ASA/PIX 7.x и более поздние версии: Уменьшение сетевых атак

Содержание

Введение

В данном документе описываются возможности уменьшения последствий различных сетевых атак, например, отказа от обслуживания (DoS-атак), с помощью устройства защиты Cisco ASA/PIX.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Информация в этом документе касается устройств адаптивной защиты Cisco серии ASA 5500, работающих под управлением ПО версии 7.0 или более поздней версии.

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.

Родственные продукты

Этот документ также можно использовать для устройств Cisco серии PIX 500, работающих под управлением ПО версии 7.0 или более поздней версии.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Защита от атак TCP SYN

Можно ли уменьшить последствия атаки TCP SYN с помощью устройств защиты ASA/PIX?

Атака TCP SYN

Атака TCP SYN является разновидностью DoS-атаки, при которой отправитель устанавливает множество соединений, которые не могут быть завершены. Это вызывает переполнение очереди подключений, делая невозможным тем самым использование сервисов обычными пользователями.

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 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.

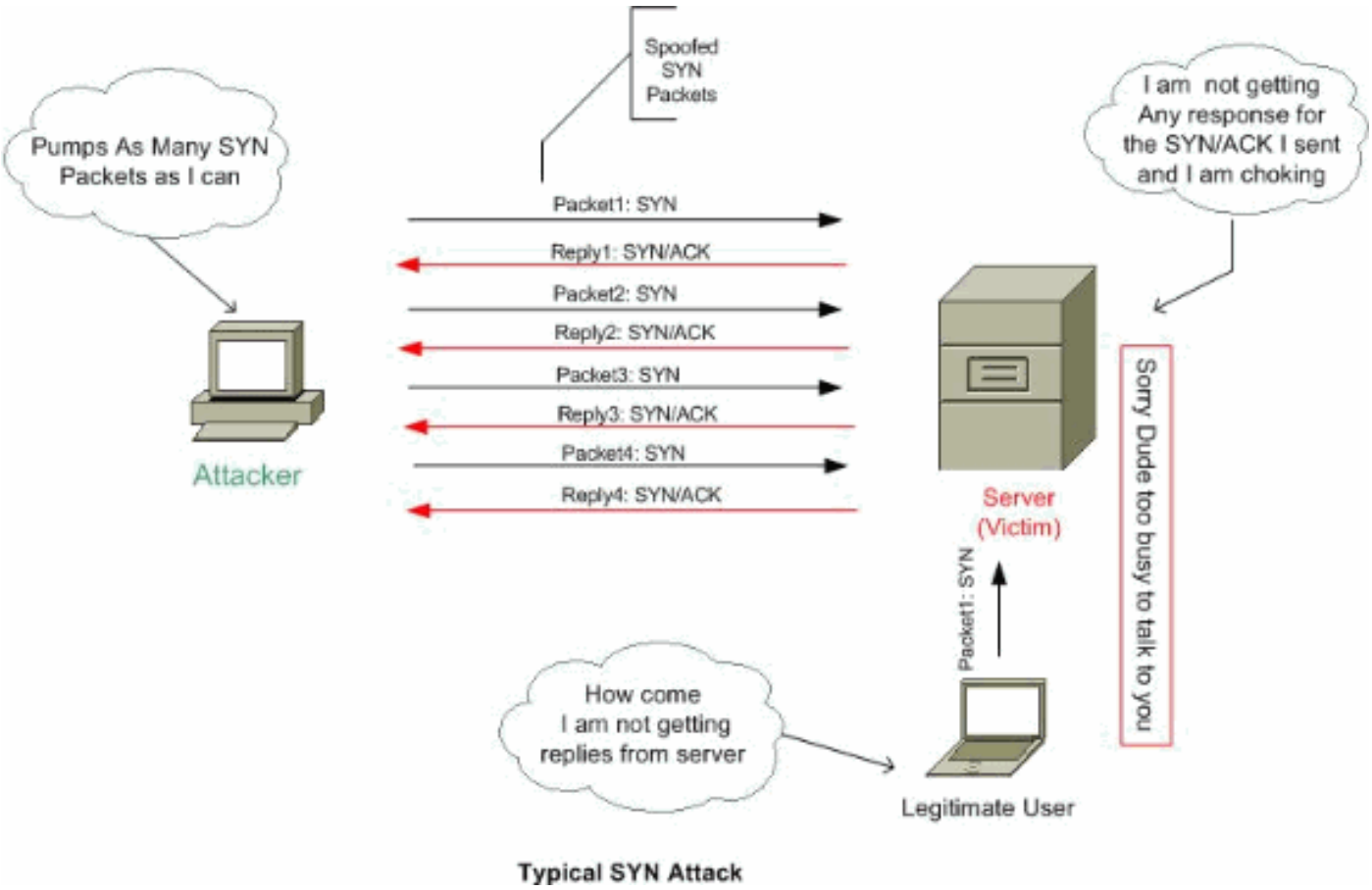
Атака TCP SYN использует недостаток этого алгоритма: атакующий узел-источник генерирует пакеты TCP SYN со случайными адресами источника и отправляет их на узел-жертву. Атакуемый хост отправляет пакет SYN ACK на случайный исходный адрес и добавляет запись в очередь соединений. Так как SYN ACK предназначен для некорректного или не существующего хоста, часть процедуры "трехэтапного установления TCP-соединения" никогда не завершится, а запись останется в очереди соединений до истечения определённого 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.

