ASA 8.2: PacketFlow via een ASA-firewall

Inhoud

Inleiding

Dit document beschrijft de pakketstroom door een Cisco adaptieve security applicatie (ASA) firewall. Het toont de procedure van Cisco ASA om interne pakketten te verwerken. Het bespreekt ook de verschillende mogelijkheden waar het pakje kon worden ingetrokken en de verschillende situaties waarin het pakje vooruitgaat.

Voorwaarden

Vereisten

Cisco raadt aan dat u kennis hebt van Cisco 5500 Series ASA's.

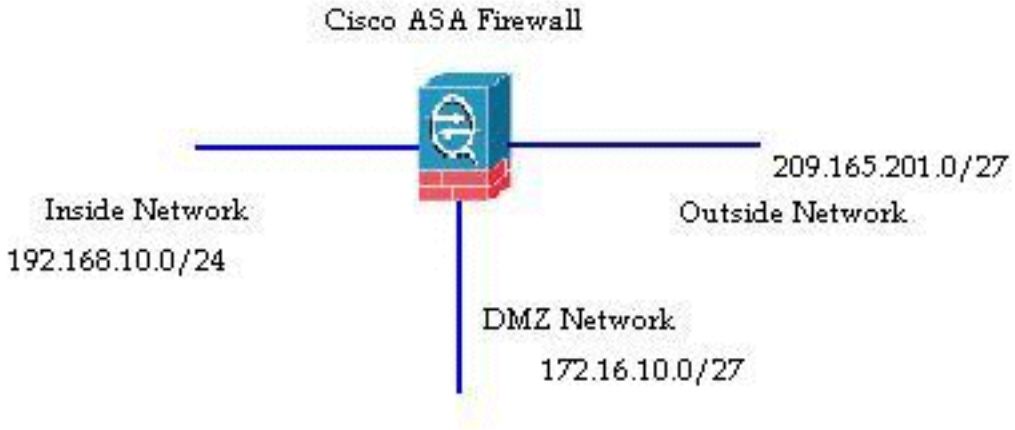
Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ASA 5500 Series ASA-systemen die softwareversie 8.2 uitvoeren.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

De interface die het pakket ontvangt wordt de **ingangsinterface** genoemd en de interface waardoor het pakket wordt afgesloten wordt de **egress-**interface genoemd. Wanneer u naar de pakketstroom door een apparaat verwijst, wordt de taak eenvoudig vereenvoudigd als u naar deze twee interfaces kijkt. Hier is een voorbeeldscenario:



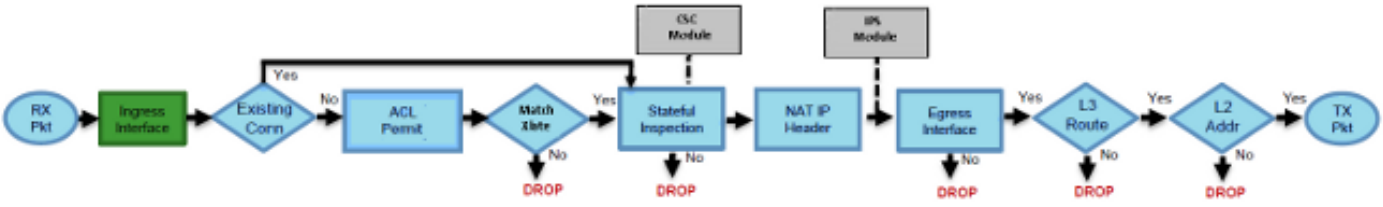
Wanneer een binnengebruiker (192.168.10.5) probeert om toegang te krijgen tot een webserver in het gedemilitariseerde zone (DMZ) netwerk (172.16.10.5) ziet de pakketstroom er zo uit:

- Bron: rede - 192.168.10.5
- Bron: poort 2966
- Doeladres - 172.16.10.5
- Doelhaven - 8080
- Infrress interface - binnenzijde
- Eigen interface - DMZ
- Gebruikte protocol - TCP (Transmission Control Protocol)

Nadat u de details van de pakketstroom zoals hier beschreven hebt bepaald, is het gemakkelijk om de kwestie aan deze specifieke verbinding ingang te isoleren.

Cisco ASA Packet Management Algoritme

Hier is een diagram van hoe Cisco ASA het pakket verwerkt dat het ontvangt:



Hier zijn de afzonderlijke stappen in detail:

1. Het pakket wordt bereikt op de ingangsinterface.
2. Zodra het pakket de interne buffer van de interface bereikt, wordt de ingangsteller van de

interface met één verhoogd.
3. Cisco ASA bekijkt eerst zijn interne details van de connectietabel om te controleren of dit een huidige verbinding is. Als de pakketstroom overeenkomt met een huidige verbinding, wordt de controle van de toegangscontrolelijst (ACL) omzeild en wordt het pakket verplaatst.Als de pakketstroom geen huidige verbinding overeenkomt, wordt de TCP-status geverifieerd. Als het een SYN-pakket of een UDP-pakket (User Datagram Protocol) is, wordt de verbindingsteller met één verhoogd en wordt het pakket voor een ACL-controle verzonden. Als dit geen SYN-pakket is, wordt het pakje ingetrokken en wordt de gebeurtenis geregistreerd.
4. Het pakket wordt verwerkt zoals in de interface-ACL's. Het wordt in sequentiële volgorde van de ACL-waarden geverifieerd en als het overeenkomt met een van de ACL-items, wordt het naar voren verschoven. Anders wordt het pakje ingetrokken en wordt de informatie geregistreerd. De ACL-toetstitel wordt met één verhoogd wanneer het pakket overeenkomt met de ACL-ingang.
5. Het pakje wordt gecontroleerd voor de vertaalregels. Als een pakje door deze controle gaat, wordt er een verbindingsingang voor deze stroom gemaakt en wordt het pakje voorwaarts beweegt. Anders wordt het pakje ingetrokken en wordt de informatie geregistreerd.
6. De verpakking wordt aan een controle onderworpen. Deze inspectie controleert of deze specifieke pakketstroom in overeenstemming is met het protocol. Cisco ASA heeft een ingebouwde inspectiemotor die elke verbinding inspecteert volgens de vooraf gedefinieerde reeks applicatieniveaus. Als de inspectie is goedgekeurd, wordt het verder gebracht. Anders wordt het pakje ingetrokken en wordt de informatie geregistreerd.Aanvullende beveiligingscontroles worden uitgevoerd als er een CSC-module (Content Security) is betrokken.
7. De IP-headerinformatie wordt vertaald zoals in de NAT/PAT-regel (Network Address Translation/Port Address Translation) en de checksum wordt dienovereenkomstig bijgewerkt. Het pakket wordt doorgestuurd naar geavanceerde inspectie en preventie security servicesmodule (AIP-SSM) voor IPS-gerelateerde beveiligingscontroles wanneer de AIP-module betrokken is.
8. Het pakje wordt naar de accu-interface gestuurd op basis van de vertaalregels. Als geen uitgang interface wordt gespecificeerd in de vertaalregel dan wordt de bestemming interface bepaald op basis van de globale routeraadpleging.
9. Op de spanning interface wordt de raadpleging van de interfaceroute uitgevoerd. Onthoud, de uitgang interface wordt bepaald door de vertaalregel die de prioriteit neemt.
10. Zodra een Layer 3 route is gevonden en de volgende hop is geïdentificeerd, wordt Layer 2 resolutie uitgevoerd. Layer 2 herschrijven van de MAC-header gebeurt in dit stadium.
11. Het pakket wordt op de draad verzonden, en de toename van de interfacetellers op de spanning interface.

Uitleg van NAT

Raadpleeg deze documenten voor meer informatie over de volgorde van de NAT-activiteiten:

- Cisco ASA-softwarerelease 8.2 en hoger
- Cisco ASA-softwarerelease 8.3 en hoger

Opdrachten weergeven

Hier zijn een paar nuttige opdrachten die u helpen de pakketstroomgegevens in verschillende fasen van het proces te volgen:

```
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
```

Syslog-berichten

Syslogberichten bieden nuttige informatie over pakketverwerking. Hier zijn een paar syslog-berichten voor uw referentie:

- Bericht op koppelteken wanneer er geen verbinding is:
  `%ASA-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`
- Dit bericht wordt weergegeven wanneer het pakket wordt ontkend door een 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`
- Bericht op borgtocht wanneer er geen vertaalregel is gevonden:
  `%ASA-3-305005: No translation group found for protocol src interface_name: source_address/source_port dst interface_name:dest_address/dest_port`
- Splitsen bericht wanneer een pakje wordt geweigerd door Security Inspection:
  `%ASA-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP`
- Syslog-bericht wanneer er geen routeinformatie is:
  `%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`

Voor een volledige lijst van alle slogberichten die door Cisco ASA zijn gegenereerd samen met een korte uitleg, verwijs naar de Cisco ASA Series SLOG Messages.

Gerelateerde informatie

- Cisco ASA-ondersteuningspagina
- Cisco ASA 5500 Series commando referentie, 8.2
- Cisco ASA 5500 Series configuratie Guide, 8.3
- Technische ondersteuning en documentatie – Cisco Systems