Solutions: Sheet 9

1. IPsec

(a) Name and briefly explain three protection goals that can be generally achieved by *IPsec*?

- Authenticity
- Confidentiality
- Integrity

(b) Name and briefly explain the two operating modes of IPsec.

- **Transport mode:** The hosts are the endpoints of the communication and have a direct and secure connection.
- **Tunnel mode:** The connection is established by a tunnel between two gateways. Different hosts can be on the gateway using the tunnel. The tunnel between the gateway is secured.
  - Advantage: Many devices but don't need to speak IPSec (endpoint don't need to change, Packet is changed on Gateways)
  - Disadvantage: No End-To-End Connection

2. Security Policy Database (SPD)

A company wants to connect two locations with a VPN based on IPsec. The following figure shows the network architecture with the two locations.

Network A (`10.1.2.0/24`) with gateway GW 1 (internal IP `10.1.2.1`, external IP `10.1.1.2`) is located at the first location.

- Network A contains a web server with IP address `10.1.2.11`.

Network B (`10.1.0.0/24`) with gateway GW 2 (internal IP `10.1.0.1`, external IP `10.1.1.1`) is located at the second location.

- Network B contains clients.

GW 1 and GW 2 have IPsec capabilities.

(a) Which mode and which protocol (AH, ESP) are suitable for this scenario? Name an advantage of tunnel mode compared to transport mode.

The tunnel mode is suitable for it as you connect two gateways instead of two endponts. Advantage is that the gateways already know IPSec, so the clients don't need to know it. Using ESP makes sense as is provides authentication, encryption, integrity checking, providing secure data transfer. ESP alone can used, but a combination of ESP and AH is possible as well. AH is then used for the client authentication.

(b) You now have the task of configuring rules for the *Outbound* Security Policy Database (SPD) for the GW 2. Since there are only two locations, the local IP of the tunnel is the fixed IP 10.1.1.1 (GW 2) and the remote IP of the tunnel is the fixed IP `10.1.1.2` (GW 1).

Create rules for the following requirements and fill in the table below:

- Protection of all HTTP connections (TCP, port `80`) to the web server `10.1.2.11` with `AES-CBC-128` and `HMAC-SHA256`.
- HTTPS connections (TCP, port `443`) to the web server `10.1.2.11` should NOT be double protected.
- IKE traffic (UDP, Port `500`) should not be protected by IPsec and is allowed to be sent anywhere.
- DNS queries (UDP, port `53`) may neither be sent to the Internet nor to network A.

In the table below, Local IP denotes the source IP(s), Remote IP denotes the destination IP(s), Proto denotes the protocols (TCP, UDP), LPort denotes the source port, RPort denotes the destination port and Policy denotes the actions to be taken.

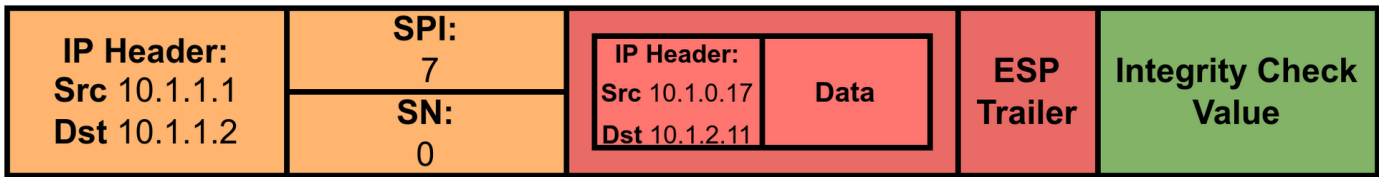
Local IP	Remote IP	Protocol	Local Port	Remote Port	Policy
`10.1.0.0/24`	`10.1.2.11`	`TCP`	ANY	`80`	`PROTECT`: Apply ESP Transport with AES-CBC-128, HMAC-SHA256
`10.1.0.0/24`	`10.1.2.11`	`TCP`	ANY	`443`	`BYPASS`
`10.1.0.0/24`	ANY	`UDP`	`500` (same port used on both sides when using IKE)	`500`	`BYPASS`
`10.1.0.0/24`	ANY	`UDP`	ANY	`53`	`DISCARD`

- `BYPASS`: Direct forwarding of the packet
- `PROTECT`: IPsec must be used, reference to SA (Security Association)
- `DISCARD`: The package is rejected

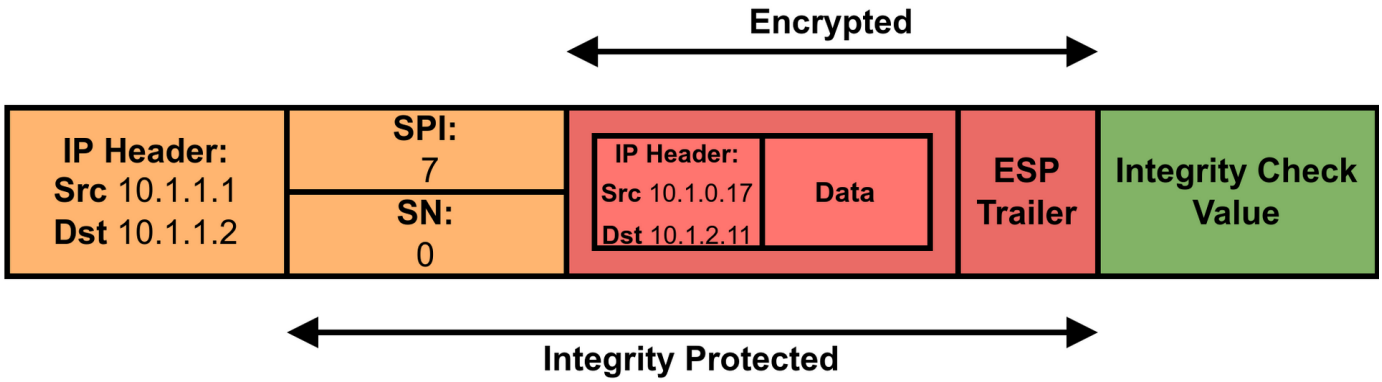
3. IPsec Packet Format

(a) Draw the structure of an IPsec protected IP packet (using the setup of the previous question) with

- Client IP: `10.1.0.17`, Server IP: `10.1.2.11`, SPI: `7` (of SA in SAD), first access



(b) Mark which parts of the package are encrypted and which are integrity protected.



(c) Explain briefly the tasks of the fields SPI and Sequence Number.

- **SPI:** The SPI Value is a 32-bit value which is used to uniqly identify an IPSec Conneciton. (Stored by SA, can get by SAD)
- **Sequence Number:** The sequence number is a 32-bit value, which is increased by one for each packet. Used to check in which order the packets need to arrive.