Exam : 642-825

Title : Implementing Secure Converged Wide Area Networks

Ver : 10-02-07

QUESTION 1:
A few small Certkiller locations use HFC cable to connect to the Certkiller WAN. Which HFC cable network statement is true about the downstream data channel to the customer and the upstream data channel to the service provider?

A. The upstream data path is assigned a channel in a higher frequency range than the downstream path has.
B. The downstream data path is assigned a 30 MHz channel and the upstream data path is assigned a 1 MHz channel.
C. The downstream data path is assigned a fixed bandwidth channel and the upstream data path uses a variable bandwidth channel.
D. Both upstream and downstream data paths are assigned in 6 MHz channels.
E. None of the above.

Answer: D

Explanation:
Hybrid fiber-coaxial (HFC): A mixed optical-coaxial network in which optical fiber replaces some or all of the traditional trunk portion of the cable network.
The HFC architecture is the evolution of an initial cable system and signifies a network that incorporates both optical fiber along with coaxial cable to create a broadband network. By upgrading a cable plant to an HFC architecture, you can deploy a data network over an HFC system to offer high-speed Internet services and you can serve more subscribers. The cable network is segmented into smaller service areas in which fewer amplifiers are cascaded after each optical node-typically five or fewer. The tree-and-branch network architecture for HFC can be a fiber backbone, cable area network, superdistribution, fiber to the feeder, or a ring.
Downstream: An RF signal transmission (TV channels, data) from source (headend) to the destination (subscribers). Downstream is also called a forward path.
Upstream: An RF signal transmission opposite to downstream-from subscribers to the headend. Upstream is also called a return or reverse path.
Delivering services over a cable network requires different RF frequencies-the outgoing frequencies are in the 50-to-860 MHz range, the incoming are in the 5-to-42 MHz range. To deliver data services over a cable network TV channels which usually operate at 6 MHz range for the downstream, and 6 MHz or less (for asymmetric cable connections) for upstream traffic from the corresponding frequency range are usually used.

QUESTION 2:
Many small Certkiller branch offices use broadband cable for data connection access. Which three modulation signaling standards are used in broadband cable technology? (Select three)

A. S-Video
B. NTSC
C. SECAM

D. PAL
E. FEC
F. FDM
G. MLP

Answer: B, C, D

Explanation:
Broadband: Data transmission where multiple pieces of data are sent simultaneously to increase the effective rate of transmission. In cable systems, the term broadband refers to the frequency-division multiplexing (FDM) of many signals in a wide radio frequency (RF) bandwidth over an HFC network, and the capability to handle vast amounts of information.
NTSC is a North American TV technical standard for analog TV systems. The standard was created in 1941 and is named after the National Television System Committee formed in 1940. The standard uses a 6-MHz modulated signal. PAL is a color encoding system used in broadcast television systems in most of Europe, Asia, Africa, Australia, Brazil, and Argentina, and uses a 6-MHz, 7-MHz, or 8-MHz modulated signal. The color difference signals an alternate phase at the horizontal line rate. SECAM is an analog color TV system used in France and certain Eastern European countries that uses an 8-MHz modulated signal.

QUESTION 3:
Some of the smaller Certkiller locations use HFC cable to connect to the Certkiller WAN. Which two statements are true about broadband cable (HFC) systems? (Select two)

A. Cable modems operate at Layers 1, 2, and 3 of the OSI model.
B. Cable modems operate at Layers 1 and 2 of the OSI model.
C. A function of the cable modem termination system is to convert the digital data stream from the end user host into a modulated RF signal for transmission onto the cable system.
D. Cable modems only operate at Layer 1 of the OSI model.
E. A function of the cable modem termination system (CMTS) is to convert the modulated signal from the cable modem into a digital signal.

Answer: B, E

Explanation:
Hybrid fiber-coaxial (HFC): A mixed optical-coaxial network in which optical fiber replaces some or all of the traditional trunk portion of the cable network.
The HFC architecture is the evolution of an initial cable system and signifies a network that incorporates both optical fiber along with coaxial cable to create a broadband network. By upgrading a cable plant to an HFC architecture, you can deploy a data network over an HFC system to offer high-speed Internet services and you can serve more subscribers. The cable network is segmented into smaller service areas in which fewer amplifiers are cascaded after each optical node-typically five or fewer. The

tree-and-branch network architecture for HFC can be a fiber backbone, cable area network, superdistribution, fiber to the feeder, or a ring.

QUESTION 4:
A Certkiller remote user is getting Internet access from the local cable provider. When an individual is connected to the Internet by way of a CATV cable service, what kind of traffic is considered upstream traffic?

A. Traffic going from the user's home traveling to the headend.
B. Broadcast traffic, including the cable TV signals.
C. Traffic between the headend and the TV signal.
D. Traffic between the headend and the supplier antenna.
E. Traffic from outside the local cable segment serving the user's home.
F. All of the above can be considered upstream

Answer: A

Explanation:
In the CATV space, the downstream channels in a cable plant (cable head-end to subscribers) is a point-to-multipoint channel. This does have very similar characteristics to transmitting over an Ethernet segment where one transmitter is being listened to by many receivers. The major difference is that base-band modulation has been replaced by a more densely modulated RF carrier with very sophisticated adaptive signal processing and forward error correction (FEC).
In the upstream direction (subscriber cable modems transmitting towards the head-end) the environment is many transmitters and one receiver. This introduces the need for precise scheduling of packet transmissions to achieve high utilization and precise power control so as to not overdrive the receiver or other amplifier electronics in the cable system. Since the upstream direction is like a single receiver with many antennas, the channels are much more susceptible to interfering noise products. In the cable industry, we generally call this ingress noise. As ingress noise is an inherent part of CATV plants, the observable impact is an unfortunate rise in the average noise floor in the upstream channel. To overcome this noise jungle, upstream modulation is not as dense as in the downstream and we have to use more effective FEC as used in the downstream.
Reference: http://www.cisco.com/warp/public/759/ipj_1-3/ipj_1-3_catv.html

---

QUESTION 5:
A new cable modem was shipped to the home of a Certkiller user, where it is being installed for the first time. When a DOCSIS 1.1 compliant cable modem first initializes, (boots up) what does it do?

A. Establishes IP connectivity (DHCP).
B. Determines the time of day.
C. Requests a DOCSIS configuration file from a TFTP server.
D. Scan for a downstream channel and the establishment of timing synchronization with the CMTS.

E. None of the above.

Answer: D

Explanation:
According to the DOCSIS (Data-over-Cable Service Interface Specifications) when you first power up a cable modem it starts scanning (starting at a low frequency) for a cable signal. When it 'hears' a cable modem stream it listens for a broadcast (from the service provider) which contains information (ie. frequency) needed to talk back with the head end. It then 'talks back' and if it communicates the right authentication information, it is allowed to proceed.
References: Page 225 of the CCNP Self-Study BCRAN (642-821) ISBN: 1-58720-084-8
http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b57f.htm

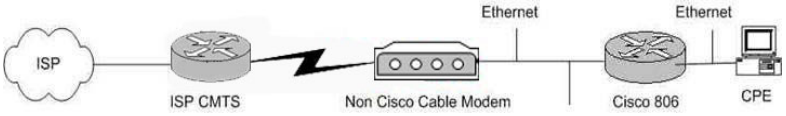
---

QUESTION 6:
You are building a small network at your home and you intend on connecting your cable modem to a Cisco router. Which router interface would you connect the modem to?

A. Synchronous serial
B. Asynchronous serial
C. Ethernet
D. auxiliary
E. BRI

Answer: C

Explanation:
In certain environments where a non Cisco Cable Modem (CM) is used, and the CM is only capable of bridging, a Cisco router such as the Cisco 806 can be connected to the Cable Modem via the Ethernet interface. The routing can then be performed by the Cisco router behind the Cable Modem and the Client PC or Customer Premises Equipment (CPE) will be connected to the Cisco router. Network Address Translation (NAT) can then be configured on the Cisco router.
When the Cisco router is connected behind the Cable Modem the first problem that might be encountered is not obtaining an IP address dynamically on the Cisco router's Ethernet interface. Most Internet Service Providers (ISPs) allow only one host or PC behind the Cable Modem. Some ISPs assign an IP address to the PC based on the host name. Therefore, if you have a Cisco router behind the Cable Modem, then the host name for the router configured using the hostname command should be the same host name given by the ISP.
Example:



QUESTION 7:
When a cable modem is being provisioned to operate with a host system for Internet services, which two options must occur before Layer 1 and 2 connectivity can occur? (Choose two)

A. The cable modem must request an IP address and core configuration information from a Dynamic Host Configuration Protocol (DHCP) server.
B. The cable modem powering up must scan and lock on the RF data channel in the downstream path.
C. The modem must request a DOCSIS configuration file from a TFTP server.
D. The cable modem must register with the CMTS.
E. The modem must read specific maintenance messages in the downstream path.

Answer: B, E

Explanation:
According to the DOCSIS (Data-over-Cable Service Interface Specifications) when you first power up a cable modem it starts scanning (starting at a low frequency) for a cable signal. When it 'hears' a cable modem stream it listens for a broadcast (from the service provider) which contains information (ie. frequency) needed to talk back with the head end. It then 'talks back' and if it communicates the right authentication information, it is allowed to proceed. Once these steps are completed, layers 1 and 2 will be operational.

QUESTION 8:
How is cable broadband technology able to transmit downstream and upstream data while at the same time delivering television content?

A. The cable operator uses the VHF hyperband to transmit and receive data signals.
B. The cable operator assigns any available spectrum to data, depending on how its own television spectrum is being used.
C. The cable operator uses specific bandwidths for data signals specified by DOCSIS.
D. The cable operator places its data signals into clean areas where there is no interference from noise or other signals.

Answer: C

Explanation:
Developed by CableLabs and approved by the ITU in March 1998, Data Over Cable Service Interface Specification (DOCSIS) defines interface standards for cable modems and supporting equipment. In a cable TV system, signals from the various channels are each given a 6-MHz slice of the cable's available bandwidth and then sent down the cable to your house. In some systems, coaxial cable is the only medium used for distributing signals.

When a cable company offers Internet access over the cable, Internet information can use the same cables because the cable modem system puts downstream data -- data sent from the Internet to an individual computer -- into a 6-MHz channel. On the cable, the data looks just like a TV channel. So Internet downstream data takes up the same amount of cable space as any single channel of programming. Upstream data -- information sent from an individual back to the Internet -- requires even less of the cable's bandwidth, just 2 MHz, since the assumption is that most people download far more information than they upload.

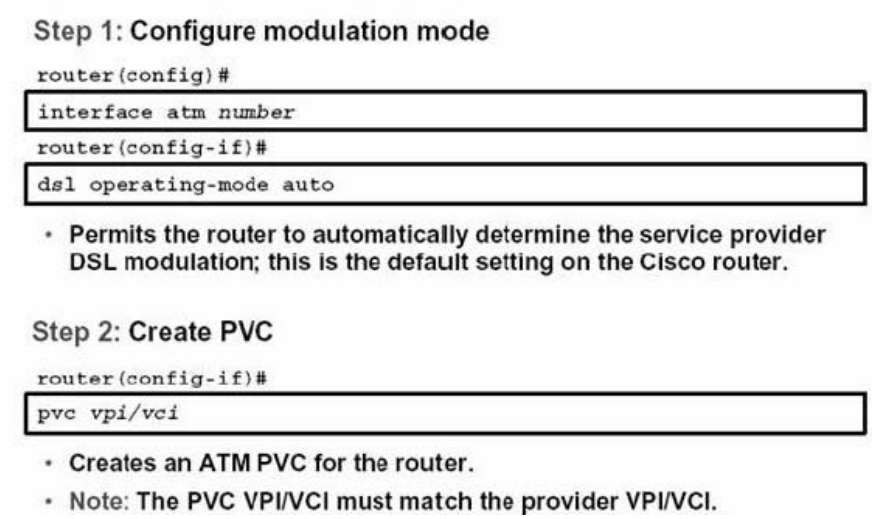
QUESTION 9:
Certkiller operates a DSL network. What does the "dsl operating-mode auto" command configure on a Cisco router?

A. It configures a Cisco router to automatically detect the proper modulation method to use when connecting an ATM interface.
B. It configures a Cisco router to automatically detect the proper DSL type (ADSL, IDSL, HDSL, VDSL) to use when connecting an ATM interface.
C. It configures a Cisco router to automatically detect the proper encapsulation method to use when connecting an ATM interface.
D. It configures a Cisco router to automatically detect the proper authentication method to use when connecting an ATM interface.
E. None of the above

Answer: A

Explanation:
dsloperating-mode auto interface configuration command to specify that the router automatically detect the DSL modulation that the service provider is using and set the DSL modulation to match. An incompatible DSL modulation configuration can result in failure to establish a DSL connection to the DSLAM of the service provider

Example:



QUESTION 10:
Certkiller is a DSL service provider using providing xDSL to its customers. Which statement about xDSL implementations is true?

A. All xDSL standards operate in lower frequencies than the POTS system and can therefore coexist on the same media.
B. Other than providing higher data rates, HDSL is identical to ADSL.
C. The ADSL standard operates in higher frequencies than the POTS system and can therefore coexist on the same media.
D. The HDSL standard operates in higher frequencies than the POTS system and can therefore coexist on the same media.
E. All xDSL standards operate in higher frequencies than the POTS system and therefore can coexist on the same media.
F. None of the above.

Answer: C

Explanation:
DSL is not a complete end-to-end solution, but rather a physical layer transmission technology similar to dial, cable, or wireless. DSL connections are deployed in the "last mile" of a local telephone network-the local loop. The connection is set up between a pair of modems on either end of a copper wire extending between the customer premises equipment (CPE) and the DSL access multiplexer (DSLAM). A DSLAM is the device located at the central office (CO) of the provider and concentrates connections from multiple DSL subscribers.
The term xDSL covers a number of DSL variations, such as ADSL, high-data-rate DSL (HDSL), Rate Adaptive DSL (RADSL), symmetric DSL (SDSL), ISDN DSL (IDSL), and very-high-data-rate DSL (VDSL). DSL types not using the voice frequencies band allow DSL lines to carry both data and voice signals simultaneously (for example, ADSL and VDSL), while other DSL types occupying the complete frequency range can carry

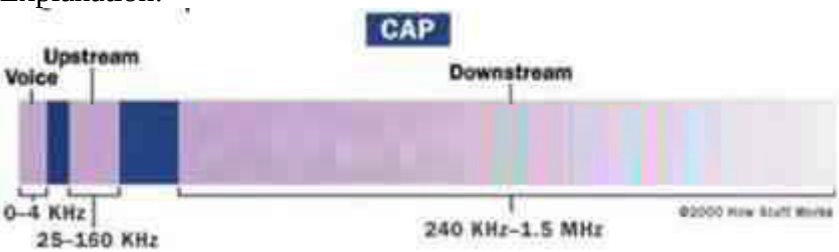
data only (for example, SDSL and IDSL). Data service provided by a DSL connection is always-on. The data rate that DSL service can provide depends upon the distance between the subscriber and the CO. The smaller the distance, the higher data rate can be achieved. If close enough to a CO offering DSL service, the subscriber might be able to receive data at rates of up to 6.1 Mbps out of a theoretical 8.448 Mbps maximum.

QUESTION 11:
Which proprietary DSL encapsulation type has the potential of dividing telephone lines into three widely separated, distinct channels for the sake of minimizing interference between voice, upstream and downstream data flows?

A. G.Lite
B. CAP
C. DMT
D. Half-rate DMT

Answer: B

Explanation:



CAP operates by dividing the signals on the telephone line into three distinct bands: Voice conversations are carried in the 0 to 4 KHz (kilohertz) band, as they are in all POTS circuits. The upstream channel (from the user back to the server) is carried in a band between 25 and 160 KHz. The downstream channel (from the server to the user) begins at 240 KHz and goes up to a point that varies depending on a number of conditions (line length, line noise, number of users in a particular telephone company switch) but has a maximum of about 1.5 MHz (megahertz). This system, with the three channels widely separated, minimizes the possibility of interference between the channels on one line, or between the signals on different lines.
References:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8) Page 248 & 249
http://www.esi-websolutions.com/technology_ADSL.htm

QUESTION 12:
Over which of the following DSL services is the foundation that Cisco's Long Reach Ethernet (LRE) is based on?

A. ADSL
B. HDSL
C. IDSL

D. VDSL
E. E. None of the above

Answer: D

Explanation:
Cisco Long Range Ethernet (LRE) solution leverages Very High Data Rate Digital Subscriber Line (VDSL) technology to dramatically extend Ethernet services over existing Category 1/2/3 twisted pair wiring at speeds from 5 to 15 Mbps (full duplex) and distances up to 5,000 feet. The Cisco LRE technology delivers broadband service on the same lines as Plain Old Telephone Service (POTS), digital telephone, and ISDN traffic. In addition, Cisco LRE supports modes compatible with Asymmetric Digital Subscriber Line (ADSL) technologies, allowing service providers to provision LRE to buildings where broadband services already exist
Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8) Page 251

QUESTION 13:
Which ADSL modulation type:
1. is prominent in residential applications
2. has 120 subchannels
3. doesn't need a splitter
4. has a 1.5 Mbps maximum downstream speed?

A. CAP
B. DMT
C. G.Lite
D. PPPoA
E. PPPoE

Answer: C

Explanation:
ITU GLITE (ITU G.992.2) describes splitterless Asymmetric Digital Subscriber Line (ADSL) Transceivers on a metallic twisted pair that allows high-speed data transmission between the Central Office (ATU-C) and the customer end remote terminal (ATU-R). G.LITE can provide ADSL transmission simultaneously on the same pair with voice (band) service, ADSL transmission simultaneously on the same pair with ISDN services (G.961 Appendix I or II); or ADSL transmission on the same pair with voice band transmission and with TCM-ISDN (G.961 Appendix III) in an adjacent pair.G.992.2 supports a maximum 1.536 Mbps downstream and 512 kbps upstream net data rate. G.LITE uses discrete Multitone (DMT) line code. DMT is based in the use of the IFFT to generate a set of sub-channels, and transmit information in each sub-channel independently. Figure 1 shows the G.LITE spectrum with indication of the POTS, upstream pilot tone, downstream pilot tone, subcarrier spacing, and number of subcarriers

for the upstream and downstream direction. Dividing the available bandwidth into a set of independent, orthogonal subchannels are the key to DMT performance. By measuring the SNR of each subchannel and then assigning a number of bits based on its quality, DMT transmits data on subcarriers with good SNRs and avoids regions of the frequency spectrum that are too noisy or severely attenuated. The underlying modulation technique is based on quadrature amplitude modulation (QAM). Each subchannel is 4.3125 kHz wide and is capable of carrying up to 15 bits. The downstream is up to 552 kHz, offering 122 subchannels, and the upstream from 26 to 138 kHz, offering 25 upstream subchannels.
Reference: http://www.vocal.com/data_sheets/full/glite.pdf

QUESTION 14:
Certain physical factors are capable of severely limiting the maximum speed available on a DSL connection. Which of the following describe the factors that are capable of it? (Choose all that apply)

A. Number of telephones attached to the local loop.
B. Gauge of wire used on the local loop.
C. Distance between the CPE and the DSLAM.
D. Bridge taps in the local loop.
E. Loading coils in the subscriber's line.

Answer: B, C

Explanation:
DSL is a highly distance-sensitive technology. As the distance from the CO increases, the signal quality and connection speeds decrease. ADSL service is limited to a maximum distance of 18,000 feet (5460 m) between the DSL CPE and the DSLAM, although many ADSL providers place an even lower limit on the distance to ensure quality. The 18,000-foot distance limitation for DSL is not a limitation for voice telephone calls, but for data transmission. The telco uses small amplifiers, called loading coils, to boost voice signals. Loading coils have a nasty tendency to disrupt DSL data signals. This means that if there are loading coils in the loop between the CPE and CO, you probably are not within an area that can receive DSL service.
Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 247

QUESTION 15:
A local Internet Service Provider is going to start offering ADSL with 640 kbps upload speed and 4Mbps download speeds. They have retained you to help in their advertisement campaign to help them find their target market. What groups of users should you target your marketing efforts to? (Choose two)

A. Central data processing facilities receiving simultaneous uploads of data from remote offices.

B. Support organizations providing ftp services for software distribution and documentation.
C. Small home offices requiring 24 hour connection to the Internet for email and web communication.
D. Web services companies providing dynamic web content serving, including video-on-demand.

Answer: A, C

Explanation:
Based on the expanding number of options currently and coming soon for the broadband market, competition for home and remote user dollars has reached a frenzied state. The deployment of broadband and similar technologies has involved quite a large amount of trial and error. The competition has seen the emergence of two primary services for widespread deployment. These are Cable and DSL.
Loosely defined, DSL is a technology that exploits unused frequencies on copper telephone lines to transmit traffic, typically at multimegabit speeds. DSL uses existing telephone wiring, without requiring any additional cabling resources. It has the capability to allow voice and high-speed data to be sent simultaneously over the same copper pair. The service is always available, so the user does not have to dial in or wait for call setup.
DSL technologies can be broken down into two fundamental classifications: asymmetric (ADSL) and symmetric (SDSL). As the name implies, ADSL uses higher downstream rates and lower upstream rates. In contrast, SDSL uses the same downstream and upstream rates. ADSL is the most commonly deployed DSL technology, and is the primary focus of the DSL portion of the CCNP Remote Access Exam.
Incorrect Answers:
B: In order to maximize the use of an FTP server, you would want a greater upload speed, since the majority of users will be downloading files from the FTP server.
D: Again, we would want to ensure that the upload speed was as large as possible, due to the fact that the majority of the bandwidth will be consumed as uploads to the end users.
Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 245 to 247

QUESTION 16:
What's true about the G.Lite (G.922) ADSL ITU standard?

A. It offers equal bandwidth for upstream and downstream data traffic.
B. It has limited operating range of less than 4,500 feet.
C. It was developed specifically for the consumer market segment requiring higher download speeds.
D. Signals cannot be carried on the same wire as POTS signals.
E. All of the above

Answer: C

Explanation:
G.Lite is the informal name for what is now a standard way to install Asymmetric Digital Subscriber Line (ADSL) service. Also known as Universal ADSL, G.Lite makes it possible to have Internet connections to home and business computers at up to 1.5 Mbps (millions of bits per second) over regular phone lines. Even at the lowest downstream rate generally offered of 384 Kbps (thousands of bits per second), G.Lite is about seven times faster than regular phone service with a V.90 modem and three times faster than an Integrated Services Digital Network (ISDN) connection. Upstream speeds from the computer are at up to 128 Kbps. (Theoretical speeds for ADSL are much higher, but the data rates given here are what is realistically expected.)
With G.Lite, your computer's analog-to-digital modem is replaced with an "ADSL modem." and the transmission from the phone company is digital rather than the analog tranmission of "plain old telephone service." G.Lite is also known as "splitterless DSL" because, unlike other DSL technologies, it does not require that a technician come to install a splitter, a device that separates voice from data signals, at the home or business (sometimes referred to as "the truck roll").
The G.Lite standard is officially known as G.992.2.
DSL technologies can be broken down into two fundamental classifications: asymmetric (ADSL) and symmetric (SDSL). As the name implies, ADSL uses higher downstream rates and lower upstream rates. In contrast, SDSL uses the same downstream and upstream rates. ADSL is the most commonly deployed DSL technology, and is the primary focus of the DSL portion of the CCNP Remote Access Exam.
DSL is a highly distance-sensitive technology. As the distance from the CO increases, the signal quality and connection speeds decrease. ADSL service is limited to a maximum distance of 18,000 feet (5460 m) between the DSL CPE and the DSLAM, although many ADSL providers place an even lower limit on the distance to ensure quality.
References:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8) Page 245 to 247
http://whatis.techtarget.com/definition/0,,sid9_gci212198,00.html

---

QUESTION 17:
When designing an ADSL network; if you want minimal local loop impairments, what should be the maximum distance of your lines?

