Vendor: Cisco

Exam Code: 640-553

Exam Name: IINS Implementing Cisco IOS Network Security

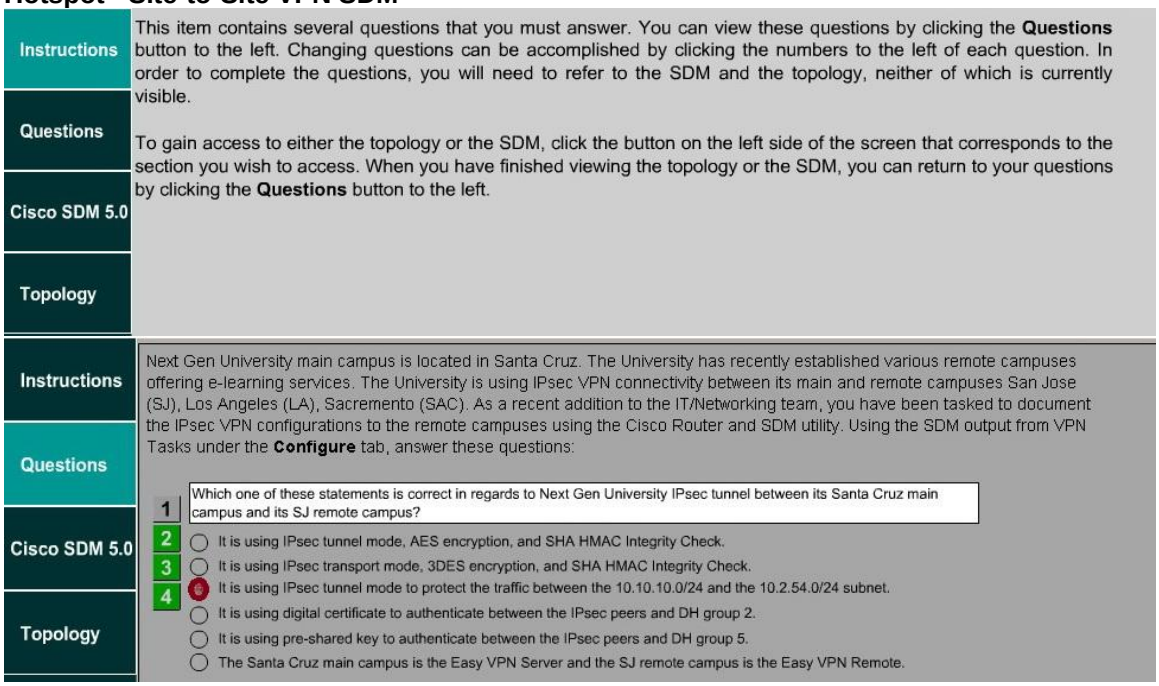
Version: 12.39

QUESTION 1
Which consideration is important when implementing Syslogging in your network?

A. Use SSH to access your Syslog information.
B. Enable the highest level of Syslogging available to ensure you log all possible event messages.
C. Log all messages to the system buffer so that they can be displayed when accessing the router.
D. Syncronize clocks on the network with a protocol such as Network Time Protocol.

Answer: D

QUESTION 2
Hotspot - Site-to-Site VPN SDM



Hotspot - Site-to-Site VPN SDM Simulation Cotains 4 Questions.

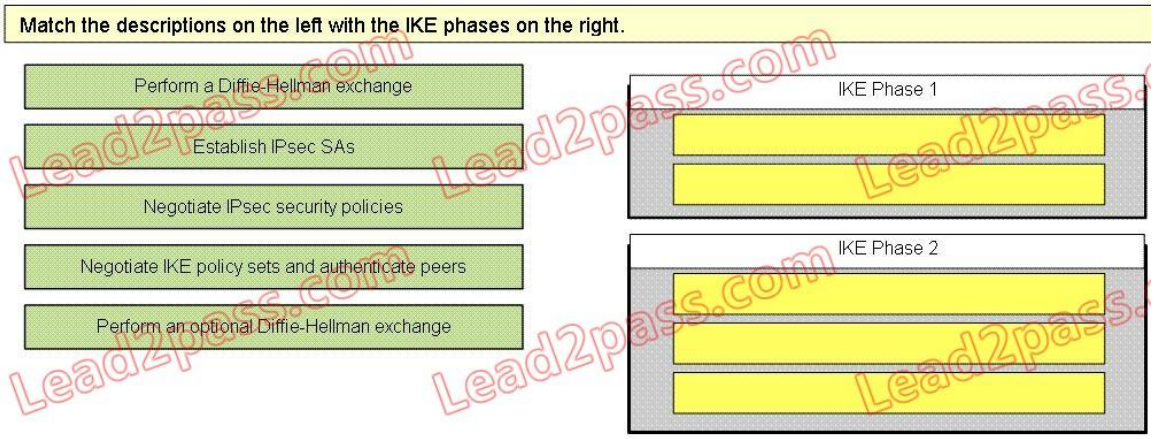
PS: You can see the Comprehensive Question Description & Topology and Answer & Explanation From Full Version.

QUESTION 3
Which statement is true when you have generated RSA keys on your Cisco router to prepare for secure device management?

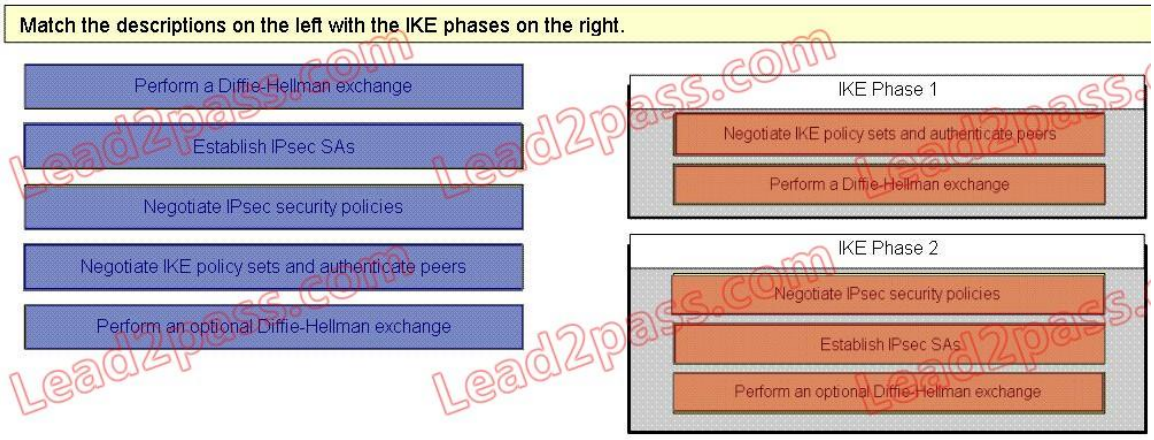
A. You must then zeroize the keys to reset secure shell before configuring other parameters.
B. The SSH protocol is automatically enabled.
C. You must then specify the general-purpose key size used for authentication with the crypto key generate rsa general-keys modulus command.
D. All vty ports are automatically enabled for SSH to provide secure management.

Answer: B

QUESTION 4
Drag and Drop



Answer:



QUESTION 5
What does level 5 in the following enable secret global configuration mode command indicate?
router#enable secret level 5 password

A. The enable secret password is hashed using MD5.
B. The enable secret password is hashed using SHA.
C. The enable secret password is encrypted using Cisco proprietary level 5 encryption.
D. Set the enable secret command to privilege level 5.
E. The enable secret password is for accessing exec privilege level 5.

Answer: E

QUESTION 6
Which statement is true about a Smurf attack?

A. It sends ping requests to a subnet, requesting that devices on that subnet send ping replies to a

target system.

B. It intercepts the third step in a TCP three-way handshake to hijack a session.

C. It uses Trojan horse applications to create a distributed collection of "zombie" computers, which can be used to launch a coordinated DDoS attack.

D. It sends ping requests in segments of an invalid size.

Answer: A

QUESTION 7

Lab – Port Security Simulation

You are the network security administrator for Big Money Bank Co . You are informed that an attacker has performed a CAM table overflow attack by sending spoofed MAC addresses on one of the switch ports. The attacker has since been identified and escorted out of the campus. You now need to take action to configure the switch port to protect against this kind of attack in the future.

For purposes of this test, the attacker was connected via a hub to the Fa0/12 interface of the switch. The topology is provided for your use. The enable password of the switch is **cisco**. Your task is to configure the Fa0/12 interface on the switch to limit the maximum number of MAC addresses that are allowed to access the port to two and to

CiscoTerminal

```
sw-class#show run
Building configuration...
Current configuration:
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname sw-class
!
!
enable secret 5 $1$0/yW$toqA0XRiCtY8gh7pM06fS0
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
 --More--
```


Answer:

PS: You can see the Comprehensive Question Description & Topology and Answer & Explanation From Full Version.

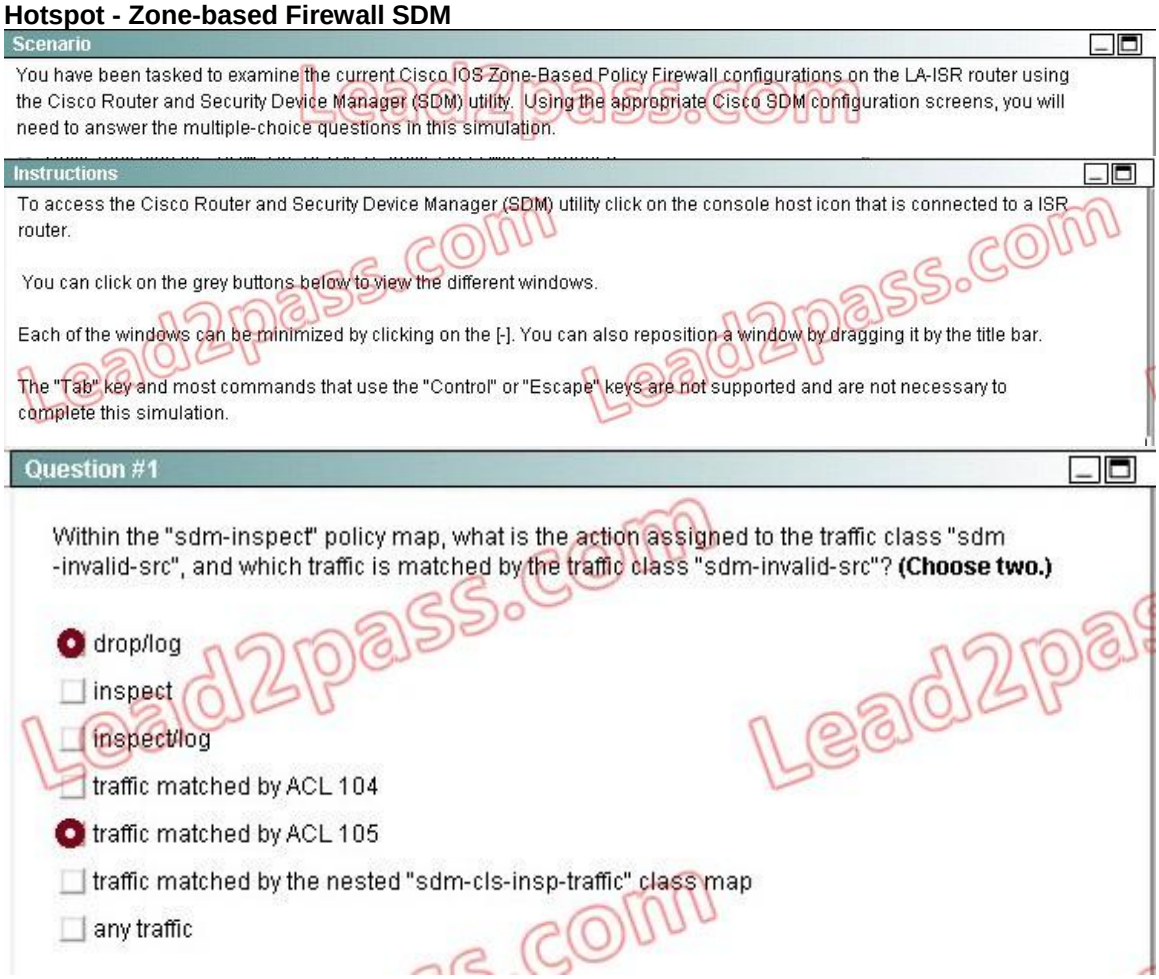
QUESTION 8

For the following attempts, which one is to ensure that no one employee becomes a pervasive security threat, that data can be recovered from backups, and that information system changes do not compromise a system's security?

A. Disaster recovery
B. Strategic security planning
C. Implementation security
D. Operations security

Answer: D

QUESTION 9
Hotspot - Zone-based Firewall SDM



Hotspot - Zone-based Firewall SDM Simulation Contains 6 Questions.

PS: You can see the Comprehensive Question Description & Topology and Answer & Explanation From Full Version.

QUESTION 10
Which three options are network evaluation techniques? (Choose three.)

A. Scanning a network for active IP addresses and open ports on those IP addresses
B. Using password-cracking utilities

C. Performing end-user training on the use of antispyware software
D. Performing virus scans

Answer: ABD

QUESTION 11
What is the key difference between host-based and network-based intrusion prevention?

A. Network-based IPS is better suited for inspection of SSL and TLS encrypted data flows.
B. Network-based IPS provides better protection against OS kernel-level attacks against hosts and servers.
C. Network-based IPS can provide protection to desktops and servers without the need of installing specialized software on the end hosts and servers.
D. Host-based IPS can work in promiscuous mode or inline mode.
E. Host-based IPS is more scalable then network-based IPS.
F. Host-based IPS deployment requires less planning than network-based IPS.

Answer: C

QUESTION 12
Which one is the most important based on the following common elements of a network design?

A. Business needs
B. Best practices
C. Risk analysis
D. Security policy

Answer: A

QUESTION 13
Refer to the exhibit. You are a network manager for your organization. You are looking at your Syslog server reports. Based on the Syslog message shown, which two statements are true? (Choose two.)

```
Feb 1 10:12:08 PST: %SYS-5-CONFIG_I: Configured from console by vty0 (10.2.2.6)
```

A. Service timestamps have been globally enabled.
B. This is a normal system-generated information message and does not require further investigation.
C. This message is unimportant and can be ignored.
D. This message is a level 5 notification message.

Answer: AD

QUESTION 14
Examine the following items, which one offers a variety of security solutions, including firewall, IPS, VPN, antispyware, antivirus, and antiphishing features?

A. Cisco 4200 series IPS appliance
B. Cisco ASA 5500 series security appliance

C. Cisco IOS router
D. Cisco PIX 500 series security appliance

Answer: B

QUESTION 15
The enable secret password appears as an MD5 hash in a router's configuration file, whereas the enable password is not hashed (or encrypted, if the password-encryption service is not enabled). What is the reason that Cisco still support the use of both enable secret and enable passwords in a router's configuration?

A. The enable password is used for IKE Phase I, whereas the enable secret password is used for IKE Phase II.
B. The enable password is considered to be a router's public key, whereas the enable secret password is considered to be a router's private key.
C. Because the enable secret password is a hash, it cannot be decrypted. Therefore, the enable password is used to match the password that was entered, and the enable secret is used to verify that the enable password has not been modified since the hash was generated.
D. The enable password is present for backward compatibility.

Answer: D

QUESTION 16
How does CLI view differ from a privilege level?

A. A CLI view supports only commands configured for that specific view, whereas a privilege level supports commands available to that level and all the lower levels.
B. A CLI view supports only monitoring commands, whereas a privilege level allows a user to make changes to an IOS configuration.
C. A CLI view and a privilege level perform the same function. However, a CLI view is used on a Catalyst switch, whereas a privilege level is used on an IOS router.
D. A CLI view can function without a AAA configuration, whereas a privilege level requires AAA to be configured.

Answer: A

QUESTION 17
When configuring Cisco IOS login enhancements for virtual connections, what is the "quiet period"?

A. A period of time when no one is attempting to log in
B. The period of time in which virtual logins are blocked as security services fully initialize
C. The period of time in which virtual login attempts are blocked, following repeated failed login attempts
D. The period of time between successive login attempts

Answer: C

QUESTION 18

What is a result of securing the Cisco IOS image using the Cisco IOS image resilience feature?

A. The show version command will not show the Cisco IOS image file location.
B. The Cisco IOS image file will not be visible in the output from the show flash command.
C. When the router boots up, the Cisco IOS image will be loaded from a secured FTP location.
D. The running Cisco IOS image will be encrypted and then automatically backed up to the NVRAM.
E. The running Cisco IOS image will be encrypted and then automatically backed up to a TFTP server.

Answer: B

QUESTION 19
Which three statements are valid SDM configuration wizards? (Choose three.)

A. Security Audit
B. VPN
C. STP
D. NAT

Answer: ABD

QUESTION 20
How do you define the authentication method that will be used with AAA?

A. With a method list
B. With the method command
C. With the method aaa command
D. With a method statement

Answer: A