1. 패킷 필터링

패킷이 방화벽을 통과하는 곳부터 서버 측의 탐험 여행을 시작한다.

방화벽의 기본 기념은 특정 서버와 해당 서버 안의 특정 애플리케이션에 액세스하는 패킷만 통과시키고, 그 외의 패킷을 차단한다.

- **패킷 필터링**

이 외에도 다양한 종류의 패킷이 많이 흐르게 되는데 그것들을 다 선별하는 것이 간단한 일이 아니므로 성능, 가격, 사용 편의성을 이유로 지금은 **패킷 필터링형**이 가장 많이 보급되었다.

- **패킷 필터링 조건 설정**

➔ 수신처나 송신처의 주소에 따라 패킷이 어디서, 어디로 흘러가는지를 판단하여 통과시킬 것인지, 차단할 것인지 결정한다.

  ■ 예를 들어 인터넷에서 웹 서버로 패킷이 들어올 경우, 수신처 IP주소가 웹 서버의 IP 주소에 일치하는 경우 패킷을 통과시킨다.

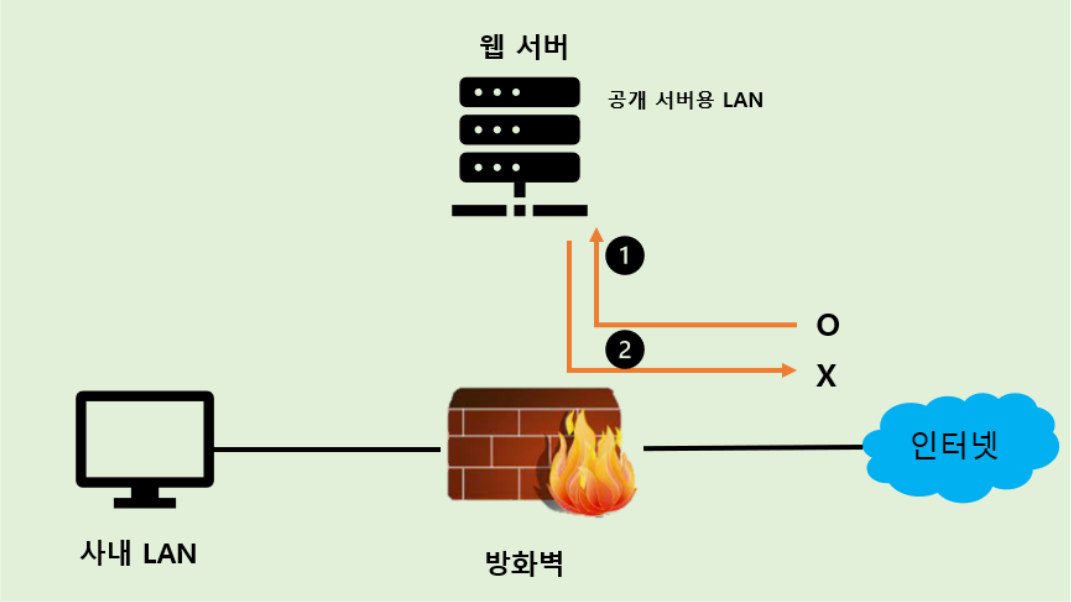


그림 1. 패킷 필터링

2. 애플리케이션 한정과 포트번호

위와 같은 상황만으로 패킷을 통제하는 경우 웹 서버를 흐르는 패킷은 전부 통과하여 위험한 상태가 된다.

따라서 애플리케이션을 한정할 때는 TCP나 UDP 헤더에 기록되어 있는 포트 번호를 조건으로 추가한다.

- ➔ 웹 서버의 포트 번호는 80번으로 결정되어 있으므로 전술한 수신처 IP주소 및 송신처 IP 주소에 수신처 포트 번호가 80번인 경우에 대한 조건도 추가한다.
- ➔ 즉 수신처의 IP주소가 웹 서버의 주소와 일치하고, 수신처 포트번호가 80번인 패킷을 통과시킨다.

3. 컨트롤 비트로 접속 방향 판단

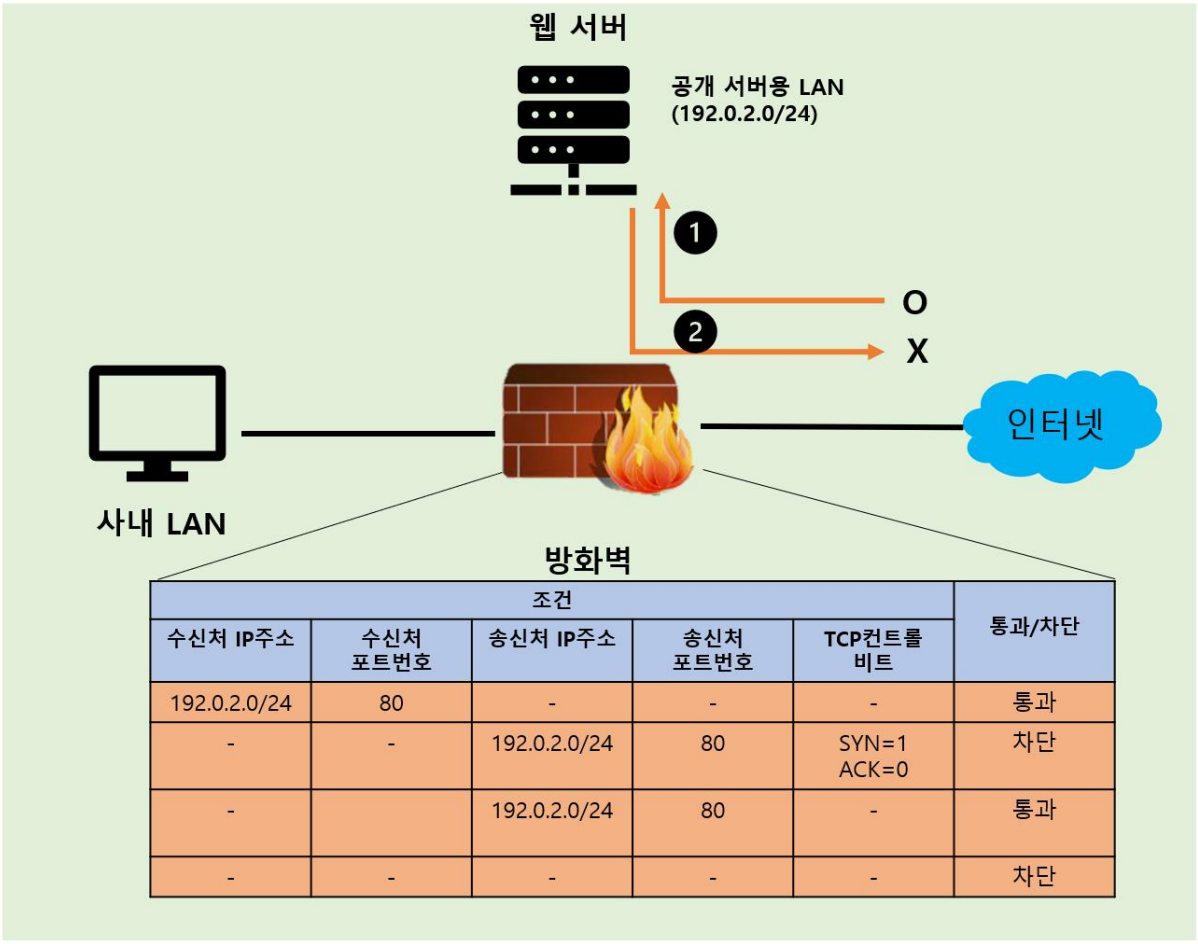
패킷이 흐르는 방향이 아니라 액세스 방향을 판단하여 정지시키기 위해 사용하는 것이 TCP헤더에 있는 **컨트롤 비트**이다.

- ➔ TCP는 최초에 행하는 접속 단계의 동작에서 3개의 패킷이 흐르는데, 최초의 패킷만 TCP 컨트롤 비트의 SYN이라는 비트가 1이 되고, ACK라는 비트가 0이 된다.
- ➔ 다른 패킷에서 같은 값을 취하는 경우는 없으므로 이 값을 조사하여 최초의 패킷과 두번째 이후의 패킷을 판별할 수 있다.

최초의 패킷이 웹 서버 측에서 인터넷 측으로 흘러갈 경우 이것을 차단하도록 설정하면 상대로부터 패킷이 돌아오는 경우가 없으므로 TCP 접속 동작은 실패한다. 이렇게 하여 웹 서버에서 인터넷으로 액세스 하는 동작을 정지시킬 수 있다.

인터넷에서 웹 서버로 액세스 할 때 최초의 패킷은 수신처가 웹 서버를 나타내고 그림 2와 같이 방화벽 테이블 조건에 만족하므로 패킷을 통과시킨다.

이런 방식으로 액세스 할 때 흐르는 패킷은 패킷 필터링을 통과하거나 차단된다.



조건					통과/차단
수신처 IP주소	수신처 포트번호	송신처 IP주소	송신처 포트번호	TCP컨트롤 비트	
192.0.2.0/24	80	-	-	-	통과
-	-	192.0.2.0/24	80	SYN=1 ACK=0	차단
-		192.0.2.0/24	80	-	통과
-	-	-	-	-	차단

그림 2. 패킷 필터링 예제

- **통과할 수 있는 것과 차단하는 것을 선별하기 어려운 경우**

➔ DNS서버에 조회하는 동작은 UDP를 사용하는데 UDP는 TCP와 달리 접속 단계의 동작이 없으므로 TCP처럼 컨트롤 비트에 의해 액세스 방향을 판별할 수 없다.

➔ 따라서 사내에서 인터넷의 DNS서버에 액세스하는 것을 허가하고, 인터넷에서 사내의 DNS서버에 액세스하는 것을 차단하는 조건을 설정할 수 없다.

➔ 이 성질은 UDP를 사용하는 애플리케이션에 공통이므로 불편을 감수하고 전부 통과시키거나, 전면 차단하는 방법을 선택해야 한다.

4. LAN 설정

그림 2와 같은 구성의 경우 인터넷과 공개 서버용 LAN을 왕래하는 패킷의 조건 설정 뿐만 아니라, 사내 LAN과 인터넷 또는 사내 LAN과 공개 서버용 LAN을 왕래하는 패킷의 조건도 설정해야 한다.

이때 조건에 서로에게 악영향을 끼치지 않도록 주의해야 한다.

- ➔ 예를 들어 사내 LAN과 공개 서버용 LAN 사이를 자유로이 왕래할 수 있도록 수신처 IP주소가 공개된 서버용 LAN과 일치하는 패킷을 전부 통과시켰다고 가정한다.
- ➔ 이후 깜빡 잊고 송신처 IP주소를 조건으로 설정하지 않으면 인터넷 측에서 흘러온 패킷이 무조건 공개 서버용 LAN에 유입되어 공개 서버용 LAN에 설치한 서버 전부가 위험에 빠지게 된다.

패킷의 통과/차단뿐만 아니라 주소 변환 기능도 가지고 있으므로 설정이 필요하다.

- ➔ 패킷 필터링과 마찬가지로 패킷의 시점과 종점을 조건으로 지정한 후 주소 변환이 필요한 경우에는 주소 변환을 하고, 필요하지 않은 경우에는 변환하지 않도록 한다.
- ➔ 따라서 주소 변환을 하면 당연히 인터넷 측에서 사내 LAN에는 액세스 할 수 없게 된다.

5. 방화벽 통과

패킷 필터링형 방화벽은 수신처 IP주소, 송신처 IP주소, 수신처 포트 번호, 송신처 포트 번호, 컨트롤 비트 등으로 패킷을 통과시킬지 판단한다.

패킷을 판단하고 차단할 경우 그 기록을 남겨 부정침입의 흔적이 나타나면 분석하여 향후 침입 대책에 도움이 되도록 한다.

통과시킨다는 판정을 내리면 패킷을 중계하는데 이 중계 동작은 라우터의 동작과 같다.

단 판정 조건이 복잡해지면 라우터의 명령으로 설정하기가 어려워지고, 패킷을 버린 기록을 남기는 것도 라우터에 크게 부담스러운 작업이기 때문에 전용 하드웨어나 소프트웨어를 사용한다.

6. 방화벽으로 막을 수 없는 공격

방화벽은 시점과 종점만 조사하므로 패킷 중에 특수한 데이터가 포함되어 있어도 이것에 신경 쓰지 않고 패킷을 통과시킨다. 이것이 웹 서버에 도착하여 문제가 발생하면 서버가 다운될 수 도 있다.

- **두 가지 대처 방법**

➔ 먼저 문제의 원인이 웹 서버 소프트웨어의 버그에 있으므로 버그를 고쳐 다운되지 않도록 하는 방법이 있다.

  ■ 버그를 수정하지 않은 새 버전이 배포될 경우 위험성이 높기 때문에 보안 구멍 정보를 수집하여 항상 버그가 없는 새로운 버전으로 갱신하는 것이 중요하다.

➔ 패킷의 내용을 조사하여 위험한 데이터가 포함되어 있는 경우 패킷을 차단하도록 장치나 소프트웨어를 방화벽과는 별도로 준비하는 방법이 있다.

  ■ 이런 경우 잠재적인 버그가 숨어있는데도 발견하지 못할 경우 패킷이 위험하다고 판단하지 못하게 되므로 패킷을 차단하지 못하게 된다.