JK0-022$^{Q\&As}$

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

QUESTION 1

Ann has taken over as the new head of the IT department. One of her first assignments was to implement AAA in preparation for the company\\'s new telecommuting policy. When she takes inventory of the organizations existing network infrastructure, she makes note that it is a mix of several different vendors. Ann knows she needs a method of secure centralized access to the company\\'s network resources. Which of the following is the BEST service for Ann to implement?

A. RADIUS

B. LDAP

C. SAML

D. TACACS+

Correct Answer: A

The Remote Authentication Dial In User Service (RADIUS) networking protocol offers centralized Authentication, Authorization, and Accounting (AAA) management for users who make use of a network service.

Incorrect Answers: B: The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

C: Security Assertion Markup Language (SAML) is an open-standard data format based on XML.

D: TACACS+ makes use of the authentication, authorization, and accounting (AAA) architecture. However, unlike RADIUS, these separate components of the protocol can be segregated and handled on separate servers.

References:

http://en.wikipedia.org/wiki/RADIUS

http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 275.

http://en.wikipedia.org/wiki/TACACS

QUESTION 2

Which of the following provides the HIGHEST level of confidentiality on a wireless network?

A. Disabling SSID broadcast

B. MAC filtering

C. WPA2

D. Packet switching

Correct Answer: C

The Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) authentication protocols were designed to address the core, easy-to-crack problems of WEP. Incorrect Answers:

A: Disabling SSID broadcasting is not the best solution. One method of protecting the network that is often recommended is to disable, or turn off, the SSID broadcast (also known as cloaking). The access point is still there, and it is still accessible by those who have been told of its existence by the administrator, but it prevents those who are just scanning from finding it. This is considered a very weak form of security, because there are still other ways, albeit a bit more complicated, to discover the presence of the access point besides the SSID broadcast.

B: MAC filtering would increase the security, but an authentication protocol such as WPA2 would still be required. Note: When MAC filtering is used, the administrator compiles a list of the MAC addresses associated with users\\' computers and enters those addresses. When a client attempts to connect and other values have been correctly entered, an additional check of the MAC address is done. If the address appears in the list, the client is allowed to join; otherwise, it is forbidden from doing so.

D: Packet switching is a method of transferring data on an Ethernet network. Packet switching does not address wireless security.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 171, 178, 183, 258

QUESTION 3

Which of the following devices is used for the transparent security inspection of network traffic by redirecting user packets prior to sending the packets to the intended destination?

A. Proxies

B. Load balancers

C. Protocol analyzer

D. VPN concentrator

Correct Answer: A

QUESTION 4

Which of the following offerings typically allows the customer to apply operating system patches?

A. Software as a service

B. Public Clouds

C. Cloud Based Storage

D. Infrastructure as a service

Correct Answer: D

Cloud users install operating-system images and their application software on the cloud infrastructure to deploy their applications. In this model, the cloud user patches and maintains the operating systems and the application software.

Incorrect Answers:

A: In the business model using software as a service (SaaS), users are provided access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis or using a subscription fee.

B: A cloud is called a "public cloud" when the services are rendered over a network that is open for public use.

C: Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers, and the physical environment is typically owned and managed by a hosting company.

References: http://en.wikipedia.org/wiki/Cloud_computing http://en.wikipedia.org/wiki/Cloud_storage

QUESTION 5

Sara, a security architect, has developed a framework in which several authentication servers work together to increase processing power for an application. Which of the following does this represent?

A. Warm site

B. Load balancing

C. Clustering

D. RAID

Correct Answer: C

Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy. Server clustering is used to provide failover capabilities / redundancy in addition to scalability as demand increases.

Incorrect Answers:

A: A warm site is part of disaster recovery and involves he provision of some of the capabilities of a hot site, but it requires the customer to do more work to become operational. Warm sites provide computer systems and compatible media capabilities.

B: Load balancing is a way of providing high availability by splitting the workload across multiple computers.

