QUESTION 1
Exhibit:
servicepassword-encryption
!
aaa new-model
aaa authentication login default line
aaa authentication login nologin name
aaa authentication login admin tacacs+ enable
aaa authentication ppp default tacacs+
!
enable secret 5 1WogB$7.0FLEFgB8Wp.C9eqNX9L/
!!
interface Group-Async
ip unnumbered Loopback0
ip tcp header-compression passive
encapsulation ppp
async mode interactive
John at Certkiller Inc. is looking at this configuration to figure out what method authenticates through the vty
port. Which method is correct?

A. no access permitted
B. line password
C. no authentication required
D. default authentication used

Answer: B

Explanation: Enabling Authentication for LoginUsing the aaaauthentication logincommand and the
following keywords, you create one or more lists of authentication methods that are tried at login. The
lists are used with the login authenticationline configuration command.
Enter the following command in global configuration mode to enable authentication for login:
Switch# aaa authentication login {default |list-name} method1 [...[method3]]The keyword list-name is any
character string used to name the list you are creating. The method keyword refers to the actual method the
authentication algorithm tries, in the sequence entered. You can enter up to three methods:

Keyword	Description
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
tacacs+	Uses TACACS+ authentication.

Reference:
http://www.cisco.com/en/US/products/hw/switches/ps637/products_configuration_guide_chapter09186a008007
f03

QUESTION 2
James the administrator on Certkiller is trying to figure out which router table is modified or prevented from updating, if a rerouting attack occurs. (Choose one)

A. ARP
B. address
C. bridging
D. routing

Answer: D

Explanation:
Route filters can be set up on any interface to prevent learning or propagating routing information inappropriately. Some routing protocols (such as EIGRP) allow you to insert a filter on the routes being advertised so that certain routes are not advertised in some parts of the network.
Reference:Managing Cisco Network Security (Ciscopress) page 233

QUESTION 3
Brain the security administrator is in charge of creating a security policy for Certkiller Inc. 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 Certkiller Inc.
B. It defines how to track down and prosecute policy offenders at Certkiller 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 Certkiller Inc.
E. It provides a process to audit existing network security at Certkiller Inc.
F. It defines which behavior is and is not allowed at Certkiller 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 (Ciscopress) page 43

QUESTION 4
Johnthe administrator at Certkiller Inc. is working on securing the router passwords.
Which IOS command encrypts all clear text passwords in a router configuration?

A. service password-encryption
B. service password md5
C. encrypt passwords
D. enable password-encryption
E. service password-encrypted

Answer: A

Explanation:
servicepassword-encryption
To encrypt passwords, use the service password-encryption global configuration command. Use the no form of
this command to disable this service.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_command_summary_chapter09186a00800
d9c26.ht

QUESTION 5
Johnthe administrator wants to know which type of key exchange mechanism is Diffie-Hellman.

A. Private key exchange
B. RSA keying
C. Public key exchange
D. AES key exchange

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 (Ciscopress) page 467

QUESTION 6
John the security administrator for Certkiller Inc. needs to identify three character mode access methods.
Choose
three character mode access methods.

A. ppp
B. tty
C. vty

D. async
E. acl
F. aux

Answer: B C F

Explanation:
AAA and Character-Mode Traffic - AAA secure character-mode traffic during login sessions via the lines"
1. Aux
2. Console
3. TTY
4. VTY
Reference: Managing Cisco Network Security (Ciscopress) page 113

QUESTION 7
Kathy the security administrator for Certkiller Inc. is working on defending the network.
One of the attacks she is working to defend is SYN flooding and is looking to know which Cisco IOS feature defends against SYN flooding DoS attacks.

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

Answer: D

Explanation:
The TCP intercept feature in Cisco IOS software protects TCP servers from SYN-flooding attacks, a type of DoS attack.
Reference:Managing Cisco Network Security (Ciscopress) page 239

QUESTION 8
The security team at Certkiller Inc. was asked the question, what attack is most often used in social engineering. They all answered this wrong. What is the correct answer?

A. Session fragment
B. Unauthorized access
C. Data manipulation
D. Malicious applets

Answer: B

Explanation:
Social engineering is when someone attempts to manipulate others to access information or access without

authorization. Social engineering has many levels, but they all have the same goal of gaining unauthorized information or access.

QUESTION 9
Jason the security administrator Certkiller Inc. wants to know by default, how long does a router wait before terminating an unattended line connection?

A. 5 minutes
B. 10 minutes
C. 20 minutes
D. 30 minutes

Answer: B

Explanation: In the page 76 of the MCNS book you see the right data is 10 minutes.

QUESTION 10
Which of the following are Cisco firewall features? (Choose three.)

A. PIX firewall
B. authentication proxy
C. flash memory
D. CBAC
E. stateful failover
F. IDS

Answer: B, D, F

Explanation:
The Cisco IOS firewall feature set was first introduced as CiscoSecure Integrated Software (CSIS). The Cisco IOS firewall overview lists the following features:
1) Standard and extended access lists
2) Dynamic access lists
3) Reflexive access lists
4) System auditing
5) TCP intercept
6) Java blocking
7) Context-based access control - CBAC examines traffic passing through the firewall at all layers (up to the application layer). CBAC is used to generate dynamic accesslists.
8) Cisco IOS firewall IDS.
9) DoS mitigation
10) Authentication proxy - Authentication proxy is used to proxy authentication requests to AAA server. This allows authentication to occur on a per-user basis.
11) Network Address Translation
12) IPSec network security
13) Neighbor router authentication

14) Event logging
15) User authentication and authorization
16) Real-time alerts
Reference: CCSP SECUR exam certification guide p.69-70

QUESTION 11
Which of the following IOS commands will you advice the Certkiller 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
http://www.cisco.com/warp/public/793/access_dial/comm_server.html

---

QUESTION 12
What is another name for packet mode when working in a NAS environment?

A. Interface
B. PPP
C. CTY
D. Async

Answer: B
http://www.cisco.com/warp/public/707/32.html

QUESTION 13
Which of the following represents the two files that are necessary to run SDM on a Cisco Router? (Select two)

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

Answer: B, D

Explanation:
The answer are
B sdm.shtml and
D sdm.tar
Do show flash on cisco router sdm the single files available are sdm.tar, sdm.shtml and sdmconfig.cfg All these fiel are necessary to run the SDM on the router, instead of the SDM.exe is to install the application on

router but not to run the application
CCSP Self-Study Securing Cisco IOS Network (Secur) CiscoPress.comJohn F Roland
Page 541
Note:
Copy the SDM files on the TFTP server to the router Flash memory, using the following CLI commands:
Router# copy tftp://<tftp server IP address>/sdm.tar flash:
Router# copy tftp://<tftp server IP address>/sdm.shtml flash:
Router# copy tftp://<tftp server IP address>/home.tar flash:
Router# copy tftp://<tftp server IP address>/home.html flash

QUESTION 14
Choose the command that you will advice the new Certkiller 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
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. The configuration requirements are explained
in the document Downloading and Installing SDM.

QUESTION 15
Which of the following protocols can you use to provide secure communications between a target router
and SDM? (Select two.)

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

Answer: A, D
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 16
Which of the following actions can you take to prevent newly configured commands from being sent to a target router?

A. delete
B. remove
C. undo
D. clear-commands
E. refresh

Answer: E
To send the commands, you have to do a Deliver. However, if you do a refresh, then the router is polled and the current configuration on the router is brought back to the SDM and any changes that were not yet delivered would be lost.
Therefore, the answer is REFRESH - E

QUESTION 17
Which one of the following actions can you take to enable SDM generated commands to reach the target router?

A. You could refresh.
B. You could save.
C. You could deliver.
D. You could download.
E. You could copy-config.

Answer: C
If you are working in Advanced mode, 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 18
Which of the following URLs is used to securely access SDM on a 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

Answer: C
Start SDM
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

---

QUESTION 19
What is the maximum amount of routers SDM can manage simultaneously?

A. 1
B. 5
C. 50
D. 100
E. determined by router model
F. all of the above

Answer: A
One. Cisco SDM is a tool for configuring, managing, and monitoring a single Cisco router. Each Cisco router is accessible with its own copy of Cisco SDM.

QUESTION 20
Which of the following is the minimum IOS release that is capable of supporting SDM?

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

Answer: D

QUESTION 21
How many devices can Cisco SDM administer?

A. 1
B. 2
C. 3
D. 4
E. There is no limit.

Answer: A
Cisco SDM is a tool for configuring, managing, and monitoring a single Cisco router. Each Cisco router is accessible with its own copy of Cisco SDM.

QUESTION 22
What version of Cisco IOS is used for SDM?

A. Version 12.2 and later

Answer: A

QUESTION 23
Which of the following configurations restricts telnet access to a 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.

QUESTION 24
Which of the following commands encrypts all router passwords?

A. service config-passwords
B. service running-encryption
C. service password-encryption
D. service encrypt-passwords

Answer: C

Explanation:
Using the global configuration command service password-encryption, causes all passwords to be encrypted so they are unreadable when the router configuration is viewed.

QUESTION 25
Which of the following configuration register values will allow a Cisco router to go immediately into ROM mode at any time during a routers operation?

A. 0x2101
B. 0x2002

C. 0x2210
D. 0x2102

Answer: B

Explanation:
If bit 8 of the configuration register is off (0x2002) the router can be sent directly into ROM mode at any time if the break key is issued, losing the running configuration. If bit 8 is turned on (0x2102), the break key can only be issued within the first 60 seconds of router boot up.

QUESTION 26
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

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.

QUESTION 27
Which of the following AAA security server protocols can the IOS Firewall support? Select all that apply.

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

Answer: C, D

Explanation:
The IOS Firewall can communicate with a AAA server running either RADIUS or TACACS+.

QUESTION 28
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 29
What is the range of the number of characters the IOS enable secret password can be?

A. 1-20
B. 1-25
C. 4-24
D. 4-30

Answer: B

Explanation:
An IOS enable secret password must be between 1 and 25 characters long. The first character cannot be a number.

QUESTION 30
Which of the following commands enables TCP Intercept?

