ASA 8.2: Fluxo de pacotes por meio de um firewall ASA

Contents

Introduction

Este documento descreve o fluxo de pacotes através de um firewall Cisco Adaptive Security Appliance (ASA). Ele mostra o procedimento do Cisco ASA para processar pacotes internos. Ele também discute as diferentes possibilidades onde o pacote poderia ser deixado e as diferentes situações onde o pacote continua adiante.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento dos Cisco 5500 Series ASAs.

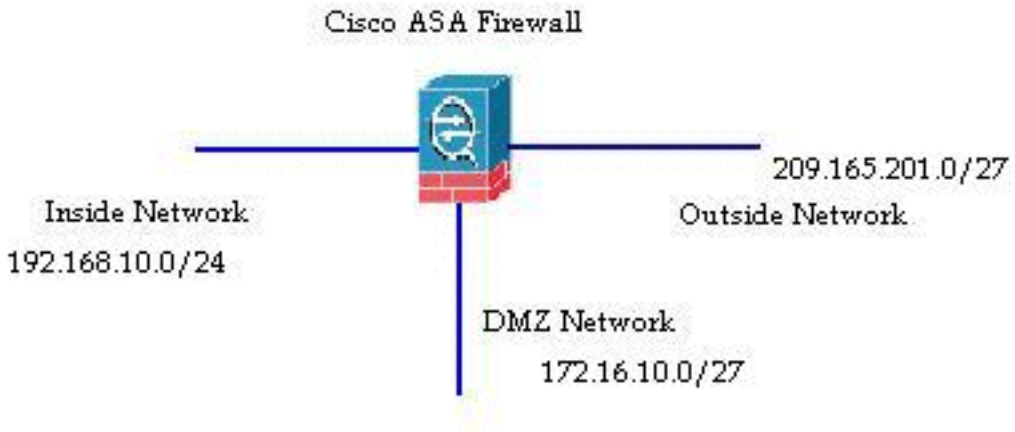
Componentes Utilizados

As informações neste documento são baseadas nos Cisco ASA 5500 Series ASAs que executam a versão 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.

Informações de Apoio

A interface que recebe o pacote é chamada de interface **de entrada** e a interface através da qual o pacote sai é chamada de interface **de saída**. Quando você se refere ao fluxo de pacotes através de qualquer dispositivo, a tarefa é facilmente simplificada se você olhar em termos dessas duas interfaces. Aqui está um exemplo de cenário:



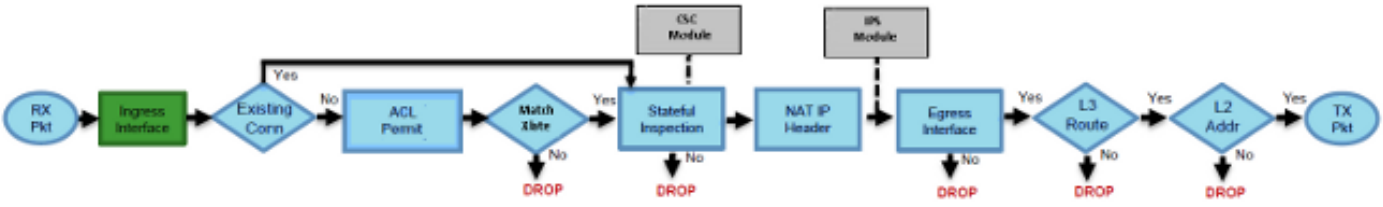
Quando um usuário interno (192.168.10.5) tenta acessar um servidor Web na rede da zona desmilitarizada (DMZ) (172.16.10.5), o fluxo de pacotes se parece com isto:

- Endereço de origem - 192.168.10.5
- Porta de origem - 22966
- Endereço destino - 172.16.10.5
- Porta de destino - 8080
- Interface de entrada - Interno
- Interface de saída - DMZ
- Protocolo usado - TCP (Transmission Control Protocol)

Depois de determinar os detalhes do fluxo do pacote conforme descrito aqui, é fácil isolar o problema a essa entrada de conexão específica.

Algoritmo do processo de pacote do Cisco ASA

Aqui está um diagrama de como o Cisco ASA processa o pacote que recebe:



Aqui estão os detalhes das etapas individuais:

1. O pacote é alcançado na interface de entrada.
2. Quando o pacote chega ao buffer interno da interface, o contador de entrada da interface é

incrementado em um.
3. O Cisco ASA primeiro examina os detalhes da tabela de conexão interna para verificar se esta é uma conexão atual. Se o fluxo do pacote corresponder a uma conexão atual, a verificação da ACL (Access Control List, lista de controle de acesso) será ignorada e o pacote será encaminhado.Se o fluxo do pacote não corresponder a uma conexão atual, o estado do TCP será verificado. Se for um pacote SYN ou UDP (User Datagram Protocol), o contador de conexão é incrementado por um e o pacote é enviado para uma verificação de ACL. Se não for um pacote SYN, o pacote será descartado e o evento será registrado.
4. O pacote é processado de acordo com as ACLs da interface. Ele é verificado na ordem sequencial das entradas da ACL e se corresponde a qualquer uma das entradas da ACL, ele avança. Caso contrário, o pacote será descartado e as informações serão registradas. A contagem de ocorrências da ACL é incrementada em um quando o pacote corresponde à entrada da ACL.
5. O pacote é verificado quanto às regras de tradução. Se um pacote passar por essa verificação, uma entrada de conexão é criada para esse fluxo e o pacote avança. Caso contrário, o pacote será descartado e as informações serão registradas.
6. O pacote é submetido a uma verificação de inspeção. Essa inspeção verifica se esse fluxo de pacote específico está ou não em conformidade com o protocolo. O Cisco ASA tem um mecanismo de inspeção integrado que inspeciona cada conexão de acordo com seu conjunto predefinido de funcionalidade no nível do aplicativo. Se passou na inspeção, ele é levado adiante. Caso contrário, o pacote será descartado e as informações serão registradas.Verificações de segurança adicionais serão implementadas se um módulo de segurança de conteúdo (CSC - Content Security) estiver envolvido.
7. As informações do cabeçalho IP são convertidas de acordo com a regra Network Address Translation/Port Address Translation (NAT/PAT) e as somas de verificação são atualizadas adequadamente. O pacote é encaminhado ao Advanced Inspection and Prevention Security Services Module (AIP-SSM) para verificações de segurança relacionadas ao IPS quando o módulo AIP está envolvido.
8. O pacote é encaminhado à interface de saída com base nas regras de conversão. Se nenhuma interface de saída for especificada na regra de conversão, a interface de destino será decidida com base na pesquisa de rota global.
9. Na interface de saída, a pesquisa da rota da interface é executada. Lembre-se de que a interface de saída é determinada pela regra de conversão que assume a prioridade.
10. Depois que uma rota de Camada 3 é encontrada e o próximo salto identificado, a resolução da Camada 2 é executada. A regravação da Camada 2 do cabeçalho MAC acontece nesse estágio.
11. O pacote é transmitido no fio e os contadores de interface incrementam na interface de saída.

Explicação de NAT

Consulte estes documentos para obter mais detalhes sobre a ordem da operação do NAT:

- Cisco ASA Software versão 8.2 e anterior
- Software Cisco ASA versão 8.3 e posterior

comandos show

Aqui estão alguns comandos úteis que ajudam a rastrear os detalhes do fluxo de pacotes em diferentes estágios do processo:

```
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
```

Mensagens de syslog

As mensagens de syslog fornecem informações úteis sobre o processamento de pacotes. Aqui estão alguns exemplos de mensagens de syslog para sua referência:

- Mensagem de syslog quando não há entrada de conexão:
  `%ASA-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`
- Mensagem de syslog quando o pacote é negado por uma 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`
- Mensagem de syslog quando não há regra de tradução encontrada:
  `%ASA-3-305005: No translation group found for protocol src interface_name: source_address/source_port dst interface_name:dest_address/dest_port`
- Mensagem de syslog quando um pacote é negado pela Inspeção de Segurança:
  `%ASA-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP`
- Mensagem de syslog quando não há informações de rota:
  `%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 obter uma lista completa de todas as mensagens de syslog geradas pelo Cisco ASA, juntamente com uma breve explicação, consulte as Mensagens de Syslog do Cisco ASA Series.

Informações Relacionadas

- Página de suporte do Cisco ASA
- Referência de comando do Cisco ASA 5500 Series, 8.2
- Guia de configuração do Cisco ASA 5500 Series, 8.3
- Suporte Técnico e Documentação - Cisco Systems