A. 1000 feet (0.3 km)
B. 4000 feet (1,5 km)
C. 12,000 feet (3.65 km)
D. 18,000 feet (5,5 km)
E. 28,000 feet (8.52 km)

Answer: D

Explanation:
DSL is a highly distance-sensitive technology. As the distance from the CO increases, the signal quality and connection speeds decrease. ADSL service is limited to a maximum

distance of 18,000 feet (5460 m) between the DSL CPE and the DSLAM, although many ADSL providers place an even lower limit on the distance to ensure quality. The 18,000-foot distance limitation for DSL is not a limitation for voice telephone calls, but for data transmission. The telco uses small amplifiers, called loading coils, to boost voice signals. Loading coils have a nasty tendency to disrupt DSL data signals. This means that if there are loading coils in the loop between the CPE and CO, you probably are not within an area that can receive DSL service.
Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 247

QUESTION 18:
A new ADSL line is being installed in the home office of the Certkiller administrator. What best describes ADSL?

A. Equal upload and downloads speeds.
B. Slow upload, fast download speeds.
C. An ISDN line with no D channel.
D. Used as a T-1 replacement.

Answer: B

Explanation:
The variation called ADSL (Asymmetric Digital Subscriber Line) is the form of DSL that will become most familiar to home and small business users. ADSL is called "asymmetric" because most of its two-way or duplex bandwidth is devoted to the downstream direction, sending data to the user. Only a small portion of bandwidth is available for upstream or user-interaction messages. However, most Internet and especially graphics- or multi-media intensive Web data need lots of downstream bandwidth, but user requests and responses are small and require little upstream bandwidth. Using ADSL, up to 6.1 megabits per second of data can be sent downstream and up to 640 Kbps upstream. The high downstream bandwidth means that your telephone line will be able to bring motion video, audio, and 3-D images to your computer or hooked-in TV set. In addition, a small portion of the downstream bandwidth can be devoted to voice rather data, and you can hold phone conversations without requiring a separate line.
Reference:
http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213915,00.html

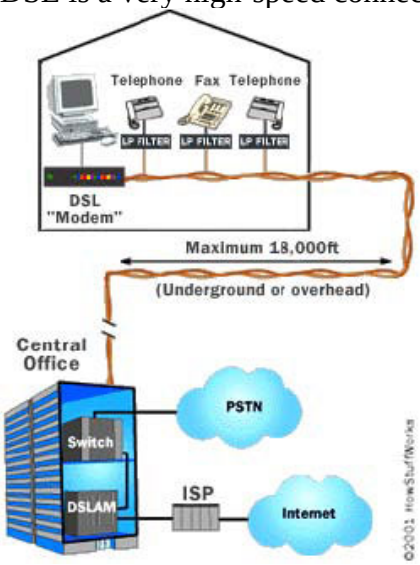
---

QUESTION 19:
Which two statements are true about DSL? (Choose two)

A. SDSL and POTS can work together.
B. It uses the unused bandwidth of your existing phone line.
C. Bandwidth is shared among users in the same geographical area.
D. It has a maximum distance limitation of 18,000 feet from the CO.

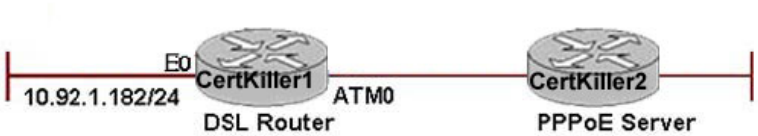
Answer: B, D

Explanation:
DSL is a very high-speed connection that uses the same wires as a regular telephone line.



Precisely how much benefit you see will greatly depend on how far you are from the central office of the company providing the ADSL service. ADSL is a distance-sensitive technology: As the connection's length increases, the signal quality decreases and the connection speed goes down. The limit for ADSL service is 18,000 feet (5,460 meters) from the central office, though for speed and quality of service reasons many ADSL providers place a lower limit on the distances for the service. At the extremes of the distance limits, ADSL customers may see speeds far below the promised maximums, while customers nearer the central office have faster connections and may see extremely high speeds in the future. ADSL technology can provide maximum downstream (Internet to customer) speeds of up to 8 megabits per second (Mbps) at a distance of about 6,000 feet (1,820 meters), and upstream speeds of up to 640 kilobits per second (Kbps). In practice, the best speeds widely offered today are 1.5 Mbps downstream, with upstream speeds varying between 64 and 640 Kbps.

QUESTION 20:
Two Certkiller routers are connected as shown below:



Certkiller 1 is configured as shown below:

```
hostname CertKiller1
!
vpdn enable
!
vpdn-group pppoe
 request-dialin
 pretocol ppnoe
!
interface Ethernet0
 ip address 10.92.1.182 255.255.255.0
 ip nat inside
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 bundle-enable
 dsl operating-mode auto
 hold-queue 224 in
 pvc 1/150
 pppoe-client dial-pool-number 1
!
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
!
ip nat inside source list 1 interface Dialer1 overload
ip route 0.0.0.0.0.0.0.0 Dialer1
!
access-list 1 permit 10.92.1.0 0.0.0.255
!
<output omitted>
```

Refer to the exhibit and the partial configuration on the Certkiller router.
The Certkiller DSL Router is connected to a service provider using a PPPoE session over a DSL line. The FTP traffic, generated from inside the network 10.92.1.0/24, fails to reach the PPPoE Server. What should be configured on the DSL Router to fix the problem?

A. The ip mtu command with a bytes argument set greater than 1500 needs to be configured for the Dialer1 interface.
B. The ip mtu command with a bytes argument set lower than 1500 needs to be configured for the ATM0 interface.
C. The ip mtu command with a bytes argument set greater than 1500 needs to be configured for the ATM0 interface.
D. The ip mtu command with a bytes argument set lower than 1500 needs to be configured for the Dialer1 interface.
E. None of the above

Answer: D

Explanation:
The MTU parameter is simply the maximum size of bytes a unit can have on an interface.
If the outgoing packet is larger than the MTU, the IP protocol might need to fragment it.
If a packet larger that the MTU has the "do not fragment" flag set, the packet is dropped.

QUESTION 21:
Part of the configuration of a Certkiller router is shown below:

```
<output omitted>
!
interface Ethernet0
 ip address 10.0.0.1 255.0.0.0
 no ip derected-broadcast
 no ip mroute-cache
!
interface ATM0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 no atm ilmi-keepalive
!
 hold-queue 224 in
!
interface Dialer0
 ip address 172.18.0.1 255.255.0.0
 no ip directed-broadcast
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap callin
 ppp chap hostname username
 ppp chap password password
!
ip classless
!
ip route 0.0.0.0 0.0.0.0 Dialer0
!
dialer-list 1 protocol ip permit
!
end
```

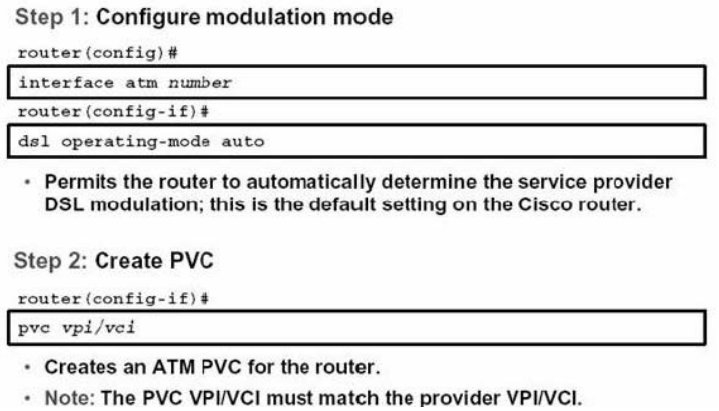
Based on the information above, what is needed to complete the PPPoA configuration on this Certkiller router?

A. The ATM PVC needs to be configured.
B. The VPDN group needs to be created.
C. PPPoE encapsulation needs to be configured on the ATM interface.
D. PAP authentication needs to be configured.
E. A static route to the ISP needs to be configured.
F. None of the above

Answer: A

Explanation:
When you configure PPPoA, a logical interface, known as a virtual access interface, associates each PPP connection with an ATM virtual circuit (VC). You can create this logical interface by configuring an ATM PVC or switched virtual circuit (SVC). This configuration encapsulates each PPP connection in a separate PVC or SVC, allowing each PPP connection to terminate at the router ATM interface as if received from a

typical PPP serial interface.



QUESTION 22:
A small Certkiller office needs to connect their Cisco router to the DSL service provider. Which three configuration steps must be taken to connect a DSL ATM interface to a service provider? (Select three)

A. Configure the ATM PVC.
B. Assign a VPDN group name.
C. Configure PPPoE on the VPDN group.
D. Enable VPDN.
E. Configure the correct PPP encapsulation on the ATM virtual circuit.
F. Configure a dialer interface.

Answer: A, E, F

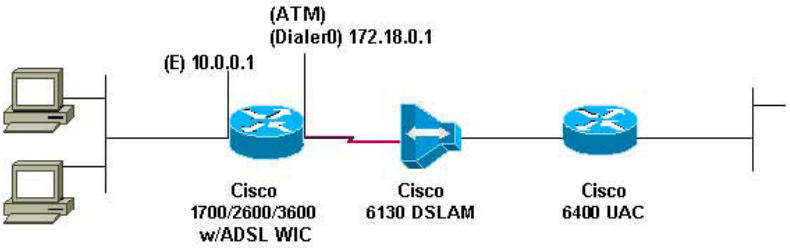
Explanation:
Configuring DSL ATM interface to a Service Provider:
1. dsl operating-mode auto interface configuration command to specify that the router automatically detect the DSL modulation that the service provider is using and set the DSL modulation to match. An incompatible DSL modulation configuration can result in failure to establish a DSL connection to the DSLAM of the service provider.
Router(Config)# interface atm number
Router(Config0f)#dsl operating-mode auto
2. Thepvc interface configuration command to set the virtual path identifier/virtual channel identifier (VPI/VCI) that is used by the DSL service provider, as shown in the table. Settings for the VPI/VCI value on the Cisco router must match the configuration on the DSLAM of the service provider switch configuration. ATM uses the VPI/VCI to identify an ATM VC.
Router(Config-if)#pvc vpi/vci
3. Define the Encapsulation:
Router(Config-atm-vc)# encapsulation aal5mux ppp dialer
4. Associate the interface with the pool
Router#(config-atm-vc)#dialer pool-member number

QUESTION 23:
Router CK1 is configured as shown below:
interface ATM0/0
no ip address
pvc 8/35
encapsulation aaa15mux ppp dialer
dialer pool-member 1
!
interface dialer 0
ip address negotiated
encapsulation ppp
dialer pool 1
no cdp enable
ppp chap hostname Certkiller
ppp chap password Certkiller
Given the above configuration, which statement is true?

A. This device is configured as a PPPoE client.
B. This device is configured as a PPPoA client.
C. This device is configured as RFC 1483/2684 bridge.
D. This device is configured an an aggregation router.

Answer: B

Explanation:
This following is an example of configuring a Cisco router as a PPPoA client. The command "encapsulation aal5muxppp dialer" placed under the ATM interface is the indication that it is using PPPoA.



Cisco ADSL WIC
!version 12.1service timestamps debug datetime msecservice timestamps datetime msec!hostname R1!ip subnet-zero!ip dhcp excluded-address 10.0.0.1!--- the DHCP pool does not lease this address;!--- it is used by interface FastEthernet0!ip dhcp pool poolnamenetwork 10.0.0.0 255.0.0.0 default-router 10.0.0.1!--- default gateway is assigned to local devices!interface FastEthernet0 ip address 10.0.0.1 255.0.0.0 no ip directed-broadcast no ip mroute-cache!interface ATM0no ip addressno ip directed-broadcastno ip mroute-cacheno atm ilmi-keepalive pvc 1/150encapsulation aal5mux ppp dialerdialer pool-member 1! hold-queue 224 in!interface Dialer0ip address 172.18.0.1 255.255.0.0ip nat outsideno ip directed-broadcastencapsulation pppdialer pool 1dialer-group 2ppp pap sent-username username password password!ip

nat inside source list 1 interface Dialer0 overloadip classlessip route 0.0.0.0 0.0.0.0 Dialer0no ip http server!access-list 1 permit 10.0.0.0 0.255.255.255dialer-list 2 protocol ip permit!end
Reference:
http://www.cisco.com/en/US/tech/ CK1 75/ CK1 5/technologies_configuration_example09186a0080093e60.shtml

---

QUESTION 24:
The configuration of the 827 ADSL router depends on tbe encapsulation method used for the ADSL connection. What are the three common encapsulation methods? (Choose three)

A. PPPoE
B. PPPoA
C. HDLC over ATM
D. DOCSIS
E. RFC 1483 Bridged
F. IP over ATM

Answer: A, B, E

Explanation:
Before you can successfully configure your Cisco DSL Router with Asymmetric Digital Subscriber Line (ADSL) service, you need specific information from your Internet Service Provider (ISP). If your ISP is unsure, unable, or unwilling to provide answers to the questions outlined below, you may not be able to correctly configure your Cisco DSL Router.
The most fundamental piece of information you will need is the type of DSL service. The following lists the type of DSL services that are available and can be configured on the Cisco 827 ADSL router:
1. Point-to-Point Protocol over Ethernet (PPPoE)
2. Point-to-Point Protocol over ATM (PPPoA)
3. RFC1483 Bridging
4. RFC1483 Routing

QUESTION 25:
Which two encapsulation methods require that an 827 ADSL router be configured with a PPP username and CHAP password? (Choose two)

A. PPPoE with the 827 configured as a bridge.
B. PPPoE with the 827 configured as the PPPoE client.
C. PPPoA
D. RFC 1483 Bridged with the 827 configured as the PPPoE client.
E. RFC 1482 Bridged with the 827 configured as a bridge.

Answer: B, C

Explanation:
When using the Point to Point Protocol over Ethernet (PPPoE) or the Point to Point Protocol over ATM (PPPoA), you must configure a PPP username and password to match the settings configured from the Internet Service Provider. This is required for both PPPoE and PPPoA in order to overcome some of the security concerns of these two Internet access methods.

QUESTION 26:
ADSL broadband connections using the PPPoE access method typically uses which type of user authentication method?

A. AAA authentication
B. DNIS authentication
C. Caller-ID authentication
D. PPP CHAP authentication
E. IPSec authentication
F. L2TP authentication

Answer: D

Explanation:
Once the DSL device is installed and configured for PPPoE the encapsulation of all traffic with PPPoE/PPP headers is performed. The default authentication mechanism for PPPoE is Password Authentication Protocol (PAP). The user has the option to configure Challenge Handshake Authentication Protocol (CHAP) or MS-CHAP manually. Generally, the CHAP method is preferred and is normally used to overcome the security limitations of PAP.

QUESTION 27:
When comparing the differences between PPPoA and PPPoE, which of the following statements are true?

A. PPPoE does not support session authentication with an aggregation router.
B. PPPaE provides simple bridged connections for a limited number of hosts.
C. PPPoA relies on client software to provide connectivity and authentication.
D. PPPoA is routed end-to-end over ATM from the user's PC to the aggregation router.
E. None of the above

Answer: D

Explanation:

Some key advantages of PPPoE and how they differ from PPPoA include:
* Per session authentication based on Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). This is the greatest advantage of

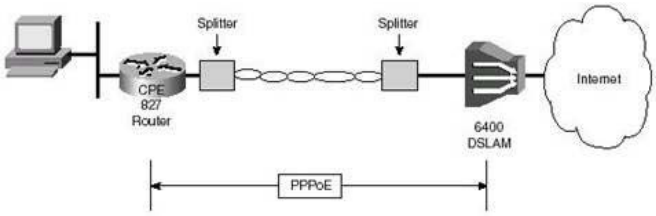
PPPoE as authentication overcomes the security hole in a bridging architecture.
* Per session accounting is possible, which allows the service provider to charge the subscriber based on session time for various services offered. The service provider may also require a minimal access charge.
* PPPoE can be used on existing CPE installations that cannot be upgraded to PPP or that do not have the ability to run PPPoA, extending the PPP session over the bridged Ethernet LAN to the PC.
* PPPoE preserves the point-to-point session used by Internet Service Providers (ISPs) in the current dialup model. PPPoE is the only protocol capable of running point-to-point over Ethernet without requiring an intermediate IP stack.
*
The Network Access Provider (NAP) or Network Service Provider (NSP) can provide secure access to a corporate gateway without managing end-to-end permanent virtual circuits (PVCs) and making use of Layer 3 routing and/or Layer 2 Tunneling Protocol (L2TP) tunnels. This makes the business model of selling wholesale services and virtual private networks (VPNs) scalable.
* PPPoE can provide a host (PC) access to multiple destinations at a given time. There can be multiple PPPoE sessions per PVC.
* The NSP can oversubscribe by deploying idle and session time-outs using an industry standard Remote Authentication Dial-In User Service (RADIUS) server for each subscriber.
* PPP can be used with the service selection gateway (SSG) feature.
Some key disadvantages of PPPoE and how they differ from PPPoA include:
* PPPoE client software must be installed on all hosts (PCs) connected to the Ethernet segment. This means that the access provider must maintain the CPE and the client software on the PC.
* Because PPPoE implementation uses RFC1483 bridging, it is susceptible to broadcast storms and possible denial-of-service attacks.
Reference:
http://www.cisco.com/warp/public/794/pppoe_arch.html

QUESTION 28:
DSL connections commonly use PPP over Ethernet (PPoE). What process does a Certkiller host have to perform to establish a PPoE SESSION_ID?

A. A DHCP request process to request and IP address and session ID.
B. A Discovery process to identify a PPPoE server and request a session ID.
C. A RARP request process to request a MAC address and session ID.
D. A BOOTP process to request a configuration and session ID.
E. None of the above

Answer: B

Explanation:



When a router wants to initiate a PPPoE session, it must first perform Discovery to identify the Ethernet MAC address of the peering device and establish a PPPoE SESSION_ID. Discovery is inherently a client/server relationship. During Discovery, a router discovers the provider DSLAM. Discovery allows the CPE router to discover all available DSLAMs, and then select one. When Discovery completes successfully, both the CPE router and the selected DSLAM have the information they will use to build their point-to-point connection over Ethernet.
Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 253

QUESTION 29:
Many Certkiller remote offices use DSL for their connectivity. Which four features are usually required for an 827 ADSL router to support a home ADSL broadband Internet connection with multiple end-user PCs? (Choose four)

A. IPSec
B. Bridging (IRB or RBE)
C. PPPoE client
D. PAT
E. DHCP server
F. Static default route

Answer: C, D, E, F

Explanation:
In Cisco IOS(r) Software Release 12.1(3)XG, a PPP over Ethernet (PPPoE) client feature was introduced for the Cisco 827 router. This feature allows the PPPoE functionality to be moved to the router. Multiple PCs can be installed behind the Cisco 827. Before their traffic is sent to the PPPoE session, it can be encrypted, filtered, and so forth. Also, Network Address Translation (NAT) can run.
PAT is neededde to be able to translate multiple internal IP addresses into one single IP address. Since the majority of DSL connections provide only IP address, this is necessary.
A DHCP server is normally required, so that IP addresses can be dynamically assigned to the PC's sharing the DSL connection.
Finally, a static default route needs to be configured on the 827 DSL router pointing out the DSL interface, so that all traffic destined for the Internet will be forwarded out to the DSL network.

QUESTION 30:
The following was issued on a Certkiller DSL router:

```
CertKillerADSL#show dsl int atm 0
                ATU-R (DS)                      ATU-C (US)
Modem Status:    Showtime (DMTDSL_SHOWTIME)
DSL Mode:        ITU G.992.1 (G.DMT)
ITU STD NUM:     0x01                            0x01
Vendor ID:       'ALCB'                          'ANDV'
Vendor Specific: 0x0000                          0x0000
Vendor Country:  0x00                            0x00
Capacity Used:    6%                             14%
Noise Margin:    31.0 dB                         27.0 dB
Output Power:    18.0 dBm                        12.0 dBm
<output omitted>

                Interaleave             Fast    Interaleave       Fast
Speed (kbps):          7616                0             896          0
<output omitted>
```

Observe the output from the show dsl int atm 0 command shown above. What does the display of the upstream and downstream speed indicate?

A. Layer 1 connectivity has been established
B. Layer 2 connectivity has been established
C. Layer 1 and 2 connectivity has been established
D. Layer 3 connectivity has been established
E. Layer 2 and 3 connectivity has been established

Answer: C

Explanation:
The output in this example shown above displays the normal operation of a DSL router that is fully functioning. If the modem state changes from "0x8" to "SHOWTIME," it means that the Cisco 827 has successfully trained with the DSLAM. This verifies connectivity at layer 1. Layer 2 connectivity can be verified via the speed of the conections both upstream and downstream. For a complete overview of the ourput from the "show dsl interface atm" command, see the link provided below:
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_chapter09186a008017

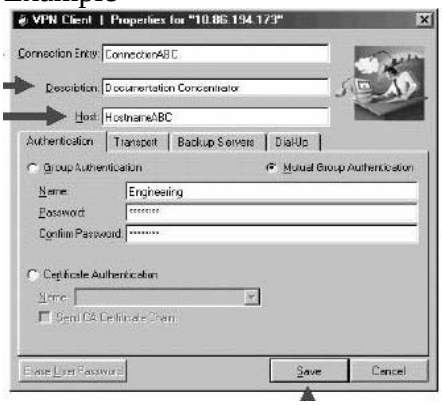
QUESTION 31:
The Cisco VPN client is being installed on a new Certkiller teleworker's laptop. When configuring the Cisco software VPN client on a PC, which values need to be entered to complete the setup when pre-shared key authentication is used?

