Настройте функцию обхода состояния TCP на серии 5500 ASA

Содержание

Введение

Этот документ описывает, как настроить функцию обхода состояния TCP, которая позволяет исходящему и входящему трафику течь через отдельные многофункциональные устройства защиты Cisco ASA серии 5500 (ASA).

Предварительные условия

Требования

Cisco ASA должен иметь, по крайней мере, базовую лицензию, установленную, прежде чем можно будет продолжить конфигурацию, которая описана в этом документе.

Используемые компоненты

Сведения в этом документе основываются на серии 5500 Cisco ASA, которая работает под управлением ПО версии 9. x.

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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Этот раздел предоставляет обзор функции обхода состояния TCP и связанных сведений о поддержке.

Обзор характеристик обхода состояния TCP

По умолчанию весь трафик, который проходит через ASA, осмотрен через Адаптивный алгоритм безопасности и или позволен через или отброшен на основе политики безопасности. Для максимизации производительности Межсетевого экрана ASA проверяет состояние каждого пакета (например, это проверяет, является ли это новым соединением или установленным соединением), и назначает его на любого путь управления сеансами (новое соединение Синхронизируют (SYN) пакет), быстрый маршрут (установленное соединение), или путь уровня управления (усовершенствованный контроль).

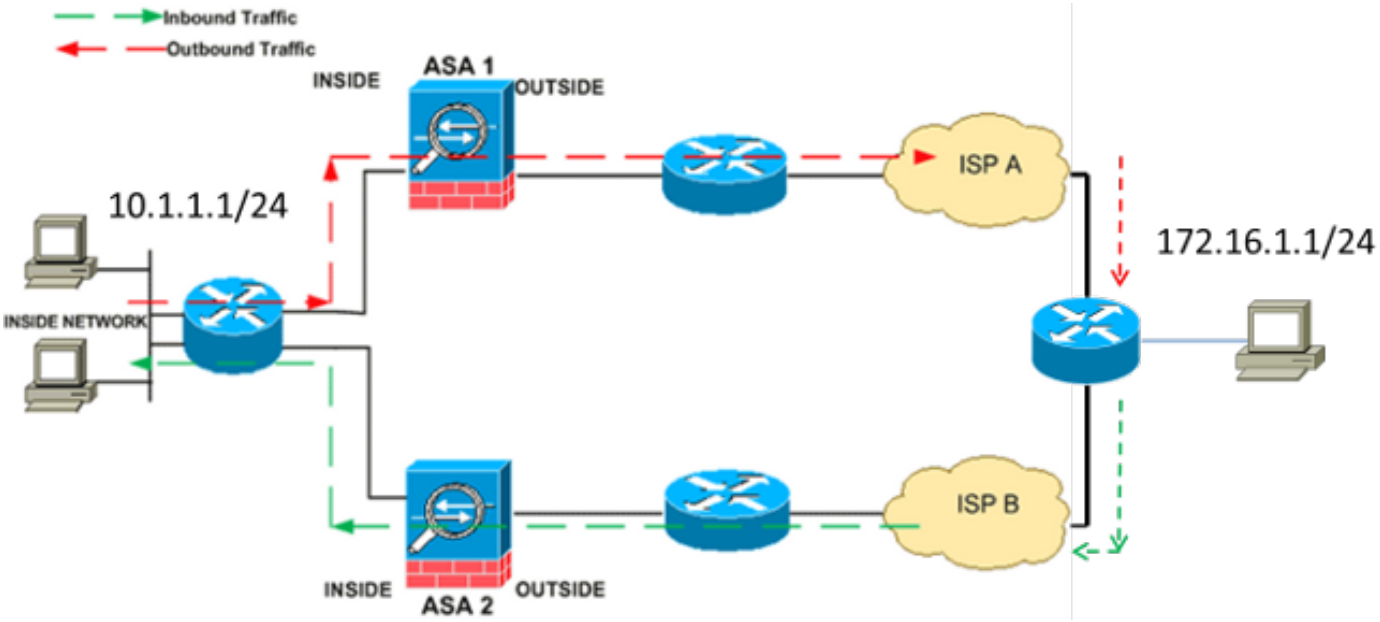
Пакеты TCP, которые совпадают с текущими соединениями в быстром маршруте, могут пройти через ASA без перепроверки каждого аспекта политики безопасности. Эта функция увеличивает производительность. Однако метод, который используется для установления сеанса в быстром маршруте (который использует SYN - пакет) и проверки, которые происходят в быстром маршруте (таком как порядковый номер TCP), может стоять на пути асимметричных решений маршрутизации; и исходящие и входящие потоки соединения должны 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 на этом соединении проходят *ASA 1*, пакеты совпадают 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 функцию обхода состояния TCP определенного трафика. Функция обхода 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, который совпадает с указанными сетями, вводит ASA, и нет никакой 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 серии 5500 Cisco ASA. Кроме того, конфигурация обхода состояния TCP может вызвать большое число соединений, если она должным образом не внедрена.

