Configuración de la Función TCP State Bypass en ASA serie 5500

Contenido

Introducción

Este documento describe cómo configurar la función de omisión de estado TCP, que permite que el tráfico entrante y saliente fluya a través de Cisco ASA 5500 Series Adaptive Security Appliances (ASA) independientes.

Prerequisites

Requirements

Cisco ASA debe tener instalada al menos la licencia base para poder continuar con la configuración que se describe en este documento.

Componentes Utilizados

La información de este documento se basa en Cisco ASA serie 5500 que ejecuta la versión de software 9.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Esta sección proporciona una descripción general de la función de desvío de estado TCP y la información de soporte relacionada.

Descripción General de la Función TCP State Bypass

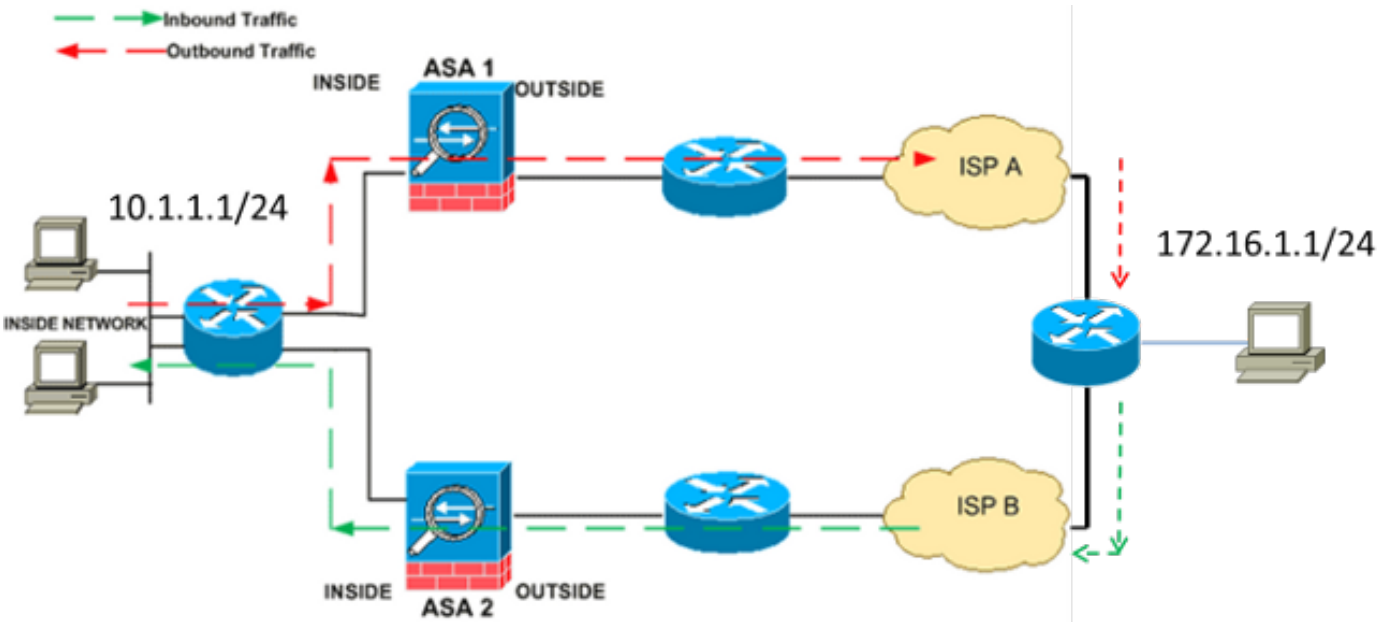
De forma predeterminada, todo el tráfico que pasa a través del ASA se inspecciona a través del algoritmo de seguridad adaptable y se permite o se descarta según la política de seguridad. Para maximizar el rendimiento del firewall, el ASA verifica el estado de cada paquete (por ejemplo, verifica si se trata de una conexión nueva o establecida) y lo asigna a la ruta de administración de la sesión (un nuevo paquete Synchronize (SYN) de conexión), a la ruta rápida (una conexión establecida) o a la ruta del plano de control (inspección avanzada).

Los paquetes TCP que coinciden con las conexiones actuales en el trayecto rápido pueden pasar a través del ASA sin una nueva verificación de todos los aspectos de la política de seguridad. Esta función maximiza el rendimiento. Sin embargo, el método que se utiliza para establecer la sesión en el trayecto rápido (que utiliza el paquete SYN) y las verificaciones que ocurren en el trayecto rápido (como el número de secuencia TCP) pueden interponerse en el camino de las soluciones de ruteo asimétricas; los flujos de salida y de entrada de una conexión deben pasar a través del mismo ASA.

Por ejemplo, una nueva conexión va a *ASA 1*. El paquete SYN pasa a través de la trayectoria de administración de la sesión y se agrega una entrada para la conexión a la tabla de trayecto rápido. Si los paquetes subsiguientes en esta conexión pasan a través de *ASA 1*, los paquetes coinciden con la entrada en el trayecto rápido y se pasan a través. Si los paquetes subsiguientes van a *ASA 2*, donde no había un paquete SYN que atravesara la trayectoria de administración de la sesión, entonces no hay entrada en la trayectoria rápida para la conexión y los paquetes se descartan.

Si tiene configurado el ruteo asimétrico en los routers ascendentes y el tráfico alterna entre dos ASA, puede configurar la función de omisión de estado TCP para el tráfico específico. La función de omisión de estado TCP altera la manera en que se establecen las sesiones en la trayectoria rápida e inhabilita las verificaciones de trayectoria rápida. Esta función trata el tráfico TCP tanto como una conexión UDP: cuando un paquete no SYN que coincide con las redes especificadas ingresa al ASA y no hay entrada de trayectoria rápida, entonces el paquete pasa a través del trayecto de administración de sesión para establecer la conexión en el trayecto rápido. Una vez en la ruta rápida, el tráfico omite las verificaciones de la ruta rápida.

Esta imagen proporciona un ejemplo de ruteo asimétrico, donde el tráfico saliente pasa a través de un ASA diferente al tráfico entrante:



Nota: La función de omisión de estado TCP está desactivada de forma predeterminada en el Cisco ASA serie 5500. Además, la configuración de omisión de estado TCP puede causar un gran número de conexiones si no se implementa correctamente.

Información de soporte

Esta sección describe la información de soporte para la función de omisión de estado TCP.

- **Context Mode** âÂ Â La función TCP state bypass se soporta en los modos de contexto simple y múltiple.
- **Firewall Mode** âÂ Â La función TCP state bypass se soporta en los modos ruteados y transparentes.
- **Failover** âÂ Â La función de omisión de estado TCP soporta failover.

Estas funciones no se soportan cuando se utiliza la función de omisión de estado TCP:

- **La inspección de la aplicación** âÂ Â La inspección de la aplicación requiere que tanto el tráfico entrante como saliente pase a través del mismo ASA, por lo que la inspección de la aplicación no se soporta con la función de omisión del estado TCP.
- **Sesiones autenticadas de autenticación, autorización y contabilidad (AAA)**. Cuando un usuario se autentica con un ASA, se niega el tráfico que regresa a través del otro ASA porque el usuario no se autenticó con ese ASA.
- **Interceptación de TCP, límite máximo de conexión embrionaria, número de secuencia TCP aleatorizado** âÂ El ASA no realiza un seguimiento del estado de la conexión, por lo que estas funciones no se aplican.

- **Normalización TCP** âÂ Â El normalizador TCP está inhabilitado.
- **Función Security Services Module (SSM) y Security Services Card (SSC)** âÂ Â No puede utilizar la función de omisión de estado TCP con ninguna aplicación que se ejecute en un SSM o SSC, como IPS o Seguridad de contenido (CSC).

