**Chapter 20: IP Security**

**TRUE OR FALSE**

T F 1. IP security is a capability that can be added to either current

version of the Internet Protocol by means of additional headers.

T F 2. The principal feature of IPsec is that it can encrypt and/or

authenticate all traffic at the IP level.

T F 3. Transport mode provides protection to the entire IP packet.

T F 4. Additional padding may be added to provide partial traffic flow

confidentiality by concealing the actual length of the payload.

T F 5. Authentication must be applied to the entire original IP packet.

T F 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 7. Both tunnel and transport modes can be accommodated by the

encapsulating security payload encryption format.

T F 8. An individual SA can implement both the AH and the ESP protocol.

T F 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 10. IPSec can guarantee that all traffic designated by the network

administrator is authenticated but cannot guarantee that it is

encrypted.

T F 11. Any traffic from the local host to a remote host for purposes of an

IKE exchange bypasses the IPsec processing.

T F 12. IPsec is executed on a packet-by-packet basis.

T F 13. The Payload Data Field is designed to deter replay attacks.

T F 14. The Security Parameters Index identifies a security association.

T F 15. The default automated key management protocol for IPsec is

referred to as ISAKMP/Oakley.

**MULTIPLE CHOICE**

1. Authentication applied to the entire original IP packet is \_\_\_\_\_\_\_\_\_ .

A) security mode B) cipher mode

C) tunnel mode D) transport mode

2. \_\_\_\_\_\_\_\_\_ defines a number of techniques for key management.

A) KEP B) KMP

C) SKE D) IKE

3. 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

4. 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.

A) confidentiality B) authentication

C) security D) key management

5. \_\_\_\_\_\_\_\_\_\_ provides the capability to secure communications across a LAN, across

private and public WANs, and across the Internet.

A) IKE B) ISA

C) IAB D) IPsec

6. The \_\_\_\_\_\_\_\_\_ facility enables communicating nodes to encrypt messages to

prevent eavesdropping by third parties.

A) security B) key management

C) authentication D) confidentiality

7. The key management mechanism that is used to distribute keys is coupled to the

authentication and privacy mechanisms only by way of the \_\_\_\_\_\_\_\_\_ .

A) IAB B) SPI

C) ESP D) SPD

8. A \_\_\_\_\_\_\_\_\_ is a one way relationship between a sender and a receiver that affords

security services to the traffic carried on it.

A) SAD B) SPD

C) SA D) SPI

9. The means by which IP traffic is related to specific SAs is the \_\_\_\_\_\_\_\_\_ .

A) TRS B) SPD

C) SAD D) SPI

10. \_\_\_\_\_\_\_\_\_ consists of an encapsulating header and trailer used to provide

encryption or combined encryption/authentication. The current specification is

RFC 4303.

A) SPI B) ESP

C) ISA D) IPsec

11. \_\_\_\_\_\_\_\_\_ identifies the type of data contained in the payload data field by

identifying the first header in that payload.

A) Security Parameters Index B) Next Header

C) Sequence Header D) Payload Data

12. A value chosen by the responder to identify a unique IKE SA is a \_\_\_\_\_\_\_\_\_ .

A) Initiator SPI B) Responder Cookie

C) Flag D) Message ID

13. IKE key determination employs \_\_\_\_\_\_\_\_\_\_ to ensure against replay attacks.

A) cookies B) groups

C) flags D) nonces

14. The \_\_\_\_\_\_\_\_\_\_ payload contains either error or status information associated

with this SA or this SA negotiation.

A) Encrypted B) Notify

C) Configuration D) Nonce

15. The \_\_\_\_\_\_\_\_\_ payload allows peers to identify packet flows for processing by

IPsec services.

A) Configuration B) Vendor ID

C) Traffic Selector D) Extensible Authentication Protocol

**SHORT ANSWER**

1. 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 \_\_\_\_\_\_\_\_\_\_ .

4. Confidentiality is provided by an encryption format known as \_\_\_\_\_\_\_\_\_\_ .

5. 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.

7. A security association is uniquely identified by three parameters: Security

Protocol Identifier, IP Destination Address, and \_\_\_\_\_\_\_\_ .

8. The \_\_\_\_\_\_\_\_\_\_ facility is concerned with the secure exchange of keys.

9. \_\_\_\_\_\_\_\_\_ can be used to provide confidentiality, data origin authentication,

connectionless integrity, an anti-replay service, and traffic flow confidentiality.

10. 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.

11. The selectors that determine a Security Policy Database are: Name, Local and

Remote Ports, Next Layer Protocol, Remote IP Address, and \_\_\_\_\_\_\_\_\_ .

12. The term \_\_\_\_\_\_\_\_\_ refers to a sequence of SAs through which traffic must be

processed to provide a desired set of IPsec services.

13. Generic in that it does not dictate specific formats, the \_\_\_\_\_\_\_\_\_ is a key exchange

protocol based on the Diffie-Hellman algorithm with added security.

14. Three different authentication methods can be used with IKE key determination:

Public key encryption, symmetric key encryption, and \_\_\_\_\_\_\_\_\_ .

15. At any point in an IKE exchange the sender may include a \_\_\_\_\_\_\_\_\_ payload to

request the certificate of the other communicating entity.