USN | | | | | | | | | | |

Internal Assessment Test 2 – June. 2022

Sub:	Network Security					Sub Code:	18EC821	Branch:	ECE	
Date:	04-06-22	Duration:	90 min's	Max Marks:	50	Sem / Sec:	8 – A, B, C, D		OBE	
Answer any FIVE FULL Questions								MARKS	CO	RBT

1.	List the major security services provided by AH and ESP.	[10]	CO3	L1
2.	Explain with the help of neat diagrams the IP Traffic Processing.	[10]	CO3	L2
3.	List and explain the IPsec documents and IPsec services.	[10]	CO3	L1
4.	What is the difference between transport mode and tunnel mode?	[10]	CO3	L2
5.	Why does ESP include a padding field?	[10]	CO3	L2
6.	Infer with the help of neat diagrams: The SSH Connection Protocol.	[10]	CO2	L2
7.	Illustrate Encapsulating Security Payload (ESP) format.	[10]	CO3	L3
8.	Explain with the help of neat diagrams the SSH Transport Layer Protocol Packet Exchange.	[10]	CO2	L2

USN | | | | | | | | | | |

Internal Assessment Test 1 – May. 2022

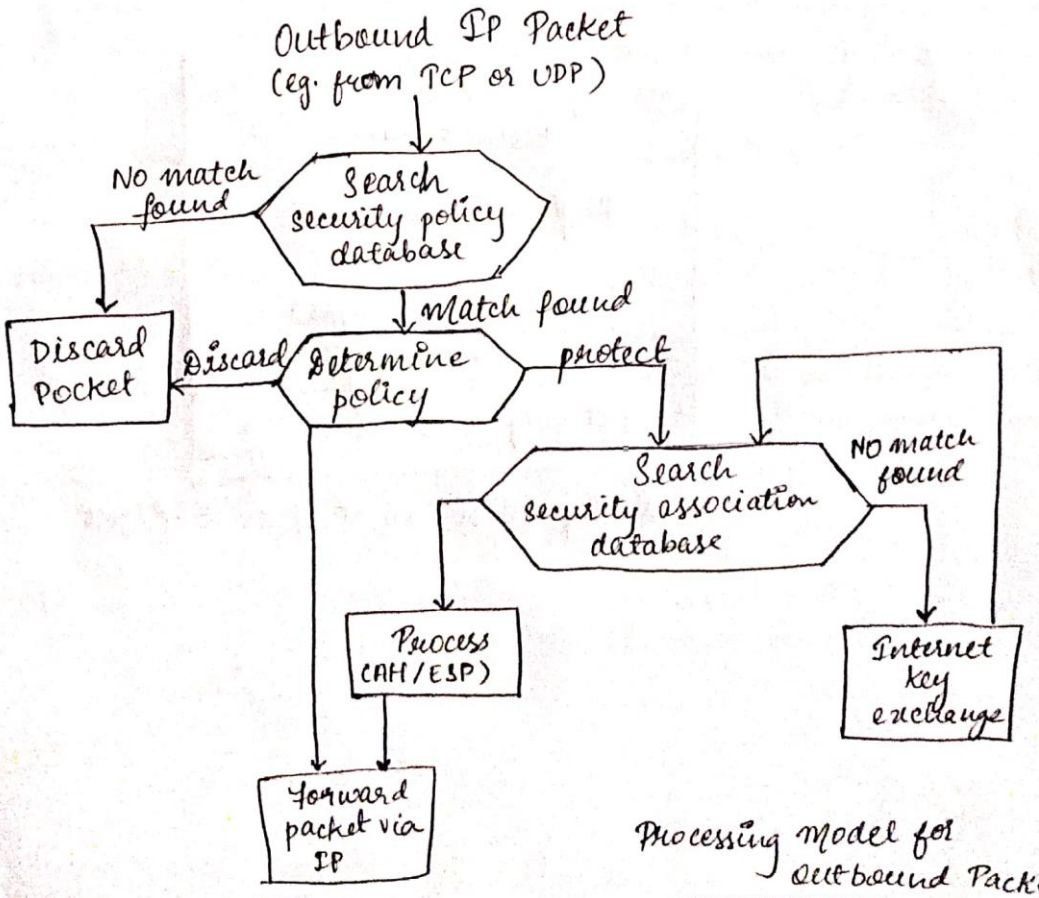
Sub:	Network Security					Sub Code:	18EC821	Branch:	ECE	
Date:	04-06-22	Duration:	90 min's	Max Marks:	50	Sem / Sec:	8 – A, B, C, D		OBE	
Answer any FIVE FULL Questions								MARKS	CO	RBT

1.	List the major security services provided by AH and ESP.	[10]	CO3	L1
2.	Explain with the help of neat diagrams the IP Traffic Processing.	[10]	CO3	L2
3.	List and explain the IPsec documents and IPsec services.	[10]	CO3	L1
4.	What is the difference between transport mode and tunnel mode?	[10]	CO3	L2
5.	Why does ESP include a padding field?	[10]	CO3	L2
6.	Infer with the help of neat diagrams: The SSH Connection Protocol.	[10]	CO2	L2
7.	Illustrate Encapsulating Security Payload (ESP) format.	[10]	CO3	L3
8.	Explain with the help of neat diagrams the SSH Transport Layer Protocol Packet Exchange.	[10]	CO2	L2

2. Explain with the help of neat diagrams the IP Traffic Processing.

Ans IP 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.

OUTBOUND PACKETS Figure highlights the main elements of the 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:



Processing Model for Outbound Packets

1. IP sec 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.

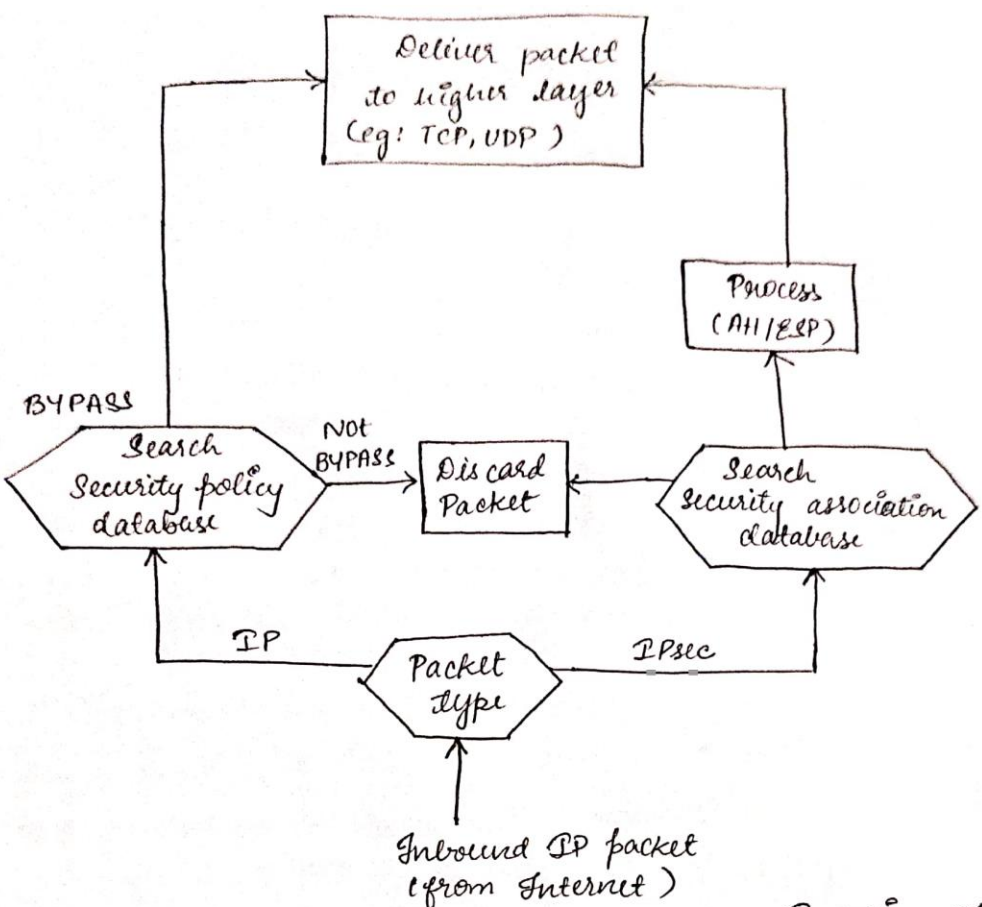
4. If the policy is PROTECT, then a search is made of the SAD for a matching entry. If no entry is found, then IKE is invoked to create an SA with the appropriate keys and an entry is made in the SA.

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.

INBOUND PACKETS

Figure below 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 (IPv6)



Processing Model for Inbound Packets

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 ~~the~~ 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 pckt body is delivered to the next higher layer such as TCP.

4. What is the difference between transport mode and tunnel mode?

Both AH and ESP support two modes of use: transport and tunnel mode.

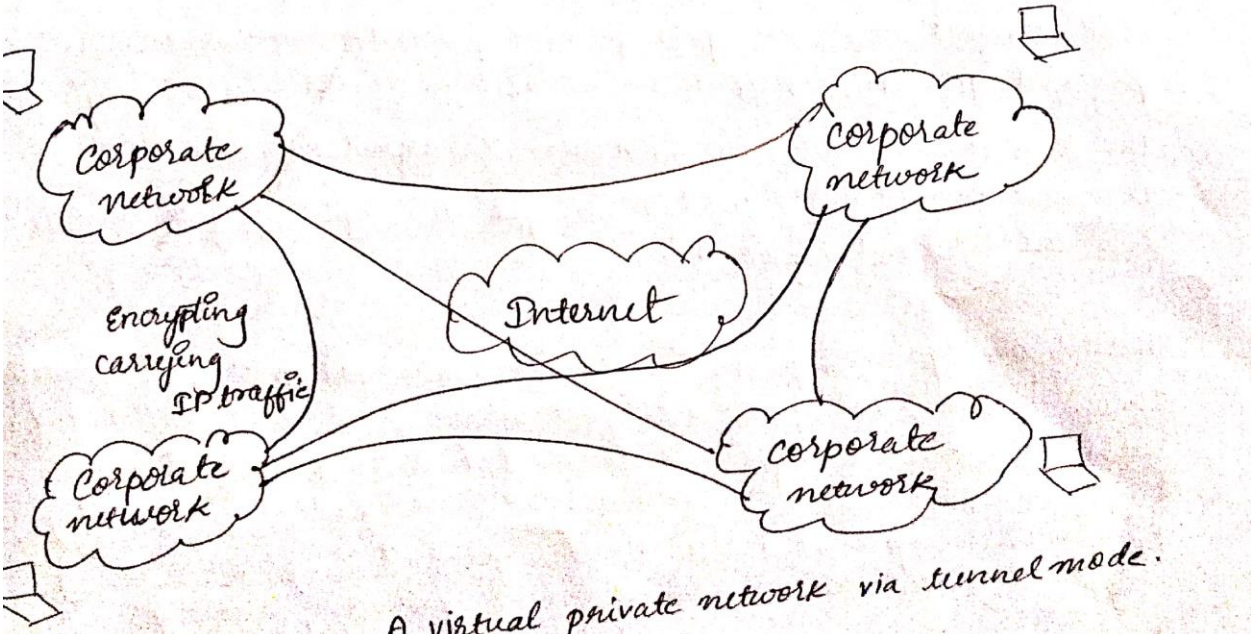
TRANSPORT MODE: It provides protection primarily for upper layer protocols. This is, transport mode protection extends to the payload of an IP packet.
Typically, transport mode is used for end-to-end communication between two hosts (eg: a client and a server, or two workstation when a host runs AH or ESP over IPv4, the payload is the data that normally follow the IP header.

ESP in transport mode encrypts optionally authenticates the IP payload. AH in transport mode authenticates the IP payload and selected portions of the IP header. Transport Mode ESP
Transport Mode ESP is used to encrypt and optionally authenticate the data carried by IP.

Tunnel mode provides protection to the entire IP packet. To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet + security fields is treated as the payload of new outer IP packet with a new outer IP header, because the original packet is encapsulated, the new, larger pckt may have totally diff source & destination addresses, adding to the security.

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. ESP in tunnel mode encrypts and optionally authenticates the entire 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 Mode SA	Tunnel Mode SA
AH	Authenticates IP payload & selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP pckt (inner header + IP payload) + selected portion of outer IP header & outer IPv6 extension headers.
ESP	Encrypts IP payload & any IPv6 extension headers following the ESP header	Encrypts entire inner IP pckt
ESP with authentication	encrypts IP payload & any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header	encrypts entire inner IP pckt. authenticates inner IP pckt.



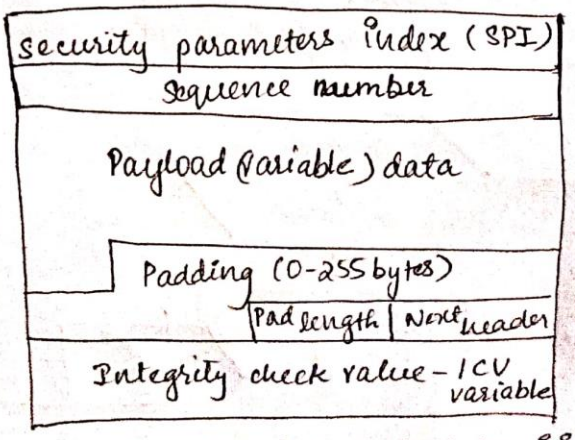
A virtual private network via tunnel mode.

5. Why does ESP include a padding field?

The padding field serves several purposes:

- If an encryption algorithm requires the plaintext to be a multiple of some no. of bytes (eg. the multiple of a single block for a block cipher), the Padding fields are 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 Heade fields be right aligned within a 32-bit word. Equivalently, the ciphet text must be an integer multiple of 32 bits. The Padding field is used to assu this alignment.

Additional padding maybe added to provide partial traffic-flow confidentiality by concealing the actual length of the payload.



(a) Top-Level format of an ESP Pckt

8. SSH Transport Layer Protocol Packet Exchanges

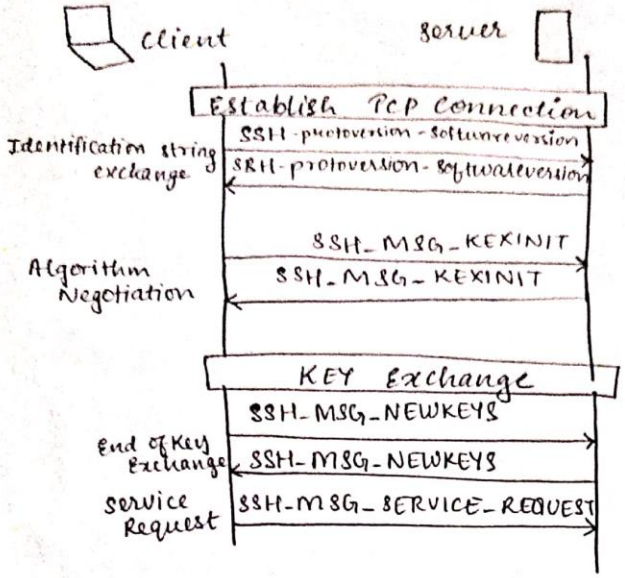
First, the client establishes a TCP connection to the server, which is done via the TCP protocol, and it is not part of the Transport Layer Protocol. Once the connection is established, the client and server exchange data, referred to as packets, in the data field of a TCP segment.

- First step in pckt exchange is identification string exchange, begins with the client sending a pckt with an identification string of the form.

SP - Space character
CR - Carriage Return
LF - Line Feed

SSH protoversion - softwareversion SP comments CR LF

- Algorithm Negotiation, each side sends an SSH_MSG_KEXINIT containing lists of supported algorithms in the order of preference to the sender. There is one list for each type of cryptographic algorithm. The algorithm includes key exchange, encryption, MAC algorithm, and compression algorithm.
- Key Exchange - The specification allows for alternative methods for key exchange but at present, only two versions of Diffie Hellman key exchange are specified. Both versions are defined in RFC 2409 & require only one pckt in each direction
- The end of key exchange is signaled by the exchange of SSH_MSG_NEWKEYS pckts.
- Service Request - Client sends an SSH_MSG_SERVICE_REQUEST pckt to request either the User Authentication or the Connection Protocol. All data is exchanged as the payload of an SSH transport layer pckt, protected by encryption and MAC.

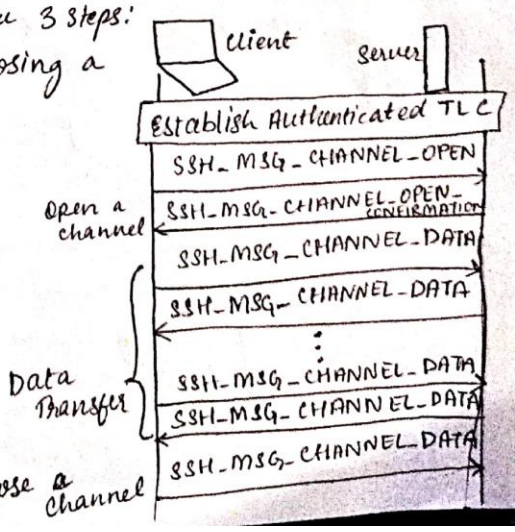


6. SSH Connection Protocol

- SSH Connection Protocol runs on top of the SSH TLP and assumes that a secure authentication is in use
- The secure authentication connection (tunnel) is used by the Connection Protocol to multiplex a no. of logical channels.

Chanel Mechanism

- All types of communication using SSH are supported using separate channels
- Either side may open a channel
- For each channel, each side associates a unique channel no.
- Channels are flow controlled using a window mechanism
- No data maybe sent to a channel until a msg is rcvd to indicate that window space is available
- The life of a channel progresses thru 3 steps:
  → Opening a channel, data transfer, closing a channel.



7. Illustrate Encapsulating Security Payload (ESP) format.

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 depends on options selected at 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.

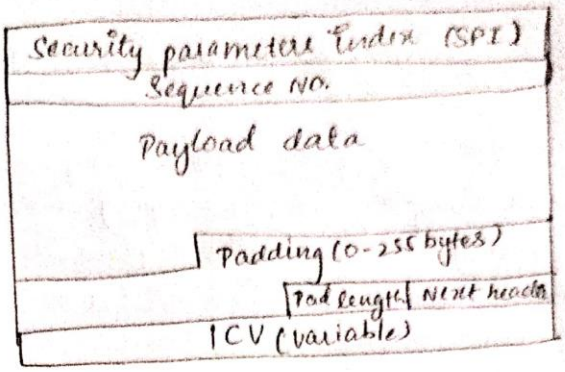
ESP format

The below format shows the top-level format of an ESP packt. It 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 transported - level segment (transp mode) or IP pckt (tunnel mode) that is protected by encryption.
- Padding (0-255 bytes) : The purpose of
- Pad length (8 bits) : Indicates the no. of pad bytes immediately preceding this field.
- Next Header (8 bits) : Identifies the type of data contained in the payload data field

Integrity Check Value : A variable length field that contains ICV computed over the ESP pckt minus the ~~auth~~ AD field

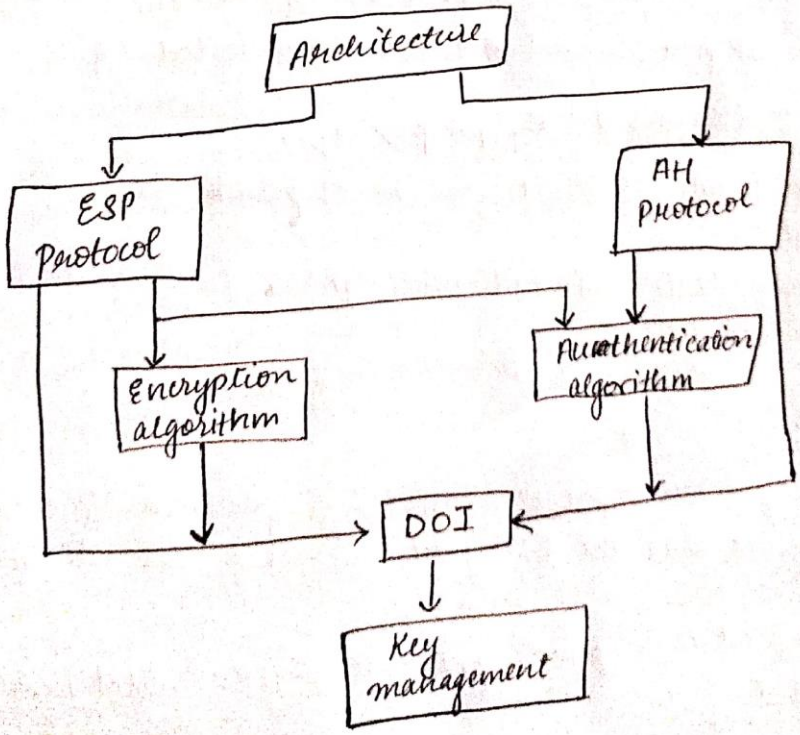
The payload data, padding, pad length, and Next Header fields are encrypted by the ESP service.



3. IPsec documents and IPsec services

IPsec documents

- Encompasses three functional areas: authentication, confidentiality and key management.
- Totality of the IPsec specification is scattered across dozens of RFCs and draft IETF documents, making this the most complex & difficult to grasp of all IETF specification.
- The best way to grasp the scope of IPsec is to consult the latest version of the IPsec document roadmap.



The documents can be categorized into the following grps:-

- 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.
- ENCAPSULATING SECURITY PAYLOAD (ESP) : Covers the pckt format & general issues related to the use of the ESP for pckt encryption & authentication.
- AUTHENTICATION HEADER (AH) : Covers the pckt format & general issues related to the use of AH for pckt authentication.
- ENCRYPTION ALGORITH : A set of documents that describe how various encryption algorithms are used for ESP.
- AUTHENTICATION ALGORITHM : A set of docs that describe how various authentication algorithms are used for AH & for the authentication option of ESP.
- KEY MANAGEMENT : Documents that describe key management schemes.
- DOMAIN OF INTERPRETATION (DOI) : Contains values needed for the other docs to relate to each other.
These include identifiers for approved encryption and authentication algorithms as well as operational parameters such as key lifetime.

IP Sec Services

- IP sec services provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s) and put in any place any cryptographic keys required to provide the requested services.
Two protocols are used to provide security : an authentication protocol designed by the header of the protocol. Authentication Header and a combined encryption/authentication protocol designated by the format of the pckt for that protocol Encapsulating Security Payload (ESP).

The services are:

→ Access control
→ Connectionless Integrity
→ Data Origin Authentication
→ Rejection of replayed pckts (a form of partial sequence Integrity)
→ Confidentiality (encryption)
→ Limited traffic flow confidentiality