Nota: Debido a que la sesión de traducción se establece por separado para cada ASA, asegúrese de configurar la traducción de direcciones de red (NAT) estática en ambos ASA para el tráfico de omisión de estado TCP. Si utiliza NAT dinámica, la dirección elegida para la sesión en *ASA 1* será diferente de la dirección elegida para la sesión en *ASA 2*.

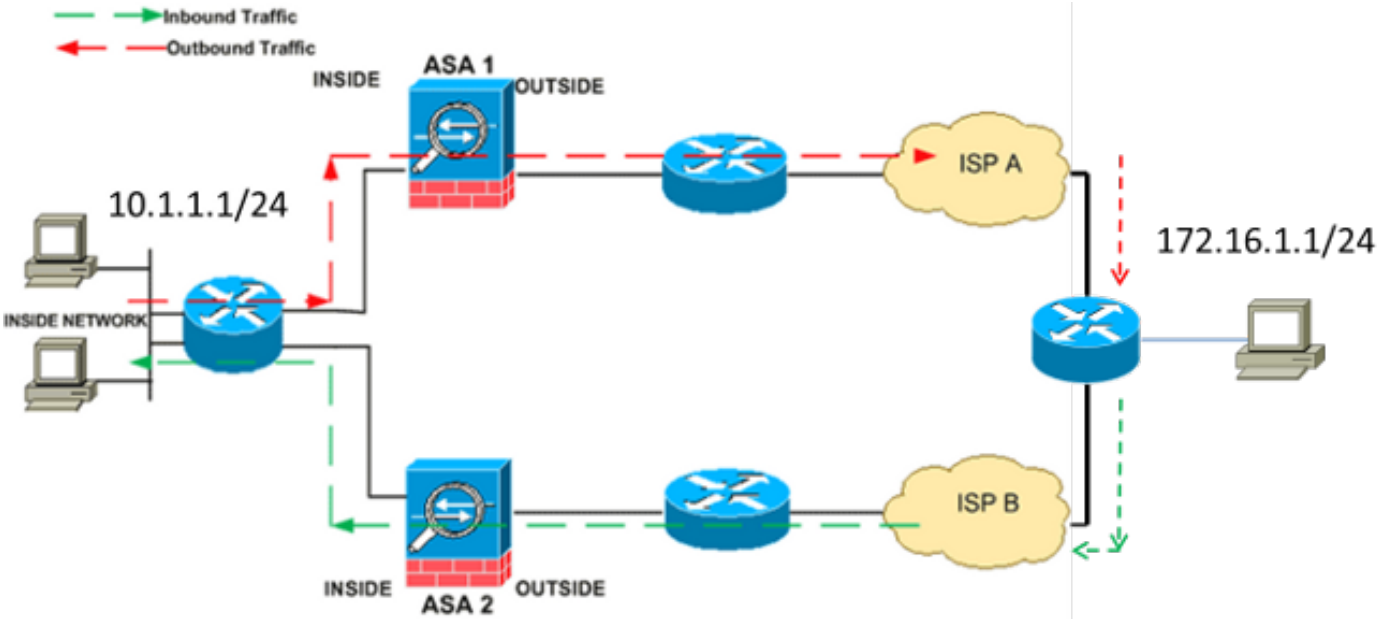
Configurar

Esta sección describe cómo configurar la función de omisión de estado TCP en ASA serie 5500 en dos escenarios diferentes.

Nota: Utilice la Command Lookup Tool (sólo clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Escenario 1

Esta es la topología que se utiliza para el primer escenario:



Nota: Debe aplicar la configuración que se describe en esta sección a ambos ASA.