A. tcp intercept enable
B. ip tcp intercept enable
C. ip tcp intercept enable list
D. ip tcp intercept list

Answer: D

Explanation:
To enable TCP Intercept define an access list for hosts you want to protect, then reference that list with the ip tcp intercept list (list) command.

QUESTION 31
What must you change the configuration register value to, when you need to perform password recovery on a router?

A. 0x2102
B. 0x2142

C. 0x2241
D. 0x2410

Answer: B

Explanation:
Setting the configuration register value to 0x2142 will force the router upon a reboot, to boot the image from flash, but to ignore the startup configuration. This allows you to set an enable secret, then to copy the running configuration to the startup configuration, thus performing password recovery.

QUESTION 32
How many incomplete connections must a router have by default before TCP Intercept will start dropping incomplete connections?

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

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 33
What is the bit length of the Diffie-Hellman group 1 algorithm?

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

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 34
Which of the following is NOT a component of AAA?

A. Authentication

B. Access
C. Administration
D. Authorization
E. Accounting
F. Authority

Answer: B, C, F

Explanation:
The three components of AAA are Authentication, Authorization, and Accounting.

QUESTION 35
Kathy is the security administrator at Certkiller Inc. and needs to identify two packet mode access methods.
Choose two packet mode access methods. (Choose two)

A. Sync
B. BRI
C. Group-sync
D. Telnet
E. tty
F. Async

Answer: B F

Explanation:
AAA and Packet-Mode Traffic
AAA technologies can also proctect dialup access in the packet or interface mode via async, group-async, Basic
Rate Interface (BRI) ISDN lines, or Primary Rate Interface (PRI) ISDN interfaces on Cisco Routers.
Reference: Managing Cisco Network Security (Ciscopress) page 114

QUESTION 36
Johnthe administrator at Certkiller Inc. is looking at the router configuration to help him look for the
following debug output, which two statements are true? (Choose two)
1d16h: %LINK-3-UPDOWN: Interface Serial3/0, changed state to up
*Mar 2 16:52:15.297: Se3/0 PPP: Treating connection as a dedicated line
*Mar 2 16:52:15.441: Se3/0 PPP: Phase is AUTHENTICATING, by this end
*Mar 2 16:52:15.445: Se3/0 CHAP: O CHALLENGE id 7 len 29 from 'NASx'

A. The user identity is NASx.
B. This is a connection attempt to an async port.
C. The connection is established on serial interface 3/0.
D. The client is attempting to setup a Serial Line Internet Protocol connection.
E. The user is authenticating using CHAP.
F. The DHCP server sends a getpass request to prompt for the password.

Answer: C E

Explanation:
ldl6h: %LINK-3-UPDOWN: Interface Serial3/0, changed state to up
The "up" means the serial interface has connectivity.
The CHAP initiation sequence and three-way handshake occur as follows:
1. The PPP link is established after dialup.
2. The network access server (NAS) tells the remote client to use CHAP.
3. The remote client responds with an OK.
4. The three-way handshake occurs as follows:
5. 1. The network access server sends a challenge message to the remote client.
2. The remote client replies with a one-way hash value.
3. The network access server processes the received hash value. If it matches the station's own calculation, authentication is acknowledged.
Reference:Managing Cisco Network Security (Ciscopress) page 123

QUESTION 37
Which of the following are commands that can be entered on an IOS Firewall router to debug communications with a AAA server? Select all that apply.

A. debug aaa all
B. debug ip aaa
C. debug aaa accounting
D. debug tacacs

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.
Debug ip aaa is not a valid command.

QUESTION 38
Where are debugging messages sent to by default on a router?

A. console line
B. internal buffers
C. vty lines
D. syslog server

Answer: A

Explanation:
By default, output from a debug command will only be sent to the console connection. Use the no logging console command to disable it.

QUESTION 39
Which of the following router commands can monitor AAA RADIUS?

A. show radius errors
B. show radius statistics
C. show ip aaa
D. show radius monitoring

Answer: B

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

QUESTION 40
John the security administrator at Certkiller Inc. needs to select three types of authentication supported by Cisco Secure ACS 3.0.1. (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 41
John from security department at Certkiller Inc. is looking for an external database for CSACS for windows. Which three external databases are supported by Cisco Secure ACS for Windows? (Choose three)

A. Token Server
B. SQL-Linux
C. Netware NDS
D. ODBC
E. Windows-NT/2000
F. AAA

Answer: C D E

Explanation:
CSNT can authenticate users who are defined in Network Operating System Security databases or directory services, such as Novell NDS or Window NT accounts database, and it supports authentication forwarding to LDAP servers. ODBC support is available to rapidly import a large number of users.
Reference: Managing Cisco Network Security (Ciscopress) page 183

QUESTION 42
Which of the following statements regarding Cisco Secure ACS are valid? (Choose all that apply.)

A. NAS has the ability to access multiple Cisco Secure ACS for Windows Server
B. Cisco Secure ACS for Window server is capable of logging only onto external server
C. The Cisco Secure ACS for Windows server supports TACACS exclusively
D. Database replication is supported by Cisco Secure ACS for Windows
E. The server used for authorization and authentication on a Cisco Secure ACS for Windows server is called CSAdmin
F. Cisco Secure ACS for Windows server use CSDBSync for manage user and group account.

Answer: A, B, D
A True
B.True
C.False, it work with TACACS and Radius Server
D. True, Database replication is supported by Cisco Secure ACS for Windows
E. False because CSAuth provides authentication and authorization services
F..False, CSDBSyns provides synchronization of the Cisco Secure user database with an external RDBMS application

---

QUESTION 43
Which of the following statements regarding Cisco Secure ACS are valid? (Choose three).

A. NAS is capable of accessing multiple Cisco Secure ACS for Windows server.
B. 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
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:
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.

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.

CSV files is not a database so option B is correct.

QUESTION 44
How much disk space is required to install AAA CSACS 3.0 for Windows?

A. 900mb
B. 100mb
C. 250mb
D. 500mb

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.

QUESTION 45
Which of the following is NOT supported by CSACS 3.0?

A. Radius/Tacacs+ secret keys
B. installation on Windows NT
C. SSL
D. HTTP

Answer: C

Explanation:
You cannot use SSL to administratively connect to the CSACS AAA server in version 3.0, but you can in 3.1 and later.

QUESTION 46
What operating systems can CSACS be installed on? Select all that apply.

A. Windows 2000
B. Unix
C. Windows NT
D. OS X
E. Solaris

Answer: A, B, C

Explanation:
CSACS is AAA software that can be installed on Windows NT, Windows 2000, and Unix. However, CSACS 3.2 can only be installed on Windows 2000 (or you can purchase a standalone appliance module from Cisco running 3.2 CSACS).

QUESTION 47
What is the minimum IOS version your NAS router must have inorder to communicate with a AAA server such as CSACS 3.0 for Windows 2000?

A. 12.3
B. 11.1
C. 11.5
D. 12.0

Answer: B

Explanation:
To set your NAS router up to communicate with a AAA server, you must have at least IOS version 11.1.

QUESTION 48
What is the RADIUS vendor-specific attribute number?

A. 26
B. 50
C. 14
D. 38

Answer: A

Explanation:
The vendor-specific RADIUS attribute (attribute number 26) allows vendors to create their own extended RADIUS attributes. Cisco is vendor ID number 9.

QUESTION 49
Which of the following is the default login URL for CSACS 3.0?

A. http://127.0.0.1:4002
B. http://127.0.0.1:2002
C. http://127.0.0.1:2502
D. http://127.0.0.1:4502

Answer: B

Explanation:
Use IP address 127.0.0.1 (local loopback) with port 2002 to access CSACS from the host CSACS is installed on. Substitute the local loopback with the IP address of the CSACS server to access the server remotely I.E. 192.168.10.10:2002.

QUESTION 50

You are the administrator for Certkiller , Inc. Your job today is to configure a start-accounting record for a Point-to-Point session to be sent to a TACACS+ server.
Which configuration command will do this?

A. aaaaccounting network default start-stop tacacs+
B. aaaauthentication ppp start tacacs+
C. aaaauthorization exec default tacacs+
D. aaaauthorization network default tacacs+
E. aaaaccounting network default stop-only tacacs+

Answer: A

Explanation:
aaaaccounting {system | network | exec | command level} {start-stop |
wait-start | stop-only} {tacacs+ | radius}
no aaa accounting {system | network | exec | command level}
networkRuns accounting for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP.
start-stopSends 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.
tacacs+Enables the TACACS-style accounting.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_command_summary_chapter09186a00800 d9c0e.ht

---

QUESTION 51

Jason the security administrator was given the following configuration statement. After looking at the command, he knows two statements are true. Which two are correct statements?
(Choose two)
router(config)#aaa authentication login default tacacs+ none

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
password. However, all other users can only use TACACS+:

none- no authorization is performed.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps4911/products_user_guide_chapter09186a008015c5c3.html

---

QUESTION 52
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
Cisco uses the Terminal Access Controller Access Control System plus (TACACS+) protocol to communicate with remote AAA servers.

QUESTION 53
Which of the following router commands will allow all 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

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 54
You are the network security administrator for Certkiller .com. Certkiller has just added TACACS+ AAA authentication to their remote access topology, requiring you to add two TACACS+ servers to the Certkiller PR perimeter router configuration. First, enable the router's AAA access control model and then add the two TACACS+ servers and their respective keys. Use the following values as necessary:
Parameter: Value
TACACS+ Server Certkiller 1 - IP address 10.10.1.2
TACACS+ Server Certkiller 1 - Key Certkiller 1
TACACS+ Server Certkiller 2 - IP address 10.10.1.3
TACACS+ Server Certkiller 2 - Key Certkiller 2
Enable secret password is " Certkiller "
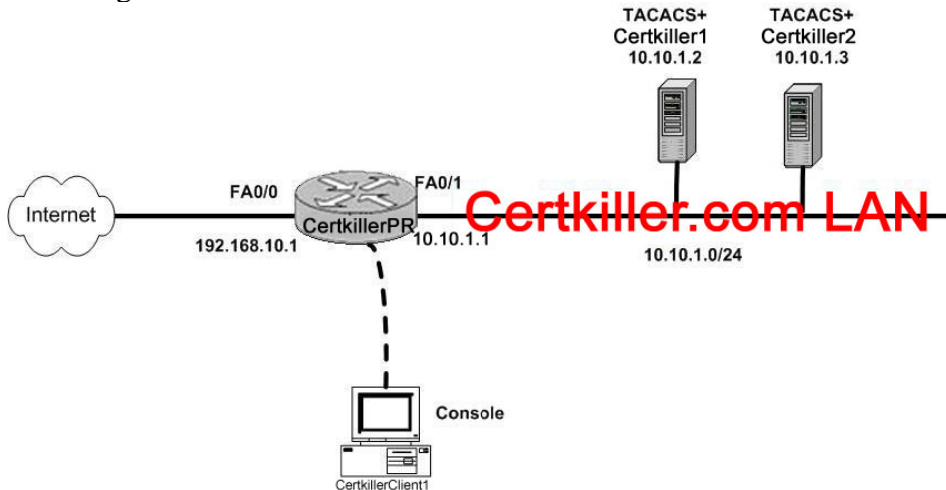Perimeter Router:

Name: Certkiller PR
FA0/0 : 192.168.10.1
FA0/1 : 10.10.1.1
Secret password: Certkiller
To configure the router click on the host icon that is connected to a router by a serial cable.

Answer:
>enable
password: Certkiller
#Config t
(config) aaa new-model
(config) Tacacs-server host 10.10.1.2 key Certkiller 1
(config) Tacacs-server host 10.10.1.3 key Certkiller 2
(config) #exit
Note:variations of simulations occur. Read carefully and be ready to adopt simulation.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps637/products_configuration_guide_chapter09186a008007f032.htm
Alternative #1:
Parameter: Value
TACACS+ Server Certkiller 1 - IP address 16.2.1.2
TACACS+ Server Certkiller 1 - Key Certkiller 1
TACACS+ Server Certkiller 2 - IP address 16.2.1.3
TACACS+ Server Certkiller 2 - Key Certkiller 2
Enable secret password is " Certkiller "
Perimeter Router:
Name: Certkiller PR
FA0/0 : 192.168.1.1
FA0/1 : 16.2.3.1
Secret password: Certkiller

QUESTION 55
Jacob at Certkiller Inc. was given the assignment to secure the network from giving out unauthorized

information. His first step is to prevent the perimeter router from divulging topology information by telling external hosts which subnets are not configured. Which command fits this objective?

A. no source-route
B. no ip route-cache
C. no service udp-small-servers
D. no ip unreachable

Answer: D

Explanation:
To enable the generation of Internet Control Message Protocol (ICMP) unreachable messages, use the ip unreachablescommand in interface configuration mode. To disable this function, use the noform of this command.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipras_r/ip1_i2g.htm#1082329

QUESTION 56
John the security administrator at Certkiller Inc. is in charge of securing the network against Chargen attacks. Which two commands prevent a Chargen attack? (Choose two)

A. no ip redirects
B. no tcp-small-servers
C. no ip-source route
D. no chargen enable
E. no udp-small-servers
F. no service finger
G. no service tcp-small-servers
H. no service udp-small-servers

Answer: G, H

Explanation:
TCP and UDP "Small Services"
By default, Cisco devices up through IOS version 11.3 offer the "small services": echo, chargen, and discard. These services, especially their UDP versions, are infrequently used for legitimate purposes, but can be used to launch denial of service and other attacks that would otherwise be prevented by packet filtering.
For example, an attacker might send a DNS packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to the Cisco's UDP echo port, the result would be the Cisco sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet, since it would be considered to be locally generated by the router itself.
Although most abuses of the small services can be avoided or made less dangerous by anti-spoofing access lists, the services should almost always be disabled in any router which is part of a firewall or lies in a security-critical part of the network. Since the services are rarely used, the best policy is usually to disable them on all routers of any description.

The small services are disabled by default in Cisco IOS 12.0 and later software. In earlier software, they may be disabled using the commands no service tcp-small-serversand no service udp-small-servers .

QUESTION 57
The security team at Certkiller Inc., is looking for the command that disables the chargenand echo services on an IOS router?

A. no tcp-small-servers
B. disable tcp small-services
C. disable small services
D. no service tcp-small-servers

Answer: D
By default, the Cisco router has a series of diagnostic ports enabled for certain UDP and TCP services including echo, chargen, and discard. When a host attaches to those ports, a small amount of CPU capacity is consumed to service these requests
Any network device that has UDP and TCP diagnostic services should be protected by a firewall or have the services disabled. For a Cisco router, this can be accomplished by using these global configuration commands.
noservice udp-small-servers
noservice tcp-small-servers

QUESTION 58
The Certkiller trainee technician wants to know what the Cisco IOS command to disable the direct broadcast is. What will your reply be?

A. no ip broadcast
B. no broadcast
C. no ip directed-broadcast
D. ip prodcast disable
E. disable ip broadcast

Answer: C

Explanation:
Unless applications or other explicit requirements need the router interfaces to have IP directed broadcasts, it should be turned off, to suppress the effects of this attack. You can use the no ip directed-broadcast command to do so on the Cisco IOS Software.
The no ip directed-broadcast interface command is the default in Cisco IOS Software Release 12.0 and later. In earlier versions, the command should be applied to every LAN interface that isn't known to forward legitimate directed broadcast.
Reference: CCSP student guide p.197

QUESTION 59
Which of the following is the Cisco IOS command to disable finger service?

A. disable finger

B. no finger
C. no finger service
D. no service finger
E. finger disable

Answer: D

Explanation:
Cisco routers provide an implementation of the finger service, which is used to find out which users are logged in to a network device. This service is equivalent to issuing a remote show users command. Although the information gained may seem harmless, it could be valuable to an attacker. You can disable the finger service with the command no service finger.
Reference: CCSP student guide p.199

QUESTION 60
Which command will deny the perimeter router the ability to divulge topology information by telling external hosts which subnets are not configured?

A. no source-route
B. no service udp-small-servers
C. no ip unreachables
D. no ip route-cache
E. all of the above

Answer: C

QUESTION 61
Which IOS command will you advice the Certkiller trainee to use to disable the processing of IP packets that includes source routing information?

A. no ip routing source
B. no ip host routing
C. no ip source-route
D. disable ip source route

Answer: C

QUESTION 62
Which command can you use to disable finger replies on a perimeter router?

A. The no finger command
B. The no finger reply command
C. The disable finger command
D. The no service finger command

Answer: D

Cisco routers provide an implementation of the "finger" service, which is used to find out which users are logged into a network device. Although this information isn't usually tremendously sensitive, it can sometimes be useful to an attacker. The "finger" service may be disabled with the command no service finger.

QUESTION 63
How do you enable the Nagle algorithm on an IOS router?

A. ip nagle
B. service nagle
C. enable service nagle
D. enable ip nagle

Answer: B

Explanation:
Use the global configuration mode command service nagle to enable the TCP congestion Nagle algorithm. The Nagle algorithm attempts to bunch traffic into fewer TCP packets, thus saving on bandwidth. This command is disabled by default.

QUESTION 64
Which of the following router commands will prevent a router from giving an attacker a valid IP address via DHCP?

A. no tcp-dhcp-servers
B. no service dhcp
C. no ip dhcp servers
D. no dhcp server

Answer: B

Explanation:
The IOS command no service dhcp will prevent the router from responding to DHCP requests on all interfaces. You cannot disable only certain interfaces, if you need to allow this service, apply proper ACL's.

QUESTION 65
What is IP spoofing?

A. altering the source ip address in packets
B. sending large amounts of icmp packets to a broadcast address
C. altering ip routing tables
D. packet sniffing

Answer: A

Explanation:

An IP spoof is when an attacker changes the source IP address of network packets, usually in attempt to bypass access lists or to DOS the real IP source

QUESTION 66
What is the global IOS command that disables Cisco Discovery Protocol (CDP) completely?

A. no cdp enable
B. no cdp server
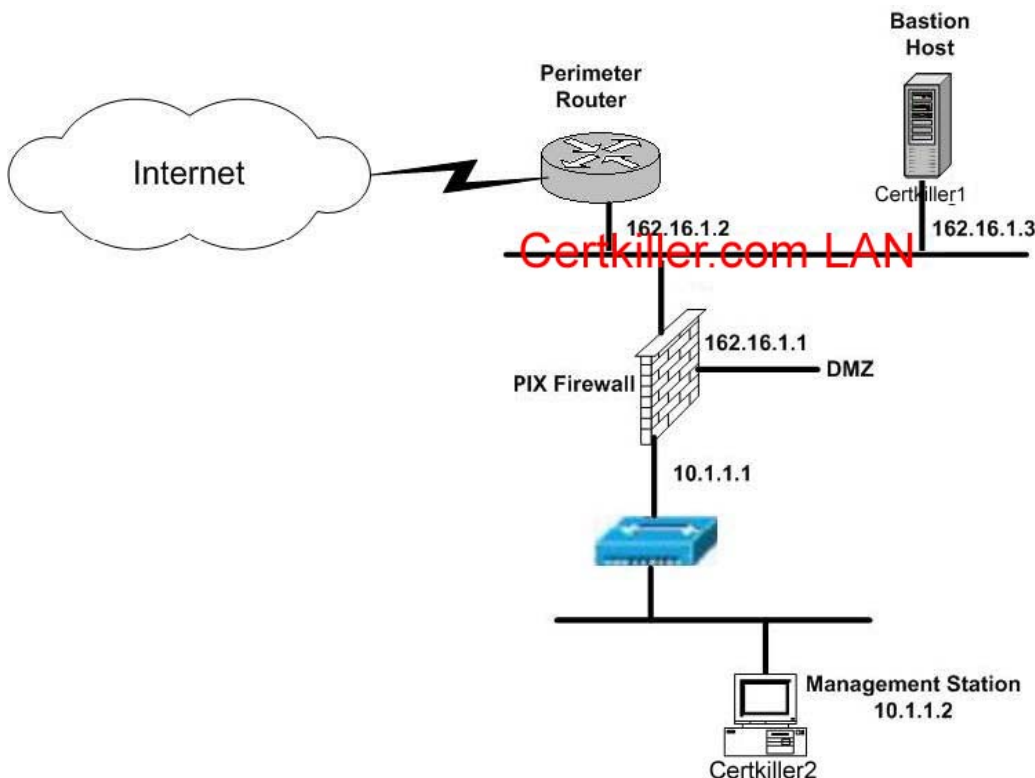C. no cdp process
D. no cdp start
E. no cdp run

Answer: E

Explanation:
Use the global configuration command no cdp run to disable CDP on all router interfaces. To disable CDP on an interface basis, go into interface configuration mode and enter no cdp enable.

QUESTION 67
Exhibit:

You are the administrator at Certkiller Inc. and you need to add an ACL statement to protect against address spoofing when applied inbound on the external interface of the perimeter router.
Which one of these commands is correct?

A. access-list 101 deny IP 162.16.1.0 0.0.0.255. 0.0.0.0 255.255.255.255

B. access-list 101 deny UDP 162.16.1.0 255.255.0.0 0.0.0.0 255.255.255.255
C. access-list 101 deny IP 162.16.1.0 255.255.255.0 0.0.0.0 255.255.255.255
D. access list 101 permit IP 162.16.1.0 255.255.0.0 0.0.0.0 255.255.255.255
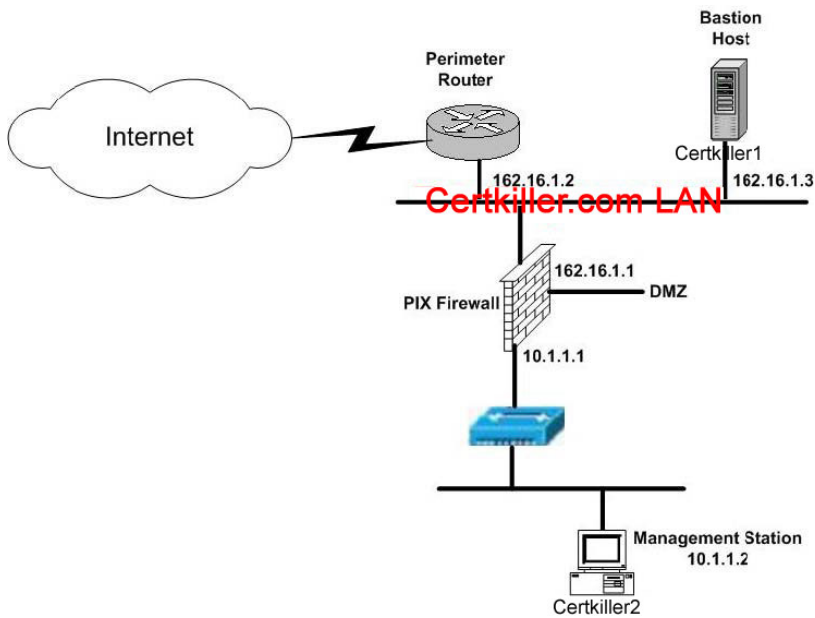
Answer: A

Explanation:
access-list101 deny IP 162.16.1.0 0.0.0.255 0.0.0.0 255 255.255.255
access-list command - command to deny access to the 162.16.1.0 0.0.0.255 addresses from any address (0.0.0.0
255.255.255.255)
Reference:Managing Cisco Network Security (Ciscopress) page Appendix C

QUESTION 68
Exhibit:

Greg has just started working as the security administrator at Certkiller Inc. His manager asked him to prevent
Internet users from pinging the PIX. Which ACL statement should be configured on the external interface of the
perimeter router?

A. access-list 102 deny tcp any 162.16.1.1 0.0.0.0
B. access-list 102 permit tcp any 162.16.1.1 0.0.0.0 echo
C. access-list 102 deny icmp any 162.16.1.1 0.0.0.0 echo-reply
D. access-list 102 deny icmp any 162.16.1.1 0.0.0.0 echo

Answer: D

Explanation:
Echo added to the end of the command implies no ping requests to the PIX.
Reference:Managing Cisco Network Security (Ciscopress) pages 728

QUESTION 69
Johnthe administrator is working on defending the network against attack. He needs to know which Cisco IOS feature defends against an unauthorized access attempt?

A. IKE
B. IPSO
C. TCP intercept
D. IOS ACLs
E. CBAC

Answer: D
Access list permits who can enter and leave the network when it is applied to the interface of a perimeter router.

QUESTION 70
Which command will you advice the Certkiller trainee technician to use to apply an access list to a router interface?

A. ip access-list
B. ip access-class
C. ip access-group
D. apply access-list

Answer: C
Cisco Self-Study CCSP SECUR page 210

QUESTION 71
Which of the following IOS commands will enable turbo access list?

A. turbo acl
B. fast ip acls
C. acl turbo
D. access-list compiled
E. all of the above

Answer: D
http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a0080080374.html#10 19763

QUESTION 72
What are the ACL number ranges for IP standard ACL's? Select all that apply.

A. 1-99
B. 100-199
C. 1300-1999
D. 800-1299

Answer: A, C

Explanation:
IP standard access lists can be numbered from 1-99 or from the expanded range of 1300-1999.

QUESTION 73
Which of the following correctly applies ACL 101 inbound on an interface?

A. ip access-class 101 inbound
B. ip access-group 101 in
C. ip access-list 101 in
D. ip access-range 101 inbound
E. ip access-group 101 inbound
F. ip access-list 101 inbound
G. ip access-class 101 in
H. ip access-range 101 in

Answer: B

Explanation:
After creating an access list, you must apply it to an interface with the access-group command in interface configuration mode, and specify the direction to monitor traffic with the in or out keyword.

QUESTION 74
Which of the following can be an IP extended ACL? Select all that apply.

A. ACL 3601
B. ACL 99
C. ACL 1401
D. ACL 100
E. ACL 2101

Answer: D, E

Explanation:
An IP extended ACL can be numbered within any of the following ranges: 100-199, 2000-2699.

QUESTION 75
Which of the following commands correctly references access list 120 in a crypto map?

A. Router(config-crypto-map)#match address 120
B. Router(config-crypto-map)#set peer 120
C. Router(config-crypto-map)#set list 120
D. Router(config-crypto-map)#match list 120

Answer: A

Explanation:
After defining a crypto map, and entering into crypto map configuration, you must specify the hosts needing encryption by defining those hosts in an access list and referencing that list with the match address (acl) command.

QUESTION 76
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

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_chapter09186a00800 ca7c1.ht

---

QUESTION 77
You are the security administrator for Certkiller 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 Certkiller Inc.
B. Provides additional visibility at intranet, extranet, and Internet perimeters at Certkiller Inc.
C. Protects the network from internal attacks and threats at Certkiller Inc.
D. Provides secure, per-application access control across network perimeters at Certkiller 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_chapter09186a00800 d9815.ht

QUESTION 78
Paul the security administrator is working to fight against DoS attacks. He has a lot of work to do, starting with knowing which three thresholds CBAC on the Cisco IOS Firewall provides against DoS attacks. (Choose three)

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

Answer: B C F
Half Open Sessions
An unusually high number of half-open sessions (connection requests that are not completed) could indicate that a DoS attack is occurring or that someone is conducting a port scan. CBAC measures both the Total number of half-open sessions and the rate of session establishment attempts. It counts total TCP and UDP half-open sessions and measures the rate of half-open session establishment once per minute. 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:Managing Cisco Network Security (Ciscopress) page 273

QUESTION 79
Which of the following represents the aggressive mode of CBAC in 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

Answer: D
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 80
What role does CBAC play?

A. CBAC creates a temporary opening in the firewall's ACLs to allow return traffic and additional data connections for permissible sessions.
B. Nothing.

Answer: A

Explanation:
CBAC creates temporary openings in ACLs at Cisco IOS firewall interfaces. These openings are created when specified traffic exits your internal network through the Cisco IOS firewall. The openings allow returning traffic that would normally be blocked. The traffic Is allowd back through the Cisco IOS firewall only if it is part of the same session as the original traffic that triggered CBAC when exiting through the Cisco IOS frewall
Reference: CCSP SECUR student guide p.237

QUESTION 81
What could be the reason why an authentication attempt to a CSACS for Windows server failed yet no log entries are in the report? (Choose two)

A. the password has expired
B. user enter incorrect password
C. Communication path between the NAS and Cisco Secure ACS server is down
D. User is not defined
E. User belong to a different group
F. CSAuth service is down on the Cisco Secure ACS Server

Answer: C, F

QUESTION 82
What OSI layers can CBAC filter on? Select all that apply.

A. layer 4
B. layer 3
C. layer 2
D. layer 7

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 83
By default how long will CBAC monitor an idle TCP session in the state table before deleting the entry?

A. 60 minutes
B. 5 minutes

C. 30 seconds
D. 20 minutes

Answer: A

Explanation:
The default CBAC global TCP idle session timeout value is 3600 seconds (60 minutes). This can be overridden for specific protocols.

QUESTION 84
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.

QUESTION 85
Which of the following access lists is CBAC unable to alter? Select all that apply.

A. ACL 1335
B. ACL 35
C. ACL 135
D. ACL 2335

Answer: A, B

Explanation:
CBAC does not alter standard IP access lists. Only an extended access list can be used to get the benefit of CBAC traffic filtering.

QUESTION 86
By default, after 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).

QUESTION 87
Which of the following encryption protocols can the Cisco IOS Firewall support? Select all that apply.

A. CAST
B. Twofish
C. DES
D. 3DES
E. AES

Answer: C, D, E

Explanation:
The Cisco IOS Firewall can support DES (56 bit), 3DES (168 bit), and AES (128, 192, 256 bit) encryption protocols for VPN tunnels.

QUESTION 88
Which of the following dynamically alters access lists?

A. CBAC
B. IPSEC
C. Kerberos
D. AAA

Answer: A

Explanation:
CBAC monitors traffic and dynamically alters access lists to allow specified return traffic. CBAC then dynamically closes the hole(s) in the access list(s) once the session is finished.

QUESTION 89
What is the command to enable logging to all configured destinations (other than the console) on a router?

A. logging facility
B. logging enable
C. logging on
D. logging server

E. logging messages
F. logging enabled

Answer: C

Explanation:
Enable logging to destinations other than the console port, such as internal buffers, terminal monitor (telnet/vty line), or a syslog server with the logging on command.

QUESTION 90
How many IDS signatures can the Cisco IOS Firewall scan for?

A. 207
B. 59
C. 426
D. 12

Answer: B

Explanation:
The IDS component of the Cisco IOS Firewall can monitor 59 different IDS signature attacks.

QUESTION 91
Which of the following will happen during the aggressive mode of the CBAC on the Cisco IOS Firewall?

A. CBAC will delete all half-open sessions.
B. CBAC will re-initiate half-open sessions.
C. CBAC will complete all half-open sessions, making them fully open sessions.
D. CBAC will delete half-open sessions as needed to accommodate new connections requests.

Answer: D

QUESTION 92
Kathy from the security department at Certkiller Inc. wants to know what does a half-open TCP session on the Cisco IOS Firewall mean.

A. Session was denied.
B. Session has not reached the established state.
C. Three-way handshake has been completed.
D. 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_chapter09186a00800
d9806.h

QUESTION 93
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)

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 94
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 95
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:

This 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 96
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 97
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:
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.

QUESTION 98
John is the administrator working on configuring the authentication proxy feature. He is not sure what the authentication proxy feature does on the Cisco IOS Firewall.

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

Answer: C
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_chapter09186a00800 d981d.ht

---

QUESTION 99
John is the administrator working on configuring the authentication proxy feature. He is not sure what the authentication proxy feature does on the Cisco IOS Firewall.

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

Answer: A

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_chapter09186a00800 d981d.ht

---

QUESTION 100
Certkiller Inc. just hired a new security administrator named Paul. He is working on authentication proxy for his first project. He does not know how the user triggers the authentication proxy after the idle timer expires. Which one of these answers is the right answer?

A. Authenticates the user.
B. Initiates another HTTP session.
C. Enters a new username and password.
D. Enters a valid username and password.

Answer: B
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_chapter09186a00800d981d.ht

---

QUESTION 101
Johnthe security administrator is having issues with the IOS Firewall authentication proxy. He needs to know what the default idle time of an enabled IOS Firewall authentication proxy before he can start using it.

A. 60 minutes
B. 5 seconds
C. 60 seconds
D. 5 minutes

Answer: A

Explanation:
ipauth-proxy auth-cache-timemin - Sets the global authentication proxy idle timeout value in minutes. If the timeout expires, user authentication entries are removed, along with any associated dynamic access lists. The default value is 60 minutes.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide_chapter09186a00800a17ec.html

---

QUESTION 102
John and Kathy are the security administrators at Certkiller Inc. with one job left for the day. They have to select
the three RADIUS servers supported by the Cisco IOS Firewall authentication proxy. Which three are the correct answers? (Choose three)

A. Oracle
B. DB2
C. Cisco Secure ACS for Windows NT/2000
D. Cisco Secure ACS for UNIX
E. Lucent
F. TACACS+

Answer: C D E

Explanation:
The supported AAA servers are CiscoSecure ACS 2.3 for Windows NT, CiscoSecure ACS 2.3 for UNIX, TACACS+ server (vF4.02.alpha), Ascend RADIUS server - radius-980618 (required avpair patch), and Livingston (now Lucent), RADIUS server (v1.16).
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide_chapter09186a00800a17ec.html

QUESTION 103
In which of the following ways will the proxy respond to HTTP if no valid authentication entry exists in the authentication?

A. Proxy will prompt the user for user name
B. Proxy will prompt the user for password
C. Proxy will prompt the user for user and password
D. Proxy will send an alert to the Cisco Secure ACS server

Answer: C
Cisco Self-Study CCSP SECUR page 257

QUESTION 104
Which of the following situations brought on by a user will trigger the authentication proxy or the Cisco firewall?

A. When a user initiate inbound interface
B. When a user logon through firewall
C. When a user initiate an FTP session through the firewall
D. When a user initiate HTTP session through the firewall

Answer: D
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/scdauthp.htm

QUESTION 105
In which location are access profiles stored with the authentication proxy features of the Cisco IOS Firewall?

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

Answer: D
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 Cisco Secure ACS, or other RADIUS, or TACACS+ authentication server.

The access profile is stored on the ACS, you define access-list entries in ACS witch are transferred to the router upon successful authentication. (and deleted when the session ends)

QUESTION 106
Which of the following factors will act as triggers for the authentication proxy on the Cisco IOS Firewall?

A. user initiating inbound interface
B. user initiating login through the firewall
C. user initiating an FTP session though the firewall
D. user initiating an HTTP session through the firewall

Answer: D

Explanation:
Unlike many Cisco IOS firewall functions, authentication proxy is not a service that is transparent to the user. On the contrary, it requires user interaction. The authentication proxy is triggered when the user initiates an HTTP session through the Cisco IOS firewall. The firewall checks to see wether the user has already been authenticated. If the user has previously authenticated, it allows the connection. If the user has not previously authenticated, the firewall propmpts the user for a username and password and verifies the user input with a TACACS+ or RADIUS server.
Reference: CCSP student guide p.255

QUESTION 107
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 108
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.

QUESTION 109
Kathy the security administrator was given the following configuration statement. After looking at the command, she knows three statements are true. Which three are correct statements?
(Choose three)
Router(config)#aaa accounting network wait-start radius

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

Answer: C, E, 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 aaa accounting 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.

QUESTION 110
Kathy the administrator for Certkiller Inc. needs to type the command that enables the AAA access control system in the global configuration.

Answer: aaa new-model

Explanation:
To enable the AAA access control model, use the aaanew-modelglobal configuration command.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1826/products_command_summary_chapter09186a00800 d9c0d.ht

QUESTION 111
Study the Exhibit below carefully:
Certkiller Router(config)#aaa account network wait-start radius
According to the configuration statement in the exhibit, 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 aaa accounting 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.

QUESTION 112
Which of the following authorization commands are valid? (Choose two.)

A. aaa authentication exec home radius
B. aaa accounting exec home radius
C. aaa authorization default none
D. aaa authorization exec home radius
E. aaa authorization network default enable
F. aaa authorization network default local

Answer: C, F
AAA Authorization {Nework or Exe or Command level or Reverse-acces or
Configuration} { default| list name } methode 1, 2 , 3 .
Methodes => Group : use the server Tacas or Raduis
=> If-authenticated : allows the user to access the request fuction if the
usetr is authenticate
=> Krb5 : instant for the Kerboros instant map
=> Local : use the local database for authorization

=> None : no authorization is performed
CCSP Self-Study Securing Cisco IOS Network (Secur) CiscoPress.comJohn F Roland Page 102

QUESTION 113
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

Answer: A

Explanation:
The router global configuration command aaa new-model, enables aaa (radius, tacacs+) configuration
commands on the router, and disables tacacs and xtacacs.

QUESTION 114
John is the administrator at Certkiller 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_chapter09186a00800
ca7c6.ht

QUESTION 115
James the administrator of Certkiller 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
Signature structure
The signature structure indicates whether the signature implementation is either content or composite. Atomic signatures occur in a single packet, whereas composite signatures ca be spread across multiple packets.
Reference: Cisco Secure Intrusion Detection System (Ciscopress) page 192

QUESTION 116
What type of IDS attack is spread out over multiple packets?

A. atomic
B. arbitrary
C. aggregate
D. compound

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.

QUESTION 117
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

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 118
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 119
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

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 120
Which of the following commands disables an IOS Firewall IDS signature from being scanned?

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

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 121
Kathy is the administrator who is configuring IOS firewall IDS. She has two issues to consider when implementing IOS Firewall IDS. Which of these will she select?
(Choose two)

A. Signature length
B. Memory usage
C. Number of router interfaces
D. Signature coverage
E. Number of DMZs

Answer: B D

Explanation:
Memory and Performance Impact
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. 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.
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
An info signature detects information-gathering activity, such as a port sweep.
An attack signature detects attacks attempted into the protected network, such as denial-of-service attempts or the execution of illegal commands during an FTP session.
Info and attack signatures can be either atomic or compound signatures. Atomic signatures can detect patterns as simple as an attempt to access a specific port on a specific host. Compound signatures can detect complex patterns, such as a sequence of operations distributed across multiple hosts over an arbitrary period of time.
The intrusion-detection signatures included in the Cisco IOS Firewall were chosen from a broad cross-section of intrusion-detection signatures as representative of the most common network attacks and information-gathering scans that are not commonly found in an operational network.
The following signatures are listed in numerical order by their signature number in the Cisco Secure IDS Network Security Database. After each signature's name is an indication of the type of signature (info or attack, atomic or compound).
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800 ca7c6.ht

QUESTION 122
John the security administrator at Certkiller Inc. is in charge of the IOS router firewall. His job today is to choose 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 server for further analysis
B. Send an alarm to Cisco IOS director or syslog
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 packet to the sender

Answer: B, D, E

Explanation:
You must configure the IDS to respond to information and attack signatures. The response can be one or more of the of three actions:
1) alarm - This command sends an alarm to the syslog server or the centralized manager.
2) Drop - This command configures the router to drop the packets.
3) Reset - the router will send the RESET flag to both parties on the connection.
Cisco Self-Study CCSP SECUR page 290

QUESTION 123
Jason the administrator at Certkiller Inc. is wondering which module is audited first when packets enter an IOS Firewall IDS and match a specific audit rule?

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

Answer: A

Explanation:
Packets going through the interface that match the audit rule are audited by a series of modules, starting with
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide_chapter09186a00800881c0.html

QUESTION 124
John the security administrator at Certkiller Inc. is working on the IOS Firewall IDS. He needs to select the command used to enable alarming on the IOS Firewall IDS to finish his day of work. Which one of these answers is correct?

A. ip audit alarm
B. ip audit syslog-server
C. ip alarm syslog-server
D. ip audit notify

Answer: D

Explanation:
ipaudit notify
To specify the methods of event notification, use the ip audit notifyglobal configuration command. Use the noform of this command to disable event notifications.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a7f83.ht

---

QUESTION 125
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
ipaudit signature
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 signaturesignature-id {disable |list acl-list}
noip audit signaturesignature-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_chapter09186a00801a7f83.ht

---

QUESTION 126
Which of the following are the systems that is capable of accepting alarms from a Cisco IOS Firewall IDS. Choose all that apply.

A. HP Openview
B. Cisco Director
C. Cisco Host sensor
D. Syslog server
E. Netview for AIX
F. DHCP server

Answer: B, D

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 127
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:
4) 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).
5) Drop the packet - The Cisco IOS firewall can dynamically create an access list that allows the system to drop the incoming packet.
6) 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 128
By default, where does the IOS Firewall IDS engine send alarms to?

A. CBAC
B. Director platform
C. CSACS
D. DMZ
E. syslog server

Answer: E

Explanation:
If an IDS info or attack signature is configured to generate an alarm, if no notification method is specified with the ip audit notify command, by default the IDS engine will send it to the syslog server.

QUESTION 129
What is the IOS Firewall command to send IDS alarms to a syslog server?

A. ip audit notify syslog
B. ip audit notify log
C. ip audit notify logging
D. ip audit specify logging
E. ip audit specify syslog
F. ip audit specify log

Answer: B

Explanation:
The IOS Firewall IDS engine can send alarms to a Director platform, or a syslog server. Use the command ip audit notify log to make the IDS engine send alarms to a syslog server. (You must also define the syslog server with the logging x.x.x.x command).

QUESTION 130
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 131
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 132
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 B, MD5. (The default IKE hash algorithm used is SHA-1).

QUESTION 133
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)#).

QUESTION 134
Which of the following are encryption algorithms? Select all that apply.

A. MD5
B. AES
C. SHA-1
D. DES
E. IKE
F. IPSEC

Answer: B, D

Explanation:
IKE and IPSEC are suites of protocols. MD5 and SHA-1 are hash protocols. DES, 3DES, and AES are encryption protocols.

QUESTION 135
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

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 136
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 137
Which of the following can ESP IPSEC transforms provide? Select all that apply.

A. authentication
B. key generation
C. split tunneling
D. encryption

Answer: A, D

Explanation:
AH is not needed in transforms to provide authentication, as ESP can provide encryption and authentication. Use this configuration if you are having conflictions with AH and NAT.

QUESTION 138
What are the protocol numbers 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 139
Johnat Certkiller Inc. just finished configuring multiple transform sets. Where does he have to specify the transform sets?

A. router interface
B. crypto map entry
C. ACL
D. ISAKMP policy

Answer: B

Explanation:
Crypto map set transform-setcommand :
Specifies 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 (Ciscopress) page 217

QUESTION 140
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
RedundancyYou 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.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_user_guide_chapter09186a00801aed88.html

---

QUESTION 141
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:
cryptokey zeroize rsa
To delete all of your router's RSA keys, use the crypto key zeroizersa global configuration command.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_summary_chapter09186a00800eea

---

QUESTION 142
Certkiller .com, a fast food company, has recently expanded and assumed the responsibility for three additional brands of fast food. Due to this expansion the computer systems have been upgraded and sensitive data will now be transmitted between the offices. Tess, the network administrator of the Certkiller .com, has decided to implement a secure IPSec connection between the two offices. The Certkiller 1 router has been completely configured. The Certkiller 2 router has been configured but is missing the IKE parameters.

IKE is enabled. Configure the following IKE parameters on the Certkiller 2 router:
1. The policy priority should be set to 200.
2. The peer authentication method should be pre-shared keys.
1. The encryption algorithm should be 3-des.
2. DH group 2 should be used.
3. The hash algorithm should be md5.
4. The pre-shared key should be specified as "fastfood".
5. The tunnel should be terminated on the serial interface.
6. All other IKE parameters are set as default.
7. You will not be able to initiate traffic to bring up the tunnel.
The routers have been configured with the following specifications:
1. The routers are named Certkiller 1 and Certkiller 2.
2. The secret password on the Certkiller 2 router is " Certkiller "
3. The IP addresses are shown.
LAB A
Name : Certkiller 2
E0/0 : 10.0.12.3/24
S0/0 : 172.18.12.2/24
Secret Password: Certkiller
LAB B
Name: Certkiller 1
E0/0: 10.0.30.3/24
S0/0: 172.18.37.2/24
Click on the picture of the host connected to a router by a serial console cable.

Answer:
Certkiller 2(config)# crypto isakmp enable
Certkiller 2(config)# crypto isakmp policy 200
Certkiller 2(config-isakmp)# encryption 3des
Certkiller 2(config-isakmp)# hash md5
Certkiller 2(config-isakmp)# authentication pre-share
Certkiller 2(config-isakmp)# group 2
Certkiller 2(config)# crypto isakmp key fastfood address 172.18.37.2
Reference:
Configuring Internet Key Exchange Security Protocol
Alternative #1
1. The policy priority should be set to 130.
LAB A
Name : Certkiller 2
E0/0 : 10.0.30.3/24
S0/0 : 172.18.1.1/24
Secret Password: Certkiller
LAB B
Name: Certkiller 1
E0/0: 10.0.11.3/24
S0/0: 172.18.2.1/24

QUESTION 143

Jason is the security administrator at Certkiller 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

setsecurity-association level per-host

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_chapter09186a00800 87228.h

QUESTION 144

John the security Administrator at Certkiller 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 (Ciscopress) page 525

QUESTION 145

Johnand Kathy are working together at Certkiller Inc. to find the more secure approach for pre-shared keys between peers.Which one of these answers is correct?

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.

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 keys to share between different pairs of peers.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_user_guide_chapter09186a0080106f69.html

---

QUESTION 146
Jason the security administrator at Certkiller Inc. is not very good with crypto ACLs. He asked the security team what the two functions that crypto ACLs performs on outbound traffic. (Choose two)

A. Selects outbound traffic that should be protected by IPSec.
B. Bypasses outbound traffic that should be protected by IPSec.
C. Select inbound traffic that should be protected by IPSec.
D. Sends outbound traffic that should 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: A E
Crypto Access Lists
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.
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/univercd/cc/td/doc/product/iaabu/pix/pix_v52/ipsec/ipsec.htm#25257

QUESTION 147
Kathy and John the security administrators are working on solving a few problems. Finding out which three statements about ESP are true will help them solve the problems they have. (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 (Ciscopress) page 529

QUESTION 148
ESP is the main topic for the day at Certkiller Inc. Which statement best describes ESP header?

A. It is inserted before an encapsulated IP header in tunnel mode.
B. It is inserted before an encapsulated IP header in transport mode.
C. It is inserted after the IP header and before the upper layer protocol header in tunnel mode.
D. It is inserted after the IP header and after the upper layer protocol header in transport mode.

Answer: A

Explanation:
Transport mode:BEFORE APPLYING ESP
--------------------------- IPv4 |orig IP hdr | | | |(any options)| TCP | Data | --------------------------- AFTER APPLYING ESP
-- IPv4 |orig IP hdr | ESP | | | ESP | ESP| |(any options)| Hdr | TCP | Data
| Trailer |Auth| -- |<----- encrypted ---->| |<------ authenticated
----->|Tunnel mode: ------------ IPv4 | new IP hdr* | | orig IP hdr* | | |
ESP | ESP| |(any options)| ESP | (any options) |TCP|Data|Trailer|Auth|
------------ |<--------- encrypted ---------->| |<----------- authenticated
---------->|
Note:
In Tunnel Mode ESP, the original IP datagram is placed in the encrypted portion of the ESP and that entire ESP frame is placed within a datagram having unencrypted IP headers. The information in the unencrypted IP headers is used to route the secure datagram from origin to destination. An unencrypted IP Routing Header might be included between the IP Header and the ESP.
This mode allows a network device, such as a router, to act as an IPSec proxy. That is, the router performs encryption on behalf of the hosts. The source's router encrypts packets and forwards them along the IPSec tunnel. The destination's router decrypts the original IP datagram and forwards it on to the destination system. The major advantage of tunnel mode is that the end systems do not need to be modified to enjoy the benefits of

the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints. As defined by the IETF, IPSec transport mode can only be used when both the source and the destination systems understand IPSec. In most cases, you deploy IPSec with tunnel mode. Doing so allows you to implement IPSec in the network architecture without modifying the operating system or any applications on your PCs, servers, and hosts.

In Transport Mode ESP, the ESP header is inserted into the IP datagram immediately prior to the transport-layer protocol header (such as TCP, UDP, or ICMP). In this mode, bandwidth is conserved because there are no encrypted IP headers or IP options.

Only the IP payload is encrypted, and the original IP headers are left intact. This mode has the advantage of adding only a few bytes to each packet. It also allows devices on the public network to see the final source and destination of the packet. This capability allows you to enable special processing (for example, quality of service) in the intermediate network based on the information on the IP header. However, the Layer 4 header will be encrypted, limiting the examination of the packet. Unfortunately, by passing the IP header in the clear, transport mode allows an attacker to perform some traffic analysis. For example, an attacker could see when one CEO sent a lot of packets to another CEO. However, the attacker would only know that IP packets were Reference: http://www.cisco.com/warp/public/707/16.html

---

QUESTION 149
Jason and Kathy the security administrators are making a game for the security to play. They want the team to match the assigned default with the IKE policy parameter.

Answer:

Explanation:
IKE Policy Parameters: Default Value
1. Message encryption algorithm 56-bit DES-CBC
2. ISAKMP established SAs lifetime 86,400 seconds (one day)
3. Key Exchange parameters 768-bit Diffie-Hellman
4. Peer authentication method RSA signature
5. Message integrity algorithm SHA 1
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_user_guide_chapter09186a0080089916.html

---

QUESTION 150
Greg is working with the security team at Certkiller Inc., to find out which three statements about the crypto ipsec security-association lifetime command are true. (Choose three)

A. Indicates data flow to be protected by IPSec.
B. Selects outbound traffic to be protected by IPSec.
C. Can optionally configure different IPSec SA lifetimes in crypto maps.
D. Configures IKE SA lifetime values.
E. IPSec SA lifetimes are negotiated during IKE Phase 2.
F. Configure global IPSec SA lifetime values used when negotiating IPSec SAs.

Answer: C E F

Explanation:
Use the crypto ipsec security-association lifetimecommand to configure global lifetimes for IPSec SAs.
There are two lifetimes: a "timed' lifetime and a "traffic-volume" lifetime. A security association expires after the first of these lifetimes is reached.
The IPSec SA idle timers are different from the global lifetimes for IPSec SAs. The expiration of the global lifetimes is independent of peer activity. The IPSec SA idle timer allows SAs associated with inactive peers to be deleted before the global lifetime has expired.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541d4.html

---

QUESTION 151
James the security administrator for Certkiller Inc. has to know which has algorithms is used to authenticate packet data before he can go any further. Which algorithm is used to authenticate packet data?

A. MD5 and SHA
B. DES and CBC
C. RSA and SHA
D. DH and RSA

Answer: A

Explanation:
1. MD5 (HMAC variant)-MD5 (Message Digest 5) is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing.
2. SHA (HMAC variant)-SHA (Secure Hash Algorithm) is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_user_guide_chapter09186a0080089917.html

---

QUESTION 152
Which of the following ESP modes is used when the final destination of compiled data is a VPN gateway?

A. transparent mode
B. tunnel mode
C. encrypted mode
D. secure mode
E. encryption mode
F. transport mode

Answer: B

Explanation:
Transport-mode - The transport mode is most commonly used when the destination is the VPN endpoint. The

original IP header is not encrypted when using the transport mode.
Cisco Self-Study CCSP SECUR page 313

QUESTION 153
The Certkiller trainee technician wants to know what services are common in both AH and ESP. what will your reply be?

A. confidentiality, connectionless integrity and anti-replay service
B. data origin authentication, confidentiality and anti-replay service
C. connectionless integrity data origin authentication and anti-replay service
D. confidentiality, connectionless integrity and data origin authentication

Answer: C
Services common to AH & ESP
AH does NOT provide encryption/confidentiality, only ESP
So A, B, D which have confidentiality are wrong, the correct answer is C

QUESTION 154
Which of the following protocols enables Cisco IOS Cryptosystem to securely exchange encryption keys for IPSEC?

A. DH
B. DES
C. ESP
D. Digital Signature Standard
E. None of the above

Answer: A

QUESTION 155
Providing end-to-end protection of message between two hosts is possible when which of the following ESP modes are used?

A. transport mode
B. encrypted mode
C. transparent mode
D. ESP mode
E. tunnel mode

Answer: A
http://www.cisco.com/warp/public/707/24.html

QUESTION 156
Which of the following factors determine an IPSEC policy?

A. to gather piece data you will need in later step to minimize mis-configuration

B. to establish IKE policy
C. to ensure the network work without encryption
D. to ensure ACL are compatible with IKE

Answer: B
Cisco Self-Study CCSP SECUR page 314
The IPSEC policies are often referred to as the IKE phase 2 policies...

QUESTION 157
Which of the following factors determine an IPSEC policy?

A. to gather piece data you will need in later step to minimize mis-configuration
B. to ensure the network work without encryption
C. to establish IKE policy
D. to ensure ACL are compatible with IKE
E. none of the above

Answer: C
Cisco Self-Study CCSP SECUR page 314
The IPSEC policies are often referred to as the IKE phase 2 policies...

QUESTION 158
Which of the following is a prerequisite for the Cisco VPN Client to begin IKE phase one communications?

A. interesting traffic
B. bypass mode traffic
C. IPSec traffic
D. Cisco Secure ACS authentication

Answer: A

QUESTION 159
Which of the following represents two common HMAC algorithms used in Cisco IOS? (Select two.)

A. HMAC-SHA-1
B. HMAC-DH-2
C. HMAC-DH-5
D. HMAC-MD5
E. HMAC-DES
F. HMAC-IKE

Answer: A, D

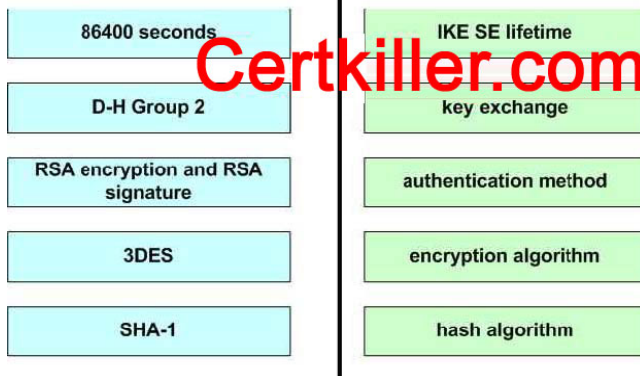Explanation: HMAC algorithms are SHA-1 & MD5

QUESTION 160
In the following diagram match the protection level with the corresponding IKE policy parameter.

Select from these		place here		authentication method
86400 seconds		place here		hash algorithm
D-H Group 2		place here		IKE SE lifetime
RSA encryption and RSA signature		place here		encryption algorithm
3DES		place here		key exchange
SHA-1				

Answer:

Select from these		IKE SE lifetime
86400 seconds		key exchange
D-H Group 2		authentication method
RSA encryption and RSA signature		encryption algorithm
3DES		hash algorithm
SHA-1		

Explanation:

QUESTION 161
What is the router IOS command to clear all IPSEC SA's?

A. clear crypto ipsec sa
B. clear crypto ipsec sa all
C. clear crypto sa
D. clear crypto ipsec sa *

Answer: C

Explanation:
Clear all IPSEC Security Associations on a router with the clear crypto sa command.

QUESTION 162
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 163
Jason the security manager at Certkiller 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 (Ciscopress) page 221

QUESTION 164
The Certkiller 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
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122sup/122sems/semsvol1/emfcpad.htm

QUESTION 165
The Certkiller 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-IKMP_SA__AUTH: Can accept Quick Mode exchange form % 15i if SA is authenticated!
B. %CRYPTO-6-IKMP_SA_NOT__OFFERED: Remote peer % 15i responded with attribute [chars] not offered or changed
C. %CRYPTO-6-IKMP_SA__NOT_AUTH: Cannot accept Quick Mode exchange from % 15i if SA is not authenticated!
D. %CRYPTO-6-IKMP_SA__OFFERED: Remote peer % 15i responded with attribute [chars] offered and changed

Answer: B

QUESTION 166
John the security administrator at Certkiller Inc. wants to know which three steps configure RSA keys. (Choose three)

A. Configure a security algorithm.
B. Configure the routers hostname and domain name.
C. Manage RSA keys.
D. Configure a hash algorithm.
E. Configure encryption.
F. Verify key configuration.

Answer: A BE
RSA-encrypted nonces - Public key cryptography requires that each party generate a pseudorandom number (a nonce) and encrypt it in the other party's RSA public key. Authentication occurs when each party decrypts the other party's nonce with a local private key and then uses the decrypted nonce to compute a keyed hash.
Reference:Managing Cisco Network Security (Ciscopress) page 539

QUESTION 167
Why is it important to give detail particular attention when entering peer RSA public keys?

A. Public keys are used to create the private keys.
B. Changes are complex to make after the keys are entered.
C. Change cannot be made after the keys are entered.
D. Mistakes made when entering the keys will cause them not to work.

Answer: D
Securing Cisco IOS Student Guide 1.1, Page 9-106

QUESTION 168
What are the available authentication options when configuring an IKE SA? Select all that apply.

A. pre-shared keys

B. SHA-1
C. RSA signatures
D. RSA encrypted nonces
E. MD5

Answer: A, C, D

Explanation:
IKE SA peer authentication can be configured in 1 of 3 ways: pre-shared keys, RSA Signatures, or RSA encrypted nonces. Pre-shared keys are used on small networks where entering the key at each peer doesn't encounter scalability issues. On larger networks where scalability is an issue, you can use RSA signatures (the default for IKE policy configuration), which use a Certificate Authority (CA) to allow peer authentication. You can also use RSA encrypted nonces which allows scalability without being forced to use a CA (public keys must still be exchanged).

QUESTION 169
Which of the following crypto map configuration commands are needed when manually entering keys instead of using IKE? Select all that apply.

A. set session-key inbound ah
B. set manual-key inbound ah
C. set session-key outbound esp
D. set manual-key outbound esp

Answer: A, C

Explanation:
If you don't use IKE and instead enter the keys manually, you must enter four keys at each peer in crypto map configuration. One key is for inbound AH, one for inbound ESP, one for outbound AH, and one for outbound ESP. The inbound key of one peer must match the outbound key of the other peer.

QUESTION 170
Which of the following Cisco IOS Firewall router commands will generate separate key pairs for RSA signatures and RSA encrypted nonces?

A. crypto rsa generate special-keys
B. crypto rsa generate association-keys
C. crypto key generate rsa double-keys
D. crypto key generate rsa usage-keys

Answer: D

Explanation:
When generating RSA keys, you can generate one pair (crypto key generate rsa) or two pairs (crypto key generate rsa usage-keys). If you generate one pair, it will be used for both RSA signatures, and RSA encrypted nonces. If you generate two pairs, each will have its own key pair.

QUESTION 171
What is the maximum key size you can generate when using RSA Encrypted Nonces as your IKE
authentication method?

A. 256 bit
B. 768 bit
C. 2048 bit
D. 1024 bit

Answer: C

Explanation:
When generating keys for IKE RSA Encrypted Nonces, you must specify key lengths at a minimum of 360 bits
and a maximum of 2048 bits.

QUESTION 172
George is the administrator at Certkiller Inc. working on acquiring a position in the security department.
He is studying the OSI layer model and is trying to find out which OSI layer does IPSecprovide security
services?

A. session
B. transport
C. network
D. presentation
E. application

Answer: C

Explanation:
IPSec uses a type of encryption known as packet encryption. It is referred to as packet encryption because it
takes place at the network layer, or layer 3 in the OSI reference model. Because this encryption takes place
above the data link layer (layer 2), communication takes place in the form of distinct packets or datagrams,
depending on which protocol controls the session (TCP or UDP). Packet encryption is often called end-to-end
encryption because the encryption process takes place only at the source and destination endpoints
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2133/products_user_guide_chapter09186a00800e9586.ht
ml

QUESTION 173
Kathy is in charge of configuring a Cisco router for IKE using RSA signatures, before she initiates the crypto
key generate rsa command, what should Kathy do?

A. Kathy should generate general purpose keys.
B. Kathy should save the command in the router configuration before she initiates the crypto key generate rsa
command.

C. Kathy should save the keys in a private configuration in NVRAM.
D. Kathy should configure a hostname and IP domain name for your router.

Answer: D
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_summary_chapter09186a00800eea

QUESTION 174
Kathy is the administrator and is working on certificates as part of her daily duties. She needs to know what defines the standard certificate format.

A. CEP
B. CRLv2
C. ISAKMP
D. X.509v3

Answer: D

Explanation:
CA supports the following standards:
1. X.509v3 certificates
2. Public-Key Cryptography Standard #7 (PKCS #7)-A standard from RSA Data Security, Inc. used to encrypt and sign certificate enrollment messages.
3. Public-Key Cryptography Standard #10 (PKCS #10)-A standard syntax from RSA Data Security, Inc. for certificate requests.
4. RSA Keys-RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA keys come in pairs: one public key and one private key.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800899

QUESTION 175
The security team at Certkiller 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
showcrypto ca certificates
To view information about your certificate, the CA's certificate, and any RA certificates, use the show crypto ca certificates EXEC command.

QUESTION 176
Johnthe manager of the I.T. Department at Certkiller Inc. wants to know, what is the purpose of the ip host global configuration command.

A. Associates an IP address.
B. Removes name-to-address mapping.
C. Binds eight addresses to a hostname.
D. Defines a static host name-to-address mapping in the host cache.

Answer: D

Explanation:
To define a static host name-to-address mapping in the host cache, use the ip host command in global configuration mode. To remove the host name-to-address mapping, use the no form of this command.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipras_r/ip1_i1g.htm#1081846

QUESTION 177
Paul the security administrator at Certkiller Inc. must choose three major tasks that must be completed in order to support CA for Cisco routers in a site-to-site configuration. (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:
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 (Ciscopress) page 646

QUESTION 178
Which of the following statements best describes a digital certificate?

A. It is assigned by CA
B. It is a public key infrastructure symmetrical key
C. It is used by IPSEC to encrypt a client session
D. It is a CA's encryption policy

Answer: A
Cisco Self-Study CCSP SECUR page 344
Both routers exchange digital certificates that have been signed by CA

QUESTION 179
The newly appointed Certkiller 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
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

---

QUESTION 180
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).

QUESTION 181
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:
Monitor the communication between a router and a Certificate Authority (CA) server with the debug crypto pki
messages command.

QUESTION 182
What directory do you place the three Cisco VPN client files (oem.ini, vpnclient.ini, .pcf) into?

A. setup.exe
B. syscon.exe
C. startup.exe
D. vpnclient.exe

Answer: A

Explanation:
The Cisco VPN software client supports the pre-configuration of VPN connections by placing three files (oem.ini, vpnclient.ini, .pcf) into the same directory as the VPN client setup.exe.

QUESTION 183
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

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 184
What Cisco VPN software client file has all the parameters of a VPN connection?

A. .pst
B. .pgs
C. .pcf
D. .pdn

Answer: C

Explanation:
A Profile Configuration File (.pcf) has all the parameters for a vpn connection. Multiple connections can be created and you can configure parameters such as Microsoft logon credentials, NT domain, Diffie-Hellman group, etc.

QUESTION 185
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 186
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.

QUESTION 187
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 Cisco EzVPN: 800, 900, and 1700 series routers, PIX 501 firewall, the 3002 Hardware Client, and the VPN software client.

QUESTION 188
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

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 189
Which of the following is NOT supported by Cisco EzVPN?

A. SHA-1
B. MD5
C. ESP
D. AH

Answer: D

Explanation:
Authentication Header is not a supported IPSEC authentication protocol on Cisco EzVPN.

QUESTION 190
What are the two components of Cisco Easy VPN (EzVPN)?

A. External
B. Server
C. Remote
D. Master

Answer: B, C

Explanation:
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.

QUESTION 191
John the security administrator is working on Cisco Easy VPN. His job today is to know what two IPSec attributes that are not supported by Cisco Easy VPN. (Choose two)

A. Tunnel mode
B. Manual keys

C. DH 2
D. RSA digital signatures
E. Pre-shared keys
F. PFS

Answer: B F

Explanation:
Table1 NonSupported 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 192

You are the administrator of Certkiller 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"?

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

Answer: B
Enabling IKE Dead Peer Detection
To enable a Cisco IOS VPN gateway (instead of the client) to send IKE DPD messages, perform the following steps
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087d1e.html#1051234

QUESTION 193

Johnthe security administrator at Certkiller 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#69962

QUESTION 194
James the 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#1051234

QUESTION 195
Which of the following are the main components of the Easy VPN feature. (Choose two.)

A. VPN CA
B. VPN Redirector
C. VPN Server

D. VPN Remote
E. VPN Access
F. VPN Tacacs+ Server

Answer: C, D
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. This cost-effective solution is ideal for remote offices with little IT support or for large customer premises equipment (CPE) deployments where it is impractical to individually configure multiple remote devices. This feature makes VPN configuration as easy as entering a password, which minimizes local IT support, increases productivity, and lowers costs.
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.
Cisco Self-Study CCSP SECUR page 363

QUESTION 196
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.

QUESTION 197
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
Table1 NonSupported 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 198
You are the administrator in charge of the Management Center for VPN routers and are having problems communicating with other VPN routers. Which protocol does the Management Center for VPN Routers use to communicate with VPN routers?

A. SNMP
B. HTTPS
C. HTTP
D. IPSec
E. SSH
F. AES

Answer: E

Explanation:
Prerequisites for Working with Router MC
Following are some prerequisites for working with Router MC:
SSH must be enabled on your devices if you want to import or deploy to live
devices.
Reference:UsingManagement Centerfor VPN Routers 1.2

QUESTION 199
Which of the following represents the predefined policy inManagement Center for VPN?

A. 3DES, SHA pre-shared key, Diffie Hellman Group 2, life-time 86400 sec
B. 3DES, MD5 pre-shared key, Diffie Hellman Group 2, life time 86400 sec

C. 3DES, SHA dynamic pre-share key, Diffie-Hellman Group 2, life-time 86400 sec
D. DES, SHA, pre-shared key, Diffie-Hellman Group 1, life time 43200 sec

Answer: C
Router MC provides various predefined policies for your convenience, including
a predefined IKE policy. If it meets your requirements, you can use the predefined
policy instead of having to create your own IKE policy.
The predefined IKE policy has the following parameters:
Encryption algorithm-3DES
NoteBefore using the default IKE policy, make sure that your routers support
3DES. If not, you can change the encryption algorithm to DES by editing
the default policy on the Global level.
Hash algorithm-SHA
Modulus Group-2
Default lifetime-86400 seconds
Authentication method-auto-generated preshared keys.

QUESTION 200
What role does the re-import function of management center for VPN router fulfill?

A. re-import device configuration from different routers
B. delete and import another copy of router configuration
C. re-import router configure that changed the command line
D. re-attempt import of router after a failed initial import

Answer: B

QUESTION 201
Which of the following are possible state activities inManagement Center for VPN? Choose three.

A. editable
B. submitted
C. edited
D. authored
E. approved
F. logged

Answer: A, B, E
Cisco Self-Study CCSP SECUR page 392~393
Editable, Approved, and Submitted status

QUESTION 202
The Certkiller trainee technician wants to know what the predefined policy in theManagement Center
for VPN Routers is. What will your reply be?

A. 3DES, SHA, pre-shared key, Diffie-Helman group #2 (1024 bit), lifetime 86400

B. 3DES, Md5, CA enrollment, Diffie-Helman group #5 (2048 bit), lifetime 86400
C. DES, SHA, pre-shared key, Diffie-Helman group #1 (786 bit), lifetime 43200
D. DES, SHA, dynamic pre-shared key, Diffie-Helman goup #2 (1024 bit), lifetime 86400
E. 3DES, SHA, CA enrollment, Diffie-Helman gourp #2 (1024 bit), lifetime 86400

Answer: D
Not all countries support the use of the 3DES encryption, so even if 3DES is the default cisco suggest changing this in the global level if your equipment doesn't support it.

New Topic: Topic 11, Mixed Questions (4 questions)

QUESTION 203
You are creating more than one crypto map for a given interface using the sequence number of each map entry to rank the map entries. What does the lower number indicate?

A. lower priority
B. higher priority
C. number of interfaces
D. number of map entries

Answer: B

QUESTION 204
If no valid authentication entry exists in the authentication proxy, how does the proxy respond to the HTTP connection request?

A. prompting the user for a username
B. prompting the user for a password
C. prompting the user for a username and password
D. sending an alert to the Cisco Secure ACS server

Answer: C

QUESTION 205
Which three methods can be used to import devices into theManagement Center for VPN routers? Select three.

A. import directly from multiple devices
B. import from configuration files
C. multiple device import from XLS file
D. import directly from single device
E. multiple device import from CSV file
F. import from resource manager essentials

Answer: B, D, E

QUESTION 206
What happens in the aggressive mode of the CBAC on the Cisco IOS firewall?

A. CBAC deletes all half-open sessions.
B. CBAC re-initiates half-open sessions.
C. CBAC completes all half-open sessions, making them fully open sessions.
D. CBAC deletes half-open sessions as required to accommodate new connection requests.

Answer: D