A. IP address of server, groupname and password, and default gateway
B. IP address of server, groupname and password, default gateway, and DNS servers
C. IP address of server, groupname, and password
D. IP address of server, groupname and password, default gateway, DNS servers, and local IP address

Answer: C

Explanation:

The Cisco virtual private network (VPN) Client for Windows (or VPN Client) is software that runs on a Microsoft Windows-based PC. The VPN Client on a remote PC, communicating with a Cisco Easy VPN Server on an enterprise network or with a service provider, creates a secure connection over the Internet.
Preshared keys-the IPsec group to which the system administrator assigned you. Your group determines how you access and use the remote network. For example, it specifies access hours, number of simultaneous logins, user authentication method, and the IPsec algorithms that your VPN Client uses.
Example



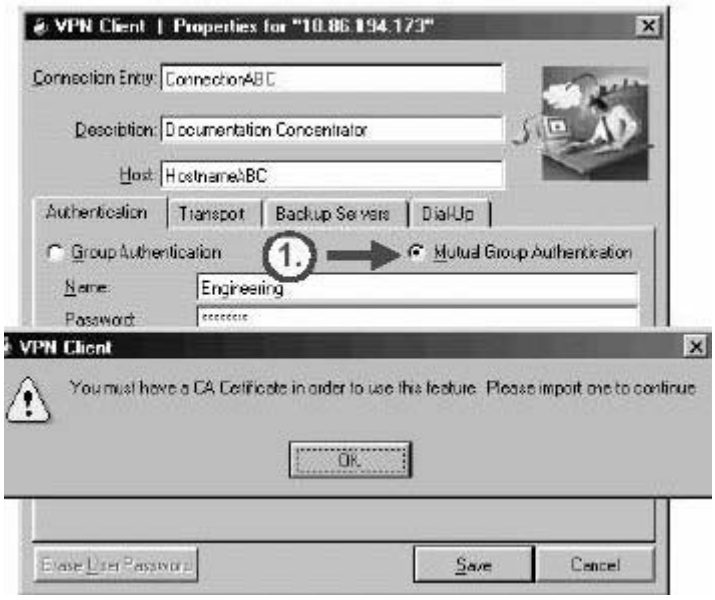
QUESTION 32:
The Cisco VPN client is being installed on a teleworkers laptop. When configuring the Cisco VPN Client, what action is required prior to installing Mutual Group Authentication?

A. The option to "Allow Local LAN Access" must be selected.
B. A group pre-shared secret must be properly configured.
C. A valid root certificate must be installed.
D. Transparent tunneling must be enabled.

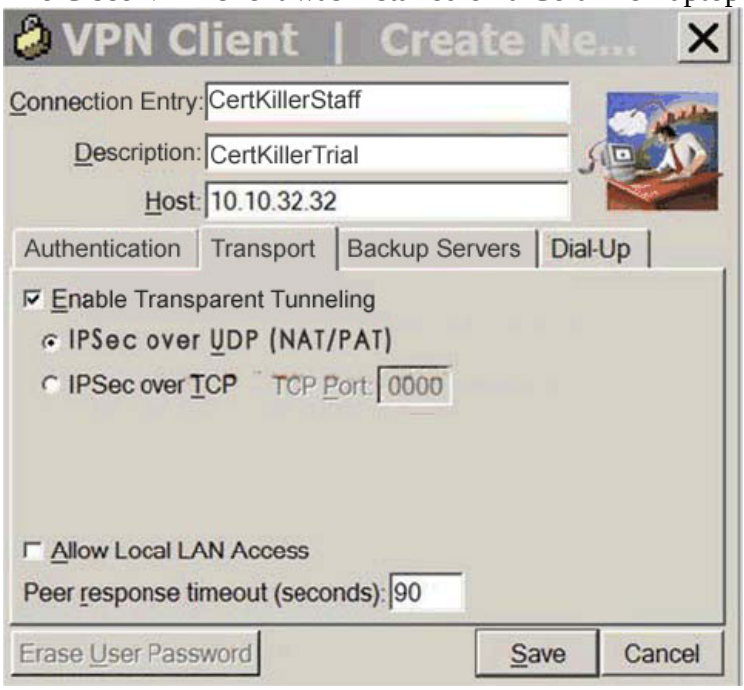
Answer: C

Explanation:
The Cisco virtual private network (VPN) Client for Windows (or VPN Client) is software that runs on a Microsoft Windows-based PC. The VPN Client on a remote PC, communicating with a Cisco Easy VPN Server on an enterprise network or with a service provider, creates a secure connection over the Internet.
Mutual authentication should be used instead of group presharedsecrets, Group presharedsecrets are vulnerable to man-in-the-middle attacks if the attacker knows the group presharedsecret.
To use mutual group authentication, you need a root certificate that is compatible with the central-site VPN installed on your system:
Step 1 Your network administrator can load a root certificate on your system during installation. When you select the Mutual Group Authentication radio button, the VPN Client software verifies whether you have a root certificate installed.
Step 2 If you do not have a root certificate installed, the VPN Client prompts you to

install one. Before you continue, you must import a root certificate. When you have installed a root certificate (if required), follow the steps for group authentication.
Example:



QUESTION 33:
The Cisco VPN client was installed on a Certkiller laptop as shown below:



Based on the diagram shown above, what does the "Allow Local LAN Access" option enable a Cisco software VPN client to do?

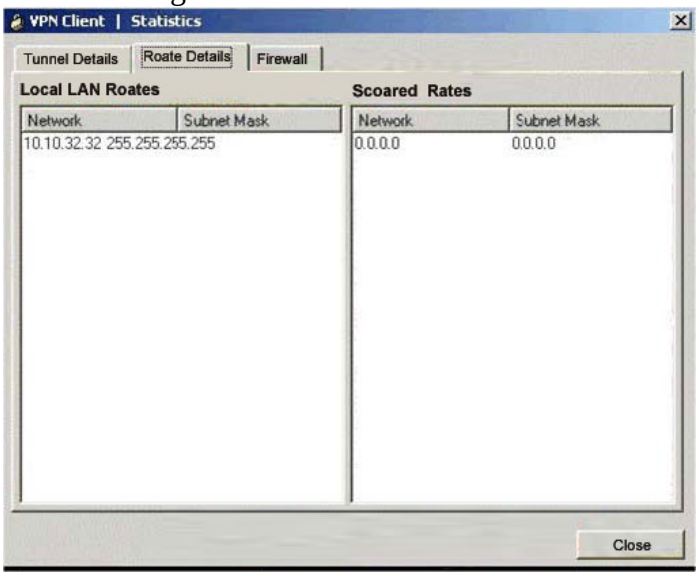
A. It allows local traffic from trusted resources to pass through the VPN connection
B. It allows a user to access the resources on the local LAN when connected through a secure gateway to a central-site VPN device

C. It allows secured remote clients to access local LAN resources through the VPN connection
D. It allows remote connections from trusted clients to access local resources

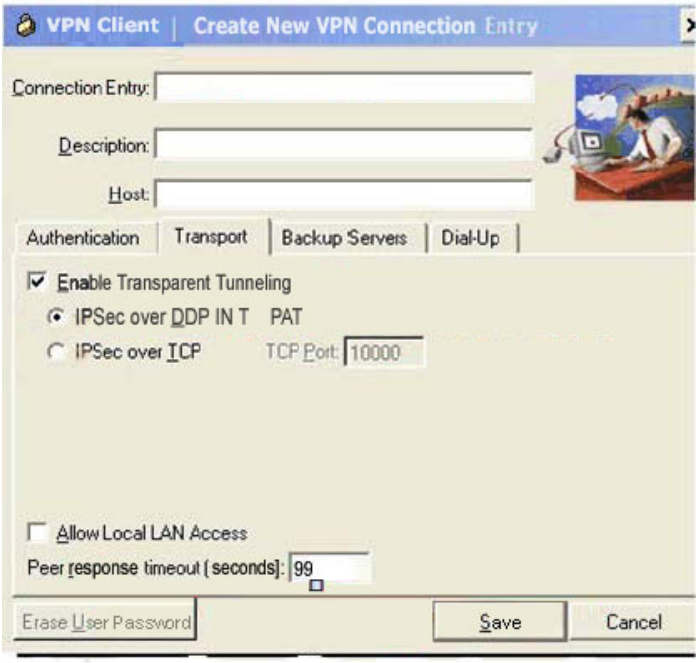
Answer: B

Explanation:
In a multiple-network interface card (NIC) configuration, local LAN access pertains only to network traffic on the interface on which the tunnel was established. The Allow Local LAN Access parameter gives you access to the resources on your local LAN (printer, fax, shared files, or other systems) when you are connected through a secure gateway to a central-site VPN device. When this parameter is enabled and your central site is configured to permit it, you can access local resources while connected. When this parameter is disabled, all traffic from your client system goes through the IPsec connection to the secure gateway. To enable this feature, check the Allow Local LAN Access check box; to disable it, uncheck the check box. If the local LAN that you are using is not secure, you should disable this feature. For example, you would disable this feature when you are using a local LAN in a hotel or airport. A network administrator at the central site configures a list of networks at the client side that you can access. You can access up to 10 networks when this feature is enabled. When the Allow Local LAN Access feature is enabled and you are connected to a central site, all traffic from your system goes through the IPsec tunnel except traffic to the networks excluded from doing so (in the network list). When this feature is enabled and configured on the VPN Client and permitted on the central-site VPN device, you can see a list of the local LANs available by looking at the routing table.

QUESTION 34:
The following VPN Client Statistics exhibit was seen on a Certkiller laptop:



A new VPN Connection Entry was made on this laptop as shown below:



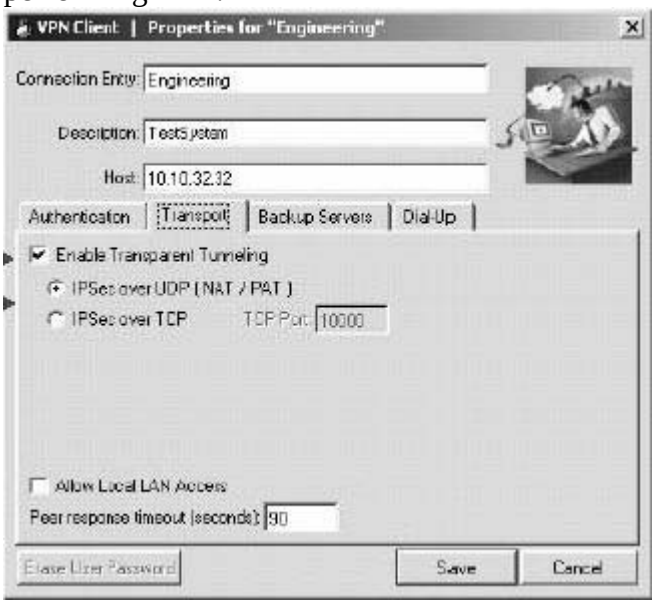
Which two statements are true about the information that is shown above from theCisco VPN client screens on this Certkiller laptop? (Select two)

A. The 10.10.32.32 network entry in the Route Details screen represents the IP address of the server end of the encrypted tunnel.
B. The 10.10.32.32 network entry in the Route Details screen represents an IP address that will be accessed without traversing the VPN.
C. Selecting IPSec over TCP on the connection entry on the right allows Local LAN Routes to be available on the Route Details on the left screen.
D. Selecting Enable Transparent Tunneling on the connection entry on the right allows Local LAN Routes to be available on the Route Details on the left screen.
E. Selecting Allow Local LAN Access on the connection entry on the right allows Local LAN Routes to be available on the Route Details on the left screen.

Answer: B, E

Explanation:
Transparent tunneling allows secure transmission between the VPN Client and a secure gateway through a router serving as a firewall, which may also be performing Network Address Translation (NAT) or Port Address Translation (PAT). Transparent tunneling encapsulates Protocol 50 (Encapsulating Security Payload, or ESP) traffic within UDP packets and can allow both Internet Security Association and Key Management Protocol (ISAKMP) and Protocol 50 to be encapsulated in TCP packets before they are sent through the NAT or PAT devices or firewalls. The most common application for transparent tunneling is behind a home router

performing PAT.



QUESTION 35:
You need to set up the Cisco VPN client software on a new Certkiller laptop. When configuring the Cisco VPN Client with transparent tunneling, what is true about the IPSec over TCP option?

A. The port number is negotiated automatically.
B. Clients will have access to the secured tunnel and local resources.
C. Packets are encapsulated using Protocol 50 (Encapsulating Security Payload, or ESP).
D. The port number must match the configuration on the secure gateway.

Answer: D

Explanation:
To enable IPsec over TCP, click the IPsec over TCP radio button. When using TCP, you must also enter the port number for TCP in the TCP port field. This port number must match the port number configured on the secure gateway. The default port number is

10000.

QUESTION 36:
The Cisco VPN client needs to be installed and configured on a new Certkiller PC. When entering the Group Authentication information while configuring the Cisco VPN Client on a PC, what information is entered in the "Name" field?

A. Login name of the user (such as "joesmith")
B. IPSec group information (such as "Engineering")
C. Host name of the remote VPN device (such as "vpn1.cisco.com")
D. Client name of the device (such as "joesmith-laptop")
E. The group pre-shared secret (such as "ClEiN1iNFTW")
F. None of the above

Answer: B

Explanation:
Group Authentication:
Step 1 Select the Group Authentication radio button.
Step 2 In the Name field, enter the name of the IPsec group to which you belong. This entry is case-sensitive.
Step 3 In the Password field, enter the password (which is also case-sensitive) for your IPsec group. The field displays only asterisks.
Step 4 Verify your password by entering it again in the Confirm Password field.

QUESTION 37:
The following output was seen on a Certkiller DSL router:

```
CertKiller3 # show dsl interface atm 0

                    ATU-R (DS)                      ATU-C(US)
Modem Status:       Showtime (DMTDSL_SHOWTIME)
DSL Mode:           ITU G.992.1 (G.DMT)
ITU STD NUM:        0x01                            0x1
Vendor ID:          'ALCB'                          'GSPN'
Vendor Specific:    0x0000                          0x0002
Vendor Country:     0x00                            0x00
Capacity Used:      97%                             100%
Noise Margin:       5.0 dB                          5.0 dB
Output Power:       9.5 dBm                         12.0 dBm
<output omitted>

                    Interleave      Fast    Interleave      Fast
Speed (kbps):       7616            0       896             0
<output omitted>
```

You work as a network engineer at Certkiller .com. You are troubleshooting a DSL connectivity issue. You have issued the show dsl interface command and received the above output. Given this information, what could be the problem?

A. An incorrect power supply is being used.
B. The service provider is not providing DSL service to this wall jack.
C. Incorrect VPI/VCI values are configured on the router.
D. The service provider is using a DSLAM that does not support the Alcatel DSL chipset.

Answer: C

Explanation:
If you experience trouble with the ADSL connection, make sure to verify the following:
That the ADSL line is connected and is using pins 3 and 4. For more information on the ADSL connection, see the hardware guide for your router.
That the ADSL CD LED is on. If it is not on, the router may not be connected to the digital subscriber line access multiplexer (DSLAM). For more information on the ADSL LEDs, see the hardware installation guide specific to your router.
That you are using the correct Asynchronous Transfer Mode (ATM) variable path indentifier/variable circuit identifier (VPI/VCI).
That the DSLAM supports discrete multi-tone (DMT) Issue 2.
Incorrect Answers:
A: The power outputs shown are normal
B: This is incorrect, due to the operational status of the modem as displayed by the "showtime" keyword.
D: In this example, the Alcatel chipset is configured, with the Globespan chipset configured as the secondary chipset. If this was not supported, the modem status would not read "showtime."

QUESTION 38:
The different Certkiller locations are connected via an MPLS network. Which device is responsible for attaching a VPN label to a packet traversing an MPLS network?

A. The customer (C) router

B. The provider (P) router
C. The customer edge (CE) router
D. The provider edge (PE) router
E. None of the above

Answer: D

Explanation:
MPLS is a switching mechanism that assigns labels (numbers) to packets, then uses those labels to forward packets. The labels are assigned at the edge of the MPLS network, and forwarding inside the MPLS network is done solely based on labels.
You can use an MPLS label stack to tell the egress PE router what to do with the VPN packet. When using the label stack, the ingress PE router labels the incoming IP packet with two labels:
1. The top label in the stack is the Label Distribution Protocol (LDP) label for the egress PE router. This label guarantees that the packet will traverse the MPLS VPN backbone and arrive at the egress PE router.
1. The second label in the stack is assigned by the egress PE router and tells the router how to forward the incoming VPN packet. The second label could point directly toward an outgoing interface, in which case the egress PE router would perform label lookup only on the VPN packet. The second label could also point to a VRF table, in which case the egress PE router would first perform a label lookup to find the target VRF table and then perform an IP lookup within the VRF table.

QUESTION 39:
If a Certkiller Label Switch Router (LSR) is properly configured, which three combinations are possible? (Select three)

A. An IP destination exists in the IP forwarding table. A received labeled packet is dropped because the label is not found in the LFIB table.
B. A received labeled packet is forwarded based on the label. After the label is swapped, the newly labeled packet is sent.
C. There is an MPLS label-switched path toward the destination. A received IP packet is dropped because the destination is not found in the IP forwarding table.
D. A received IP packet is forwarded based on the IP destination address and the packet is sent as an IP packet.
E. A received labeled IP packet is forwarded based upon both the label and the IP address.
F. A received IP packet is forwarded based on the IP destination address and the packet is sent as a labeled packet.
G. None of the above are possible

Answer: B, D, F

Explanation:
LSRs and edge LSRs are usually capable of doing both label switching and IP routing.

Their names are based on their positions in an MPLS domain. Routers that have all interfaces enabled for MPLS are called LSRs because they mostly forward labeled packets. Routers that have some interfaces that are not enabled for MPLS are usually at the edge of an MPLS domain autonomous systems (ASs). These routers also forward packets based on IP destination addresses and label them if the outgoing interface is enabled for MPLS.
For example, an edge LSR receives a packet for destination 10.1.1.1, imposes label 21, and forwards the frame to the LSR in the MPLS backbone. LSR swaps label 21 with label 25 and forwards the frame. The edge LSR removes label 25 and forwards the packet based on IP destination address 10.1.1.1.
LSRs of all types must perform these functions:
1. Exchange routing information (control plane)
2. Exchange labels (control plane)
3. Forward packets (data plane): Frame mode MPLS forwards packets based on the 32-bit label

---

QUESTION 40:
Certkiller uses frame-mode MPLS in a portion of its WAN. Which statement is true about the default operation of frame-mode MPLS?

A. LSRs must wait to get the next-hop label from their downstream neighbors before propagating information.
B. LSRs will only propagate label mappings to their neighbors by request.
C. Labels are sequentially generated for neighbors.
D. Interfaces can share the same labels.
E. None of the above

Answer: D

Explanation:
Label allocation and distribution in a Unicast IP routing network and MPLS functionality, including label allocation and distribution, can be divided into these steps:
Step 1 The routers exchange information using standard or vendor-specific Interior Gateway Protocol (IGP), such as Open Shortest Path First [OSPF], Intermediate System-to-Intermediate System [IS-IS], and Enhanced Interior Gateway Routing Protocol [EIGRP]).
Step 2 Local labels are generated. One locally unique label is assigned to each IP destination found in the main routing table and stored in the Label Information Base (LIB) table.
Step 3 Local labels are propagated to adjacent routers, where these labels might be used as next-hop labels (stored in the Forwarding Information Base [FIB] and Label Forwarding Information Base [LFIB] tables to enable label switching).
Step 4 Every label switch router (LSR) builds its LIB, LFIB, and FIB data structures based on received labels.

QUESTION 41:
Certkiller uses a frame-mode MPLS WAN. Which three statements about frame-mode MPLS are true? (Select three)

A. The MPLS data plane takes care of forwarding based on either destination addresses or labels.
B. MPLS has three distinct components consisting of the data plane, the forwarding plane, and the control plane.
C. Whenever a router receives a packet that should be CEF-switched, but the destination is not in the FIB, the packet is dropped.
D. The CEF FIB table contains information about outgoing interfaces and their corresponding Layer 2 header.
E. The control plane is a simple label-based forwarding engine that is independent of the type of routing protocol or label exchange protocol.
F. To exchange labels, the control plane requires protocols such as Tag Distribution Protocol (TDP) or MPLS Label Distribution Protocol (LDP).
G. None of the above

Answer: A, C, F

Explanation:
Label allocation and distribution in a Unicast IP routing network and MPLS functionality, including label allocation and distribution, can be divided into these steps:
Step 1 The routers exchange information using standard or vendor-specific Interior Gateway Protocol (IGP), such as Open Shortest Path First [OSPF], Intermediate System-to-Intermediate System [IS-IS], and Enhanced Interior Gateway Routing Protocol [EIGRP]).
Step 2 Local labels are generated. One locally unique label is assigned to each IP destination found in the main routing table and stored in the Label Information Base (LIB) table.
Step 3 Local labels are propagated to adjacent routers, where these labels might be used as next-hop labels (stored in the Forwarding Information Base [FIB] and Label Forwarding Information Base [LFIB] tables to enable label switching).
Step 4
Every label switch router (LSR) builds its LIB, LFIB, and FIB data structures based on received labels.
These data structures contain label information:
1. The LIB, in the control plane, is the database used by Label Distribution Protocol (LDP) where an IP prefix is assigned a locally significant label that is mapped to a next-hop label that has been learned from a downstream neighbor.
2. The LFIB, in the data plane, is the database used to forward labeled packets. Local labels, previously advertised to upstream neighbors, are mapped to next-hop labels, previously received from downstream neighbors.
1. The FIB, in the data plane, is the database used to forward unlabeled IP packets. A forwarded packet is labeled if a next-hop label is available for a specific destination IP network. Otherwise, a forwarded packet is not labeled.

QUESTION 42:
You are responsible for managing and maintaining the Certkiller MPLS network.
What is the function of the MPLS data plane?

A. The data plane exchanges Layer 3 routing information using OSPF, EIGRP, IS-IS, and BGP protocols.
B. The data plane exchanges labels using the label exchange protocols TDP, LDP, BGP, and RSVP.
C. The data plane uses the Forwarding Information Base (FIB) to forward packets based on the routing information.
D. The data plane uses Label Forwarding Information Base (LFIB) to forwards packets based on the labels.

Answer: D

Explanation:
The LFIB, in the data plane, is the database used to forward labeled packets. Local labels, previously advertised to upstream neighbors, are mapped to next-hop labels, previously received from downstream neighbors.

QUESTION 43:
While troubleshooting a problem the Certkiller network administrator used a protocol analyzer to capture the contents of an MPLS label. What are the four fields in an MPLS label? (Select four)

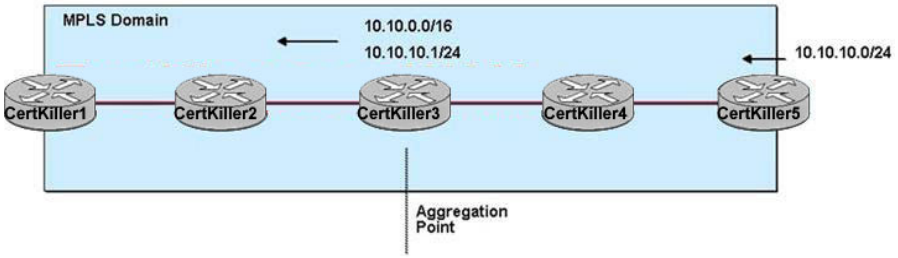
A. TTL
B. Version
C. Label
D. Bottom-of-stack indicator
E. Experimental
F. Protocol

Answer: A, C, D, E

Explanation:
MPLS Label Filed Details:

20-bit label	The actual label. Values 0 to 15 are reserved
3-bit experimental (EXP) field	Undefined in the RFC. Used by Cisco to define a class of service (CoS) (IP precedence)
Bottom-of-stack bit	MPLS allows multiple labels to be inserted. The bottom-of-stack bit determines if this label is the last label in the packet. If this bit is set (1), it indicates that this is the last label
8-bit Time to Live (TTL) field	Has the same purpose as the TTL field in the IP header

QUESTION 44:
The Certkiller WAN is shown in the following exhibit:



All routers participate in the MPLS domain. An IGP propagates the routing information for network 10.10.10.0/24 from Certkiller 5 to Certkiller 1. However, router Certkiller 3 summarizes the routing information to 10.10.0.0/16. How will the routes be propagated through the MPLS domain?

A. None of the networks will be labeled and propagated through the MPLS domain because aggregation breaks the MPLS domain.
B. Certkiller 3 will label the summary route using a pop label. The route will then be propagated through the rest of the MPLS domain. Certkiller 3 will label the 10.10.10.0/24 network and forward to Certkiller 2 where the network will be dropped.
C. Certkiller 3, using LDP, will advertise labels for both networks, and the information will be propagated throughout the MPLS domain.
D. Certkiller 3 will label the 10.10.10.0/24 network using a pop label which will be propagated through the rest of the MPLS domain. Certkiller 3 will label the summary route and forward to Certkiller 2 where the network will be dropped.
E. None of the above.

Answer: B

Explanation:
A label represents a forwarding equivalence class, but it does not represent a particular path through the network. In general, the path through the network continues to be chosen by the existing Layer 3 routing algorithms such as OSPF, Enhanced IGRP, and BGP. That is, at each hop when a label is looked up, the next hop chosen is determined by the dynamic routing algorithm.

QUESTION 45:
Certkiller is an MPLS network provider connecting multiple customer networks. In an MPLS VPN implementation, how are overlapping customer prefixes propagated?

A. A route target is attached to each customer prefix.
B. Because customers have their own interfaces, distributed CEFs keep the forwarding tables separate.
C. Separate BGP sessions are established between each customer edge LSR.
D. A separate instance of the core IGP is used for each customer.

E. Because customers have their own unique LSPs, address space is kept separate.
F. None of the above.

Answer: A

Explanation:
One of the routing options in a simple VPN is to use a static route on the PE and a static default route on the CE. This is an optimal solution for simple spoke VPN sites (sites with only one link into the P-network) that have only one IP subnet per site.
Using static routes also prevents the customer or the service provider from intentionally or accidentally flooding the other with a false and possibly overwhelming amount of routing information and thus strengthens the Service Provider's control over customer routing.
Instead of using static routing you can use an IGP, such as RIP version 2 or OSPF, to advertise customer networks between the PE-routers and the CErouters. This option is normally used when the customer manages the CE routers, when there is more than one IP prefix per customer site, or when the site is multihomed (has more than one link into the P-network or a separate Internet connection).
The IGP metric can be preserved by copying it into the BGP MED attribute (default action) and copying it back from the MED attribute into the IGP metric (configured with metric transparent option of the redistribute command).

QUESTION 46:
The Certkiller network administrator is trying to optimize the convergence time in their MPLS network. Which statement is true about convergence in an MPLS network?

A. MPLS convergence will take place at the same time as the routing protocol convergence.
B. MPLS convergence will take place after the routing protocol convergence.
C. MPLS must be reconfigured after the routing protocol convergence.
D. MPLS convergence will take place before the routing protocol convergence.
E. None of the above.

Answer: B

Explanation:
MPLS is a switching mechanism that assigns labels (numbers) to packets, then uses those labels to forward packets. The labels are assigned at the edge of the MPLS network, and forwarding inside the MPLS network is done solely based on labels. Labels usually correspond to a path to Layer 3 destination addresses, similar to IP destination-based routing. Labels can also correspond to Layer 3 VPN destinations (MPLS VPN) or non-IP parameters, such as a Layer 2 circuit or outgoing interface on the egress router. This includes Cisco Systems solutions for transporting Layer 2 packets over an MPLS backbone, such as Any Transport over MPLS (AToM), quality of service (QoS), or source address. MPLS is designed to support forwarding of protocols other than TCP/IP.

Label switching within the network is performed in the same manner regardless of the Layer 3 protocol. In MPLS labeling in larger networks, only the edge routers perform a routing lookup. All the core routers forward packets based on the labels, which leads to faster forwarding of packets through the service provider network.

QUESTION 47:
Certkiller is an MPLS provider connecting multiple customer VPN's. Which three statements below are correct concerning MPLS-based VPNs? (Select three)

A. A VPN client is required for client-initiated deployments.
B. An MPLS-based VPN is highly scalable because no site-to-site peering is required.
C. Scalability becomes challenging for a very large, fully meshed deployment.
D. Route Targets (RTs) are attributes attached to a VPNv4 BGP route to indicate its VPN membership.
E. A VPN client is not required for users to interact with the network.
F. Authentication is done using a digital certificate or pre-shared key.

Answer: B, D, E

Explanation:
With the introduction of Multiprotocol Label Switching (MPLS), which combines the benefits of Layer 2 switching with Layer 3 routing and switching, it became possible to construct a technology that combines the benefits of an overlay VPN (such as security and isolation among customers) with the benefits of simplified routing that a peer-to-peer VPN implementation brings. The new technology, called MPLS/VPN, results in simpler customer routing and somewhat simpler service provider provisioning, and makes possible a number of topologies that are hard to implement in either the overlay or peer-to-peer VPN models. MPLS also adds the benefits of a connection-oriented approach to the IP routing paradigm, through the establishment of label-switched paths, which are created based on topology information rather than traffic flow.

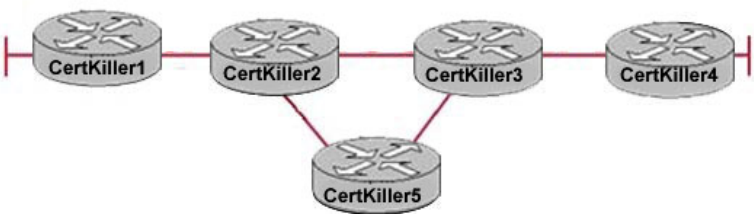
QUESTION 48:
All Certkiller remote locations connect via a fully meshed MPLS WAN. Which three statements regarding MPLS are true? (Select three)

A. Frame-mode MPLS inserts a 32-bit label between the Layer 3 and Layer 4 headers.
B. The control plane is responsible for forwarding packets.
C. The two major components of MPLS include the control plane and the data plane.
D. Cisco Express Forwarding (CEF) must be enabled as a prerequisite to running MPLS on a Cisco router.
E. MPLS is designed for use with frame-based Layer 2 encapsulation protocols such as Frame Relay, but is not supported by ATM because of ATM fixed-length cells.
F. OSPF, EIGRP, IS-IS, RIP, and BGP can be used in the control plane.

Answer: C, D, F

Explanation:
To support multiple protocols, MPLS divides the classic router architecture into two major components:
* Control plane: Control plane takes care of the routing information exchange and the label exchange between adjacent devices.
* Data plane: Data plane takes care of forwarding based on either destination addresses or labels; this is also known as the forwarding plane.
A large number of different routing protocols, such as Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System-to-Intermediate System (IS-IS), Routing Information Protocol (RIP), and BGP, can be used in the control plane. The control plane also requires protocols, such as the label exchange protocols: MPLS Label Distribution Protocol (LDP) or BGP (used by MPLS VPN). Resource Reservation Protocol (RSVP) is used by MPLS Traffic Engineering to reserve resources (bandwidth) in the network. The data plane, however, is a simple label-based forwarding engine that is independent of the type of routing protocol or label exchange protocol. The Label Forwarding Information Base (LFIB) table is used to store the label information that the forwarding engine uses to forward packets. The LFIB table is populated by the label exchange protocol used (LDP, BGP, or RSVP).

QUESTION 49:
A number of Certkiller routers are connected as shown below:



Routers Certkiller 2 and Certkiller 3 have established LDP neighbor sessions. Troubleshooting discovered that labels are being distributed between the two routers but no label swapping information is in the LFIB. What is the most likely cause of this problem?

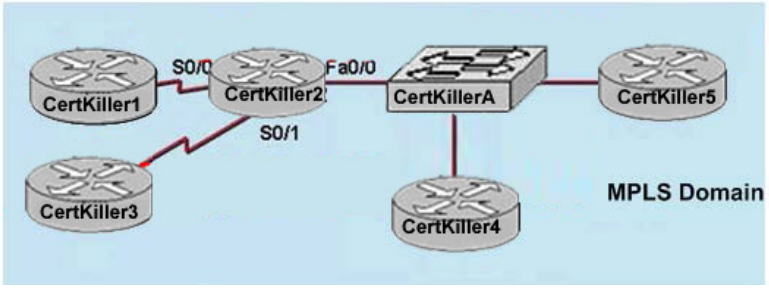
A. IP CEF has not been enabled on both routers Certkiller 2 and Certkiller 3.
B. The IGP is summarizing the address space.
C. LDP is using the loopback address as the LDP ID and the loopback address is not in the routing table.
D. LDP has been enabled on one router and TDP has been enabled on the other.
E. BGP neighbor sessions have not been configured on both routers.
F. None of the above

Answer: A

Explanation:
To configure MPLS, follow these steps:
* Configure CEF: CEF must be running as a prerequisite to running MPLS on a Cisco

router.
Example: ip cef [distributed]
* Configure MPLS on a frame mode interface: All MPLS backbone interfaces should be enabled for MPLS.
Example:
Router(config-if)#mpls ip : Enable switching on Frame mode interface
Router(config-if)#mpls label protocol [tdp | ldp | both] : Starts selected label distribution protocol on the specified interface.
* Configure the maximum transmission unit (MTU) size in label switching: To prevent labeled packets from exceeding the maximum size, you may need to increase the MTU on the MPLS interface.
Example:
Router(config-if)# mpls mtu bytes

QUESTION 50:
The Certkiller WAN is shown below:



Part of the Certkiller 2 router configuration is shown below:

```
hostname CertKiller2
!
ip cef
!
<output omitted>

interface serial0/0
  mpls ip
  mpls label protpcol tdp
!
interface serial0/1
  mpls ip
  mpls label protocol ldp
```

MPLS must be enabled on all routers in the Certkiller MPLS domain that consists of Cisco routers and equipment of other vendors. What MPLS distribution protocol(s) should be used on router R2 FastEthernet interface Fa0/0 so that the Label Information Base (LIB) table is populated across the MPLS domain?

A. Only TDP should be enabled on Fa0/0 interface.

B. MPLS cannot be enabled in a domain consisting of Cisco and non-Cisco devices.
C. Both distribution protocols LDP and TDP should be enabled on the Fa0/0 interface.
D. Only LDP should be enabled on Fa0/0 interface.
E. None of the above

Answer: C

Explanation:
Enable Tag Distribution Protocol (TDP) or Label Distribution Protocol (LDP) on the interface by using either tag switching or label switching. You enable the support for MPLS on a device by using mpls ip global configuration command, although this should be on by default, and then individually on every frame mode interface that participates in MPLS processes.
MPLS support is enabled by default in Cisco routers. MPLS can be disabled using the no mpls ip interface configuration command. You must configure MPLS individually on every frame mode interface that will participate in MPLS using the mpls ip command in interface configuration mode. After enabling MPLS on the interface, you must select the label distribution protocol using the mpls label protocol command in interface configuration mode.
Router(config-if)#mpls label protocol [tdp | ldp | both] : Starts selected label distribution protocol on the specified interface.

QUESTION 51:
A new Certkiller router was configured with the following commands:

```
ip cef
!
interface Serial 3/1
 ip access-group block in
interface Serial 2/1
 mpls ip
!
ip access list block deny tcp any any eq 711
ip access list block permit ip any any
```

The configuration above was found on an Internet Service Provider's (ISP) Multiprotocol Label Switching (MPLS) network. What is its purpose?

A. To prevent customers from running TDP with the ISP routers
B. To prevent customers from running LDP with the ISP routers
C. To prevent other ISPs from running LDP with the ISP routers
D. To prevent man-in-the-middle attacks
E. To use CBAC to shut down Distributed Denial of Service attacks
F. To use IPS to protect against session-replay attacks
G. None of the above

Answer: A

Explanation:

Tag Distribution Protocol (TDP) uses 711 port number and Label Distribution Protocol (LDP) uses 646 port number. In Exhibit deny to port number 711 means deny to TDP.

QUESTION 52:

The following output was displayed on router Certkiller 1:

```
CertKiller1# show mpls forwarding-table detail

Local Outgoing      Prefix            Bytes tag Outgoing      Next Hop
tag   tag or V      or Tunnel Id       witched  interface
26    t  agged      10.253.0.0/16     0         Et4/0/0       172.27.32.4
        MAC/Encaps=0/0, MTU=1504, Tag Stack{}
28    1/33          10.15.0.0/16      0         AT0/0.1       point2point
        MAC/Encaps=4/8, MTU=4470, Tag Stack{1/33(vcd=2)}
        00020900 00002000
29    Pop tag       10.91.0.0/16      0         Hs5/0         point2point
        MAC/Encaps=4/4, MTU=4474, Tag Stack{}
        FF030081
      1/36          10.91.0.0/16      0         AT0/0.1       point2point
        MAC/Encaps=4/8, MTU=4470, Tag Stack{1/36(vcd=3)}
        00030900 00003000
30    32            10.250.0.97/32    0         Et4/0/2       10.92.0.7
        MAC/Encaps=14/18, MTU=1500, Tag Stack{32}
        00E00 8 9E2A0 E E/E/84 28847  0020000
      32            10.259.0.97/32    0         Hs5/0         point2point
        MAC/Encaps=4/8, MTU=4470, Tag Stack{32}
        FF030081 00020000
```

On the basis of the command output shown above, which statement is true?

A. Traffic associated with local label 26 will be forwarded to an interface that is not associated with label switching.
B. Traffic associated with local label 29 will be forwarded to an interface that is not associated with label switching.
C. The value 32 is a local label ID.
D. Traffic associated with local label 30 will have a next hop of 10.250.0.97/32.
E. None of the above.

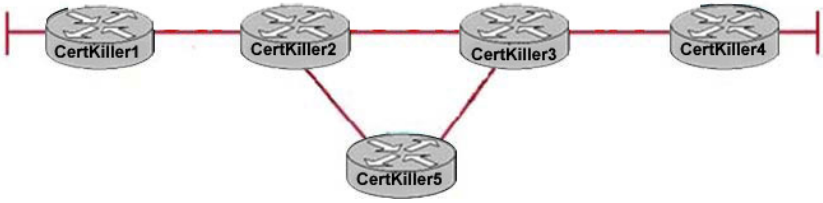
Answer: A

Explanation:
To display the contents of the Multiprotocol Label Switching (MPLS) Label Forwarding Information Base (LFIB), use the show mpls forwarding-table command in privileged EXEC mode.
showmpls forwarding-table [network {mask | length} | labels label [- label] | interface interface | next-hop address | lsp-tunnel [tunnel-id]] [vrf vrf-name] [detail]

show mpls forwarding-table Field Descriptions	
Field	**Description**
Local label	Label assigned by this router.
Outgoing Label or VC **Note** VC is not applicable to the Cisco 10000 series routers.	Label assigned by the next hop or virtual path identifier (VPI)/virtual channel identifier (VCI) used to get to next hop. The entries in this column include the following: **Note** VPI and VCI are not applicable to the Cisco 10000 series routers. • [T]—Means forwarding through an LSP tunnel. • No Label—Means that there is no label for the destination from the next hop or that label switching is not enabled on the outgoing interface.
	• Pop Label—Means that the next hop advertised an implicit NULL label for the destination and that the router popped the top label. • Aggregate—Means there are several prefixes for one local label. This entry is used when IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network. **Note** IPv6 traffic is not applicable to the Cisco 10000 series routers.
Prefix or Tunnel Id	Address or tunnel to which packets with this label are sent. **Note** If IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network, "IPv6" is displayed here.
Bytes Label Switched	Number of bytes switched with this incoming label.
Outgoing interface	Interface through which packets with this label are sent.
Next Hop	IP address of the neighbor that assigned the outgoing label.
Bundle adjacency exp(vcd)	Bundle adjacency information. Includes the MPLS EXP value and the corresponding VCD.
MAC/Encaps	Length in bytes of the Layer 2 header and length in bytes of the packet encapsulation, including the Layer 2 header and label header.
MTU	MTU of the labeled packet.
Label Stack	All the outgoing labels. If the outgoing interface is transmission convergence (TC)-ATM, the VCD is also shown. **Note** TC-ATM is not applicable to the Cisco 10000 series routers.
00010000AAAA030000008847 00013000	The actual encapsulation in hexadecimal form. A space is shown between Layer 2 and the label header.

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1612/products_feature_guide09186a008008093f.html#

QUESTION 53:
The Certkiller WAN is depicted below:



MPLS and LDP are enabled on routers Certkiller 2 and Certkiller 3 and all interfaces are enabled. However, the routers will not establish an LDP neighbor session. Troubleshooting has revealed that there is forwarding information in the FIB table, but there is no forwarding information in the LFIB table. Which issue would cause this problem?

A. IP CEF is not enabled on one or both of the routers.
B. One or both of the routers are using the loopback address as the LDP ID and the loopback is not being advertised by the IGP.
C. BGP neighbor sessions have not been configured on one or both of the routers.
D. MPLS has been enabled on the interface but has not been enabled globally on one or both of the routers.

Answer: B

Explanation:
MPLS-switched packets are forwarded based on information contained in the Label Forwarding Information Base (LFIB). A packet leaving a router over a label-switched interface will receive labels with values specified by the LFIB. Labels are associated with destinations in the LFIB according to Forwarding Equivalence Classes (FECs). A FEC is a grouping of IP packets which travel over the same path and receive the same forwarding treatment. The most simple example of a FEC is all packets traveling to a certain subnet. Another example could be all packets with a given IP precedence going to an Interior Gateway Protocol (IGP) next hop associated with a group of Border Gateway Protocol (BGP) routes.
The Label Information Base (LIB) is a structure which stores labels received from all Label Distribution Protocol (LDP) or Tag Distribution Protocol (TDP) neighbors. For Cisco implementation, labels are sent for all routes in a given router's routing table (with the exception of BGP routes), to all LDP or TDP neighbors. All labels received from neighbors are retained in the LIB, whether or not they are used. If the labels are received from a downstream neighbor for their FEC, then the labels stored in the LIB are used for packet forwarding by the LFIB. Meaning the labels used for forwarding are those received from a router's next hop to a destination, according to the router's Cisco Express Forwarding (CEF) and routing tables.
If label bindings are received from a downstream neighbor for prefixes (including subnet mask) which do not appear in a router's routing and CEF tables, these bindings will not be used. In a similar manner, if a router advertises labels for a subnet/subnet mask pair, which do not correspond to the routing updates also advertised by this router for the same subnet/subnet mask pair, these labels will not be used by upstream neighbors and the Label Switched Path (LSP) between these devices will fail.

QUESTION 54:
Two Certkiller routers are configured as IPSec VPN peers. Which IPsec VPN term describes a policy contract that specifies how two peers will use IPsec security services to protect network traffic?

A. Encapsulation security payload
B. Security Association
C. Transform set
D. Authentication Header
E. None of the above

Answer: B

Explanation:
A Virtual Private Network (VPN) is defined as network connectivity deployed on a shared infrastructure with the same policies and security as a private network.
A VPN can be between two end systems, or it can be between two or more networks. A VPN can be built using tunnels and encryption. VPNs can occur at any layer of the OSI protocol stack. A VPN is an alternative WAN infrastructure that replaces or augments existing private networks that use leased-line or enterprise-owned Frame Relay or ATM networks.
VPNs provide three critical functions:
1. Confidentiality (encryption) - The sender can encrypt the packets before transmitting them across a network. By doing so, no one can access the communication without permission. If intercepted, the communications cannot be read.
2. Data integrity - The receiver can verify that the data was transmitted through the Internet without being altered.
3. Origin authentication - The receiver can authenticate the source of the packet, guaranteeing and certifying the source of the information.
Security Association (SA) - A set of policy and key(s) used to protect information. The ISAKMP SA is the shared policy and key(s) used by the negotiating peers in this protocol to protect their communication

---

QUESTION 55:
Certkiller uses GRE tunnels over an IPSec VPN. Which three statements are correct about a GRE over IPsec VPN tunnel configuration on Cisco IOS routers? (Select three)

A. Crypto maps must specify the use of IPsec transport mode.
B. A crypto ACL will dictate the GRE traffic to be encrypted between the two IPsec peers.
C. A crypto ACL will dictate the ISAKMP and IPsec traffic to be encrypted between the two IPsec peers.
D. A dynamic routing protocol can be configured to run over the tunnel interface.
E. The crypto map must be applied on the tunnel interface.
F. The crypto map must be applied on the physical interface.

Answer: B, D, F

Explanation:
Although the Internet has created new opportunities for companies to streamline business processes, enter new markets, and work with partners and customers more effectively, it has also created a greater reliance on networks and a need to protect against a wide range of security threats. The main function that a VPN offers for this protection is encryption through a tunnel:
1. Tunnels provide logical, point-to-point connections across a connectionless IP

network. This enables the use of advanced security features. Tunnels for VPN solutions employ encryption to protect data from being viewed by unauthorized entities and to perform multiprotocol encapsulation, if necessary. Encryption is applied to the tunneled connection to make data legible only to authorized senders and receivers.
2. Encryption ensures that messages cannot be read by anyone but the intended recipient. As more information travels over public networks, the need for encrypting the information becomes more important. Encryption transforms content information into a ciphertext that is meaningless in its encrypted form. The decryption function restores the ciphertext back into content information intended for the recipient.
Cisco Generic Routing Encapsulation
This multiprotocol carrier protocol encapsulates IP, CLNP, and any other protocol packets inside IP tunnels.
With GRE tunneling, a Cisco router at each site encapsulates protocol-specific packets in an IP header, creating a virtual point-to-point link to Cisco routers at other ends of an IP cloud, where the IP header is removed.
By connecting multiprotocol sub networks in a single-protocol backbone environment, IP tunneling allows network expansion across a single-protocol backbone environment.
GRE tunneling allows desktop protocols to take advantage of the enhanced route selection capabilities of IP.
GRE does not provide encryption and can be monitored with a protocol analyzer.

QUESTION 56:
You have been tasked with configuring a new router to be added to te Certkiller IPSec VPN. What are the four main steps in configuring an IPsec site-to-site VPN tunnel on Cisco routers? (Choose four)

A. Create a crypto access list to define which traffic should be sent through the tunnel.
B. Create a crypto map and apply it to the outgoing interface of the VPN device.
C. Define the ISAKMP policy.
D. Define the pre-shared key used in the DH (Diffie-Hellman) exchange.
E. Define the IPsec transform set.
F. Configure dynamic routing over the IPsec tunnel interface.

Answer: A, B, C, E

Explanation:
IPsec provides a mechanism for secure data transmission over IP networks, ensuring confidentiality, integrity, and authenticity of data communications over unprotected networks such as the Internet. IPsec encompasses a suite of protocols and is not bound to any specific encryption or authentication algorithms, key generation technique, or security association (SA). IPsec provides the rules while existing algorithms provide the encryption, authentication, key management, and so on.
* Determine the key distribution method - Determine the key distribution method based on the numbers and locations of IPSec peers. For a small network, keys may be distributed manually. For larger networks, use a CA server to support scalability of IPSec peers. Then, configure the Internet Security Association Key Management Protocol

(ISAKMP) to support the selected key distribution method.
* Determine the authentication method - Determine the authentication method based on the key distribution method. Cisco IOS software supports either pre-shared keys, RSA encrypted nonces, or RSA signatures to authenticate IPSec peers. This lesson focuses on using pre-shared keys.
* Identify IPSec peer IP addresses and host names
- Determine the details of all of the IPSec peers that will use ISAKMP and pre-shared keys for establishing security associations (SAs). This information will be used to configure IKE.
* Determine ISAKMP policies for peers - An ISAKMP policy defines a combination or "suite" of security parameters to be used during the ISAKMP negotiation. Each ISAKMP negotiation begins with each peer agreeing on a common, or shared, ISAKMP policy. Determine the ISAKMP policy suites in advance of configuration. Then, configure IKE to support the policy details that have been determined. Examples of ISAKMP policy details are included in the following list:
o Encryption algorithm
o Hash algorithm
o IKE SA lifetime

QUESTION 57:
Certkiller uses IPSec technology throughout their network. Which three benefits do IPsec VPNs provide? (Select three)

A. Data integrity
B. QoS
C. Confidentiality
D. Adaptive threat defense
E. Origin authentication
F. A fully-meshed topology with low overhead

Answer: A, C, E

Explanation:
IPsec provides a mechanism for secure data transmission over IP networks, ensuring confidentiality, integrity, and authenticity of data communications over unprotected networks such as the Internet. IPsec encompasses a suite of protocols and is not bound to any specific encryption or authentication algorithms, key generation technique, or security association (SA). IPsec provides the rules while existing algorithms provide the encryption, authentication, key management, and so on.

QUESTION 58:
The branch Certkiller locations are connected via an IPSec VPN. Which three IPsec VPN statements are true? (Select three)

A. Main mode is the method used for the IKE phase two security association negotiations.

B. To establish IKE SA, main mode utilizes six packets while aggressive mode utilizes only three packets.
C. IKE keepalives are unidirectional and sent every ten seconds.
D. Quick mode is the method used for the IKE phase one security association negotiations.
E. IKE uses the Diffie-Hellman algorithm to generate symmetrical keys to be used by IPsec peers.
F. IPsec uses the Encapsulating Security Protocol (ESP) or the Authentication Header (AH) protocol for exchanging keys.

Answer: B, C, E

Explanation:
IPSec is the choice for secure corporate VPNs. IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services using Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec
IPSec is the main option featured in this topic for securing enterprise VPNs. Unfortunately, IPSec supports only IP unicast traffic. If IP-unicast packets are being tunneled, then a single encapsulation provided by IPSec is sufficient and much less complicated to configure and troubleshoot.

QUESTION 59:
Certkiller uses GRE tunnels over their IPSec VPN. Which three features are benefits of using GRE tunnels in conjunction with IPsec for building site-to-site VPNs? (Select three)

A. It supports multi-protocol (non-IP) traffic over the tunnel
B. It uses Virtual Tunnel Interface (VTI) to simplify the IPsec VPN configuration
C. It allows dynamic routing over the tunnel
D. It reduces IPsec headers overhead since tunnel mode is used
E. It simplifies the ACL used in the crypto map

Answer: A, C, E

Explanation:
Cisco Generic Routing Encapsulation
GRE know as OSI Layer3 tunneling protocol:
Uses IP for transport
Use an additional header to support any other OSI Layer3 protocol as Payload (e.g.,IP, IPX, AppleTalk)
GRE is a tunneling protocol initially developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. Routing protocols are often used across the tunnel to enable dynamic exchange or routing information in the virtual

network.
The multiprotocol functionality is provided by adding an additional GRE header between the payload and the tunneling IP header. This multiprotocol carrier protocol encapsulates IP, CLNP, and any other protocol packets inside IP tunnels. With GRE tunneling, a Cisco router at each site encapsulates protocol-specific packets in an IP header, creating a virtual point-to-point link to Cisco routers at other ends of an IP cloud, where the IP header is removed. By connecting multiprotocol sub networks in a single-protocol backbone environment, IP tunneling allows network expansion across a single-protocol backbone environment. GRE tunneling allows desktop protocols to take advantage of the enhanced route selection capabilities of IP.
GRE does not provide encryption and can be monitored with a protocol analyzer

---

QUESTION 60:
Certkiller uses GRE tunnels to pass routing protocol traffic across its IPSec VPN. Which IPsec mode will encrypt a GRE tunnel to provide multiprotocol support and reduced overhead?

A. Transport
B. Tunnel
C. Multipoint GRE
D. 3DES
E. None of the above

Answer: A

Explanation:
GRE is good at tunneling:
- Multiprotocol support-Provides virtual point-to-point connectivity, allowing routing protocols to be used
- GRE is poor at security-only very basic plaintext authentication can be implemented using the tunnel key (not very secure)
- GRE cannot accommodate typical security requirements
- Confidentiality-Data source authentication-Data integrity. The main function of GRE is to provide powerful yet simple tunneling. It supports any OSI Layer 3 protocol as payload, for which it provides virtual point-to-point connectivity. It also allows the usage of routing protocols across the tunnel. The main limitation of GRE is that it lacks strong security functionality. It only provides basic plaintext authentication using the tunnel key, which is not secure, and tunnel source and destination addresses. A reasonably secure VPN requires these characteristics that are not provided by GRE:
Cryptographically strong confidentiality (that is, encryption) Data source authentication that is not vulnerable to man-in-the-middle attacks Data integrity assurance that is not vulnerable to man-in-the-middle attacks and spoofing

---

QUESTION 61:
The Certkiller Easy VPN network was configured with RRI. Which statement describes Reverse Route Injection (RRI)?

A. A static route is created on the Cisco Easy VPN server for the internal IP address of each VPN client.
B. A static route that points towards the Cisco Easy VPN server is created on the remote client.
C. A default route is injected into the route table of the remote client.
D. A default route is injected into the route table of the Cisco Easy VPN server.
E. None of the above.

Answer: A

Explanation:
Reverse Route Injection (RRI) to inject remote networks into an Interior Gateway Protocol (IGP) and distribute it to other routers in the network.
RRI should be used when the following conditions occur:-
- More than one VPN server is used-Per-client static IP addresses are used with some clients (instead of using per-VPN-server IP pools)
- RRI ensures the creation of static routes.
- Redistributing static routes into an IGP allows the servers siterouters to find the appropriate Easy VPN Server for return traffic to clients.

QUESTION 62:
Two Certkiller IPsec routers use DH to establish a VPN connection. Which feature is an accurate description of the Diffie-Hellman (DH) exchange between two IPsec peers?

A. It allows the two peers to communicate its digital certificate to each other during IKE phase 1
B. It allows the two peers to jointly establish a shared secret key over an insecure communications channel
C. It allows the two peers to negotiate its IPsec transforms during IKE phase 2
D. Itallows the two peers to communicate the pre-shared secret key to each other during IKE phase 1
E. It allows the two peers to authenticate each other over an insecure communications channel
F. None of the above

Answer: B

Explanation:
One of the most important aspects of creating a secure VPN involves exchanging the keys. The Diffie-Hellman algorithm provides a way for two users, A and B, to establish a shared secret key that only they know. The shared secret key can be established even though users A and B are communicating over an insecure channel. This secret key is then used to encrypt data using the secret key encryption algorithm selected by A and B. Two numbers which are shared are "p", a prime number and "g", a number less than "p"

with some restrictions.
A and B each create a large random number that is kept secret, called "XA" and "XB".
The Diffie-Hellman algorithm is now performed. Both A and B carry out computations and exchange results.
The final result is a common value "K". A user who knows "p" or "g" cannot easily calculate the shared secret value, because of the difficulty in factoring large prime numbers.
It is important to note that A and B have no method for determining each other's identity.
The exchange is vulnerable to a man-in-the-middle attack. Diffie-Hellman provides for confidentiality but does not provide for authentication. Authentication is achieved by the use of digital signatures in the Diffie-Hellman message exchanges

---

QUESTION 63:
Certkiller uses GRE tunnels over their IPSec VPN to pass routing information.
Which statement is true about an IPsec/GRE tunnel?

A. Crypto map ACL is not needed to match which traffic will be protected.
B. GRE encapsulation occurs before the IPsec encryption process.
C. The GRE tunnel source and destination addresses are specified within the IPsec transform set.
D. An IPsec/GRE tunnel must use IPsec tunnel mode.
E. None of the above.

Answer: B

Explanation:
The main function of GRE is to provide powerful yet simple tunneling. It supports any OSI Layer 3 protocol as payload, for which it provides virtual point-to-point connectivity. It also allows the usage of routing protocols across the tunnel. The main limitation of GRE is that it lacks strong security functionality. It only provides basic plaintext authentication using the tunnel key, which is not secure, and tunnel source and destination addresses. A reasonably secure VPN requires these characteristics that are not provided by GRE: Cryptographically strong confidentiality (that is, encryption) Data source authentication that is not vulnerable to man-in-the-middle attacks Data integrity assurance that is not vulnerable to man-in-the-middle attacks and spoofing

---

QUESTION 64:
AN IPSec secure tunnel is being built between routers CK1 and CK2 . In IPSec, what are the common services provided by Authentication Header (AH) and Encapsulation Security Payload (ESP)?

A. Data origin authentication, confidentiality, and anti-replay service
B. Confidentiality, data integrity, and anti-replay service
C. Data integrity, data origin authentication, and anti-replay service
D. Confidentiality, data integrity, and data origin authentication
E. Confidentiality, data integrity and authorization.

Answer: C

Explanation:
AH (Authentication Header) is used to provide data integrity and authentication. It does not provide any form of encryption to the payload of the packet. AH uses a keyed one-way hash function (also called an HMAC) such as MD5 or SHA-1 to guarantee the integrity and origin of the packet. Optionally, it can provide anti-replay protection.
ESP (Encapsulating Security Payload) is primarily used to provide payload encryption. With the current revisions of the RFC for ESP, it also includes the ability to provide authentication and integrity.
Because ESP can do all the services needed in a secure VPN network (including optional Ahs services), most implementations do not include any AH options. When the IPSec standard was created, its developers took into account the need for increased security. Therefore, IPSec can use different algorithms for payload encryption, such as DES to give you 56-bit encryption or 3DES to give you 168-bit encryption. As the need for stronger payload encryption arises, the standard will allow vendors to implement other algorithms.
Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 435 & 436

QUESTION 65:
IPSec is being used for the Certkiller VPN. In the IPSec protocol; what are the responsibilities of the Internet Key Exchange (IKE)? (Choose all that apply)

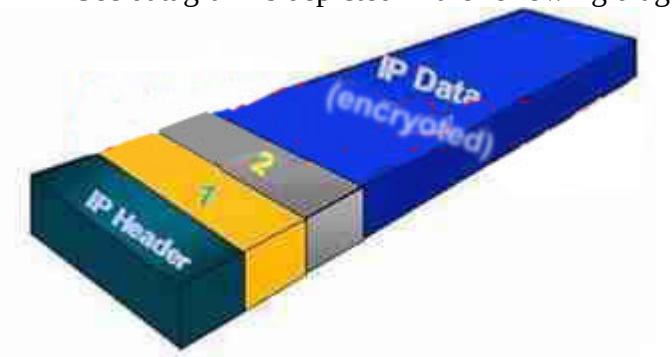
A. Negotiating protocol parameters
B. Integrity checking user hashes
C. Authenticating both sides of a connection
D. Implementing tunnel mode
E. Exchanging public keys
F. Packet encryption

Answer: A, C, E

Explanation:
Internet Key Exchange (IKE) is used to establish all the information needed for a VPN tunnel. Within IKE, you negotiate your security policies, establish your SAs, and create and exchange your keys that will be used by other algorithms such as DES. IKE is broken down into two phases, described next.
Phase One of IKE
Phase one is used to negotiate policy sets, authenticate peers, and create a secure channel between peers. IKE phase one can happen in one of two modes, main mode or aggressive mode. The major difference is that in main mode, three different and distinct exchanges take place to add to the security of the tunnel, whereas in aggressive mode everything is sent in a single exchange.

Phase Two of IKE
IKE phase two is used to negotiate the IPSec security parameters (such as the IPSec transform sets), establish SAs, and optionally perform additional Difie-Hellman exchanges. IKE phase two has only one mode, called quick mode, which happens only after IKE phase one has completed.
Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8)
Page 438 to 439

QUESTION 66:
An IPSec datagram is depicted in the following diagram:

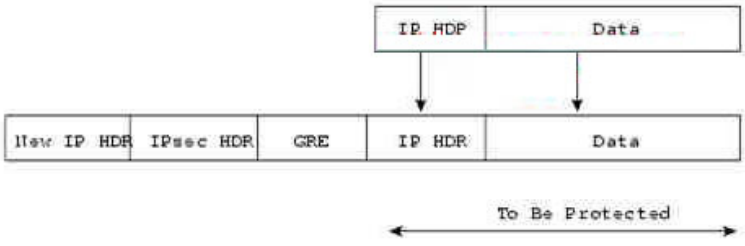


In this datagram, what is the name of the header that is marked with a 2? (Hint: It provides data authentication and confidentiality)

A. AH header
B. ESP header
C. SA header
D. MPLS VPN header
E. None of the above

Answer: B

Explanation:



IPsec defines a new set of headers to be added to IP datagrams. These new headers are placed after the outer IP header. These new headers provide information for securing the payload of the IP packet as follows:
Authentication Header (AH)-This header, when added to an IP datagram, ensures the integrity and authenticity of the data, including the invariant fields in the outer IP header.

It does not provide confidentiality protection. AH uses a keyed-hash function rather than digital signatures, because digital signature technology is slow and would greatly reduce network throughput.
Encapsulating Security Payload (ESP)-This header, when added to an IP datagram, protects the confidentiality, integrity, and authenticity of the data. If ESP is used to validate data integrity, it does not include the invariant fields in the IP header.
Reference: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/depip_wp.htm

---

QUESTION 67:
IPSec is being used for the Certkiller VPN. Which of the IPSEC protocols is capable of negotiating security associations?

A. AH
B. ESP
C. IKE
D. SSH
E. MD5
F. None of the above

Answer: C

Explanation:
IKE is a key management protocol standard that is used in conjunction with the IPSec standard.
IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.
IKE is a hybrid protocol, which implements the Oakley key exchange and Skeme key exchange inside the ISAKMP framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.) IKE automatically negotiates IPSec security associations and enables IPSec secure communications without manual preconfiguration.
Specifically, IKE provides the following benefits:
* Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
* Allows you to specify a lifetime for the IPSec security association.
* Allows encryption keys to change during IPSec sessions.
* Allows IPSec to provide anti-replay services.
* Permits CA support for a manageable, scalable IPSec implementation.
* Allows dynamic authentication of peers.

QUESTION 68:
IPSec is being used for the Certkiller VPN. Which of the phrases below are true about IPSec IKE Phase 2? (Choose all that apply)

A. It determines the key distribution method

B. It identifies IPSec peer details
C. It selects manual or IKE-initiated SAs
D. It determines the authentication method
E. It negotiates ISAKMP policies for peers
F. It selects the IPSec algorithms and parameters for optimal security and performance

Answer: C, E, F

Explanation:
IKE Phase 1
The basic purpose of IKE phase 1 is to authenticate the IPSec peers and to set up a secure channel between the peers to enable IKE exchanges.
IKE phase 1 performs the following functions:
* Authenticates and protects the identities of the IPSec peers
* Negotiates a matching IKE SA policy between peers to protect the IKE exchange
* Performs an authenticated Diffie-Hellman exchange with the end result of having matching shared secret keys
* Sets up a secure tunnel to negotiate IKE phase 2 parameters
IKE Phase 2
The purpose of IKE phase 2 is to negotiate IPSec SAs to set up the IPSec tunnel. IKE phase 2 performs the following functions:
* Negotiates IPSec SA parameters protected by an existing IKE SA
* Establishes IPSec security associations
* Periodically renegotiates IPSec SAs to ensure security
* Optionally performs an additional Diffie-Hellman exchange

QUESTION 69:
IPSec is being used for the Certkiller network between routers CK1 and CK2 .
During the ISAKMP negotiation process in IKE Phase 1 mode (where ISAKMP looks for a policy that is the same on both peers) which peer would be responsible for matching the policies?

A. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match with its policy.
B. The remote peer sends all its policies to the initiating peer, and the initiating peer tries to find a match with its policies.
C. Both peers end all their policies to the other peer, and each peer tries to find a match with its policies.
D. Both peers end all their policies to the other peer, but just the initiating peer tries to find a match with its policies.

Answer: A

Explanation:
When the IKE negotiation begins, IKE looks for an IKE policy that is the same on both

peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the other peer's received policies. The remote peer checks each of its policies in order of its priority (highest priority first) until a match is found.
A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote peer's policy specifies a lifetime less than or equal to the lifetime in the policy being compared. (If the lifetimes are not identical, the shorter lifetime-from the remote peer's policy-will be used.)
If no acceptable match is found, IKE refuses negotiation and IPSec will not be established.
If a match is found, IKE will complete negotiation, and IPSec security associations will be created.

QUESTION 70:
IPSec is being used for the Certkiller VPN. What is true about the security protocol ESP (Encapsualtion Security Payload) in IPSec? (Choose three)

A. IP packet is expanded by transport mode: 37 bytes (3DES) or 63 bytes (AES); tunnel mode: 57bytes (3DES) or 83 bytes (AES).
B. IP packet is expanded by: transport mode 56 bytes: tunnel mode 128 bytes.
C. Authentication is mandatory and the whole packet as well as the header is authenticated.
D. Authentication is optional and the outer header is not authenticated.
E. The ESP security protocol provides data confidentiality.
F. The ESP security protocol provides no data confidentiality.

Answer: A, C, E

Explanation:
ESP is the Encapsulating Security Payload: A security protocol which provides data privacy services and optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.
Both the older RFC 1829 ESP and the updated ESP protocol are implemented. The updated ESP protocol is per the latest version of the "IP Encapsulating Security Payload" Internet Draft (draft-ietf-ipsec-esp-v2-xx.txt).
RFC 1829 specifies DES-CBC as the encryption algorithm; it does not provide data authentication or anti-replay services. The updated ESP protocol allows for the use of various cipher algorithms and (optionally) various authentication algorithms. Cisco IOS implements the mandatory 56-bit DES-CBC with Explicit IV as the encryption algorithm, and MD5 or SHA (HMAC variants) as the authentication algorithms. The updated ESP protocol provides anti-replay services.
Reference: IPSec Network Security
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

---

QUESTION 71:
What is true about the security protocol AH (Authentication Header) used in a secure IPSec tunnel? (Choose three)

A. Authentication is mandatory.
B. Authentication is optional.
C. The IP packet is expanded by transport mode 37 bytes(3DES(or 63 bytes(AES); tunnel mode 57 bytes(3DES) or 83 bytes(AES).
D. The IP packet is expanded by transport mode 56 bytes; tunnel mode 128 bytes.
E. The IPSec AH security protocol does provide data confidentiality.
F. The IPSec AH security protocol does not provide data confidentiality.

Answer: A, C, F

Explanation:
Authentication Header: A security protocol which provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).
Both the older RFC 1828 AH and the updated AH protocol are implemented. The updated AH protocol is per the latest version of the "IP Authentication Header" Internet Draft (draft-ietf-ipsec-auth-header-xx.txt).
RFC 1828 specifies the Keyed MD5 authentication algorithm; it does not provide anti-replay services. The updated AH protocol allows for the use of various authentication algorithms; CiscoIOS has implemented the mandatory MD5 and SHA (HMAC variants) authentication algorithms. The updated AH protocol provides anti-replay services.
Reference: IPSec Network Security
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

---

QUESTION 72:
Which of the following statements is true about IPSec security associations (SAs)?

A. SAs contain unidirectional specifications only.
B. SAs describe the mechanics if implementing a key exchange protocol.
C. A single SA ca be used for both AH and ESP encapsulation protocols.
D. A single SA is negotiated by peers requesting secure communication.
E. Active SAs are stored in a local database called the IPSec database.

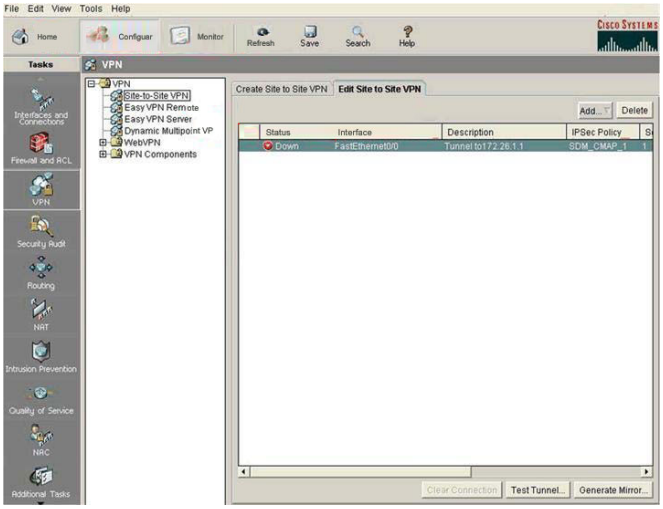
Answer: A

Explanation:
An SA is a set of security parameters used by a tunnel for authentication and encryption. Key management tunnels use one SA for both directions of traffic; data management tunnels use at least one SA for each direction of traffic. Each endpoint assigns a unique identifier, called a security parameter index (SPI), to each SA.
A set of SAs is needed for a protected data pipe, one per direction per protocol. For

example, if you have a pipe that supports Encapsulating Security Protocol (ESP) between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPSec endpoint) address, security protocol (AH or ESP), and SPI.
Note the following regarding SAs:
IP Security (IPSec) SAs are unidirectional and are unique in each security protocol.
An Internet Key Exchange (IKE) SA is used by IKE only, and unlike the IPSec SA, it is bidirectional.
IKE negotiates and establishes SAs on behalf of IPSec.
A user can also establish IPSec SAs manually.
Reference:
http://www.cisco.com/en/US/products/sw/cscowork/ps4565/products_user_guide_chapter09186a008043bd31.ht

---

QUESTION 73:
The network administrator logged into a Certkiller device using SDM as shown below:



A site-to-site VPN connection has been configured using the SDM shown above.
What option can aid in the configuration of the VPN on the peer router?

