ASA 8.2: Flujo de paquetes a través de un firewall ASA

Contenido

Introducción

Este documento describe el flujo de paquetes a través de un firewall Cisco Adaptive Security Appliance (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.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de los ASA de la serie 5500 de Cisco.

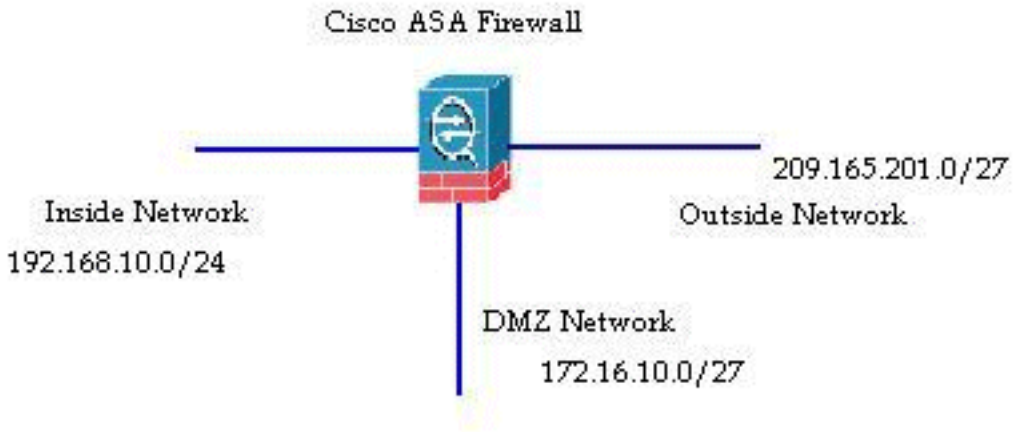
Componentes Utilizados

La información de este documento se basa en los Cisco ASA serie 5500 ASA que ejecutan la versión de software 8.2.

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.

Antecedentes

La interfaz que recibe el paquete se denomina la interfaz de **ingreso** y la interfaz a través de la cual sale el paquete se denomina interfaz de **salida**. Cuando se hace referencia al flujo de paquetes a través de cualquier dispositivo, la tarea se simplifica fácilmente si se observa en términos de estas dos interfaces. A continuación se muestra un escenario de ejemplo:



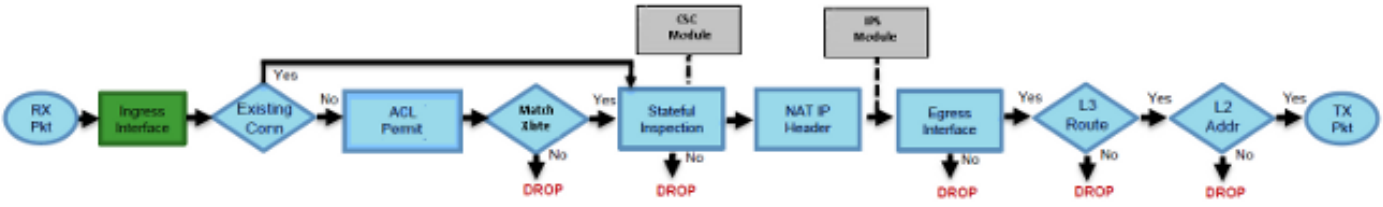
Cuando un usuario interno (192.168.10.5) intenta acceder a un servidor web en la red de zona desmilitarizada (DMZ) (172.16.10.5), el flujo de paquetes tiene el siguiente aspecto:

- Dirección de origen - 192.168.10.5
- Puerto de origen - 22966
- Dirección de destino: 172.16.10.5
- Puerto de destino: 8080
- Interfaz de entrada - Interior
- Interfaz de salida - DMZ
- Protocolo utilizado: TCP (protocolo de control de transmisión)

Después de determinar los detalles del flujo de paquetes como se describe aquí, es fácil aislar el problema a esta entrada de conexión específica.

Algoritmo de proceso de paquetes Cisco ASA

A continuación se muestra un diagrama de cómo Cisco ASA procesa el paquete que recibe:



Estos son los pasos individuales en detalle:

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

interfaz se incrementa en uno.
3. Cisco ASA examina primero los detalles de su tabla de conexión interna para verificar si se trata de una conexión actual. Si el flujo de paquetes coincide con una conexión actual, se omite la comprobación de la Lista de control de acceso (ACL) y se mueve el paquete hacia delante.Si el flujo de paquetes no coincide con una conexión actual, se verifica el estado TCP. Si se trata de un paquete SYN o de un paquete UDP (protocolo de datagramas de usuario), el contador de conexión se incrementa en uno y el paquete se envía para una verificación ACL. Si no es un paquete SYN, el paquete se descarta y se registra el evento.
4. El paquete se procesa según las ACL de la interfaz. Se verifica en orden secuencial de las entradas de ACL y si coincide con alguna de las entradas de ACL, avanza. De lo contrario, se descarta el paquete y se registra la información. El recuento de aciertos de ACL se incrementa en uno cuando el paquete coincide con la entrada de ACL.
5. El paquete se verifica para las reglas de traducción. Si un paquete pasa a través de esta verificación, se crea una entrada de conexión para este flujo y el paquete avanza. De lo contrario, se descarta el paquete y se registra la información.
6. El paquete está sujeto a una Verificación de Inspección. Esta inspección verifica si este flujo de paquete específico cumple o no con el protocolo. Cisco ASA cuenta con un motor de inspección integrado que inspecciona cada conexión según su conjunto predefinido de funciones de nivel de aplicación. Si pasó la inspección, se mueve hacia adelante. De lo contrario, se descarta el paquete y se registra la información.Se implementarán comprobaciones de seguridad adicionales si se incluye un módulo de seguridad de contenido (CSC).
7. La información del encabezado IP se traduce según la regla Traducción de direcciones de red/ Traducción de direcciones de puerto (NAT/PAT) y las sumas de comprobación se actualizan en consecuencia. El paquete se reenvía al Advanced Inspection and Prevention Security Services Module (AIP-SSM) para realizar comprobaciones de seguridad relacionadas con IPS cuando se trata del módulo AIP.
8. El paquete se reenvía a la interfaz de salida según las reglas de traducción. Si no se especifica ninguna interfaz de salida en la regla de traducción, la interfaz de destino se decide en función de la búsqueda de ruta global.
9. En la interfaz de salida, se realiza la búsqueda de ruta de la interfaz. Recuerde que la interfaz de salida está determinada por la regla de traducción que toma la prioridad.
10. Una vez que se ha encontrado una ruta de Capa 3 y se ha identificado el siguiente salto, se realiza la resolución de Capa 2. La reescritura de Capa 2 del encabezado MAC ocurre en esta etapa.
11. El paquete se transmite en el cable y los contadores de interfaz aumentan en la interfaz de salida.

Explicación de NAT

Consulte estos documentos para obtener más detalles sobre el orden de funcionamiento de NAT:

- Software Cisco ASA versión 8.2 y anteriores
- Software Cisco ASA versión 8.3 y posteriores

Comandos show

Estos son algunos comandos útiles que ayudan a realizar el seguimiento de los detalles del flujo

de paquetes en diferentes etapas del 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 información útil sobre el procesamiento de paquetes. A continuación se muestran algunos ejemplos de mensajes de syslog para su referencia:

- Mensaje de Syslog cuando no hay 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 un ACL niega el paquete:
  `%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 no se encuentra ninguna regla de traducción:
  `%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 registro del sistema cuando la inspección de seguridad niega un paquete:
  `%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 obtener una lista completa de todos los mensajes de syslog generados por Cisco ASA junto con una breve explicación, refiérase a Mensajes de Syslog de Cisco ASA Series.

Información Relacionada

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