Сведения о поддержке

В этом разделе описываются сведения о поддержке для функции обхода состояния TCP.

- **Режим Г¦¦ контекста** функция обхода состояния TCP поддерживается на сингле и многоконтекстных режимах.
- **Режим межсетевого экрана Г¦¦** функция обхода состояния TCP поддерживается в маршрутизировавшем и прозрачных режимах.
- **Аварийное переключение Г¦¦** состояние TCP обходит аварийное переключение поддержек характеристик.

Когда вы используете функцию обхода состояния TCP, эти функции не поддерживаются:

- Контроль приложения Г¦¦ **контроля приложения** требует, что оба, входящий и исходящий трафик проходит через тот же ASA, таким образом, контроль приложения не поддерживается с функцией обхода состояния TCP.
- **Аутентификация, авторизация и учет (AAA) аутентифицировала** Г¦¦ **сеансов**, Когда пользователь аутентифицируется с одним ASA, трафик, который возвращается через другой ASA, запрещен, потому что пользователь не аутентифицировался с тем ASA.
- **Перехват TCP, максимальный предел неустановившегося соединения, рандомизация Г¦¦**

порядкового номера TCP, которую ASA не отслеживает состояния соединения, таким образом, эти функции не применены.

- **Нормализация Г¦ TCP** нормализатор TCP отключена.
- **Модуль служб безопасности (SSM) и функциональность Г¦ Карты сервисов безопасности (SSC)**, Вы не можете использовать функцию обхода состояния TCP ни с какими приложениями, которые работают на SSM или SSC, таком как IPS или Безопасность содержания (CSC).

Примечание: Поскольку сеанс преобразования установлен отдельно для каждого ASA, гарантируйте настройку статической трансляции сетевых адресов (NAT) на обоих из ASA для трафика обхода состояния TCP. При использовании динамического NAT адрес, который выбран для сеанса на *ASA 1*, будет отличаться от адреса, который выбран для сеанса на *ASA 2*.