Дополнительные сведения об атаке TCP SYN см. в разделе Защита от атак TCP SYN Flood.



Typical SYN Attack

Смягчение

В данном разделе описываются способы уменьшения последствий от SYN-атак, путем установления предела максимального количества TCP- и UDP-соединений, максимального количества полуоткрытых соединений, задания времени ожидания подключения, а также отключения рандомизации последовательности TCP.

При достижении максимального количества полуоткрытых соединений устройство защиты отвечает на каждый пакет SYN, отправленный серверу, пакетом SYN+ACK, и не пропускает SYN пакет ко внутреннему серверу. Если внешнее устройство отвечает ACK пакетом, то устройство защиты определяет, что этот запрос настоящий, и не является частью потенциальной SYN-атаки. Устройство защиты устанавливает соединение с сервером и объединяет соединения. Если устройство защиты не получает пакет ACK от сервера, оно принудительно разрывает полуоткрытое соединение из-за превышения лимита времени.

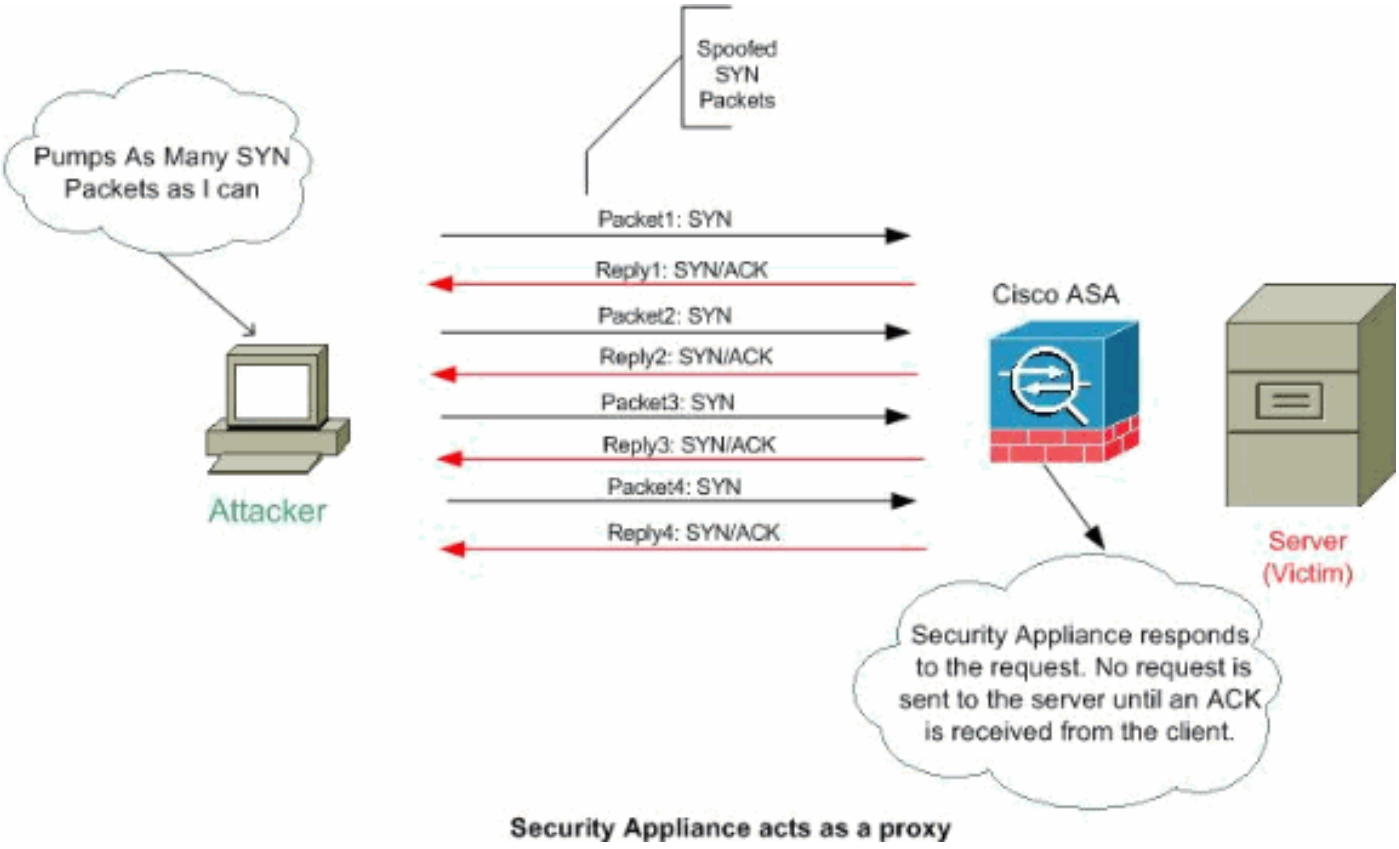
Каждое TCP-соединение имеет два номера начальной последовательности (ISN): один генерируется клиентом, другой - сервером. Устройство защиты назначает в произвольном порядке ISN для пакетов TCP SYN, проходящих в обоих направлениях.

Назначение в произвольном порядке номера ISN защищенному узлу позволяет предотвратить возможность предугадать злоумышленнику следующий номер ISN для нового соединения и таким образом подменить новый сеанс.

Назначение случайного значения для ISN TCP может быть отключено. Пример:

- Если используется другой встроенный межсетевой экран, который назначает ISN в случайном порядке, то нет необходимости двум межсетевым экранам выполнять эту операцию, несмотря на то, что это не влияет на изменения объема трафика.
- Если используется внешнее соединение BGP (eBGP) с многократными переходами через устройство защиты, и узлы eBGP используют MD5, рандомизация нарушит контрольную сумму MD5.
- Если используется устройство WAAS, для работы которого необходимо, чтобы устройство защиты не назначало случайным образом номера последовательности соединений.

Примечание: Можно также настроить максимальные числа подключений, максимальные неустановившиеся соединения и рандомизацию последовательности TCP в конфигурации NAT. Если настройки для одного и того же типа трафика производились обоими методами, то устройство защиты будет использовать то значение, которое является минимальным. Если рандомизация TCP последовательности была отключена другим методом, устройство защиты отключает рандомизацию TCP последовательности.



Выполните следующие шаги для назначения предела количества соединений:

1. **Для определения типа трафика добавьте карту класса с помощью команды class-map, как описано в разделеИспользование системы модульных политик.**
2. **Чтобы добавить или отредактировать карту политик, определяющую действия над трафиком, отнесенным к карте классов, введите следующую команду:**`hostname(config)#`**`policy-map name`**
3. Чтобы указать карту классов из шага 1, которой требуется присвоить действие, введите команду:`hostname(config-pmap)#`**`class class_map_name`**
4. Чтобы установить максимальное количество соединений (TCP и UDP), максимальное

количество полуоткрытых соединений, максимальное количество полуоткрытых соединений для каждого клиента (per-client-embryonic-max), максимальное количество соединений для каждого клиента (per-client-max) или отключить рандомизацию TCP-последовательности, введите следующую команду:`hostname(config-pmap-c)#` **`set connection`** `{[`**`conn-max`** `number] [`**`embryonic-conn-max`** `number] [`**`per-client-embryonic-max`** `number] [`**`per-client-max`** `number][`**`random-sequence-number`** `{`**`enable`** `|` **`disable`**`}}` Где число принимает целочисленные значения от 0 до 65535. По умолчанию установлено значение 0, что означает отсутствие ограничений на количество соединений.Можно ввести эту команду в одну строку (в любой последовательности), либо можно вводить каждый атрибут в виде отдельной команды. В текущей конфигурации команды объединены в одну строку.

5. Чтобы установить тайм-аут для соединений, полуоткрытых соединений и полузакрытых соединений, введите следующую команду:`hostname(config-pmap-c)#` **`set connection`** `{[`**`embryonic`** `hh[:mm[:ss]]] [`**`half-closed`** `hh[:mm[:ss]]] [`**`tcp`** `hh[:mm[:ss]]]}` **Где embryonic чч[:мм[:сс] - время в диапазоне от 0:0:5 до 1192:59:59. По умолчанию 0:0:30. Также можно установить значение 0, означающее, что время соединения не истечет.Значения half-closed чч[:мм[:сс] и tcp чч[:мм[:сс] - время в диапазоне от 0:5:0 до 1192:59:59. По умолчанию half-closed имеет значение 0:10:0, а tcp - 1:0:0. Также можно установить значение 0, означающее, что время соединения не истечет.**Можно ввести эту команду в одну строку (в любой последовательности), либо можно вводить каждый атрибут в виде отдельной команды. В текущей конфигурации команды объединены в одну строку.**Зарождающееся (полуоткрытое) соединение — это запрос TCP-соединения, в котором не завершен необходимый этап установления связи между источником и адресатом.Полузакрытое соединение — это когда соединение закрыто только с одной стороны путем отправки пакета FIN.** При этом TCP-соединение все еще поддерживается узлом.**Per-client-embryonic-max — максимальное количество полуоткрытых соединений, разрешенных для каждого клиента; имеет значение от 0 до 65535. По умолчанию значение равно 0, что означает неограниченное число соединений.Per-client-max — максимальное количество одновременно открытых соединений, разрешенных для каждого клиента; имеет значение от 0 до 65535. По умолчанию значение равно 0, что означает неограниченное число соединений.**
6. Чтобы активировать карту политик на одном или нескольких интерфейсах, введите следующую команду:`hostname(config)#` **`service-policy policymap_name`** *`{global | interface interface_name}`* **Где global означает, что карта политик применяется ко всем интерфейсам, а interface применяет карту политик к одному интерфейсу.** Допускается только одна глобальная политика. Можно заменить глобальную политику на интерфейсе, применив на нем политику обслуживания. К каждому интерфейсу может применяться только одна карта политик.

Пример:

```
ciscoasa(config)#class-map tcp_syn ciscoasa(config-cmap)#match port tcp eq 80 ciscoasa(config-cmap)#exit ciscoasa(config)#policy-map tcpmap ciscoasa(config-pmap)#class tcp_syn ciscoasa(config-pmap-c)#set connection conn-max 100 ciscoasa(config-pmap-c)#set connection embryonic-conn-max 200 ciscoasa(config-pmap-c)#set connection per-client-embryonic-max 10 ciscoasa(config-pmap-c)#set connection per-client-max 5 ciscoasa(config-pmap-c)#set connection random-sequence-number enable ciscoasa(config-pmap-c)#set connection timeout embryonic 0:0:45 ciscoasa(config-pmap-c)#set connection timeout half-closed 0:25:0 ciscoasa(config-pmap-c)#set connection timeout tcp 2:0:0 ciscoasa(config-pmap-c)#exit ciscoasa(config-pmap)#exit ciscoasa(config)#service-policy tcpmap global
```

Примечание: Для проверки общего числа полуоткрытых сеансов для какого-то конкретного

хоста используйте эту команду:

```
ASA-5510-8x# show local-host all Interface dmz: 0 active, 0 maximum active, 0 denied Interface
management: 0 active, 0 maximum active, 0 denied Interface xx: 0 active, 0 maximum active, 0
denied Interface inside: 7 active, 18 maximum active, 0 denied local host: <10.78.167.69>, TCP
flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark =
unlimited UDP flow count/limit = 0/unlimited
```

Примечание: Линия, `TCP  `, отображает количество полуоткрытых сеансов.

Защита от подмены IP-адреса

Могут ли устройства PIX/ASA блокировать атаки, связанные с подменой IP-адреса?

Подмена IP-адресов (IP Spoofing)

Для получения доступа злоумышленники создают пакеты с поддельным IP-адресами отправителя. Это позволяет находить уязвимости в приложениях, использующих информацию об IP-адресе для аутентификации, а также позволяет неавторизованному пользователю получить доступ к целевой системе (возможно даже с правами администратора root). Примерами являются службы rsh и rlogin.

Можно направлять пакеты через межсетевые экраны с функцией фильтрации и маршрутизации, если они не настроены на фильтрацию входящих пакетов, адрес источника которых находится в локальном домене. Необходимо отметить, что описываемый тип атаки возможен даже тогда, когда атакующий не получает пакеты в ответ.

Примеры конфигураций, которые являются потенциально уязвимыми:

- Межсетевые экраны с функциями Proxy, когда proxy-приложения используют IP-адрес источника для аутентификации
- Маршрутизаторы, работающие с внешними сетями, поддерживающие несколько внутренних интерфейсов
- Маршрутизаторы с двумя интерфейсами, поддерживающие деление внутренней сети на подсети

Смягчение

Механизм Unicast Reverse Path Forwarding (uRPF) защищает против подмены IP-адресов (когда пакет использует неправильный IP-адрес источника, чтобы скрыть адрес своего истинного источника), гарантируя, что все пакеты имеют тот IP-адрес источника, который соответствует правильному интерфейсу источника, указанному в таблице маршрутизации.

Обычно устройства защиты проверяют только адрес получателя для определения, куда пересылать пакет. Unicast RPF заставляет устройства защиты также проверять и адрес источника. **Поэтому данный механизм называется Reverse Path Forwarding (пересылка по обратному пути).** Для любого трафика, который необходимо пропускать через устройство защиты, в таблице маршрутизации устройства защиты должен быть указан обратный маршрут к источнику. Посмотрите RFC 2267 для получения дополнительной информации.

Примечание: `:-%PIX-1-106021: Deny protocol reverse path check from src_addr to dest_addr on interface int_name  ,  `. **Отключите проверку обратного пути с помощью команды no ip**

verify reverse-path interface (имя интерфейса), чтобы решить эту проблему:

`no ip verify reverse-path interface (interface name)`
Для внешнего трафика, например, устройство защиты может использовать маршрут по умолчанию для обеспечения защиты Unicast RPF. Если трафик поступает из внешнего интерфейса, при этом адрес источника отсутствует в таблице маршрутизации, устройство защиты использует маршрут по умолчанию для правильного определения внешнего интерфейса в качестве интерфейса-источника.

Если трафик поступает на внешний интерфейс с адреса, который присутствует в таблице маршрутизации, но связан с внутренним интерфейсом, устройство защиты удаляет пакет. Подобным образом происходит, если трафик поступает на внутренний интерфейс с неизвестного адреса источника, при этом устройство защиты удаляет пакет, поскольку подходящий маршрут (маршрут по умолчанию) указывает на внешний интерфейс.

