Configure la característica de puente del estado TCP en las 5500 Series ASA

Contenido

Introducción

Este documento describe cómo configurar la característica de puente del estado TCP, que permite que el saliente y el tráfico entrante atraviesen el Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 separado (ASA).

Prerrequisitos

Requisitos

Cisco ASA debe tener por lo menos la licencia baja instalada antes de que usted pueda proceder con la configuración que se describe en este documento.

Componentes Utilizados

La información en este documento se basa en las 5500 Series de Cisco ASA que funciona con la versión de software 9.x.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Antecedentes

Esta sección proporciona una descripción de la característica de puente del estado TCP y de la información de servicio técnico relacionada.

Descripción general de características de puente del estado TCP

Por abandono, todo el tráfico que pasa con el ASA se examina vía el algoritmo de seguridad adaptable y se permite a través o se cae basado en la política de seguridad. Para maximizar el funcionamiento del Firewall, el ASA marca el estado de cada paquete (por ejemplo, marca si es una nueva conexión o una conexión establecida) y le asigna a cualquier la trayectoria de la administración de la sesión (una nueva conexión sincroniza el paquete (SYN)), el trayecto rápido (una conexión establecida), o la trayectoria del avión del control (examen avanzado).

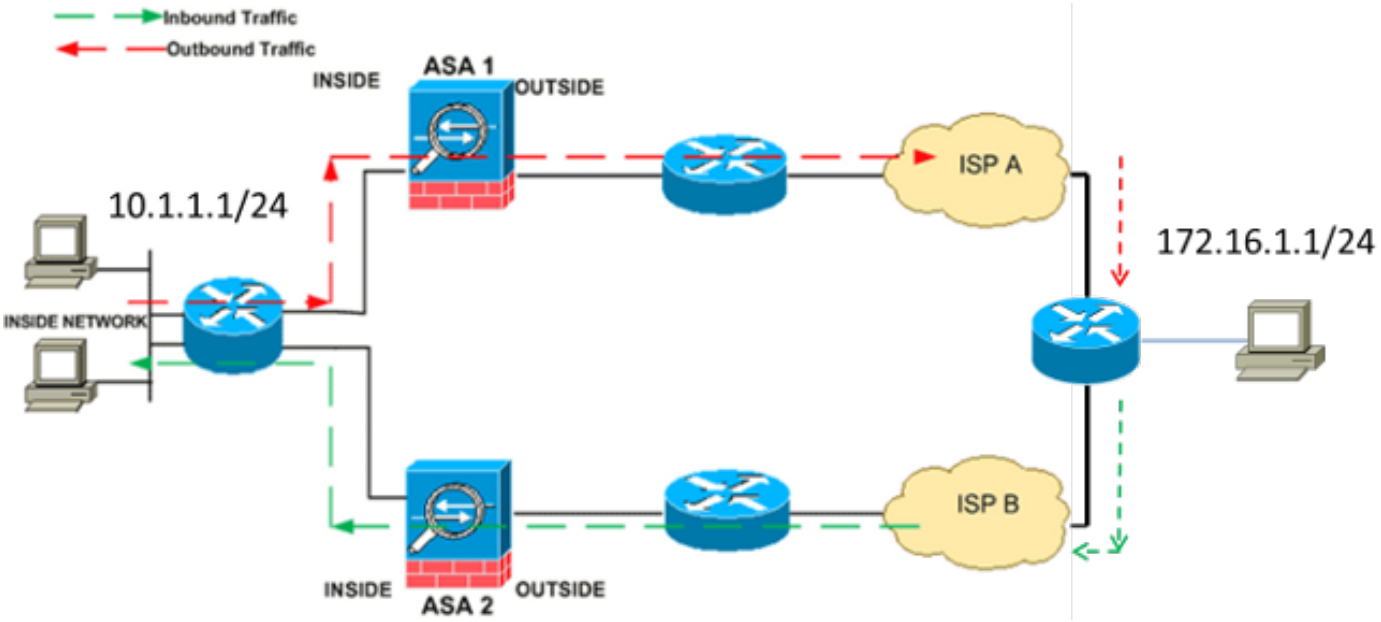
Los paquetes TCP que hacen juego las conexiones actuales en el trayecto rápido pueden pasar con el ASA sin una reinspección de cada aspecto de la política de seguridad. Esta característica maximiza el funcionamiento. Sin embargo, el método que se utiliza para establecer la sesión en el trayecto rápido (que utiliza el paquete SYN) y los controles que ocurren en el trayecto rápido (tal como el número de secuencia TCP) puede colocarse de la manera de soluciones asimétricas de la encaminamiento; los flujos salientes y entrantes de una conexión deben pasar con el mismo ASA.

Por ejemplo, una nueva conexión va a *ASA 1.* El paquete SYN pasa a través de la trayectoria de la administración de la sesión, y una entrada para la conexión se agrega a la tabla del trayecto rápido. Si los paquetes subsiguientes en esta conexión pasan con *ASA 1*, los paquetes hacen juego 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 pasó a través de la trayectoria de la administración de la sesión, después no hay entrada en el trayecto rápido para la conexión, y se caen los paquetes.

Si usted tiene Asymmetric Routing configurado en los routeres ascendentes, y el tráfico alterna entre dos ASA, después usted puede configurar la característica de puente del estado TCP para el tráfico específico. La característica de puente del estado TCP altera la manera que las sesiones están establecidas en el trayecto rápido y inhabilita los controles del trayecto rápido. Esta característica trata tráfico TCP mucho mientras que trata una conexión UDP: cuando un paquete NON-SYN que corresponde con las redes específicadas ingresa el ASA, y allí no es ninguna entrada del trayecto rápido, después el paquete pasa a través de la trayectoria de la administración de la sesión para establecer la conexión en el trayecto rápido. Una vez en el

trayecto rápido, el tráfico desvía los controles del trayecto rápido.

Esta imagen proporciona un ejemplo del Asymmetric Routing, adonde el tráfico saliente pasa con un diverso ASA que el tráfico entrante:



> Nota: La característica de puente del estado TCP se inhabilita por abandono en las 5500 Series de Cisco ASA. Además, la configuración de puente del estado TCP puede causar un número alto de conexiones si no se implementa correctamente.

Información de servicio técnico

Esta sección describe la información de servicio técnico para la característica de puente del estado TCP.

- El del Â del âÂ del **modo del contexto la** característica de puente del estado TCP se soporta en solo y los modos de contexto múltiple.
- El del Â del âÂ del **modo firewall la** característica de puente del estado TCP se soporta en ruteado y los modos transparentes.
- del Â del âÂ de la **Conmutación por falla la** Conmutación por falla de los soportes de característica de puente del estado TCP.

Estas características no se soportan cuando usted utiliza la característica de puente del estado TCP:

- La Inspección de la aplicación del del Â del âÂ de la **Inspección de la aplicación** requiere que ambos que el tráfico entrante y saliente pasa con el mismo ASA, así que la Inspección de la aplicación no se soporta con la característica de puente del estado TCP.
- **El Authentication, Authorization, and Accounting (AAA) autenticó el** del Â del âÂ de las **sesiones** cuando un usuario autentica con un ASA, el tráfico que las devoluciones vía el otro ASA están negadas porque el usuario no autenticó con ese ASA.

- **La Intercepción de tráfico de TCP, límite máximo de la conexión embrionaria,** del Â del âÂ de la **distribución aleatoria del número de secuencia TCP El** ASA no hace pista del estado de la conexión, así que estas características no son aplicadas.

- Se inhabilita el del Â del âÂ de la **normalización TCP el** normalizador TCP.

- **El módulo de Servicios de seguridad (SS) y** del Â del âÂ de las **funciones del indicador luminoso LED amarillo de la placa muestra gravedad menor de los Servicios de seguridad (SSC)** usted no puede utilizar la característica de puente del estado TCP con ninguna aplicaciones que se ejecuten en un SS o SSC, tal como IPS o Seguridad contenta (CSC).

