Lecture NS09 2018

Chapter 20

1. **Q2: What are the benefits of IPsec?**

   A2:slide 8

   1. When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter

   2. IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.

   3. IPsec is below the transport layer (TCP, UDP) and so is transparent to applications.

   4. IPsec can be transparent to end users.
   5. IPsec can provide security for individual users if needed.

2. **Describe IP traffic processing models**

Fig.20.3 and 20.4, pp. 671—673

Q2_A:

IPsec is executed on a packet-by-packet basis. When IPsec is implemented, each outbound IP packet is processed by the IPsec logic before transmission, and each inbound packet is processed by the IPsec logic after reception and before passing the packet contents on to the next higher layer (e.g., TCP or UDP). We look at the logic of these two situations in turn.

Outbound Packets: Figure 20.3 highlights the main elements of IPsec processing for outbound traffic. A block of data from a higher layer, such as TCP, is passed down to the IP layer and an IP packet is formed, consisting of an IP header and an IP body. Then the following steps occur:

1. IPsec searches the SPD for a match to this packet.
2. If no match is found, then the packet is discarded and an error message is generated.
3. If a match is found, further processing is determined by the first matching entry in the SPD. If the policy for this packet is DISCARD, then the packet is discarded. If the policy is BYPASS, then there is no further IPsec processing; the packet is forwarded to the network for transmission.

4. If the policy is PROTECT, then a search is made of the SAD for a matching entry. If no entry is found, then IKE is invoked to create an SA with the appropriate keys and an entry is made in the SA.
5. The matching entry in the SAD determines the processing for this packet. Either encryption, authentication, or both can be performed, and either transport or tunnel mode can be used. The packet is then forwarded to the network for transmission.

