Описание и отслеживание лавинной передачи пакетов с помощью маршрутизаторов Cisco

Содержание

Введение

Атаки, провоцирующие отказ в обслуживании (DoS), распространены в Интернете. При подобной атаке необходимо в первую очередь выяснить, к какому виду атак она относится. Часто атаки типа DoS связаны с насыщением интенсивным пакетным трафиком или иным потоком повторяющихся пакетов.

Во многих случаях возможно вычленить поток DoS-атаки из общего потока пакетов, применив к пакетам программные записи списка контроля доступа Cisco IOS®. Это практичный способ фильтрации атак. Он также полезен для определения характеристик неизвестных атак и для выявления реального источника атак с фальшивыми пакетами.

Для подобных целей, особенно при противодействии новым или необычным атакам, можно применять такие функциональные возможности маршрутизаторов Cisco, как ведение журнала отладки и IP-учет. В последних же версиях программного обеспечения Cisco IOS основными средствами определения характеристик и отслеживания распространенных видов атак являются списки контроля доступа и журналы списков контроля доступа.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Наиболее распространенные DoS-атаки

Потенциально возможно широкое разнообразие DoS-атак. Даже не принимая во внимание атаки на ошибки в ПО, способные при сравнительно небольшом трафике нарушить работу систем, нельзя спорить с тем фактом, что любой IP-пакет, который можно пересылать через сеть, способен служить орудием DoS-атаки с насыщением трафиком. Во время атаки необходимо допускать, что происходящее может и не подпадать под обычные категории.

Однако в свете этой оговорки следует исходить из того, что многие атаки аналогичны. Злоумышленники избирают распространенные виды атак, поскольку они особенно эффективны, исключительно трудно прослеживаемы или поскольку доступны подходящие инструменты. У многих инициаторов DoS-атак отсутствуют как навыки, так и мотивация для создания собственных инструментов, поэтому в ход идут программы, найденные в Интернете. Эти инструменты обычно переживают ограниченный период популярности.

На момент написания данного материала (июль 1999 г.) большая часть обращений в службу поддержки Cisco касалась Smurf-атак. У таких атак сразу две жертвы: «конечная цель» и «отражатель». Нарушитель посылает провоцирующий поток эхозапросов ICMP (ping) на широковещательный адрес подсети рефлектора. Адреса источников этих пакетов подменяются адресом конечной цели атаки. На каждый пакет, посланный инициатором, отвечают много хостов из отражающей подсети. В результате конечная цель насыщается потоком трафика, и происходит непродуктивная загрузка пропускной способности каналов обеих жертв.

Другая подобная атака, называемая Fraggle, также использует направленные широковещательные рассылки, но вместо эхозапроса по межсетевому протоколу управляющих сообщений (ICMP) в ней используется эхозапрос UDP. Атака Fraggle обычно достигает меньшего коэффициента усиления, чем Smurf, и она менее популярна.

Частым внешним симптомом Smurf-атак является перегрузка сетевого канала. Полное описание этих атак, и мер по защите, находится на Странице информации Атак "отказ в обслуживании".

Другая обычная атака –SYN flood, в которой целевая машина насыщается запросами

соединения TCP. Адреса и TCP-порты источников пакетов запроса соединения подменяются случайным образом. Цель – заставить целевой хост обрабатывать информацию о состоянии большого количества соединений, которые никогда не будут завершены.

Атаки с помощью пакетов синхронизации (SYN) обычно обнаруживаются потому, что целевой узел (часто HTTP- или SMTP-сервер) становится чрезвычайно медленным, дает сбои и зависает. Также возможно, что трафик, возвращающийся от целевого хоста, создаст проблемы на маршрутизаторах. Это связано с тем, что возвратный трафик направляется по случайным адресам отправителей исходных пакетов. Не обладая локализованным характером «настоящего» IP-трафика, он может вызвать переполнение кэш-памяти маршрутов. Данная проблема часто проявляется на маршрутизаторах Cisco в виде нехватки памяти маршрутизатора.

Smurf- и SYN-атаки – наиболее распространенные виды атак с отказом в обслуживании (DoS), о которых сообщается компании Cisco, поэтому их оперативное выявление очень важно. Оба вида атак, равно как и некоторые атаки второго уровня, такие как атака насыщения ICMP-пакетами (ping flood), легко распознаются при использовании списков контроля доступа Cisco.

