Ejemplo de Configuración de la Función ASA 8.2.X TCP State Bypass

Contenido

Introducción

Este documento describe cómo configurar la función de desvío del estado TCP. Esta función permite flujos entrantes y salientes a través de dispositivos de seguridad adaptable Cisco ASA serie 5500 independientes.

Prerequisites

Requisitos de Licencia

Los Cisco ASA 5500 Series Adaptive Security Appliances deben tener al menos la licencia básica.

Componentes Utilizados

La información de este documento se basa en Cisco Adaptive Security Appliance (ASA) con la versión 8.2(1) y posteriores.

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

Omisión de estado TCP

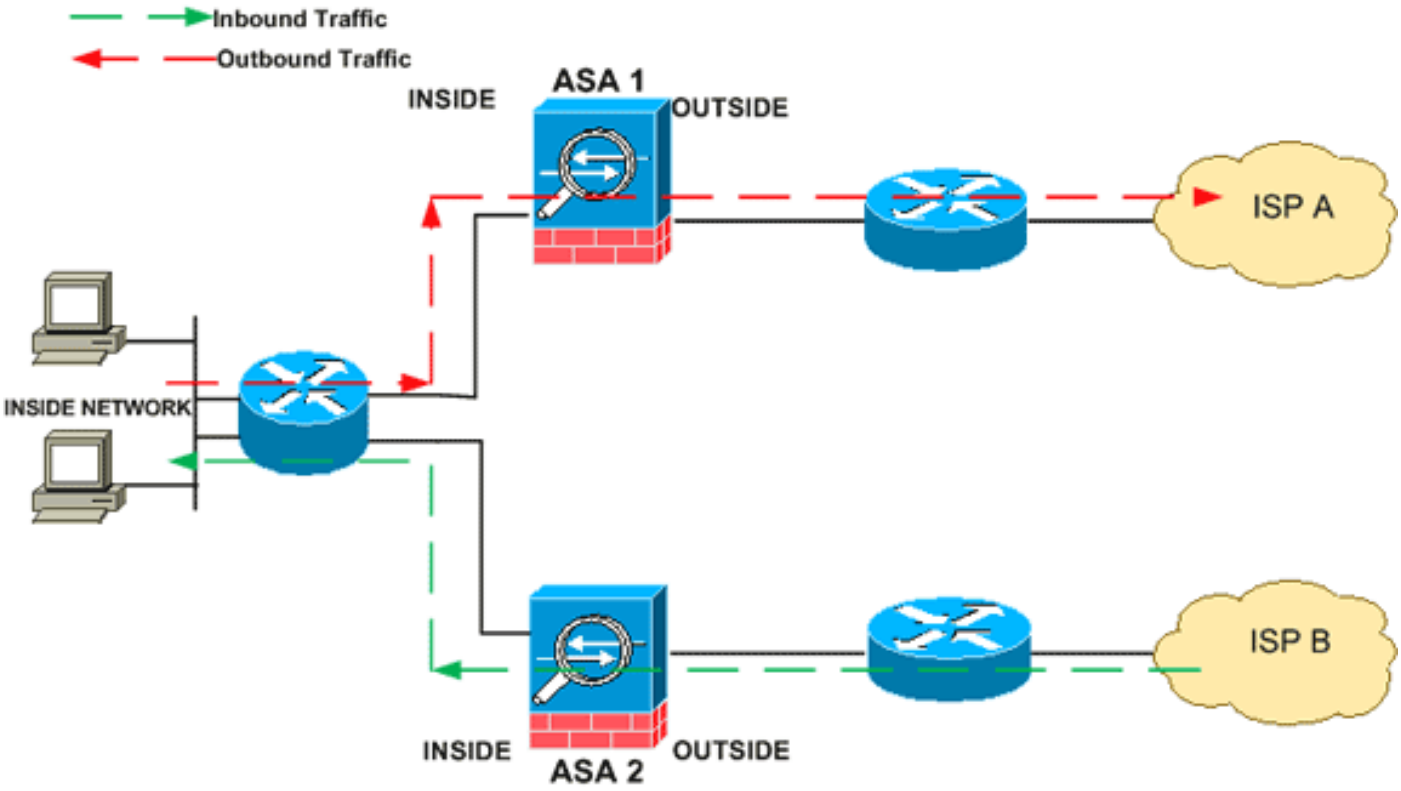
De forma predeterminada, todo el tráfico que pasa a través del dispositivo de seguridad adaptable (ASA) de Cisco se inspecciona mediante el algoritmo de seguridad adaptable y se permite pasar o descartar según la política de seguridad. Para maximizar el rendimiento del firewall, el ASA verifica el estado de cada paquete (por ejemplo, ¿se trata de una nueva conexión o de una conexión establecida?) y la asigna a la ruta de administración de la sesión (un nuevo paquete 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 existentes en el trayecto rápido pueden pasar a través del dispositivo de seguridad adaptable sin volver a verificar todos los aspectos de la política de seguridad. Esta función maximiza el rendimiento. Sin embargo, el método utilizado para establecer la sesión en el trayecto rápido (que utiliza el paquete SYN) y las verificaciones que se producen en el trayecto rápido (como el número de secuencia TCP) pueden interponerse en el camino de las soluciones de ruteo asimétricas: tanto el flujo entrante como el saliente 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 de esta conexión pasan a través de *ASA 1*, los paquetes coincidirán con la entrada en el trayecto rápido y se transmitirán. 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 el desvío de estado TCP para tráfico específico. El estado de omisión de TCP altera la manera en que se establecen las sesiones en el trayecto rápido e inhabilita las verificaciones del trayecto rápido. 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 una 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 inhabilitada de forma predeterminada en los Cisco ASA 5500 Series Adaptive Security Appliances.

