Question: 1

Which of the following protocols is used with a tunneling protocol to provide security?
A. FTP
B. EAP
C. IPSec
D. IPX/SPX

Answer: C

Explanation:
Internet Protocol Security (IPSec) is used with Layer 2 Tunneling Protocol (L2TP). It is a standard-based protocol that provides the highest level of virtual private network (VPN) security. IPSec can encrypt virtually everything above the networking layer. It secures both data and password.

Question: 2

Which of the following user authentications are supported by the SSH-1 protocol but not by the SSH-2 protocol? Each correct answer represents a complete solution. Choose all that apply.
A. Kerberos authentication
B. TIS authentication
C. Password-based authentication
D. Rhosts (rsh-style) authentication

Answer: DBA

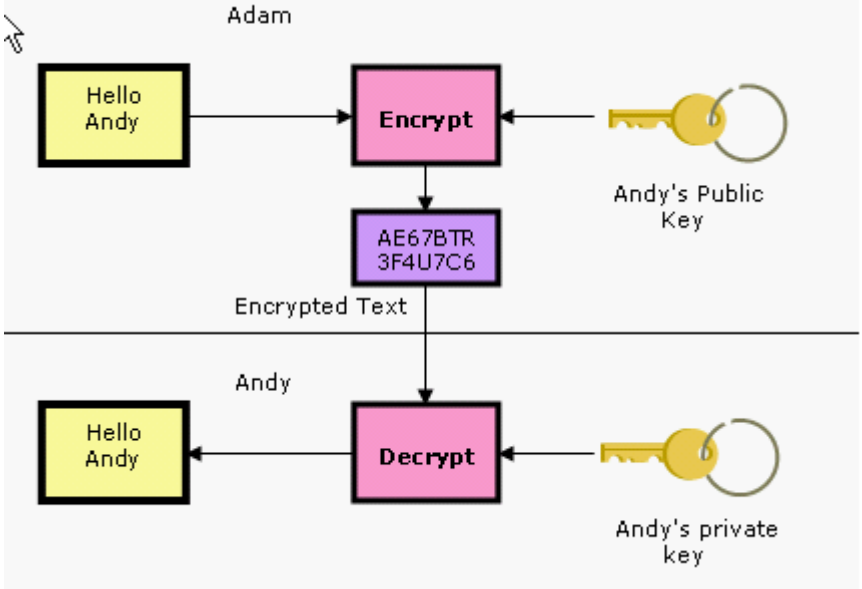
Explanation:
The Rhosts (rsh-style), TIS, and Kerberos user authentication methods are supported by the SSH-1 protocol but not by SSH-2 protocol.
Answer option C is incorrect. Password-based authentication is supported by both the SSH-1 and SSH-2 protocols.

Question: 3

Adam wants to encrypt an email message with an asymmetric key encryption scheme, so that he can send it to his friend Andy. Which of the following is the requirement to encrypt the email, so that only Andy can read it?
A. Andy's public key
B. Adam's private key
C. Andy's private key
D. Adam's public key

Answer: A

Explanation:
Adam has to use Andy's public key in order to encrypt his email, so that only Andy can read it. In an asymmetric key encryption scheme, anyone can encrypt messages using the public key, but only the holder of the paired private key can decrypt. The security depends on the secrecy of that private key.
Public-key cryptography is a cryptographic approach, which involves the use of asymmetric key algorithms instead of or in addition to symmetric key algorithms. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver. The asymmetric key algorithms are used to create a mathematically related key pair: a secret private key and a published public key. Use of these keys allows protection of the authenticity of a message by creating a digital signature of a message using the private key, which can be verified using the public key. It also allows protection of the confidentiality and integrity of a message, by public key encryption, encrypting the message using the public key, which can only be decrypted using the private key.



Question: 4

Which of the following firewalls inspects the actual contents of packets?
A. Circuit-level firewall
B. Application-level firewall
C. Stateful inspection firewall
D. Packet filtering firewall

Answer: B

Explanation:
The application level firewall inspects the contents of packets, rather than the source/destination or connection between the two. An Application level firewall operates at the application layer of the OSI model.
Answer option A is incorrect. The circuit-level firewall regulates traffic based on whether or not a trusted connection has been established. It operates at the session layer of the OSI model.
Answer option D is incorrect. The packet filtering firewall filters traffic based on the headers. It operates at the network layer of the OSI model.
Answer option C is incorrect. The stateful inspection firewall assures the connection between the two parties is valid and inspects packets from this connection to assure the packets are not malicious.

Question: 5

Which of the following processes is used by remote users to make a secure connection to internal resources after establishing an Internet connection?
A. Packet sniffing
B. Tunneling
C. Packet filtering
D. Spoofing

Answer: B

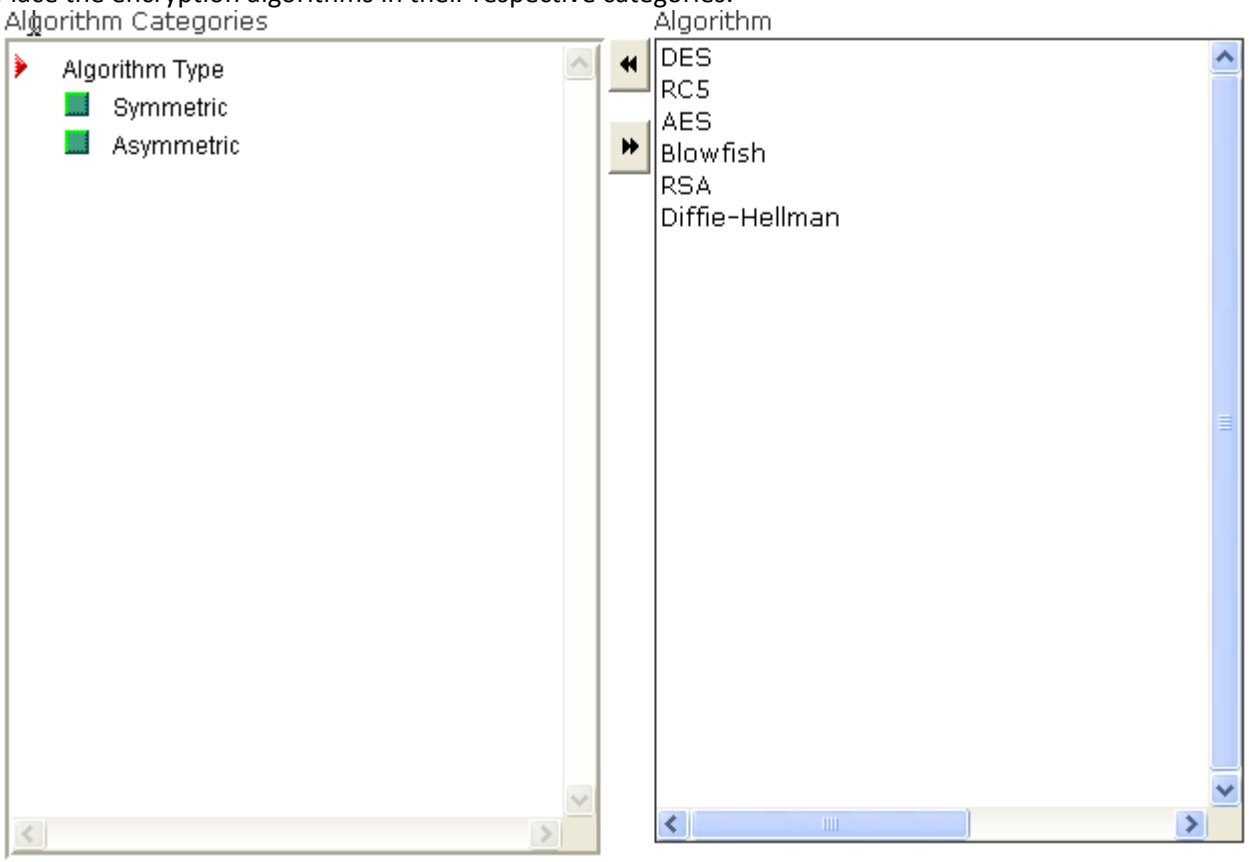
Explanation:
Tunneling is a process used by remote users to make a secure connection to internal resources after establishing an Internet connection. The tunnel is created between the two ends by encapsulating the data in a mutually agreed-upon protocol for transmission.
Answer option C is incorrect. Packet filtering is a method that allows or restricts the flow of specific types of packets to provide security. It analyzes the incoming and outgoing packets and lets them pass or stops them at a network interface based on the source and destination addresses, ports, or protocols. Packet filtering provides a way to define precisely which type of IP traffic is allowed to cross the firewall of an intranet. IP packet filtering is important when users from private intranets connect to public networks, such as the Internet.

Answer option A is incorrect. Packet sniffing is a process of monitoring data packets that travel across a network. The software used for packet sniffing is known as sniffers. There are many packet-sniffing programs that are available on the Internet. Some of these are unauthorized, which can be harmful for a network's security.

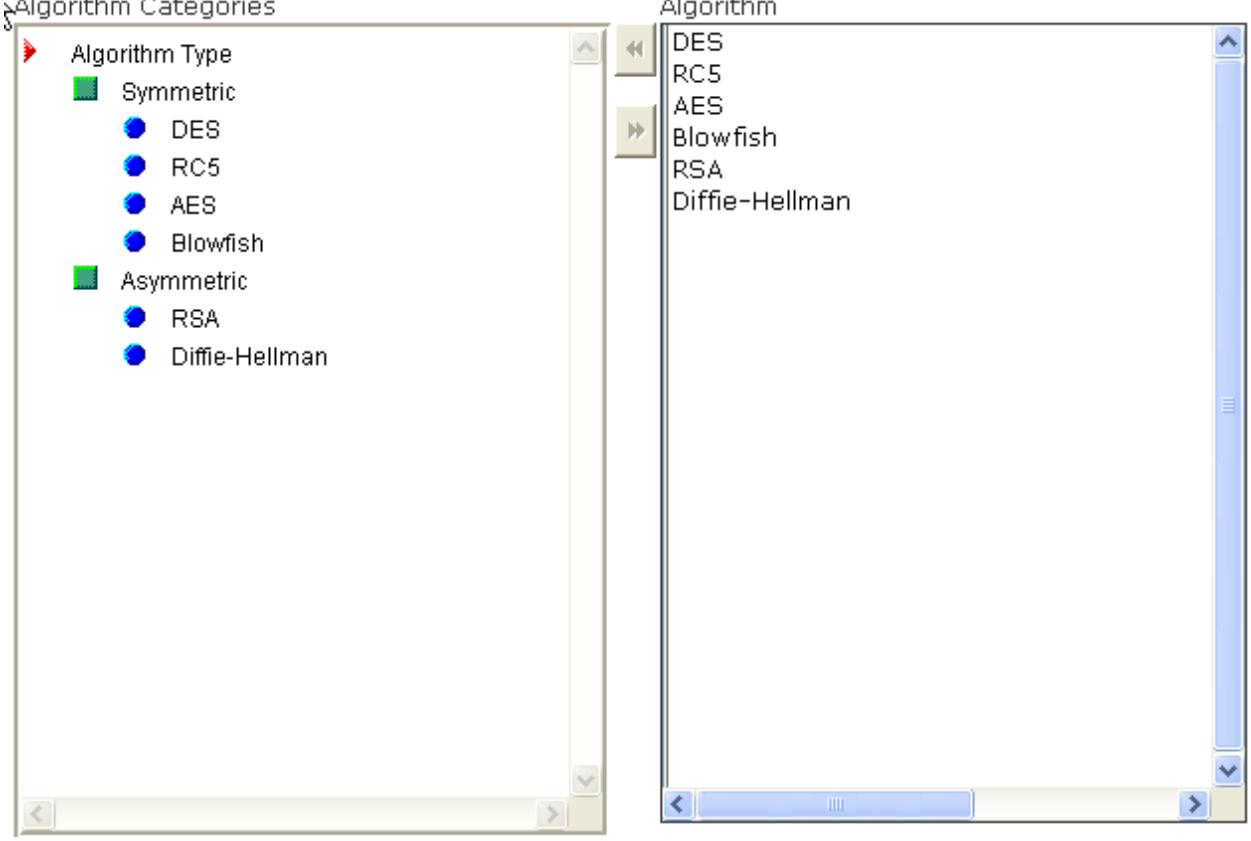
Answer option D is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.

Question: 6

Place the encryption algorithms in their respective categories.



Answer:



Explanation:
The following are symmetric encryption algorithms:
DES
RC5
AES
Blowfish

Question: 7
Which of the following protocols provides certificate-based authentication for virtual private networks (VPNs)?
A. L2TP
B. HTTPS
C. PPTP
D. SMTP

Answer: A

Explanation:
Layer 2 Tunneling Protocol (L2TP) is a more secure version of Point-to-Point Tunneling Protocol (PPTP). It provides tunneling, address assignment, and authentication. L2TP allows transfer of Point-to-Point Protocol (PPP) traffic between different networks. L2TP combines with IPSec to provide both tunneling and security for Internet Protocol (IP), Internetwork Packet Exchange (IPX), and other protocol packets across IP networks. It provides certificate-based authentication for virtual private networks (VPNs).
Answer option C is incorrect. Point-to-Point Tunneling Protocol (PPTP) is a remote access protocol. It is an extension of the Point-to-Point Protocol (PPP). PPTP is used to securely connect to a private network by a remote client using a public data network, such as the Internet. Virtual private networks (VPNs) use the tunneling protocol to enable remote users to access corporate networks securely across the Internet. PPTP supports encapsulation of encrypted packets in secure wrappers that can be transmitted over a TCP/IP connection.
Answer options B and D are incorrect. The HTTPS and SMTP protocols are not used in virtual private networks (VPNs).

Question: 8

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. A firewall has been configured on the network. You configure a filter on the router. You verify that SMTP operations have stopped after the recent configuration. Which of the following ports will you have to open on the router to resolve the issue?

A. 20
B. 80
C. 25
D. 21

Answer: C

Explanation:
In order to resolve the issue, you will have to open port 25 on the router. By default, SMTP uses TCP port 25 for communication.

Question: 9

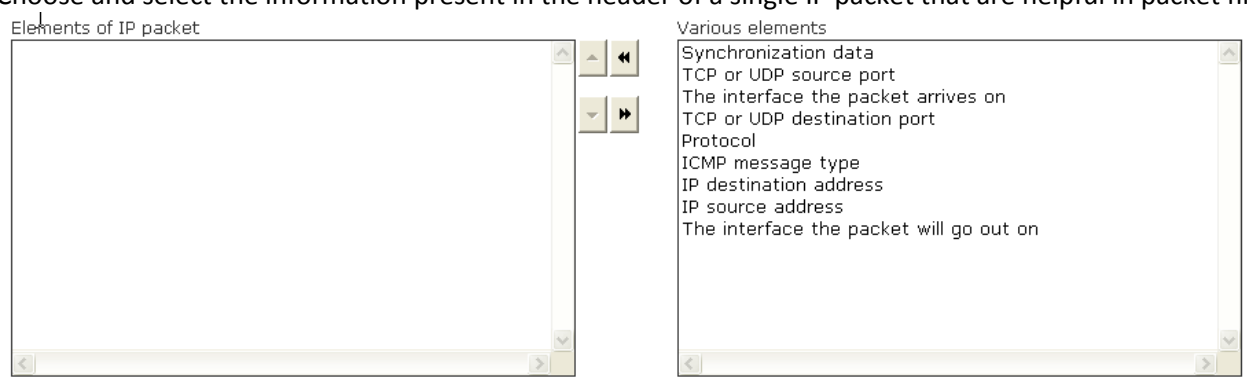
Which of the following methods of encryption uses a single key to encrypt and decrypt data?
A. Asymmetric
B. PGP
C. S/MIME
D. Symmetric

Answer: D

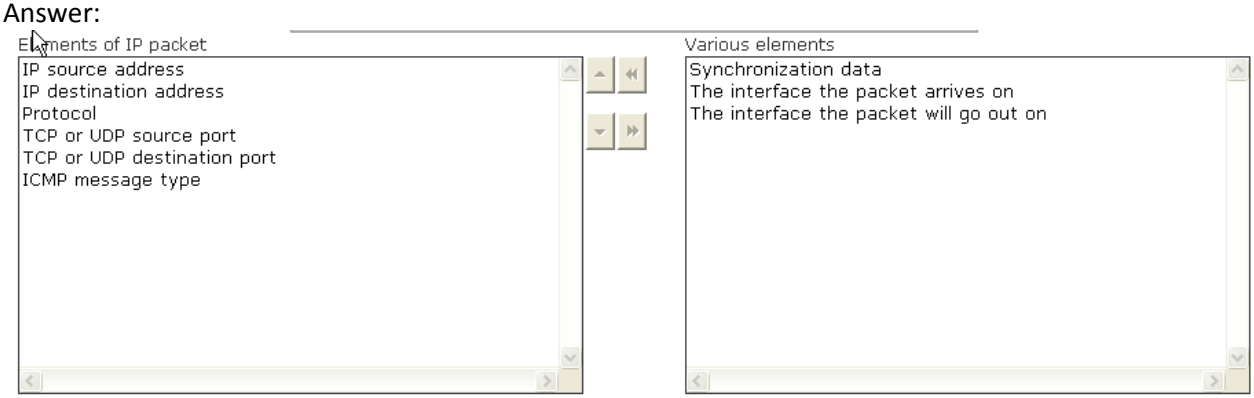
Explanation:
Symmetric encryption is a type of encryption that uses a single key to encrypt and decrypt data. Symmetric encryption algorithms are faster than public key encryption. Therefore, it is commonly used when a message sender needs to encrypt a large amount of data. Data Encryption Standard (DES) uses symmetric encryption key algorithm to encrypt data.
Answer option A is incorrect. Asymmetric encryption is a type of encryption that uses two keys - a public key and a private key pair for data encryption. The public key is available to everyone, while the private or secret key is available only to the recipient of the message. For example, when a user sends a message or data to another user, the sender uses a public key to encrypt the data. The receiver uses his private key to decrypt the data.
Answer options C and B are incorrect. Secure Multipart Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP) are types of asymmetric encryption. Both are based on public key cryptography where each user has two keys, a public key for encrypting and a private key for decrypting messages.

Question: 10

Choose and select the information present in the header of a single IP packet that are helpful in packet filtering.

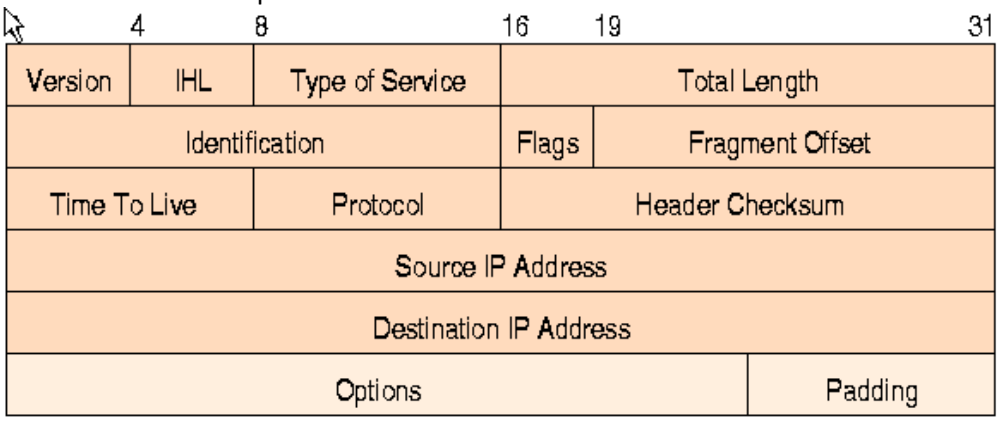


Answer:



Explanation:

An IP packet is a formatted unit of data carried by a packet mode computer network. A packet consists of two kinds of data: control information and user data (also known as payload). The control information provides data the network needs to deliver the user data, for example: source and destination addresses, error detection codes like checksums, and sequencing information. Typically, control information is found in packet headers and trailers, with user data in between. IP packets are composed of a header and payload. Every IP packet has a set of headers containing certain information. The main information is as follows:
IP source address
IP destination address
Protocol (whether the packet is a TCP, UDP, or ICMP packet)
TCP or UDP source port
TCP or UDP destination port
ICMP message type
The structure of an IP packet is as follows:



Question: 11
SSH is a network protocol that allows data to be exchanged between two networks using a secure channel. Which of the following encryption algorithms can be used by the SSH protocol?
Each correct answer represents a complete solution. Choose all that apply.
A. DES
B. Blowfish
C. IDEA
D. RC4

Answer: CAB

Explanation:
SSH connections can use IDEA, Blowfish, and DES encryption algorithms.
Answer option D is incorrect. The RC4 encryption algorithm is used by the SSL protocol.

Question: 12

Which of the following protocols are used to provide secure communication between a client and a server over the Internet?
Each correct answer represents a part of the solution. Choose two.
A. HTTP
B. SNMP
C. TLS
D. SSL

Answer: DC

Explanation:
SSL and TLS protocols are used to provide secure communication between a client and a server over the Internet.

Question: 13

Fill in the blank with the appropriate term.
The_____ is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

A. Public Key

Answer: A

Explanation: The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique for each CA. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA) . For each user, the user identity, the public key, their binding, validity conditions and other attributes are made unforgeable in public key certificates issued by the CA.