Классификационный список контроля доступа для выявления DoS-атак

Представим себе маршрутизатор с двумя интерфейсами. Интерфейс Ethernet 0 соединен с внутренней локальной сетью предприятия или небольшого поставщика услуг Интернета. Интерфейс Serial 0 обеспечивает подключение к Интернету через вышестоящего поставщика услуг. Скорость входящих пакетов на интерфейсе Serial 0 совпадает с полосой пропускания канала, и хосты в локальной сети работают медленно, со сбоями, зависаниями или проявляют другие признаки DoS-атаки. На небольшом узле, с которым соединен маршрутизатор, нет сетевого анализатора, а у персонала отсутствует необходимый опыт для интерпретации данных анализатора, даже если бы они были.

Теперь предположим, что применяется список контроля доступа, как в этом примере выходных данных:

```
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

Этот список не выполняет никакой фильтрации трафика: все записи являются разрешающими (permit). Однако поскольку этот список позволяет классифицировать пакеты нужным образом, его можно использовать для предварительной диагностики всех трех типов атак: smurf, насыщение SYN-пакетами и Fraggle.

Конечная цель в атаке типа Smurf

Команда show access-list выдает данные наподобие следующих:

```
Extended IP access list 169
    permit icmp any any echo (2 matches)
    permit icmp any any echo-reply (21374 matches)
    permit udp any any eq echo
    permit udp any eq echo any
    permit tcp any any established (150 matches)
    permit tcp any any (15 matches)
    permit ip any any (45 matches)
```

Большая часть трафика, который приходит на последовательный интерфейс, составляют пакеты отклика на эхозапросы ICMP. Это вероятный признак атаки типа Smurf, и наш узел является его конечной целью, а не отражателем. Изменив список контроля доступа, можно извлечь дополнительную информацию об атаке, как показывает следующий пример выходных данных:

```
interface serial 0
no ip access-group 169 in

no access-list 169
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply log-input
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

Изменение состоит в том, что к записи списка контроля доступа, которая соответствует подозрительному трафику, добавляется ключевое слово log-input. (В выпусках ПО Cisco IOS до 11.2 такого ключевого слова нет. Вместо него следует использовать ключевое слово log.). В этом случае маршрутизатор отмечает в журнале сведения о пакетах, подпадающих под критерии списка контроля доступа. Если ранее была задана команда logging buffered, то можно будет просматривать получаемые сообщения по команде show log (из-за ограничения скорости для накопления сообщений может потребоваться некоторое время). Сообщения будут иметь приблизительно следующий вид:

```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.72
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.154
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
```

```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.59
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.82
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.56
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.84
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.33
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
```

Адреса отправителей пакетов отклика на эхозапрос группируются по префиксам адресов 192.168.212.0/24, 192.168.45.0/24 и 172.16.132.0/24. (Частные адреса, принадлежащие сетям 192.168.x.x и 172.16.x.x, в Интернете отсутствуют; пример приведен для лабораторной среды.). Такая картина очень характерна для Smurf-атаки, и адреса отправителей соответствуют отражателям атаки. Установив владельцев этих адресных блоков по соответствующей базе данных WHOIS в Интернете, можно связаться с администраторами этих сетей и просить их помощи при отражении атаки.

При Smurf-атаках важно помнить, что отражатели являются пострадавшими, а не нарушителями. Взломщики крайне редко используют собственные исходные адреса в IP-пакетах при DoS-атаках с насыщением трафиком, а в случае Smurf-атаки это попросту невозможно. Любой адрес в пакете насыщения трафиком следует считать либо полностью фальсифицированным, либо исходящим от атакуемого устройства определенного рода. Самая конструктивная тактика для конечной цели Smurf-атаки – обратиться к отражателям и либо попросить их перенастроить свои сети так, чтобы атака прекратилась, либо заручиться их помощью в выявлении первоисточника провоцирующего потока.

Поскольку реальный вредоносный эффект для конечной цели Smurf-атаки обычно состоит в перегрузке входящего интернет-канала, проблему редко удается решить без обращения к отражателям. К тому времени, когда пакеты будут доставлены на любой из целевых компьютеров, основной вред уже будет нанесен.

Временным решением является обращение к вышестоящему поставщику услуг для фильтрации в его сети всех эхооткликов ICMP или эхооткликов ICMP от указанных отражателей. Не рекомендуется оставлять этот вид фильтра постоянно действующим. Даже в случае временного фильтра фильтровать следует только эхоотклики, а не все пакеты ICMP. Другое возможное решение состоит в использовании вышестоящим поставщиком услуг механизмов управления качеством обслуживания (QoS) и ограничения скорости для сужения полосы пропускания, доступной для эхооткликов. Разумное ограничение полосы пропускания можно оставить на неограниченное время. Оба этих подхода зависят от функциональных возможностей оборудования вышестоящего поставщика услуг, и иногда его функций недостаточно.

Отражатель в атаке типа Smurf

Если входящий трафик состоит из эхозапросов, а не эхооткликов (другими словами, если количество пакетов, подпадающих под первую, но не под вторую запись списка контроля доступа, превышает ожидаемое значение), то можно подозревать, что имеет место атака типа Smurf, в которой сеть используется как отражатель, либо простое насыщение запросами. В обоих случаях, если атака была успешной, будет ожидаться насыщение как исходящей стороны последовательного канала, так и входящей. На практике заметен коэффициент усиления, из-за которого исходящее направление будет перегружено даже сильнее, чем входящее.

Отличить Smurf-атаку от простого насыщения эхозапросами можно по нескольким признакам:

- Провоцирующие пакеты в атаке Smurf отправляются на направленный широковещательный адрес, а не на индивидуальный адрес, в то время как при обычном насыщении эхозапросами всегда используются индивидуальные адреса. **Используемые адреса можно просмотреть, добавив ключевое слово log-input к соответствующей записи списка контроля доступа.**
- **Если ваша система играет роль отражателя в Smurf-атаке, то команда show interface на Ethernet-стороне системы будет показывать непропорционально высокий выходной широковещательный трафик. При этом команда ip traffic display обычно также показывает непропорционально большое число отправляемых широковещательных пакетов.** Типичное насыщение эхозапросами не влияет на объем фонового широковещательного трафика.
- Если ваша система используется в Smurf-атаке как отражатель, то объем трафика, выходящего в Интернет, будет превышать объем входящего трафика. В общем случае на последовательном интерфейсе будет больше исходящих, чем входящих пакетов. Даже если провоцирующий поток занимает всю пропускную способность входного интерфейса, поток откликов может быть больше входящего потока, вследствие чего регистрируются потери пакетов.

У отражателя Smurf-атаки выбор действий не столь ограничен, как у конечной жертвы. **Чтобы прекратить атаку, отражателю обычно бывает достаточно надлежащим образом использовать команду no ip directed-broadcast (или аналогичные команды в системах, отличных от IOS).** Эти команды актуальны в каждой конфигурации, даже в отсутствие активной атаки. Дополнительную информацию о защите своего оборудования Cisco от использования в качестве орудия Smurf-атак можно найти в документе Повышение уровня безопасности маршрутизаторов Cisco. Для большего количества общей информации о smurf-атаках в целом, и для получения информации о защите оборудования не марки CISCO, обращаются к Странице информации Атак "отказ в обслуживании".

Отражатель smurf-атак находится на одну позицию ближе к источнику атаки, чем конечная цель, и может быстрее обнаружить атаку. Для отслеживания источника атаки следует заручиться содействием Интернет-провайдера. Для принятия мер после обнаружения источника следует обратиться в правоохранительные органы соответствующего профиля. Если преследуется цель выявить источник атаки, то подключать правоохранительные органы рекомендуется как можно раньше. Техническая сторона отслеживания атак с насыщением трафиком освещена в разделе Отслеживание.

Fraggle

Атака типа Fraggle является аналогом атаки типа smurf, за исключением того, что для провоцирующего потока используются эхозапросы UDP вместо эхозапросов ICMP. В третьей и четвертой строках списка доступа указаны атаки типа Fraggle. Меры по реагированию для жертв атаки – те же, за исключением того, что отклик UDP в большинстве сетей менее важен как служебный элемент по сравнению с откликом ICMP. Поэтому такие отклики можно блокировать полностью с меньшей вероятностью негативных последствий.