Información de soporte

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

- Modo de contexto: compatible en modo de contexto único y múltiple.
- Modo de firewall: compatible en modo ruteado y transparente.
- Conmutación por fallas: admite conmutación por fallas.

Estas funciones no se soportan cuando se utiliza el desvío de estado TCP:

- Inspección de aplicaciones: la inspección de aplicaciones requiere que tanto el tráfico entrante como el saliente pasen a través del mismo ASA, por lo que la inspección de aplicaciones no se admite con la derivación de estado TCP.
- Sesiones autenticadas AAA: cuando un usuario se autentica con un ASA, el tráfico que regresa a través del otro ASA será denegado porque el usuario no se autenticó con ese ASA.
- TCP Intercept, límite máximo de conexión embrionaria, número de secuencia TCP aleatorizado: el ASA no realiza un seguimiento del estado de la conexión, por lo que estas funciones no se aplican.
- Normalización de TCP: el estándar TCP está desactivado.
- Funcionalidad SSM y SSC: no puede utilizar el desvío de estado TCP ni ninguna aplicación que se ejecute en un SSM o SSC, como IPS o CSC.

Pautas de NAT: Debido a que la sesión de traducción se establece por separado para cada ASA, asegúrese de configurar 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 desvío de estado TCP en el dispositivo de seguridad adaptable (ASA) Cisco ASA serie 5500.

Configuración de la Función de Omisión de Estado TCP

Complete estos pasos para configurar la función de omisión de estado TCP en el Cisco ASA 5500 Series Adaptive Security Appliance:

1. Utilice 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 de stateful firewall. El mapa de clase utilizado en este ejemplo es *tcp_bypass*.
   ```
   ASA(config)#class-map tcp_bypass
   ```

2. Utilice el comando match para especificar el tráfico interesante en el mapa de clase. Cuando utilice Modular Policy Framework, utilice el comando **match access-list** en el modo de configuración class-map para utilizar una lista de acceso para identificar el 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
   ```

   tcp_bypass es el nombre de la lista de acceso utilizada en este ejemplo. Consulte Identificación del Tráfico (Mapa de Clase de Capa 3/4) para obtener más información sobre cómo especificar el tráfico interesante.
3. Utilice el comando policy-map name para agregar un policy map o editar un policy map (que ya está presente) que establezca las acciones a realizar con el tráfico de class map especificado ya. Cuando utilice Modular Policy Framework, utilice el comando **policy-map** (sin la palabra clave type) en el modo de configuración global para asignar acciones al tráfico que identificó con un mapa de clase de 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
   ```

4. Utilice el comando class en el modo de configuración policy-map para asignar el mapa de clase (*tcp_bypass*) ya creado al mapa de política (*tcp_bypass_policy*) donde puede 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
   ```

5. Utilice 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
   ```

6. Utilice el service-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. Utilice el comando **service-policy** para habilitar un conjunto de políticas en una interfaz.**global** aplica el policy map a todas las interfaces, y **interface** aplica la política a una interfaz. Sólo se permite una política global. Puede invalidar la política global en una interfaz aplicando una política de servicio a esa interfaz. Sólo puede aplicar un policy map a cada interfaz.

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

A continuación se muestra una configuración de ejemplo para el desvío de 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 muestra el número de conexiones TCP y UDP activas y proporciona información sobre las conexiones de varios tipos. Para mostrar el estado de conexión para el tipo de conexión designado, utilice el comando show conn en el modo EXEC privilegiado. Este comando soporta las direcciones IPv4 y IPv6. La visualización de salida para las conexiones que utilizan **omisión de estado TCP** incluye el indicador **b**.

Troubleshoot

Mensaje de error

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 dispositivo de seguridad descartó los paquetes ICMP debido a las verificaciones de seguridad agregadas por la función de ICMP con estado que generalmente son respuestas de eco ICMP sin una solicitud de eco válida ya transmitida a través del dispositivo de seguridad o mensajes de error ICMP no relacionados con ninguna sesión TCP, UDP o ICMP ya establecida en el dispositivo de seguridad.

ASA muestra este registro incluso si se habilita el desvío de estado TCP porque no es posible desactivar esta funcionalidad (es decir, verificar las entradas de retorno ICMP para el tipo 3 en la tabla de conexión). Pero la función de omisión de estado TCP funciona correctamente.

Utilice este comando para evitar que aparezcan estos mensajes:

```
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