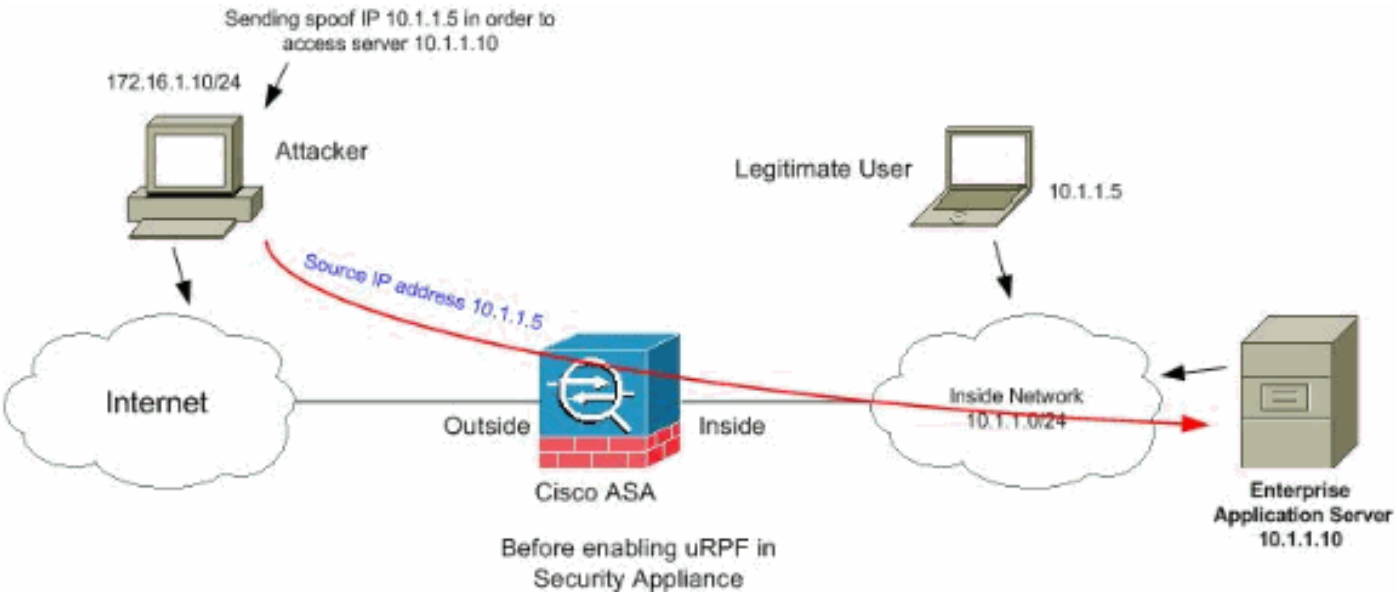
Unicast RPF реализуется следующим образом:

- Для пакетов ICMP сеанс не устанавливается, поэтому каждый пакет проверяется.
- Для пакетов UDP и TCP устанавливаются сеансы, поэтому для начального пакета выполняется проверка обратного маршшрута. Последующие пакеты, приходящие во время сессии, проверяются с помощью состояния существования, поддерживаемого во время сессии. Все последующие пакеты проверяются, чтобы гарантировать их прохождение через тот же интерфейс, который использовался для начального пакета.

Чтобы разрешить Unicast RPF, введите следующую команду:

```
hostname(config)#ip verify reverse-path interface interface_name
```
Пример:

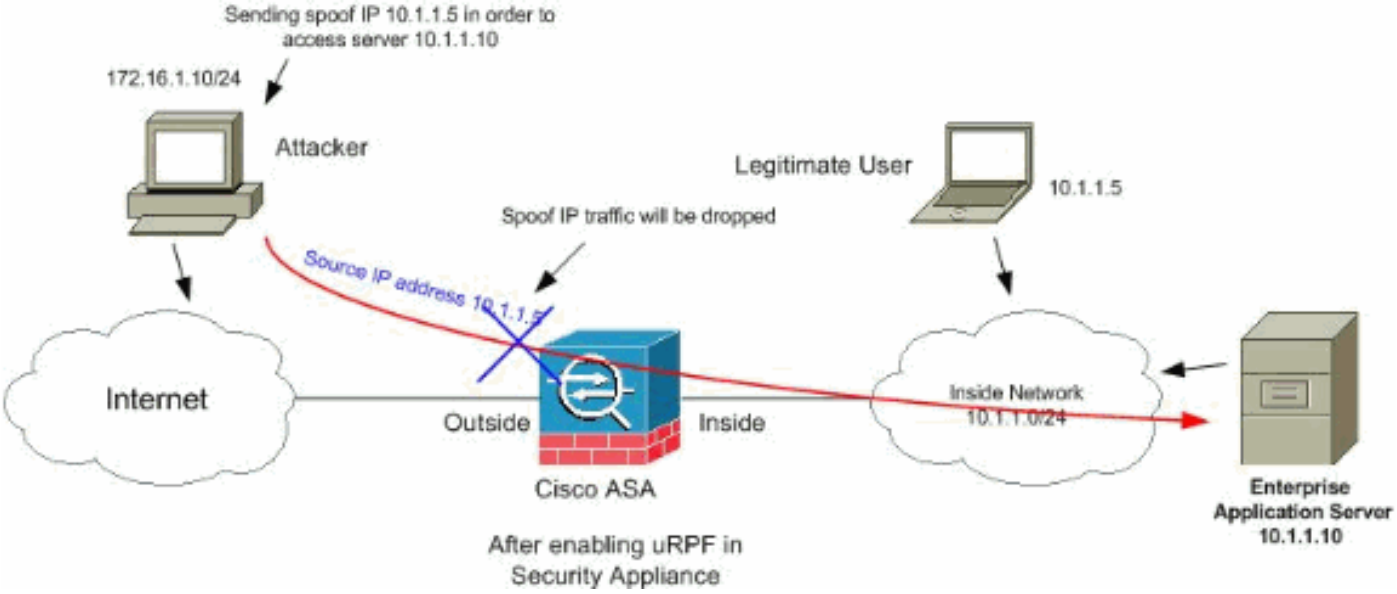
Как видно из рисунка, атакующий ПК направляет запрос серверу приложений 10.1.1.10 путем отправки пакета с поддельным IP-адресом источника 10.1.1.5/24, а сервер посылает пакет на реальный IP-адрес 10.1.1.5/24 в ответ на этот запрос. Этот вид запрещенного пакета будет атаковать как сервер приложений, так и обычного пользователя во внутренней сети.



Unicast RPF может предотвратить атаки, основанные на подмене адреса источника.

Необходимо настроить uRPF на внешнем интерфейсе устройства ASA, как показано ниже:

```
ciscoasa(config)#ip verify reverse-path interface outside
```



Определение подмены адреса с помощью сообщений системного журнала

Устройство защиты хранит полученные сообщения об ошибках в системном журнале, как показано ниже. Это свидетельствует о потенциальных атаках с использованием поддельных пакетов или о асимметричной маршрутизации.

1. **%PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name** **Пояснение**Это сообщение относится к соединениям. Это сообщение возникает, когда попытка подключиться к внутреннему адресу запрещена политикой безопасности, определенной для конкретного типа трафика. *Возможные значения tcp_flags соответствуют флагам в заголовке TCP во время запрета соединения.* Например, был получен пакет TCP, для которого в устройстве защиты указано состояние "соединение отсутствует", из-за чего он был удален. *Значение tcp_flags в этом пакете будет FIN и ACK.Возможны следующие значения tcp_flags:*ACK — количество полученных подтверждений.FIN — данные были отправлены.PSH — получатель передал данные в приложение.RST — соединение было сброшено.SYN — номера последовательностей были синхронизированы для начала соединения.URG — указатель срочности считался действующим.Существует много причин сбоя статического преобразования в устройстве PIX/ASA. Но общей причиной является то, что интерфейс демилитаризованной зоны (DMZ) имеет тот же уровень безопасности (0), что и внешний интерфейс.Для решения этой проблемы необходимо назначить разные уровни безопасности для всех интерфейсовДополнительные сведения см. в разделе Настройка параметров интерфейса.Это сообщение об ошибке появляется также в случае, если внешнее устройство отправляет к внутреннему клиенту пакет IDENT, удаляемый межсетевым экраном PIX. Для получения дополнительных сведений обратитесь к документу Снижение производительности PIX из-за проблем с протоколом IDENT
2. **%PIX|ASA-2-106007: Deny inbound UDP from outside_address/outside_port to**

`inside_address/inside_port due to DNS {Response|Query}` **Пояснение**Это сообщение относится к соединениям. **Это сообщение появляется в случае неудачного соединения, вызванного командой outbound deny.** В качестве переменных протокола могут выступать ICMP, TCP или UDP.**Рекомендуемое действие: Для проверки исходящих списков используйте команду show outbound.**

3. `%PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst interface_name: IP_address (type dec, code dec)`**Пояснение**Устройство защиты запрещает любые входящие пакеты ICMP. По умолчанию пакеты ICMP запрещены до особого разрешения.
4. `%PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.`**Пояснение**Это сообщение создается при поступлении пакета на интерфейс устройства защиты с IP-адресом 0.0.0.0 и MAC-адресом интерфейса устройства защиты. Кроме того, это сообщение создается, когда устройство защиты отбрасывает пакет с неверным адресом источника, который может включать в себя один из следующих неверных адресов:Сеть, замкнутая на себя (127.0.0.0)Широковещательные адреса (ограниченные, адреса сети, подсети и всех подсетей)Узла назначения (land.c)**Для дальнейшего улучшения обнаружения поддельных пакетов используйте команду icmp, чтобы настроить устройство защиты отбрасывать пакеты с адресами источника из внутренней сети. Это из-за того, что команда access-list устарела и может работать неправильно.Рекомендуемое действие:** Определите, пытается ли внешний пользователь взломать защищенную сеть. Определите неверно настроенных клиентов.
5. `%PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to IP_address`**Пояснение**Устройство защиты получает пакет с IP-адресом источника, равному IP-адресу получателя и портом получателя, равному порту источника. Это сообщение показывает наличие поддельного пакета, созданного для атаки систем. Эта атака также известна как LAND-атака.**Рекомендуемое действие:** Если сообщение продолжает возникать, это может говорить о том, что атака происходит в данный момент. В пакете не содержится достаточно информации для определения, откуда происходит атака.
6. `%PIX|ASA-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name`**Пояснение**Атака происходит в данный момент. Кто-то пытается подделать IP-адрес входящего соединения. Unicast RPF, также называемый обратной проверкой маршрута, обнаруживает пакет, у которого адрес источника не соответствует маршруту, и предполагает, что он является частью атаки на устройство защиты.**Это сообщение возникает при включении Unicast RPF с помощью команды ip verify reverse-path.** Эта функция обрабатывает пакеты, поступающие на интерфейс. Если она настроена обрабатывать внешний трафик, то устройство защиты будет проверять пакеты, поступающие из внешней сети.Устройство защиты проверяет маршрут на основании адреса источника. Если запись не найдена и маршрут не определен, в системном журнале появится сообщение о том, что соединение отключено.При обнаружении маршрута устройство защиты проверяет, какому интерфейсу он соответствует. Если пакет поступает на другой интерфейс, он либо является поддельным, либо используется ассиметричная маршрутизация, при которой возможны более одного маршрута к узлу назначения. Устройство защиты не поддерживает ассиметричную маршрутизацию.**Если устройство защиты настроено на внутреннем интерфейсе, оно выполняет проверку статического маршрута с помощью команды route или с помощью RIP.** Если адрес источника не обнаружен, предполагается, что пользователь внутри сети выполняет подмену

адресов.**Рекомендуемое действие:** Если атака происходит в данный момент времени, при включенной этой функции никаких действий от пользователя не требуется. Устройство защиты отражает атаку.**Примечание: Команда show asp drop** показывает пакеты или соединения, отброшенные ускоренным путем безопасности (asp), который мог бы помочь вам устранять проблему. Она также отображает время последнего обнуления счетчиков пути ускоренной защиты. **Используйте команду show a drop rpf-violated, по которой происходит увеличение значения счетчика в случае, когда команда ip verify reverse-path используется для интерфейса и устройство защиты получает пакет, для которого проверка маршрута IP-адреса источника выявляет, что интерфейс не соответствует тому, на который поступил пакет.**`ciscoasa#`**`show asp drop frame rpf-violated` `Reverse-path verify failed 2` **Примечание: Рекомендация:** Проверьте маршрут к источнику, используя IP-адрес, указанный в следующем системном сообщении, и разберитесь, почему от него исходит поддельный трафик.**Примечание: Системные сообщения:** 106021

7. `%PIX|ASA-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name`**Пояснение**Пакет, соответствующий соединению, поступает на интерфейс, который отличается от интерфейса, с которого начиналось соединение.Например, если пользователь начинает соединение на внутреннем интерфейсе, а устройство защиты обнаруживает то же соединение на интерфейсе периметра, то у устройства защиты имеется более одного пути к узлу назначения. Такая схема известна как ассиметричная маршрутизация и не поддерживается устройством защиты.Атакующий также может попытаться поместить пакеты из одного соединения в другое, чтобы пройти устройство защиты. В любом случае устройство защиты отобразит соответствующее сообщение и разорвет соединение.**Рекомендуемое действие: Это сообщение появляется в случае, когда не настроена команда ip verify reverse-path.** Убедитесь, что маршрутизация не является асимметричной.
8. `%PIX|ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_ID`**Пояснение**IP-пакет был отклонен ACL. **Этот сообщение отображается в случае, когда для ACL включен параметр log.Рекомендуемое действие:** Если в сообщениях указан один и тот же адрес источника, это сообщение может говорить о сборе базовых сведений (футпринтинге) или попытке сканирования портов. Свяжитесь с удаленными администраторами узлов.
9. `%PIX|ASA-3-210011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.`
10. `%ASA-4-419002: Received duplicate TCP SYN from in_interface:src_address/src_port to out_interface:dest_address/dest_port with different initial sequence number.`**Пояснение**В сообщении системного журнала указывается, что установление нового соединения через межсетевой экран приводит к превышению по крайней мере одного из пределов максимального количества соединений. В сообщении системного журнала указываются как пределы соединений, заданные с помощью статических команд, так и заданные с помощью системы модульных политик Cisco. Новое соединение будет запрещено межсетевым экраном до тех пор, пока одно из существующих соединений не будет разорвано, в результате чего будет уменьшено значение счетчика соединений до значения ниже настроенного максимума.*cnt — счетчик количества текущих соединенийlimit — заданный предел количества соединенийdir* — — направление трафика (входящий или исходящий)*sip — IP-адрес источникаsport — порт источникаsip — IP-адрес узла назначениядport —*

*порт узла назначенияif_name — имя или интерфейс, на котором получен трафик (может быть первичным или вторичным).***Рекомендуемое действие:** Из-за того, что предел количества соединений задается с определенной целью, сообщение системного журнала может свидетельствовать о возможной DoS-атаке, в случае которой источником трафика может выступать узел с поддельным IP-адресом. Если IP-адреса источника не являются полностью случайными, может помочь определение источника и блокировка его с помощью списка доступа. В других случаях для изоляция нежелательного трафика от разрешенного может помочь применение анализатора пакетов, с последующим анализом источника трафика.

Возможности обнаружения основных угроз в ASA 8.x

Устройство защиты Cisco ASA/PIX поддерживает функцию обнаружения угроз начиная с версии ПО 8.0. Используя возможности обнаружения основных угроз, устройство защиты следит за количеством отклоненных пакетов и за возникновением событий, связанных з безопасностью, ориентируясь на:

- Отказ из-за списков доступа
- Неправильный формат пакетов (например, из-за параметров invalid-ip-header или invalid-tcp-hdr-length)
- Превышение предела числа соединений (как пределов общесистемных ресурсов, так и заданных в конфигурации)
- Обнаружение DoS-атаки (например, неверный SPI, сбой проверки межсетевого экрана, отслеживающего состояние соединений)
- Сбой проверки основного межсетевого экрана (этот параметр объединяет в себе из рассматриваемого списка все случаи отклонения пакетов, связанные с работой межсетевого экрана. Он не включает в себя отклонения пакетов, не вызванные межсетевым экраном, например, из-за перегрузки интерфейса, потери пакетов на прикладном уровне и обнаружение атак, связанных со сканированием).)
- Обнаружение подозрительных ICMP-пакетов
- Потеря пакетов на прикладном уровне
- Interface overload
- Обнаружение сканирования (этот параметр следит за атаками сканирования, например, когда первый TCP-пакет не является SYN-пакетом, или когда TCP-соединение не устанавливается при трехэтапной процедуре установления соединения. Обнаружение угрозы, связанной с полным сканированием портов (дополнительные сведения см. в документеНастройка обнаружения угроз, связанных со сканированием портов) собирает информацию об активности сканирования и обрабатывает ее, например, относя узлы к разряду атакующих, автоматически разрывая с ними соединение).)
- Обнаружение незавершенных сеансов, например, обнаружение атак типа TCP SYN или атак, связанных с отсутствием отправки данных в сеансе UDP.

