ASA 8. 2. X примеров конфигурации функции обхода состояния TCP

Содержание

Введение

В этом документе описан порядок настройки функции обхода состояния TCP. Эта функция позволяет исходящие и входящие потоки через отдельные многофункциональные устройства защиты Cisco ASA серии 5500.

Предварительные условия

Требования к лицензии

Многофункциональные устройства защиты Cisco ASA серии 5500 должны иметь, по крайней мере, базовую лицензию.

Используемые компоненты

Сведения в этом документе основываются на устройстве адаптивной защиты Cisco (ASA) с версией 8.2 (1) и позже.

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

См. Cisco Technical Tips Conventions для получения информации об условных обозначениях в документации.

Обход состояния TCP

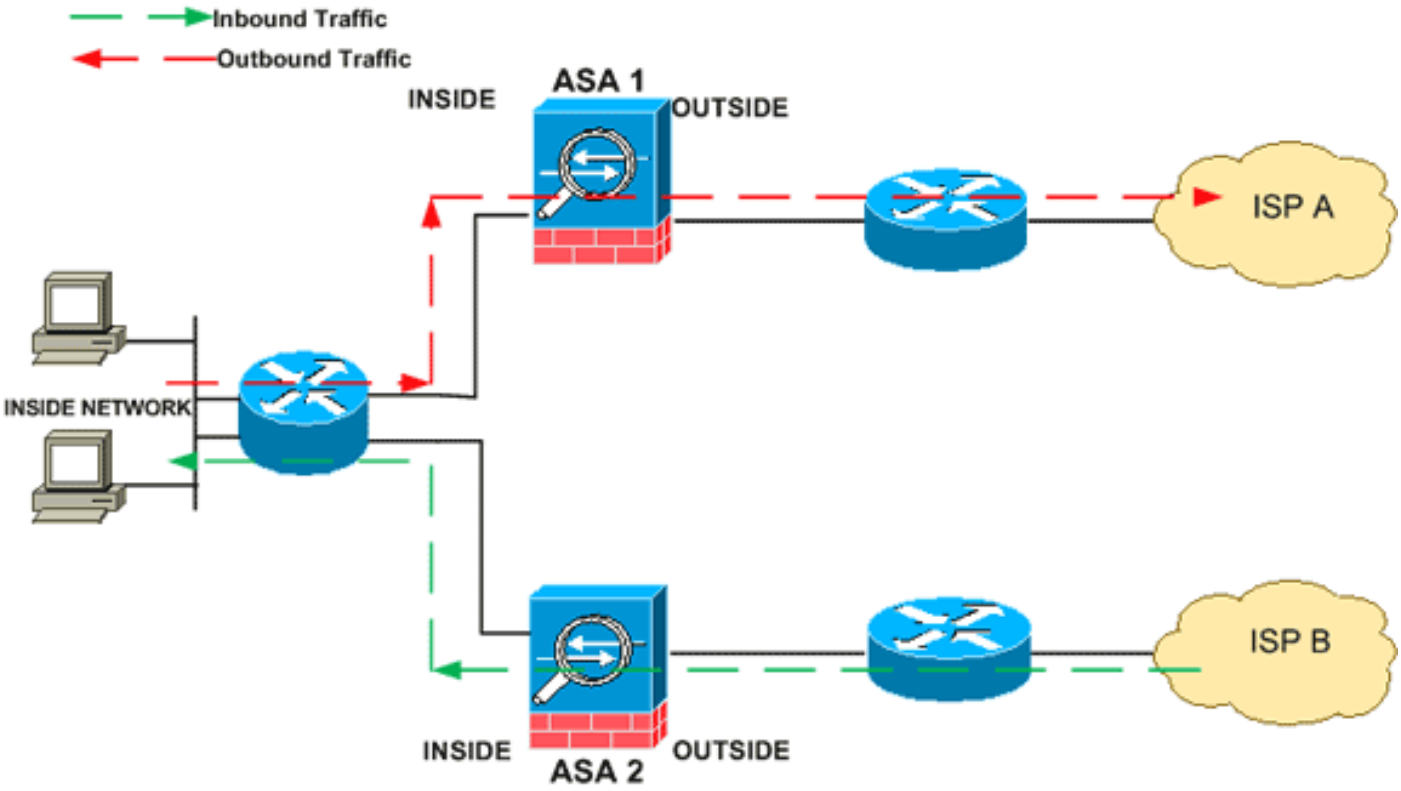
По умолчанию весь трафик, который проходит через устройство адаптивной защиты Cisco (ASA), осмотрен с помощью Адаптивного алгоритма безопасности и или позволен через или отброшен на основе политики безопасности. Для максимизации производительности межсетевого экрана ASA проверяет состояние каждого пакета (например, действительно ли это - новое соединение или установленное соединение?) и назначает его на любого путь управления сеансами (SYN - пакет нового соединения), быстрый маршрут (установленное соединение), или путь уровня управления (усовершенствованный контроль).

