Содержание

Введение

Иногда, сеть получает поток пакетов Атаки типа отказ в обслуживании (DOS) наряду с трафиком обычной сети. В таких ситуациях, вы можете использовать механизм, названный «ограничение тарифа», чтобы снизить производительность, для того, чтобы сеть не вышла из строя. Вы можете использовать Cisco IOS® для того, чтобы добиться ограничения тарифа, используя эти схемы:

- Committed Access Rate (CAR)
- Формирование трафика
- Формирование и определение политик через модульный интерфейс командной строки для обеспечения качества обслуживания (QOS CLI)

В этом документе обсуждается CAR, для использования при DoS атаках. Другие схемы являются просто вариантами базового понятия.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco IOS Software Release 11.1CC и 12.0 магистралей, которые поддерживают CAR.
- Программное обеспечение Cisco IOS версии 11.2 и позже, которые поддерживают Формирование трафика.
- Cisco IOS Software Release 12.0XE, 12.1E, 12.1T, которые поддерживают Modular QoS CLI.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

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

ICMP/Smurf ограничения скорости

Настройте их access-lists:

Для включения CAR необходимо включить технологию CEF на коробке. Кроме того, необходимо настроить CEF-коммутируемый интерфейс для CAR.

Пример выходных данных использует значения пропускной способности для пропускных способностей типа DS3. Выберите значения на основе полосы пропускания интерфейса и скорости, на которой вы хотите ограничить определенный тип трафика. Для меньших входных интерфейсов можно настроить низшие скорости.

Пакеты TCP SYN ограничения скорости

11.1 (X) CC

Если вы знаете, какой узел под нападением, то установите эти списки доступа:

Примечание: В этом примере, под нападением узел 10.0.0.1.

Если вы не знаете, какой хост под атакой DoS, и вы хотите защитить сеть, настроить эти списки доступа:

Примечание: Ограничение скорости к 64000 битов в секунду для всех Пакетов TCP SYN.

12.0 (X) [S/T/M]

Если вы знаете, какой узел под нападением, то установите эти списки доступа:

Примечание: В данном примере, 10.0.0.1 хост под огнем.

Если вы не уверены, какой хост под атакой, и вы хотите защитить сеть, настроить эти списки доступа:

Примечание: Ограничение скорости к 64000 битов в секунду для всех Пакетов TCP SYN.

Вопросы и ответы по CAR

Как определить значения для Использования для правил CAR для ограничивания SYN - пакетов?

Общие сведения о сети. Тип трафика определяет количество активных сеансов TCP для фиксированного размера данных.

- WWW-трафик содержит гораздо более богатую смесь пакетов TCP Syn, чем FTP-трафик от серверного пула.
- Стек PC-клиента склонен подтверждать любой другой пакет TCP. Другие стеки могут подтвердить меньше или чаще.
- Проверьте, необходимо ли применить эти правила CAR на край индивидуального пользователя или в Границе сети заказчика.

Для WWW вот соединение трафика:

Для каждого пятитысячного файла, который вы загружаете с сетевого узла, узел сети получает 560 байт так, как показанно здесь:

- 80 байтов [SYN, ACK]
- 400 байт / [320 байтная структура HTTP, 2 сообщения ACK]
- 80 байт [FIN, ACK]

Предположим, что соотношение между выхода трафика из Интернета на узле и входящего трафика с сетевго узла 10-е: 1. Объем трафика, который составляет SYN - пакеты, 120:1.

Если у вас есть Ссылка OC3, вы ограничиваете скорость Пакетов TCP SYN 155 Мбит/с / 120 == 1.3 Мбит/с.

На входном интерфейсе в маршрутизаторе веб - фермы настройте:

Скорость Пакета TCP SYN становится меньшей, как длина ваших сеансов TCP становится более длинной.

Файлы MP3 имеют тенденцию быть 4 - 5 mgbps в размере в среднем. Загрузка 4 mgbps генерирует файл входящего трафика, составляющего 3160 байт:

- 80 байтов [SYN, ACK]
- 3000 байтов [ACK + FTP get]
- 80 байт [FIN, ACK]

Скорость передачи пакетов TCP SYN для исходящего трафика составляет 1500 Мбит/с / 120000 == 1,3 Кбит/с.

Настройка:

Как я Знаю, ограничиваю ли я слишком много SYN - пакетов?

Если вы знаете свою обычную скорость подключения на ваших серверах, можно сравнить рисунки прежде и после включения CAR. Сравнение помогает вам определять возникновение понижения вашей скорости подключения. Если вы находите понижение скорости, инкрементно увеличиваете ваши Параметры CAR для разрешения большего количества сеансов.

Проверьте, в состоянии ли пользователи установить сеансы TCP легко. Если ваши пределы CAR слишком строги, пользователи должны предпринять множественные попытки установить сеанс TCP.

Возможно ли разблокировать CAR в маршрутизаторе GSR?

Да. Механизм 0 и Механизм 1 линейная карта поддерживают CAR. Cisco IOS Software Release 11.2 (14) gs2 и позже оказывает поддержку CAR. Влияние на производительность CAR зависит от количества правил CAR, которые вы применяете.

Влияние на производительность также больше на Механизме 1 линейная карта, чем на Механизме 0 линейных карт. Если вы хотите включить CAR на Механизме 0 линейных карт, необходимо знать об идентификаторе ошибки Cisco CSCdp80432 (только зарегистрированные клиенты). Если вы хотите включить CAR к многоадресному трафику rate-limit, гарантировать, что идентификатор ошибки Cisco CSCdp32913 (только зарегистрированные клиенты) не влияет на вас. CSCdm56071 идентификатора ошибки Cisco (только зарегистрированные клиенты) является другим дефектом, о котором необходимо знать перед включением CAR.

Можно ли активировать распределенную согласованную скорость доступа (dCAR) для Cisco 7500?

Да, dCAR поддержек платформ RSP/VIP в программном обеспечении Cisco IOS версии 11.1(20)CC и все 12.0 Выпусков ПО.

Производительность коллизии CAR в некоторой степени. На основе Конфигурации CAR можно достигнуть скорости линии [для интернет-трафика Соединения] с VIP2-50 [через dCAR] на OC3. Гарантируйте, что идентификатор ошибки Cisco CSCdm56071 (только зарегистрированные клиенты) не влияет на вас. Если вы хотите использовать выходные данные CAR, идентификатор ошибки Cisco, CSCdp52926 (только зарегистрированные клиенты) может влиять на ваше подключение. При включении dCAR идентификатор ошибки Cisco, CSCdp58615 (только зарегистрированные клиенты) может вызвать сбой VIP.

Можно ли включить CAR на маршрутизаторе Cisco 7200?

Да. NPE поддерживает CAR в программном обеспечении Cisco IOS версии 11.1(20)CC и все 12.0 Выпусков ПО.

Производительность коллизии CAR в некоторой степени, на основе Конфигурации CAR. Доберитесь исправляет для этих дефектов: Идентификатор ошибки Cisco CSCdm85458 (только зарегистрированные клиенты) и идентификатор ошибки Cisco CSCdm56071 (только

зарегистрированные клиенты).

Примечание: Большое число Записей car в интерфейсе/подчиненном интерфейсе ухудшает производительность, потому что маршрутизатор должен выполнить линейный поиск на Операторах CAR для обнаружения оператора "CAR", который совпадает.

Другие функции и возможности

Входящие IP-пакеты ACL

Программное обеспечение Cisco IOS версии 12.0(22)S содержит IP, Получают характеристику ACL на Интернет-маршрутизаторе Cisco 12000 серии.

IP Получает характеристику ACL, предоставляет простые фильтры для трафика, предназначенного для достижения маршрутизатора. Маршрутизатор может защитить высокоприоритетный трафик протокола маршрутизации от атаки, потому что функция фильтрует весь входной список контроля доступа (ACL) на входном интерфейсе. IP Получает трафик фильтров характеристики ACL на распределенных линейных платах, прежде чем процессор маршрута получит пакеты. Эта функция позволяет пользователям фильтровать лавинные рассылки Отказа в обслуживании (DoS) против маршрутизатора. Поэтому эта функция предотвращает снижение производительности процессора маршрута.

См. IP Получают APL для получения дополнительной информации.

Средство отслеживания IP-источника

Программное обеспечение Cisco IOS версии 12.0(21)S поддерживает функцию IP-датчика источника на Интернет-маршрутизаторе Cisco 12000 серии. Программное обеспечение Cisco IOS версии 12.0(22)S поддерживает эту функцию на маршрутизаторе Cisco серии 7500.

Функция IP-датчика источника позволяет вам собирать информацию о трафике, который течет к хосту, который вы подозреваете, под атакой. Эта функция также позволяет вам легко прослеживать атаку до точки входа в сети. При определении точки входа в сеть через эту функцию можно использовать ACL или CAR для блокирования атаки эффективно.

См. IP-датчик источника для получения дополнительной информации.

Дополнительные сведения

- Защита сети от вируса Nimda
- IP получает APL
- Средство отслеживания IP-источника
- Cisco Systems – техническая поддержка и документация