list iacl
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 – Anti-spoofing and Fragmentation Denies !--- These ACEs deny fragments and spoofs
```

```
of !--- internal space as an external source. !--- Deny fragments to the infrastructure block.
deny ipv6 any 2001:0DB8:C18::/48 fragments !--- Deny our internal space as an external source.
!--- This is only deployed at the AS edge. deny ipv6 2001:0DB8::/32 any
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 – Explicit Permit !--- Permit only
applications/protocols whose destination !--- address is part of the infrastructure IP block. !-
-- The source of the traffic should be known and authorized. !--- Note: This template must be
tuned to the !--- specific source address environment of the network. Variables in !--- the
template need to be changed. !--- Permit multiprotocol BGP. permit tcp host 2001:0DB8:C19:2:1::F
host 2001:0DB8:C18:2:1::1 eq bgp permit tcp host 2001:0DB8:C19:2:1::F eq bgp host
2001:0DB8:C18:2:1::1 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 –
Explicit Deny to Protect Infrastructure deny ipv6 any 2001:0DB8:C18::/48
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 4 – Explicit Permit for
Transit Traffic permit ipv6 any any
```

Дополнительные сведения

- Страница поддержки списков доступа
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация