TLS/IPSec summary

zaterdag 7 januari 2023 13:45

IPSec

AH: Authentication Header
ESP: Encapsulating Security Payload

Transport mode:

- Used between hosts
- Header is not encrypted (in ESP), but parts of it are authenticated (in AH)
- Only the payload is protected (from destination to destination)

Tunnel mode:

- Entire IP packet is protected (including header) and becomes payload of new IP packet
- Can be used between hosts, gateways, or between host and gateway

A Key Encapsulation Mechanism (KEM) encapsulates the symmetric key used in hybrid encryption using asymmetric cryptography of some sort.

Wireguard is a simple VPN protocol

TLS

Transport Layer Security provides transparency for higher layers and runs on top of TCP.
A TLS record can have different types/protocols:

- Handshake: initiate session, which includes authenticating server & client and establishing keys
- Application: data transfer, which include computing MACs for integrity and encrypting MACs and data
- Alert: alert the other side of exceptional conditions (errors and warnings)

The pre-master secret is the value obtained from the key exchange, which is then used to construct the master secret. When using DH(E) or ECDH(E), the pre-master secret can be described as the result of a Diffie-Hellman key exchange. When using RSA, the pre-master secret is a randomly generated bit-string encrypted by the client for the server.