Пакеты TCP, которые совпадают с существующими соединениями в быстром маршруте, могут пройти через устройство адаптивной безопасности, не перепроверяя каждый аспект политики безопасности. Эта функция увеличивает производительность. Однако метод использовал устанавливать сеанс в быстром маршруте (который использует SYN - пакет), и проверки, которые происходят в быстром маршруте (таком как порядковый номер TCP), может стоять на пути асимметричных решений маршрутизации: и исходящий и входящий поток соединения должен пройти через тот же ASA.

Например, новое соединение переходит *к ASA 1*. SYN - пакет проходит через путь управления сеансами, и запись для соединения добавлена к таблице быстрого маршрута. Если последующие пакеты этого соединения пройдут *ASA 1*, то пакеты будут совпадать с записью в быстром маршруте и проходятся. Если последующие пакеты переходят *к ASA 2*, где не было SYN - пакета, который прошел путь управления сеансами, то нет никакой записи в быстром маршруте для соединения, и пакеты отброшены.

Если вам настроили асимметричную маршрутизацию на вышестоящих маршрутизаторах и альтернативах трафика между двумя ASA, то можно настроить обход состояния TCP для определенного трафика. Обход состояния TCP изменяет способ, которым сеансы установлены в быстром маршруте, и отключает проверки быстрого маршрута. Эта функция рассматривает Трафик TCP очень, как это рассматривает UDP - подключение: когда не-SYN - пакет, совпадающий с указанными сетями, вводит ASA, и нет записи быстрого маршрута, тогда пакет проходит путь управления сеансами для установления соединения в быстром маршруте. Однажды в быстром маршруте, трафик обходит проверки быстрого маршрута.

Этот образ предоставляет пример асимметричной маршрутизации, где исходящий трафик проходит другой ASA, чем входящий трафик:



Примечание: Опция обхода состояния TCP отключена по умолчанию на многофункциональных устройствах защиты Cisco ASA серии 5500.

Сведения о поддержке

Этот раздел предоставляет сведения о поддержке для функции обхода состояния TCP.

- Режим контекста — Поддерживаемый на сингле и многоконтекстном режиме.
- Режим межсетевого экрана — Поддерживаемый в маршрутизировавшем и прозрачном режиме.
- Аварийное переключение — Поддерживает аварийное переключение.

Эти функции не поддерживаются при использовании обхода состояния TCP:

- Контроль приложения — Контроль приложения требует, чтобы оба входящих и исходящих трафика прошли через тот же ASA, таким образом, контроль приложения не поддерживается с обходом состояния TCP.
- AAA аутентифицировал сеансы — Когда пользователь аутентифицируется с одним ASA, трафик, возвращающийся через другой ASA, будет запрещен, потому что пользователь не аутентифицировался с тем ASA.
- Перехват TCP, максимальный предел неустановившегося соединения, рандомизация порядкового номера TCP — ASA не отслеживает состояние соединения, таким образом, не применены эти функции.
- Нормализация TCP — нормализатор TCP отключен.
- SSM и функциональность SSC — Вы не можете использовать обход состояния TCP и любое приложение, работающее на SSM или SSC, таком как IPS или CSC.

NAT Рекомендации: Поскольку сеанс преобразования установлен отдельно для каждого ASA, убедиться настроить статический NAT на обоих ASA для трафика обхода состояния TCP; при использовании динамического NAT адрес, выбранный для сеанса на *ASA 1*, будет отличаться от адреса, выбранного для сеанса на *ASA 2*.

Настройка

В этом разделе описывается настроить функцию обхода состояния TCP на многофункциональном устройстве защиты Cisco ASA серии 5500 (ASA).

Конфигурация функции обхода состояния TCP

Выполните эти шаги для настройки функции обхода состояния TCP на многофункциональном устройстве защиты Cisco ASA серии 5500:

1. Используйте class-map class_map_name команда для создания *карты классов*. Карта классов используется для определения трафика, для которого вы хотите отключить контроль самонастраивающегося межсетевого экрана. Карта классов, используемая в данном примере, является *tcp_bypass*.`ASA(config)#`**`class-map tcp_bypass`**
2. Используйте команду parameter соответствия для определения представляющего интерес трафика в карте классов. При использовании Модульной Системы политик используйте **команду match access-list** в режиме конфигурации схемы классов для использования списка доступа для определения трафика, к которому вы хотите применить действия. Вот пример этой конфигурации:`ASA(config)#`**`class-map tcp_bypass`** `ASA(config-cmap)#`**`match access-list tcp_bypass`** *tcp_bypass* является названием access-list, используемого в данном примере. См. Определение Трафика (Карта классов Уровня 3/4) для получения дополнительной информации об определении представляющего интерес трафика.
3. Используйте команду названия policy-map, чтобы добавить карту политик или отредактировать карту политик (который уже присутствует), который заставляет действия уже брать с трафиком карты классов, заданным. При использовании Модульной Системы политик используйте **команду policy-map** (без ключевого слова типа) в режиме глобальной конфигурации, чтобы назначить действия торговать этим, вы определили с картой классов Уровня 3/4 (class-map или команда class-map type management). В данном примере карта политик является *tcp_bypass_policy*:`ASA(config-cmap)#`**`policy-map tcp_bypass_policy`**
4. Используйте команду класса в режиме конфигурации карты политик для присвоения карты классов *(tcp_bypass)* уже созданный к карте политик *(tcp_bypass_policy)*, где можно назначить действия на трафик карты классов. В данном примере карта классов является *tcp_bypass*:`ASA(config-cmap)#`**`policy-map tcp_bypass_policy`** `ASA(config-pmap)#`**`class tcp_bypass`**
5. Используйте команду обхода состояния TCP расширенных настроек соединения набора в режиме конфигурации класса для активации опции обхода состояния TCP. Эта команда была представлена в версии 8.2 (1). Режим конфигурации класса доступен от режима конфигурации карты политик как показано в данном примере:`ASA(config-cmap)#`**`policy-map tcp_bypass_policy`** `ASA(config-pmap)#`**`class tcp_bypass`** `ASA(config-pmap-c)#`**`set connection advanced-options tcp-state-bypass`**
6. Используйте стратегию обслуживания policymap_name [глобальный | интерфейс *intf*] команда в режиме глобальной конфигурации для активации карты политик глобально на всех интерфейсах или на предназначенном интерфейсе. Для отключения политики обслуживания используйте **эту команду с параметром no**. Использование **команда service-policy** для включения ряда политики по **interface.global** применяет карту политик ко всем интерфейсам и **интерфейсу**, применяет политику к одному интерфейсу.

Допускается только одна глобальная политика. Можно заменить глобальную политику на интерфейсе, применив на нем политику обслуживания. Можно применить только одну карту политик к каждому интерфейсу.`ASA(config-pmap-c)#service-policy tcp_bypass_policy outside`

Вот пример конфигурации для обхода состояния TCP:

```
!--- Configure the access list to specify the TCP traffic !--- that needs to by-pass inspection to improve the performance. ASA(config)#access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any !--- Configure the class map and specify the match parameter for the !--- class map to match the interesting traffic. ASA(config)#class-map tcp_bypass ASA(config-cmap)#description "TCP traffic that bypasses stateful firewall" ASA(config-cmap)#match access-list tcp_bypass !--- Configure the policy map and specify the class map !--- inside this policy map for the class map. ASA(config-cmap)#policy-map tcp_bypass_policy ASA(config-pmap)#class tcp_bypass !--- Use the set connection advanced-options tcp-state-bypass !--- command in order to enable TCP state bypass feature. ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass !--- Use the service-policy policymap_name [ global | interface intf ] !--- command in global configuration mode in order to activate a policy map !--- globally on all interfaces or on a targeted interface. ASA(config-pmap-c)#service-policy tcp_bypass_policy outside ASA(config-pmap-c)#static (inside,outside) 192.168.1.224 10.1.1.0 netmask 255.255.255.224
```

Проверка

Команда show conn отображает количество активного TCP и UDP - подключений и предоставляет сведения о соединениях различных типов. Для отображения состояния соединения для определяемого типа соединения используйте команду show conn в привилегированном режиме EXEC. Эта команда поддерживает адреса IPv4 и IPv6. Выходной показ для соединений, которые используют **обход состояния TCP**, включает флаг **b**.

Устранение неполадок

ASA отображает это сообщение об ошибках даже после того, как будет активирована ОБХОДНАЯ СОСТОЯНИЕМ TCP опция.

```
%PIX|ASA-4-313004:Denied ICMP type=icmp_type, from source_address oninterface interface_name to dest_address:no matching session
```

Пакеты ICMP были отброшены устройством безопасности из-за проверок безопасности, добавленных функцией ICMP с отслеживанием состояния, которые обычно являются или эхо - ответ ICMP без допустимого запроса эха, уже прошел через устройство безопасности или сообщения об ошибках ICMP, не отнесенные к любому TCP, UDP или сеансу ICMP, уже установленному в устройстве безопасности.

ASA отображает этот журнал, даже если обход состояния TCP включен, потому что отключение этой функциональности (т.е. проверке ICMP возвращают записи для Типа 3 в таблице подключений) не возможно. Но функция обхода состояния TCP работает правильно.

Используйте эту команду, чтобы препятствовать тому, чтобы появились эти сообщения:

```
hostname(config)#no logging message 313004
```

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация