GSR: Получение списков управления доступом

Содержание

Введение

Этот документ описывает новую функцию защиты — списки управления доступом для входящих вызовов (rACL)1 и излагает рекомендации и указания по развертыванию rACL. Списки управления доступом для входящих вызовов используются для повышения уровня безопасности на маршрутизаторах Cisco 12000, защищая процессор гигабитного канала маршрутизатора (GRP) от ненужного трафика и спама. Списки ACL для входящих вызовов добавлены в порядке особого исключения из ограничений цикла сопровождения для выпуска ПО Cisco IOS® 12.0.21S2 и встроены в выпуск ПО Cisco IOS 12.0(22)S.

Защита GRP

Данные, полученные маршрутизатором гигабитного коммутатора (GSR), могут быть разделены на две общих категории:

- Трафик, который проходит через маршрутизатор по пути пересылки.
- Трафик, который должен быть передан через тракт приема GRP для дальнейшего анализа.

На нормальных работах большая часть трафика просто течет через GSR по пути к другим назначениям. Однако GRP должен обработать определенные типы данных, прежде всего протоколы маршрутизации, доступ удаленного маршрутизатора и трафик при управлении сетью (такие как Простой протокол управления сетью [SNMP]). В дополнение к этому трафику другие пакеты Уровня 3 могли бы потребовать гибкости обработки GRP. Они

включали бы определенные IP - режимы и определенные формы пакетов Протокола ICMP. См. приложение на получают смежности и плыл на плоскодонке пакеты для дополнительных сведений относительно rACL и трафика тракта приема на GSR.

GSR имеет несколько путей данных, каждое обслуживание различные формы трафика. Передача трафика происходит от входящей линейной карты (LC) к системе коммутации, а затем к выходной карте для доставки на следующий интервал связи. В дополнение к пути данных транзитного трафика GSR имеет два других пути для локальной обработки требования трафика: LC к ЦП LC и LC к ЦП LC к матрице к GRP. Следующая таблица содержит пути для нескольких часто используемых возможностей и протоколов.

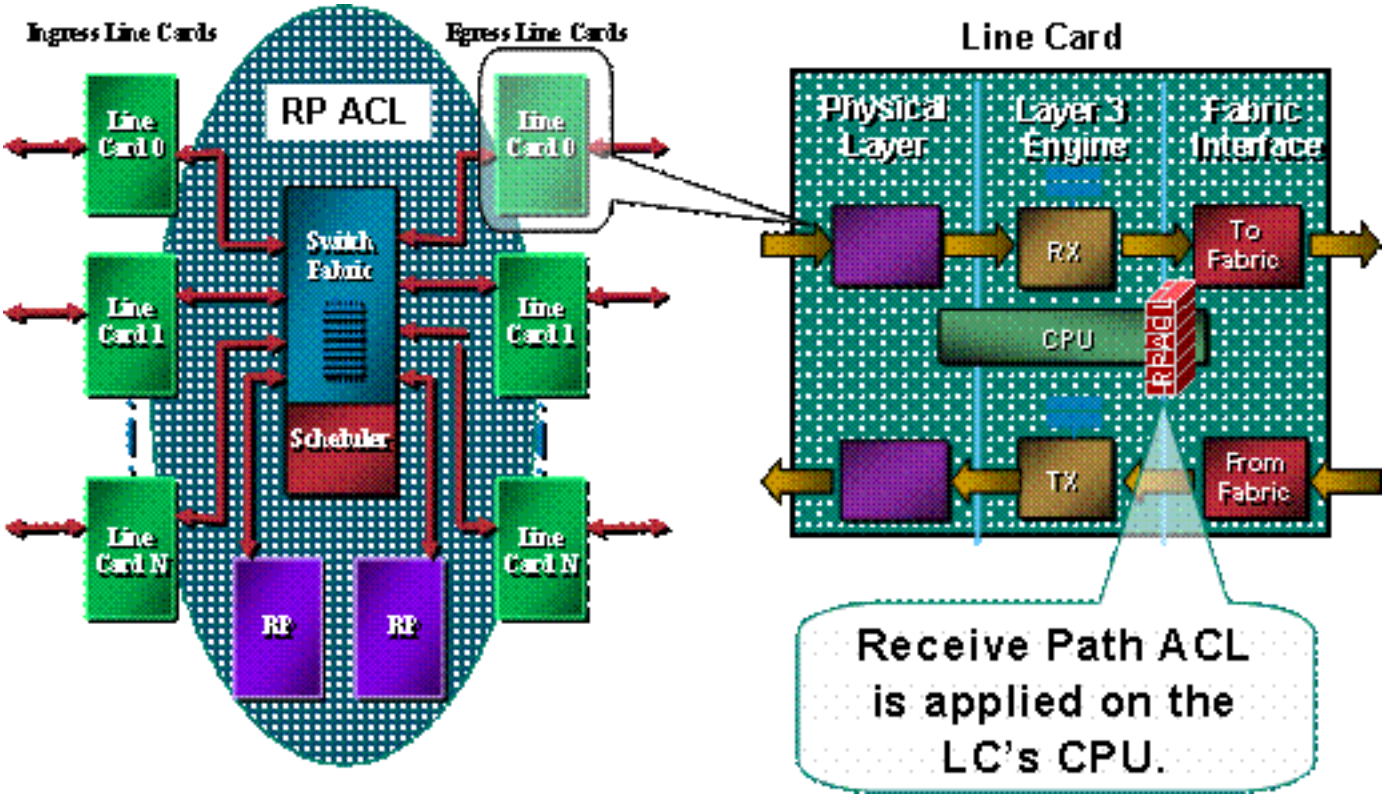
Тип трафика	Путь данных
Обычный (транзитный) трафик	LC к матрице к LC
Маршрутизация Протоколов/SSH/SNMP	LC к ЦП LC к матрице к GRP
ЭХО - ЗАПРОС ICMP (эхо-запрос)	LC к ЦП LC
Регистрация	

Процессор маршрута для GSR имеет ограниченную возможность обработки трафика, доставленного с LC и предназначенного для самого GRP. Если большой объем данных требует плавания на плоскодонке к GRP, тот трафик может сокрушить GRP. Это приводит к эффективной атаке атаки Denial of Service (DoS). ЦП GRP изо всех сил пытается не отставать от просмотра пакетов и начинает отбрасывать пакеты, лавинно рассылая очереди Выборочного сброса пакетов (SPD) и ожидание ввод. [2] GSRs должны быть защищены против трех сценариев, которые могут следовать из атак DoS, направленных на GRP маршрутизатора.

- Потери пакетов протокола маршрутизации при широковещательной передаче с обычным приоритетом
- Сеанс управления (Telnet, Secure Shell [SSH], SNMP) потеря пакета от лавинной рассылки обычного приоритета
- Потеря пакета из высокоприоритетного лавинного спуфинга

Потенциальные потери данных протокола маршрутизации во время лавинной рассылки обычного приоритета в настоящее время облегчаются статической классификацией и ограничением скорости трафика, предназначенного к GRP от LC. К сожалению, у этого подхода есть ограничения. Если атака отправлена через несколько LC, ограничение скорости для трафика обычного приоритета, предназначенного к GRP, недостаточно для гарантии защиты высокоприоритетным данным протокола маршрутизации. Понижение порога, в котором данные обычного приоритета отброшены для обеспечивания такой защиты только, усиливает потерю трафика управления от лавинной рассылки обычного приоритета.

Поскольку этот образ показывает, rACL выполняется на каждом LC, прежде чем пакет будет передан к GRP.



Механизм защиты для GRP требуется. rACL влияют на трафик, который передается GRP из-за, получают смежности. Получите смежности, смежности скоростной маршрутизации Cisco для трафика, предназначенного к IP-адресам маршрутизатора, таким как широковещательный адрес или адреса, настроенные на интерфейсах маршрутизатора. [3] Дополнительную информацию см. в разделе приложения по, получают смежности и плыл на плоскодонке пакеты.

Трафик, который вводит LC, сначала передается локальному ЦП LC и пакетам, которые требуют, обработка GRP помещены в очередь для передачи процессору маршрута. Получение ACL создается в GRP, а затем передается в центральные процессоры различных LC. Прежде чем трафик передается от ЦП LC до GRP, трафик по сравнению с rACL. Если разрешено, в то время как весь другой трафик запрещен, трафик проходит к GRP. RACL проверяется прежде функции ограничения скорости LC к GRP. Поскольку rACL используется для всех полученных сообщений о смежности, то некоторые пакеты, обрабатываемые CPU на LC (например, эхо-запросы) также подлежат фильтрации rACL. Это следует принимать во внимание при создании записей rACL.

Получите ACL, часть первая программного диапазона multipart для механизмов для защиты ресурсов в маршрутизаторе. Последующие задачи будут включать компонент ограничения скорости в rACL.

Влияние на производительность

Никакая память не использована кроме этого необходимого для удержания одиночной записи конфигурации и самого определенного списка доступа. RACL скопирован к каждому LC, таким образом, небольшая область памяти взята на каждом LC. В целом, используемые ресурсы являются крохотными, особенно при сравнении с преимуществами развертываний.

Получить ACL не влияет на производительность переданного трафика. RACL только применяется для получения трафика смежности. Переданный трафик никогда не подвергается rACL. Транзитный трафик фильтруется при помощи списков управления

доступом на интерфейсе. Эти “обычные” ACL применены к интерфейсам в указанном направлении. Трафик подвергается Обработке ACL до обработки rACL, таким образом, трафик, запрещенный интерфейсным ACL, не будет получен rACL. [4]

LC, выполняющий фактическую фильтрацию (другими словами, LC, получающий трафик, фильтруемый rACL), будет иметь повышенную загрузку ЦП из-за обработки rACL. Эта повышенная загрузка ЦП, однако, вызвана большим объемом трафика, предназначенного к GRP; преимущество GRP защиты rACL далеко перевешивает повышенную загрузку ЦП на LC. Загруженность CPU на LC будет меняться в зависимости от типа механизма LC. Например, учитывая ту же атаку, LC механизма 3 будет иметь более низкую загрузку ЦПУ, чем механизм 0 LC.

Включение турбо ACL (при помощи **команды access-list compiled**) преобразовывает ACL в очень эффективную серию записей таблицы поиска. Когда турбо ACL включены, глубина rACL не влияет на производительность. Другими словами, скорость обработки независима от количества записей в ACL. Если rACL будет короток, то турбо ACL не значительно увеличат производительность, но используют память; с короткими rACL скомпилированные ACL вероятны не необходимые.

Путем защиты GRP rACL помогает гарантировать маршрутизатор и, в конечном счете, устойчивость сети во время атаки. Как описано выше, rACL обработан на ЦП LC, таким образом, загрузка ЦПУ на каждом LC увеличится, когда большой объем данных будет направлен на маршрутизатор. На E0/E1 и некоторых связках (bundle) E2, загрузке ЦПУ 100 + % мог бы привести к протоколу маршрутизации и отбрасываниям канального уровня. Эти отбрасывания локализованы на плате, а процессы маршрутизации GRP защищены для поддержания устойчивости· Когда под нагрузкой большая и только передают приоритетам 6 и 7 трафика к протоколу маршрутизации, карты E2 с поддерживающим регулировку микрокодом [5] активируют режим дросселирования. Другие типы модуля имеют архитектуры multiqueue; например, карты E3 имеют три очереди к ЦП, с пакетами протокола маршрутизации (приоритеты 6/7) в отдельном, очереди с высоким приоритетом. Высокий ЦП LC, пока пакеты с высоким приоритетом не вызывают его, не приведет к отбрасываниям протокола маршрутизации. Пакеты к очередям с более низким приоритетом будут отброшены хвостом. Наконец, основанные на E4 карты имеют восемь очередей к ЦП с одним специализированным пакетам протокола маршрутизации.

Синтаксис

Получить ACL применен со следующей командой глобальной кофигурации для распределения rACL каждому LC в маршрутизаторе.

[no] ip receive access-list *<num>*

В этом синтаксисе ***<num>*** определен следующим образом.

[no] ip receive access-list *<num>*

Базовый шаблон и примеры ACL

Чтобы быть в состоянии использовать эту команду, необходимо определить список доступа, который определяет трафик, которому нужно позволить говорить с маршрутизатором. В список доступа должны быть включены протоколы маршрутизации и управление трафиком

(протокол пограничных шлюзов BGP, протокол открытого поиска кратчайшего пути OSPF, SNMP, SSH, Telnet). Дополнительные сведения см. в разделе указаний по развертыванию.

В следующем примере ACL предоставляет простую структуру и некоторые примеры конфигурации, которые можно настроить на определенное использование. В списке ACL содержатся параметры конфигурации для нескольких широко используемых служб и протоколов. Для SSH, Telnet и SNMP, адрес обратной связи используется в качестве назначения. Для протоколов маршрутизации используется фактический интерфейсный адрес. Выбор интерфейсов маршрутизатора для использования в rACL определяется политиками и операциями локального узла. Например, если loopback используются для всех сеансов с равноправным участием BGP, то только те loopback должны быть разрешены в **операторах permit** для BGP.

[no] ip receive access-list *<num>*

Как со всеми ACL Cisco, существует неявная **инструкция deny** в конце списка доступа, таким образом, будет запрещен любой трафик, который не совпадает с записью в ACL.

Примечание: Регистрационное ключевое слово может использоваться, чтобы помочь классифицировать трафик, предназначенный к GRP, который не разрешен. Несмотря на то, что **регистрационное** ключевое слово предоставляет полезные сведения в подробные данные соответствий ACL, чрезмерные соответствия к записи ACL, которая использует это ключевое слово, увеличат загрузку ЦПУ LC. Влияние на производительность, привязанное к регистрации, будет меняться в зависимости от типа модуля LC. В целом регистрация должна использоваться только при необходимости на механизмах 0/1/2. Для механизмов 3/4/4 +, регистрируя результаты в намного меньшем количестве влияния из-за производительности повышенной загрузки CPU и архитектуры multiqueue.

Уровень детализации данного списка доступа определяется локальной политикой безопасности (например, уровнем фильтрации, необходимым для окружения OSPF).

rACLS и фрагментированные пакеты

Списки ACL имеют ключевое слово fragments, которое активирует специальный режим обработки фрагментированных пакетов. В целом на неначальный фрагменты, которые совпадают с операторами L3 (независимо от информации о L4) в ACL, влияют **разрешение** или **инструкция deny** записи, с которой совпадают. **Обратите внимание на то, что использование ключевого слова fragments может привести к большей степени структурированности запрещенных или разрешенных неначальных фрагментов.**

В контексте rACL фильтрация фрагментов добавляет дополнительный уровень защиты от атаки DoS, которая использует только неначальный фрагменты (такие как FO> 0). **Использование инструкции deny для неначальных фрагментов в начале rACL запрещает доступ к маршрутизатору для всех неначальных фрагментов**. Если **опровергать** заявление **фрагмента** существует в rACL, под редкими случаями действительный сеанс мог бы потребовать фрагментации и поэтому фильтруется.

Например, считайте частичный ACL показанным ниже.

```
access-list 110 deny tcp any any fragments
access-list 110 deny udp any any fragments
access-list 110 deny icmp any any fragments
```

```
<rest of ACL>
```

В то время как нефрагментированные пакеты или начальные фрагменты проходят к следующим строкам rACL, незатронутого **опровергать** заявлениями **фрагмента**, добавление этих записей в начало rACL запрещает любой доступ неначальный фрагмента к GRP. Вышеупомянутый фрагмент rACL также упрощает классификацию атаки начиная с каждого протокола – Универсального протокола передачи дэйтаграмм (UDP), TCP, и ICMP – инкременты отдельные счетчики в ACL.

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

Оценка рисков

Гарантируйте, что rACL не фильтрует предельный трафик, такой как протоколы маршрутизации или интерактивный доступ к маршрутизаторам. Фильтрация необходимый трафик могла привести к неспособности удаленно обратиться к маршрутизатору, таким образом требуя консольного соединения. Поэтому лабораторные конфигурации должны подражать действительному развертыванию максимально близко.

Как всегда, Cisco рекомендует протестировать эту функцию в лабораторной работе до развертываний.

Приложения и примечания

Прием смежных узлов и выбиваемых пакетов

Как описано ранее в этом документе, некоторые пакеты требуют Обработки протокола маршрутизации шлюзов. Пакеты направляются из области перенаправления данных к GRP. Это - список стандартных форм данных Уровня 3, которые требуют доступа GRP.

- Протоколы маршрутизации
- Трафик управления многоадресной рассылкой (OSPF, Протокол маршрутизатора горячего резервирования [HSRP], Протокол распределения метки [TDP], Независимая от протокола групповая адресация [PIM] и такой)
- Пакеты Многопротокольной коммутации по меткам (MPLS), нуждающиеся во фрагментации
- Пакеты с определенными параметрами IP, такими как оповещение маршрутизатора
- Первый пакет многоадресных рассылок
- Фрагментированные пакеты ICMP, которые требуют повторной сборки
- Весь трафик, предназначенный к самому маршрутизатору (за исключением трафика, обрабатываемого на LC)

Так как rACL применяются для получения смежностей, rACL фильтрует некоторый трафик, который не плывется на плоскодонке к GRP, но является получить смежностью. Наиболее частый пример – запрос эха ICMP (проверка доступности). Эхо-запросы протокола ICMP, направленные к маршрутизатору, обрабатываются ЦП LC; так как запросы, получают смежности, они также фильтруются rACL. Поэтому для того, чтобы были разрешены эхо-тесты для интерфейсов (или петель) маршрутизатора, в rACL должны быть явно разрешены эхо-запросы.

Смежности получения можно просмотреть с помощью команды show ip cef.

```
12000-1#show ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           drop                Null0 (default route handler entry)
1.1.1.1/32          attached            Null0
2.2.2.2/32          receive
64.0.0.0/30         attached            ATM4/3.300
...
```

Инструкции по развертыванию

Cisco рекомендует осторожные способы развертывания. Для успешного развертывания rACL существующий контроль и требования доступа панели управления должны быть хорошо поняты. В некоторых сетях, определяя точный профиль трафика должен был создать списки фильтрации, могло бы быть трудным. В приведенном ниже руководстве описан крайне консервативный подход к развертыванию списков rACL с использованием повторяющихся конфигураций rACL, которые помогают определять и затем фильтровать трафик.

1. **Определите протоколы, которые используются в сети с классификацией ACL.**Разверните rACL, который разрешает все известные протоколы, которые обращаются к GRP. Этот rACL “обнаружения” должен иметь оба набора адресов источника и назначения **любому**. **Регистрация используется для создания списка адресов источника, которые совпадают с выражениями permit протокола**. В дополнение к **оператору разрешения протокола разрешение любая любая строка журнала** в конце rACL может использоваться для определения других протоколов, которые фильтровались бы rACL, и это могло бы потребовать доступа к GRP.Цель состоит в том, чтобы определить, какие протоколы использует определенная сеть. Регистрация должна использоваться для анализа для определения то, “что еще” могло бы связываться 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 недолго, и только если необходимо классифицировать трафик.**
2. **Рассмотрите идентифицированные пакеты и начните фильтровать доступ к GRP.Как только пакеты, отфильтрованные rACL на шаге 1, будут определены и проверены, разверните rACL с инструкцией permit any any 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 any log в конце может помочь в определении любых неожиданных пакетов, предназначенных для GRP.** В rACL будет обеспечена основная защита, а сетевые инженеры смогут гарантировать, что весь необходимый трафик является разрешенным.Цель состоит в том, чтобы протестировать диапазон протоколов, которые должны связаться с маршрутизатором, не имея явного диапазона Источника IP и адресов назначения (DA).
3. **Ограничьте макро-диапазон адресов источника.**Разрешите использовать в качестве адреса источника только полный диапазон выделенного блока бесклассовой междоменной маршрутизации (CIDR). Например, если вы были выделены 171.68.0.0/16 для вашей сети, затем разрешаете адреса источника от просто 171.68.0.0/16.Это позволяет снизить риск, не нарушая работы служб. Это также предоставляет точки данных устройств/людей снаружи вашего блока CIDR, который мог бы обращаться к вашему оборудованию. Весь внешний адрес будет отброшен.Узлы Внешнего BGP потребуют исключения, так как адреса разрешенного источника для сеанса лягут вне

блока CIDR.Эта фаза может действовать в течение нескольких дней, во время которых собираются данные для следующей фазы сужения rACL.

4. **Сузьте выражения разрешения rACL, чтобы только позволить известные авторизовавшие адреса источника.**Все более и более ограничивайте адрес источника, чтобы только разрешить источники, которые связываются с GRP.
5. **Ограничьте адреса назначения (DA) на rACL.** *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.[6]

Пример развертывания

В приведенном ниже примере описано, как ACL для входящих вызовов защищают маршрутизатор на основе следующей адресации.

- Адресный блок ISP - 169.223.0.0/16.
- Блок инфраструктуры интернет-провайдера является 169.223.252.0/22.
- Возвратная петля для маршрутизатора 169.223.253.1/32.
- Маршрутизатор – это центральный магистральный маршрутизатор, поэтому активны только внутренние сеансы BGP.

Учитывая эту информацию, начальная буква получает ACL, могло быть что-то как пример ниже. Поскольку адресный блок инфраструктуры известен, сначала будет разрешен весь блок. Позже, более подробные записи управления доступом (ACE) будут добавлены, поскольку точные адреса получены для всех устройств, нуждающихся в доступе к маршрутизатору.

```
!
no access-list 110
!
!--- This ACL is an explicit permit ACL. !--- The only traffic permitted will be packets that !-
-- match an explicit permit ACE.

!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 – Explicit Permit !--- Permit only applications whose destination address !--- is
the loopback and whose source addresses !--- come from an valid host.

!
!--- Note: This template must be tuned to the network's !--- specific source address
environment. Variables in !--- the template need to be changed.

!
!--- Permit BGP. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq bgp
! !--- Permit OSPF. ! access-list 110 permit ospf 169.223.252.0 0.0.3.255 host 224.0.0.5 ! !---
Permit designated router multicast address, if needed. ! access-list 110 permit ospf
169.223.252.0 0.0.3.255 host 224.0.0.6 access-list 110 permit ospf 169.223.252.0 0.0.3.255 host
169.223.253.1 ! !--- Permit EIGRP. ! access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host
224.0.0.10 access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host 169.223.253.1 ! !--- Permit
remote access by Telnet and SSH. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq 22 access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq
telnet ! !--- Permit SNMP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq snmp ! !--- Permit NTP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255
host 169.223.253.1 eq ntp ! !--- Router-originated traceroute: !--- Each hop returns a message
that ttl !--- has been exceeded (type 11, code 3); !--- the final destination returns a message
```

```
that !--- the ICMP port is unreachable (type 3, code 0). ! access-list 110 permit icmp any
169.223.253.1 ttl-exceeded access-list 110 permit icmp any 169.223.253.1 port-unreachable ! !---
Permit TACACS for router authentication. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255
host 169.223.253.1 established ! !--- Permit RADIUS. ! ! access-list 110 permit udp
169.223.252.0 0.0.3.255 169.223.253.1 log ! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !---
Phase 2 – Explicit Deny and Reaction !--- Add ACEs to stop and track specific packet types !---
that are destined for the router. This is the phase !--- where you use ACEs with counters to
track and classify attacks.

!
!--- SQL WORM Example – Watch the rate of this worm. !--- Deny traffic destined to UDP ports
1434 and 1433. !--- from being sent to the GRP. This is the SQL worm. ! access-list 110 deny udp
any any eq 1433 access-list 110 deny udp any any eq 1434 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 – Explicit Denies for
Tracking !--- Deny all other traffic, but count it for tracking.

!
access-list 110 deny udp any any
access-list 110 deny tcp any any range 0 65535
access-list 110 deny ip any any
```

Примечания

1. Для повышения устойчивости к DoS-атакам см. инструкции "Общие сведения о выборочном отбрасывании пакетов и очереди задерживаемых данных".
2. Для получения дополнительной информации относительно скоростной маршрутизации Cisco и смежностей, обратитесь к Обзору скоростной маршрутизации Cisco.
3. Для подробное обсуждение руководств по развертыванию ACL и связанных команд, обратитесь к Реализации ACL на Интернет-маршрутизаторах Cisco 12000 серии.
4. Это относится к Vanilla, Border Gateway Protocol Policy Accounting (BGPPA), Per Interface Rate Control (PIRC) и комплектам Frame Relay Traffic Policing (FRTP).
5. Этап 2 защиты Тракта приема обеспечит создание интерфейса управления, автоматически ограничивая, какой IP-адрес будет слушать входящие пакеты.

Дополнительные сведения

- Страница поддержки списков доступа
- Техническая поддержка - Cisco Systems