Насыщение пакетами SYN

Пятая и шестая строки списка контроля доступа имеют следующий вид:

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
```

Первая из этих строк описывает любой пакет TCP с установленным битом ACK. В нашем случае это соответствует любому пакету, тип которого отличается от TCP SYN. Вторая строка описывает только пакеты типа TCP SYN. По показаниям счетчиков для этих записей списка легко выявить насыщение пакетами SYN. В нормальном трафике TCP-пакетов, отличных от SYN, насчитывается как минимум вдвое больше, чем пакетов SYN, а обычно – вчетверо или впятеро. Во время атаки с насыщением пакетами SYN их число обычно во много раз превышает число иных TCP-пакетов.

В отсутствие атаки единственной причиной подобной динамики является массивная перегрузка подлинными запросами подключения. В общем случае такая перезагрузка не случается внезапно и не сопровождается таким числом пакетов SYN, как реальная атака с насыщением пакетами SYN. **Кроме того, атаки с насыщением пакетами SYN часто содержат пакеты с абсолютно недействительными адресами отправителей. Ключевое слово log-input позволяет узнать, не являются ли подобные адреса источниками запросов подключения.**

Некоторое сходство с насыщением пакетами SYN демонстрирует атака, именуемая атакой на таблицу процессов. В отличие от насыщения пакетами SYN, где отправляются только начальные запросы подключения, в атаке на таблицу процессов установление сеанса TCP происходит до конца, но протокольный трафик никогда не пересылается – сеанс остается бездействующим до истечения периода неактивности. Поскольку для атаки на таблицу процессов необходимо завершить начальное установление сеанса TCP, ее обычно приходится инициировать с IP-адресом реальной машины, к которой атакующая сторона имеет доступ (обычно через похищенные реквизиты доступа). По этой причине атаку на таблицу процессов можно легко отличить от насыщения пакетами SYN, используя механизм ведения журнала пакетов. Все пакеты SYN в атаке на таблицу процессов исходят из одного или нескольких адресов, максимум – из одной или нескольких подсетей.

Возможности реагирования для жертв атак с насыщением пакетами SYN очень ограничены. Обычно объектами атак избираются важные системы, и блокирование доступа к системе – именно та цель, которую преследуют злоумышленники. Многие продукты семейства маршрутизаторов и межсетевых экранов, включая продукты Cisco, характеризуются функциями, которые можно использовать для уменьшения воздействия потоков SYN, однако, эффективность таких функций зависит от среды. Дополнительные сведения можно найти в документации по набору функций межсетевого экрана Cisco IOS, в описании функции перехвата TCP в Cisco IOS и в документе Повышение уровня безопасности маршрутизаторов Cisco.

Существует возможность отследить потоки SYN, но этот процесс требует участия каждого поставщика услуг Интернета на протяжении всего пути от атакующего до жертвы. Если принимается решение отследить источник атаки с насыщением пакетами SYN, то следует

на самом раннем этапе подключить правоохранительные органы и наладить взаимодействие с собственным вышестоящим поставщиком услуг. Дополнительные сведения об отслеживании с использованием оборудования Cisco см. в разделе Отслеживание данного документа.

Другие виды атак

При обнаружении признаков атаки и определении ее типа на основе IP-адресов источника и получателя, номеров протоколов и номеров портов можно проверить свое предположение, используя списки контроля доступа. Создайте запись списка доступа, подходящую для ожидаемого трафика, примените ее к соответствующему интерфейсу, а затем наблюдайте за счетчиками совпадения или ведите журнал трафика.

Неочевидные свойства механизма ведения журналов и регистрации

Счетчик в записи списка контроля доступа подсчитывает все совпадения с этой записью. Если список доступа действует сразу для двух интерфейсов, то счетчик будет показывать совокупное количество.

В журнале списка контроля доступа не отображается каждый пакет, соответствующий записи. Скорость записи в журнал ограничена для предотвращения перегрузки ЦПУ. В журнале можно увидеть достаточно репрезентативную выборку пакетов, но не каждый пакет. Помните о том, что в журнале показаны не все пакеты.

В некоторых версиях программного обеспечения журнал списка контроля доступа работает только в определенных режимах коммутации. Если для записи списка контроля доступа насчитано много совпадений, но в журнале ничего не регистрируется, попробуйте очистить кэш маршрутов, чтобы задействовать коммутацию пакетов в контексте процесса. Будьте осторожны при выполнении этой операции на сильно загруженных маршрутизаторах с большим числом интерфейсов. При переформировании кэша трафик часто может выпадать. При всякой возможности используйте технологию Cisco Express Forwarding.

Списки контроля доступа и ведение журналов сказываются на производительности, но незначительно. Будьте внимательны с маршрутизаторами, работающими при загрузке ЦПУ порядка 80% и при использовании списков контроля доступа на наиболее высокоскоростных интерфейсах.

Отслеживание

Адреса источников пакетов в DoS-атаке почти всегда имеют значения, не имеющие никакого отношения к реальному источнику атаки. Поэтому для установления источника они бесполезны. Единственный надежный способ определения источника атаки – отследить его, двигаясь в обратном направлении от узла к узлу сети. Этот процесс предполагает перенастройку маршрутизаторов и анализ информации в журналах. Требуется участие операторов всех сетей на пути от нападавшего до жертвы. Для организации такой совместной работы обычно привлекаются правоохранительные органы, также привлекаемые для принятия каких-либо мер в отношении нарушителя.

Процесс отслеживания источников насыщения пакетами DoS относительно прост. Начиная от маршрутизатора (назовем его «маршрутизатор A»), про который известно, что он переносит трафик атаки, можно определить маршрутизатор («маршрутизатор B»), от

которого маршрутизатор A этот трафик получает. Затем пользователь входит в маршрутизатор B и узнает, с какого маршрутизатора (обозначим его «C») в B поступает трафик. Это продолжается до тех пор, пока не будет найден первичный источник.

В этом методе есть несколько нюансов, которые описаны ниже:

- Фактически первичным источником может быть компьютер, взломанный злоумышленником, но принадлежащий и работающий под управлением другой жертвы. В этом случае выявление источника DoS-атаки – только первый шаг.
- Злоумышленники знают, что их возможно отследить, и обычно ограничивают продолжительность своих атак. Может не хватить времени на то, чтобы реально отследить лавинный поток.
- Атаки могут исходить из множества источников, особенно если злоумышленник довольно опытный. Важно попытаться идентифицировать как можно больше источников.
- Процесс отслеживания также тормозится трудностями координации. Весьма часто у одного или нескольких участвующих операторов сетей нет хорошо подготовленного персонала.
- Даже если злоумышленника удалось найти, принять против него меры иногда сложно из-за юридических и политических препятствий.

Попытки отследить источник DoS-атак чаще всего кончаются безрезультатно. По этой причине большинство операторов сетей даже не пытается отследить атаку до тех пор, пока не возникает крайняя необходимость. Другие же пытаются отслеживать только «серьезные» атаки с разными определениями уровня «серьезности». Некоторые операторы готовы сотрудничать только при подключении правоохранительных органов.

Отслеживание в режиме log-input

При отслеживании атаки, проводимой через маршрутизатор Cisco, наиболее эффективный способ – создать запись списка контроля доступа, соответствующую трафику атаки, назначить ей ключевое слово log-input и применить список контроля доступа на исходящем направлении интерфейса, через который поток атакующего трафика отправляется к конечной цели. В записях журнала, создаваемых списком контроля доступа, указывается интерфейс маршрутизатора, через который поступает трафик, и (если это интерфейс многоточечного соединения) адрес 2-го уровня устройства, с которого принимается трафик. *Адрес 2-го уровня может быть использован для определения следующего маршрутизатора в цепочке, например, с помощью команды show ip arp mac-адрес.*

Атака SYN

Для отслеживания насыщения пакетами SYN можно создать список контроля доступа, подобный следующему:

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any host victim-host log-input
access-list 169 permit ip any any
```