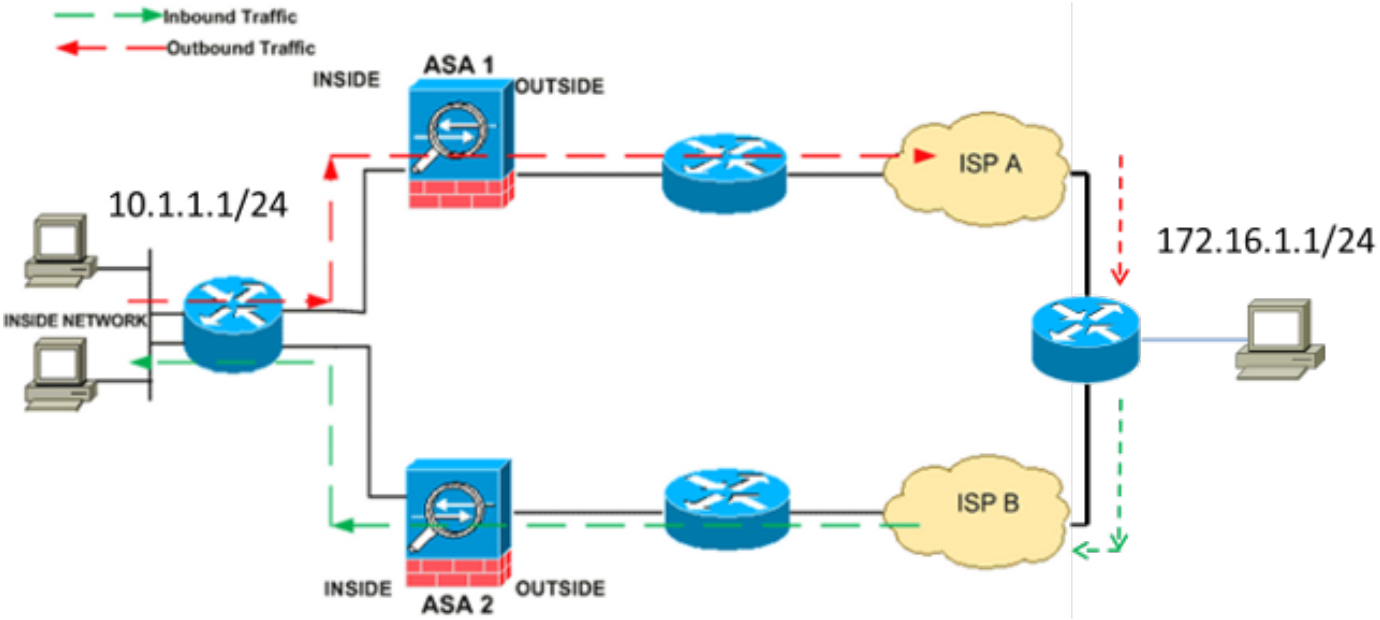
Настройка

В этом разделе описывается настроить функцию обхода состояния TCP на серии 5500 ASA в двух других сценариях.

Примечание: Используйте Средство поиска команд Command Lookup Tool (только зарегистрированные клиенты) для получения дополнительных сведений о командах, которые используются в этом разделе.

Сценарий 1

Это - топология, которая используется для первого сценария:



Примечание: Необходимо применить конфигурацию, которая описана в этом разделе к

обоим из ASA.

Выполните эти шаги для настройки функции обхода состояния TCP:

1. Введите **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.**Примечание:** Карта классов, которая используется в данном примере, является **tcp_bypass**.`ASA(config)#class-map tcp_bypass`
2. Введите **команду parameter соответствия** для определения трафика интереса в карте классов. При использовании Модульной Системы политик используйте **команду match access-list** в режиме *конфигурации схемы классов* для использования списка доступа для идентификации 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
   ```

   Примечание: tcp_bypass является названием access-list, который используется в данном примере. См. Трафик Определения (Карта классов Уровня 3/4) раздел *руководства по настройке Cisco ASA 5500 с помощью CLI, 8.2* для получения дополнительной информации о том, как задать трафик интереса.
3. Введите команду **названия policy-map**, чтобы добавить карту политик или отредактировать карту политик (который уже присутствует), который назначает действия для исполнения в отношении трафика карты заданного класса. При использовании Модульной Системы политик используйте **команду policy-map** (без ключевого слова *типа*) в *режиме глобальной конфигурации* для присвоения действий на трафик, который 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. Введите команду **класса** в режим *конфигурации карты политик* для присвоения созданной карты классов *(tcp_bypass)* на карту политик *(tcp_bypass_policy)* так, чтобы можно было 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. Введите команду **обхода состояния TCP расширенных настроек соединения набора** в *режим 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. Введите **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**. Введите **команду service-policy** для включения ряда политики по интерфейсу. **Глобальное ключевое слово** применяет карту политик ко всем интерфейсам, и **интерфейсное** ключевое слово применяет карту политик только к одному интерфейсу. Допускается только одна

глобальная политика. Для переопределения глобальной политики на интерфейсе можно применить политику обслуживания к тому интерфейсу. Можно применить только одну карту политик к каждому интерфейсу. Например:

```
ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
```

Вот пример конфигурации для функции обхода состояния TCP на *ASA1*:

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

ASA1(config)#access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.

ASA1(config)#class-map tcp_bypass
ASA1(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA1(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.

ASA1(config-cmap)#policy-map tcp_bypass_policy
ASA1(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA1(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.

ASA1(config-pmap-c)#service-policy tcp_bypass_policy outside

!--- NAT configuration

ASA1(config)#object network obj-10.1.1.0
ASA1(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

Вот пример конфигурации для функции обхода состояния TCP на *ASA2*:

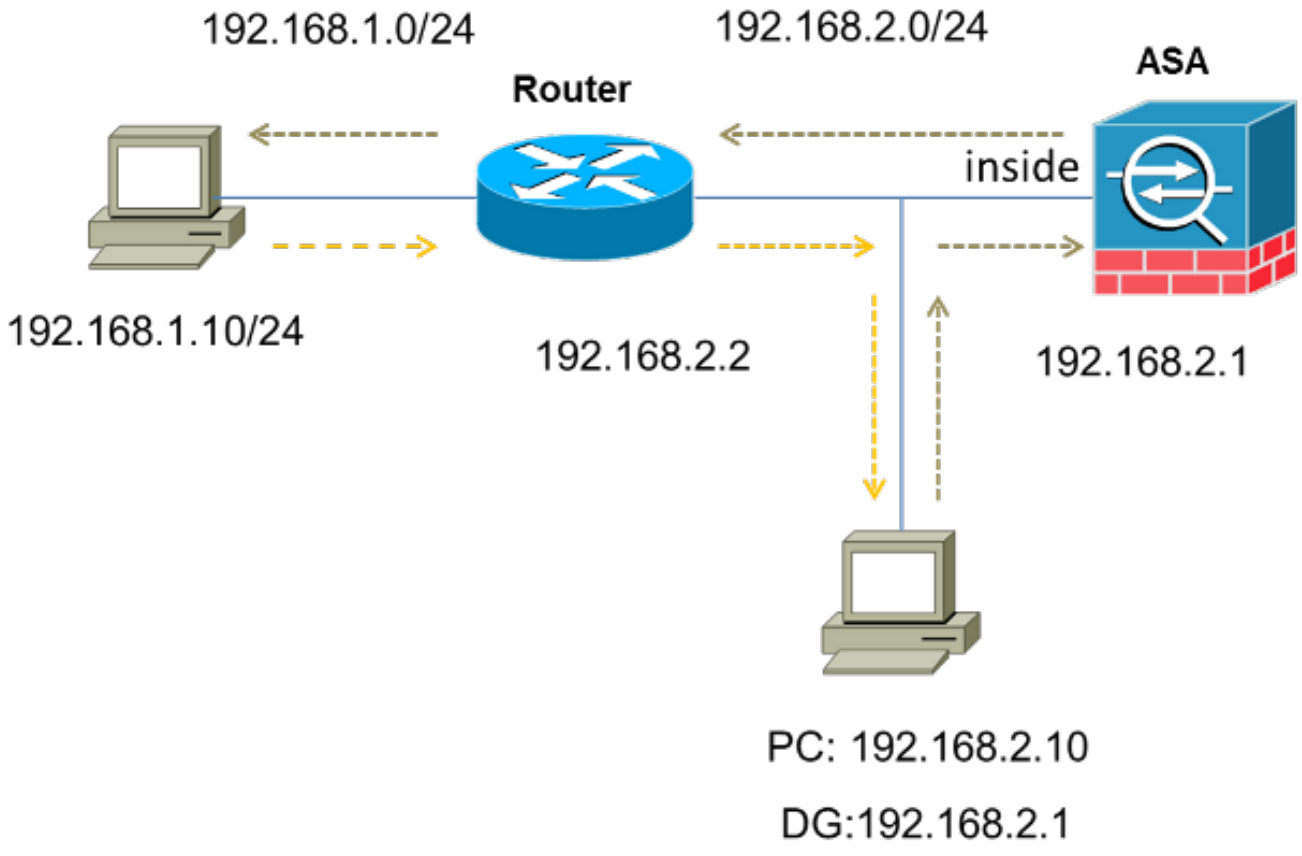
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

ASA2(config)#access-list tcp_bypass extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.

ASA2(config)#class-map tcp_bypass
ASA2(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA2(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.
```

```
ASA2(config-cmap)#policy-map tcp_bypass_policy
ASA2(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA2(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.

ASA2(config-pmap-c)#service-policy tcp_bypass_policy outside

!--- NAT configuration

ASA2(config)#object network obj-10.1.1.0
ASA2(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

Сценарий 2

В этом разделе описывается настроить функцию обхода состояния TCP на ASA для сценариев, которые используют асимметричную маршрутизацию, где трафик вводит и оставляет ASA от того же интерфейса *(u-превращение)*.

Вот топология, которая используется в этом сценарии:



Выполните эти шаги для настройки функции обхода состояния TCP:

1. Создайте *access-list* для соответствия с трафиком, который должен обойти контроль TCP:
   ```
   ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
   192.168.1.0 255.255.255.0
   ```
2. Введите 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.**Примечание:** Карта классов, которая используется в данном примере, является **tcp_bypass**.
   ```
   ASA(config)#class-map tcp_bypass
   ```
3. Введите команду parameter соответствия для определения трафика интереса к карте классов. При использовании Модульной Системы политик используйте **команду match access-list** в режиме *конфигурации схемы классов* для использования списка доступа для идентификации 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
   ```
   Примечание: tcp_bypass является названием access-list, который используется в данном примере. См. Определение Трафика (Карта классов Уровня 3/4) раздел *руководства по настройке Cisco ASA 5500 с помощью CLI, 8.2* для получения дополнительной информации о том, как задать трафик интереса.
4. Введите команду названия policy-map, чтобы добавить карту политик или отредактировать карту политик (который уже присутствует), который устанавливает действия для исполнения в отношении трафика карты заданного класса. При использовании Модульной Системы политик используйте **команду policy-map** (без ключевого слова *типа*) в *режиме глобальной конфигурации* для присвоения действий на трафик, который 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
   ```
5. Введите команду класса в режим *конфигурации карты политик* для присвоения созданной карты классов *(tcp_bypass)* на карту политик *(tcp_bypass_policy)* так, чтобы можно было 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
   ```
6. Введите команду обхода состояния TCP расширенных настроек соединения набора в *режим 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
   ```
7. Введите 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**. Введите **команду service-policy** для включения ряда политики по интерфейсу. **Глобальное ключевое слово** применяет карту политик ко всем интерфейсам, и **интерфейсное** ключевое слово применяет политику только к одному интерфейсу. Допускается только одна глобальная политика. Для переопределения глобальной политики на интерфейсе можно

применить политику обслуживания к тому интерфейсу. Можно применить только одну карту политик к каждому интерфейсу. Например:

```
ASA(config-pmap-c)#service-policy tcp_bypass_policy inside
```

8. Разрешите тот же уровень безопасности для трафика на ASA:

```
ASA(config)#same-security-traffic permit intra-interface
```

Вот пример конфигурации для функции обхода состояния TCP на ASA:

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to bypass inspection to improve the performance.

ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
192.168.1.0 255.255.255.0

!--- 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 inside

!--- Permit same security level traffic on the ASA to support U-turning

ASA(config)#same-security-traffic permit intra-interface
```

Проверка

Введите команду show conn для просмотра количества активного TCP и UDP - подключений и информации о соединениях различных типов. Для отображения состояния соединения для определяемого типа соединения введите команду show conn в *привилегированный режим EXEC*.

> **Примечание:** Эта команда поддерживает адреса IPv4 и IPv6. Выходные данные, которые отображены для соединений, которые используют функцию обхода состояния TCP, включают флаг **b**.

Ниже представлен пример выходных данных:

```
ASA(config)show conn
1 in use, 3 most used
```

```
TCP tcp 10.1.1.1:49525 tcp 172.16.1.1:21, idle 0:01:10, bytes 230, flags b
```

Устранение неполадок

Нет никаких определенных сведений об устранении проблем для этой функции. См. эти документы для общих сведений об устранении проблем подключения:

- Захваты пакета ASA с CLI и примером конфигурации ASDM
- ASA 8. 2: поток пакетов через межсетевой экран Cisco ASA

  Примечание: Обходные соединения состояния TCP не реплицированы в резервный модуль в паре аварийного переключения.

Сообщения об ошибках

ASA отображает это сообщение об ошибках даже после того, как будет активирована опция обхода состояния TCP:

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

Пакеты Протокола ICMP отброшены ASA из-за проверок безопасности, которые добавлены функцией ICMP с отслеживанием состояния. Это обычно или *эхо - ответ ICMP* без допустимого *запроса эха*, уже прошел через ASA или сообщения об ошибках ICMP, которые не отнесены ни к какому TCP, UDP или сеансу ICMP, в настоящее время устанавливаемому в ASA.

ASA отображает этот журнал, даже если опция обхода состояния TCP активирована, потому что выведение из строя этой функциональности (т.е. проверки ICMP *возвращаются*, записи для Типа 3 в таблице подключений) не возможно. Однако функция обхода состояния TCP работает правильно.

Введите эту команду для предотвращения появления этих сообщений:

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

Дополнительные сведения

- Диспетчер адаптивных устройств защиты Cisco (Cisco Adaptive Security Device Manager)
- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация