Ejemplo de configuración de la característica de puente del estado ASA 8.2.X TCP

Contenido

Introducción

Este documento describe cómo configurar la función de desvío del estado TCP. Esta característica permite saliente y entrante atraviesa el Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 separado.

prerrequisitos

Requisitos de Licencia

El Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 debe tener por lo menos la licencia baja.

Componentes Utilizados

La información en este documento se basa en el dispositivo de seguridad adaptante de Cisco (ASA) con la versión 8.2(1) y posterior.

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

Refiera a los convenios de los consejos técnicos de Cisco para la información sobre las convenciones sobre documentos.

El TCP estado puente

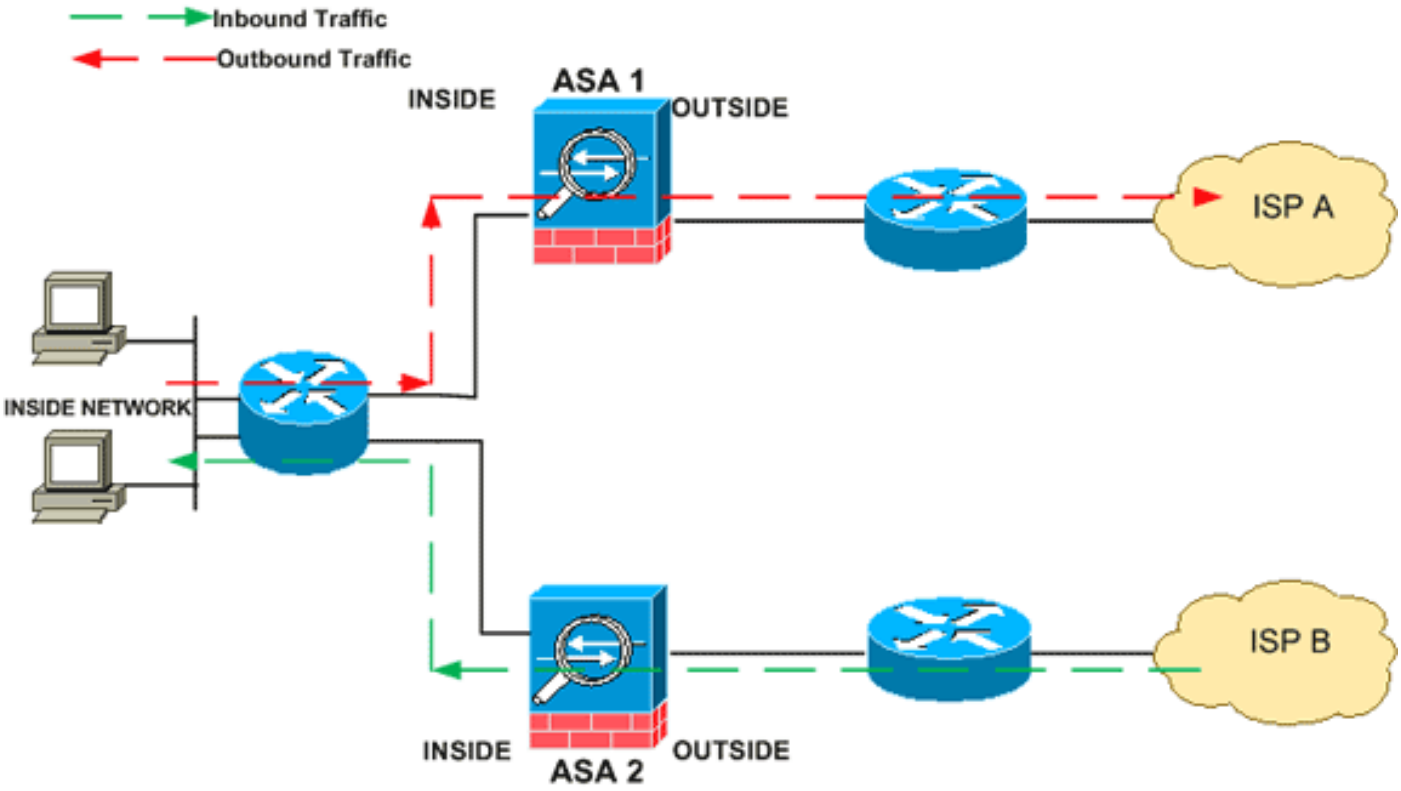
Por abandono, todo el tráfico que pasa a través del dispositivo de seguridad adaptante de Cisco (ASA) se examina usando el algoritmo de seguridad adaptable y se permite a través o se cae basado en la política de seguridad. Para maximizar el funcionamiento del Firewall, el ASA marca el estado de cada paquete (por ejemplo, está éste una nueva conexión o una conexión establecida?) y lo asigna a la trayectoria de la administración de la sesión (un paquete SYN de la nueva conexión), al trayecto rápido (una conexión establecida), o a la trayectoria del avión del control (examen avanzado).

Los paquetes TCP que hacen juego las conexiones existentes en el trayecto rápido pueden pasar a través del dispositivo de seguridad adaptante sin la reinspección de cada aspecto de la política de seguridad. Esta característica maximiza el funcionamiento. Sin embargo, el método usado para establecer la sesión en el trayecto rápido (que utiliza el paquete SYN) y los controles que ocurren en el trayecto rápido (tal como número de secuencia TCP) puede colocarse de la manera de soluciones asimétricas de la encaminamiento: el flujo saliente y entrante de una conexión debe 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 de esta conexión pasan con *ASA 1*, los paquetes harán 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 puente del estado TCP para el tráfico específico. Puente del estado TCP altera la manera que las sesiones se establecen 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 no hay una entrada del trayecto rápido, después el paquete pasa a través de la trayectoria de la administración de la sesión 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 el Dispositivos de seguridad adaptable Cisco ASA de la serie 5500.

Información de servicio técnico

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

- Modo del contexto — Soportado en solo y el modo de contexto múltiple.
- Modo firewall — Soportado en ruteado y el modo transparente.
- Conmutación por falla — Soporta la Conmutación por falla.

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

- Inspección de la aplicación — La Inspección de la aplicación requiere ambo el tráfico entrante y saliente a pasar con el mismo ASA, así que la Inspección de la aplicación no se soporta con puente del estado TCP.
- El AAA autenticó las sesiones — Cuando un usuario autentica con un ASA, el tráfico que vuelve vía el otro ASA será negado porque el usuario no autenticó con ese ASA.
- Intercepción de tráfico de TCP, límite máximo de la conexión embrionaria, distribución aleatoria del número de secuencia TCP — El ASA no no pierde de vista el estado de la conexión, así que estas características no son aplicadas.
- Normalización TCP — Se inhabilita el normalizador TCP.
- Funciones SS y de SSC — Usted no puede utilizar puente del estado TCP y ninguna aplicación que se ejecutan en un SS o SSC, tal como IPS o CSC.

Guías de consulta NAT: Porque establecen a la sesión de traducción por separado para cada ASA, esté seguro de configurar el NAT estático en ambos ASA para el tráfico de puente del estado TCP; si usted utiliza el NAT dinámico, el direccionamiento elegido para la sesión sobre *ASA 1* diferenciará del direccionamiento elegido para la sesión sobre *ASA 2.*

Configurar

Esta sección describe cómo configurar la característica de puente del estado TCP en el dispositivo de seguridad adaptante de las 5500 Series de Cisco ASA (ASA).

Configuración de la característica de puente del estado TCP

Complete estos pasos para configurar la característica de puente del estado TCP en el dispositivo de seguridad adaptante de las 5500 Series de Cisco ASA:

1. Utilice 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. La correspondencia de la clase usada en este ejemplo es *tcp_bypass*.`ASA(config)#class-map tcp_bypass`
2. Utilice el comando parameter de la coincidencia para especificar el tráfico interesante en la correspondencia de la clase. Al usar 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 identificar el 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` *los tcp_bypass* son el nombre de la lista de acceso usada en este ejemplo. Refiera a identificar el tráfico (mapa de la clase de la capa 3/4) para más información sobre especificar el tráfico interesante.
3. Utilice 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 tomar con el tráfico de la correspondencia de la clase especificado ya. Al usar 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 para traficar 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. Utilice el comando class en el modo de la configuración de correspondencia de políticas para asignar la correspondencia de la clase (*tcp_bypass*) creada ya a la correspondencia de políticas (*tcp_bypass_policy*) donde usted puede 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. Utilice 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. Utilice 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. Utilice el **comando service-policy** de habilitar un conjunto de las directivas en un interface.global aplica la correspondencia de políticas a todas las interfaces, y la **interfaz** aplica la directiva a una interfaz. Se permite solamente una política global. Usted puede reemplazar la política global en una interfaz aplicando una

política de servicio a esa interfaz. Usted puede aplicar solamente una correspondencia de políticas a cada interfaz.`ASA(config-pmap-c)#service-policy tcp_bypass_policy outside`

Aquí está una configuración de muestra para puente del estado 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
```

Verificación

El comando show conn visualiza el número de TCP activo y de conexiones UDP y proporciona la información sobre las conexiones de los diversos tipos. Para visualizar al estado de la conexión para el Tipo de conexión señalado, utilice el comando show conn en el modo EXEC privilegiado. Este comando soporta las direcciones IPv4 y IPv6. La visualización de la salida para las conexiones que utilizan **puente del estado TCP** incluye el indicador **B.**

Troubleshooting

Mensaje de error

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

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

Los paquetes icmp fueron caídos por el dispositivo de seguridad debido a las revisiones de seguridad agregadas por la característica stateful ICMP que son generalmente respuestas de eco ICMP sin un pedido de eco válido pasajero ya a través del dispositivo de seguridad o mensajes de error ICMP no relacionados con cualquier sesión TCP, UDP, o ICMP establecida ya en el dispositivo de seguridad.

El ASA visualiza este registro incluso si se habilita puente del estado TCP porque inhabilitar estas funciones (es decir, marcando el ICMP vuelva las entradas para el tipo 3 en la tabla de conexiones) no es posible. Pero la característica de puente del estado TCP trabaja correctamente.

Utilice este comando para evitar que estos mensajes aparezcan:

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

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances

- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems