ASA 8.2: O pacote corre através de um Firewall ASA

Índice

Introdução

Este documento descreve o pacote corre através de um Firewall adaptável da ferramenta de segurança de Cisco (ASA). Mostra o procedimento de 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.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do Cisco 5500 Series ASA.

Componentes Utilizados

A informação neste documento é baseada no 5500 Series ASA de Cisco ASA que executa a versão de software 8.2.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

A relação que recebe o pacote é chamada a **interface de ingresso** e a relação através de que as saídas do pacote são chamadas a **interface de saída**. Quando você refere o pacote corra através de todo o dispositivo, a tarefa está simplificado facilmente se você a olha em termos destas duas relações. Está aqui um exemplo de cenário:

Quando um usuário interno (192.168.10.5) tentar alcançar um servidor de Web na rede da zona desmilitarizada (DMZ) (172.16.10.5), o fluxo de pacote de informação olha como este:

- Endereço de origem - 192.168.10.5
- Porta de origem - 22966
- Endereço de destino - 172.16.10.5
- Porta do destino - 8080
- Interface de ingresso - Para dentro
- Interface de saída - DMZ
- Protocolo usado - TCP (protocolo Protocolo de control de transmisión (TCP))

Depois que você determina os detalhes do fluxo de pacote de informação como descrito aqui, é fácil isolar a edição a esta entrada de conexão específica.

Algoritmo do processo do pacote de Cisco ASA

Está aqui um diagrama de como Cisco ASA processa o pacote que recebe:

São aqui as etapas individuais em detalhe:

1. O pacote é alcançado na interface de ingresso.
2. Uma vez que o pacote alcança o buffer interno da relação, o contador de entrada da relação está incrementado por uma.
3. Cisco ASA olha primeiramente seus detalhes da tabela da conexão interna a fim verificar se esta é uma conexão atual. Se o fluxo de pacote de informação combina uma conexão atual, a seguir a verificação do Access Control List (ACL) está contorneada e o pacote é movido para a frente.Se o fluxo de pacote de informação não combina uma conexão atual, a seguir o estado TCP está verificado. Se é um pacote SYN ou pacote UDP (protocolo de datagrama de usuário), a seguir o contador da conexão está incrementado por um e o pacote é enviado para uma verificação ACL. Se não é um pacote SYN, o pacote está deixado cair e o evento é registrado.
4. O pacote é processado conforme a relação ACL. Verifica-se no ordem sequencial das entradas ACL e se combina algumas das entradas ACL, move-se para a frente. Se não, o pacote é deixado cair e a informação é registrada. A contagem da batida ACL está incrementada por uma quando o pacote combina a entrada ACL.
5. O pacote é verificado para as Regras de tradução. Se um pacote passa através desta verificação, a seguir uma entrada de conexão está criada para este fluxo e o pacote move-se para a frente. Se não, o pacote é deixado cair e a informação é registrada.
6. O pacote é sujeitado a uma verificação da inspeção. Esta inspeção verifica mesmo se este fluxo de pacote de informação específico é em conformidade com o protocolo. Cisco ASA tem um motor incorporado da inspeção que inspecione cada conexão conforme seu grupo

predefinido de funcionalidade do nível de aplicativo. Se passou a inspeção, é movido para a frente. Se não, o pacote é deixado cair e a informação é registrada.As verificações de segurança adicional estarão executadas se um módulo satisfeito da Segurança (CSC) é involvido.

7. A informação de cabeçalho IP é traduzida conforme a regra da tradução de endereço de porta da tradução de endereço de rede (NAT/PAT) e as somas de verificação são atualizadas em conformidade. O pacote é enviado ao módulo de Serviços de segurança avançado da inspeção e da prevenção (AIP-SSM) para verificações de segurança relativas IPS quando o módulo de AIP é involvido.
8. O pacote é enviado à interface de saída baseada nas Regras de tradução. Se nenhuma interface de saída é especificada na regra de tradução, a seguir a interface de destino está decidida com base na consulta global da rota.
9. Na interface de saída, a consulta da rota da relação é executada. Recorde, a interface de saída é determinado pela regra de tradução que toma a prioridade.
10. Uma vez que uma rota da camada 3 foi encontrada e o salto seguinte esteve identificado, mergulhe 2 que a definição é executada. A reescrita da camada 2 do cabeçalho de MAC acontece nesta fase.
11. O pacote é transmitido no fio, e os contadores de interface incrementam na interface de saída.

Explicação do NAT

Refira estes documentos para mais detalhes na ordem da operação de NAT:

- Versão de software 8.2 de Cisco ASA e mais adiantado
- Versão de software 8.3 de Cisco ASA e mais atrasado

Comandos show

Estão aqui alguns comandos úteis que ajudam a seguir os detalhes do fluxo de pacote de informação em fases diferentes no 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

Os mensagens do syslog fornecem a informação util sobre o processamento do pacote. Estão aqui alguns mensagens do syslog do exemplo para sua referência:

- Mensagem do syslog quando não houver nenhuma 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 do syslog quando o pacote for negado por um 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 do syslog quando houver nenhuma 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 do syslog quando um pacote for negado pela inspeção da Segurança:
  ```
  %ASA-4-405104: H225 message received from outside_address/outside_port to
  inside_address/inside_port before SETUP
  ```
- Mensagem do syslog quando não houver nenhuma informação 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 uma lista completa de todos os mensagens do syslog gerados por Cisco ASA junto com uma explicação resumida, refira os mensagens do syslog da série de Cisco ASA.

Informações Relacionadas

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