В этом случае в журнале регистрируются все пакеты SYN, предназначенные для конечного узла, включая допустимые пакеты SYN. Для определения наиболее вероятного фактического пути к источнику атаки тщательно проанализируйте записи в журнале. В большинстве случаев источником потока является адрес, с которого поступает наибольшее количество соответствующих пакетов. Сами по себе IP-адреса источников не означают

ничего. Обращать внимание следует на интерфейсы источников и их MAC-адреса. Иногда возможно отличить пакеты атаки с насыщением от нормальных пакетов, поскольку первые могут иметь недействительные адреса источника. Любой пакет с недопустимым адресом, скорее всего, является частью лавины.

Трафик может исходить из нескольких источников, хотя для атак с насыщением пакетами SYN это бывает редко.

Провоцирующий поток в атаке типа Smurf

Для отслеживания провоцирующего потока в атаке типа Smurf используйте следующий список контроля доступа:

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any host victim-host log-input
access-list 169 permit ip any any
```

Помните, что первая запись не ограничивается пакетами, направляемыми на адрес отражателя. Причиной этого является то, что в большинстве Smurf-атак используются сети с несколькими отражателями. Не находясь в контакте с конечным адресатом, невозможно знать все адреса отражателей. По мере приближения отслеживания к источнику атаки можно наблюдать эхозапросы все большему числу адресатов; это хороший признак.

Однако при наличии большого объема трафика ICMP это может породить чрезвычайно большой журнал, который сложно прочесть. В этом случае можете ограничить круг получателей адресом одного из известных отражателей. Другая полезная тактика – использовать запись, учитывающую обширное распространение сетевых масок 255.255.255.0 в Интернете. В силу механизма, с помощью которого атакующие находят отражатели, адреса отражателей в Smurf-атаках с большей вероятностью будут соответствовать маске. Адреса хостов, оканчивающиеся на .0 или .255, в Интернете распространены крайне мало. Поэтому возможно построить относительно узкий механизм распознавания для провоцирующих потоков Smurf-атаки, как показано в следующих выходных данных:

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any host victim-host log-input
access-list 169 permit ip any any
```

Такой список помогает убрать из журнала многие пакеты, представляющие собой «шум», но практически не снижает вероятность обнаружения дополнительных провоцирующих потоков по мере приближения к источнику атаки.

Отслеживание без режима log-input

Ключевое слово режима log-input существует только в выпусках ПО Cisco IOS, начиная с 11.2, и в некоторых версиях ПО 11.1, специально ориентированных на рынок поставщиков услуг. Старое ПО не поддерживает это ключевое слово. Если используется маршрутизатор с более старым программным обеспечением, то есть три возможных варианта:

- Создание списка контроля доступа без ведения журнала, но с записями, отвечающими подозрительному трафику. *Список вводится в действие на входной стороне каждого интерфейса, после чего контролируются показания счетчиков.* Обращать внимание нужно на интерфейсы с высоким числом совпадений. Этот способ практически не влияет на производительность, его хорошо использовать для определения исходного

интерфейса. Самый существенный недостаток этого метода заключается в том, что он не позволяет получить адреса источника канального уровня и поэтому пригоден главным образом для линий «точка-точка».

- **Создание записей списка контроля доступа с ключевым словом log (вместо log-input).** В этом режиме список снова применяется к входящей стороне каждого интерфейса по очереди. Этот метод не позволяет узнать MAC-адреса источника, но может использоваться для просмотра IP-данных, например для проверки того, что поток пакетов действительно является частью атаки. Снижение производительности может быть как умеренным, так и весьма высоким. Новые выпуски ПО справляются с нагрузкой лучше, чем старые выпуски.
- **Применение команды debug ip packet detail для сбора сведений о пакетах.** Этот метод позволяет получить MAC-адреса, однако может серьезно сказаться на производительности. Прибегая к нему, легко совершить ошибку и нарушить работоспособность маршрутизатора. При использовании данного метода убедитесь, что маршрутизатор коммутирует трафик атаки в скоростном, автономном или оптимальном режиме. Посредством списка контроля доступа ограничьте отладку только той информацией, которая действительно необходима. Сохраняйте отладочные сведения для буфера локального журнала, но отключите журналирование отладочных сведений для сеансов Telnet и для консоли. Если возможно, организуйте дежурство около маршрутизатора, чтобы по мере необходимости можно было включать и выключать питание маршрутизатора.**Помните, что команда debug ip packet не выдает информацию о пакетах, обрабатываемых в режиме быстрой коммутации. Для сбора данных нужно выполнить команду clear ip cache. Каждая из команд clear выдает один или два пакета отладочных данных.**

Дополнительные сведения

- Kerberos
- Cisco Systems – техническая поддержка и документация