Complete estos pasos para configurar la función de omisión de estado TCP:

1. Ingrese el comando class-map class_map_name para crear un *mapa de clase*. El mapa de clase se utiliza para identificar el tráfico para el que desea inhabilitar la inspección stateful

firewall.**Nota:** El mapa de clase que se utiliza en este ejemplo es **tcp_bypass**.

```
ASA(config)#class-map tcp_bypass
```

2. Ingrese el comando **match parámetro** para especificar el tráfico de interés dentro del mapa de clase. Cuando utilice el Marco de política modular, utilice el comando **match access-list** en el *modo de configuración class-map* para utilizar una lista de acceso para la identificación del tráfico al que desea aplicar acciones. Este es un ejemplo de esta configuración:

```
ASA(config)#class-map tcp_bypass
ASA(config-cmap)#match access-list tcp_bypass
```

Nota: tcp_bypass es el nombre de la lista de acceso que se utiliza en este ejemplo. Refiérase a la sección Identificación del Tráfico (Mapa de Clase de Capa 3/4) de la *Guía de Configuración de Cisco ASA 5500 Series mediante la CLI, 8.2* para obtener más información sobre cómo especificar el tráfico de interés.

3. Ingrese el comando **policy-map name** para agregar un policy map o editar un policy map (que ya está presente) que asigne las acciones que se deben realizar con respecto al tráfico de class map especificado. Cuando utilice el Marco de política modular, utilice el comando policy-map (sin la palabra clave *type*) en el modo *configuración global* para asignar acciones al tráfico que identificó con un mapa de clase de la capa 3/4 (el comando *class-map* o el comando *class-map type management*). En este ejemplo, el policy map es **tcp_bypass_policy**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```

4. Ingrese el comando **class** en el *modo de configuración de mapa de políticas* para asignar el mapa de clase creado (*tcp_bypass*) al mapa de políticas (*tcp_bypass_policy*) de modo que pueda asignar las acciones al tráfico de mapa de clase. En este ejemplo, el mapa de clase es **tcp_bypass**:

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

5. Ingrese el comando **set connection advanced-options tcp-state-bypass** en el *modo de configuración de clase* para habilitar la función de omisión de estado TCP. Este comando se introdujo en la versión 8.2(1). El modo *de configuración de clase* es accesible desde el *modo de configuración de mapa de políticas*, como se muestra en este ejemplo:

```
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. Ingrese el **service-policy policy policy policy map_name [global | interface *intf*]** en el *modo de configuración global* para activar un policy map globalmente en todas las interfaces o en una interfaz de destino. Para inhabilitar la política de servicio, utilice la forma **no** de este comando. Ingrese el comando **service-policy** para habilitar un conjunto de políticas en una interfaz. La palabra clave **global** aplica el policy map a todas las interfaces, y la palabra clave **interface** aplica el policy map a una sola interfaz. Sólo se permite una política global. Para invalidar la política global en una interfaz, puede aplicar una política de servicio a esa interfaz. Sólo puede aplicar un policy map a cada interfaz. Aquí tiene un ejemplo:

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

A continuación se muestra un ejemplo de configuración para la función de omisión de estado TCP en *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
```

A continuación se muestra un ejemplo de configuración para la función de omisión de estado TCP en *ASA2*:

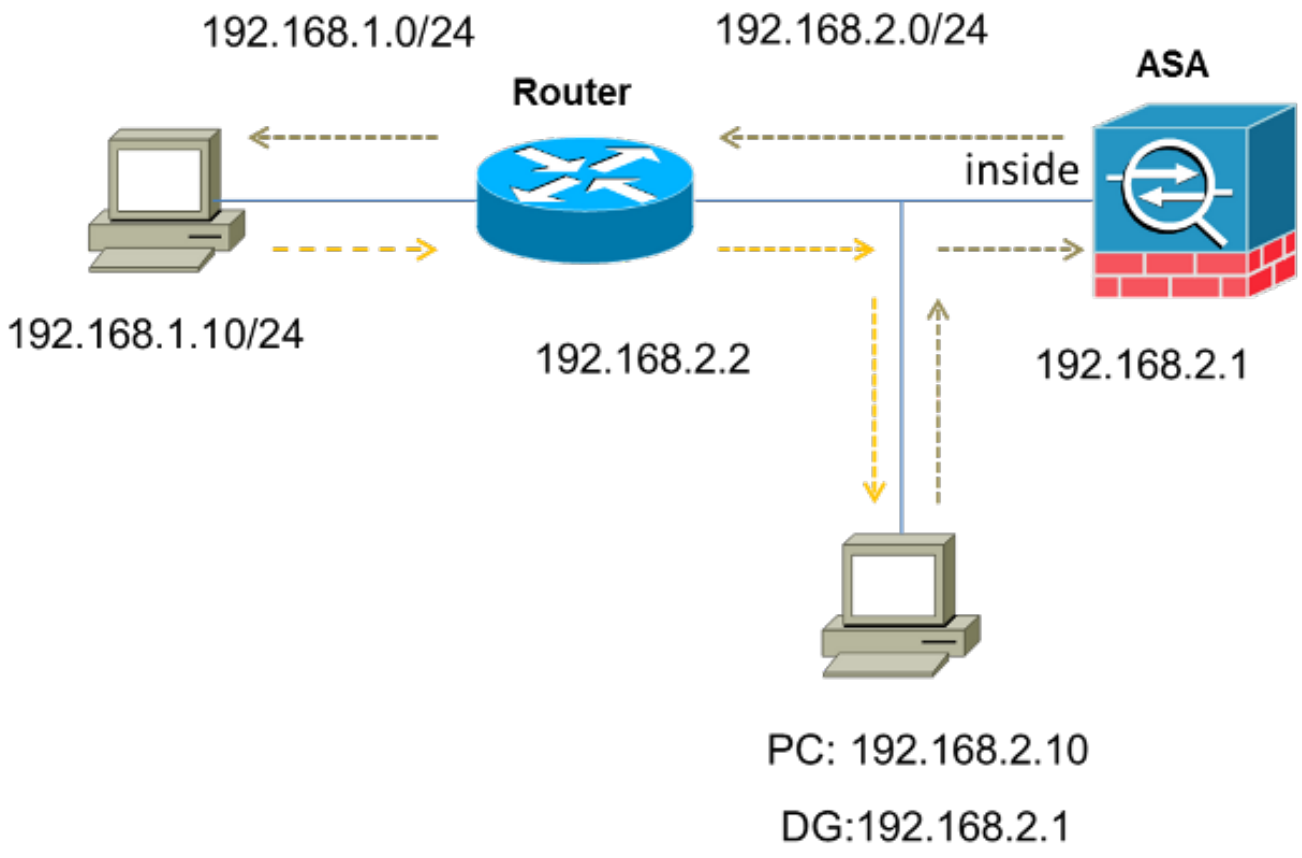
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

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
```

Escenario 2

Esta sección describe cómo configurar la función de omisión de estado TCP en el ASA para escenarios que utilizan ruteo asimétrico, donde el tráfico entra y sale del ASA de la misma interfaz (*giro u*).

Esta es la topología que se utiliza en este escenario:



Complete estos pasos para configurar la función de omisión de estado TCP:

1. Cree una *lista de acceso* para que coincida con el tráfico que debe omitir la inspección 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. Ingrese el comando class-map class_map_name para crear un *mapa de clase*. El mapa de clase se utiliza para identificar el tráfico para el que desea inhabilitar la inspección stateful firewall.**Nota:** El mapa de clase que se utiliza en este ejemplo es **tcp_bypass**.
```
ASA(config)#class-map tcp_bypass
```
3. Ingrese el comando match parámetro para especificar el tráfico de interés en el mapa de clase. Cuando utilice el Marco de política modular, utilice el comando **match access-list** en el modo de configuración *class-map* para utilizar una lista de acceso para la identificación del tráfico al que desea aplicar acciones. Este es un ejemplo de esta configuración:

```
ASA(config)#class-map tcp_bypass
ASA(config-cmap)#match access-list tcp_bypass
```
Nota: tcp_bypass es el nombre de la lista de acceso que se utiliza en este ejemplo. Refiérase a la sección Identificación del Tráfico (Mapa de Clase de Capa 3/4) de la *Guía de Configuración de Cisco ASA 5500 Series mediante la CLI, 8.2* para obtener más información sobre cómo especificar el tráfico de interés.
4. Ingrese el comando policy-map name para agregar un policy map o editar un policy map (que ya está presente) que establezca las acciones que se deben realizar con respecto al tráfico de class map especificado. Cuando utilice el Marco de política modular, utilice el comando policy-map (sin la palabra clave *type*) en el modo de *configuración global* para asignar las acciones al tráfico que identificó con un mapa de clase de la capa 3/4 (el comando *class-map* o *class-map type management*). En este ejemplo, el policy map es **tcp_bypass_policy**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```
5. Ingrese el comando class en el modo de configuración *policy-map* para asignar el mapa de clase creado (*tcp_bypass*) al mapa de políticas (*tcp_bypass_policy*) de modo que pueda asignar acciones al tráfico de mapa de clase. En este ejemplo, el mapa de clase es **tcp_bypass**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
```
6. Ingrese el comando set connection advanced-options tcp-state-bypass en el *modo de configuración de clase* para habilitar la función de omisión de estado TCP. Este comando se introdujo en la versión 8.2(1). Se puede acceder al modo de *configuración de clase* desde el *modo de configuración de policy-map*, como se muestra en este ejemplo:

```
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. Ingrese el service-policy policy policy policy map_name [global | interface *intf*] en el modo *global configuration* para activar un policy map globalmente en todas las interfaces o en una interfaz de destino. Para inhabilitar la política de servicio, utilice la forma **no** de este comando. Ingrese el comando **service-policy** para habilitar un conjunto de políticas en una interfaz. La palabra clave **global** aplica el policy map a todas las interfaces, y la palabra clave **interface** aplica la política a una sola interfaz. Sólo se permite una política global. Para invalidar la política global en una interfaz, puede aplicar una política de servicio a esa interfaz. Sólo puede aplicar un policy map a cada interfaz. Aquí tiene un ejemplo:

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

8. Permitir el mismo nivel de seguridad para el tráfico en ASA:

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

A continuación se muestra un ejemplo de configuración para la función de omisión de estado TCP en el 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
```

Verificación

Escriba el **show conn** para ver el número de conexiones TCP y UDP activas y la información sobre las conexiones de varios tipos. Para mostrar el estado de conexión para el tipo de conexión designado, introduzca el **show conn** en el modo *EXEC privilegiado*.

> **Nota:** Este comando soporta las direcciones IPv4 y IPv6. El resultado que se muestra para las conexiones que utilizan la función de omisión de estado TCP incluye el indicador **b**.

A continuación se presenta un ejemplo de salida:

```
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
```

Troubleshoot

No hay información específica de troubleshooting para esta función. Consulte estos documentos para obtener información general sobre la resolución de problemas de conectividad:

- Ejemplo de Configuración de Capturas de Paquetes ASA con CLI y ASDM
- ASA 8.2: Flujo de paquetes a través del firewall Cisco ASA

  Nota: Las conexiones de omisión de estado TCP no se replican en la unidad standby en un par de failover.

Mensajes de error

El ASA muestra este mensaje de error incluso después de habilitar la función de omisión de estado TCP:

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

El ASA descarta los paquetes del protocolo de mensajes de control de Internet (ICMP) debido a las comprobaciones de seguridad que agrega la función de ICMP con estado. Estos son generalmente las respuestas de *eco* ICMP sin una *solicitud de eco* válida ya transmitida a través del ASA, o los mensajes de error ICMP que no están relacionados con ninguna sesión TCP, UDP o ICMP actualmente establecida en el ASA.

El ASA muestra este registro incluso si la función de omisión de estado TCP está habilitada porque la inhabilitación de esta funcionalidad (es decir, las verificaciones de las entradas *de retorno* ICMP para el tipo 3 en la tabla de conexión) no es posible. Sin embargo, la función de omisión de estado TCP funciona correctamente.

Ingrese este comando para evitar la aparición de estos mensajes:

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

Información Relacionada

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems