

CHAPTER - 8

IP SECURITY



8.1 IP SECURITY OVERVIEW

○ KEY POINTS

- IP security (IPsec) can be added to either current version of the Internet Protocol (IPv4 or IPv6) by means of additional headers.
- IPsec encompasses three functional areas: authentication, confidentiality, and key management.
- Authentication uses of the HMAC message authentication code.
- Authentication can be applied to the entire original IP packet (tunnel mode) or to all of the packet except for the IP header (transport mode).
- Confidentiality is provided by an encryption format known as encapsulating security payload. Both tunnel and transport modes can be accommodated.
- IKE(Internet Key Exchange) defines a number of techniques for key management.

8.1 IP SECURITY OVERVIEW

- In 1994, the Internet Architecture Board (IAB) identified key areas for security mechanisms in a report titled “Security in the Internet Architecture”.
- Some important areas are:
 - Need to secure the network infrastructure from unauthorized monitoring
 - Control of network traffic
 - The need to secure end-user-to-end-user traffic using authentication
 - Encryption mechanisms
- IAB included authentication and encryption as necessary security features in the next-generation IP, IPv6.
- The IPsec specification now exists as a set of Internet Standards.



Applications of IPsec

- IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.
- *Secure branch office connectivity over the Internet.*
 - A company can build a VPN over the internet for the business to rely on internet only saving cost and n/w management overhead.
- *Secure remote access over the Internet.*
 - An end user equipped with IP security protocols can make a local call to an Internet Service Provider (ISP) and gain secure access to a company network reducing the cost of toll charges for traveling employees and telecommuters.



Applications of IPsec

- *Establishing extranet and intranet connectivity with partners.*
 - For secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.
- *Enhancing electronic commerce security.*
 - Even though some Web and electronic commerce applications have built-in security protocol, IPsec guarantees that all designated traffic is both encrypted and authenticated



Applications of IPsec

- The principal feature of IPsec is that it can encrypt and/or authenticate all traffic at the IP level.
- Thus, all distributed applications (including remote logon, client/server, e-mail, file transfer, Web access, and so on) can be secured.



An IP Security Scenario

- Figure 8.1 is a typical scenario of IPsec usage.
- An organization maintains LANs at dispersed locations. Nonsecure IP traffic is conducted on each LAN.
- For traffic offsite through WAN IPsec protocols are used, which operate in networking devices, such as a router or firewall, that connect each LAN to the outside world.
- The IPsec networking device encrypts and compresses all traffic going into the WAN and decrypts and decompresses traffic coming from the WAN.
- For individual users who dial into the WAN, workstations must implement the IPsec protocols to provide security.



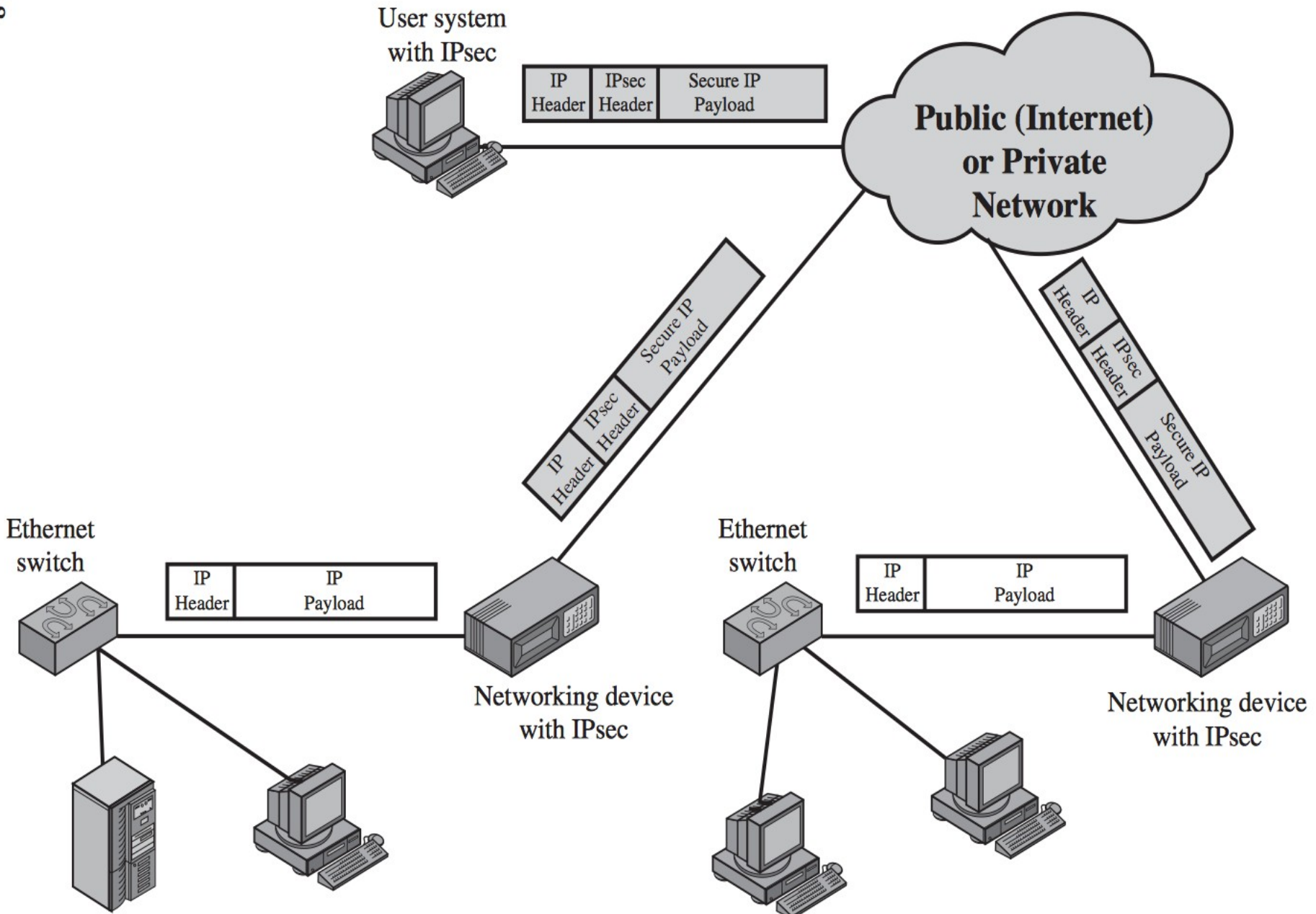


Figure 19.1 An IP Security Scenario

Benefits of IPsec

- IPsec provides strong security that can be applied to all traffic crossing the perimeter (Firewall or router).
- Traffic within a company or workgroup does not incur the overhead of security-related processing.
- 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.
- IPsec is below the transport layer (TCP, UDP) and so is transparent to applications so upper-layer software, including applications, is not affected.
- There is no need to change software on a user or server system when IPsec is implemented in the firewall or router.



Benefits of IPsec

- IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.
- IPsec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.



Routing Applications

- IPsec can play a vital role in the routing architecture required for internetworking. [HUIT98] lists the following examples of the use of Ipsec. IPsec can assure that:
 - A router advertisement (a new router advertises its presence) comes from an authorized router.
 - A neighbor advertisement (a router seeks to establish or maintain a neighbor relationship with a router in another routing domain) comes from an authorized router.
 - A redirect message comes from the router to which the initial IP packet was sent.
 - A routing update is not forged.
- Without such security measures, an opponent can disrupt communications or divert some traffic.



IPsec Documents

- IPsec encompasses three functional areas: authentication, confidentiality, and key management.
- The totality of the IPsec specification is scattered across dozens of RFCs and draft IETF(Internet Engineering Task Force) documents making it difficult to grasp.
- The documents can be categorized into the following groups.
- **Architecture:** Covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology. The current specification is RFC 4301, *Security Architecture for the Internet Protocol*.



IPsec Documents

- **Authentication Header (AH):** AH is an extension header for message authentication. The current specification is RFC 4302, *IP Authentication Header*.
- Because message authentication is provided by ESP, the use of AH is deprecated. It is included in IPsecv3 for backward compatibility but should not be used in new applications.
- **Encapsulating Security Payload (ESP):** an encapsulating header and trailer used to provide encryption or combined encryption/authentication.
- The current specification is RFC 4303, *IP Encapsulating Security Payload (ESP)*.




IPsec Documents

- **Internet Key Exchange (IKE):** A collection of documents describing the key management schemes. The main specification is RFC 4306, Internet Key Exchange (IKEv2) Protocol, but there are a number of related RFCs.
- **Cryptographic algorithms:** A large set of documents that define and describe cryptographic algorithms for encryption, message authentication, pseudorandom functions (PRFs), and cryptographic key exchange.
- **Other:** There are a variety of other IPsec-related RFCs, including those dealing with security policy and management information base (MIB) content.



IPsec Services

- IPsec provides security services by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.
 - Two protocols are used to provide security: an authentication protocol and a combined encryption/authentication protocol.
 - RFC 4301 lists the following services:
 - Access control
 - Connectionless integrity
 - Data origin authentication
 - Rejection of replayed packets (a form of partial sequence integrity)
 - Confidentiality (encryption)
 - Limited traffic flow confidentiality
- 

Transport and Tunnel Modes

- Both AH and ESP support two modes of use: transport and tunnel mode.
- **Tunnel Mode:** After the AH or ESP fields are added to the IP packet, the entire packet plus security fields is treated as the payload of new outer IP packet with a new outer IP header.
- The entire original, inner, packet travels through **a tunnel** from one point of an IP network to another; no routers along the way are able to examine the inner IP header.
- Tunnel mode is used when one or both ends of a security association (SA) are a security gateway, such as a firewall or router that implements IPsec.
- With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications without implementing Ipsec.
- ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header.
- AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header.

Transport and Tunnel Modes

Table 8.1 Tunnel Mode and Transport Mode Functionality

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.



Transport and Tunnel Modes

- **Transport Mode:** Provides primary protection to upper-layer protocols, for end-to-end communication between two hosts.
- When a host runs AH or ESP over IPv4, the payload is the data that normally follow the IP header.
- For IPv6, the payload is the data that follow both the IP header and any IPv6 extensions headers, with the possible exception of the destination options header, which may be included in the protection.
- ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header.
- AH in transport mode authenticates the IP payload and selected portions of the IP header.

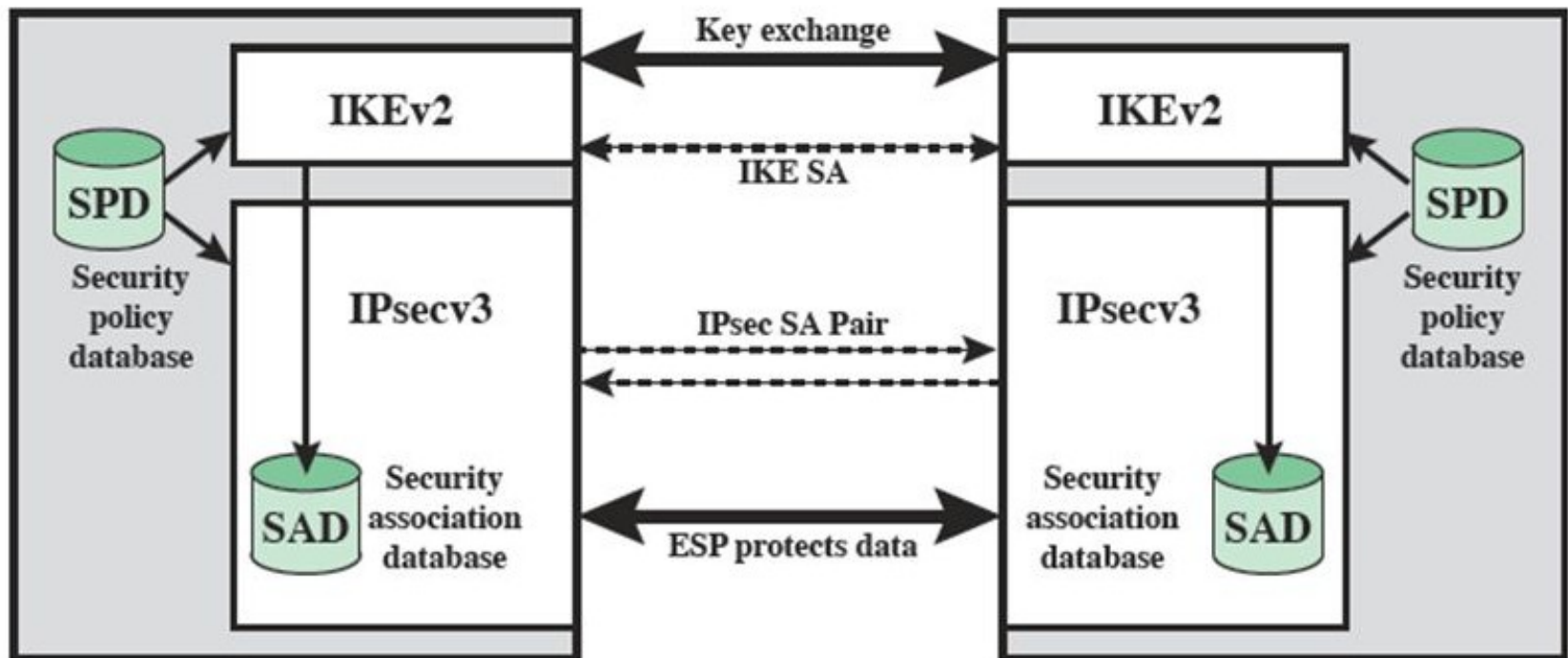


8.2 IP SECURITY POLICY

- IPsec is the concept of a security policy applied to each IP packet that transits from a source to a destination.
- IPsec policy is determined by the interaction of two databases, the security association database (**SAD**) and the security policy database (**SPD**).
- **Security Associations**
- Security association (SA) is key to both the authentication and confidentiality mechanisms for IP.
- An association is a one-way logical connection between a sender and a receiver that affords security services to the traffic carried on it.
- If a peer relationship is needed for two-way secure exchange, then two security associations are required



Figure 8.2 IPsec Architecture



IP SECURITY POLICY

- A security association is uniquely identified by three parameters.
- **Security Parameters Index (SPI):** A bit string assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
- **IP Destination Address:** This is the address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router.
- **Security Protocol Identifier:** This field from the outer IP header indicates whether the association is an AH or ESP security association.



Security Association Database

- A security association is normally defined by the following parameters in an SAD entry.
- **Security Parameter Index:** A 32-bit value to uniquely identify the SA. In a SAD entry for an outbound SA, the SPI is used to construct the packet's AH or ESP header and for an inbound SA, the SPI is used to map traffic to the appropriate SA.
- **Sequence Number Counter:** A 32-bit value used to generate the Sequence Number field in AH or ESP headers (required for all implementations).



Security Association Database

- **Sequence Counter Overflow:** A flag indicating whether overflow of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on this SA (required for all implementations).
- **Anti-Replay Window:** Used to determine whether an inbound AH or ESP packet is a replay (required for all implementations).
- **AH Information:** Authentication algorithm, keys, key lifetimes, and related parameters being used with AH (required for AH implementations).



Security Association Database

- **ESP Information:** Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP (required for ESP implementations).
- **Lifetime of this Security Association:** A time interval or byte count after which an SA must be replaced with a new SA (and new SPI) or terminated (required for all implementations).
- **IPsec Protocol Mode:** Tunnel, transport, or wildcard.
- **Path MTU:** Any observed path maximum transmission unit and aging variables (required for all implementations).



Security Policy Database

- The means by which IP traffic is related to specific SAs (or no SA in the case of traffic allowed to bypass IPsec) is the nominal Security Policy Database (SPD).
- SPD contains entries, each of which defines a subset of IP traffic and points to an SA for that traffic.
- Each SPD entry is defined by a set of IP and upper-layer protocol field values, called *selectors*.
- These selectors are used to filter outgoing traffic in order to map it into a particular SA.



Security Policy Database

- Outbound processing obeys the following general sequence for each IP packet.
 1. Compare the values of the appropriate fields in the packet (the selector fields) against the SPD to find a matching SPD entry, which will point to zero or more SAs.
 2. Determine the SA if any for this packet and its associated SPI.
 3. Do the required IPsec processing (i.e., AH or ESP processing).



Security Policy Database

- The following selectors determine an SPD entry:
- **Remote IP Address:** A single IP address, an enumerated list or range of addresses, or a wildcard (mask) address.
- **Local IP Address:** A single IP address, an enumerated list or range of addresses, or a wildcard (mask) address.
- **Next Layer Protocol:** The IP protocol header (IPv4, IPv6, or IPv6 Extension) includes a field (Protocol for IPv4, Next Header for IPv6 or IPv6 Extension) that designates the protocol operating over IP.
- This is an individual protocol number, ANY, or for IPv6 only, OPAQUE. If AH or ESP is used, then this IP protocol header immediately precedes the AH or ESP header in the packet.



Security Policy Database

- **Name:** A user identifier, not a field in the IP or upper-layer headers but is available if IPsec is running on the same operating system as the user.
- **Local and Remote Ports:** These may be individual TCP or UDP port values, an enumerated list of ports, or a wildcard port.



Host SPD Example

Table 8.2 Host SPD Example

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

- The entries in the SPD should be self-explanatory. For example, UDP port 500 is the designated port for IKE.
- Any traffic from the local host to a remote host for purposes of an IKE exchange bypasses the IPsec processing.

Host SPD Example

- An SPD on a host system (as opposed to a network system such as a firewall or router) reflects the following configuration:
- A local network configuration consists of two networks.
- The basic corporate network configuration has the IP network number 1.2.3.0/24.
- The local configuration also includes a secure LAN, often known as a DMZ, that is identified as 1.2.4.0/24.
- The DMZ is protected from both the outside world and the rest of the corporate LAN by firewalls.
- The host in this example has the IP address 1.2.3.10, and it is authorized to connect to the server 1.2.4.10 in the DMZ.



IP Traffic Processing

- IPsec is executed on a packet-by-packet basis.
- With IPsec, 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.



IP Traffic Processing

- **OUTBOUND PACKETS** Figure 8.3 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.
 - 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.



IP Traffic Processing

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.



Processing Model for Outbound Packets

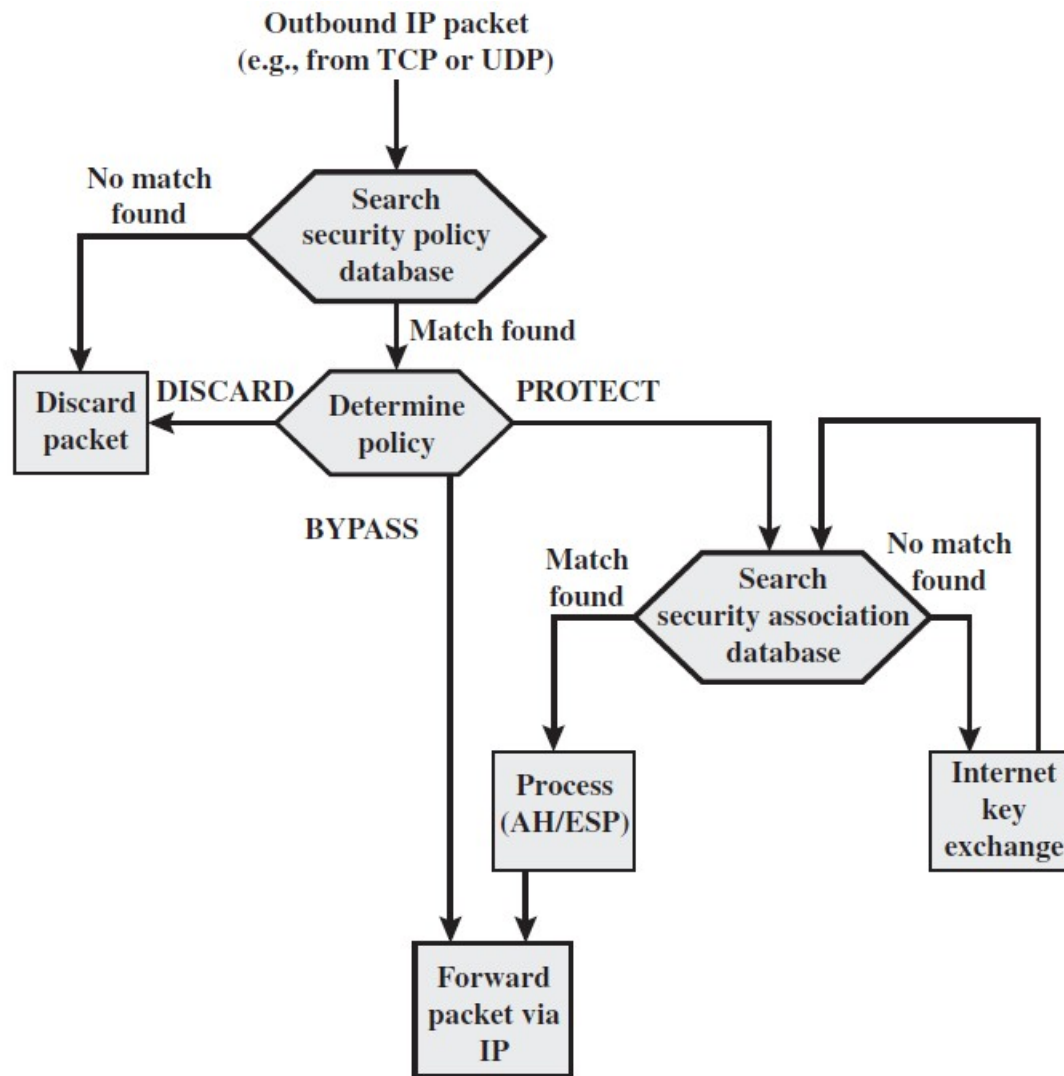


Figure 8.3 Processing Model for Outbound Packets

IP Traffic Processing

- **INBOUND PACKETS** Figure 8.4 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.



IP Traffic Processing

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.



Processing Model for Inbound Packets

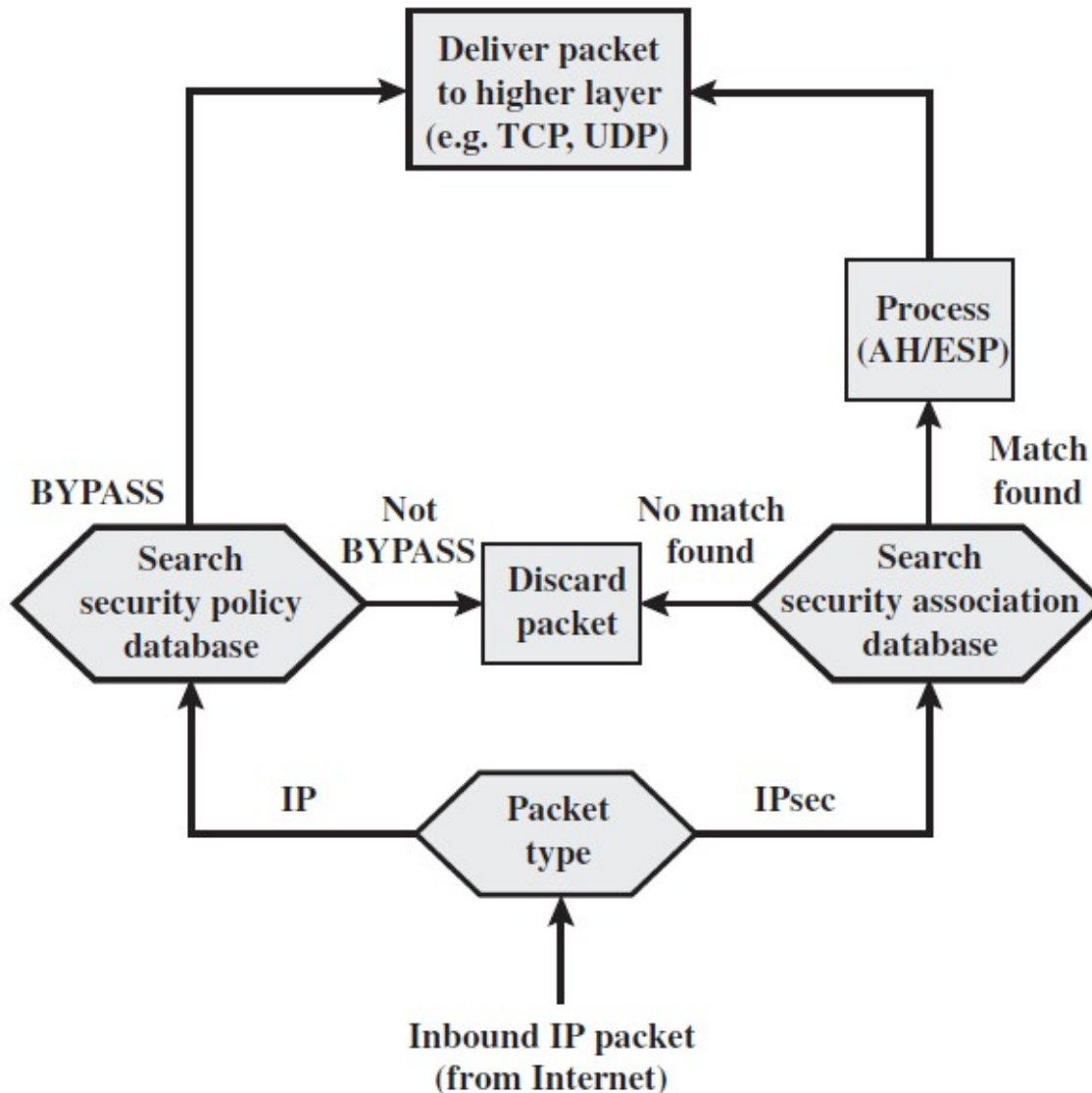


Figure 8.4 Processing Model for Inbound Packets

8.3 ENCAPSULATING SECURITY PAYLOAD

- ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality.
- The set of services provided to the time of Security Association (SA) establishment and on the location of the implementation in a network topology.
- ESP can work with a variety of encryption and authentication algorithms, including authenticated encryption algorithms such as GCM.



ESP Format

- An ESP packet contains the following fields.
- *Security Parameters Index (32 bits)*: Identifies a security association.
- *Sequence Number (32 bits)*: A monotonically increasing counter value; this provides an anti-replay function, as discussed for AH.
- *Payload Data (variable)*: This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
- *Padding (0-255 bytes)*: The purpose of this field is discussed later.



ESP Format

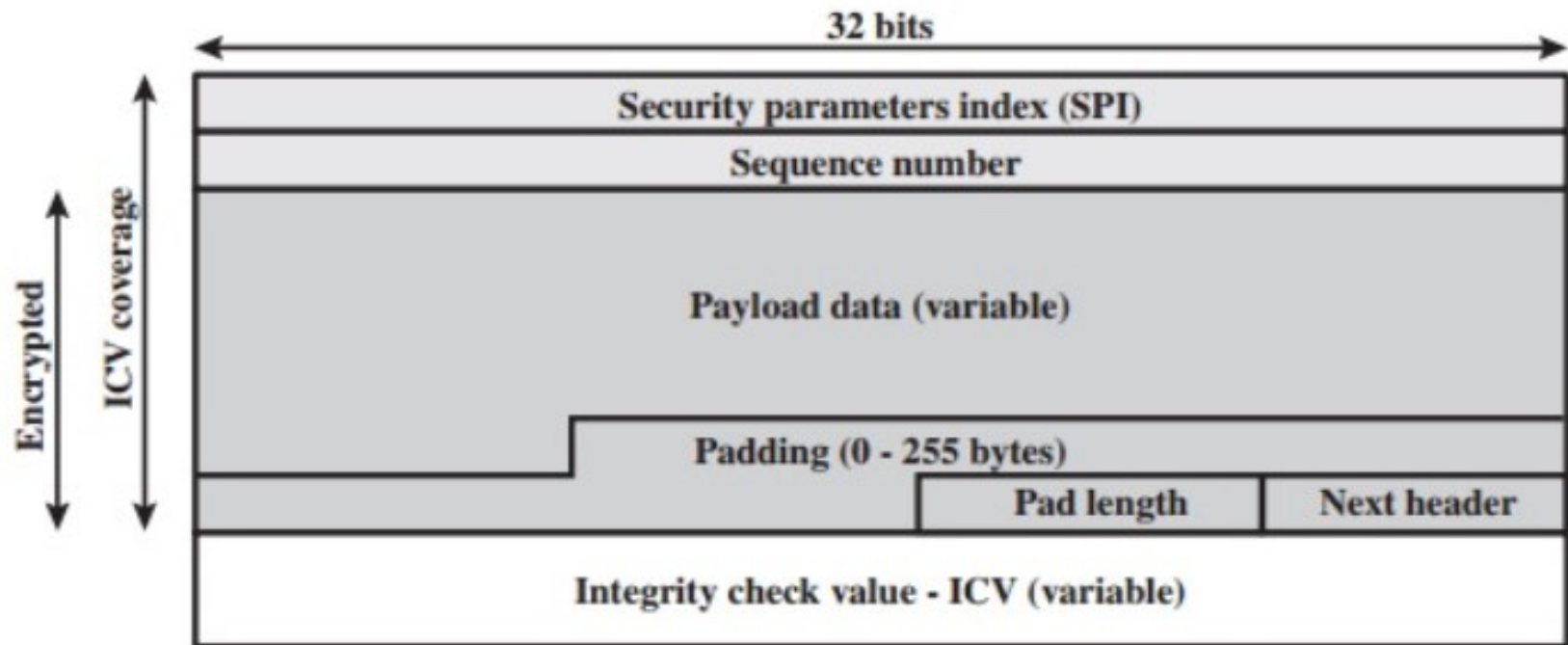
- *Pad Length (8 bits)*: Indicates the number of pad bytes immediately preceding this field.
- *Next Header (8 bits)*: Identifies the type of data contained in the payload data field by identifying the first header in that payload (for example, an extension header in IPv6, or an upper-layer protocol such as TCP).
- *Integrity Check Value (variable)*: A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field.



ESP Format

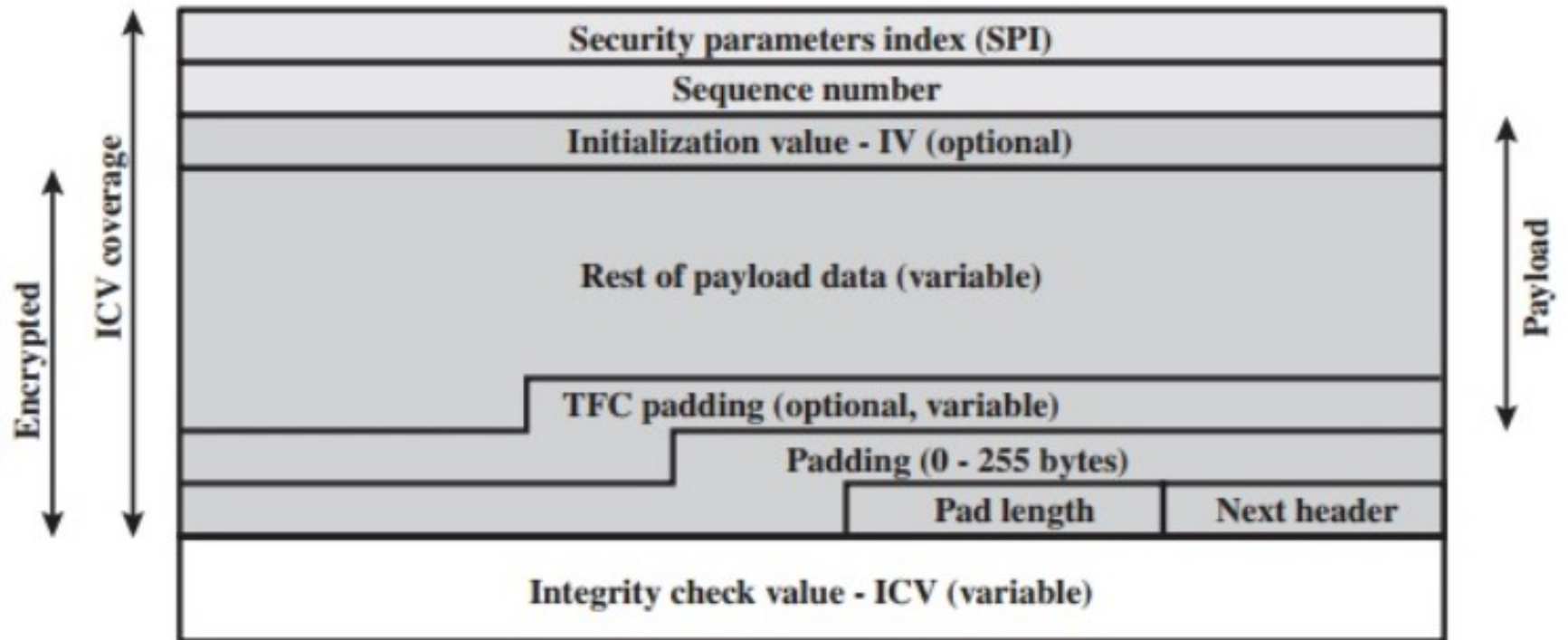
- Two additional fields may be present in the payload (Figure 8.5b).
- An initialization value (IV), or nonce, is present if this is required by the encryption or authenticated encryption algorithm used for ESP.
- If tunnel mode is being used, then the IPsec implementation may add traffic flow confidentiality (TFC) padding after the Payload Data and before the Padding field, as explained subsequently.





(a) Top-level format of an ESP Packet





(b) Substructure of payload data



Encryption and Authentication Algorithms

- The Payload Data, Padding, Pad Length, and Next Header fields are encrypted by the ESP service.
- If the algorithm used to encrypt requires cryptographic synchronization data, such as an initialization vector (IV), then these data may be carried explicitly at the beginning of the Payload Data field.
- If included, an IV is usually not encrypted.
- The ICV field is optional used only if the integrity service is selected.
- The ICV is computed after the encryption is performed.
- This order of processing facilitates rapid detection and rejection of replayed or bogus packets by the receiver prior to decrypting the packet, reducing the impact of denial of service (DoS) attacks.



Padding

- If an encryption algorithm requires the plaintext to be a multiple of some number of bytes (e.g., the multiple of a single block for a block cipher), the Padding field is used to expand the plaintext (consisting of the Payload Data, Padding, Pad Length, and Next Header fields) to the required length.
- The ESP format requires that the Pad Length and Next Header fields be right aligned within a 32-bit word. Equivalently, the ciphertext must be an integer multiple of 32 bits. The Padding field is used to assure this alignment.
- Additional padding may be added to provide partial traffic-flow confidentiality by concealing the actual length of the payload.



Anti-Replay Service

- A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination.
- The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence.
- The Sequence Number field is designed to thwart such attacks.
- For every new SA the sender initializes a sequence number counter to 0. Each time that a packet is sent on this SA, the sender increments the counter and places the value in the Sequence Number field.
- If anti-replay is enabled (the default), the sender must not allow the sequence number to cycle past $2^{32} - 1$ back to zero.
- Otherwise, there would be multiple valid packets with the same sequence number.
- If the limit of $2^{32} - 1$ is reached, the sender should terminate this SA and negotiate a new SA with a new key.



Anti-Replay Service

- Because IP is a connectionless, the IPsec authentication document dictates that the receiver should implement a window of size W , with a default of $W=64$.
- The right edge of the window represents the highest sequence number, N , so far received for a valid packet.
- For any packet with a sequence number in the range from $N - W + 1$ to N that has been correctly received (i.e., properly authenticated), the corresponding slot in the window is marked.