  Nota: Porque establecen a la sesión de traducción por separado para cada ASA, asegúrese de que usted configure la traducción de dirección de red estática (NAT) en ambos ASA para el tráfico de puente del estado TCP. Si usted utiliza el NAT dinámico, el direccionamiento que se elige para la sesión sobre *ASA 1* diferenciará del direccionamiento que se elige para la sesión sobre *ASA 2.*

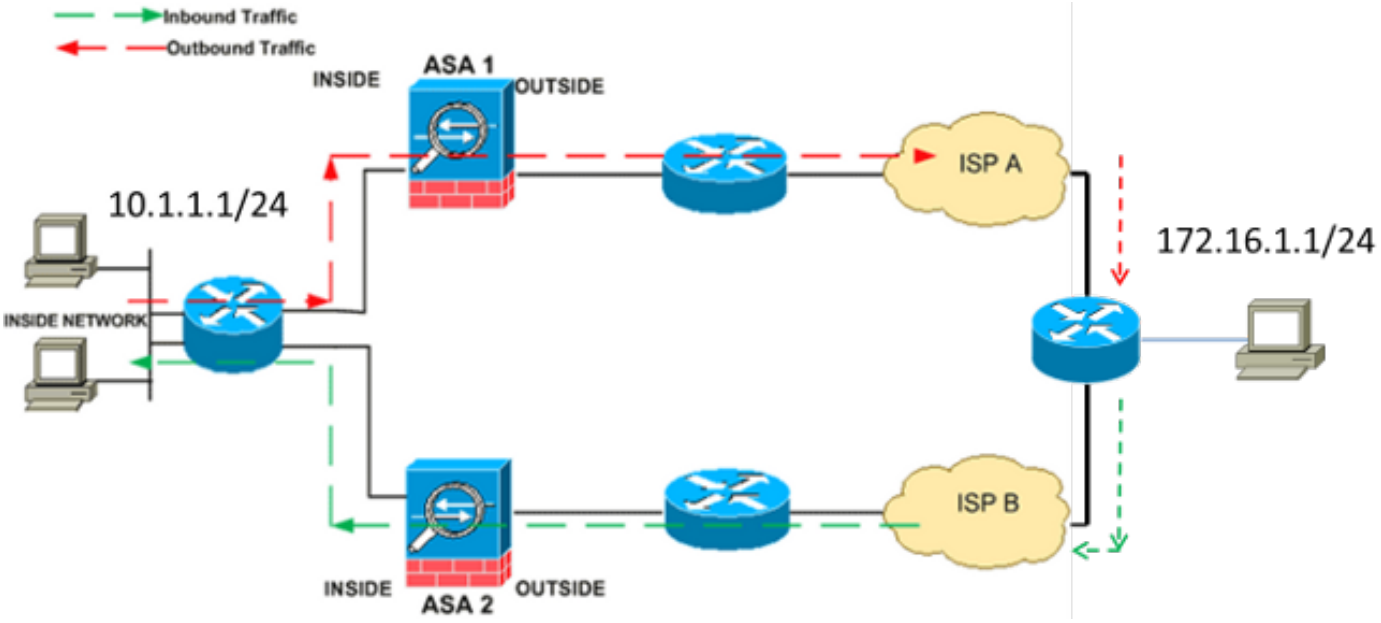
Configurar

Esta sección describe cómo configurar la característica de puente del estado TCP en las 5500 Series ASA en dos diversos escenarios.

Nota: Utilice la herramienta de búsqueda de comandos (clientes registrados solamente) para obtener más información sobre los comandos que se utilizan en esta sección.

Escenario 1

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



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

Complete estos pasos para configurar la característica de puente del estado TCP:

1. Ingrese el comando del class_map_name del clase-mapa para crear una *correspondencia de la clase*. La correspondencia de la clase se utiliza para identificar el tráfico para el cual usted quiere inhabilitar el examen del escudo de protección con estado.Nota: La correspondencia de la clase que se utiliza en este ejemplo es **tcp_bypass**.`ASA(config)#`**`class-map tcp_bypass`**
2. Ingrese el comando parameter del emparejamiento para especificar el tráfico del interés dentro de la correspondencia de la clase. Cuando usted utiliza el Marco de políticas modular, utilice el **comando access-list de la coincidencia** en el modo del *configuración class-map* para utilizar una lista de acceso para la identificación del tráfico al cual usted quiere aplicar las acciones. Aquí está un ejemplo de esta configuración:

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

   Nota: **Los tcp_bypass** son el nombre de la lista de acceso que se utiliza en este ejemplo. Refiera a la sección de identificación del tráfico (mapa de la clase de la capa 3/4) de la *guía de configuración de las 5500 Series de Cisco ASA que usa el CLI, 8.2* para más información sobre cómo especificar el tráfico del interés.
3. Ingrese el comando name del directiva-mapa para agregar una correspondencia de políticas o editar una correspondencia de políticas (que esté ya presente) que asigna las acciones para ser respetos admitidos al tráfico de la correspondencia de la clase especificada. Cuando usted utiliza el Marco de políticas modular, utilice el **comando policy-map** (sin la palabra clave del *tipo*) en el *modo de configuración global* para asignar las acciones al tráfico que usted identificó con una correspondencia de la clase de la capa 3/4 (el **comando management del tipo del clase-mapa** o del clase-**mapa**). En este ejemplo, la correspondencia de políticas es **tcp_bypass_policy**:

   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```
4. Ingrese el comando class en el modo de la *configuración de correspondencia de políticas* para asignar la correspondencia creada de la clase (*tcp_bypass*) a la correspondencia de políticas (*tcp_bypass_policy*) de modo que usted pueda asignar las acciones al tráfico de la correspondencia de la clase. En este ejemplo, la correspondencia de la clase es **tcp_bypass**:

   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```
5. Ingrese el comando de TCP-estado-puente de las avanzado-opciones de la conexión del conjunto en el *modo de configuración de clase* para habilitar la característica de puente del estado TCP. Este comando fue introducido en la versión 8.2(1). *El modo de configuración de clase* es accesible del modo de la *configuración de correspondencia de políticas*, tal y como se muestra en de 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 policymap_name de la servicio-directiva [global | interconecte el comando del *intf*] en el *modo de configuración global* para activar una correspondencia de políticas global en todas las interfaces o en una interfaz apuntada. Para inhabilitar la política de servicio, no utilice la **ninguna** forma de este comando. Ingrese el **comando service-policy** para habilitar un conjunto de las directivas en una interfaz. **La palabra clave global** aplica la correspondencia de políticas a todas las interfaces, y la palabra clave de la **interfaz** aplica la correspondencia de políticas a solamente una interfaz. Se permite solamente una política

global. Para reemplazar la política global en una interfaz, usted puede aplicar una política de servicio a esa interfaz. Usted puede aplicar solamente una correspondencia de políticas a cada interfaz. Aquí tiene un ejemplo:

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

Aquí está un ejemplo de configuración para la característica de puente del 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
```

Aquí está un ejemplo de configuración para la característica de puente del estado TCP en *ASA2*:

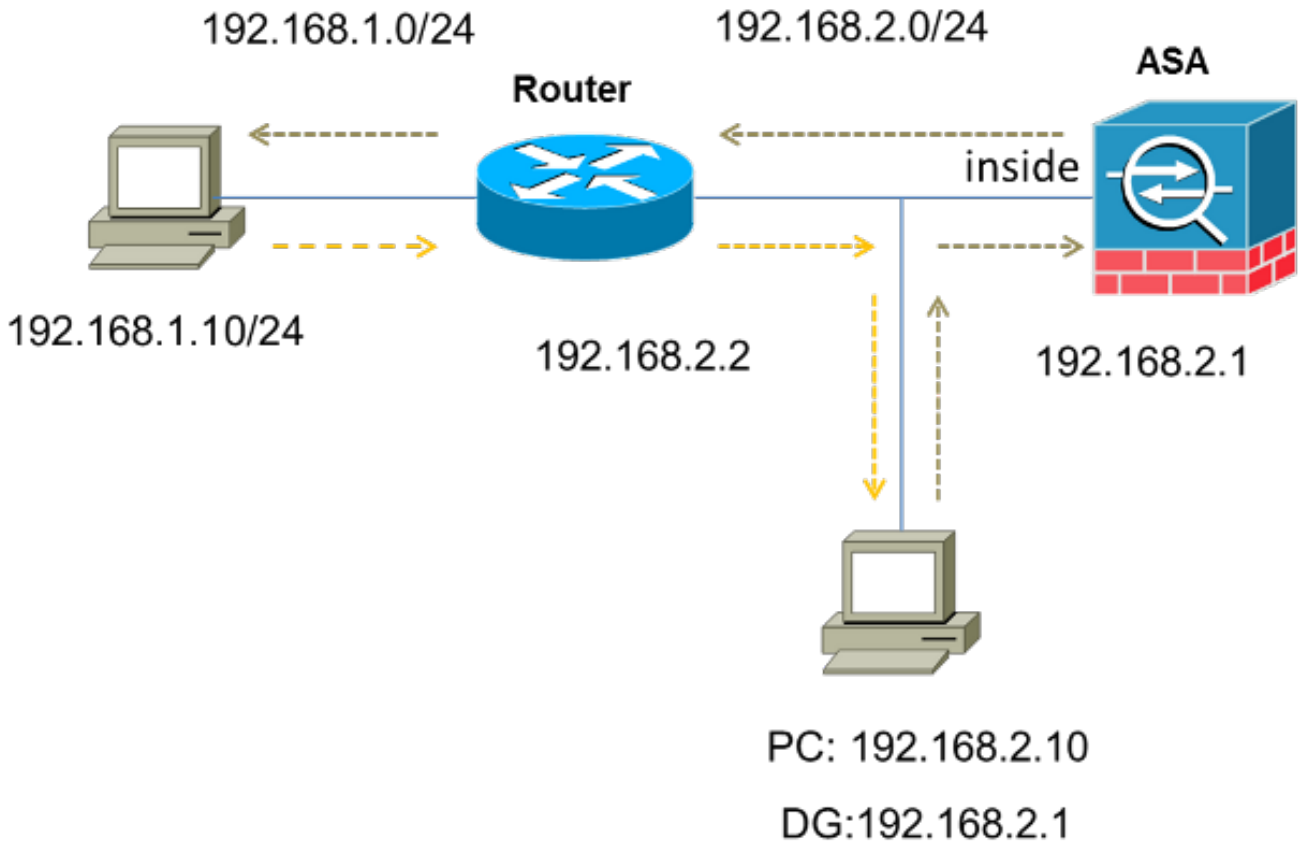
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

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 característica de puente del estado TCP en el ASA para los escenarios que utilizan el Asymmetric Routing, donde el tráfico ingresa y sale del ASA de la misma interfaz (u-*torneado*).

Aquí está la topología que se utiliza en este escenario:



Complete estos pasos para configurar la característica de puente del estado TCP:

1. Cree una *lista de acceso* para hacer juego el tráfico que debe desviar el examen 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 del class_map_name del clase-mapa para crear una *correspondencia de la clase*. La correspondencia de la clase se utiliza para identificar el tráfico para el cual usted quiere inhabilitar el examen del escudo de protección con estado.Nota: La correspondencia de la clase que se utiliza en este ejemplo es **tcp_bypass**.
   ```
   ASA(config)#class-map tcp_bypass
   ```
3. Ingrese el comando parameter del emparejamiento para especificar el tráfico del interés en la correspondencia de la clase. Cuando usted utiliza el Marco de políticas modular, utilice el **comando access-list de la coincidencia** en el modo del *configuración class-map* para utilizar una lista de acceso para la identificación del tráfico al cual usted quiere aplicar las acciones. Aquí está un ejemplo de esta configuración:
   ```
   ASA(config)#class-map tcp_bypass
   ```
   ```
   ASA(config-cmap)#match access-list tcp_bypass
   ```
   Nota: **Los tcp_bypass** son el nombre de la lista de acceso que se utiliza en este ejemplo. Refiera a identificar la sección del tráfico (mapa de la clase de la capa 3/4) de la *guía de configuración de las 5500 Series de Cisco ASA que usa el CLI, 8.2* para más información sobre cómo especificar el tráfico del interés.
4. Ingrese el comando name del directiva-mapa para agregar una correspondencia de políticas o editar una correspondencia de políticas (que esté ya presente) esa fija las acciones para ser respetos admitidos al tráfico de la correspondencia de la clase especificada. Cuando usted utiliza el Marco de políticas modular, utilice el **comando policy-map** (sin la palabra clave del *tipo*) en el *modo de configuración global* para asignar las acciones al tráfico que usted identificó con una correspondencia de la clase de la capa 3/4 (el **comando management del tipo del clase-mapa** o del clase-**mapa**). En este ejemplo, la correspondencia de políticas es **tcp_bypass_policy**:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```
5. Ingrese el comando class en el modo de la *configuración de correspondencia de políticas* para asignar la correspondencia creada de la clase (*tcp_bypass*) a la correspondencia de políticas (*tcp_bypass_policy*) de modo que usted pueda asignar las acciones al tráfico de la correspondencia de la clase. En este ejemplo, la correspondencia de la clase es **tcp_bypass**:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```
6. Ingrese el comando de TCP-estado-puente de las avanzado-opciones de la conexión del conjunto en el *modo de configuración de clase* para habilitar la característica de puente del estado TCP. Este comando fue introducido en la versión 8.2(1). *El modo de configuración de clase* es accesible del modo de la *configuración de correspondencia de políticas*, tal y como se muestra en de 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 policymap_name de la servicio-directiva [global | interconecte el comando del *intf*] en el *modo de configuración global* para activar una correspondencia de políticas global en todas las interfaces o en una interfaz apuntada. Para inhabilitar la política de servicio, no utilice la **ninguna** forma de este comando. Ingrese el **comando service-policy** para habilitar un conjunto de las directivas en una interfaz. **La palabra clave global** aplica la correspondencia de políticas a todas las interfaces, y la palabra clave de la **interfaz** aplica la directiva a solamente una interfaz. Se permite solamente una política global. Para reemplazar la política global en una interfaz, usted puede aplicar una política de servicio a esa interfaz. Usted puede aplicar solamente una correspondencia de políticas a cada

interfaz. Aquí tiene un ejemplo:

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

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

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

Aquí está un ejemplo de configuración para la característica de puente del 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

Ingrese el comando show conn para ver el número de TCP activo y de conexiones UDP y la información sobre las conexiones de los diversos tipos. Para visualizar al estado de la conexión para el Tipo de conexión señalado, ingrese el comando show conn en el *modo EXEC privilegiado*.

> Nota: Este comando soporta las direcciones IPv4 y IPv6. La salida que se visualiza para las conexiones que utilizan la característica de puente del 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
```

Troubleshooting

No hay información de Troubleshooting específica para esta característica. Refiera a estos documentos para la información de Troubleshooting general de la Conectividad:

- Capturas de paquetes ASA con el CLI y el ejemplo de la Configuración de ASDM
- ASA 8.2: El paquete atraviesa el Firewall de Cisco ASA

  Nota: Las conexiones de puente del estado TCP no se replican a la unidad en espera en un par de fallas.

Mensajes de error

El ASA visualiza este mensaje de error incluso después se habilita la característica de puente del estado TCP:

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

Los paquetes del Internet Control Message Protocol (ICMP) son caídos por el ASA debido a las revisiones de seguridad que son agregadas por la característica stateful ICMP. Éstos son generalmente respuestas de eco ICMP sin un *pedido de eco* válido pasajero ya a través del ASA, o los mensajes de error ICMP que no se relacionan con ninguna sesión TCP, UDP, o ICMP establecida actualmente en el ASA.

El ASA visualiza este registro incluso si se habilita la característica de puente del estado TCP porque la incapacidad de estas funciones (es decir, marca de las entradas de la *vuelta* ICMP para el tipo 3 en la tabla de conexiones) no es posible. Sin embargo, la característica de puente del estado TCP trabaja correctamente.

Ingrese este comando para prevenir el aspecto 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