ASA 8.2: ASA 방화벽을 통한 패킷 흐름

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance) 방화벽을 통한 패킷 흐름에 대해 설명합니다. 내부 패킷을 처리하는 Cisco ASA 절차가 표시됩니다. 또한 패킷이 삭제될 수 있는 다양한 가능성과 패킷이 앞으로 진행되는 다양한 상황에 대해서도 설명합니다.

사전 요구 사항

요구 사항

Cisco는 Cisco 5500 Series ASA에 대한 지식을 보유하고 있는 것을 권장합니다.

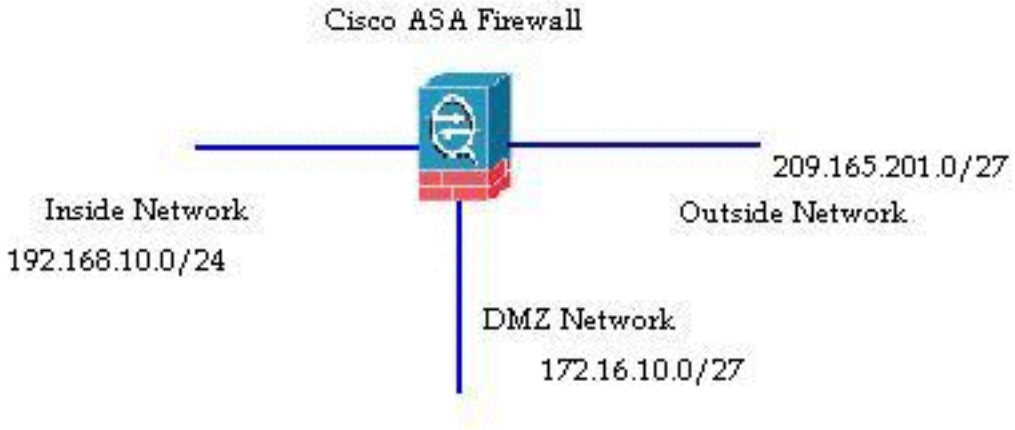
사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 8.2를 실행하는 Cisco ASA 5500 Series ASA를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

패킷을 수신하는 인터페이스를 **인그레스** 인터페이스라고 하며 패킷이 종료되는 인터페이스를 이그레스 인터페이스라고 **합니다**. 어떤 디바이스에서든 패킷 흐름을 참조할 때, 이러한 두 인터페이스의 관점에서 보면 작업이 쉽게 간소화됩니다. 다음은 샘플 시나리오입니다.



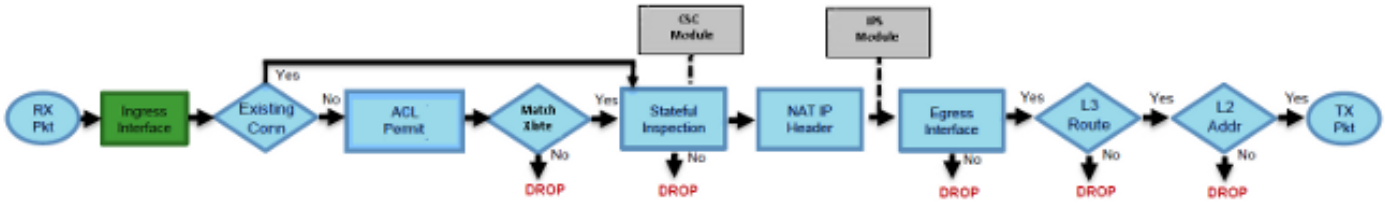
내부 사용자(192.168.10.5)이 DMZ(demilitarized zone) 네트워크(172.16.10.5)에서 웹 서버에 액세스하려고 할 때 패킷 흐름은 다음과 같습니다.

- 소스 주소 - 192.168.10.5
- 소스 포트 - 22966
- 대상 주소 - 172.16.10.5
- 대상 포트 - 8080
- 인그레스 인터페이스 - 내부
- 이그레스 인터페이스 - DMZ
- 사용된 프로토콜 - TCP(Transmission Control Protocol)

여기에 설명된 대로 패킷 흐름의 세부사항을 확인한 후 이 특정 연결 항목으로 문제를 쉽게 격리할 수 있습니다.

Cisco ASA 패킷 프로세스 알고리즘

다음은 Cisco ASA에서 수신하는 패킷을 처리하는 방법에 대한 다이어그램입니다.



개별 단계는 다음과 같습니다.

1. 패킷은 인그레스 인터페이스에서 도달합니다.
2. 패킷이 인터페이스의 내부 버퍼에 도달하면 인터페이스의 입력 카운터가 1씩 증가합니다.
3. Cisco ASA는 먼저 내부 연결 테이블 세부 정보를 확인하여 현재 연결인지 확인합니다. 패킷 흐름이 현재 연결과 일치하면 ACL(Access Control List) 검사가 우회되고 패킷이 앞으로 이동합니다.패킷 흐름이 현재 연결과 일치하지 않으면 TCP 상태가 확인됩니다. SYN 패킷 또는 UDP(User Datagram Protocol) 패킷인 경우 연결 카운터가 1씩 증가하며 ACL 확인을 위해 패

킷이 전송됩니다. SYN 패킷이 아니면 패킷이 삭제되고 이벤트가 기록됩니다.
4. 패킷은 인터페이스 ACL에 따라 처리됩니다. ACL 항목의 순차적 순서로 확인되며 ACL 항목과 일치하는 경우 앞으로 이동합니다. 그렇지 않으면 패킷이 삭제되고 정보가 기록됩니다. 패킷이 ACL 항목과 일치하면 ACL 적중 횟수가 1씩 증가합니다.
5. 패킷이 변환 규칙에 대해 확인됩니다. 패킷이 이 이 검사를 통과하면 이 흐름에 대한 연결 항목이 생성되고 패킷이 앞으로 이동합니다. 그렇지 않으면 패킷이 삭제되고 정보가 기록됩니다.
6. 패킷에 검사 검사가 수행됩니다. 이 검사는 이 특정 패킷 흐름이 프로토콜을 준수하는지 여부를 확인합니다. Cisco ASA에는 미리 정의된 애플리케이션 레벨 기능 집합에 따라 각 연결을 검사하는 내장형 검사 엔진이 있습니다. 검사를 통과하면 앞으로 이동합니다. 그렇지 않으면 패킷이 삭제되고 정보가 기록됩니다.CSC(Content Security) 모듈이 포함된 경우 추가 보안 검사가 구현됩니다.
7. IP 헤더 정보는 NAT/PAT(Network Address Translation/Port Address Translation) 규칙에 따라 변환되며 이에 따라 체크섬이 업데이트됩니다. AIP 모듈이 포함된 경우 IPS 관련 보안 검사를 위해 AIP-SSM(Advanced Inspection and Prevention Security Services Module)에 패킷이 전달됩니다.
8. 패킷은 변환 규칙에 따라 이그레스 인터페이스로 전달됩니다. 변환 규칙에 지정된 이그레스 인터페이스가 없으면 전역 경로 조회를 기반으로 대상 인터페이스가 결정됩니다.
9. 이그레스 인터페이스에서 인터페이스 경로 조회가 수행됩니다. 이그레스 인터페이스는 우선 순위를 사용하는 변환 규칙에 의해 결정됩니다.
10. 레이어 3 경로가 발견되고 다음 홉이 확인되면 레이어 2 확인이 수행됩니다. MAC 헤더의 레이어 2 재작성은 이 단계에서 수행됩니다.
11. 패킷은 와이어에서 전송되며 인터페이스 카운터는 이그레스 인터페이스에서 증가합니다.

NAT 설명

NAT 작업 순서에 대한 자세한 내용은 다음 문서를 참조하십시오.

- Cisco ASA Software 버전 8.2 이하
- Cisco ASA 소프트웨어 버전 8.3 이상

명령 표시

프로세스의 여러 단계에서 패킷 흐름 세부사항을 추적하는 데 도움이 되는 몇 가지 유용한 명령어는 다음과 같습니다.

```
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 메시지

Syslog 메시지는 패킷 처리에 대한 유용한 정보를 제공합니다. 참고용에 대한 몇 가지 syslog 메시

지 예는 다음과 같습니다.

- 연결 항목이 없는 경우 Syslog 메시지:
  ```
  %ASA-6-106015: Deny TCP (no connection) from IP_address/port to
  IP_address/port flags tcp_flags on interface interface_name
  ```
- ACL에서 패킷을 거부하면 Syslog 메시지:
  ```
  %ASA-4-106023: Deny protocol src [interface_name:source_address/source_port]
  dst interface_name:dest_address/dest_port by access_group acl_ID
  ```
- 변환 규칙이 없는 경우 Syslog 메시지:
  ```
  %ASA-3-305005: No translation group found for protocol src interface_name:
  source_address/source_port dst interface_name:dest_address/dest_port
  ```
- 보안 검사에서 패킷을 거부할 경우 Syslog 메시지:
  ```
  %ASA-4-405104: H225 message received from outside_address/outside_port to
  inside_address/inside_port before SETUP
  ```
- 경로 정보가 없는 경우 Syslog 메시지:
  ```
  %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
  ```

Cisco ASA에서 생성된 모든 syslog 메시지의 전체 목록과 간단한 설명은 Cisco ASA Series Syslog 메시지를 참조하십시오.

관련 정보

- Cisco ASA 지원 페이지
- Cisco ASA 5500 Series 명령 참조, 8.2
- Cisco ASA 5500 Series 컨피그레이션 가이드, 8.3
- 기술 지원 및 문서 – Cisco Systems