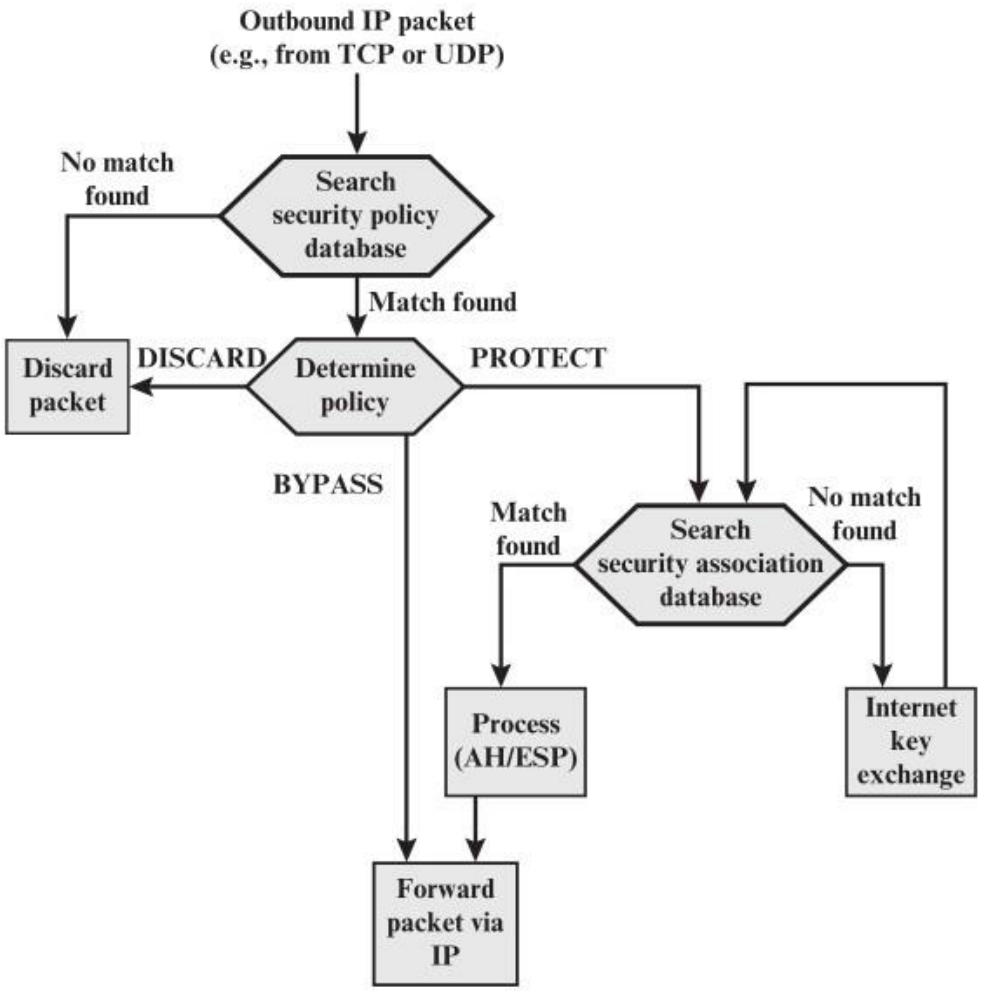


Figure 20.3 Processing Model for Outbound Packets

Inbound Packets: Figure 20.4 highlights the main elements of IPsec processing for inbound traffic. An incoming IP packet triggers the IPsec processing. The following steps occur:

1. IPsec determines whether this is an unsecured IP packet or one that has ESP or AH headers/trailers, by examining the IP Protocol field (IPv4) or Next Header field (IPv6).

2. If the packet is unsecured, IPsec searches the SPD for a match to this packet. If the first matching entry has a policy of BYPASS, the IP header is processed and stripped off and the packet body is delivered to the next higher layer, such as TCP. If the first matching entry has a policy of PROTECT or DISCARD, or if there is no matching entry, the packet is discarded.
3. For a secured packet, IPsec searches the SAD. If no match is found, the packet is discarded. Otherwise, IPsec applies the appropriate ESP or AH processing. Then, the IP header is processed and stripped off and the packet body is delivered to the next higher layer, such as TCP.

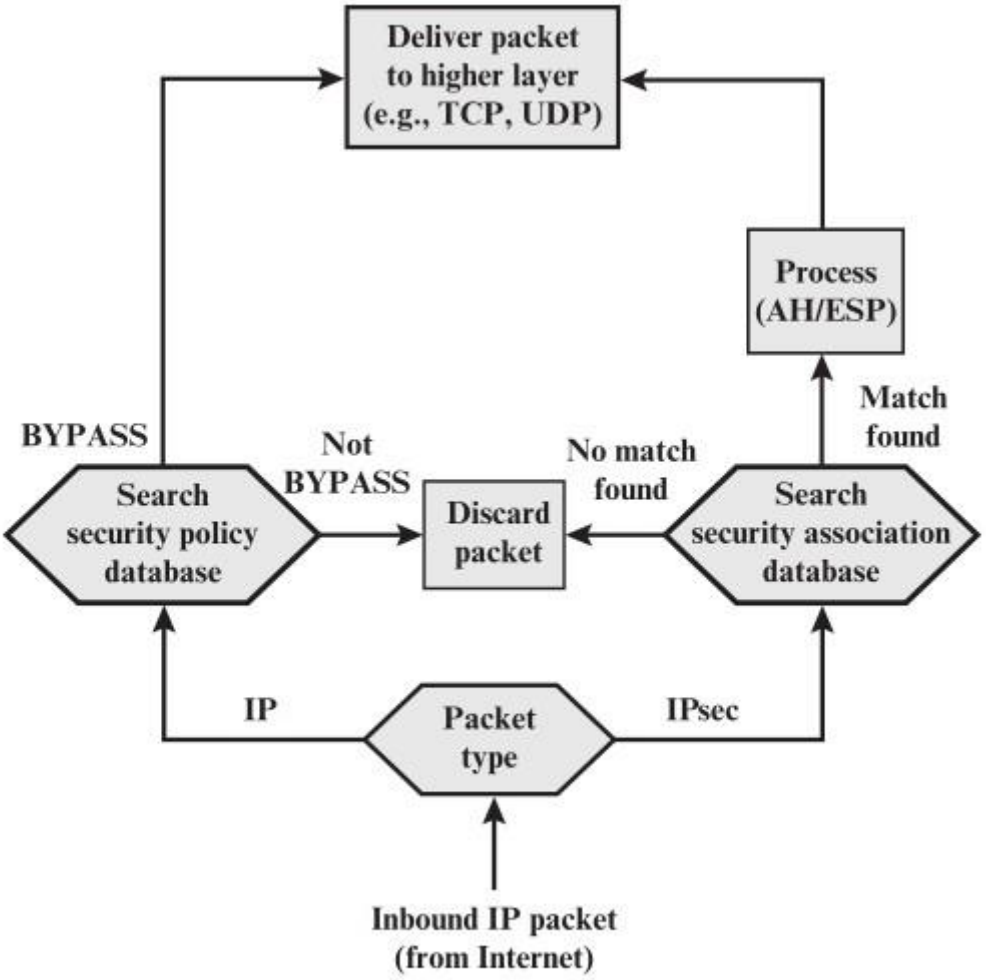


Figure 20.4 Processing Model for Inbound Packets

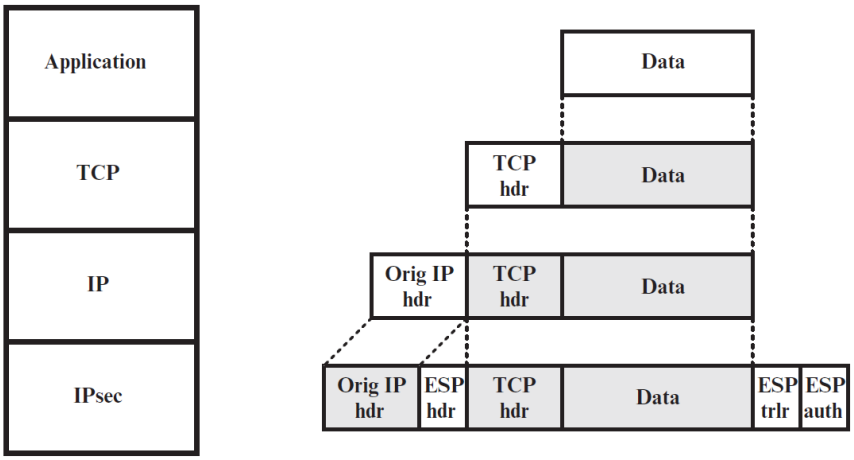
3. Explain basic functions of the Encapsulating Security Payload(ESP)

ESP can be used to provide

- confidentiality,

- data origin authentication,
- connectionless integrity,
- an anti-replay service,
- limited traffic flow confidentiality.
- The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology.

4. Describe the transport and Tunnel modes

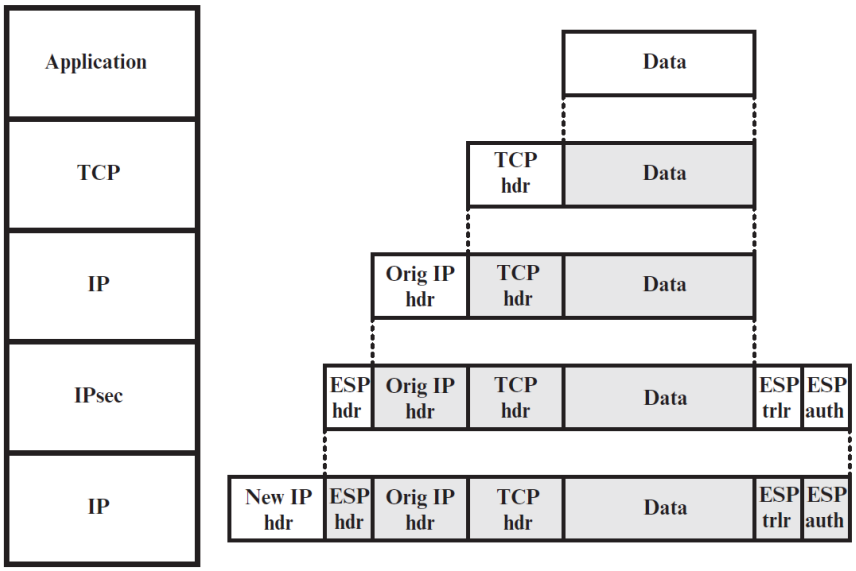


(a) Transport mode

Transport mode operation may be summarized as follows:

1. At the source, the block of data consisting of the ESP trailer plus the entire transport-layer segment is encrypted and the plaintext of this block is replaced with its ciphertext to form the IP packet for transmission. Authentication is added if this option is selected.
2. The packet is then routed to the destination.
3. recover the plaintext transport-layer segment

Whereas the transport mode is suitable for protecting connections between hosts that support the ESP feature, the tunnel mode is useful in a configuration that includes a firewall or other sort of security gateway that protects a trusted network from external networks.



(b) Tunnel mode

The following steps occur for transfer of a transport-layer segment from the external host to the internal host:

1. The source prepares an inner IP packet with a destination address of the target internal host. This packet is prefixed by an ESP header; then the packet and ESP trailer are encrypted and Authentication Data may be added.
2. The outer packet is routed to the destination firewall. Each intermediate router examines and process the outer IP header plus any outer IP extension headers but does not need to examine the ciphertext.
3. The destination firewall examines and processes the outer IP header plus any outer IP extension headers. Then, on the basis of the SPI in the ESP header, the destination node decrypts the remainder of the packet to recover the plaintext inner IP packet. This packet is then transmitted in the internal network.
4. The inner packet is routed through zero or more routers in the internal network to the destination host.

Q1: What are the basic approaches to bundling SAs?

A1:

Transport adjacency: Refers to applying more than one security protocol to the same IP packet, without invoking tunneling. This approach to combining AH and ESP allows for only one level of combination; further nesting yields no added benefit since the processing is

performed at one IPSec instance: the (ultimate) destination.

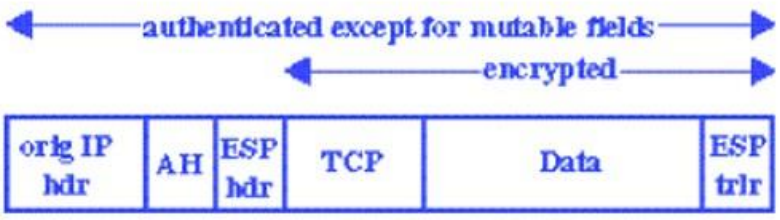
Iterated tunneling: Refers to the application of multiple layers of security protocols effected through IP tunneling. This approach allows for multiple levels of nesting, since each tunnel can originate or terminate at a different IPSec site along the path.

Q2: End-to-end authentication and encryption are desired between two hosts. Draw figures to show each following packet content on the network layer.

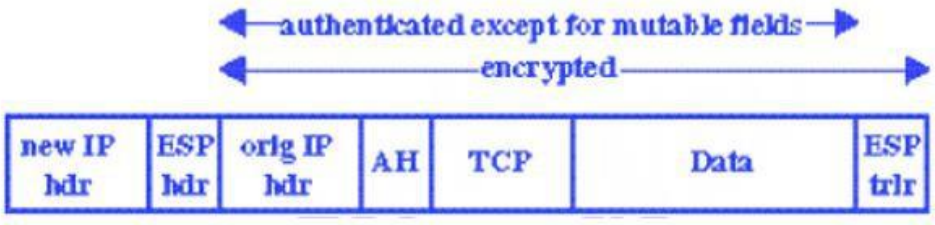
6. **Transport adjacency with encryption applied before authentication.**
7. **A transport SA bundled inside a tunnel SA with authentication applied before encryption.**

A2:

(a)



(b)



Q3: There are a number of weaknesses to Diffie–Hellman. It is vulnerable to a clogging attack and a man-in-the-middle attack. What method does the IKE use to thwart these attacks?

A3:

IKE employs a mechanism known as cookies to thwart clogging attacks.

IKE authenticates the Diffie – Hellman exchange to thwart man-in-the-middle attacks.