Когда устройство защиты обнаруживает угрозу, оно сразу оставляет в системном журнале сообщение (730100).

Обнаружение основных угроз оказывает эффект на производительность только при наличии отклоненных пакетов или потенциальных угроз. Даже в этом сценарии потеря производительности будет незначительна.

Команда show threat-detection rate используется для определения потенциальных атак, когда пользователь вошел в устройство защиты.

```
ciscoasa#show threat-detection rate Average(eps) Current(eps) Trigger Total events 10-min ACL
drop: 0 0 0 16 1-hour ACL drop: 0 0 0 112 1-hour SYN attck: 5 0 2 21438 10-min Scanning: 0 0 29
193 1-hour Scanning: 106 0 10 384776 1-hour Bad pkts: 76 0 2 274690 10-min Firewall: 0 0 3 22 1-
hour Firewall: 76 0 2 274844 10-min DoS attck: 0 0 0 6 1-hour DoS attck: 0 0 0 42 10-min
Interface: 0 0 0 204 1-hour Interface: 88 0 0 318225
```

Для получения дополнительных сведений о настройке обратитесь к разделу Настройка обнаружения основных угроз руководства по настройке ASA 8.0.

Сообщение системного журнала 733100

:

```
%ASA-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max
configured rate is rate_val; Current average rate is rate_val per second, max configured rate is
rate_val; Cumulative total count is total_cnt
```

Определенный объект в сообщении системного журнала превысил пиковую величину порогового значения или среднее пороговое значение. Объект может являться результатом отказа узла, порта TCP/UDP, IP-протокола или различных других отказов из-за потенциальных атак. Он указывает на наличие потенциальной атаки на систему.

Примечание: Эти сообщения об ошибках с разрешением применимы только к ASA 8.0 и позже.

1. Объект — общий или определенный источник данных об уровне отказа, которым может являться:Межсетевой экранBad pktsRate limitDoS attck (DoS-атаки)ACL dropConn limitICMP attkСканированиеSYN attckInspectInterface
2. rate_ID — настроенная величина, которая была превышена. Для большинства объектов можно указать до трех различных величин для разных интервалов.
3. rate_val — определенное значение величины.
4. total_cnt — общее значение с момента создания объекта или его обнуления.

Ниже в трех примерах показано, как отображаются эти переменные:

- Для интерфейса, отказавшего из-за ограничений процессора или шины:`%ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per second, max configured rate is 8000; Current average rate is 2030 per second, max configured rate is 2000; Cumulative total count is 3930654`
- Для отказа сканирования из-за потенциальных атак:`ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per second_ max configured rate is 10; Current average rate is 245 per second_ max configured rate is 5; Cumulative total count is 147409 (35 instances received)`
- Для недопустимых пакетов из-за потенциальных атак:`%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per second, max configured rate is 400; Current average rate is 760 per second, max configured rate is 100; Cumulative total count is 1938933`

Рекомендуемое действие:

Выполните следующие шаги в зависимости от указанного в сообщении типа объекта:

1. Если в сообщении системного журнала указан один из объектов:Межсетевой экранBad pktsRate limitDoS attackACL dropConn limitICMP attkСканированиеSYN attckInspectInterfaceПроверьте, является ли уровень отказа допустимым для рабочей среды.
2. *Измените пороговое значение для определенного типа рассоединения на подходящее, выполнив команду threat-detection rate xxx, где xxx имеет одно из следующих значений:*aCL dropbad-packet-dropconn-limit-dropdos-dropfw-dropicmp-dropinspect-dropinterface-dropscanning-threatsyn-attack
3. Если объектом в сообщении системного журнала является TCP или UDP порт, IP-протокол или отказавший узел, убедитесь, что выбрано подходящее значение отключения для рабочей системы.
4. **Измените пороговое значение для определенного типа рассоединения на подходящее, выполнив команду threat-detection rate bad-packet-drop.** Для получения дополнительных сведений о настройке обратитесь к разделу Настройка обнаружения основных угроз руководства по настройке ASA 8.0.

Примечание: Если не нужно, чтобы появлялось сообщение о превышении порога отключений, можно отключить его с помощью команды no threat-detection basic-threat.

Дополнительные сведения

- Страница поддержки устройств адаптивной безопасности Cisco ASA серии 5500
- Страница поддержки маршрутизаторов Cisco PIX серии 500
- Защита от атак TCP SYN
- Бюллетень Cisco Applied Mitigation: Определение и снижение последствий от уязвимостей типа DoS-атак в модуле коммутации содержимого
- Бюллетень Cisco Applied Mitigation: Определение и снижение последствий от различных уязвимостей в устройствах защиты Cisco PIX и ASA и модуле служб сетевого экрана
- Подмена IP-адресов (IP Spoofing)
- Cisco Systems – техническая поддержка и документация