Internet Security

https://youtu.be/6Iuj0xRGMr8

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

IPSec

PGP

Firewalls

IPSec

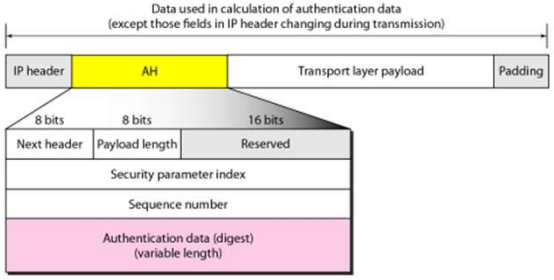
IPSec이란

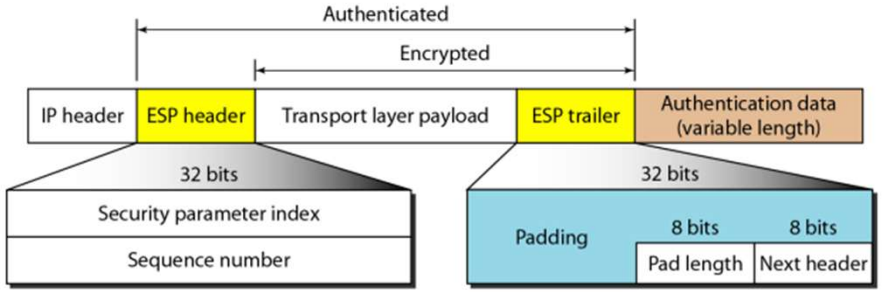
네트워크에서의 안전한 연결을 설정하기 위한 **프로토콜 세트**

1. 인증 헤더(AH)

발신자 인증 데이터가 포함된 헤더를 추가, 권한 없이 당사자가 수정하지 못하도록 패킷을 보호한다.

패킷을 수신할 때 컴퓨터는 페이로드의 암호화 해시 계산 결과를 헤더와 비교하여 무결성을 검증한다.





2. 보안 페이로드 캡슐화(ESP)

전체 IP 패킷 또는 페이로드에 대해서만 암호화를 수행한다. 암호화를 할 때 패킷에 헤더와 트레일러를 추가한다.

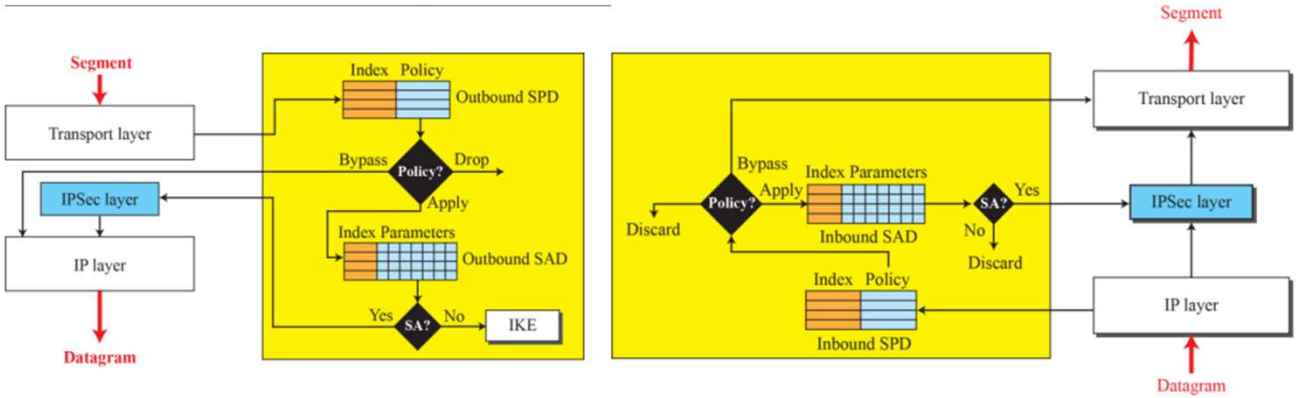
IPSec

IPSec이란

3. Internet Key Exchange(IKE)

두 디바이스 간에 보안 연결을 설정하는 프로토콜이다.

두 디바이스 모두 암호화 키 및 알고리즘을 협상하여 후속 데이터 패킷을 송수신하는 보안 연결(SA)을 설정



IPSec

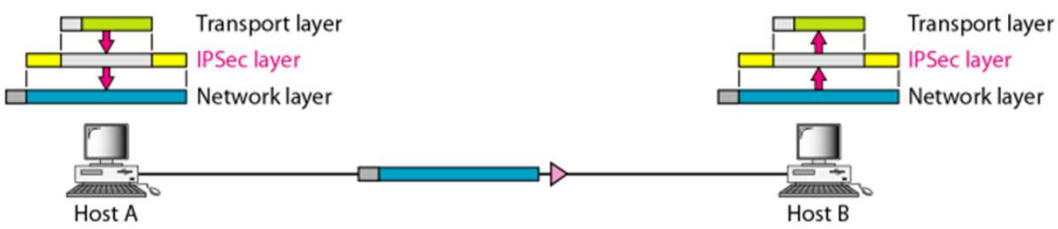
IPSec의 종류

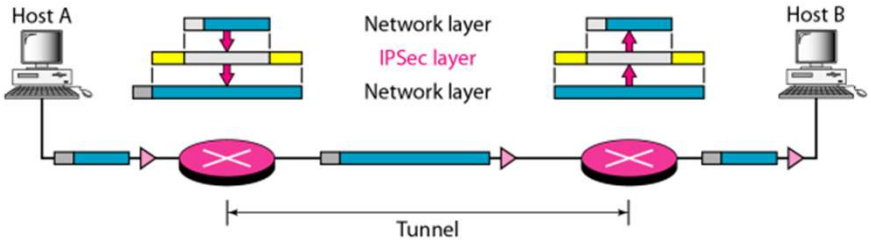
1. Transport Mode

데이터 패킷의 페이로드만 암호화하고 IP 헤더를 원래 형식으로 유지한다.

암호화되지 않은 패킷 헤더를 통해 라우터는 각 데이터 패킷의 대상 주소를 식별.

그래서 가깝고 신뢰할 수 있는 네트워크에서 사용된다.





2. Tunnel Mode

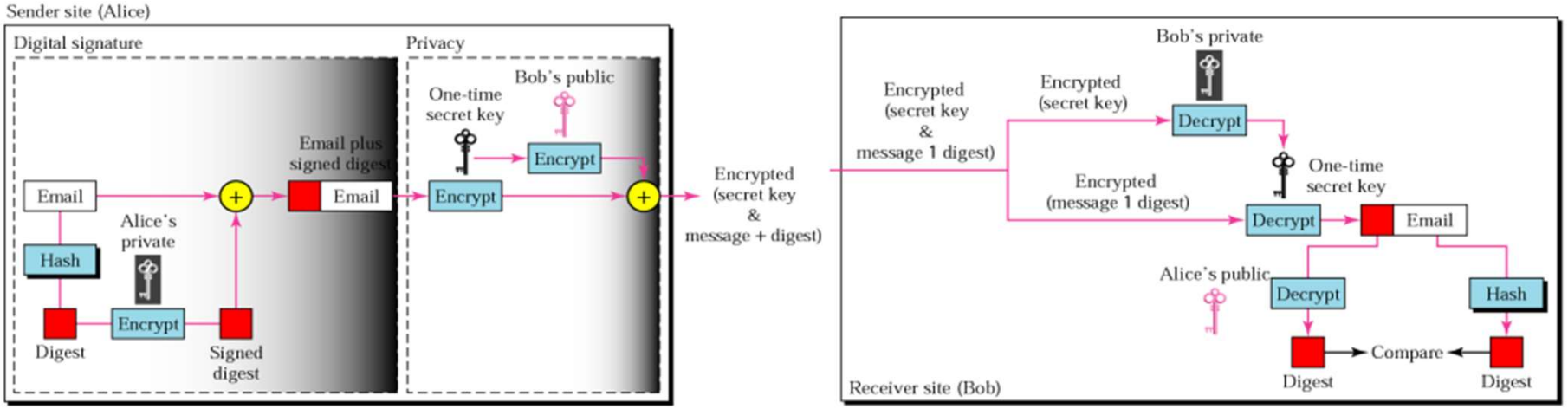
페이로드와 헤더를 포함한 모든 데이터를 암호화하고, 새로운 헤더를 추가한다.

PGP

PGP란?

Pretty Good Privacy의 줄임말로 어플리케이션 계층에 존재하는 보안 프로토콜이다.

PGP는 이메일의 인증과 기밀성을 위해 만들어졌다. → SA처럼 따로 session을 설립할 필요가 없다.

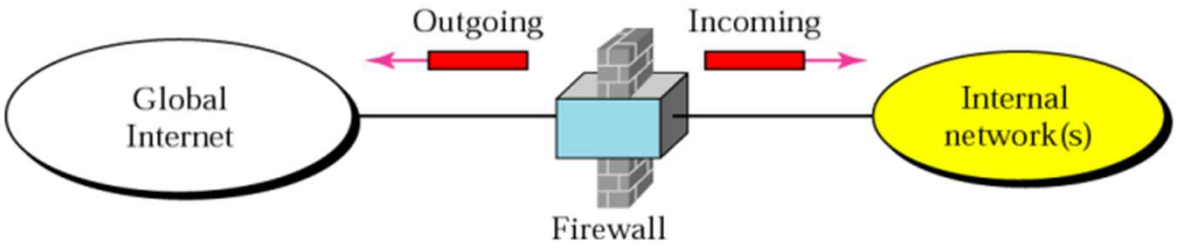


Firewalls

Firewalls(방화벽)이란?

미리 정의된 보안 규칙에 기반한 들어오고 나가는 네트워크 트래픽을 모니터링하고 제어하는 네트워크 보안 시스템이다.

방화벽은 일반적으로 신뢰할 수 있는 내부 네트워크, 신뢰할 수 없는 외부 네트워크 간의 장벽을 구성한다.



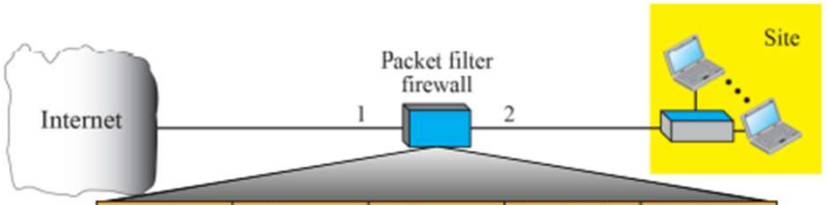
Firewalls

Firewalls(방화벽의)의 종류

Packet-Filter Firewall(Transport layer)

패킷을 검사하여 미리 설정된 정책에 맞지 않을 경우 차단하는 형태의 방화벽을 말한다. 패킷을 다루기 때문에 TCP/IP 네트워크 계층에서 동작하는 방화벽이다.

미리 설정되어 있는 정책만을 검사하기 때문에 더 많은 트래픽을 처리할 수 있는 장점이 있다.



Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	*	*	80

Firewalls

Firewalls(방화벽의)의 종류

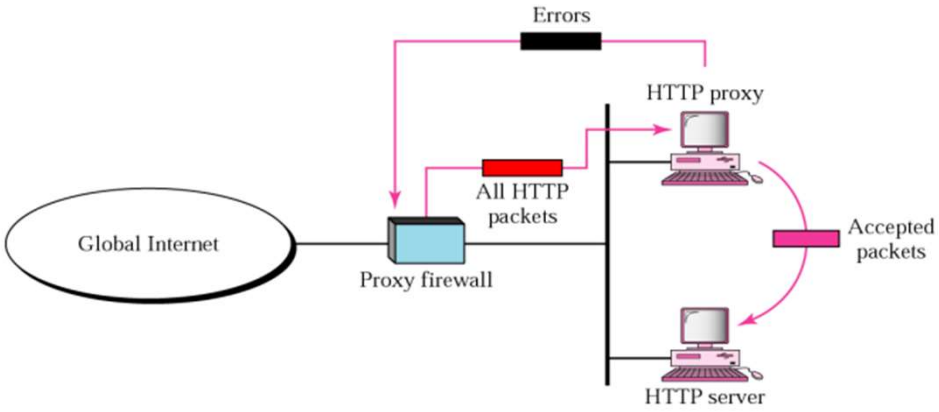
Proxy Firewall(application layer)

세션에 포함되어 있는 정보의 유해성을 검사하기 위해서 방화벽에서 세션을 종료하고 새로운 세션을 형성하는 방식의 방화벽이다.

전송하는 곳에서 받는 곳까지 세션을 가로채서 출발지에서 방화벽까지의 세션과 방화벽에서 목적지까지의 두 세션으로 만든 다음

하나의 세션에서 다른 세션으로 정보를 넘겨주기 전에 검사를 수행하는 형태이다.

패킷 필터에 비해 방화벽에 더 많은 부하를 주어 속도는 느리지만 많은 검사를 수행할 수 있고, 프로토콜 변경 등 추가적인 기능을 수행 가능.



Q & A