Cisco 642-502

Securing Networks with Cisco Routers and Switches

Q&A with explanations

Version 5.0

Leading The Way
in IT Testing And Certification Tools

www.testking.com

Important Note, Please Read Carefully

Other TestKing products
A) Offline Testing engine
Use the offline Testing engine product topractice the questions in an exam environment.
B) Study Guide (not available for all exams)
Build a foundation of knowledge which will be useful also after passing the exam.

Latest Version
We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at TestKing and update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1.Go towww.testking.com
2.Click on **Member zone/Log in**
3.The latest versions of all purchased products are downloadable from here. Just click the links.
For mostupdates,itisenough just to print the new questions at the end of the new version, not the whole document.

Feedback
If you spot a possible improvement then please let us know. We always interested in improving product quality.
Feedback should be send to feedback@testking.com. You should include the following: Exam number, version, page number, question number, and your login ID.

Our experts will answer your mail promptly.

Copyright
Each iPAD file contains a unique serial number associated with your particular name and contact information for security purposes. So if we find out that a particular iPAD file is being distributed by you, TestKing reserves the right to take legal action against you according to the International Copyright Laws.

Table of Contents

Total number of questions: 145

Topic 1: Implement Layer 2 security (13 questions)

Section 1: Utilize Cisco IOS and Cat OS commands to mitigate Layer 2 attacks (5 questions)

QUESTION NO: 1
A new TestKing switch has been installed and you wish to secure it. Which Cisco Catalyst IOS command can be used to mitigate a CAM table overflow attack?

A. switch(config-if)# port-security maximum 1
B. switch(config)# switchport port-security
C. switch(config-if)# port-security
D. switch(config-if)# switchport port-security maximum 1
E. switch(config-if)# switchport access
F. switch(config-if)# access maximum 1

Answer: D
Explanation:
Enabling and Configuring Port Security:
Beginning in privileged EXEC mode, follow these steps to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to configure and enter interface configuration mode.
Step 3	switchport mode access	Set the interface mode as access; an interface in the default mode (dynamic desirable) cannot be configured as a secure port.
Step 4	switchport port-security	Enable port security on the interface.
Step 5	**switchport port-security maximum** *value*	(Optional) Set the maximum number of secure MAC addresses for the interface. The range is 1 to 132; the default is 1.

To ensure that only a single station's MAC address is allowed on a given port, specify the value of the "switchport port-security maximum" command to 1. This will safeguard against CAM overflow attacks.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps5206/products_configuration_guide_chapter09186a008

QUESTION NO: 2 SIMULATION

The following diagram displays a portion of the TestKing network:

You work for the TestKing.com, which has a server connected to their infrastructure through a switch named Houston. Although TestKing.com uses VLANs for security, an attacker is trying to overflow the CAM table by sending out spoofed MAC addresses through a port on the same switch as the server. Your task is to configure the switch to protect the switch from a CAM table overflow attack. For purposes of this test, we will assume that the attacker is plugged into port Fa0/12. The topology is pictured in the exhibit. The enable password for the switch is TestKing. The following passwords have been assigned to the Houston switch:

Console passwords: california
VTY lines 0-4 password: city
Enable passwords: TestKing

Start the simulation by clicking on the host.

Answer:
Switch1(config)# interface fastethernet0/12
Switch1(config-if)# switchport mode access
Switch1(config-if)# switchport port-security
Switch1(config-if)# switchport port-security maximum 1
Switch1(config-if)# end

Explanation:
Enabling and Configuring Port Security:

Beginning in privileged EXEC mode, follow these steps to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to configure and enter interface configuration mode.
Step 3	switchport mode access	Set the interface mode as access; an interface in the default mode (dynamic desirable) cannot be configured as a secure port.
Step 4	switchport port-security	Enable port security on the interface.
Step 5	**switchport port-security maximum** *value*	(Optional) Set the maximum number of secure MAC addresses for the interface. The range is 1 to 132; the default is 1.

To ensure that only a single station's MAC address is allowed on a given port, specify the value of the "switchport port-security maximum" command to 1. This will safeguard against CAM overflow attacks.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps5206/products_configuration_guide_chapter09186a008

QUESTION NO: 3

You want to increase the security of a newly installed switch. Which Cisco Catalyst IOS command is used to mitigate a MAC spoofing attack?

A. switch(config-if)# port-security mac-address 0000.ffff.aaaa
B. switch(config)# switchport port-security mac-address 0000.ffff.aaaa
C. switch(config-if)# switchport port-security mac-address 0000.ffff.aaaa
D. switch(config)# port-security mac-address 0000.ffff.aaaa

E. switch(config-if)# mac-address 0000.ffff.aaaa
F. switch(config)# security mac-address 0000.ffff.aaaa

Answer: C
Explanation:
You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.
If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a workstation attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs. If a workstation with a secure MAC that is address configured or learned on one secure port attempts to access another secure port, a violation is flagged.
After you have set the maximum number of secure MAC addresses on a port, the secure addresses are included in an address table in one of these ways:

You can configure all secure MAC addresses by using the **switchport port-security mac-address** mac_address interface configuration command.

You can allow the port to dynamically configure secure MAC addresses with the MAC addresses of connected devices.

You can configure a number of addresses and allow the rest to be dynamically configured.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080

QUESTION NO: 4
The security administrator for TestKing Inc. is working on defending the network against SYN flooding attacks. Which of the following are tools to protect the network from TCP SYN attacks?

A. Route authentication
B. Encryption
C. ACLs
D. TCP intercept

E. None of the above.

Answer: D
Explanation:
The TCP intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks, which are a type of denial-of-service attack.
A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a web site, accessing e-mail, using FTP service, and so on.
The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP synchronization (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. The number of SYNs per second and the number of concurrent connections proxied depends on the platform, memory, processor, and other factors
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a008(

QUESTION NO: 5
Which of the following IOS commands will you advise the TestKing trainee technician to use when setting the timeout for router terminal line?

A. exec-timeout minute [seconds]
B. line-timeout minute [seconds]
C. timeout console minute [seconds]
D. exec-time minutes [seconds]

Answer: A
Explanation:

The exec timeout command prevents unauthorized users from misusing abandoned sessions (for instance if the network administrator went on vacation and left an enabled login session active on his desktop system). There is a trade-off here between security (shorter timeouts) and usability (longer timeouts). Check your local policies and operational needs to determine the best value. In most cases, this should be no more than 10 minutes. To configure the timeout values, perform the following steps:

router(config)# line INSTANCE
router(config-line)# exec-timeout $(EXEC_TIMEOUT)
router(config-line)# exit

Reference: http://www.cisco.com/warp/public/793/access_dial/comm_server.html

Section 2: Implement Cisco Identity-Based Networking Services (2 questions)

QUESTION NO: 1
The TestKing network is implementing IBNS. In a Cisco Identity-Based Networking Service (IBNS) implementation, the endpoint that is seeking network access is known as what?

A. Host
B. Authentication
C. PC
D. Authentication server
E. Client
F. Supplicant

Answer: F
Explanation:
In IBNS, the supplicant is the end device that is seeking network access. The supplicant is a software component on the user workstation that answers a challenge from the authenticator. Supplicant functionality may also be implemented on network devices to authenticate to upstream devices.
Reference: Securing Networks with Cisco Routers and Switches (SNRS) Courseware Page 3-30.

QUESTION NO: 2
A new IBNS system is being installed in the TestKing network. The Cisco Identity-Based Networking Services (IBNS) solution is based on which two standard implementations? (Choose two.)

A. TACACS+
B. RADIUS
C. 802.11
D. 802.1x
E. 802.1q
F. IPSec

Answer: B, D
Explanation:
The Cisco IBNS solution is based on standard RADIUS and 802.1X implementations. It interoperates with all IETF authentication servers that comply with these two standards. Cisco has enhanced the Cisco Secure ACS to provide a tight integration across all Cisco switches.
Reference: Securing Networks with Cisco Routers and Switches (SNRS) Courseware Page 3-24.

Section 3: Implement Cisco 802.1X Port-Based Authentication (3 questions)

QUESTION NO: 1
You wish to configure 802.1X port control on your switch. Which three keywords are used with the dot1x port-control command? (Choose three.)

A. enable
B. force-authorized
C. force-unathorized
D. authorized
E. unauthorized
F. auto

Answer: B, C, F

Explanation:
To enable manual control of the authorization state on a port, use the "dot1x port-control" command. To return to the default setting, use the no form of this command.
dot1x port-control {auto | force-authorized | force-unauthorized}
no dot1x port-control {auto | force-authorized | force-unauthorized}
Syntax Description:

auto	Enables 802.1X authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1X authentication exchange between the switch and the client.
force-authorized	Disables 802.1X authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.
force-unauthorized	Denies all access through the specified interface by forcing the port to transition to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

Reference:
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_command_reference_chapter09186a008

QUESTION NO: 2
The TestKing network has rolled out an 802.1X based system. In an 802.1x implementation, the authenticator acts as a gateway to which device?

A. Host
B. Authenticator
C. PC
D. Authentication server
E. Client

F. Supplicant

Answer: D
Explanation:
The table below outlines the definitions for the authentication server and the authenticator:

802.1X Terminology	
Term	**Definition**
Authenticator	(Referred to as the "authenticator") entity at one end of a point-to-point LAN segment that enforces host authentication. The authenticator is independent of the actual authentication method and functions only as a pass-through for the authentication exchange. It communicates with the host, submits the information from the host to the authentication server, and authorizes the host when instructed to do so by the authentication server.
Authentication server	Entity that provides the authentication service for the authenticator PAE. It checks the credentials of the host PAE and then notifies its client, the authenticator PAE, whether the host PAE is authorized to access the LAN/switch services.

Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080

QUESTION NO: 3
The TestKing network is using an 802.1X implementation. In an 802.1x implementation, the supplicant directly connects to, and obtains network access permission through which device?

A. Host
B. Authenticator
C. PC
D. Authentication server
E. Client
F. Supplicant

Answer: B
Explanation:
In Identity Based Networking Services, the supplicant is the end device that is seeking network access. The supplicant is a software component on the user workstation that answers a challenge from the authenticator.
The authenticator is the entity at one end of a point-to-point LAN segment that enforces host authentication. The authenticator is independent of the actual authentication method and functions only as a pass-through for the authentication exchange. It communicates with the host, submits the information from the host to the authentication server, and authorizes the host when instructed to do so by the authentication server.
Reference: Securing Networks with Cisco Routers and Switches (SNRS) Courseware Page 3-30.

Section 4: Identify and describe Layer 2 security best practices (3 questions)

QUESTION NO: 1
Which two are typical Layer 2 attacks? (Choose two.)

A. MAC spoofing
B. CAM table overflow
C. Route poisoning
D. DHCP Starvation
E. ARP Starvation
F. Spam
G. Worm Hole

Answer: A, B
Explanation:
Layer 2 network attacks include all of the following:

CAM Table Overflow
VLAN Hopping
Spanning-Tree Protocol Manipulation
MAC Spoofing Attack
Private VLAN Attacks
DHCP Starvation
Cisco Discovery Protocol
VLAN Trunking Protocol
IEEE 802.1x

MAC Spoofing Attack
MAC spoofing attacks involve the use of a known MAC address of another host to attempt to make the target switch forward frames destined for the remote host to the network attacker. By sending a single frame with the other host's source Ethernet address, the network attacker overwrites the CAM table entry so that the switch forwards packets destined for the host to the network attacker. Until the host sends traffic it will not receive any traffic. When the host sends out traffic, the CAM table entry is rewritten once more so that it moves back to the original port.

CAM Table Overflow:
The CAM table in a switch contains information such as the MAC addresses available on a given physical port of a switch, as well as the associated VLAN parameters. When a Layer 2 switch receives a frame, the switch looks in the CAM table for the destination MAC address. If an entry exists for the MAC address in the CAM table, the switch forwards the frame to the port designated in the CAM table for that MAC address. If the MAC address does not exist in the CAM table, the switch forwards the frame out every port on the switch, effectively acting like a hub. If a response is seen, the switch updates the CAM table.
Reference:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008(

QUESTION NO: 2
You want to increase the security levels at layer 2 within the TestKing switched LAN. Which three are typical Layer 2 attack mitigation techniques? (Select three)

A. Switch security
B. Port security
C. ARP snooping

D. DHCP snooping
E. Port snooping
F. 802.1x authentication

Answer: B, D, F
Explanation:
Network Attack Mitigation:
Use the port security commands to mitigate MAC-spoofing attacks. The port security command provides the capability to specify the MAC address of the system connected to a particular port. The command also provides the ability to specify an action to take if a port-security violation occurs. However, as with the CAM table-overflow attack mitigation, specifying a MAC address on every port is an unmanageable solution.
Hold-down timers in the interface configuration menu can be used to mitigate ARP spoofing attacks by setting the length of time an entry will stay in the ARP cache. However, hold-down timers by themselves are insufficient. Modification of the ARP cache expiration time on all end systems would be required as well as static ARP entries. Even in a small network this approach does not scale well. One solution would be to use private VLANs to help mitigate these network attacks.
Another solution that can be used to mitigate various ARP-based network exploits is the use of DHCP snooping along with Dynamic ARP Inspection (DAI). These Catalyst feature validate ARP packets in a network and permit the interception, logging, and discarding of ARP packets with invalid MAC address to IP address bindings.
DHCP Snooping provides security by filtering trusted DHCP messages and then using these messages to build and maintain a DHCP snooping binding table. DHCP Snooping considers DHCP messages originating from any user facing port that is not a DHCP server port or an upling to a DHCP server as untrusted. From a DHCP Snooping perspective these untrusted, user-facing ports should not send DHCP server type responses such as DHCPOffer, DHCPAck, or DHCPNak. Untrusted DHCP messages are messages received from outside the network or firewall. The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information corresponding to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network. The DHCP snooping binding table can contain both dynamic as well as static MAC address to IP address bindings.
Another effective mitigation strategy is to deploy 802.1x on access switches and wireless access points to ensure that all access to the network infrastructure requires authentication. Consider deploying PEAP for use with wireless LANs.
Reference:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008(

QUESTION NO: 3
The TestKing security administrator is in charge of creating a security policy for the company. Which two statements about the creation of a security policy are true? (Choose two)

A. It helps Chief Information Officers determine the return on investment of network security at TestKing Inc.
B. It defines how to track down and prosecute policy offenders at TestKing Inc.
C. It helps determine which vendor security equipment or software is better than others.
D. It clears the general security framework so you can implement network security at TestKing Inc.
E. It provides a process to audit existing network security at TestKing Inc.
F. It defines which behavior is and is not allowed at TestKing Inc.

Answer: E, F
Explanation:
Reasons to create a network security policy:
1. Provides a process to audit existing network security
2. Provides a general security framework for implementing network security
3. Defines which behavior is and is not allowed
4. Often helps determine which tools and procedures are needed for the organization
5. Helps communicate consensus among a group of key decision-makers and defines responsibilities of users and administrators
6. Defines a process for handling network security incidents
7. Enables global security implementation and enforcement
8. Creates a basis for legal action if necessary
Reference: Managing Cisco Network Security, Cisco Press, page 43

Topic 2: Configure Cisco IOS Firewall features to meet security requirements (26 questions)

Section 1: Identify and describe the capabilities of the IOS firewall feature set (5 questions)

QUESTION NO: 1
The TestKing routers have all been upgraded to a firewall feature set IOS. What are three main components of the Cisco IOS Firewall feature set? (Choose three)

A. Context-based Access Control
B. Port security
C. Authentication proxy
D. Authentication, authorization, and accounting
E. Intrusion Prevention System
F. Neighbor router authentication

Answer: A, C, E
Explanation:
The Cisco IOS firewall feature set contains the following features:

Context-Based Access Control (CBAC)-CBAC creates temporary openings in access lists at firewall interfaces. These openings are created when specified traffic exits your internal network through the firewall. The openings allow returning traffic (that would normally be blocked) and additional data channels to enter your internal network back through the firewall. The traffic is allowed back through the firewall only if the traffic is part of the same session as the original traffic that triggered CBAC when exiting through the firewall.

Cisco IOS Intrusion Prevention System (IPS)-The Cisco IOS IPS feature restructures the existing Cisco IOS Intrusion Detection System (IDS), allowing customers to choose to load the default, built-in signatures or to load a Signature Definition File (SDF) called attack-drop.sdf onto the router. The attack-drop.sdf file contains 118 high-fidelity Intrusion Prevention System (IPS) signatures, providing customers with the latest available detection of security threats.

Cisco IOS Firewall Authentication Proxy-Authentication proxy provides dynamic, per-user authentication and authorization, authenticating users against industry standard TACACS+ and RADIUS authentication protocols. Per-user authentication and authorization of connections provide more robust protection against network attacks.
Reference:
http://www.cisco.com/en/US/products/ps5854/prod_configuration_guide09186a00802c9587.html

QUESTION NO: 2
Router TK1 is configured with the IOS firewall feature set to prevent TCP based attacks. How many incomplete connections must this router have by default before TCP Intercept will start dropping incomplete connections?

A. 500
B. 1100
C. 700
D. 900
E. 200
F. 250

Answer: B
Explanation:
Once the number of incomplete connections (TCP SYN) reaches 1100, TCP Intercept will start deleting incomplete sessions (oldest session first, by default). Configure the incomplete session threshold with the "ip tcp intercept max-incomplete high (number)" command.

QUESTION NO: 3
Which of the following represents the behavior of the CBAC aggressive mode in a Cisco IOS firewall?

A. Delete all half-open session
B. Re-initiate half open session
C. Complete all half open sessions, make the full open session
D. Delete half-open session as needed to accommodate new connection requests
E. All of the above, based on configuration

Answer: D
Explanation:

A TCP SYN attack occurs when an attacking source host generates TCP SYN packets with random source addresses and sends them in rapid succession to a victim host. The victim destination host sends a SYN ACK back to the random source address and adds an entry to the connection queue. Since the SYN ACK is destined for an incorrect or nonexistent host, the acknowledgment is never completed and the entry remains in the connection queue until a timer expires. The connection queue fills up and legitimate users cannot use TCP services. However, with CBAC, TCP packets flow from the outside only in response to traffic sent from the inside. The attacking host can't get its packets through, and the attack does not succeed. In addition, by inspecting inbound on the external interface (interface serial 0 in the example above), CBAC can account for half-open connections through the firewall and begin closing those half-open connections in an aggressive mode. The firewall will calm down once the number of half-open connections settles down to a user-defined value.

QUESTION NO: 4
What OSI layers can CBAC filter on? Select all that apply.

A. Layer 4
B. Layer 3
C. Layer 2
D. Layer 7
E. Layer 5

Answer: A, B, D
Explanation:
Access lists can filter traffic based on layer 3 and layer 4 information, while CBAC can filter traffic based on layer 3, 4, and 7 (application layer) information.

QUESTION NO: 5
Router TK1 has been upgraded with the Cisco firewall IOS. Which of the following cannot be configured on a router unless the IOS Firewall feature set is installed? (Select all that apply)

A. PAM
B. Authentication Proxy
C. IDS
D. CBAC

Answer: A, B, C, D

Explanation:

CBAC, PAM, IDS, Authentication Proxy are the four main components of the Cisco IOS Firewall and cannot be configured until the IOS Firewall feature set is installed on the router. The following table describes these features in more detail:

Context-based Access Control	"Configuring Context-Based Access Control"	Context-based Access Control (CBAC) examines not only network layer and transport layer information, but also examines the application-layer protocol information (such as FTP information) to learn about the state of TCP and UDP connections. CBAC maintains connection state information for individual connections. This state information is used to make intelligent decisions about whether packets should be permitted or denied, and dynamically creates and deletes temporary openings in the firewall. CBAC also generates real-time alerts and audit trails. Enhanced audit trail features use SYSLOG to track all network transactions. Real-time alerts send SYSLOG error messages to central management consoles upon detecting suspicious activity. Using CBAC inspection rules, you can configure alerts and audit trail information on a per-application protocol basis. CBAC is only available in the Cisco IOS Firewall feature set.
Cisco IOS Firewall Intrusion Detection System	"Configuring Cisco IOS Firewall Intrusion Detection System"	The Cisco IOS Firewall Intrusion Detection System (IDS) acts as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router, scanning each to match any of the IDS signatures. When it detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog. The network administrator can configure the IDS system to choose the appropriate response to various threats. When packets in a session match a signature, the IDS system can be configured to: • Send an alarm to a syslog server or a Cisco NetRanger Director (centralized management interface) • Drop the packet • Reset the TCP connection

Authentication Proxy	"Configuring Authentication Proxy"	The Cisco IOS Firewall authentication proxy feature allows network administrators to apply specific security policies on a per-user basis. Previously, user identity and related authorized access was associated with a user's IP address, or a single security policy had to be applied to an entire user group or sub network. Now, users can be identified and authorized on the basis of their per-user policy, and access privileges tailored on an individual basis are possible, as opposed to general policy applied across multiple users.
Port to Application Mapping	"Configuring Port to Application Mapping"	Port to Application Mapping (PAM) is a feature of Cisco IOS Firewall. PAM allows you to customize TCP or UDP port numbers for network services or applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application. The information in the PAM table enables CBAC supported services to run on nonstandard ports.

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a008(

Section 2: Configure CBAC to dynamically mitigate identified threats to the network (8 questions)

QUESTION NO: 1

Router TK1 is being used to prevent Denial of Service attacks on the TestKing network. Which three thresholds does CBAC on the Cisco IOS Firewall provide against DoS attacks? (Choose three)

A. The number of half-open sessions based upon time
B. The total number of half-open TCP or UDP sessions
C. The number of fully open sessions based upon time
D. The number of half-open TCP-only sessions per host
E. The total number of fully open TCP or UDP sessions
F. The number of fully open TCP-only sessions per host

Answer: A, B, D
Explanation:
Enhanced denial-of-service detection and prevention defends networks against popular attack modes, such as SYN (synchronize/start) flooding, port scans, and packet injection, by inspecting packet sequence numbers in TCP connections. If numbers are not within expected ranges, the router drops suspicious packets. When the router detects unusually high rates of new connections, it issues an alert message, and subsequently drops half-open TCP connection state tables. This prevents system resource depletion.
When the Cisco IOS Firewall detects a possible attack, it tracks user access by source or destination address and port pairs. It also details the transaction, creating an audit trail. The CBAC process can be configured to monitor these half opened sessions based on the total number within a given time frame, the total number at any given point, or the total number per any individual host. When the number of existing half-open sessions exceeds the max-incomplete high number, CBAC deletes half-open sessions as required to accommodate new connection requests. The software continues to delete half-open requests until the number of existing half-open sessions drops below max-incomplete low number.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps1018/prod_bulletin09186a008010e040.html

QUESTION NO: 2
The TestKing network is concerned about SPAM and wants to use IOS tools to prevent SPAM attacks. By default, how many message recipients must an email have for the IOS Firewall to consider it a spam attack?

A. 250
B. 500

C. 100
D. 25
E. 5000
F. 50000
G. None of the above

Answer: A
Explanation:
By default, the Cisco IOS Firewall will fire an alarm for a spam attack if an email contains 250 or more recipients.
To specify the number of recipients in a mail message over which a spam attack is suspected, use the "ip audit smtp" global configuration command. To set the number of recipients to the default setting, use the no form of this command.

ip audit smtp spam number-of-recipients

Syntax Description

spam	Specifies a threshold beyond which the Cisco IOS Firewall IDS alarms on spam e-mail.
number-of-recipients	Integer in the range of 1-65535 that designates the maximum number of recipients in a mail message before a spam attack is suspected. Use with the spam keyword. The default is 250 recipients.

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a008(

QUESTION NO: 3
The security administrator at TestKing is seeing a large number of half opened TCP sessions. What are half open TCP sessions?

A. Sessions that were denied.

B. Sessions that have not reached the established state.
C. Sessions where the three-way handshake has been completed.
D. Sessions where the firewall detected return traffic.

Answer: B
Explanation:
An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For UDP, "half-open" means that the firewall has detected traffic from one direction only.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_command_reference_chapter09186a008(

QUESTION NO: 4
What command configures the amount of time CBAC will wait for a TCP session to become established before dropping the connection in the state table?

A. ip inspect global syn-establish (seconds)
B. ip inspect tcp global syn-time (seconds)
C. ip inspect global tcp syn (seconds)
D. ip inspect tcp synwait-time (seconds)
E. None of the above

Answer: D
Explanation:
Use the IOS Firewall global configuration mode command ip inspect tcp synwait-time (seconds) command to set the CBAC timeout value for TCP session establishment. The default is 30 seconds.

QUESTION NO: 5
You have been tasked with setting up a new router with CBAC. How do you configure the CBAC global UDP idle session timeout?

A. ip inspect udp-session-timeout (seconds)
B. ip inspect udp-idle (seconds)

C. ip inspect udp-timeout (seconds)
D. ip inspect udp idle-time (seconds)

Answer: D
Explanation:
Determine the global UDP idle session state table timeout value with the ip inspect udp idle-time (seconds) command. This global value (along with the global tcp idle timeout) can be overridden on a per-protocol basis.

QUESTION NO: 6
You have been tasked with setting up a new TestKing router with CBAC. How do you set the threshold of half-open sessions CBAC will allow per minute before deleting them?

A. ip inspect one-minute incomplete (number)
B. ip inspect one-minute (number)
C. ip inspect one-minute high (number)
D. ip inspect one-minute high incomplete (number)
E. ip inspect max-incomplete minute high (number)

Answer: C
Explanation:
The "ip inspect one-minute high (number)" command will set the number of new, half-open connections per minute CBAC will allow before deleting them. The default is 500 per minute.

QUESTION NO: 7
You are setting up a new TestKing router with CBAC. Which of the following commands will alter the CBAC DNS timeout timer to 10 seconds?

A. ip inspect dns-server-timeout 10
B. ip inspect dns-server-timer 10
C. ip inspect dns-timeout 10
D. ip inspect dns-timer 10

Answer: C
Explanation:
To configure the time CBAC will keep a DNS session open in the state table, use the global configuration command ip inspect dns-timeout (seconds). The default is five seconds.

QUESTION NO: 8
You are setting up a new TestKing router with CBAC. If CBAC is configured to inspect telnet traffic on an interface, how should outbound telnet traffic be configured in any ACL's?

A. Outbound telnet should be permitted in any acl's
B. Outbound telnet should be denied in any acl's
C. Telnet should not be referenced at all in the acl
D. Outbound telnet should be denied only if inbound telnet is allowed

Answer: A
Explanation:
With CBAC, the ACL's need to allow the initial outbound traffic. If the traffic is not allowed outbound access, CBAC will not have a chance to monitor and restrict the return session traffic.

Section 3: Verify and troubleshoot CBAC configuration and operation (4 questions)

QUESTION NO: 1
CBAC has been configured on router TK1 to increase the security of the TestKing network. CBAC intelligently filters TCP and UDP packets based on which protocol-session information?

A. Network layer
B. Transport layer
C. Data-link
D. Application layer
E. Presentation layer

F. Session layer
G. Physical layer

Answer: D
Explanation:
Context-based Access Control (CBAC) in Cisco IOS Firewall is an advanced traffic filtering technology that intelligently filters transmission control protocol (TCP) and user datagram protocol (UDP) packets to determine whether they contain malicious viruses or worms. CBAC can be configured to permit specified TCP and UDP traffic through a firewall only when the connection is initiated from within the network to be protected. Without CBAC, traffic filtering is limited to access list implementations that examine packets at the network layer or at the transport layer. CBAC examines not only these but also the application-layer protocol information to learn about the state of a TCP or UDP session.

QUESTION NO: 2
John and Kathy are working on configuring the IOS firewall together. They are figuring out what CBAC uses for inspection rules to configure on a per-application protocol basis. Which one of these is the correct one?

A. ODBC filtering
B. Tunnel, transport models, or both
C. Alerts and audit trails
D. Stateful failover
E. None of the above

Answer: C
Explanation:
CBAC also generates real-time alerts and audit trails. Enhanced audit trail features use SYSLOG to track all network transactions. Real-time alerts send SYSLOG error messages to central management consoles upon detecting suspicious activity. Using CBAC inspection rules, you can configure alerts and audit trail information on a per-application protocol basis.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a008(

QUESTION NO: 3
You are the security administrator for TestKing and you need to know what CBAC does on the Cisco IOS Firewall. Which one of these is the best answer?

A. Creates specific security policies for each user at TestKing Inc.
B. Provides additional visibility at intranet, extranet, and Internet perimeters at TestKing Inc.
C. Protects the network from internal attacks and threats at TestKing Inc.
D. Provides secure, per-application access control across network perimeters at TestKing Inc.

Answer: D
Explanation:
Context-based Access Control (CBAC) examines not only networklayer and transportlayer information, but also examines the application-layer protocol information (such as FTP information) to learn about the state of TCP and UDP connections. CBAC maintains connection state information for individual connections. This state information is used to make intelligent decisions about whether packets should be permitted or denied, and dynamically creates and deletes temporary openings in the firewall.
Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a008(

QUESTION NO: 4
By default, how many half-open sessions need to be in the state table before CBAC will begin to delete the half-open sessions?

A. 500
B. 250
C. 1000
D. 2000
E. 100
F. 50

Answer: A
Explanation:

By default, CBAC will begin to delete half-open sessions when there are 500 in the state table. It will keep deleting half-open sessions until the minimum half-open sessions threshold is met (default is 400).

Section 4: Configure authentication proxy to apply security policies on a per-user basis (5 questions)

QUESTION NO: 1
The authentication proxy feature has been configured on one of the TestKing routers. What does authentication proxy on the Cisco IOS Firewall do?

A. Creates specific authorization policies for each user with Cisco Secure ACS, dynamic, per-user security and authorization
B. Provides additional visibility at intranet, extranet, and Internet perimeters
C. Creates specific security policies for each user with Cisco Secure ACS, dynamic, per-user authentication and authorization
D. Provides secure, per-application access control across network perimeters

Answer: C
Explanation:
The Cisco IOS Firewall authentication proxy feature allows network administrators to apply specific security policies on a per-user basis. Previously, user identity and related authorized access was associated with a user's IP address, or a single security policy had to be applied to an entire user group or sub network. Now, users can be identified and authorized on the basis of their per-user policy, and access privileges tailored on an individual basis are possible, as opposed to general policy applied across multiple users. With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecureACS, or other RADIUS, or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a008(

QUESTION NO: 2
You have been tasked with configuring authentication proxy on one of the TestKing routers. Which command is required to specify the authorization protocol for authentication proxy?

A. auth-proxy group tacacs+
B. aaa auth-proxy default group tacacs+
C. authorization auth-proxy default group tacacs+
D. aaa authorization auth-proxy default group tacacs+
E. aaa authorization auth-proxy group tacacs+
F. aaa authorization auth-proxy default group

Answer: D
Explanation:
To configure authentication proxy for accounting, begin by using the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa new-model	Enables AAA.
Step 2	Router(config)# aaa authentication login default group tacacs+	Defines the list of authentication methods at login.
Step 3	Router(config)# aaa authorization auth-proxy default group tacacs+	Uses the auth-proxy keyword to enable authentication proxy for AAA methods.

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a0080080348.html

QUESTION NO: 3

The TestKing administrator is working on configuring the authentication proxy feature. Which of the following best describes the authentication proxy feature of the Cisco IOS?

A. Use a general policy applied across multiple TestKing Inc. users
B. Use a single security policy that is applied to an entire user group or subnet at TestKing Inc.
C. Apply specific security polices on a per-user basis at TestKing Inc.
D. Keep the TestKing Inc. user profiles active even where there is no active traffic from the authenticated users.

Answer: C
Explanation:
The Cisco IOS Firewall authentication proxy feature allows network administrators to apply specific security policies on a per-user basis. Previously, user identity and related authorized access was associated with a user's IP address, or a single security policy had to be applied to an entire user group or sub network. Now, users can be identified and authorized on the basis of their per-user policy, and access privileges tailored on an individual basis are possible, as opposed to general policy applied across multiple users. With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecureACS, or other RADIUS, or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a008(

QUESTION NO: 4
You are configuring the authentication feature on a new TestKing router. Which of the following correctly sets the IOS Firewall authentication-proxy idle timer to 20 minutes?

A. ip auth-proxy auth-cache 20
B. ip auth-proxy auth-time 20
C. ip auth-proxy auth-cache-time 20
D. ip auth-proxy idle 20
E. ip auth-proxy idle timer 20

Answer: C
Explanation:
Use the global configuration mode command "ip auth-proxy auth-cache-time (minutes)" to determine the acceptable idle period for users authenticated through the IOS Firewall before they must re-authenticate.

QUESTION NO: 5
You are configuring the authentication feature on a new TestKing router. Which of the following configures an authentication proxy rule for the IOS Firewall?

A. ip inspect-proxy name proxyname http
B. ip auth-proxy name proxyname http
C. ip auth-rule proxyname http
D. ip proxy-name proxyname http

Answer: B
Explanation:
Create an authentication proxy rule with the global configuration mode command ip auth-proxy name (name) http. Apply the proxy rule to an interface to force users to authenticate through the firewall.

Section 5: Verify and troubleshoot authentication proxy configuration and operation (4 questions)

QUESTION NO: 1
The authentication proxy feature has been configured on one of the TestKing routers. Where are access profiles stored with the authentication proxy features of the Cisco IOS Firewall?

A. PIX Firewall
B. Cisco router
C. Cisco VPN Concentrator
D. Cisco Secure ACS authentication server

Answer: D
Explanation:
With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecureACS, or other RADIUS, or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a008(

QUESTION NO: 2
Refer to the output of a "sh ip auth-proxy cache" command issued on a TestKing router below. Which port is being used by the client?

TK2# sh ip auth-proxy cache
Authentication Proxy Cache
Client Name aaauser, Client IP 10.0.2.12, Port 2636, timeout 5, Time Remaining 3, state ESTAB

Based on this information, which port is being used by the client?

A. 1645
B. 1646
C. 1812
D. 2636
E. 2640
F. 8080

Answer: D
Explanation:
Use the "show ip auth-proxy" to display either the authentication proxy entries or the running authentication proxy configuration. Use the cache keyword to list the host IP address, the source port number, the timeout value for the authentication proxy, and the state for connections using authentication proxy. If authentication proxy state is HTTP_ESTAB, the user authentication was successful. In this example, the client was established using port 2636.

QUESTION NO: 3
How does a user on the TestKing LAN trigger the authentication proxy after the idle timer has expired?

A. The proxy authenticates the user
B. The user initiates another HTTP session
C. The user enters a new username and password
D. The user enters a valid username and password
E. None of the above

Answer: B
Explanation:
How the Authentication Proxy Works:
When a user initiates an HTTP session through the firewall, the authentication proxy is triggered. The authentication proxy first checks to see if the user has been authenticated. If a valid authentication entry exists for the user, the connection is completed with no further intervention by the authentication proxy. If no entry exists, the authentication proxy responds to the HTTP connection request by prompting the user for a username and password.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a008(

QUESTION NO: 4
Router TK1 has been configured for authentication proxy. What is the default idle time of an enabled IOS Firewall authentication proxy?

A. 5 seconds
B. 50 seconds
C. 5 minutes
D. 60 minutes
E. 3600 minutes
F. 1 Day

Answer: D
Explanation:

To set the authentication proxy idle timeout value (the length of time an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity), use the "ipauth-proxy auth-cache-time" command in global configuration mode. To set the default value, use the no form of this command.

ip auth-proxy auth-cache-time min
Syntax Description

min	Specifies the length of time in minutes that an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity. Enter a value in the range 1 to 2,147,483,647. The default value is 60 minutes.

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_command_reference_chapter09186a008(

Topic 3: Configure Cisco IOS-based IPS to identify and mitigate threats to network resources (20 questions)

Section 1: Identify and describe the capabilities of the IOS-IPS feature set (6 questions)

QUESTION NO: 1
A new TestKing router is being configured for IDS services. Choose the two types of signature implementations that the IOS Firewall IDS can detect. (Choose two.)

A. Atomic
B. Dynamic
C. Regenerative
D. Cyclical
E. Compound
F. Complex

Answer: A, E
Explanation:
The Cisco IOS firewall IDS can detect atomic and compound signatures:
Atomic signatures detect simple patterns (ie: attempt on a specific host or within a single packet) while compound signatures detect complex patterns (ie: attack on multiple hosts, over extended time periods with multiple packets).

QUESTION NO: 2
On router R2, the "show ip ips config" command was issued as shown below:

```
R2#sh ip ips conf
Configured SDF Locations:
 flash:my-signatures.sdf
Builtin signatures are enabled but not loaded
Last successful SDF load time: 03:55:17 UTC Mar 2 2002
IDS fail closed is enabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through Net Director is disabled
Event notification through SDEE is disabled
Total Active Signatures: 183
Total Inactive Signatures: 0
Signature 1107:0 disable
PostOffice:HostID:0 OrgID:0 Msg dropped:0
        :Curr Event Buf Size:0  Configured:100
Post Office is not enabled - No connections are active
IDS Rule Configuration
 IPS name SECURIPS
Interface Configuration
 Interface FastEthernet0/1
  Inbound IPS rule is SECURIFS
  Outgoing IPS rule is not set
```


Refer to the exhibit. Given the output of the show ip ips configuration command, how many signatures are active?

A. 0

B. 50
C. 83
D. 100
E. 183
F. 1107
G. None of the above.

Answer: E
Explanation:
From the output shown above the total number of active signatures that this router is monitoring is 183.
Note: The 1107:0 signature is a specific signature ID, which has been manually disabled in this example. This value does not refer to the total number of signatures.

QUESTION NO: 3
Select two issues that you should consider when implementing IOS Firewall IDS. (Choose two)

A. The memory usage
B. The number of DMZs
C. The signature coverage
D. The number of router interfaces
E. The signature length

Answer: A, C
Explanation:
The performance impact of intrusion detection will depend on the configuration of the signatures, the level of traffic on the router, the router platform, and other individual features enabled on the router such as encryption, source route bridging, and so on. Enabling or disabling individual signatures will not alter performance significantly; however, signatures that are configured to use Access Control Lists will have a significant performance impact.
Because this router is being used as a security device, no packet will be allowed to bypass the security mechanisms. The IDS process in the Cisco IOS Firewall router sits directly in the packet path and thus will search each packet for signature matches. In some cases, the entire packet will need to be searched, and state information and even application state and awareness must be maintained by the router.

For auditing atomic signatures, there is no traffic-dependent memory requirement, but the memory usage should be monitored with IDS. For auditing compound signatures, CBAC allocates memory to maintain the state of each session for each connection. Memory is also allocated for the configuration database and for internal caching.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a008(

QUESTION NO: 4
To prevent against attacks on your network, you have enabled your router for Intrusion Detection Services. What are the three actions that the IOS Firewall IDS router may perform when a packet, or a number of packets in a session, match a signature? (Choose three)

A. Forward packet to the Cisco IDS Host Sensor for further analysis
B. Send an alarm to the Cisco IDS Directory or Syslog server
C. Send an alarm to Cisco Secure ACS
D. Set the packet reset flag and forward the packet through
E. Drop the packet immediately
F. Return the packet to the sender

Answer: B, D, E
Explanation:
The Cisco IOS firewall IDS can be configured to react to suspected malicious traffic in any combination of three ways:
1) Send an alarm - The Cisco IOS firewall IDS can be configured to send an alarm to a syslog server or a centralized management system such as the Cisco Secure IDS Director, the IDS Management Console (IDS MC), the Cisco IDS Event Viewer, or the Cisco Secure Policy Manager (CSPM).
2) Drop the packet - The Cisco IOS firewall can dynamically create an access list that allows the system to drop the incoming packet.
3) Reset the TCP connection - The Cisco IOS firewall can forward packets to both source and destination with the RESET flag set.
Reference: CCSP student guide, p.283

QUESTION NO: 5

A packet is passing through a TestKing IOS IDS system. Which module is audited first when packets enter an IOS Firewall IDS and match a specific audit rule?

A. TCP
B. ICMP
C. IP
D. Application level
E. UDP

Answer: C
Packets going through the interface that match the audit rule are audited by a series of modules, starting with IP; and then either ICMP, TCP, or UDP (as appropriate); and finally, the Application level.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide_chapter09186a00800881c

QUESTION NO: 6
The IOS Firewall is capable of taking certain types of action in cases where a packet or a number of packets in a session, match a signature. What are these actions? (Choose all that apply)

A. It will drop the packet immediately
B. It can return the packet to the sender
C. It can forward packet to the Cisco Ids Host Sensor for further analysis
D. It will the Cisco IDS Director or Syslog server by sending an alarm to it
E. It will send an alarm to Cisco Secure ACS
F. It can set the packets' reset flag and forward the packet through

Answer: A, D, F
Explanation:
The Cisco IOS firewall IDS can be configured to react to suspected malicious traffic in any combination of three ways:
1) Send an alarm - The Cisco IOS firewall IDS can be configured to send an alarm to a syslog server or a centralized management system such as the Cisco Secure IDS Director, the IDS Management Console (IDS MC), the Cisco IDS Event Viewer, or the Cisco Secure Policy Manager (CSPM).

2) Drop the packet - The Cisco IOS firewall can dynamically create an access list that allows the system to drop the incoming packet.
3) Reset the TCP connection - The Cisco IOS firewall can forward packets to both source and destination with the RESET flag set.
Reference: CCSP student guide, p.283

Section 2:Configure the IPS features to identify threats and dynamically block them from entering the network (7 questions)

QUESTION NO: 1
A new Cisco IDS system has been installed to protect the TestKing network from outside attacks. What kind of signatures trigger on a single packet? (Choose one)

A. Regenerative
B. Cyclical
C. Atomic
D. Dynamic
E. Compound
F. None of the above

Answer: C
Explanation:
An atomic attack represents exploits contained within a single packet. For example, the "ping of death" attack is a single, abnormally large ICMP packet.

QUESTION NO: 2
A perimeter router configured for TCP Intercept is being installed in the TestKing network to prevent TCP based attacks. What is the default mode TCP Intercept operates in?

A. Intercept
B. Aggressive
C. 3-way
D. Responsive

E. Watch

Answer: A
Explanation:
TCP Intercept can be in either intercept mode or passive watch mode. In intercept mode, each TCP SYN packet will be intercepted and responded to on behalf of the server it is protecting. With passive watch mode, TCP Intercept monitors the connection to the server to make sure the connection becomes complete. If the server cannot complete the connection within a configurable time period, TCP Intercept will send a reset packet to the server, clearing up the server's resources.

QUESTION NO: 3
You are configuring a new TestKing router to prevent SPAM attacks. Which of the following commands correctly sets the IOS Firewall IDS spam threshold?

A. ip audit smtp spam 500
B. ip audit smtp spam 500 notify
C. ip audit smtp name spam 500
D. ip audit ids spam 500
E. None of the above

Answer: A
Explanation:
Set the threshold at which a spam alarm is triggered for the number of recipients in an email with the "ip audit smtp spam (number)" command.

QUESTION NO: 4
While logged into a TestKing router, which of the following commands can be used to verify your IOS Firewall IDS configuration? (Select all that apply)

A. show ip audit attack
B. show ip audit statistics
C. show ip audit all
D. show ip audit tcp
E. show ip audit info

Answer: B, C
Explanation:
To verify your IOS Firewall IDS configuration there are six options with the show ip audit command: all, configuration, interfaces, name, sessions, and statistics.

QUESTION NO: 5
While logged into a TestKing router, which of the following commands specifies that the IOS Firewall IDS engine drops packets and resets TCP connections for information signatures?

A. ip audit name audit1 info attack drop reset
B. ip audit name audit1 info action drop reset
C. ip audit name audit1 info sig action drop reset
D. ip audit name audit1 sig info drop reset
E. None of the above

Answer: B
Explanation:
Specify the action the IOS Firewall IDS engine should take (reset, drop, alarm) for informational and attacks signatures with the ip audit name command.

QUESTION NO: 6
Which of the following commands disables an IOS Firewall IDS signature from being scanned in a TestKing Cisco router?

A. ip audit ids attack signature (sig#) disable
B. ip audit ids signature (sig#) disable
C. ip audit attack signature (sig#) disable
D. ip audit signature (sig#) disable
E. None of the above

Answer: D
Explanation:
Use the ip audit signature (signature number) disable command to stop the IOS Firewall from scanning traffic for that signature attack.

QUESTION NO: 7
Kathy the security administrator is working on the IOS Firewall IDS feature. She needs to select the command used to configure the IOS Firewall IDS to globally disable a specific signature.

A. ip audit signature sig-id global
B. ip audit signature sig-id disable
C. ip audit disable sig-id
D. ip audit disable signature sig-id

Answer: B
Explanation
To attach a policy to a signature, use the ip audit signature command in global configuration mode. To remove the policy, use the no form of this command. If the policy disabled a signature, then the no form of this command reenables the signature. If the policy attached an access list to the signature, the no form of this command removes the access list.
ipaudit signature signature-id {disable | list acl-list}
noip audit signature signature-id
Syntax Description:
signature-id - Unique integer specifying a signature as defined in the NetRanger Network Security Database.
Disable - Disables the ACL associated with the signature.
List - Specifies an ACL to associate with the signature.
acl-list - Unique integer specifying a configured ACL on the router. Use with the list keyword.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a008(

Section 3:Verify and troubleshoot IDS operation (4 questions)

QUESTION NO: 1

You need to configure a TestKing router to support IPS features. What is the purpose of the "ip ips sdf builtin" command?

A. to load IPS on a router using the built-in signatures
B. to load IP on a router using the attack-drop signatures
C. to unload IPS built-in signatures
D. to delete the IPS built-in signatures
E. to load IPS on a router using the built-in micro-engine
F. to disable IPS on a router using the built-in micro-engine

Answer: A
Explanation:
Normally, when an IPS router boots up, the built-in signature files are loaded. To instruct the router not to load the built-in signatures if it cannot find the specified signature definition files (SDFs), use the "no ip ips sdf builtin" command in global configuration mode. To instruct the router to use the pre-built signature files upon startup, use the "ip ips sdf builtin" command.
Note:
If the no ip ips sdf builtin command is issued and the router running Intrusion Prevention System (IPS) fails to load the SDF, you will receive an error message stating that IPS is completely disabled.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a008(

QUESTION NO: 2
Johnis the administrator at TestKing Inc. and his assignment today is to find the two types of signature implementations that the IOS Firewall IDS can detect. Which two are correct? (Choose two)

A. Atomic
B. Compound
C. Dynamic
D. Regenerative
E. Cyclical
F. Complex

Answer: A, B

Explanation:
Cisco IOS Firewall IDS Signature List
The following is a complete list of Cisco IOS Firewall IDS signatures. A signature detects patterns of misuse in network traffic. In Cisco IOS Firewall IDS, signatures are categorized into four types:
1. Info Atomic
2. Info Compound
3. Attack Atomic
4. Attack Compound
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a008(

QUESTION NO: 3
James the administrator of TestKing Inc. is working on the IDS for the network. He needs to know what kind of signatures trigger on a single packet. (Choose one)

A. Regenerative
B. Cyclical
C. Dynamic
D. Atomic
E. Compound

Answer: D
The signature structure indicates whether the signature implementation is either content or composite. Atomic signatures occur in a single packet, whereas composite signatures can be spread across multiple packets.
Reference: Cisco Secure Intrusion Detection System (Cisco Press) page 192

QUESTION NO: 4
What type of IDS attack is spread out over multiple packets?

A. Atomic
B. Arbitrary
C. Aggregate
D. Compound
E. None of the above

Answer: D
Explanation:
When an IDS signature attack uses multiple packets, it's called a compound attack. For the IOS Firewall to detect this type of attack, it must keep suspicious packets in memory to follow up on later packets of the session to see if it is an actual attack.

Section 4:Maintain and update the signatures (3 questions)

QUESTION NO: 1
You wish to disable the signature with ID 1000 on your router. Choose the correct command to disable signature 1000 in the SDF file on this router.

A. 1000 disable
B. no ip ips signature 1000
C. no ip ips dignature 1000 enable
D. ip ips signature 1000 disable
E. ip signature 1000 disable
F. signature 1000 disable

Answer: D
Explanation:
To instruct the router to scan for a given signature but not take any action if the signature is detected, use the ip ips signature command in global configuration mode.

ip ips signature signature-id [sub-signature-id] disable [list acl-list]

You may want to disable a signature (or set of signatures) if your deployment scenario deems the signatures unnecessary. The following example shows how to instruct the router not to report on signature 1000, if detected:

TK1(config)ip ips signature 1000 disable

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a008(

QUESTION NO: 2
Choose the correct command that will load the SDF into a new TestKing router and merge the new signatures with those that are already loaded in this router.

A. copy flash ips-sdf
B. copy url ips-sdf
C. copy ips-sdf url
D. write flash ips-sdf
E. write ips-sdf url
F. write url ips-sdf

Answer: B
Explanation:
Issue the copy url ips-sdf command to load the SDF in the router from the location specified via the url argument. When the new SDF is loaded, it is merged with the SDF that is already loaded in the router, unless the /erase keyword is issued, which overwrites the current SDF with the new SDF.
CiscoIOS Intrusion Prevention System (IPS) will attempt to retrieve the SDF from each specified location in the order in which they were configured in the startup configuration. If Cisco IOS IPS cannot retrieve the signatures from any of the specified locations, the built-in signatures will be used.
If the no ip ips sdf built-in command is used, Cisco IOS IPS will fail to load. IPS will then rely on the configuration of the ip ips fail command to either fail open or fail closed.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a008(

QUESTION NO: 3
The SDF uses which type of file format, with a definition of each signature along with relevant configurable actions?

A. ASCI
B. HTML
C. JPEG
D. Word

E. Text
F. XML
G. None of the above

Answer: F
Explanation:
Signature Definition File (SDF):
The SDF is integral to Cisco IOS Software IPS. The SDF is an Extensible Markup Language (XML) file with a definition of each signature along with relevant configurable actions. Cisco IOS Software IPS reads in the SDF, parses the XML, and populates its internal tables with the information necessary to detect each signature. The SDF contains the signature definition and configuration. Actions such as alarm, drop, or reset can be selected for individual signatures within the SDF. The SDF can be modified so the router will only detect specific signatures; as a result, it can contain all or asubset of the signatures supported in Cisco IOS Software IPS. The user specifies the location of the SDF. The SDF can reside on the local flash file system (recommended) or on a remote server.
Reference:
http://www.cisco.com/en/US/products/ps6634/products_white_paper0900aecd80327257.shtml

Topic 4: Configure basic IPSec VPNs to secure site-to-site and remote access to network resources (44 questions)

Section 1: Select the correct IPSecimplementation based on specific stated requirements (6 questions)

QUESTION NO: 1
Router TK1 is being configured for IPSec. After configuring multiple transform sets, where do you specify the transform sets?

A. ACL
B. ISAKMP policy
C. Router interface
D. Crypto map entry

Answer: D

Explanation:
The "crypto map set transform-set" command is used to specify which transform sets can be used with the crypto map entry. List multiple transform sets in order of priority, with the highest-priority transform set first.
Reference: Cisco Secure PIX Firewall (Cisco Press) page 217

QUESTION NO: 2
Two TestKing hosts need to securely pass data between them. Which ESP mode is used to provide end-to-end protection of message payload between two hosts?

A. Transport mode
B. Encrypted mode
C. ESP mode
D. Tunnel mode
E. None of the above

Answer: A
Explanation:
With ESP, there are two modes of operation: transport mode is used to encrypt normal connections between two hosts; tunnel mode encapsulates the original package in a new header. Tunnel mode is to be used when the destination is a VPN gateway.

QUESTION NO: 3 DRAG DROP
You have entered configuration mode on a new TestKing VPN router in order to create an ISAKMP policy using pre-shared keys, 3DES encryption, and DH Group 2. Click and drag the five necessary commands to the ordered steps below:

Answer:
Explanation:

QUESTION NO: 4
Crypto access lists have been configured on a TestKing IPSec router. What are two functions that crypto ACLs perform? (Choose two)

A. Bypasses outbound traffic that should be protected by IPSec
B. Select inbound traffic that should be protected by IPSec
C. Selects outbound traffic that should be protected by IPSec
D. Sends outbound traffic that should not be protected by IPSec as clear text
E. Discards outbound traffic that should not be protected by IPSec
F. Discards outbound traffic that requires protection by IPSec

Answer: C, D
Explanation:
Crypto access lists are used to define which IP traffic will be protected by crypto and which traffic will not be protected by crypto. For example, access lists can be created to protect all IP traffic between Subnet A and Subnet Y or between Host A and Host B. (These access lists are similar to access lists used with the access-group command. With the access-group command, the access-list determines which traffic to forward or block at an interface.)

The access lists themselves are not specific to IPSec. It is the crypto map entry referencing the specific access list that defines whether IPSec processing is applied to the traffic matching a permit in the access list. For traffic not matching, the packets are to be process normally and forwarded as clear text.
Crypto access lists associated with IPSec crypto map entries have four primary functions:
1. Select outbound traffic to be protected by IPSec (permit = protect).
2. Indicate the data flow to be protected by the new security associations (specified by a single permit entry) when initiating negotiations for IPSec security associations.
3. Process inbound traffic to filter out and discard traffic that should have been protected by IPSec.
4. Determine whether or not to accept requests for IPSec security associations on behalf of the requested data flows when processing IKE negotiation from the peer. (Negotiation is only done for ipsec-isakmp crypto map entries.) In order for the peer's request to be accepted during negotiation, the peer must specify a data flow that is "permitted" by a crypto access list associated with an ipsec-isakmp crypto map command entry.

Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_user_guide_chapter09186a0080089921.h

QUESTION NO: 5
A co-worker at TestKing wants to know which type of key exchange mechanism is Diffie-Hellman. What is the correct answer?

A. Private key exchange
B. RSA keying
C. Public key exchange
D. AES key exchange
E. All of the above.

Answer: C
Explanation:
Diffie-Hellman is used to securely exchange public keys so that shared secret keys can be securely generated for use as DES keys.
Reference: Managing Cisco Network Security (Cisco Press) page 467

QUESTION NO: 6

John the security administrator is configuring a Cisco router for IPSec using pre-shared keys, why should he configure a crypto map with two peers specified for redundancy?

A. The second peer becomes the primary peer.
B. The second peer monitors activity of the first peer.
C. If the first peer cannot be contacted, the second peer is used.
D. There are not circumstances in which you should do this.

Answer: C
Explanation:
You can define multiple peers by using crypto maps to allow for redundancy. If one peer fails, there will still be a protected path. The peer that packets are actually sent to is determined by the last peer that the PIX Firewall heard from (received either traffic or a negotiation request from) for a given data flow. If the attempt fails with the first peer, IKE tries the next peer on the crypto map list.

Section 2: Configure IPSecEncryption for site-to-site VPN using pre-shared keys (10 questions)

QUESTION NO: 1
You are configuring IPSec on one of the TestKing routers. Choose the correct command to allow IKE to establish the IPSec security associations on this router.

A. crypto map 10 isakmp
B. crypto map 10 manual
C. crypto map MYMAP ipsec-isakmp
D. crypto map MYMAP ipsec-manual
E. crypto map MYMAP 10 ipsec-isakmp
F. crypto map MYMAP 10 ipsec-manual

Answer: E
Explanation:
Creating Crypto Map Entries that Use IKE to Establish Security Associations:

When IKE is used to establish security associations, the IPSec peers can negotiate the settings they will use for the new security associations. This means that you can specify lists (such as lists of acceptable transforms) within the crypto map entry.
To create crypto map entries that will use IKE to establish the security associations, use the following command in global configuration mode:

Step	Command	Purpose
1	crypto map *map-name seq-num* **ipsec-isakmp**	Names the crypto map entry to create (or modify). This command puts you into the crypto map configuration mode.

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a008(

QUESTION NO: 2
The following output was seen from the TestKing router named R2:

R2#**sh crypto ipsec sa**

interface: FastEthernet0/1
Crypto map tag: MYMAP, local addr 172.30.2.2

protected vrf: (none)
local ident (addr/mask/prot/port): (172.30.2.2/255.255.255.255/0/0
remote ident (addr/mask/prot/port): (172.30.7.2/255.255.255.255/0/0
current_peer 172.30.7.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 172.30.2.2, remote crypto endpt.: 172.30.7.2
path mtu 1500, ip mtu 1500
current outbound spi: 0x5FAA1A55(1604983381)

inbound esp sas:
spi: 0x2831CBC6(674352070)
transform: esp-des ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: 1, crypto map: MYMAP
sa timing: remaining key lifetime (k/sec): (4511705/3537)
IV size: 8 bytes
replay detection support: N
Status: **ACTIVE**

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x5FAA1A55(1604983381)
transform: esp-des ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: 2, crypto map: MYMAP
sa timing: remaining key lifetime (k/sec): (4511705/3524)
IV size: 8 bytes
replay detection support: N

Given the output of the show crypto ipsec sa command shown above, which encryption algorithm is being used?

A. PCP
B. ESP
C. DES
D. 3DES
E. AH
F. HMAC

Answer: C
Explanation:
With any IPSec communication process, there are really two separate uni-directional tunnels being created. One is used for inbound traffic, and the other is used for outbound communications. As can be seen from the output shown above, the transform set for each is specified as ESP-DES, meaning that the ESP is used (as opposed to the alternative AH), and DES is being used as the encryption algorithm.

QUESTION NO: 3
You are configuring the IPSEC timers on a TestKing router. Which of the following commands correctly sets the IPSEC SA lifetime value to 30 minutes?

A. crypto ipsec sa lifetime 30
B. crypto ipsec security-association lifetime 1800
C. crypto ipsec sa lifetime 1800
D. crypto ipsec security-association lifetime 30

Answer: B
Explanation:

The IPSEC SA lifetime value can be configured between 120 and 86,400 seconds with the command: crypto ipsec security-association lifetime (seconds). You can also set the IPSEC SA lifetime value in kilobytes transmitted with the crypto ipsec security-association lifetime kilobytes (kilobytes) command. Whenever either value (seconds elapsed or kilobytes transmitted) is reached, the Security Associations will need to be renegotiated. These commands can be entered in global configuration mode, thus applying them to all SA's, or can be configured in crypto map configuration mode. Lifetime values entered in crypto map configuration will override the global configuration values.

QUESTION NO: 4
You need to configure a TestKing router for IPSEC. Which of the following correctly configures authentication and encryption for an IPSEC transform set?

A. crypto ipsec transform-set secure ah-hmac-md5 esp-des
B. crypto ipsec transform-set secure ah-md5 esp-3des
C. crypto ipsec transform-set secure esp-sha-hmac esp-3des
D. crypto ipsec transform-set secure ah-md5 esp-des-hmac

Answer: C
Explanation:
This transform set uses esp-3des for encryption, and uses esp-sha-hmac for authentication. The transform set in answer D is close, but the authentication transform would need to read like this: ah-md5-hmac.

QUESTION NO: 5
You want to configure a TestKing router for IPSec using default values. Which of the following is NOT an IOS Firewall default IKE policy parameter?

A. MD5
B. DH group 1
C. DES
D. Lifetime 86,400 seconds
E. RSA-Signatures

Answer: A

Explanation:
Answers A through E are the default IOS Firewall router IKE policy values, except for answer A, MD5. (The default IKE hash algorithm used is SHA-1). Although MD5 can be configured, the default is SHA-1.

QUESTION NO: 6
You need to configure a Cisco router for IPSec. Which of the following Cisco IOS router commands will properly configure pre-shared keys for IKE authentication?

A. Router(config-crypto)#authentication pre-share
B. Router(config-policy)#authentication pre-share
C. Router(config-isakmp)#authentication pre-share
D. Router(config-ike)#authentication pre-share

Answer: C
Explanation:
Configure IKE policy parameters in isakmp configuration mode (Router(config-isakmp)#).
The initial detailed steps are as follows:
DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** Example: Router# configure terminal	Enters global configuration mode.
Step 3	**crypto isakmp policy** Example: Router(config)# crypto isakmp policy 1	Defines an Internet Key Exchange (IKE) policy and enables ISAKMP policy configuration mode.
Step 4	**encryption** Example: Router(config-isakmp)# encryption 3des	Specifies the encryption algorithm within an IKE policy.
Step 5	**hash** Example: Router(config-isakmp)# hash md5	Specifies the hash algorithm within an IKE policy.
Step 6	**authentication** Example: Router(config-isakmp)# authentication pre-share	Specifies the authentication method within an IKE policy.
Step 7	**exit** Example: Router(config-isakmp)# exit	Exits ISAKMP policy configuration mode and enables global configuration mode.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide_chapter09186a008032a10

QUESTION NO: 7
You are configuring a TestKing router for IPSec. What type of crypto map would you need to create if you are using IKE for IPSEC?

A. crypto map map1 100 ipsec-manual
B. crypto map map1 100 ike-dynamic
C. crypto map map1 100 ipsec-isakmp
D. crypto map map1 100 isakmp-key
E. crypto map map1 100 dynamic
F. None of the above

Answer: C
Explanation:
When creating a crypto map, specify that the map will use IKE with the ipsec-isakmp keyword. If you are not using IKE, and are instead using manual keys, enter the ipsec-manual crypto map keyword.

QUESTION NO: 8
You want to configure a TestKing router for IPSec using default values. What is the IOS Firewall IPSEC SA default lifetime value (in seconds)?

A. 50,400
B. 3,600
C. 21,600
D. 86,400

Answer: B
Explanation:
The default IPSEC SA lifetime value is set to 3600 seconds (1 hour). Do not confuse this IPSEC SA lifetime value with the ISAKMP (IKE) SA lifetime value which is set to 86,400 seconds (1 day) by default.

QUESTION NO: 9
The security administrator at TestKing wants to use the most secure approach for using pre-shared keys between peers. Which one of these answers is the most secure?

A. Specify the same key to share with multiple remote peers.
B. Specify different keys to share between different pairs of peers.
C. Specify different keys to share with multiple remote peers.
D. Specify the same key to share between different pairs of peers.
E. None of the above

Answer: B
Explanation:
Specify the shared keys at each peer. A given pre-shared key is shared between two peers. At a given peer you could specify the same key to share with multiple peers; however, a more secure approach is to specify different keys to share between different pairs of peers.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_user_guide_chapter09186a0080106f69.ht

QUESTION NO: 10
Jason is the security administrator at TestKing Inc. and his assignment today is to find out in crypto map configuration mode, which command lets you manually specify the IPSec session keys with a crypto map entry?

A. set crypto map
B. set ipsec-manual
C. no set security-association
D. set security-association

Answer: D
Explanation:
To

specify that separate IP Security security associations should be requested for each source/destination host pair, use the set security-association level per-host crypto map configuration command. To specify that one security association should be requested for each crypto map access list permit entry, use the no form of this command.
Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_summary_chapter09186a008(

Section 3: Configure IPSecEncryption for site-to-site VPN using certificate authority (4 questions)

QUESTION NO: 1
Regarding IPSec and Certificate Authorities (CA), which of the following choices define the standard certificate format?

A. CEP
B. CRLv2
C. ISAKMP
D. X.509v3
E. None of the above

Answer: D
Explanation:
The X.509 standard specifies that digital certificates contain standardized information. A CA (Certificate Authority) vouches for the authenticity of their public keys. A digital signature which meets ITU (International Telecommunications Union) Telecommunication Standardization (ITU-T) PKIX X.509 version 3 [RFC 2459] standard is generated based on
1. detailed information about the key holder
2. an expiration date, after which the certificate is expired
3. (with v3), a Compromised Key List (CKL)
Reference:
http://www.microsoft.com/technet/prodtechnol/exchange/guides/E2k3MsgSecGuide/b26b91d9-d569-4d1f-91

QUESTION NO: 2
A TestKing IPSec device is being configured for CA support. Choose the correct command to generate two RSA key pairs for use with certificate authority.

A. key generate rsa general-keys
B. key generate rsa usage-keys
C. crypto key generate rsa general-keys
D. crypto key generate rsa usage-keys
E. enable crypto key generate rsa general-keys
F. enable crypto key generate rsa usage-keys

Answer: D
Explanation:
Special-Usage Keys:
If you generate special-usage keys, two pairs of RSA keys will be generated. One pair will be used with any Internet Key Exchange (IKE) policy that specifies RSA signatures as the authentication method, and the other pair used with any IKE policy that specifies RSA-encrypted nonces as the authentication method. (You configure RSA signatures or RSA-encrypted nonces in your IKE policies as described in the CiscoIOS Security Configuration Guide.)
A certification authority (CA) is used only with IKE policies specifying RSA signatures, not with IKE policies specifying RSA-encrypted nonces. (However, you could specify more than one IKE policy and have RSA signatures specified in one policy and RSA-encrypted nonces in another policy.)
If you plan to have both types of RSA authentication methods in your IKE policies, you might prefer to generate special-usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special-usage keys, one key is used for both purposes, increasing that key's exposure.)
To generate special-usage RSA keys, use the "crypto key generate rsa usage-keys" command.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087cac.html

QUESTION NO: 3

You are configuring a new TestKing router for CA support. Which of the following router commands correctly sets the location (URL) of a CA server into the router configuration?

A. Router (crypto-set)#enrollment mode (URL)
B. Router (crypto-ca)#enrollment mode (URL)
C. Router (ca-scep)#enrollment url (URL)
D. Router (ca-identity)#enrollment url (URL)

Answer: D
Explanation:
Specify the location of the CA server with the ca-identity configuration mode command enrollment url (URL).
To configure the PKI, use the following commands beginning in privileged EXEC mode (first 7 steps only shown):

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **no crypto ca id** *name*	Clears the old certificate if one exists.
Step 3	Router(config)# **crypto key zeroize rsa**	Clears the existing RSA key.
Step 4	Router(config)# **hostname** *router-name*	Configures the router hostname if this has not been done already.
Step 5	Router(config)# **ip domain-name** *domain-name*	Configures the router's IP domain name.
Step 6	Router(config)# **crypto ca identity** *name*	Enters CA-identity configuration mode and declares a Certification Authority (CA) name. For example, the CA name could be fieldlabs.cisco.com.
Step 7	Router(ca-identity)# **enrollment url** *url*	Uses a nonstandard cgi-bin script location URL.

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a008(

QUESTION NO: 4
The security administrator at TestKing Inc. must choose three major tasks that must be completed in order to support CA for Cisco routers in a site-to-site configuration. What are these three steps? (Choose three)

A. Configure an authentication proxy.
B. Configure a CA server.
C. Configure IKE.
D. Test and verify IPSec.
E. Test and verify the RADIUS server.
F. Configure CA support.

Answer: C, D, F
Explanation:
The tasks for configuring IPSec operation for CA support is as follows:

Task 1: Prepare for IPSec
Task 2: Configure CA support
Task 3: Configure IKE for IPSec
Task 4: Configure IPSec
Task 5: Verify VPN configuration - Verify IPSec

Reference: Managing Cisco Network Security (Cisco Press) page 646

Section 4: Verify and troubleshoot IPSecoperation (11 questions)

QUESTION NO: 1
What is the bit length of the Diffie-Hellman group 1 algorithm?

A. 768 bits
B. 512 bytes
C. 512 bits

D. 768 bytes
E. 1024 bits
F. 2048 bits
G. None of the above

Answer: A
Explanation:
The Diffie-Hellman protocol uses complex mathematical algorithms to generate a secret key over an insecure link such as the Internet. Only the public keys are exchanged, the secret key that is generated is never sent over the link. Diffie-Hellman group 1 uses 768 bit keys.

QUESTION NO: 2
Which of the following commands can debug communications between an IOS router, and a CA server?

A. debug crypto dss exchange
B. debug crypto ca server
C. debug crypto ca engine
D. debug crypto pki messages

Answer: D
Explanation:
You can monitor the communication between a router and a Certificate Authority (CA) server with the debug crypto pki messages command.

QUESTION NO: 3
The newly appointed TestKing trainee technician wants to know of which cryptographic key system RSA is an example of. What would your reply be?

A. symmetrical
B. asymmetrical
C. Diffie-Hellman
D. DES

Answer: B
There are two types of cryptographic keys; public keys -- sometimes called asymmetric key -- and symmetric keys. RSA and Diffie-Hellman are common public key algorithms and RC4, DES and IDEA common symmetric key algorithms. You cannot directly compare public key lengths (for example RSA keys) with symmetric key lengths (DES, RC4); this is an important point which confuses many people.

QUESTION NO: 4
The security team at TestKing Inc., is looking for the command that lets you view any configured CA certificates?

A. crypto key generate rsa
B. show crypto key mypubkey rsa
C. show crypto key pubkey-chain rsa
D. show crypto ca certificates

Answer: D
To view information about your certificate, the CA's certificate, and any RA certificates, use the "show crypto ca certificates" EXEC command.

QUESTION NO: 5
The TestKing trainee technician wants to know which error message indicates that ISAKMP peers failed protection suit negotiation for ISAKMP. What will your reply be?

A. %Crypto-6-IKMP_SA_AUTH Can accept Quick Mode exchange form %15 if SA is authenticated
B. %Crypto-6-IKMP_SA_OFFERED Remote peer% respond attribute [chars] offered
C. %Crypto-6-IKMP_SA_NOT_OFFERED Remote peer% respond attribute [chars] not offered
D. %Crypto-6-IKMP_SA_NO_AUTH Remote peer% respond attribute [chars] not offered

Answer: C
Explanation:
Error Message:

%CRYPTO-6-IKMP_SA_NOT_OFFERED : Remote peer [IP_address] responded with attribute [chars] not offered or changed
ExplanationIKE peers negotiate policy by having the initiator offer a list of possible protection suites. The responder has returned a type of protection suite that the initiator did not offer.
Recommended Action Contact the remote peer.
Reference:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122sup/122sems/semsvol1/emfcpad.htm

QUESTION NO: 6
Jason the security manager at TestKing Inc. is working on the PIX firewall. He needs to figure out which two types of commands are used for testing and verifying IPSec and ISAKMP? (Choose two)

A. clear
B. show
C. interface
D. crypto map
E. crypto isakmp policy
F. debug

Answer: B, F
Explanation:
Testing and verifying the overall IPSec configuration:
The final step in configuring IPSec for pre-shared keys is to verify that all the IKE and IPSec values were configured correctly and to test it to ensure that it works properly. The PIX Firewall contains a number of show, clear, and debug commands that are useful for testing and verifying IKE and IPSec, which are summarized in this section.
Reference: Managing Cisco Network Security (Cisco Press) page 221

QUESTION NO: 7
What IOS router command is entered to view all current IKE SA's?

A. show ipsec
B. show crypto isakmp sa

C. show isakmp
D. show crypto ipsec sa
E. show ipsec sa
F. show isakmp sa

Answer: B
Explanation:
View the status of current IKE Security Associations on a router with the show crypto isakmp sa command. (ISAKMP is the same process as IKE)

QUESTION NO: 8
Regarding IPSec operation, what are the protocol numbers used for ESP and AH?

A. 84, 85
B. 69, 70
C. 50, 51
D. 96, 97

Answer: C
Explanation:
The two IPSEC protocols ESP (encryption and authentication), and AH (authentication) are protocol numbers 50, and 51, respectively.

QUESTION NO: 9
Kathy is looking for the command that deletes all of the routers RSA keys.
Which command is correct?

A. crypto key zeroize rsa
B. crypto key remove rsa
C. crypto key delete rsa
D. crypto key remove rsa all

Answer: A
Explanation:

To delete all of your router's RSA keys, use the crypto key zeroize rsa global configuration command.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_summary_chapter09186a008(

QUESTION NO: 10
John the security Administrator at TestKing Inc. is working on IPSec. He quizzes Kathy about AH. He asks her which three statements about AH are true. (Choose three)

A. AH encrypts the payload for data confidentiality.
B. AH provides connectionless integrity for the IP datagrams.
C. AH encapsulates the data.
D. AH provides protection against replay.
E. AH uses symmetric secret algorithms.
F. AH provides data origin authentication for the IP datagrams.

Answer: B, D, F
Explanation:
Authentication Header - A security protocol that provides authentication and optional replay-detection services. AH acts as a digital signature to ensure data in the IP packet has not been tampered with. AH does not provide data encryption and decryption services.
Reference: Managing Cisco Network Security (Cisco Press) page 525

QUESTION NO: 11
A TestKing router is being configured for IPSec using ESP. Which of the following are true regarding ESP? (Choose three)

A. ESP provides protection to the outer headers.
B. ESP encapsulates the data.
C. ESP uses symmetric secret key algorithms.
D. ESP verifies the integrity of the ESP datagram.
E. ESP uses asymmetric secret key algorithms.
F. ESP encrypts the payload for data confidentiality.

Answer: B, C, F
Explanation:
ESP is a security protocol used to provide confidentiality (that is, encryption), data origin authentication, integrity, optional anti-replay service, and limited traffic flow confidentiality by defeating traffic flow analysis.
ESP provides confidentiality by performing encryption at the IP packet layer. It supports a variety of symmetric encryption algorithms.
Reference: Managing Cisco Network Security (Cisco Press) page 529

Section 5: Configure EZ-VPN server (3 questions)

QUESTION NO: 1
Johnthe security administrator at TestKing Inc. is using Cisco Easy VPN and needs to know which of these statements are true about Cisco Easy VPN.

A. All members of a user group must originate on the same model and type of Cisco VPN Client.
B. Only VPN-enabled Cisco routers and PIX Firewalls may be used as Easy VPN servers.
C. The maximum amount of Cisco VPN Clients supported by a VPN server is 50.
D. Centrally managed IPSec polices are pushed to the Cisco VPN Clients by the VPN server.

Answer: D
Explanation:
The Easy VPN Server feature introduces server support for the Cisco VPN Client Release 3.x and later software clients and Cisco VPN hardware clients. The feature allows a remote end user to communicate using IP Security (IPSec) with any CiscoIOS Virtual Private Network (VPN) gateway. Centrally managed IPSec policies are "pushed" to the client by the server, minimizing configuration by the end user.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087d1e.html#6

QUESTION NO: 2

The TestKing security administrator is working on the Cisco Easy VPN. He needs to select the three types of IPSec encryption algorithms supported by Cisco Easy VPN. (Choose three)

A. DES
B. 3DES
C. NULL
D. ESP
E. IPCOMP-LZS
F. HMAC-MD5

Answer: A B C
Explanation:
Supported IPSec Protocol Options and Attributes
Encryption Algorithms (IPSec)
1. DES
2. 3DES
3. NULL

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087d1e.html#1

QUESTION NO: 3
Which of the following represents the main components that the Cisco Easy VPN feature set consists of? (Choose two)

A. Easy VPN CA
B. Easy VPN RADIUS Server
C. Easy VPN Access
D. Easy VPN Server
E. Easy VPN Remote
F. Easy VPN TACACS+ Server

Answer: D, E
Cisco EzVPN consists of two components: Easy VPN Server, and Easy VPN Remote. The EzVPN Server is the Head-End VPN device and can push a configuration to the EzVPN Remote device.

Section 6: Configure EZ-VPN remote using both hardware and software clients. (7 questions)

QUESTION NO: 1
Two TestKing devices are connected via the Cisco EZVPN service. Which Easy VPN feature enables two IPSec peers to determine if the other is still "alive"?

A. Dead Peer Timeout
B. No Pulse Timer
C. Peer Death Monitor
D. Dead Peer Detection
E. Peer Heartbeat
F. All of the above
G. None of the above.

Answer: D
Explanation:
The IPSec Dead Peer Detection Periodic Message Option feature allows you to configure your router to query the liveliness of its Internet Key Exchange (IKE) peer at regular intervals. The benefit of this approach over the default approach (on-demand dead peer detection) is earlier detection of dead peers.
DPD and Cisco IOS keepalives function on the basis of the timer. If the timer is set for 10 seconds, the router will send a "hello" message every 10 seconds (unless, of course, the router receives a "hello" message from the peer). The benefit of IOS keepalives and periodic DPD is earlier detection of dead peers.
Reference:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455afd.html

QUESTION NO: 2
You are configuring a new TestKing router with the EzVPN feature. What EzVPN feature allows a remote host to encrypt all data needing to go to the EzVPN Server, but sending all other traffic in clear text to its local ISP?

A. Initial Contact
B. DPD
C. Split Tunneling
D. Remote Administration
E. None of the above

Answer: C
Explanation:
The Remote EzVPN client can be configured to use Split Tunneling which allows a connection to the EzVPN server, and a connection to the local ISP. This allows all traffic not destined to the EzVPN server to go to the ISP, unencrypted. If Split Tunneling is not used, all traffic will go to the EzVPN server encrypted, then rerouted out to the Internet to its final destination.

QUESTION NO: 3
You are configuring a new TestKing router with the EzVPN feature. What is the EzVPN feature that allows a Remote host to re-establish a connection to a Server, if the Remote host is accidentally disconnected?

A. Mode Configuration
B. DPD
C. Split Tunneling
D. Initial Contact
E. None of the above

Answer: D
Explanation:
Initial Contact is used by a host when first establishing a connection to the EzVPN Server, telling the Server to delete any previous SA's with the host. This is done because if a host is disconnected from the Server, and the Server is not aware of it, the host will not be able to reconnect with the Server unless the SA's are reset. Initial Contact makes sure the host can connect.

QUESTION NO: 4
You are configuring a new TestKing router with the EzVPN feature. What are the two components of Cisco Easy VPN (EzVPN)?

A. External
B. Server
C. Remote
D. Master
E. Slave
F. Client

Answer: B, C
Explanation:
Cisco Easy VPN consists of two components: Cisco Easy VPN Remote and Cisco Easy VPN Server. The Cisco Easy VPN Remote feature allows Cisco IOS routers, Cisco PIX Security Appliances, Cisco VPN 3002 Hardware Clients and the Cisco VPN Client to receive security policies upon a VPN tunnel connection from a Cisco Easy VPN Server, minimizing configuration requirements at the remote location.
The Cisco Easy VPN Server allows Cisco IOS routers, Cisco PIX Security Appliances, and Cisco VPN 3000 Concentrators to act as VPN head-end devices in site-to-site or remote-access VPNs, where the remote office devices are using the Cisco Easy VPN Remote feature. This feature pushes security policies defined at the central site to the remote VPN device, helping to ensure that those connections have up-to-date policies in place before the connection is established. Additionally, a device enabled with the Cisco Easy VPN Server can terminate VPN tunnels initiated by mobile remote workers running the Cisco VPN Client software on PCs. This flexibility allows mobile and remote workers to access critical data and applications on their corporate intranet.
Reference: Cisco Self-Study CCSP SECUR page 363

QUESTION NO: 5
You are configuring a new TestKing router with the EzVPN feature. What are the IPSec attributes that Cisco Easy VPN is incapable of supporting? (Choose all that apply)

A. Manual keys
B. PFS
C. RSA digital signatures
D. Tunnel mode
E. DH 2
F. Pre-shared keys

Answer: A, B
The following table lists the Non Supported IPSec Protocol Options and Attributes:

Options	Attributes
Authentication Types	Authentication with public key encryption Digital Signature Standard (DSS)
Diffie-Hellman Group	1
IPSec Protocol Identifier	IPSEC_AH
IPSec Protocol Mode	Transport mode
Miscellaneous	Manual keys Perfect Forward Secrecy (PFS)

QUESTION NO: 6
You are the administrator of TestKing Inc. and your job today is to find out which Easy VPN feature enables two IPSec peers to determine if the other is still alive. What feature does this?

A. Dead Peer Timeout
B. Dead Peer Detection
C. No Pulse Timer
D. Peer Death Monitor
E. Peer Heartbeat

Answer: B
Explanation:

The IPSec Dead Peer Detection Periodic Message Option feature allows you to configure your router to query the liveliness of its Internet Key Exchange (IKE) peer at regular intervals. The benefit of this approach over the default approach (on-demand dead peer detection) is earlier detection of dead peers.

Reference:

http://www.cisco.com/en/US/products/ps6635/products_white_paper09186a00801ee19a.shtml

QUESTION NO: 7

You are configuring a new TestKing router as an EzVPN client. Which of the following can act as a Cisco EzVPN Remote client? (Select all that apply)

A. 1700 router
B. 7200 router
C. VPN Software Client
D. 3002 VPN Hardware Client

Answer: A, C, D

Explanation:

The following devices can act as the Remote in a Cisco EzVPN: 800, 900, and 1700 series routers, PIX 501 firewall, the 3002 Hardware Client, and the VPN software client.

Section 7: Troubleshoot EZ-VPN (3 questions)

QUESTION NO: 1

The following command was issued on one of the TestKing routers:

```
R7#sh crypto ipsec client ezvpn
Easy VPN Remote Phase: 2
Tunnel name : VPNGATE1
Inside interface list: FastEthernet0/0,
Outside interface: FastEthernet0/1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.0.2.39
Mask: 255.255.255.255
Default Domain: cisco.com
```

Given the output of the show crypto ipsec client ezvpn command shown above, what can you determine?

A. The default domain is cisco
B. The socket is up and ready for data.
C. The remote router address is 10.0.2.39.
D. The tunnel is up and SAs have been established.
E. The tunnel is terminated at a remote router called VPNGATE1.
F. All hosts connecting through this router will have the address of 10.0.2.39.

Answer: D
Explanation:
The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an active Virtual Private Network (VPN) connection when the router is in client mode:
Router# **show crypto ipsec client ezvpn**

Tunnel name: hw1
Inside interface list: FastEthernet0/0, Serial1/0,
Outside interface: Serial0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 209.165.201.0
Mask: 255.255.255.224
DNS Primary: 209.165.201.1

DNS Secondary: 209.165.201.2
NBMS/WINS Primary: 209.165.201.3
NBMS/WINS Secondary: 209.165.201.4
Default Domain: cisco.com

The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an inactive VPN connection:
Router# **show crypto ipsec client ezvpn**

Current State: IDLE
Last Event: REMOVE INTERFACE CFG
Router#

The table belowdescribes significant fields shown by the **show crypto ipsec client ezvpn** command:

Table 40 show crypto ipsec client ezvpn Field Descriptions

Field	Description
Current State	Displays whether the VPN tunnel connection is active or idle. Typically, when the tunnel is up, the current state is IPSEC ACTIVE.
Last Event	Displays the last event performed on the VPN tunnel. Typically, the last event before a tunnel is created is SOCKET UP.
Address	Displays the IP address used on the outside interface.
Mask	Displays the subnet mask used for the outside interface.
DNS Primary	Displays the primary domain name system (DNS) server provided by the Dynamic Host Configuration Protocol (DHCP) server.
DNS Secondary	Displays the secondary DNS server provided by the DHCP server.
Domain Name	Displays the domain name provided by the DHCP server.
NBMS/WINS Primary	Displays the primary NetBIOS Microsoft Windows Name Server provided by the DHCP server.
NBMS/WINS Secondary	Displays the secondary NetBIOS Microsoft Windows Name Server provided by the DHCP server.

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a008(

QUESTION NO: 2
You are configuring a new TestKing router as an EZVPN server. What is the IOS version that first introduced EzVPN server?

A. 12.2(6)T
B. 12.3(1)T

C. 12.2(5)T
D. 12.2(8)T

Answer: D
Explanation:
Cisco 1700, 7100, and 7200 routers can act as an EzVPN server starting in IOS version 12.2(8)T.

QUESTION NO: 3
You are configuring a new TestKing router with the EzVPN feature. What are the two Diffie-Hellman (DH) groups that the IOS EzVPN server supports?

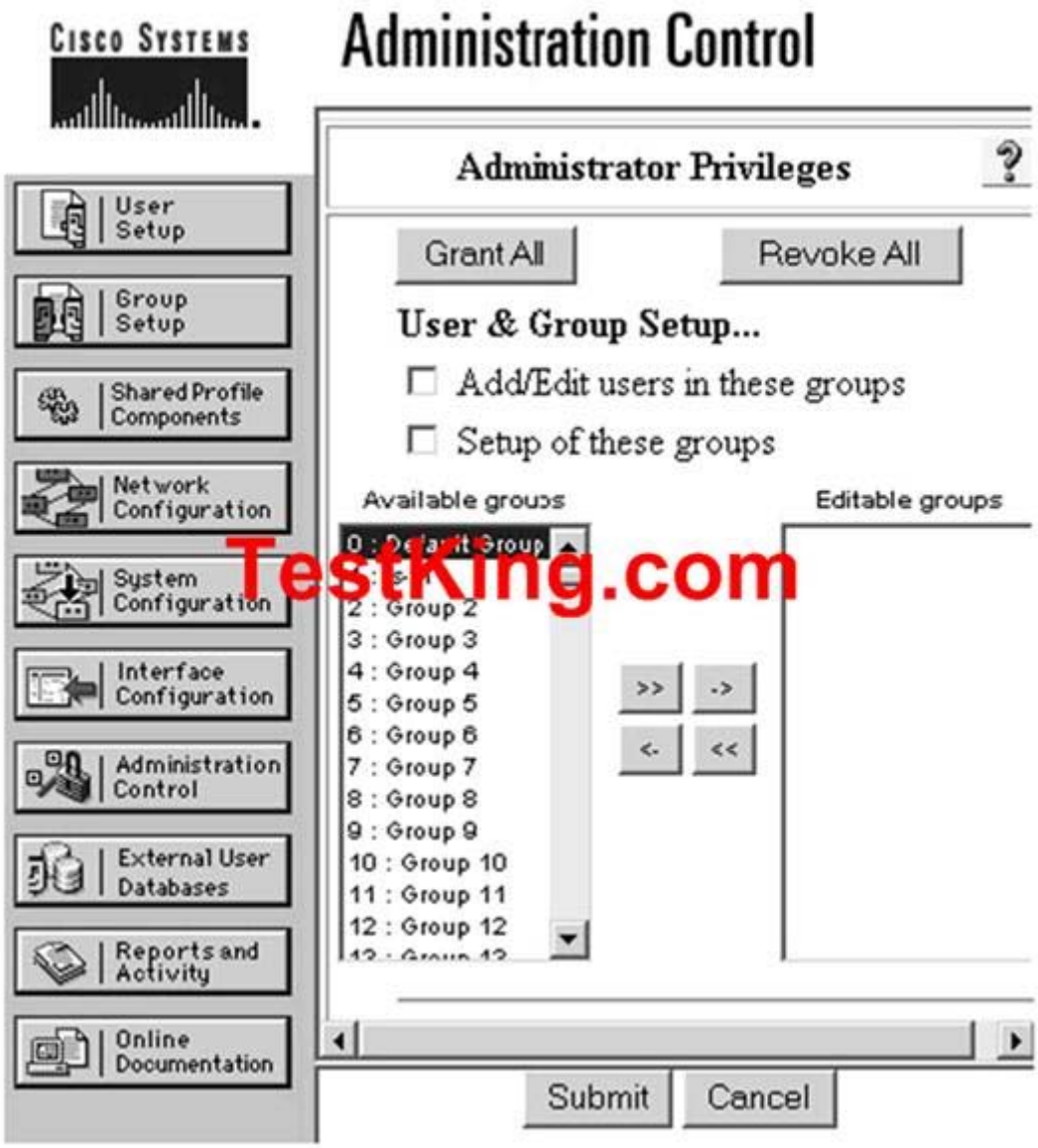
A. Group 2
B. Group 1
C. Group 3
D. Group 4
E. Group 5

Answer: A, E
Explanation:
The Cisco IOS EzVPN Server only supports Diffie-Hellman Groups 2 (1024 bit) and 5 (1536 bit). Group 1 (768 bit) is not supported.

Topic 5: Configure authentication, authorization and accounting to provide basic secure access control for networks (22 questions)

Section 1: Configure administrative access to the Cisco Secure ACS server (3 questions)

QUESTION NO: 1
While working on a CSACS the following was seen:



Refer to the Cisco Secure ACS Administration Privileges setup screen in the exhibit above. Which button should be checked to give administrative privileges to everything?

A. Add/Edit users in these groups
B. Cancel
C. Grant All
D. Revoke All
E. Setup of these groups
F. Submit

Answer: C
Explanation:
To add a CiscoSecure ACS administrator account, follow these steps (first 4 steps only shown) below:
Step 1:
In the navigation bar, click Administration Control.
Step 2:
Click Add Administrator.
The Add Administrator page appears.
Step 3:
Complete the boxes in the Administrator Details table:
a.
In the Administrator Name box, type the login name (up to 32 characters) for the new CiscoSecure ACS administrator account.
b.
In the Password box, type the password (up to 32 characters) for the new CiscoSecure ACS administrator account.
c.
In the Confirm Password box, type the password a second time.
Step 4:
To select all privileges, including user group editing privileges for all user groups, click "Grant All".
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_chapter09186a0080205a43.h

QUESTION NO: 2

A new Cisco ACS has been installed in the TestKing network. Which three statements about Cisco Secure ACS are true? (Choose three.)

A. NAS can access multiple Cisco Secure ACS for Windows servers.
B. Cisco Secure ACS for Windows server can only log onto external server.
C. The Cisco Secure ACS for Windows server supports only TACACS+.
D. Database replication is supported by the Cisco Secure ACS for Windows servers.
E. The service used for authentication and authorization on a Cisco Secure ACS for Windows server is called CSAdmin.
F. The Cisco Secure ACS for Windows server uses the CSDBsynch service to manage the user and group accounts.

Answer: A, B, D
Explanation:
With ACS, the ability to determine if and where an authentication request is to be forwarded is defined in the distribution table in the Network Configuration window. Multiple CiscoSecureACSes can be used throughout the network and, depending on a defined character string entered with the username (for example, mary@corporate.com, where @corporate.com is the defined character string), when the user dials in to the NAS and a match is found in the distribution table, the authentication request is then forwarded to a remote AAAserver to permit or deny access to the network.
The database replication and RDBMS synchronization features provided with CiscoSecureACS help automate the process of updating your CiscoSecureACS database and network configuration. Database replication allows you to replicate various parts of the configuration, including user and group information, from a CiscoSecureACS primary server to one or more CiscoSecureACS backup or client systems. Replication allows you to automate the creation of mirror CiscoSecureACSes.
If your network is geographically dispersed, the remote logging feature helps you simplify the process of gathering the accounting logs generated on each CiscoSecureACS. Each CiscoSecureACS can be configured to point to a centralized CiscoSecureACS to be used as the logging server. The centralized CiscoSecureACS still has all the capabilities of a AAAserver but also becomes a central repository for all accounting logs that are sent.
Incorrect Answers:
C: Both TACACS and RADIUS are supported.
E: CSAuth is used for authorization and authentication on the Cisco Secure ACS, not CSAdmin.
F: CSDBSync is used to provide synchronization with an external RDBMS database, not for managing users and account info.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_chapter09186a008007e350.h

QUESTION NO: 3
You need to install CSACS 3.0 on a TestKing server. How much hard disk space is required to install AAA CSACS 3.0 for Windows?

A. 900mb
B. 100mb
C. 250mb
D. 500mb
E. None of the above

Answer: C
Explanation:
Installation of CSACS 3.0 on a Windows server will need at least 250Mb of disk space for installation, more if the user database will be stored on the machine.

Section 2: Configure AAA clients on the Cisco Secure ACS (for routers) (3 questions)

QUESTION NO: 1
The security administrator at TestKing Inc. needs to select three types of authentication supported by Cisco Secure ACS 3.0.1. What are the three methods? (Choose three)

A. HMAC
B. EAP-TLS
C. DH-1
D. AAA
E. LEAP
F. EAP-MD5

Answer: B, E, F
Explanation:

EAP-MD5, EAP-TLS-In addition to supporting LEAP, CiscoSecureACS supports EAP-MD5 and EAP-TLS authentication. EAP is an IETF RFC standard for carrying various authentication methods over any PPP connection. EAP-MD5 is a username/password method incorporating MD5 hashing for security. EAP-TLS is a method for authenticating both CiscoSecureACS and users with X.509 digital certificates. This method also provides dynamic session key negotiation.

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_note09186a00800ada4c.html

QUESTION NO: 2

A new Cisco ACS has been installed in the TestKing network. Which of the following statements regarding Cisco Secure ACS are valid? (Choose three)

A. The NAS is capable of accessing multiple Cisco Secure ACS for Windows server.
B. The Cisco Secure ACS for Windows servers can log onto external servers.
C. Database replication is supported by the Cisco secure ACS fro Windows servers.
D. The service used for authentication and authorization on a Cisco.
E. The Cisco Secure ACS for Windows server supports only TACACS+.
F. The Cisco Secure ACS for Windows server uses the CSDBsynch service to manage the user and group accounts.

Answer: A, B, C

Explanation:

Cisco Secure ACS logs a variety of user and system activities. Depending on the log, and how you have configured Cisco Secure ACS, logs can be recorded in one of two formats:
 Comma-separated value (CSV) files-The CSV format records data in columns separated by commas. This format is easily imported into a variety of third-party applications, such as Microsoft Excel or Microsoft Access. After data from a CSV file is imported into such applications, you can prepare charts or perform queries, such as determining how many hours a user was logged in to the network during a given period. For information about how to use a CSV file in a third-party application such as Microsoft Excel, please see the documentation supplied by the third-party vendor. You can access the CSV files either on the Cisco Secure ACS server hard drive or by downloading the CSV file from the HTML interface. For more information about downloading the CSV file from the HTML interface, see the "Viewing a CSV Report" section.

 ODBC-compliant database tables-ODBC logging enables you to configure Cisco Secure ACS to log directly in an ODBC-compliant relational database, where it is stored in tables, one table per log. After the data is exported to the relational database, you can use the data however you need. For more information about querying the data in your relational database, refer to the documentation supplied by the relational database vendor.

QUESTION NO: 3
AAA needs to be configured on one of the TestKing routers. Which of the following router commands enables the AAA process?

A. aaa new-model
B. aaa setup-dbase
C. aaa config-login
D. aaa server-sync
E. None of the above

Answer: A
Explanation:
Enable AAA by using the "aaa new-model" global configuration command.
AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

Authentication-Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption.

Authorization-Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

Accounting-Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a008(

Section 3: Configure users, groups and access rights (3 questions)

QUESTION NO: 1
One of the TestKing routers is configured as shown below:

```
!
username cisco password 0 cisco
memory-size iomem 10
clock timezone EDT -5
no network-clock-participate slot 1
no network-clock-participate wic 0
no aaa new-model
ip subnet-zero

interface FastEthernet0/0
 ip address 10.0.2.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.30.2.2 255.255.255.0
 duplex auto
 speed auto
!

line con 0
 login local
line aux 0
line vty 0 4
 password cisco
 login
```


After reviewing the running configuration file shown above, what can you determine?

A. No one will be able to login.
B. No one will be able to console in.

C. The wrong authentication method is applied to lines.
D. Users will use the local database to log in to console.
E. Users will use the password cisco to log in to console.
F. Users will use the local database to log in to vty.

Answer: D
Explanation:
To establish a username-based authentication system, use the username command in global configuration mode. To enable password checking at login, use the login local command in line configuration mode. The login local could be used for console connections, as well as telnet connections into the router.

QUESTION NO: 2
The TestKing security administrator was given the following configuration statement:

router(config)#aaa authentication login default tacacs+ none

After looking at the command, he knows two statements are true. Which two are correct statements? (Choose two)

A. TACACS is the default login method for all authentication.
B. No authentication is required to login.
C. IF TACACS process is unavailable, no access is permitted.
D. RADIUS is the default login method for all authentication.
E. If the RADIUS process is unavailable, no login is required.
F. IF the TACACS process is unavailable, no login is required.

Answer: A, F
Explanation:
The command line in this question uses TACACS+ for authentication first. If a Cisco Secure ACS or TACACS is not available, use the NAS's local user database password. However, all other users can only use TACACS+: Finally, if both of these methods fail, then the "none" keyword specifies that no authentication is to be used, and to allow all users.
none - no authorization is performed.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps4911/products_user_guide_chapter09186a008015c5c3.h

QUESTION NO: 3
Which of the following configurations restricts telnet access to a TestKing router by requiring the password "cisco"?

A. line vty 0 4
 login cisco
B. line vty 0 4
 set password cisco
 login
C. line vty 0 4
 password cisco
 login
D. line vty 0 4
 set login
 set password cisco

Answer: C
Explanation:
To restrict telnet access to a Cisco router, you must configure the virtual terminal lines (VTY) that telnet uses. Require a login with the login line configuration command (enabled on vty lines by default). You must also set a password with the password (password) line configuration command, or remote user telnet connections will be refused, informing them that a login is required, but no password is set.

Section 4:Configure router to enable AAA to use TACACS+ (5 questions)

QUESTION NO: 1
The TACACS server on your network has been issued the 10.1.1.4 IP address. Choose the correct global IOS command that will specify this TACACS server.

A. host 10.1.1.4
B. server 10.1.1.4

C. tacacs-server host 10.1.1.4
D. tacacs-server 10.1.1.4
E. tacacs-host host 10.1.1.4
F. server-tacacs host 10.1.1.4

Answer: C
Explanation:
The "tacacs-server host" command enables you to specify the names of the IP host or hosts maintaining a TACACS+ server. Because the TACACS+ software searches for the hosts in the order specified, this feature can be useful for setting up a list of preferred daemons.
The following example shows how to configure TACACS+ as the security protocol for PPP authentication:

aaanew-model
aaaauthenticationppptestgrouptacacs+local
tacacs-serverhost10.1.2.3
tacacs-serverkeygoaway
interfaceserial0
pppauthenticationchappaptest

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a008(

QUESTION NO: 2
You need to configure router TK1 to support AAA in the TestKing network. Which configuration command on TK1 causes a start-accounting record for a Point-to-Point session to be sent to a TACACS+ server?

A. aaa authentication ppp start tacacs+
B. aaa authorization exec default tacacs+
C. aaa authorization network default tacacs+
D. aaa accounting network default stop-only tacacs+
E. aaa accounting network default start-stop tacacs+

Answer: E
Explanation:

To enable AAA accounting of requested services for billing or security purposes when you use TACACS+, use the aaa accounting global configuration command.

aaaaccounting {system | network | exec | command level} {start-stop | wait-start | stop-only} {tacacs+ | radius}

Syntax Description

system	Performs accounting for all system-level events not associated with users, such as reloads.
network	Runs accounting for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP.
exec	Runs accounting for EXEC session (user shells). This keyword might return user profile information such as **autocommand** information.
command	Runs accounting for all commands at the specified privilege level.
level	Specifies the command level to track for accounting. Valid entries are 0 through 15.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting notice was received by the accounting server.
wait-start	As in **start-stop**, sends both a start and a stop accounting notice to the accounting server. However, if you use the **wait-start** keyword, the requested user service does not begin until the start accounting notice is acknowledged. A stop accounting notice is also sent.
stop-only	Sends a stop accounting notice at the end of the requested user process.
tacacs+	Enables the TACACS-style accounting.
radius	Enables the RADIUS-style authorization.

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1824/products_command_reference_chapter09186a008(

QUESTION NO: 3 DRAG DROP
You need to configure your TestKing router to enable AAA, start authentication and accounting using TACACS+ server 10.0.2.12 (with key: ciscosecure) using the default TACACS+ groups. Click and drag the correct commands to the ordered steps.

Answer:
Explanation:

QUESTION NO: 4
Which of the following router commands will allow all of the TestKing users to be authenticated, even if the TACACS+ server fails?

A. aaa authentication list1 tacacs+ any
B. aaa authentication list1 tacacs+ none
C. aaa authentication list1 tacacs+ allow
D. aaa authentication list1 tacacs+ disabled
E. None of the above

Answer: B
Explanation:
The none keyword at the end of this aaa command allows the user to be authenticated by not requiring any form of authentication if the tacacs+ server is tried first, but did not respond.

QUESTION NO: 5
Which of the following represents a protocol that is commonly used to communicate AAA information between Cisco routers and AAA servers?

A. TACACS+
B. SSL
C. Syslog
D. SSH
E. ARAP

Answer: A
Explanation:
Cisco uses the Terminal Access Controller Access Control System plus (TACACS+) protocol to communicate with remote AAA servers. TACACS is the Cisco proprietary method of communications, similar to the industry standard RADIUS method.

Section 5: Configure router to enable AAA to use a Radius server (3 questions)

QUESTION NO: 1
You have been tasked to configure router TK1 to operate with the TestKing RADIUS server. Choose the correct command to enable RADIUS authentication on the router.

A. login default group radius
B. aaa authentication login radius
C. aaa authentication login group radius
D. authentication login default group radius
E. aaa authorization login default group radius
F. aaa authentication login default group radius

Answer: F
Explanation:
Login Authentication
You can use the **aaaauthentication login** command to authenticate users who want exec access into the access server (tty, vty, console and aux).
Example 1: Exec Access using Radius then Local
aaaauthentication login default group radius local
In the command above:
1. the named list is the default one (default).
2. there are two authentication methods (group radius and local).
All users are authenticated using the Radius server (the first method). If the Radius server doesn't respond, then the router's local database is used (the second method). For local authentication, define the username name and password:
username xxx password yyy
Because we are using the list default in the aaa authentication login command, login authentication is automatically applied for all login connections (such as tty, vty, console and aux).
Note:The server (Radius or TACACS+) will not reply to an aaaauthentication request sent by the access server if there is no IP connectivity, if the access server is not correctly defined on the AAA server or the AAA server is not correctly defined on the access server.
Note: Using the example above, if we do not include the local keyword, we have:
aaaauthentication login default group radius
Note:

If the AAA server does not reply to this authentication request, the authentication will fail (since the router does not have an alternate method to try).
Note:The group keyword provides a way to group existing server hosts. The feature allows the user to select a subset of the configured server hosts and use them for a particular service.
Reference:
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080093c81.shtml

QUESTION NO: 2
A TestKing router needs to be configured to support RADIUS. Choose the correct command to set the RADIUS key to cisco for all RADIUS servers.

A. router(config)# key cisco
B. router(config)# server key cisco
C. router(config)# radius-server cisco
D. router(config)# radius key cisco
E. router(config)# radius-server key cisco
F. router(config-if)# radius-server key cisco

Answer: E
Explanation:
Timeout, retransmission, and encryption key values are applied globally to all RADIUS servers in the router configuration with three unique global commands: radius-server timeout, radius-server retransmit, and radius-server key.
If you have at least one RADIUS server that does not have a per-server key, use the radius-serverkey command in global configuration mode to set the authentication and encryption key for all RADIUS communications between the router and the RADIUS server.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_feature_guide09186a0080087cdc.html

QUESTION NO: 3
The following configuration was applied to a TestKing router:

```
TestKingRouter(config)#aaa account network wait-start
radius
```

According to the configuration statement shown above, which of the following statements are valid? *Choose all that apply)

A. The accounting record are stored on a RADIUS server
B. Start-accounting records for network service requests are sent to the local database.
C. Stop-accounting record for network service requests are sent to the RADIUS server.
D. The accounting records are stored on TACACS+ server.
E. Stop-accounting record for network service requests are sent to TACACS+ server.
F. The requested service cannot start until the acknowledgment has been received from the RADIUS server.

Answer: A, C, F
Explanation:
Router(config)#aaa accounting network wait-start radius

aaaaccounting {system | network | connection | exec | command level} {start-stop | wait-start | stop-only} **tacacs+**

* Use the **aaaaccounting** command to enable accounting and to create named method lists that define specific accounting methods on a per-line or per-interface basis.
* Network - Enables accounting for all network-related requests, including SLIP, PPP, PPP network control protocols, and ARAP
* wait-start - This keyword causes both a start and stop accounting record to be sent to the accounting server. However, the requested user service does not begin until the start accounting record is acknowledged. A stop accounting record is also sent.

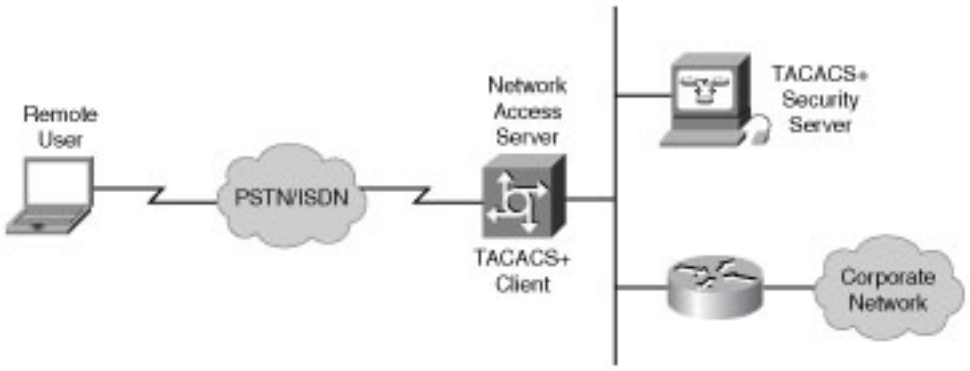
Section 6: Verify and troubleshoot AAA operation (5 questions)

QUESTION NO: 1
An AAA server has just been installed on your Cisco network. Which protocol is commonly used to communicate AAA information between Cisco routers and AAA servers?

A. SSH
B. ARAP
C. TACACS+

D. SSL
E. Syslog

Answer: C
Explanation:
TACACS+ is an improved version of TACACS. TACACS+ forwards username and password information to a centralized security server. The diagram below shows a typical TACACS+ topology:



TACACS+ uses TCP as the communication protocol between the remote client and security server and it supports the AAA architecture.

QUESTION NO: 2
Part of the configuration file for router TK1 is shown below:

```
username cisco password 0 cisco
aaa new-model
aaa authentication login vty_in local
aaa authentication login con_in group tacacs+ local
aaa session-id common
interface FastEthernet0/0
 ip address 10.0.2.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.30.2.2 255.255.255.0
 duplex auto
 speed auto
accesslist 101 permit tcp any any eq 80
 line con 0
  login authentication con_in
 line aux 0
 line vty 0 4
  password cisco
  login authentication vty_in
```


Refer to the exhibit above. The TestKing administrator cannot telnet to the router. The administrator is not prompted for a username or password and cannot ping the router. After reviewing the output of a show running-config command, what do you determine is the problem?

A. AAA is not enabled.
B. Everything is configured correctly (the problem must be caused by something else).
C. An access control list is blocking traffic.
D. The wrong passwords are being used.
E. The TACACS server must be unreachable.
F. The wrong authentication method is applied to lines.

Answer: B

Explanation:
Based on the configuration shown above, users that telnet into the router are to be authenticated via the AAA line labeled "vty_in." This line says that the local user database should be used, so users that enter "cisco" as the username and "cisco" as the password will be granted access to the router. Therefore, everything is indeed configured correctly, so there must be a different underlying problem. This is further reinforced by the fact that the router can also not be pinged.
Incorrect Answers:
A: This is enabled through the use of the "aaa new-model" command.
C: Although an access list is configured, it is not applied on any interface so it is not being used.
D: The problem in this case is that the users were not prompted for a username or a password.
E: The local database on the router is used for authentication, so this is not an issue.
F: The line configuration is correct.

QUESTION NO: 3
AAA is being configured on a new TestKing router. Which of the following AAA security server protocols can the Cisco IOS Firewall support? (Select all that apply)

A. MD5
B. RSA Signatures
C. TACACS+
D. RADIUS
E. CA
F. IPSec

Answer: C, D
Explanation:
The IOS Firewall can communicate with an AAA server running either RADIUS or TACACS+. RADIUS is an industry standard method of AAA, while TACACS+ is a Cisco proprietary method.

QUESTION NO: 4

Which of the following are commands that can be entered on a TestKing IOS Firewall router to debug communications with an AAA server? (Select all that apply)

A. debug aaa all
B. debug ip aaa
C. debug aaa accounting
D. debug tacacs
E. debug interface tacacs
F. None of the above

Answer: C, D
Explanation:
Use the "debug tacacs" command to just debug TACACS communication, or use a general command like "debug aaa accounting" for debugging TACACS and RADIUS.

QUESTION NO: 5
Which of the following router commands can you use to monitor AAA RADIUS?

A. show radius errors
B. show radius statistics
C. show ip aaa
D. show radius monitoring
E. None of the above

Answer: B
Explanation:
Use the router command show radius statistics to view general RADIUS statistics for authentication and accounting.

Topic 6: Use management applications to configure and monitor IOS security features (13 questions)

Section 1: Initialize SDM communications on Cisco routers (7 questions)

QUESTION NO: 1
The TestKing admin wants to connect to a router using SDM. Select the two protocols used to provide secure communications between SDM and the target router. (Select two)

A. HTTPS
B. RCP
C. Telnet
D. SSH
E. HTTP
F. AES

Answer: A, D
Explanation:
Cisco SDM communicates with routers for two purposes: to access the Cisco SDM application files for download to the PC and to read and write the router configuration and status. Cisco SDM uses HTTP(s) to download the application files to the PC. A combination of HTTP(s), Telnet/SSH is used to read and write the router configuration.

QUESTION NO: 2
Which of the following IOS commands should you use to enable local authentication for the HTTP interface.

A. router# ip http authentication enable
B. router# http authentication local
C. router(config)# ip http authentication enable
D. router(config)# ip http authentication local
E. router(config)# ip http authentication enable local
F. router(config)# ip http authentication local enable

Answer: D
Explanation:

The "ip http authentication" command enables you to specify a particular authentication method for HTTP server users. The HTTP server uses the enable password method to authenticate a user at privilege level 15. The "ip http authentication" command now lets you specify enable, local, TACACS, or authentication, authorization, and accounting (AAA) HTTP server user authentication.

Local Authentication with Cisco IOS Software Releases 11.3.3.T or later

```
!--- This is the part of the configuration related to
local authentication.

!
aaa new-model
aaa authentication login default local
aaa authorization exec default local
username one privilege 15 password one
username three password three
username four privilege 7 password four
ip http server
ip http authentication local
!
```

Reference:
http://www.cisco.com/en/US/tech/tk59/technologies_configuration_example09186a0080178a51.shtml

QUESTION NO: 3
You want to ensure that SDM has been successfully installed on router TK1. Select the command below that is used to verify that SDM has been installed on a Cisco router.

A. show manager
B. show version
C. show sdm

D. show running-config
E. show flash

Answer: E
Explanation:
Issue the "show flash' command on Cisco routers to ensure that SDM has been installed. The SDM files that will be visible from this command are the sdm.tar, sdm.shtml, and sdmconfig.cfg. All of these files are necessary to run the SDM on the router.
Reference: CCSP Self-Study Securing Cisco IOS Network (SECUR) Cisco Press, John F Roland Page 541

QUESTION NO: 4
You wish to ensure that you can use SDM on router TK1. Which four files are required for basic HTTP connectivity to SDM? (Choose four)

A. home.html
B. home.tar
C. home.cfg
D. sdm.tar
E. sdm.html
F. sdmconfig-xxx.cfg

Answer: A, B, D, F
Explanation:
To verify that SDM files are present, issue the following CLI command:
Router# show flash:

If SDM software is present, you see output resembling the following:
System flash directory:

```
File Length Name/status
 1 5148536 c831-k9o3y6-mz.122-13.ZH1.bin
 2 14617 sdm.shtml
 3 669 sdmconfig-83x.cfg
 4 2290688 sdm.tar
 5 14617 sdm.shtml.hide
 6 1446 home.html
 7 214016 home.tar
 8 1446 home.html.hide
```

[7686035 bytes used, 17434224 available, 24903680 total]
24576K bytes of processor board System flash (Read/Write)
As can be seen by the output above, the home.html, home.tar, sdm.tar, and sdmconfig-xxx.cfg files are needed for SDM to run.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod_installation_guide09186a00803e4727.html

QUESTION NO: 5
You wish to see if router TK1 is capable of supporting SDM. What is the minimum IOS release that supports SDM?

A. 11.2
B. 12.0
C. 12.1
D. 12.2
E. 6.1

Answer: D
Explanation:
SDM was first available in IOS 12.2. More specifically, SDM was initially compatible with the CiscoIOS images listed in the table below:

Table 1 SDM-Supported Routers and Cisco IOS Versions	
SDM-Supported Routers	SDM-Supported Cisco IOS Versions
Cisco 831and 837	• 12.2(13)ZH or later
Cisco 836	• 12.2(13)ZH or later
Cisco 1701	• 12.2(13)ZH or later
Cisco 1711 and 1712	• 12.2(15)ZL or later
Cisco 1710, 1721, 1751, 1751-v, 1760, and 1760-v	• 12.2(13)ZH or later
Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and 2691	• 12.2(11)T6 or later
Cisco 3640, 3661, and 3662	• 12.2(11)T6 or later
Cisco 3620	• 12.2(11)T6 or later
Cisco 3640A	• 12.2(13)T3 or later
Cisco 3725 and 3745	• 12.2(11)T6 or later
Cisco 7204VXR and 7206VXR	• 12.3(2)T or later
Cisco 7301	• 12.3(2)T or later

Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod_release_note09186a00801e7fef.html

QUESTION NO: 6
Choose the command that you will advice the new TestKing trainee technician to use to verify that SDM has been installed on a Cisco router.

A. show manager
B. show version
C. show flash
D. show sdm
E. show running-config

Answer: C

Explanation:
The quickest test is to connect your PC to the lowest-numbered Ethernet port with a cross-over cable and browse to http://<router ip-address> and see if Cisco SDM launch point is present on the resulting web page. If you have a Cisco 83x, 1701, 1710, 1711, or 1712 router, configure the PC to obtain an IP address automatically. If you have any other supported router, configure the PC with the static IP address 10.10.10.2. Alternatively, you can use the CLI to check that the Cisco SDM files are present in the router Flash memory: enter show flash and look for the Cisco SDM file set: sdm.tar, sdm.shtml, sdmconfig-xxxx.cfg. If the files are present, then confirm that the router configuration is set to support Cisco SDM.

QUESTION NO: 7
Which of the following represents the two files that are necessary to run SDM on a new TestKing Cisco router? (Select two)

A. secure.shtml
B. sdm.shtml
C. sdm.exe
D. sdm.tar
E. home.tar
F. index.htm

Answer: B, D
Explanation:
Issue the "show flash' command on Cisco routers to ensure that SDM has been installed. The SDM files that will be visible from this command are the sdm.tar, sdm.shtml, and sdmconfig.cfg. All of these files are necessary to run the SDM on the router.
Reference: CCSP Self-Study Securing Cisco IOS Networks, Cisco Press, John F Roland, Page 541

Section 2: Perform a LAN interface configuration of a Cisco router using SDM (4 questions)

QUESTION NO: 1
Cisco Security Device Manager is running on a new TestKing router. Select the maximum number of routers SDM can manage simultaneously?

A. 1
B. 5
C. 50
D. 100
E. 500
F. 1000
G. Determined by router model

Answer: A
Explanation:
Cisco Router and Security Device Manager (SDM) is a web-based configuration tool that allows you to configure LAN and WAN interfaces, routing, Network Admission Control (NAC), Network Address Translation (NAT), firewalls, Intrusion Prevention System (IPS), Virtual Private Networks (VPNs), and other features on a single router. SDM is used an application used to manage each router individually.

QUESTION NO: 2
You need to configure a new TestKing router to support management via HTTP. Choose the two commands that are used to enable the router's HTTP server for AAA. (Choose two.)

A. http server
B. ip http server
C. enable ip http server
D. http authentication aaa
E. http server authentication aaa
F. ip http authentication aaa

Answer: B, F
Explanation:
In Cisco IOS® Software Release 11.2, a feature to manage the router through HTTP was added. The ip http authentication command enables you to specify a particular authentication method for HTTP server users. The HTTP server uses the enable password method to authenticate a user at privilege level 15. The

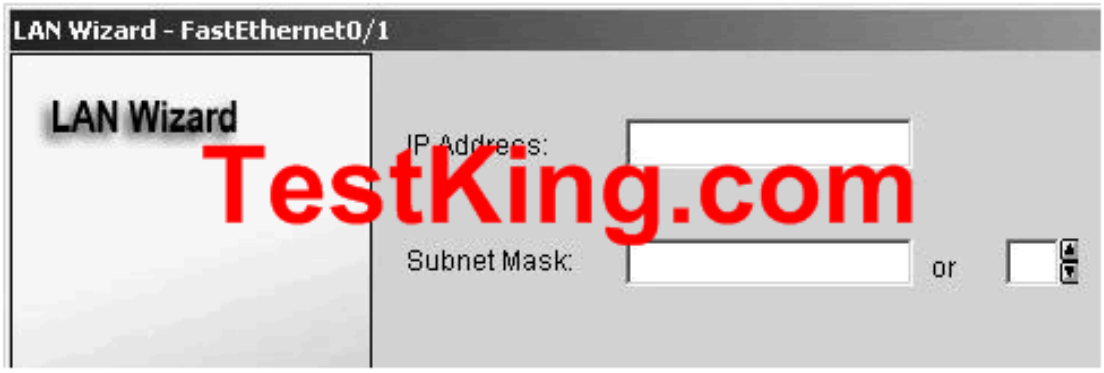
ip http authentication command now lets you specify enable, local, TACACS, or authentication, authorization, and accounting (AAA) HTTP server user authentication. In addition to this command, the "ip http server" command is needed to enable the http service on the router.

Reference:

http://www.cisco.com/en/US/tech/tk59/technologies_configuration_example09186a0080178a51.shtml#local

QUESTION NO: 3

The following wizard was seen on a TestKing router's web management portal.



Referring to the LAN Wizard screen shown above, how many bits would you input to configure this host for a subnet consisting of two hosts on subnet 172.26.26.0?

A. 3
B. 4
C. 24
D. 30
E. 128
F. 255

Answer: D

Explanation:

For any given subnet that supports only two hosts, the subnet mask of 255.255.255.252 (/30) should be used. This will provide for a network of 4 IP addresses, with only two usable IP addresses available for end hosts. Using the wizard, the number 30 should be input for the bits used in the subnet mask.

QUESTION NO: 4
Which of the following URLs is used to securely access SDM on a TestKing router with an IP address of 10.0.5.12?

A. https://10.0.5.12/flash/sdm.tar
B. https://10.0.5.12/flash/sdm.html
C. https://10.0.5.12/flash/sdm.shtml
D. https://10.0.5.12/flash/sdm
E. http://10.0.5.12/flash/sdm.shtml

Answer: C
Explanation:
SDM is stored in the router Flash memory. It is invoked by executing an HTML file in the router archive, which then loads the signed SDM Java file. To launch SDM:

Step 1 From your browser, type in the following universal resource locator (URL):

https://<router IP address>

https://... specifies that the Secure Socket Layer (SSL) protocol be used for a secure connection.

Example: https://10.0.5.12/flash/sdm.shtml

Section 3: Use SDM to define and establish a site-to-site VPN (2 questions)

QUESTION NO: 1
A network administrator is using SDM to manage one of the TestKing routers. Which one of the following actions is used to send SDM generated commands to the target router?

A. Refresh
B. Save
C. Deliver
D. Download
E. Copy-config

Answer: C
Explanation:
If you are working in advanced mode of the SDM, you must save your work by clicking the Deliver button on the SDM toolbar. The Deliver window allows you to preview the commands that you are sending to the router, and allows you to specify that you want the commands saved to the router's startup configuration.

QUESTION NO: 2
You are managing a TestKing router via the SDM web interface. Which of the following actions is used to prevent newly configured SDM commands from being sent to a target router?

A. Delete
B. Remove
C. Undo
D. Clear-commands
E. Refresh

Answer: E
Explanation:
The refresh option reloads configuration information from the router. If there are any undelivered commands, SDM displays a message window telling you that if you refresh, you will lose undelivered commands. If you want to deliver the commands, click No in the window, and then click Deliver on the SDM toolbar.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_chapter09186a00803d5ab7.h

Topic 7: Miscellaneous/Incomplete Questions (7 questions)

QUESTION NO: 1
EXHIBIT (Incomplete):

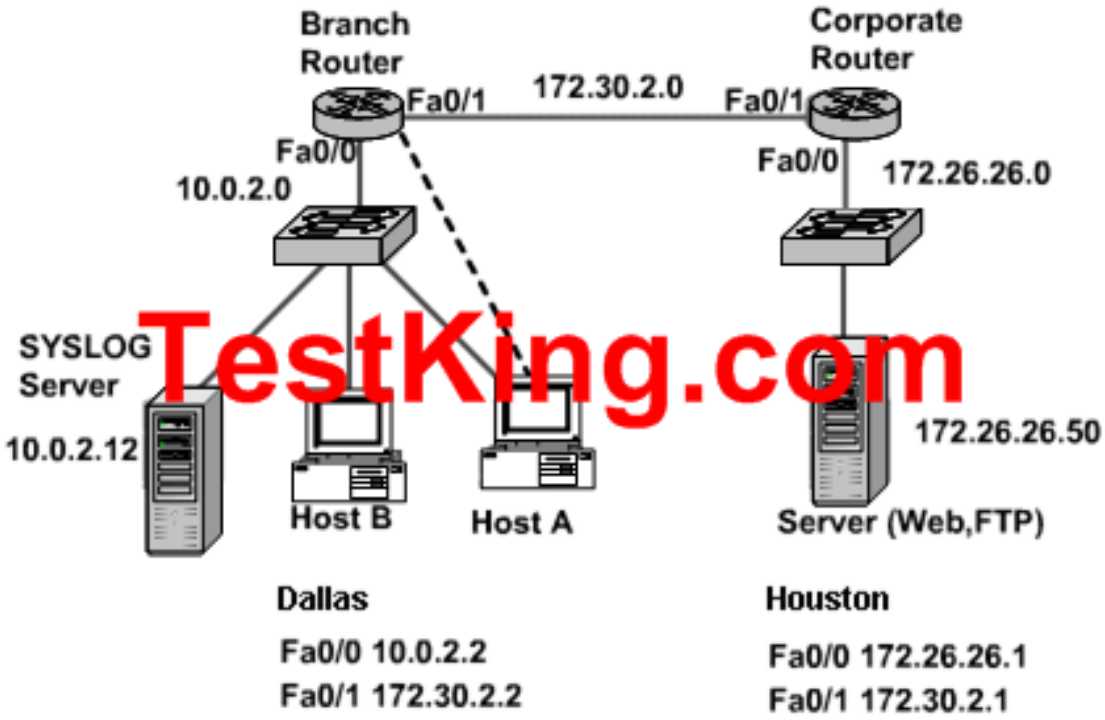
Refer to the Cisco Router and Security Device Manager page in the exhibit. What would be the best result of clicking the "Launch the selected task" button in the VPN configuration screen?

A. to start the GRE site-to-site VPN connection configuration
B. to edit the site-to-site VPN connection
C. to start the security audit
D. to start the Easy VPN Server configuration
E. to start the default site-to-site VPN connection configuration
F. to start the Easy VPN Remote configuration

Answer: E

QUESTION NO: 2 SIMULATION

The TestKing network is shown in the following exhibit:



You have been assigned to configure CBAC on a branch router for TestKing.com. One router from your oil company is named Dallas. The topology is pictured in the graphic. The corporate router has already been configured. All that is left to do is to configure CBAC on the local router to inspect Web and FTP traffic to the corporate server and to allow ICMP from any source to any destination and EIGRP from the outside interface of the corporate router to the outside interface of the branch router but block everything else. Access control list 100 has already been built and applied to Fa0/0. Do not modify access control list 100. You should add no more than three access control list statements. Logging has been enabled but you must configure the SYSLOG server address. The enable password for the router is cisco. The following passwords have been assigned to the Dallas router:

Console password: california

Vty lines 0-4 password: state

Answer:
Explanation:

```
testking# conf t
testking(config)# logging 10.0.2.12
//We specify the SYSLOG server.

testking(config)# ip inspect audit-trail
testking(config)# no ip inspect alert-off
//Used for auditing and reporting paculiar types of
packets.

testking(config)# ip inspect tcp synwait-time 30
testking(config)# ip inspect tcp finwait-time 5
//These settings are helpful in managing half-open
sessions.
//We stick with default values

testking(config)# ip inspect name FWRULE http timeout
300
testking(config)# ip inspect name FWRULE ftp timeout
300
//Configure inspect rules for users accessing Houston
Web and FTP service

testking(config)# access-list 101 permit icmp any any
testking(config)# access-list 101 permit eigrp
172.30.2.1 172.30.2.2
testking(config)# access-list 101 deny ip any any
//Using 101 to permit icmp and eigrp traffic and deny
any other traffic

testking(config)# interface Fa0/1
testking(config-if)# ip inspect name FWRULE out
testking(config-if)# ip access-group 101 in
//Placing them on the interface

testking(config-if)# end
testking(config)# copy run start
```

QUESTION NO: 3

Note: Additional information is available in the router simulation. (*Not available here*)

From where are the signatures being loaded from?

A. Built-in signatures
B. TFTP server
C. Flash
D. NVRAM

Answer: C

QUESTION NO: 4
An authentication attempt to a Cisco Secure ACS for Windows server failed, yet no log entries are in the reports. What are two possible causes of this problem? (Choose two.)

A. user is not defined
B. user belongs to the wrong group
C. CSAUTH service is down on the Cisco Secure ACS server
D. Password has expired

E. User entered an incorrect password
F. Communication path between the NAS and Cisco Secure ACS server is down

Answer: C, F

QUESTION NO: 5

Note: Additional information is available in the router simulation. (*Not available here*)

How many signatures are loaded?

A. 0
B. 82
C. 100
D. 1000

Answer: B

QUESTION NO: 6

Note: Additional information is available in the router simulation. (*Not available here*)

How many inactive signatures are loaded?

A. 0
B. 82
C. 100
D. 1000

Answer: A

QUESTION NO: 7

Note: Additional information is available in the router simulation. (*Not available here*)

To which interface is the rule applied to?

A. S0/0
B. S0/1
C. Fa0/0
D. Fa0/1

Answer: D