ASA 8.2: El paquete atraviesa un Firewall ASA

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Algoritmo del proceso del paquete de Cisco ASA](#)
[Explicación del NAT](#)
[Comandos show](#)
[Mensajes de Syslog](#)
[Información Relacionada](#)

Introducción

Este documento describe el paquete atraviesa un Firewall adaptante del dispositivo de seguridad de Cisco (ASA). Muestra el procedimiento de Cisco ASA para procesar los paquetes internos. También discute las diversas posibilidades por las que el paquete se podría perder y diversas situaciones en las que el paquete sigue adelante.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de las Cisco 5500 Series ASA.

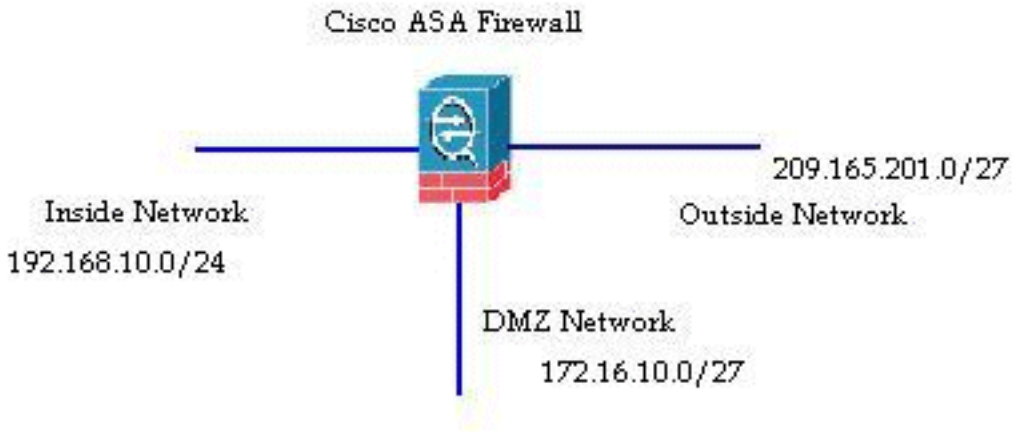
Componentes Utilizados

La información en este documento se basa en las 5500 Series ASA de Cisco ASA que funcionan con la versión de software 8.2.

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.

Antecedentes

La interfaz que recibe el paquete se llama la **interfaz de ingreso** y la interfaz a través de las cuales las salidas del paquete se llaman la **interfaz de egreso**. Cuando usted refiere al paquete atraviese cualquier dispositivo, la tarea se simplifica fácilmente si usted la mira en términos de estas dos interfaces. Aquí está un escenario de ejemplo:



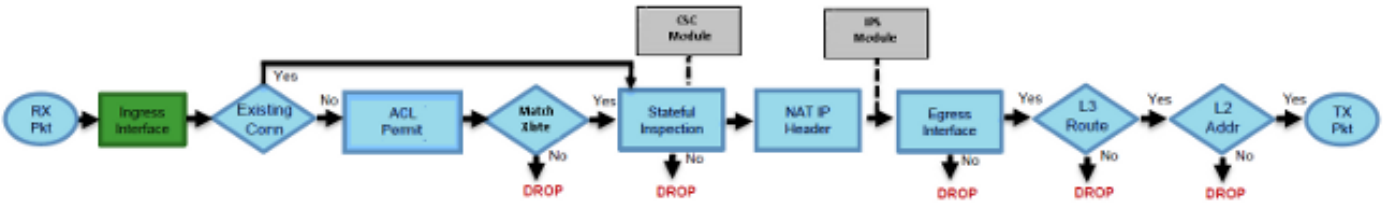
Cuando un usuario interior (192.168.10.5) intenta acceder a un servidor Web en la red de la zona desmilitarizada (DMZ) (172.16.10.5), el flujo de paquetes parece esto:

- Dirección de origen - 192.168.10.5
- Puerto de origen - 22966
- Dirección destino - 172.16.10.5
- Puerto destino - 8080
- Interfaz de ingreso - Dentro
- Interfaz de egreso - DMZ
- Protocolo usado - TCP (protocolo Protocolo de control de transmisión (TCP))

Después de que usted determine los detalles del flujo de paquetes según lo descrito aquí, es fácil aislar el problema a este específico Entrada de conexión.

Algoritmo del proceso del paquete de Cisco ASA

Aquí está un diagrama de cómo Cisco ASA procesa el paquete que recibe:



Aquí están los pasos individuales detalladamente:

1. El paquete se alcanza en la interfaz de ingreso.
2. Una vez que el paquete alcanza el búfer interno de la interfaz, una incrementa al contador

de entradas de la interfaz.
3. Cisco ASA primero mira sus detalles de la tabla de la conexión interna para verificar si esto es una conexión actual. Si el flujo de paquetes hace juego una conexión actual, después se desvía el control de la lista de control de acceso (ACL) y el paquete se mueve adelante.Si el flujo de paquetes no hace juego una conexión actual, después se verifica el estado TCP. Si es un paquete SYN o paquete UDP (protocolo UDP), después el contador de la conexión es incrementado por uno y el paquete se envía para un control ACL. Si no es un paquete SYN, se cae el paquete y se registra el evento.
4. El paquete se procesa según la interfaz ACL. Se verifica en el orden consecutivo de las entradas ACL y si hace juego las entradas ACL unas de los, se mueve adelante. Si no, se cae el paquete y se registra la información. La cuenta del golpe ACL es incrementada por una cuando el paquete hace juego la entrada ACL.
5. El paquete se verifica para las Reglas de traducción. Si un paquete pasa a través de este control, después a Entrada de conexión se crea para este flujo y el paquete se mueve adelante. Si no, se cae el paquete y se registra la información.
6. El paquete se sujeta a un control del examen. Este examen verifica independientemente de si este flujo de paquetes específico esté de acuerdo con el protocolo. Cisco ASA tiene un motor incorporado del examen que examine cada conexión según su conjunto predefinido de las funciones del nivel de la aplicación. Si pasó el examen, se mueve adelante. Si no, se cae el paquete y se registra la información.Los controles de seguridad complementaria serán implementados si un módulo contento de la Seguridad (CSC) está implicado.
7. La información de encabezado IP se traduce según la regla de la traducción de dirección de puerto de la traducción de la dirección de red (NAT/PAT) y las sumas de comprobación se ponen al día por consiguiente. El paquete se remite al módulo de Servicios de seguridad avanzado del examen y de la prevención (AIP-SSM) para las revisiones de seguridad relacionadas IPS cuando el módulo AIP está implicado.
8. El paquete se remite a la interfaz de egreso basada en las Reglas de traducción. Si no se especifica ninguna interfaz de egreso en la regla de traducción, después la interfaz de destino se decide sobre la base de las operaciones de búsqueda globales de la ruta.
9. En la interfaz de egreso, se realizan las operaciones de búsqueda de la ruta de la interfaz. Recuerde, la interfaz de egreso es determinado por la regla de traducción que toma la prioridad.
10. Una vez que se ha encontrado una ruta de la capa 3 y se ha identificado el salto siguiente, acode 2 que se realiza la resolución. La reescritura de la capa 2 del encabezado MAC sucede en esta etapa.
11. El paquete se transmite en el alambre, y los contadores de la interfaz incrementan en la interfaz de egreso.

Explicación del NAT

Refiera a estos documentos para más detalles por orden del Funcionamiento de NAT:

- Versión de software 8.2 de Cisco ASA y anterior
- Versión de software 8.3 de Cisco ASA y posterior

Comandos show

Aquí están algunos comandos útiles que ayudan a seguir los detalles del flujo de paquetes en

diversas etapas en el proceso:

```
show interface
show conn
show access-list
show xlate
show service-policy inspect
show run static
show run nat
show run global
show nat
show route
show arp
```

Mensajes de Syslog

Los mensajes de Syslog proporcionan la información útil sobre el proceso del paquete. Aquí están algunos mensajes de Syslog del ejemplo para su referencia:

- Mensaje de Syslog cuando hay ningún Entrada de conexión:`%ASA-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`
- Mensaje de Syslog cuando el paquete es negado por un ACL:`%ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port by access_group acl_ID`
- Mensaje de Syslog cuando hay ninguna regla de traducción encontrada:`%ASA-3-305005: No translation group found for protocol src interface_name: source_address/source_port dst interface_name:dest_address/dest_port`
- Mensaje de Syslog cuando un paquete es negado por el examen de la Seguridad:`%ASA-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP`
- Mensaje de Syslog cuando no hay información de ruta:`%ASA-6-110003: Routing failed to locate next-hop for protocol from src interface:src IP/src port to dest interface:dest IP/dest port`

Para una lista completa de todos los mensajes de Syslog generados por Cisco ASA junto con una explicación abreviada, refiera a los mensajes de Syslog de la serie de Cisco ASA.

Información Relacionada

- Página de soporte de Cisco ASA
- Referencia de comandos de las 5500 Series de Cisco ASA, 8.2
- Guía de configuración de las 5500 Series de Cisco ASA, 8.3
- Soporte Técnico y Documentación - Cisco Systems