Определение стратегий защиты от атак типа "отказ в обслуживании" TCP SYN

Содержание

Краткое изложение

Сетевые устройства поставщика услуг Интернета могут потенциально стать жертвами атак, провоцирующими отказ в обслуживании (DoS).

- **Атака TCP SYN:** От отправителя исходит большой объем подключений, которые не могут быть завершены. Это вызывает переполнение очереди подключений, делая невозможным тем самым использование сервисов обычными пользователями.

В этом документе содержится техническое описание того, как происходят потенциальные атаки TCP SYN, и предлагаемые способы использования программного обеспечения Cisco IOS для защиты от них.

Примечание: Программное обеспечение Cisco IOS 11.3 имеет функцию для активного предотвращения атак "отказ в обслуживании" TCP. Эта функция описана в документе Настройка перехвата TCP (предотвращение DoS-атак).

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

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

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

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

Описание проблемы

Атака TCP SYN

При установлении обычного TCP-соединения хост назначения принимает пакет SYN (начало синхронизации) от исходного хоста и передает в обратном направлении пакет SYN ACK (подтверждение синхронизации). Узел назначения должен получить пакет ACK (подтверждение) в ответ на отправленный пакет SYN ACK, прежде чем соединение будет установлено. Это называется трехэтапным установлением TCP-соединения."

Ожидая получение пакета ACK в ответ на SYN ACK, ограниченная по размеру очередь соединений на узле назначения отслеживает соединения, которые ожидают завершения установления. Эта очередь обычно быстро очищается, потому что поступление пакета ACK ожидается через нескольких миллисекунд после получения пакета SYN ACK.

Атака TCP SYN использует недостаток этого алгоритма: атакующий узел-источник генерирует пакеты TCP SYN со случайными адресами источника и отправляет их на узел-жертву. Атакуемый хост отправляет пакет SYN ACK на случайный исходный адрес и добавляет запись в очередь соединений. Так как пакет SYN ACK предназначен для некорректного или несуществующего хоста, часть трехэтапного установления соединения никогда не завершится и запись останется в очереди соединений до истечения определенного промежутка времени, обычно около 1 минуты. Путем генерирования большого количества фальшивых TCP SYN пакетов со случайных IP-адресов можно переполнить очередь подключений и заблокировать работу TCP-сервисов (таких как электронная почта, передача файлов или WWW) для обычных пользователей.

Нет простого способа выявить организатора атаки, поскольку IP-адрес источника является поддельным.

Внешние проявления этой проблемы включают невозможность получить электронную почту, неспособность принимать соединения сервисов WWW или FTP, или на хосте имеется много TCP-соединений, имеющих состояние SYN_RCVD.

Защита от атак на сетевые устройства

Устройства за межсетевыми экранами

Атака TCP SYN характеризуется притоком пакетов SYN от случайных IP-адресов источника. Любое устройство за межсетевым экраном, останавливающим входящие пакеты SYN, уже защищено от этого типа атаки. В этом случае дальнейших мер не требуется. Межсетевыми экранами могут, например, выступать устройства Cisco Private Internet Exchange (PIX) и маршрутизаторы Cisco с настроенными списками контроля доступа. Примеры настройки списков контроля доступа на маршрутизаторе Cisco см. в документе Укрепление безопасности в IP-сетях.

Устройства со службами, доступными извне (серверы электронной почты, открытые web-серверы)

Предотвращение атак SYN на устройства за межсетевым экраном от случайных IP-адресов относительно просто, так как можно использовать список контроля доступа для явного ограничения входящего доступа несколькими IP-адресами. Однако в случае web-сервера или сервера электронной почты, открытого для доступа из Интернета, невозможно определить, принадлежит ли IP-адрес источника добросовестному пользователю или злоумышленнику. Таким образом, не существует очевидной защиты от атаки со стороны случайного IP-адреса. Для хостов доступно несколько вариантов решений:

- Увеличение размера очереди подключений (очереди SYN ACK).
- Сокращение времени ожидания трехэтапного установления соединения.
- Применение исправлений в программном обеспечении поставщиков (в случае доступности таковых) для обнаружения и обхода проблемы.

У поставщика хоста следует поинтересоваться наличием конкретных исправлений для предупреждения атаки TCP SYN ACK.

Примечание: IP-адреса фильтрации в сервере неэффективны, так как атакующий может варьироваться свой IP-адрес, и адрес может или может не совпасть с адресом легитимного хоста.

Защита сети от непреднамеренной эксплуатации в качестве базы для атаки

Поскольку основной механизм атаки отказа в обслуживании заключается в генерации трафика с произвольных IP-адресов, рекомендуется фильтровать трафик, предназначенный для Интернета. Основной принцип — отбрасывать пакеты с недопустимыми исходными IP-адресами, по мере того как они поступают в Интернет. Это не предотвратит DoS-атаки на сеть, но поможет атакованным сторонам исключить ваше расположение из источников атакующих. Кроме того, это сделает сеть менее привлекательной в качестве базы для данного класса атак.

Предотвращение передачи недопустимых IP-адресов

С помощью фильтрации пакетов на маршрутизаторах, которые соединяют вашу сеть с Интернетом, вы можете разрешить выход в интернет только пакетам с допустимыми IP-адресами отправителей.

Например, если ваша сеть представлена IP-сетью 172.16.0.0 и ваш маршрутизатор подключается к поставщику услуг Интернета, используя последовательный интерфейс 0/1, то можно применить список контроля доступа следующим образом:

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 0/1
ip access-group 111 out
```

Примечание: Последняя строчка в списке доступа определяет, выходил ли в Интернет какой-либо трафик с недопустимым адресом источника. Эта строка не так важна, зато помогает обнаружить источник вероятных атак.

Предотвращение приема недопустимых IP-адресов

Для ISP, обслуживающих конечные сети, мы настоятельно рекомендуем подтверждение входящих пакетов от клиентов. Это можно выполнить, используя фильтры входящих пакетов на своих граничных маршрутизаторах.

Например, если через последовательный интерфейс serial 1/0 с вашим маршрутизатором связаны следующие номера сетей ваших клиентов, то можно создать указанный ниже список контроля доступа:

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0.

access-list 111 permit ip 192.168.0.0 0.0.15.255 any
access-list 111 permit ip 172.18.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 1/0
ip access-group 111 in
```

Примечание: Последняя строка списка доступа определяет, есть ли трафик с недопустимыми адресами источника, поступающими в Интернет. Эта строка необязательна, но она поможет обнаружить расположение источника возможной атаки.

Данная тема подробно обсуждалась в списке рассылки NANOG [Североамериканской группы операторов сетей]. Архивы списка доступны по адресу: http://www.merit.edu/mail.archives/nanog/index.html

Подробное описание DoS-атаки TCP SYN и подмены IP-адресов см. в документах: http://www.cert.org/advisories/CA-1996-21.html

http://www.cert.org/advisories/CA-1995-01.html

Дополнительные сведения

- Техническая поддержка - Cisco Systems