Questions

- List and briefly describe some benefits of IPsec.
- **Secure branch office connectivity over the Internet**
- **Secure remote access over the Internet:**
- **Establishing extranet and intranet connectivity with partners: IPSec can be used to secure**
- **Enhancing electronic commerce security:**

List and briefly define different categories of IPsec documents

- Access control;
- connectionless integrity;
- data origin authentication;
- rejection of replayed packets (a form of partial sequence integrity);
- confidentiality (encryption); and limited traffic flow confidentiality

- What parameters identify an SA and what parameters characterize the nature of a particular SA?
- 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:** Currently, only unicast addresses are allowed; 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.

What is the difference between transport mode and tunnel mode?

- **Transport mode provides protection primarily for upper-layer** protocols. That is, transport mode protection extends to the payload of an IP packet.
- **Tunnel mode provides protection to the entire IP** packet.

- What are the types of secret key algorithm used in IPsec?

Why does ESP include a padding field?

- 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. **2. 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. **3. Additional padding may be added**
- to provide partial traffic flow confidentiality by concealing the actual
- length of the payload.

- 1.IP security is a capability that can be added to either current version of the Internet Protocol by means of additional headers.
-
- 2. The principal feature of IPsec is that it can encrypt and/or authenticate all traffic at the IP level.
-
- 3. Transport mode provides protection to the entire IP packet.

- T
- T
- F

- Additional padding may be added to provide partial traffic flow confidentiality by concealing the actual length of the payload.
-
- 5. Authentication must be applied to the entire original IP packet.
-
- 6. An end user whose system is equipped with IP security protocols can make a local call to an ISP and gain secure access to a company network.

- T
- F
- T

- Both tunnel and transport modes can be accommodated by the encapsulating security payload encryption format.
-
- 8. An individual SA can implement both the AH and the ESP protocol.
-
- 9. By implementing security at the IP level an organization can ensure secure networking not only for applications that have security mechanisms but also for the many security ignorant applications

- T
- F
- T

- IPSec can guarantee that all traffic designated by the network administrator is authenticated but cannot guarantee that it is encrypted.
-
- 11. Any traffic from the local host to a remote host for purposes of an IKE exchange bypasses the IPsec processing.
-
- 12. IPsec is executed on a packet-by-packet basis.

- F
- T
- T

- 13. The Payload Data Field is designed to deter replay attacks
- The Security Parameters Index identifies a security association.
-
- The default automated key management protocol for IPsec is referred to as ISAKMP/Oakley.

- F
- T
- T

- Authentication applied to the entire original IP packet is _____ .
-
- A) security mode B) cipher mode
-
- C) tunnel mode D) transport mode

- . _____ defines a number of techniques for key management.
-
- A) KEP B) KMP
-
- C) SKE D) IKE

- Authentication applied to all of the packet except for the IP header is _____ .
- Authentication applied to the entire original IP packet is _____
- Authentication makes use of the _____ message authentication code
- IKE key determination employs _____ to ensure against replay attacks

- transport mode
- tunnel mode
- HMAC
- nonces

- IPsec encompasses three functional areas: authentication, key management, and _____
- IPsec provides security services at the _____ layer by enabling a system to select required security protocols, determine the algorithms to use for the services and put in place any cryptographic keys required to provide the requested services
- The _____ facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties.

- Confidentiality
- IP
- confidentiality

- The _____ facility is concerned with the secure exchange of keys.
- The _____ mechanism assures that a received packet was in fact transmitted by the party identified as the source in the packet header and assures that the packet has not been altered in transit.

- key management
- authentication

- The key management mechanism that is used to distribute keys is coupled to the authentication and privacy mechanisms only by way of the _____
- The means by which IP traffic is related to specific SAs is the _____ .

- SPI
- SPD

- Three different authentication methods can be used with IKE key determination: Public key encryption, symmetric key encryption, and _____ .

- Digital Signatures

- _____ consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication. The current specification is RFC 4303.
- _____ defines a number of techniques for key management.

- ESP
- IKE
- _____ mode is used when one or both ends of an SA are a security gateway, such as a firewall or router that implements IPsec.
- _____ provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.
- Tunnel IPSec

- Authentication applied to all of the packet except for the IP header is _____ .
-
- A) tunnel mode B) transport mode
-
- C) association mode D) security mode

- IPsec encompasses three functional areas: authentication, key management, and
- _____ .
-
- 2. _____ mode is used when one or both ends of an SA are a security gateway, such as a firewall or router that implements IPsec.
-
- 3. IPsec policy is determined primarily by the interaction of two databases: The security policy database and the _____ .

- confidentiality
- Tunnel
- security association database (SAD)

- Confidentiality is provided by an encryption format known as _____ .
- A _____ attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination.
- 6. Authentication makes use of the _____ message authentication code.

- encapsulating security payload
- replay
- HMAC