ASA 8.2: Paketfluss durch eine ASA-Firewall

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Cisco ASA Paketprozess-Algorithmus](#)
[Erläuterung der NAT](#)
[Befehle anzeigen](#)
[Syslog-Meldungen](#)
[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt den Paketfluss über eine Cisco Adaptive Security Appliance (ASA)-Firewall. Es zeigt die Cisco ASA-Prozedur zur Verarbeitung interner Pakete. Außerdem werden die verschiedenen Möglichkeiten erläutert, wie das Paket verworfen werden kann und in welchen Situationen das Paket vorankommt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit den Cisco ASAs der Serie 5500 vertraut sind.

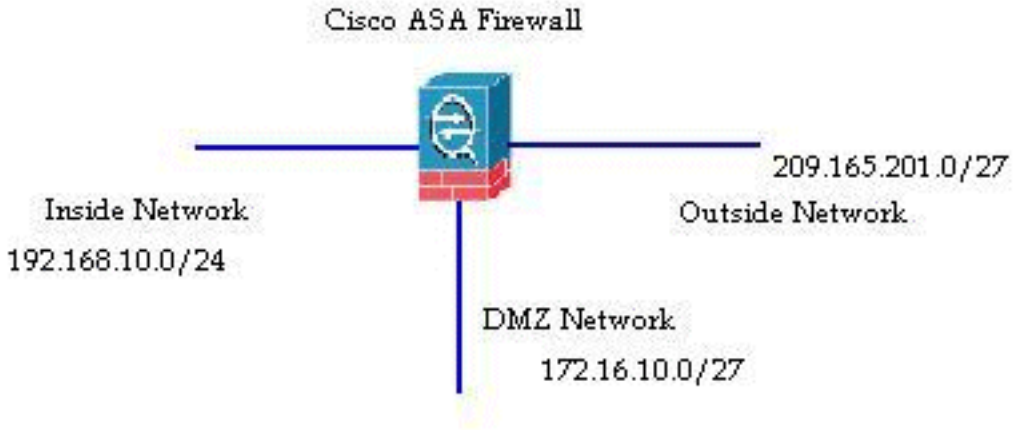
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf ASAs der Cisco Serie ASA 5500, die Software Version 8.2 ausführen.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Die Schnittstelle, die das Paket empfängt, wird als **Eingangs-**Schnittstelle bezeichnet und die Schnittstelle, über die das Paket beendet wird, als **Ausgangs-**Schnittstelle bezeichnet. Wenn Sie sich auf den Paketfluss durch ein Gerät beziehen, wird die Aufgabe leicht vereinfacht, wenn Sie diesen beiden Schnittstellen zuordnen. Hier ein Beispielszenario:



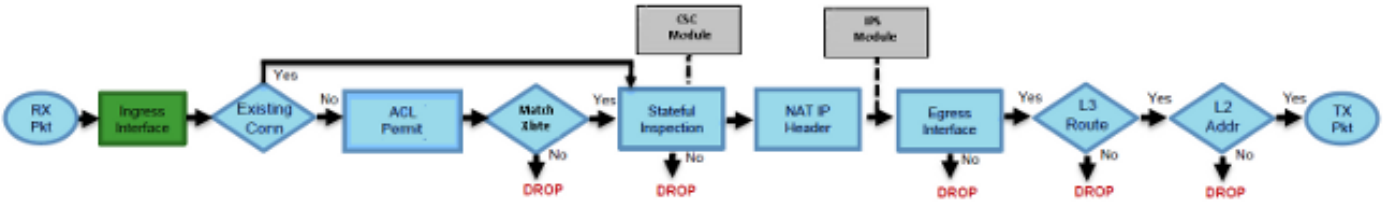
Wenn ein interner Benutzer (192.168.10.5) versucht, auf einen Webserver im DMZ-Netzwerk (Demilitarized Zone) (172.16.10.5) zuzugreifen, sieht der Paketfluss wie folgt aus:

- Quelladresse - 192.168.10.5
- Quellport - 22966
- Zieladresse - 172.16.10.5
- Ziel-Port - 8080
- Eingangsschnittstelle - Inside
- Ausgangsschnittstelle - DMZ
- Verwendetes Protokoll - TCP (Transmission Control Protocol)

Nachdem Sie die Details des Paketflusses wie hier beschrieben ermittelt haben, können Sie das Problem leicht auf diesen spezifischen Verbindungeintrag zurückführen.

Cisco ASA Paketprozess-Algorithmus

Im folgenden Diagramm wird dargestellt, wie die Cisco ASA das empfangene Paket verarbeitet:



Im Folgenden werden die einzelnen Schritte im Detail beschrieben:

1. Das Paket wird an der Eingangsschnittstelle erreicht.
2. Sobald das Paket den internen Puffer der Schnittstelle erreicht hat, wird der Eingangszähler

der Schnittstelle um eins erhöht.

3. Die Cisco ASA überprüft zunächst die Details der internen Verbindungstabelle, um festzustellen, ob es sich um eine aktuelle Verbindung handelt. Wenn der Paketfluss mit einer aktuellen Verbindung übereinstimmt, wird die Überprüfung der Zugriffskontrollliste (ACL) umgangen und das Paket wird vorwärts verschoben.Wenn der Paketfluss nicht mit einer aktuellen Verbindung übereinstimmt, wird der TCP-Status überprüft. Wenn es sich um ein SYN-Paket oder ein UDP-Paket (User Datagram Protocol) handelt, wird der Verbindungszähler um eins erhöht, und das Paket wird zur ACL-Prüfung gesendet. Wenn es sich nicht um ein SYN-Paket handelt, wird das Paket verworfen und das Ereignis protokolliert.
4. Das Paket wird gemäß den Schnittstellen-ACLs verarbeitet. Sie wird in sequenzieller Reihenfolge der ACL-Einträge überprüft. Wenn sie mit einem der ACL-Einträge übereinstimmt, wird der Vorgang fortgesetzt. Andernfalls wird das Paket verworfen und die Informationen protokolliert. Die ACL-Trefferanzahl wird um eins erhöht, wenn das Paket mit dem ACL-Eintrag übereinstimmt.
5. Das Paket wird auf die Übersetzungsregeln überprüft. Wenn ein Paket diese Prüfung durchläuft, wird für diesen Datenfluss ein Verbindungseintrag erstellt und das Paket wird weitergeleitet. Andernfalls wird das Paket verworfen und die Informationen protokolliert.
6. Das Paket wird einer Überprüfung unterzogen. Bei dieser Überprüfung wird überprüft, ob dieser spezifische Paketfluss mit dem Protokoll übereinstimmt. Die Cisco ASA verfügt über eine integrierte Prüfungs-Engine, die jede Verbindung entsprechend der vordefinierten Funktionalität auf Anwendungsebene überprüft. Wenn sie die Prüfung bestanden hat, wird sie fortgeführt. Andernfalls wird das Paket verworfen und die Informationen protokolliert.Zusätzliche Sicherheitsüberprüfungen werden implementiert, wenn ein Content Security (CSC)-Modul involviert ist.
7. Die IP-Headerinformationen werden gemäß der Network Address Translation/Port Address Translation (NAT/PAT)-Regel übersetzt und die Prüfsummen werden entsprechend aktualisiert. Das Paket wird an das Advanced Inspection and Prevention Security Services Module (AIP-SSM) für IPS-bezogene Sicherheitsüberprüfungen weitergeleitet, wenn das AIP-Modul beteiligt ist.
8. Das Paket wird basierend auf den Übersetzungsregeln an die Ausgangsschnittstelle weitergeleitet. Wenn in der Übersetzungsregel keine Ausgangsschnittstelle angegeben ist, wird die Zielschnittstelle basierend auf der globalen Routensuche festgelegt.
9. Auf der Ausgangsschnittstelle wird die Suche nach der Schnittstellenroute durchgeführt. Beachten Sie, dass die Ausgangsschnittstelle durch die Übersetzungsregel bestimmt wird, die die Priorität einnimmt.
10. Sobald eine Layer-3-Route gefunden und der nächste Hop identifiziert wurde, wird die Layer-2-Auflösung ausgeführt. Die Layer-2-Neufassung des MAC-Headers erfolgt in dieser Phase.
11. Das Paket wird über die Leitung übertragen, und Schnittstellenzähler werden an der Ausgangsschnittstelle erhöht.

Erläuterung der NAT

Weitere Einzelheiten zur Reihenfolge der NAT-Operationen finden Sie in diesen Dokumenten:

- Cisco ASA Software Version 8.2 oder frühere Version
- Cisco ASA Software Version 8.3 oder höher

Befehle anzeigen

Im Folgenden sind einige nützliche Befehle aufgeführt, mit denen Sie die Details des Paketflusses in den verschiedenen Prozessstufen verfolgen können:

```
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-Meldungen

Syslog-Meldungen bieten nützliche Informationen zur Paketverarbeitung. Hier einige Beispiele für Syslog-Meldungen:

- Syslog-Meldung, wenn kein Verbindungsprotokoll vorhanden ist:
  `%ASA-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`
- Syslog-Meldung, wenn das Paket von einer ACL abgelehnt wird:
  `%ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port by access_group acl_ID`
- Syslog-Meldung, wenn keine Übersetzungsregel gefunden wurde:
  `%ASA-3-305005: No translation group found for protocol src interface_name: source_address/source_port dst interface_name:dest_address/dest_port`
- Syslog-Meldung, wenn ein Paket von der Sicherheitsüberprüfung abgelehnt wird:
  `%ASA-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP`
- Syslog-Meldung, wenn keine Routeninformationen vorliegen:
  `%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`

Eine vollständige Liste aller von der Cisco ASA generierten Syslog-Meldungen sowie eine kurze Erläuterung finden Sie in den Syslog-Meldungen der Cisco ASA-Serie.

Zugehörige Informationen

- Cisco ASA Support-Seite
- Cisco ASA 5500 Series Command Reference, 8.2
- Konfigurationsleitfaden für die Cisco Serie ASA 5500, 8.3
- Technischer Support und Dokumentation - Cisco Systems