D: RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 234-235, 444

QUESTION 6

While configuring a new access layer switch, the administrator, Joe, was advised that he needed to make sure that only devices authorized to access the network would be permitted to login and utilize resources. Which of the following should the administrator implement to ensure this happens?

A. Log Analysis

B. VLAN Management

C. Network separation

D. 802.1x

Correct Answer: D

802.1x is a port-based authentication mechanism. It\\'s based on Extensible Authentication Protocol (EAP) and is commonly used in closed-environment wireless networks. 802.1x was initially used to compensate for the weaknesses of Wired Equivalent Privacy (WEP), but today it\\'s often used as a component in more complex authentication and connection-management systems, including Remote Authentication Dial-In User Service (RADIUS), Diameter, Cisco System\\'s Terminal Access Controller Access-Control System Plus (TACACS+), and Network Access Control (NAC).

Incorrect Answers:

A: Log analysis is the art and science of reviewing audit trails, log files, or other forms of computer-generated records for evidence of policy violations, malicious events, downtimes, bottlenecks, or other issues of concern.

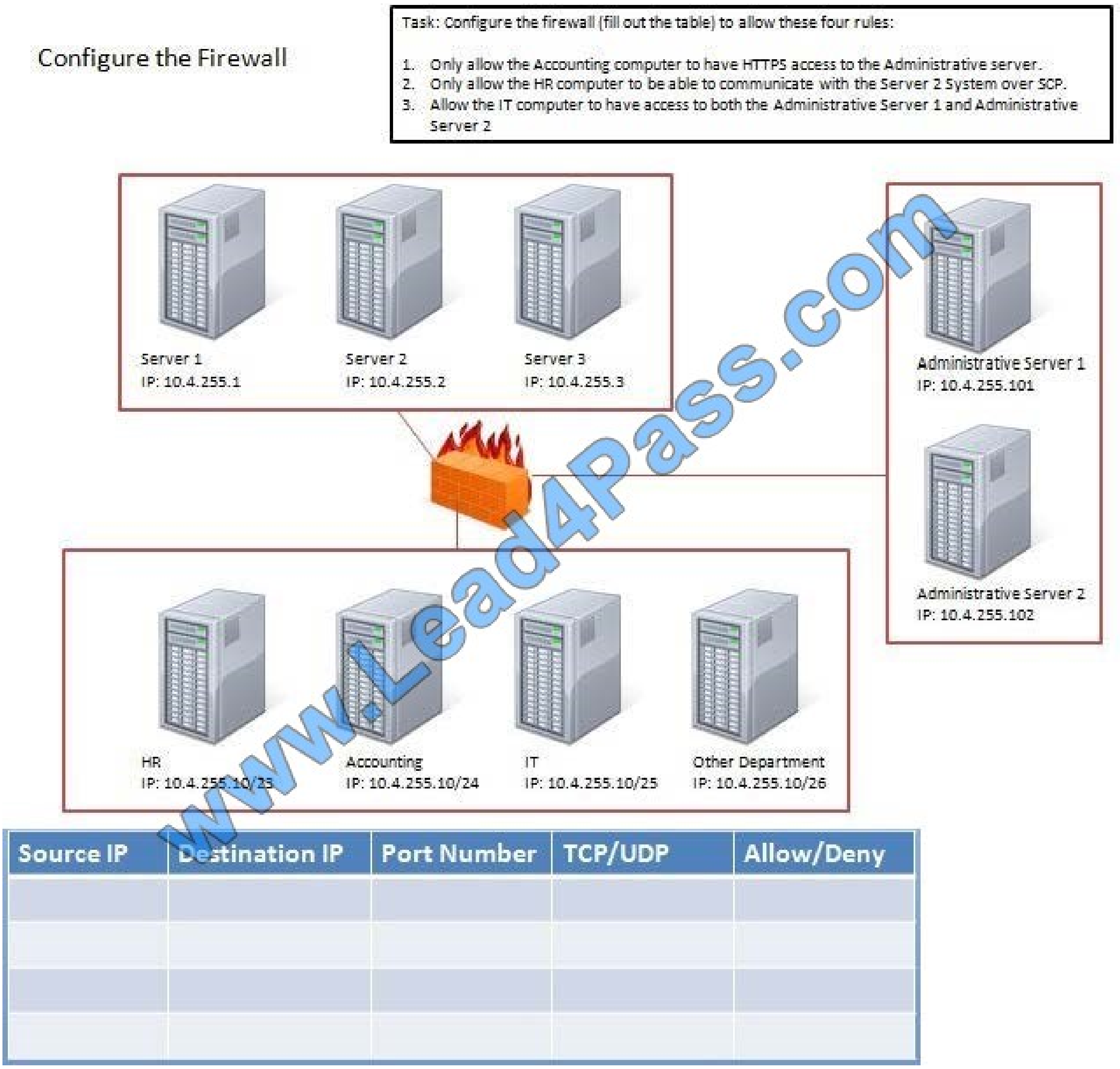
B: VLAN management is the use of VLANs to control traffic for security or performance reasons.

C: Bridging between networks can be a desired feature of network design. Network bridging is self-configuring, is inexpensive, maintains collision-domain isolation, is transparent to Layer 3+ protocols, and avoids the 5-4-3 rule\\'s Layer 1 limitations. However, network bridging isn\\'t always desirable. It doesn\\'t limit or divide broadcast domains, doesn\\'t scale well, can cause latency, and can result in loops. In order to eliminate these problems, you can implement network separation or segmentation. There are two means to accomplish this. First, if communication is necessary between network segments, you can implement IP subnets and use routers. Second, you can create physically separate networks that don\\'t need to communicate. This can also be accomplished later using firewalls instead of routers to implement secured filtering and traffic management.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 23, 25, 26.

QUESTION 7



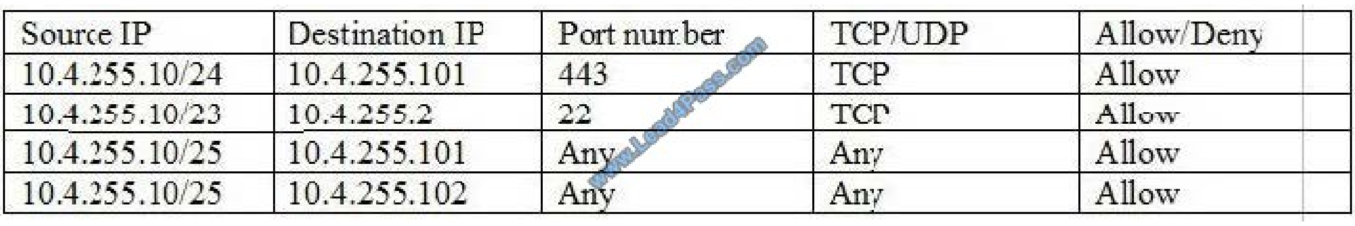
Configure the Firewall

Task: Configure the firewall (fill out the table) to allow these four rules:

1. Only allow the Accounting computer to have HTTPS access to the Administrative server.
2. Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
3. Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2

Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

Correct Answer: Explanation



Source IP	Destination IP	Port number	TCP/UDP	Allow/Deny
10.4.255.10/24	10.4.255.101	443	TCP	Allow
10.4.255.10/23	10.4.255.2	22	TCP	Allow
10.4.255.10/25	10.4.255.101	Any	Any	Allow
10.4.255.10/25	10.4.255.102	Any	Any	Allow

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule\\'s criteria:

Block the connection

Allow the connection

Allow the connection only if it is secured

TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent. Two hosts communicate packet results with each other. TCP also

ensures that packets are decoded and sequenced properly. This connection is persistent during the session. When the session ends, the connection is torn down.

UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it\\'s considerably faster than TCP.

The sessions don\\'t establish a synchronized session like the kind used in TCP, and UDP doesn\\'t guarantee error-free communications. The primary purpose of UDP is to send small packets of information. The application is responsible for

acknowledging the correct reception of the data.

Port 22 is used by both SSH and SCP with UDP.

Port 443 is used for secure web connections HTTPS and is a TCP port. Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication

between 10.4.255.10/24 (Accounting) and 10.4.255.101

(Administrative server1)

Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)

Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between:

10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1) 10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 77, 83, 96, 157.

QUESTION 8

After encrypting all laptop hard drives, an executive officer\\'s laptop has trouble booting to the operating system. Now that it is successfully encrypted the helpdesk cannot retrieve the data.

Which of the following can be used to decrypt the information for retrieval?

A. Recovery agent

B. Private key

C. Trust models

D. Public key

Correct Answer: A

To access the data the hard drive need to be decrypted. To decrypt the hard drive you would need the proper private key. The key recovery agent can retrieve the required key. A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed.

Incorrect Answers:

B: The private key is not readily accessible. You would have to

C: A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate. A trust model cannot recover keys.

D: The public key cannot be used to decrypt the hard drive.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-285, 285-289

QUESTION 9

A company is about to release a very large patch to its customers. An administrator is required to test patch installations several times prior to distributing them to customer PCs.

Which of the following should the administrator use to test the patching process quickly and often?

A. Create an incremental backup of an unpatched PC

B. Create an image of a patched PC and replicate it to servers

C. Create a full disk image to restore after each installation

D. Create a virtualized sandbox and utilize snapshots

Correct Answer: D

Sandboxing is the process of isolating a system before installing new applications or patches on it so as to restrict the software from being able to cause harm to production systems. Before the patch is installed, a snapshot of the system

should be taken. Snapshots are backups that can be used to quickly recover from poor updates, and errors arising from newly installed applications.

Incorrect Answers:

A, C: Creating a full disk image or an incremental backup to restore after each installation could prove useful but less efficient than using snapshots.

B: Replicating a patched PC to all servers does not test the patch, and does not ensure quick recoverability should the patch cause the PC to crash.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 203, 204-205 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 208,

QUESTION 10

Which of the following is true about the CRL?

A. It should be kept public

B. It signs other keys

C. It must be kept secret

D. It must be encrypted

Correct Answer: A

The CRL must be public so that it can be known which keys and certificates have been revoked. In the operation of some cryptosystems, usually public key infrastructures (PKIs), a certificate revocation list (CRL) is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted.

Incorrect Answers:

B: A CRL is a database of revoked keys and signatures. It does not sign other keys.

C: Keeping the CRL secret would be against the purpose of the CRL, which is to provide information regarding revoked keys and certificates.

D: The CRL must be readily available so it should not be encrypted.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 279-285, 285

QUESTION 11

Which of the following is the default port for TFTP?

A. 20

B. 69

C. 21

D. 68

Correct Answer: B

TFTP makes use of UDP port 69.

Incorrect Answers:

A, C: FTP (File Transfer Protocol) uses ports 20 and 21

D: Port 68 TCP/UDP is used by Bootstrap Protocol (BOOTP) Client; as well Dynamic Host Configuration Protocol (DHCP).

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 51.
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 12

The Chief Technology Officer (CTO) wants to improve security surrounding storage of customer passwords.

The company currently stores passwords as SHA hashes. Which of the following can the CTO implement requiring the LEAST change to existing systems?

A. Smart cards

B. TOTP

C. Key stretching

D. Asymmetric keys

Correct Answer: A

Smart cards usually come in two forms. The most common takes the form of a rectangular piece of plastic with an embedded microchip. The second is as a USB token. It contains a built in processor and has the ability to securely store and process information. A "contact" smart card communicates with a PC using a smart card reader whereas a "contactless" card sends encrypted information via radio waves to the PC. Typical scenarios in which smart cards are used include interactive logon, e-mail signing, e-mail decryption and remote access authentication. However, smart cards are programmable and can contain programs and data for many different applications. For example smart cards may be used to store medical histories for use in emergencies, to make electronic cash payments or to verify the identity of a customer to an e-retailer. Microsoft provides two device independent APIs to insulate application developers from differences between current and future implementations: CryptoAPI and Microsoft Win32?SCard APIs. The Cryptography API contains functions that allow applications to encrypt or digitally sign data in a flexible manner, while providing protection for the user\\'s sensitive private key data. All cryptographic operations are performed by independent modules known as cryptographic service providers (CSPs). There are many different cryptographic algorithms and even when implementing the same algorithm there are many choices to make about key sizes and padding for example. For this reason, CSPs are grouped into types, in which each supported CryptoAPI function, by default, performs in a way particular to that type. For example, CSPs in the PROV_DSS provider type support DSS Signatures and MD5 and SHA hashing.

Incorrect Answers:

B: A time-based one-time password (TOTP) is a temporary code, generated by an algorithm, for use in authenticating access to computer systems. The algorithm that generates each password uses the current time of day as one of its factors, ensuring that each password is unique. Time- based one-time passwords are commonly used for two-factor authentication and have seen growing adoption by cloud application providers. In two-factor authentication scenarios, a user must enter a traditional, static password and a TOTP to gain access. In this question, the company currently stores passwords as SHA hashes. This suggests that the passwords are not temporary passwords. Therefore this answer is incorrect.

C: In cryptography, key stretching refers to techniques used to make a possibly weak key, typically a password or passphrase, more secure against a brute force attack by increasing the time it takes to test each possible key. Passwords or passphrases created by humans are often short or predictable enough to allow password cracking. Key stretching makes such attacks more difficult. Key stretching is used to make passwords stronger. One method is to apply a hash to the password. In this question, the passwords are already hashed. Therefore this answer is incorrect.

D: Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes. Asymmetric keys are not used to further secure hashed passwords. Therefore this answer is incorrect.

References: https://msdn.microsoft.com/en-us/library/ms953432.aspx
http://searchconsumerization.techtarget.com/definition/time-based-one-time-password-TOTP
http://en.wikipedia.org/wiki/Key_stretching

QUESTION 13

Layer 7 devices used to prevent specific types of html tags are called:

A. Firewalls

B. Content filters

C. Routers

D. NIDS

Correct Answer: B

A content filter is a is a type of software designed to restrict or control the content a reader is authorised to access, particularly when used to limit material delivered over the Internet via the Web, e-mail, or other means. Because the user and

the OSI layer interact directly with the content filter, it operates at Layer 7 of the OSI model.

Incorrect Answers:

A, C, D: These devices deal with controlling how devices in a network gain access to data and permission to transmit it, as well as controlling error checking and packet synchronization. It, therefore, operates at Layer 2 of the OSI model.

References:

http://en.wikipedia.org/wiki/Content-control_software#Types_of_filtering http://en.wikipedia.org/wiki/OSI_model

QUESTION 14

Which of the following components MUST be trusted by all parties in PKI?

A. Key escrow

B. CA

C. Private key

D. Recovery key

Correct Answer: B

A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. In a simple trust model all parties must trust the CA. In a more complicated trust model all parties must trust the Root CA.

Incorrect Answers:

A: Key escrow is nothing that needs to be trusted.

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages)

and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee\\'s private messages have been called into question.

C: A private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages.

D: A recovery key has no specific function within a PKI.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 278-290

QUESTION 15

A security administrator must implement a secure key exchange protocol that will allow company clients to autonomously exchange symmetric encryption keys over an unencrypted channel. Which of the following MUST be implemented?

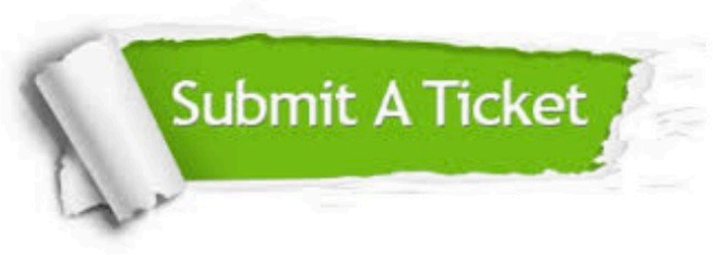
A. SHA-256

B. AES

C. Diffie-Hellman

D. 3DES

Correct Answer: C


Submit A Ticket