A. The VPN Components option on the VPN tab
B. The Generate Mirror option on the VPN Edit tab
C. The Monitor Mode option on the VPN Status tab
D. The IPSec Policies from the VPN Components tab

Answer: B

Explanation:
Step1
From the left frame, select VPN.
Step2
Select Site-to-Site VPN. in the VPN tree, and then click the Edit tab.
Step3
Select the VPN connection that you want to use as a template, and click Generate Mirror.

SDM displays the Generate Mirror screen.
Step4
From the Peer Device field, select the IP address of the peer device for which you want to generate a suggested configuration.
The suggested configuration for the peer device appears on the Generate Mirror screen.
Step5
Click Save to display the Windows Save File dialog box, and save the file.

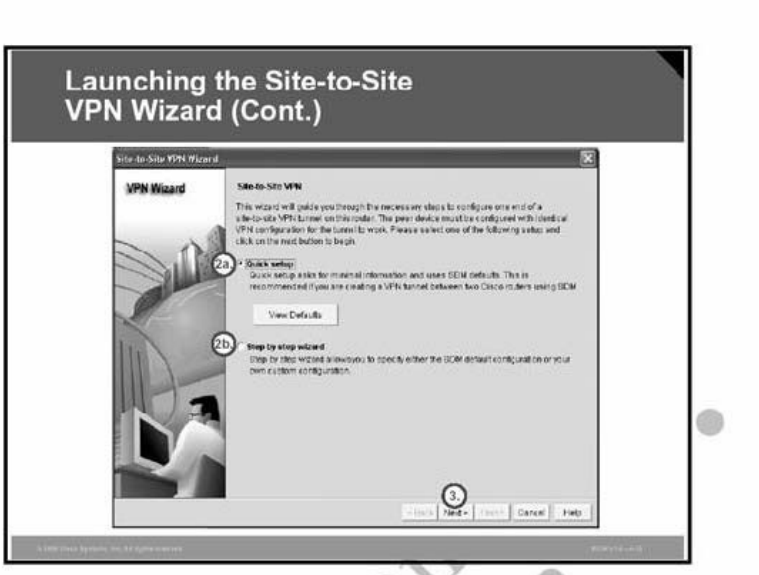
QUESTION 74:
The following exhibit shows the Cisco VPN Wizard:

You need to use the VPN wizard to create an IPSec VPN between two Certkiller devices. When you are using the Quick Setup option of the Site-to-Site VPN wizard on the SDM to configure an IPsec VPN, which three settings can you configure? (Select three)

A. The encapsulation security payload
B. The crypto map
C. The transform set priority
D. The peer identity
E. The source interface and destination IP address
F. The pre-shared key

Answer: D, E, F

Explanation:
Abut Cisco SDM
- SDM is anembeddedweb-based management tool.
- Providesintelligent wizards to enable quicker and easier deployments,and does not require knowledge of Cisco IOS CLI or security expertise.
- Contains toolsfor more advanced users: ACL editor-VPN crypto map editor-Cisco IOS CLI preview



Step 2 A window will open, asking you which wizard mode to use:

a. The **Quick setup** uses SDM-default IKE policies and IPsec transform sets.

b. The **Step by step wizard** allows you to specify all the details.

Step 3 Click the **Next** button to configure the parameters of the VPN connection.

When you select the quick Setup you need to configure i. The peer identity ii. The source interface and destination IP address iii. The pre-shared key

---

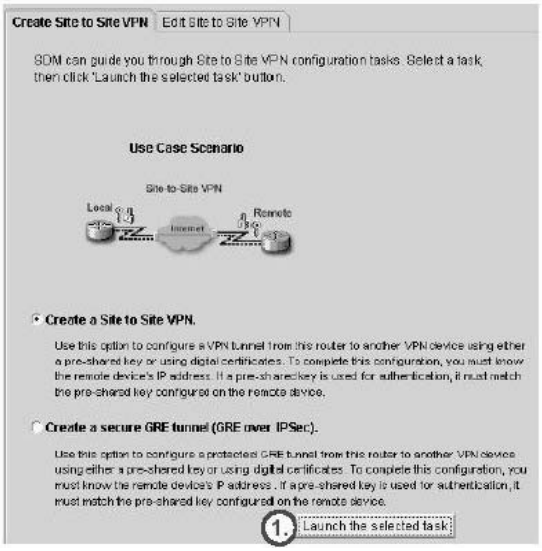
QUESTION 75:

You need to configure a GRE tunnel on a Certkiller IPSec router. When you are using the SDM to configure a GRE tunnel over IPsec, which two parameters are required when defining the tunnel interface information? (Select two)

A. The crypto ACL number
B. The IPSEC mode (tunnel or transport)
C. The GRE tunnel interface IP address
D. The GRE tunnel source interface or IP address, and tunnel destination IP address
E. The MTU size of the GRE tunnel interface

Answer: C, D

Explanation:
The main function of GRE is to provide powerful yet simple tunneling. It supports any OSI Layer 3 protocol as payload, for which it provides virtual point-to-point connectivity. It also allows the usage of routing protocols across the tunnel. The main limitation of GRE is that it lacks strong security functionality. It only provides basic plaintext authentication using the tunnel key, which is not secure, and tunnel source and destination addresses. A reasonably secure VPN requires these characteristics that are not provided by GRE: Cryptographically strong confidentiality (that is, encryption) Data source authentication that is not vulnerable to man-in-the-middle attacks Data integrity assurance that is not vulnerable to man-in-the-middle attacks and spoofing



While configuring the GRE tunnel on SDM you need to specify i. The GRE tunnel interface IP address ii. The GRE tunnel source interface or IP address, and tunnel destination IP address

---

QUESTION 76:

You want to use dynamic routing protocols over the Certkiller IPSec WAN using GRE tunnels. Which three routing protocols can be configured when configuring a site-to-site GRE over IPsec tunnel using SDM? (Select three)

A. IGRP
B. EIGRP
C. BGP
D. OSPF
E. RIP
F. IS-IS

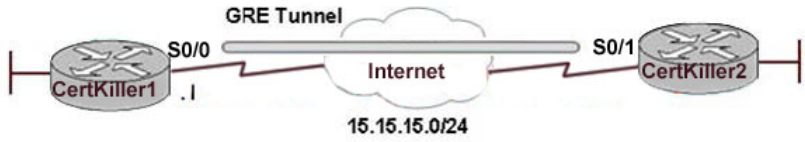
Answer: B, D, E

Explanation:
According to Cisco.com, While configuring the site-to-site GRE over IPSec tunnel using SDM, it can supports only RIP, EIGRP and OSPF for more details:
http://www.cisco.com/en/US/products/ps6660/products_white_paper0900aecd804f1693.shtml

---

QUESTION 77:

Two Certkiller routers are connected together as shown below:



Configuration exhibit #1:

```
CertKiller1 #show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES manual administratively down down
Serial0/0                  15.15.15.1      YES manual administratively down down
Serial0/1                  unassigned      YES manual administratively down down
Tunnel1                    10.10.10.1      YES manual up                    down
```

Configuration exhibit #2:

```
CertKiller1#show interfaces tunnel 1
Tunnel1 is up, line protocol is down
  Hardware is Tunnel
  Internet address is 10.10.10.1/24
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalite ndt set
  Tunnel source 15.15.15.1, destination 15.15.15.2
  Tunnel prctocol/transport GRE/IP, key disabled, sequencing disabled
  Tunnel TTL 255
  Checksumming of packets disabled,  fast tunneling enabled
  Last input rever, output 00:10:38, output hang never
  Last clearing of  show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 4
  Queueing strategy: fifo
  Output queue :0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
```

A GRE tunnel has been configured between the Certkiller 1 headquarters router and the Certkiller 2 branch site router. Based on the information shown above, why are users at the branch site unable to access the corporate intranet?

A. The source IP address of the GRE tunnel must be different from the IP address of interface S0/0 on router Certkiller 1.
B. The interface S0/0 on router Certkiller 1 must be enabled with the no shutdown command.
C. The destination IP address of the GRE tunnel must be different from the IP address of the interface S0/1 on router Certkiller 2.
D. The IP address of the interface tunnel1 must be the same as the IP address of the interface S0/0 on router Certkiller 1.
E. The GRE tunnel must be configured with the encapsulation ppp command.
F. None of the above

Answer: B

Explanation: The Physical status of Serial 0/0 of Certkiller 1 Router is administratively Down. To bring up you need to enter no shutdown command in interface configuration mode.

QUESTION 78:
A new Certkiller router must be added to the IPSec VPN. When configuring a site-to-site IPsec VPN tunnel on this router, which configuration must be the exact reverse of the other IPsec peer?

A. The crypto map
B. The crypto ACL
C. The IPsec transform
D. The pre-shared key
E. The ISAKMP policy

F. None of the above

Answer: B

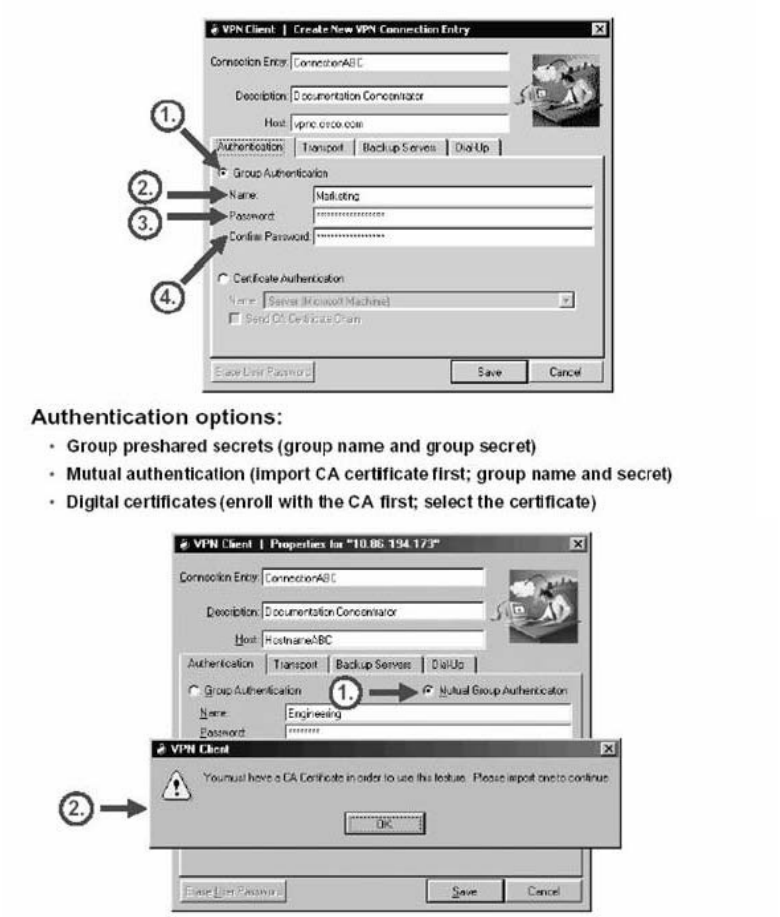
Explanation:
The crypto ACLs identify the traffic flows that will be protected. Extended IP ACLs select IP traffic to encrypt by protocol, IP address, network, subnet, and port. Although the ACL syntax is unchanged from extended IP ACLs, the meanings are slightly different for crypto ACLs. When using crypto ACLs, permit specifies that matching packets must be encrypted and deny specifies that matching packets do not need to be encrypted. Crypto ACLs behave similar to an extended IP ACL applied to the outbound traffic on an interface.

QUESTION 79:
When establishing a VPN connection from the Cisco software VPN client of a Certkiller device to the Certkiller Easy VPN server router using pre-shared key authentication, what is entered in the configuration GUI of the Cisco software VPN client to identify the group profile that is associated with this VPN client?

A. The group name
B. The client name
C. The organizational unit
D. The distinguished name
E. None of the above

Answer: A

Explanation:
The Cisco virtual private network (VPN) Client for Windows (or VPN Client) is software that runs on a Microsoft Windows-based PC. The VPN Client on a remote PC, communicating with a Cisco Easy VPN Server on an enterprise network or with a service provider, creates a secure connection over the Internet. This lesson describes the process of setting up a Cisco VPN Client on a laptop to create a secure connection, called a tunnel, between your computer and a private network.
* To use VPN Client, you must create at least one connection entry that includes this information:
* The VPN device (the remote server) to access.
1. Preshared keys-the IPsec group to which the system administrator assigned you. Your group determines how you access and use the remote network. For example, it specifies access hours, number of simultaneous logins, user authentication method, and the IPsec algorithms that your VPN Client uses.
2. Certificates-the name of the certificate that you are using for authentication.
3. Optional parameters that govern VPN Client operation and connection to the remote network.



QUESTION 80:

The following output was displayed on a Certkiller router:

```
Connection  Interface   IP-Address     State  Algorithm     Encrypt  Decrypt
2           Ethernet0   172.21.111.9   set    DES_56_CFB64  41       32
3           Ethernet1   172.29.13.2    set    DES_56_CFB64  110      65
4           Serial0     172.17.42.1    set    DES_56_CFB64  36       27
```

Based on what is shown above, which statement is true about the output of the show crypto engine connections active command?

A. The state of "set" indicates that the connection is configured but not connected to a peer.
B. All three interfaces are active and are encrypting and decrypting traffic.
C. No subinterfaces are involved in VPN connections.
D. The device that is shown has not established a VPN connection with a peer.
E. None of the above.

Answer: B

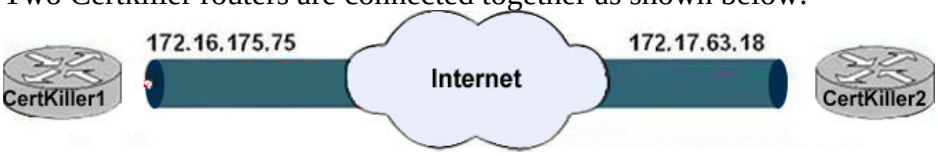
Explanation:
showcrypto engine connections activeTo view the current active encrypted session connections for all crypto engines, use the show crypto engine connections active privileged EXEC command.
The following is sample output from the show crypto engine connections active command:
Router1# show crypto engine connections active
Connection Interface IP-Address State Algorithm Encrypt Decrypt
2 Ethernet0 172.21.114.9 set DES_56_CFB64 41 32
3 Ethernet1 172.29.13.2 set DES_56_CFB64 110 65
4 Serial0 172.17.42.1 set DES_56_CFB64 36 27
The following is sample output from the show crypto engine connections active command on a Cisco7500 series router, where the VIP is in slot 4:
Router1# show crypto engine connections active 4
Connection Interface IP-Address State Algorithm Encrypt Decrypt
2 Ethernet0 172.21.114.9 set DES_56_CFB64 41 32
3 Ethernet1 172.29.13.2 set DES_56_CFB64 110 65
4 Serial0 172.17.42.1 set DES_56_CFB64 36 27
Router1# show crypto engine connections active vip
Connection Interface IP-Address State Algorithm Encrypt Decrypt
2 Ethernet0 172.21.114.9 set DES_56_CFB64 41 32
3 Ethernet1 172.29.13.2 set DES_56_CFB64 110 65
4 Serial0 172.17.42.1 set DES_56_CFB64 36 27

Field	**Description**
Connection	Identifies the connection by its number. Each active encrypted session connection is identified by a positive number from 1 to 299. These connection numbers correspond to the table entry numbers.
Interface	Identifies the interface involved in the encrypted session connection. This will display only the actual interface, not a subinterface (even if a subinterface is defined and used for the connection).

IP-Address	Identifies the IP address of the interface. Note that if a subinterface is used for the connection, this field will display "unassigned."
State	The state "set" indicates an active connection.
Algorithm	Identifies the Data Encryption Standard (DES) algorithm used to encrypt/decrypt packets at the interface.
Encrypt	Shows the total number of encrypted outbound IP packets.
Decrypt	Shows the total number of decrypted inbound IP packets.

QUESTION 81:

Two Certkiller routers are connected together as shown below:



Certkiller 1 is condigured as shown below:

```
CertKiller1# show run
  <output omitted>
  crypto isakmp policy 1
    authentication pre-share
    encryption 3des
  crypto isakmp key AnDtEk address 172.17.63.18
  !
  crypto ipsec transform-set trans2 esp-3des
  esp-md5-hmac
  !
  crypto map vpomap2 local-address Ethernet1
  crypto map vpomap2 10 IPSec-isakmp
    set peer 172.17.63.18
    set transform-set trans2
    match address 110
  interface Ethernet1
    ip address 172.16.175.75 255.255.255.0
  interface Tunnel0
    ip address 10.10.2.1 255.255.255.252
    ip mtu 1400
    tunnel source Ethernet1
    tunnel destination 172.17.63.18
    crypto map vpnmap2
```

Certkiller 2 is condigured as shown below:

```
CertKiller2# show run
    <output omitted>
    crypto isakmp policy 1
      authentication pre-share
      encryption 3des
    crypto isakmp key AnDtEk address 172.16.175.75
    !
    crypto ipsec transform-set trans2 esp-3des
    esp-md5-hmac
    !
    crypto map vpnmap2 local-address Ethernet1
    crypto map vpnmap2 10 IPSec-isakmp
      set peer 172.16.175.75
      set transform-set trans2
      match address 110
    interface Ethernet1
      ip address 172.17.63.18 255.255.255.0
    interface Tunnel0
      ip address 10.10.2.2 255.255.255.252
      ip mtu 1400
      tunnel source Ethernet1
      tunnel destination 172.16.175.75
      crypto map vpnmap2
```

Based on the information provided above, what is missing in the configuration of both IPSec peers concerning the IPSec/GRE configuration?

A. DH group configuration under the crypto ipsec transform-set trans2
B. access-list 110 on both peers to encrypt GRE traffic between 172.16.175.75 and 172.17.63.18
C. mode transport under the crypto ipsec transform-set trans2
D. crypto map vpnmap2 on the Ethernet1 interface
E. mode tunnel under the crypto ipsec transform-set trans2

F. access-list 110 on both peers to permit ISAKMP and IPSec traffic between 172.16.175.75 and 172.17.63.18

Answer: B

Explanation:
Ensure existing access lists (ACLs) on perimeter routers, firewalls, or other routers do not block IPSec traffic. Perimeter routers typically implement a restrictive security policy with ACLs, where only specific traffic is permitted and all other traffic is denied. Such a restrictive policy blocks IPSec traffic. Add specific permit statements to the ACL to allow IPSec traffic.
Ensure that the ACLs are configured so that ISAKMP, Encapsulating Security Payload (ESP), and Authentication Header (AH) traffic are not blocked at interfaces used by IPSec. ISAKMP uses UDP port 500, ESP is assigned IP protocol number 50, and AH is assigned IP protocol number 51. In some cases, a statement must be added to router ACLs to explicitly permit this traffic

---

QUESTION 82:
Part of the configuration of an existing Certkiller router is shown below:

```
<Output Omitted>
!
crypto isakmp policy 1
 authentication pre-share
 cryoption 3des
!
cryopto isakmp key CERTKILLER 12 4 address 172.17.63.18
!
crypto ipsec transform-set TRANS2 esp-3des esp-md5-hmac
!
crypto map VPNMAP2 local-address Ethernet1
crypto map VPNMAP2 10 IPSec-isakmp
 set peer 172.17.63.18
 set transform-set TRANS2
 match address 110
!
interface Ethernet1
 ip address 172.16.175.75 255.255.255.0
!
interface Tunnel0
 ip address 10.10.2.1 255.255.255.252
 [redacted]
!
ip route 0.0.0.0 0.0.0.0 172.16.175.1
!
<Output Omitted>
```

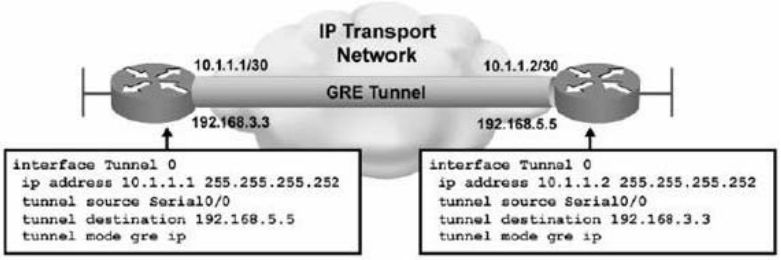
Based on the information shown above, which three statements describe the steps that are required to configure an IPsec site-to-site VPN using a GRE tunnel? (Select three)

A. The command "access-list 110 permit ip" must be configured to specify which hosts can use the tunnel.
B. The "tunnel source Ethernet1" command must be configured on the Tunnel0 interface.
C. The "tunnel source Tunnel0" command must be configured on the Tunnel0 interface.
D. The command "access-list 110 permit gre" must be configured to specify which traffic will be encrypted.
E. The "tunnel destination 172.17.63.18" command must be configured on the Tunnel0

interface.
F. The "tunnel mode gre" command must be configured on the Tunnel0 interface.

Answer: B, D, E

Explanation:
Tunnels provide logical, point-to-point connections across a connectionless IP network. This enables the use of advanced security features. Tunnels for VPN solutions employ encryption to protect data from being viewed by unauthorized entities and to perform multiprotocol encapsulation, if necessary. Encryption is applied to the tunneled connection to make data legible only to authorized senders and receivers



- GRE tunnel is up and protocol up if:
  - Tunnel source and destination are configured
  - Tunnel destination is in routing table
  - GRE keepalives are received (if used)
- GRE is the default tunnel mode.

QUESTION 83:
The following output was displayed on a Certkiller router:

```
interface: FastEthernet0/1
      crypto map tag: MYMAP, local addr. 172.30.1.2
      lacal ident (addn/mask/prot/port):
(172.30.1.2/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port):
(172.30.2.2/255.255.255.255/0/0)
      current_peer: 172.30.2.2
       PERMIT, flags=(origin_is_acl,)
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
     #pkts decaps: 0,  #pkts decrypt:0,  #pkts verify 0
      #send errors 0, #recv errors 0
local crypto endpt. 172.30.1.2, remote crypto endpt.: 172.30.2.2
      path mtu 1500, media mtu 1500
      current outbound spi: 0
      inbound esp sas:
      inbound ah sas:
      outbound esp sas:
      outbound ah sas:
```

Based on the output shown above, what command was issued?

A. debug crypto ipsec
B. show crypto map
C. show crypto ipsec sa
D. show crypto ipsec transform-set

E. None of the above

Answer: C

Explanation:
show crypto ipsec sa : To display the settings used by current SAs. Non-zero encryption and decryption statistics can indicate a working set of IPSec SAs.

QUESTION 84:
Part of the configuration file of a Certkiller router is shown below:

```
interface Tunnel0
 no ip address
 tunnel source Serial1/0
 tunnel destination 150.0.0.2

!
interface Serial1/0
 ip address 150.0.0.1 255.255.255.0
 crypto map toBB
```

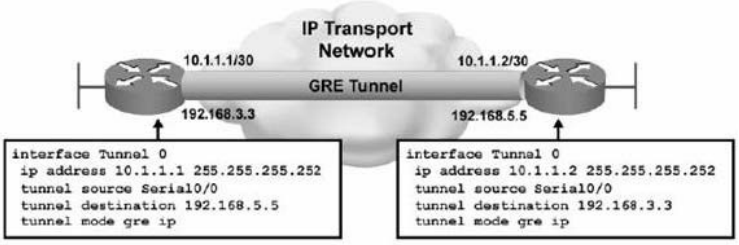
Given the partial configuration that is shown above, which tunneling encapsulation is used?

A. DVMRP
B. cayman
C. GRE multipoint
D. GRE
E. None of the above

Answer: D

Explanation:
Tunnels provide logical, point-to-point connections across a connectionless IP network. This enables the use of advanced security features. Tunnels for VPN solutions employ encryption to protect data from being viewed by unauthorized entities and to perform multiprotocol encapsulation, if necessary. Encryption is applied to the tunneled

connection to make data legible only to authorized senders and receivers



- GRE tunnel is up and protocol up if:
  - Tunnel source and destination are configured
  - Tunnel destination is in routing table
  - GRE keepalives are received (if used)
- GRE is the default tunnel mode.

QUESTION 85:

Study the exhibit regarding RouterA in the Certkiller network below:

```
RouterA# show crypto isakmp policy
Protection suite priority 15
      encryption algorithm:  DES - Data Encryption Standard (56 bit keys)
      hash algorithm:        Message Digest 5
      authentication method: Rivest-Shamir-Adleman Signature
      Diffie-Hellman Group:  #2 (1024 bit)
      lifetime:              5000 seconds, no volume limit
Protection suite priority 20
      encryption algorithm:  DES - Data Encryption Standard (56 bit keys)
      hash algorithm:        Secure Hash Standard
      authentication method: preshared Key
      Diffie-Hellman Group:  #1 (768 bit)
      lifetime:              10000 seconds, no volume limit
Protection suite of priority 110
      encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
      hash algorithm:        Message Digest 5
      authentication method: Rivest-Shamir-Adleman Encryption
      Diffie-Hellman group:  #1 (768 bit)
      lifetime:              86400 seconds, no volume limit
Default protection suite
      encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
      hash algorithm:        Secure Hash Standard
      authentication method: Rivest-Shamir-Adleman Signature
```

Based on the information shown above, how many IKE policies were administratively defined above?

A. 0
B. 1
C. 2
D. 3
E. 4

Answer: D

Explanation:
There are three policies in the exhibit (using priority 15, 20 and 110, respectively) which were manually configured on this router. The default policy is not explicitly defined, and is included as the default IKE parameters on Cisco IP Sec routers.

QUESTION 86:

Two Certkiller locations are trying to connect to each other over a VPN, but the

connection is failing. Which common problem causes an IPSEC VPN to fail?

A. ACLs configured in the IPSEC traffic path blocking ISAKMP, ESP, and AH traffic.
B. Multiple transform sets configured but only one transform set is specified in the crypto map entry.
C. Crypto ACL configuration errors where permit is used to specify that matching packets must be encrypted.
D. Multiple interfaces sharing the same crypto map set.
E. None of the above

Answer: A

Explanation:
By default, IPSec and all packets that traverse the PIX Firewall are subjected to blocking as specified by inbound conduit, outbound list or interface access-list. To enable IPSec packets to traverse the PIX Firewall, ensure that you have statements in conduits, outbound lists or interface access-lists that permit the packets. The same holds true for IPSec routers that have access lists configured.
IKE uses UDP port 500. The IPSec ESP and AH protocols use protocol numbers 50 and 51.
Ensure your access lists are configured so that protocol 50, 51 and UDP port 500 traffic is not blocked at interfaces used by IPSec. In some cases you may be required to add a statement to your access lists to explicitly permit this traffic.

QUESTION 87:
An IPSec tunnel has just been created on the Certkiller network, and you wish to verify it. Which command will display the configured IKE policies?

A. show crypto isakmp policy
B. show crypto ipsec
C. show crypto isakmp
D. show crypto map
E. None of the above

Answer: A

Explanation:
To display the parameters for each Internet Key Exchange (IKE) policy, use the show crypto isakmp policy command in EXEC mode.
The following is sample output from the show crypto isakmp policy command after two IKE policies have been configured (with priorities 15 and 20, respectively):
CK1 # show crypto isakmp policy
Protection suite priority 15
encryption algorithm: DES - Data Encryption Standard (56 bit keys)
hash algorithm: Message Digest 5
authentication method: Rivest-Shamir-Adleman Signature

Diffie-Hellman Group: #2 (1024 bit)
lifetime: 5000 seconds, no volume limit
Protection suite priority 20
encryption algorithm: DES - Data Encryption Standard (56 bit keys)
hash algorithm: Secure Hash Standard
authentication method: preshared Key
Diffie-Hellman Group: #1 (768 bit)
lifetime: 10000 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys)
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman Group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit

QUESTION 88:
While troubleshooting an IPSec VPN, the following was seen on router R1:

Refer to the graphic. Which configuration statements match the debug output shown above?

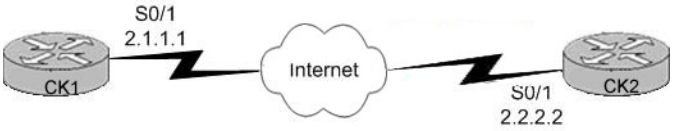
A. crypto isakmp policy 100
encr aes
authentication rsa-encr
group 5
B. crypto isakmp policy 100
encr 3des
authentication pre-share
group 2
C. crypto isakmp policy 100
hash md5

authentication rsa-sig
D. crypto isakmp policu 100
encr des
lifetime 7200
E. crypto isakmp policy 100
hash md5
group 1
lifetime 7200

Answer: B

Explanation:
The answer lies near the bottom of the output, where it states "found peer pre-shared key matching 10.1.1.1" and "local preshared key found." Choice B is the only choice that is configured for using pre-shared key authentication.

QUESTION 89:
The Certkiller network is shown in the following exhibit:




```
CK1#show crypto isakmp sa
dst       src       state      conn-id slot
2.1.1.1   2.2.2.2   QM_IDLE          3    0
```

Refer to the exhibit above. A network administrator is verifying a site-to-site IPSec VPN configuration. Based on the output shown, what must be true about CK1 and CK2 ?

A. CK1 and CK2 have not completed IKE Phase 1.
B. CK1 and CK2 have not completed IKE Phase 2.
C. CK1 and CK2 are authenticated IKE peers.
D. CK1 and CK2 maintain unidirectional IPSec SAs with each other.
E. CK1 and CK2 have timed out their IPSec SAs.

Answer: C

Explanation:
The QM idle is the normal operating state of the secrurity association (SA).
The following is sample output from the show crypto isakmp sa command after IKE negotiations have been successfully completed between two peers:
Router# show crypto isakmp saf_vrf/i_vrf dst src state conn-id
slot /vpn2 172.21.114.123 10.1.1.1 QM_IDLE 13 0Table29 through
Table32 show the various states that may be displayed in the output of the show crypto isakmp sa command. When an Internet Security Association and Key Management Protocol (ISAKMP) SA exists, it will most likely be in its quiescent state (QM_IDLE). For long exchanges, some of the MM_xxx states may be observed.

Table 29 States in Main Mode Exchange

State	Explanation
MM_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is "larval" at this stage—there is no state.
MM_SA_SETUP	The peers have agreed on parameters for the ISAKMP SA.
MM_KEY_EXCH	The peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated.
MM_KEY_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transtions immediately to QM_IDLE, and a Quick Mode exchange begins.

Table 30 States in Aggressive Mode Exchange

State	Explanation
AG_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is "larval" at this stage—there is no state.
AG_INIT_EXCH	The peers have done the first exchange in aggressive mode, but the SA is not authenticated.
AG_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE, and a quick mode exchange begins.

Table 31 States in Quick Mode Exchange

State	Explanation
QM_IDLE	**The ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent quick mode exchanges. It is in a quiescent state.**

Table 32 show crypto isakmp sa Field Descriptions

Field	Description
f_vrf/i_vrf	The front door virtual routing and forwarding (FVRF) and the inside VRF (IVRF) of the IKE SA. If the FVRF is global, the output shows f_vrf as an empty field.

Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_chapter09186a008017

QUESTION 90:
EIGRP is being used in the Certkiller IPSev VPN. When configuring an IPsec VPN to backup a WAN connection, what can be configured to influence the EIGRP routing process to select the primary WAN link over the backup IPsec tunnel?

A. Configure the EIGRP variance to 2.
B. Configure a longer delay value on the tunnel interface.
C. Configure the EIGRP variance to 1.
D. Configure a longer EIGRP hello interval on the tunnel interface.
E. Configure a lower clock rate value on the tunnel interface.
F. Configure a higher bandwidth value on the tunnel interface.
G. None of the above

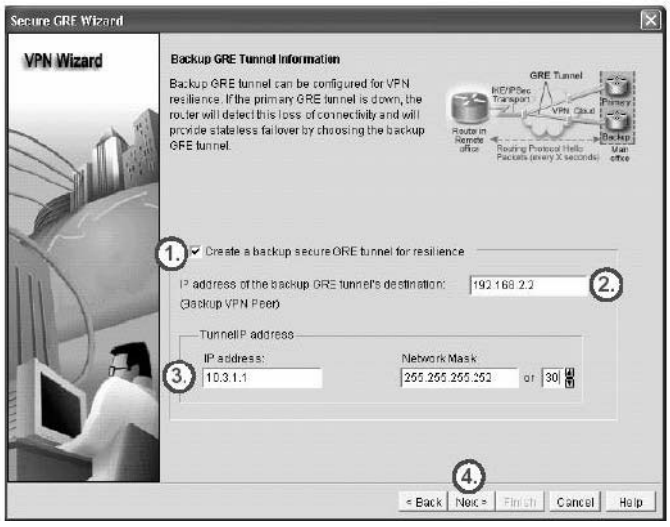
Answer: B

QUESTION 91:
In order to increase the uptime of the network, you have been tasked with designing and configuring a fault tolerant IPSec WAN. What can be configured to provide resiliency when using SDM to configure a site-to-site GRE over IPsec VPN tunnel?

A. A backup GRE over IPsec tunnel
B. Redundant dynamic crypto maps
C. HSRP
D. Load balancing using two GRE over IPsec tunnels
E. Stateful IPsec failover

Answer: A

Explanation:
Optionally, you can create a second GRE tunnel that will be used in case the primary tunnel fails:
Step 1 Check Create a backup secure GRE tunnel for resilience.
Step 2 Define the IP address of the backup VPN peer.
Step 3 Define the inner IP address and the subnet mask for the logical tunnel interface.
Step 4 Click the Next button to proceed to the next task.



QUESTION 92:
You need to increase the network availability of the Certkiller IPSec WAN. Which high availability option uses the concept of a virtual IP address to ensure that the default IP gateway for an IPsec site-to-site tunnel is always reachable?

A. Reverse Route Injection (RRI)
B. Dynamic Crypto Map
C. Backup IPsec peer
D. HSRP
E. GRE over IPsec
F. None of the above

Answer: D

Explanation:
IPsec VPNs can experience any one of a number of different typesof failures:
-Access link failure
-Remote peer failure
-Device failure
IPsec should be designed and implemented with redundancy and high-availability mechanisms to mitigate these failures.
IPsec-based VPNs provide connectivity between distant sites using an untrusted transport network. Network connectivity consists of links, devices, or sometimes just paths across networks whose topology is not known. Any of these components can fail, making the VPN inoperable. IPsec VPNs requiring high availability should be designed and implemented with redundancy in order to survive failures.
HSRP can be used at:
-Head end: Two head-end IPsec devices appear as one to remote peers
- Remote site: Two IPsec gateways appear as one to local devices
Active HSRP device uses a virtual IP and MAC address. Standby HSRP device takes over virtual IP and MAC address when active HSRP device goes down. HSRP Operation
A large class of legacy hosts that do not support dynamic router discovery are typically configured with a default gateway (router). Running a dynamic router discovery mechanism on every host may not be feasible for a number of reasons, including administrative overhead, processing overhead, security issues, or lack of a protocol implementation for some platforms. HSRP provides failover services to these hosts.
Using HSRP, a set of routers works in concert to present the illusion of a single virtual router to the hosts on the LAN. This set of routers is known as an HSRP group or a standby group. A single router elected from the group is responsible for forwarding the packets that hosts send to the virtual router. This router is known as the active router. Another router is elected as the standby router. In the event that the active router fails, the standby router assumes the packet-forwarding duties of the active router. Although an arbitrary number of routers may run HSRP, only the active router forwards the packets sent to the virtual router. To minimize network traffic, only the active and standby routers send periodic HSRP messages after the protocol has completed the election process. If the active router fails, the standby router takes over as the active router. If the standby router fails or becomes the active router, another router is elected as the standby router. On a particular LAN, multiple hot standby groups may coexist and overlap. Each standby group emulates a single virtual router. The individual routers may participate in multiple groups. In this case, the router maintains separate state and timers for each group. Each standby group has a single, well-known MAC address as well as an IP address.

QUESTION 93:
You have been assigned the task of setting up Easy VPN connection in the Certkiller network. During the Easy VPN Remote connection process, which phase involves pushing the IP address, Domain Name System (DNS), and split tunnel attributes to

the client?

A. The VPN client establishment of an ISAKMP SA
B. Mode configuration
C. VPN client initiation of the IKE phase 1 process
D. IPsec quick mode completion of the connection
E. None of the above

Answer: B

Explanation:
1.
If the Easy VPN Server indicates successful authentication, the VPN client requests the remaining configuration parameters from the Easy VPN Server:
2. Mode configuration starts.
3. The remaining system parameters (IP address, DNS, split tunneling information, and so on) are downloaded to the VPN client.
4. Remember that the IP address is the only required parameter in agroup profile; all other parameters are optional.
The remaining system parameters (IP address, Domain Name System [DNS], split tunnel attributes, and so on) are pushed to the VPN client at this time using mode configuration. The IP address is the only required parameter in a group profile; all other parameters are optional.

QUESTION 94:
You need to configure a new Certkiller remote location to connect to corporate using Easy VPN. Which two statements about Cisco Easy VPN are true? (Select two)

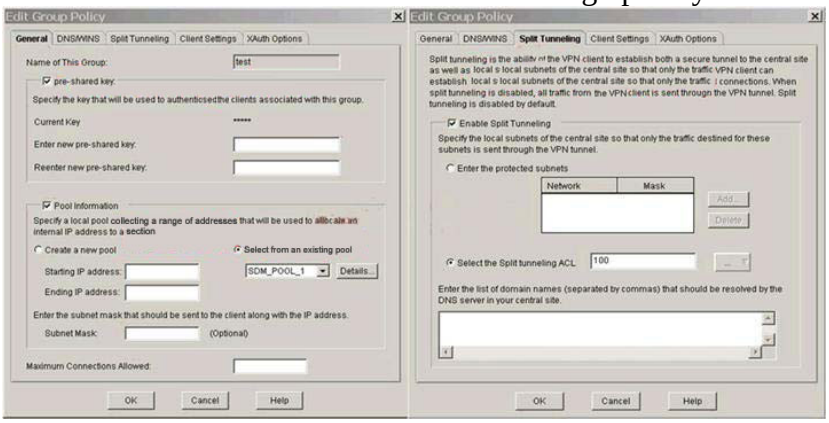
A. Easy VPN is only appropriate for smaller deployments.
B. Easy VPN tunnel endpoint addresses can be the virtual IP address of an HSRP configuration.
C. Easy VPN does not support split tunnels.
D. An IOS router, a PIX firewall or a VPN client can operate as an Easy VPN terminal point.
E. A VPN client can also be configured to operate as an Easy VPN server.

Answer: B, D

Explanation:
Cisco Easy VPN has two main functions:
-Simplify client configuration
-Centralize client configuration and dynamically push the configuration to clients
How are these two goals achieved ?
-IKE Mode Config functionality is used to download some configuration parameters to clients.
-Clients are preconfigured with a set of IKE policies and IPsec transform sets.

Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of the two routers. The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing the Cisco Unity Client protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN Server. This server can be a dedicated VPN device, such as a Cisco VPN 3000 Concentrator, a Cisco PIX Firewall, or a Cisco IOS router that supports the Cisco Unity Client protocol.
After the Cisco Easy VPN Server has been configured, a VPN connection can be created with minimal configuration on an Easy VPN Remote client, such as a Cisco 800 Series router or a Cisco 1700 Series router. When the Easy VPN Remote initiates the VPN tunnel connection, the Cisco Easy VPN Server pushes the IPsec policies to the Easy VPN Remote client and creates the corresponding VPN tunnel connection.

QUESTION 95:
The Certkiller network administrator is setting up Easy VPN as shown below:



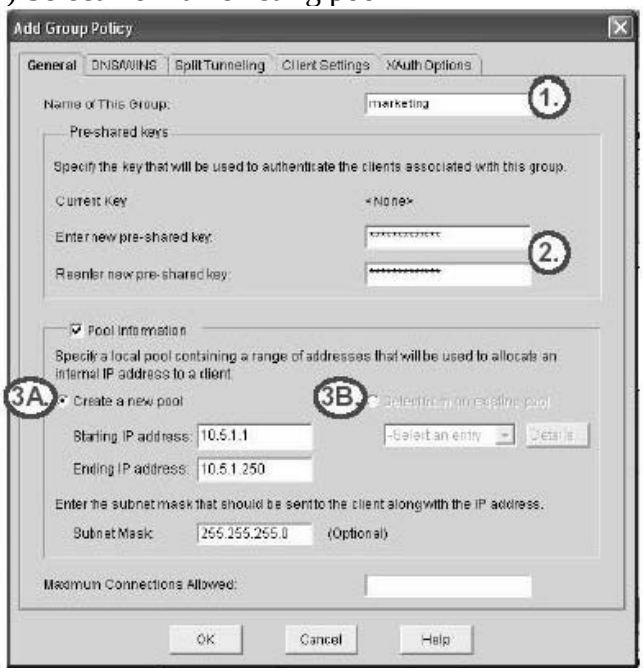
Based on the exhibit above, which two statements are true about the Easy VPN Server configuration that is shown? (Select two)

A. Split tunneling is disabled because no protected subnets have been defined.
B. To connect, the remote VPN client will use a groupname of "test."
C. Digital Certificate is used to authenticate the remote VPN client.
D. The remote VPN client will be assigned an internal IP address from the SDM_POOL_1 IP address pool.
E. Split tunneling is enabled where traffic that matches ACL 100 will not be encrypted.

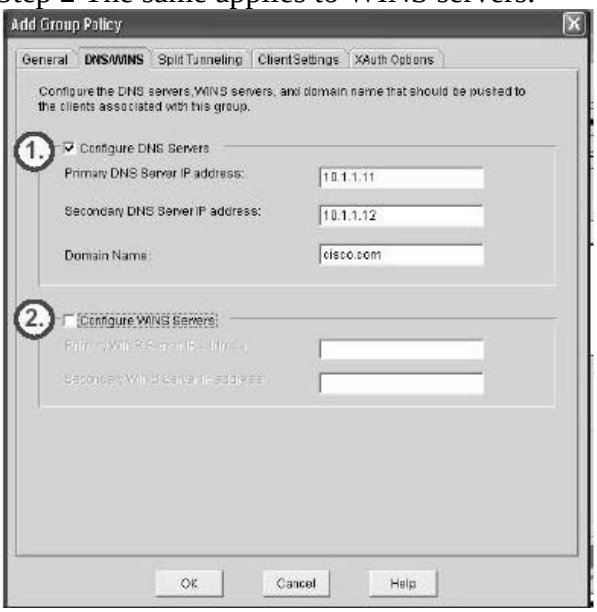
Answer: B, D

Explanation:
Use the General tab to configure the minimum required parameters for a functional group policy:
Step 1 Define a name of the group.

Step 2 Enter the preshared secret for the group.
Step 3 Specify an IP address pool from which addresses will be taken and assigned to clients. You have these two options:
A) Create a new pool
B) Select from an existing pool

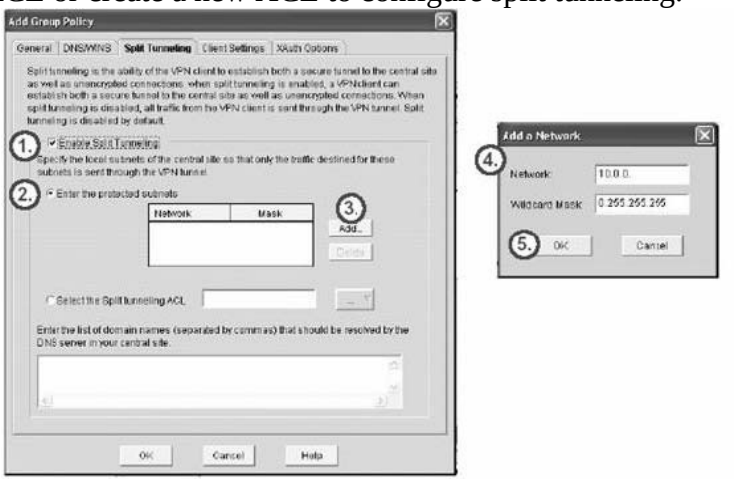


1.2. Select the DNS/WINS tab to configure the DNS and WINS servers:
Step 1 You should specify any internal DNS servers that may be required by clients in order to be able to resolve hostnames that are only reachable inside the VPN.
Step 2 The same applies to WINS servers.

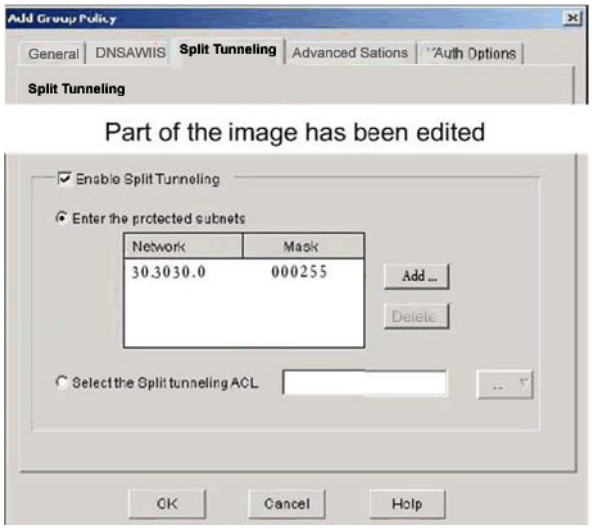


You should keep split tunneling disabled (default) to prevent any compromised client PC from becoming a proxy between the Internet and the VPN.
If, however, split tunneling is required, you should complete one of the following two

configuration options on the Split Tunneling tab:
Step 1 Check the Enable Split Tunneling check box.
Step 2 Click the Enter the protected subnets radio button.
Step 3 Click Add to add a network.
Step 4 In the Add a Network window, define protected networks (all other destinations will be reachable by bypassing the tunnel).
Step 5 Click OK.
Alternatively, click the Select the Split tunneling ACL radio button to use an existing ACL or create a new ACL to configure split tunneling.



QUESTION 96:
The Certkiller network administrator used SDM to configure a new router as shown below:



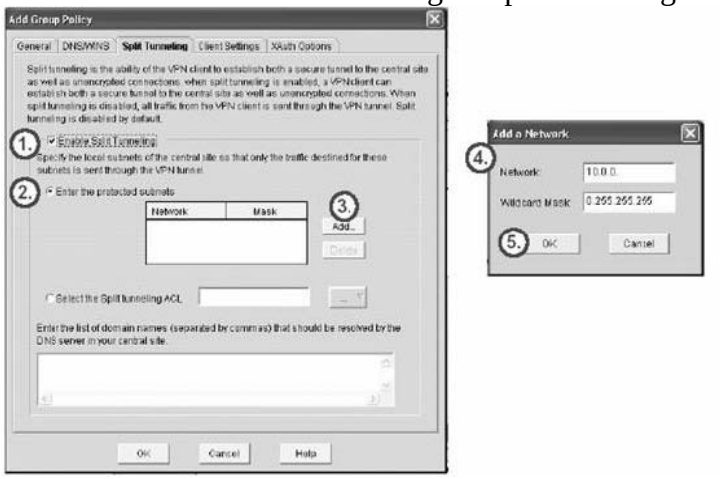
Which statement is true about the configuration of split tunnels using SDM?

A. Any protected subnets that are entered represent subnets at the VPN server site that will be accessed without going through the encrypted tunnel.
B. Any protected subnets that are entered represent subnets at the VPN server site that will be accessed through the encrypted tunnel.
C. Any protected subnets that are entered represent subnets at the end user's site that will

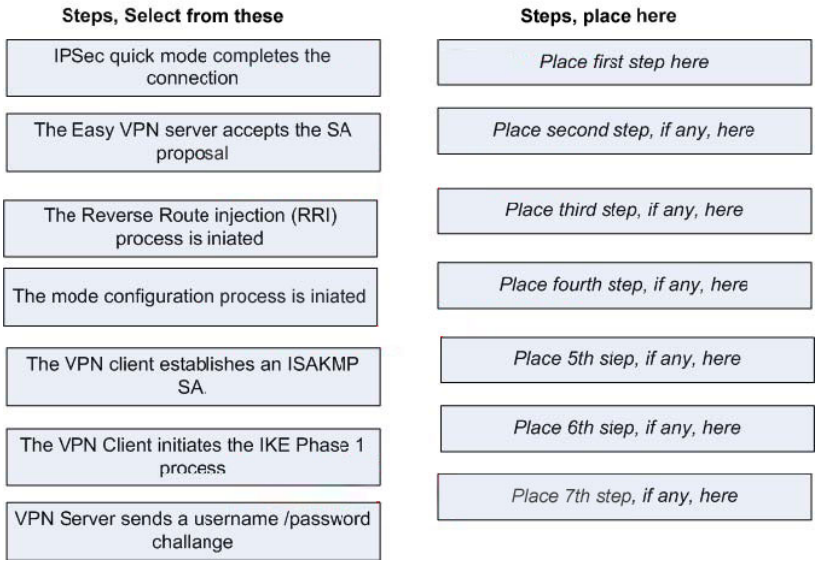
be accessed through the encrypted tunnel.
D. Any protected subnets that are entered represent subnets at the end user's site that will be accessed without going through the encrypted tunnel.

Answer: B

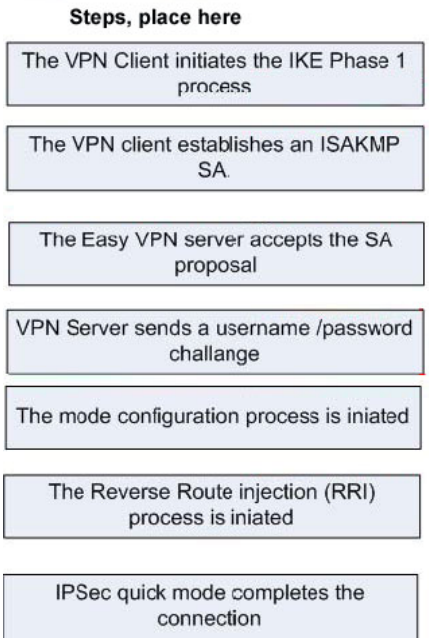
Explanation:
You should keep split tunneling disabled (default) to prevent any compromised client PC from becoming a proxy between the Internet and the VPN.
If, however, split tunneling is required, you should complete one of the following two configuration options on the Split Tunneling tab:
Step 1 Check the Enable Split Tunneling check box.
Step 2 Click the Enter the protected subnets radio button.
Step 3 Click Add to add a network.
Step 4 In the Add a Network window, define protected networks (all other destinations will be reachable by bypassing the tunnel).
Step 5 Click OK.
Alternatively, click the Select the Split tunneling ACL radio button to use an existing ACL or create a new ACL to configure split tunneling.



QUESTION 97:
DRAG DROP
You need to explain the Easy VPN connection process steps to a junior Certkiller network administrator. Drag each Cisco Easy VPN connection process on the left to its step on the right.



Answer:



QUESTION 98:

You need to configure Easy VPN on a new Certkiller router using the SDM. Which two statements are true about the use of SDM to configure the Cisco Easy VPN feature on a router? (Select two)

A. The Easy VPN server address must be configured when configuring the SDM Easy VPN Server wizard.
B. An Easy VPN connection is a connection that is configured between two Easy VPN clients.
C. The SDM Easy VPN Server wizard displays a summary of the configuration before applying the VPN configuration.

D. The SDM Easy VPN Server wizard recommends using the Quick setup feature when configuring a dynamic multipoint VPN.
E. The SDM Easy VPN Server wizard can be used to configure user XAuth authentication locally on the router or externally with a RADIUS server.
F. The SDM Easy VPN Server wizard can be used to configure a GRE over IPSec site-to-site VPN or a dynamic multipoint VPN (DMVPN).

Answer: C, E

Explanation:
Cisco Easy VPN has two main functions:
-Simplify client configuration
-Centralize client configuration and dynamically push the configuration to clients
How are these two goals achieved ?
-IKE Mode Config functionality is used to download some configuration parameters to clients.
-Clients are preconfigured with a set of IKE policies and IPsec transform sets.
Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of the two routers. The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing the Cisco Unity Client protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN Server. This server can be a dedicated VPN device, such as a Cisco VPN 3000 Concentrator, a Cisco PIX Firewall, or a Cisco IOS router that supports the Cisco Unity Client protocol.
After the Cisco Easy VPN Server has been configured, a VPN connection can be created with minimal configuration on an Easy VPN Remote client, such as a Cisco 800 Series router or a Cisco 1700 Series router. When the Easy VPN Remote initiates the VPN tunnel connection, the Cisco Easy VPN Server pushes the IPsec policies to the Easy VPN Remote client and creates the corresponding VPN tunnel connection.

QUESTION 99:
Certkiller uses the Easy VPN feature to connect remote users to the corporate network. Which three statements about the Cisco Easy VPN feature are true? (Select three)

A. If the VPN server is configured for Xauth, the VPN client waits for a username / password challenge.
B. The VPN client initiates aggressive mode (AM) if a pre-shared key is used for authentication during the IKE phase 1 process.
C. When connecting with a VPN client, the VPN server must be configured for ISAKMP group 1, 2 or 5.
D. The Cisco Easy VPN feature only supports transform sets that provide authentication

and encryption.
E. The VPN server can only be enabled on Cisco PIX Firewalls and Cisco VPN 3000 series concentrators.
F. The VPN client verifies a server username/password challenge by using a AAA authentication server that supports TACACS+ or RADIUS.

Answer: A, B, D

Explanation:
Cisco Easy VPN has two main functions:
-Simplify client configuration
-Centralize client configuration and dynamically push the configuration to clients
How are these two goals achieved ?
-IKE Mode Config functionality is used to download some configuration parameters to clients.
-Clients are preconfigured with a set of IKE policies and IPsec transform sets.
Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of the two routers. The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing the Cisco Unity Client protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN Server. This server can be a dedicated VPN device, such as a Cisco VPN 3000 Concentrator, a Cisco PIX Firewall, or a Cisco IOS router that supports the Cisco Unity Client protocol.
After the Cisco Easy VPN Server has been configured, a VPN connection can be created with minimal configuration on an Easy VPN Remote client, such as a Cisco 800 Series router or a Cisco 1700 Series router. When the Easy VPN Remote initiates the VPN tunnel connection, the Cisco Easy VPN Server pushes the IPsec policies to the Easy VPN Remote client and creates the corresponding VPN tunnel connection.
If the Easy VPN Server is configured for Xauth, the VPN client waits for a username/password challenge:
-The user enters a username/password combination.
-The username/password information is checked against authentication entities using AAA.
All Easy VPN Servers should be configured to enforce user authentication

---

QUESTION 100:
A new Certkiller router was configured as shown in the exhibit below:

```
CertKiller1(config)#ip inspect tcp synwait-time 30
CertKiller1(config)#ip inspect tcp finwait-time 5
CertKiller1(config)#ip inspect tcp idle-time 3600
CertKiller1(config)#ip inspect udp idle-time 30
CertKiller1(config)#ip inspect dns-timeout 5
CertKiller1(config)#ip inspect max-incomplete high 500
CertKiller1(config)#ip inspect max-incomplete low 400
CertKiller1(config)#ip inspect one-minute high 500
CertKiller1(config)#ip inspect one-minute low 400
CertKiller1(config)#ip inspect tcp max-incomplete host 50 block-time 0
```

Based on the information above, what two types of attacks does this IOS firewall configuration prevent? (Selcet two)

A. Trojan horse
B. Java applets
C. DDOS
D. SYN flood
E. packet sniffers

Answer: C, D

Explanation:
Denial of Service (DoS) is an attack designed to render a computer or network incapable of providing normal services. The most common DoS attacks will target the computer's network bandwidth or connectivity. Bandwidth attacks flood the network with such a high volume of traffic, that all available network resources are consumed and legitimate user requests cannot get through. Connectivity attacks flood a computer with such a high volume of connection requests, that all available operating system resources are consumed and the computer can no longer process legitimate user requests.
A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include
* attempts to "flood" a network, thereby preventing legitimate network traffic
*
attempts to disrupt connections between two machines, thereby preventing access to a service
* attempts to prevent a particular individual from accessing a service
* attempts to disrupt service to a specific system or person
SYN flood is an asymmetric resource starvation attack in which the attacker floods the victim with TCP SYN packets and the victim allocates resources to accept perceived incoming connections. As mentioned above, the proposed Host Identity Payload and Protocol (HIP) are designed to mitigate the effects of a SYN flood attack. Another technique, SYN Cookies (see http://cr.yp.to/syncookies.html), is implemented in some TCP/IP stacks.
1. ipinspect tcp synwait-time To define how long the software will wait for a TCP session to reach the established state before dropping the session, use the ip inspect tcp synwait-time command in global configuration mode
2. ipinspect tcp finwait-time To define how long a TCP session will still be managed

after the firewall detects a FIN-exchange, use the ipinspect tcp finwait-time command in global configuration mode. To reset the timeout to the default of 5 seconds, use the no form of this command.
ip inspect tcp finwait-time seconds [vrf vrf-name]
no ip inspect tcp finwait-time
3. ipinspect tcp idle-time To specify the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity), use the ip inspect tcp idle-time command in global configuration mode. To reset the timeout to the default of 3600 seconds (1 hour), use the no form of this command.
ip inspect tcp idle-time seconds [vrf vrf-name]
no ip inspect tcp idle-time
4. ipinspect dns-timeout To specify the Domain Name System (DNS) idle timeout (the length of time during which a DNS name lookup session will still be managed while there is no activity), use the ip inspect dns-timeout command in global configuration mode. To reset the timeout to the default of 5 seconds, use the no form of this command.
ip inspect dns-timeout seconds [vrf vrf-name]
no ip inspect dns-timeout seconds [vrf vrf-name]
5. ipinspect max-incomplete high To define the number of existing half-open sessions that will cause the software to start deleting half-open sessions, use the ip inspect max-incomplete high command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the no form of this command.
ip inspect max-incomplete high number [vrf vrf-name]
no ip inspect max-incomplete high
6. ipinspect max-incomplete low To define the number of existing half-open sessions that will cause the software to stop deleting half-open sessions, use the ip inspect max-incomplete low command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the no form of this command.
ip inspect max-incomplete low number [vrf vrf-name]
no ip inspect max-incomplete low
7. ipinspect tcp max-incomplete host To specify threshold and blocking time values for TCP host-specific denial-of-service (DoS) detection and prevention, use the ip inspect tcp max-incomplete host command in global configuration mode. To reset the threshold and blocking time to the default values, use the no form of this command.
ip inspect tcp max-incomplete host number block-time minutes [vrf vrf-name]
no ip inspect tcp max-incomplete host

QUESTION 101:
The Certkiller security administrator is concerned about network attacks. Which two network attack statements are true? (Select two)

A. Access attacks can consist of UDP and TCP SYN flooding, ICMP echo-request floods, and ICMP directed broadcasts.
B. IP spoofing can be reduced through the use of policy-based routing.
C. DoS attacks can be reduced through the use of access control configuration, encryption, and RFC 2827 filtering.
D. DoS attacks can consist of IP spoofing and DDoS attacks.

E. IP spoofing exploits known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information.
F. Access attacks can consist of password attacks, trust exploitation, port redirection, and man-in-the-middle attacks.

Answer: D, F

Explanation:
An attack against an enterprise network occurs in several stages. In the initial stages, the attacker may have only limited information about the target. One of the primary attacker objectives is to gather intelligence about the target vulnerabilities. The process of unauthorized collection of information about the network weaknesses is called a reconnaissance attack.
Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information.
DoS attacks are one of the most publicized forms of attack, and are also among the most difficult to completely eliminate. They can employ various techniques, such as overwhelming network resources, to render systems unavailable or reduce their functionality. A DoS attack on a server sends extremely large volumes of requests over a network or the Internet. These large volumes of requests cause the attacked server to dramatically slow down, resulting in the attacked server becoming unavailable for legitimate access and use. Distributed DoS attacks are the "next generation" of DoS attacks on the Internet. Victims of distributed DoS attacks experience packet flooding from many different sources (possibly spoofed IP source addresses) that overwhelm the network connectivity. In the past, the typical DoS attack involved a single attempt to flood a target host with packets. With distributed DoS tools, an attacker can conduct the same attack using thousands of systems.

QUESTION 102:
The Certkiller security administrator is concerned about the use of aunauthorized packet sniffers on the network. Which two statements below about packet sniffers or packet sniffing are true? (Select two)

A. To reduce the risk of packet sniffing, cryptographic protocols such as Secure Shell Protocol (SSH) and Secure Sockets Layer (SSL) should be used.
B. Packet sniffers can only work in a switched Ethernet environment.
C. To reduce the risk of packet sniffing, traffic rate limiting and RFC 2827 filtering should be used.
D. A packet sniffer requires the use of a network adapter card in nonpromiscuous mode to capture all network packets that are sent across a LAN.
E. To reduce the risk of packet sniffing, strong authentication, such as one time passwords, should be used.

Answer: A, E

Explanation:
A packet sniffer is a software application that uses a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN. Packet sniffers can only work in the same collision domain. Promiscuous mode is a mode in which the network adapter card sends all packets received on the physical network wire to an application for processing. Plaintext is information sent across the network that is not encrypted. Some network applications distribute network packets in plaintext. Because the network packets are not encrypted, they can be processed and understood by any application that can pick them off the network and process them.
A network protocol specifies the protocol operations and packet format. Because the specifications for network protocols, such as TCP/IP, are widely published, a third party can easily interpret the network packets and develop a packet sniffer. Numerous freeware and shareware packet sniffers are available that do not require the user to understand anything about the underlying
Configuration management is an essential component of the network availability. Therefore, its security is of paramount importance. You should use secure management protocols when configuring all network devices. Some management protocols, such as SSH and SSL, have been designed with security in mind and can be used in the management solution. Other protocols, such as Telnet and Simple Network Management Protocol version 2 (SNMPv2), must be made secure by protecting the data with IPsec. IPsec provides the encryption and authentication needed to combat an attacker who tries to compromise the data exchange. You should use access lists to further limit connectivity to the network devices and hosts. The access lists should permit management access, such as SSH or HTTPS, only from the legitimate management hosts.

QUESTION 103:
The security administrator is implementing Cisco tools to mitigate the risks of network attacks. Which two statements about common network attacks are true? (Select two)

A. Access attacks can consist of password attacks, trust exploitation, port redirection, and man-in-the-middle attacks.
B. Reconnaissance attacks can consist of password attacks, trust exploitation, port redirection and Internet information queries.
C. Access attacks can consist of password attacks, ping sweeps, port scans, and man-in-the-middle attacks.
D. Reconnaissance attacks can consist of packet sniffers, port scans, ping sweeps, and Internet information queries.
E. Reconnaissance attacks can consist of ping sweeps, port scans, man-in-middle attacks and Internet information queries.
F. Access attacks can consist of packet sniffers, ping sweeps, port scans, and man-in-the-middle attacks.

Answer: A, D

Explanation:
Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. Reconnaissance is also known as information gathering, and in most cases, precedes an actual access or DoS attack. First, the malicious intruder typically conducts a ping sweep of the target network to determine which IP addresses are alive. Then, the intruder determines which services or ports are active on the live IP addresses. From this information, the intruder queries the ports to determine the type and version of the application and operating system running on the target host. In many cases, the intruders look for vulnerable services that they can exploit later when there is less likelihood that anyone is looking. Reconnaissance is somewhat analogous to a thief surveying a neighborhood for vulnerable homes, such as an unoccupied residence, or a house with an easy-to-open door or window to break into. Reconnaissance attacks can consist of the following:
* Packet sniffers
* Port scans
* Ping sweeps
* Internet information queries
Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information.

QUESTION 104:
The Certkiller security administrator is concerned about reconnaissance attacks.
Which two protocols can be used to prevent a reconnaissance attack? (Select two)

A. IPsec
B. NTP
C. SNMP
D. SSH
E. Telnet
F. FTP

Answer: A, D

Explanation:
Configuration management is an essential component of the network availability. Therefore, its security is of paramount importance. You should use secure management protocols when configuring all network devices. Some management protocols, such as SSH and SSL, have been designed with security in mind and can be used in the management solution. Other protocols, such as Telnet and Simple Network Management Protocol version 2 (SNMPv2), must be made secure by protecting the data with IPsec. IPsec provides the encryption and authentication needed to combat an attacker who tries to compromise the data exchange.

QUESTION 105:
You want to be sure to protect the Certkiller network against reconnaissance

attacks. What technique can help to counter a reconnaissance attack?

A. Implement a switched infrastructure.
B. Disable port redirection.
C. Disable accounts after a specific number of unsuccessful logins.
D. Configure RFC 2827 filtering.
E. None of the above.

Answer: A

Explanation:
Switched Infrastructure
This technology, very common today, counters the use of packet sniffers in the network environment. If an entire organization deploys switched Ethernet, hackers can gain access only to the traffic that flows on the specific port to which they connect. A switched infrastructure obviously does not eliminate the threat of packet sniffers, but it can greatly reduce their effectiveness.

QUESTION 106:
The Certkiller network is concerned about security attacks. Which can be used to mitigate Trojan horse attacks?

A. RFC 2827 filtering
B. Implementation of traffic rate limiting
C. The disabling of port redirection
D. The use of antivirus software
E. Implementing anti-DoS features
F. None of the above

Answer: D

Explanation:
Antivirus software can detect most viruses and many Trojan horse applications and prevent them from spreading in the network. Keeping up-to-date with the latest developments in these sorts of attacks can also lead to a more effective posture against these attacks. As new virus or Trojan horse applications are released, enterprises need to keep up-to-date with the latest antivirus software and application versions and patches. Deploying host-based intrusion prevention systems, such as the Cisco Security Agent (CSA), provides a very effective defense-in-depth method to prevent attacks against the hosts.

QUESTION 107:
The Certkiller security administrator is researching ways to prevent worm attacks on Certkiller devices. What is a possible way to prevent a worm attack on a host PC?

A. Implement TACACS+.

B. Enable SSH.
C. Enable encryption.
D. Keep the operating system current with the latest patches.
E. None of the above.

Answer: D

Explanation:
Application Layer Attacks
These are some of the measures that you can take to reduce your risks:
* Read operating system and network log files or have them analyzed. It is important to review all logs and take action accordingly.
* Subscribe to mailing lists that publicize vulnerabilities. Most application and operating system vulnerabilities are published on the web by various sources.
* Keep your operating system and applications current with the latest patches. Always test patches and fixes in a nonproduction environment. This practice prevents downtime and keeps errors from being generated unnecessarily.
* Use IDS, IPS, or both to scan for known attacks, monitor and log attacks, and ultimately prevent attacks. Using these systems is essential to identifying security threats and mitigating some of these threats. In most cases, mitigation can be done automatically.

QUESTION 108:
The Certkiller security administrator is implementing Cisco devices to mitigate the threat of worms and viruses. Which two statements about worms, viruses, or Trojan horses are true? (Select two)

A. A virus cannot spread to a new computer without human assistance.
B. A worm can spread itself automatically from one computer to the next over an unprotected network.
C. A virus has three components: an enabling vulnerability, a propagation mechanism, and a payload.
D. A Trojan horse virus propagates itself by infecting other programs on the same computer.
E. A Trojan horse has three components: an enabling vulnerability, a propagation mechanism, and a payload.
F. A worm is a program that appears desirable but actually contains something harmful.

Answer: A, B

Explanation:
* Viruses are malicious software programs that are attached to other programs and which execute a particular unwanted function on a user workstation. A virus propagates itself by infecting other programs on the same computer. Viruses can do serious damage, such as erasing files or erasing an entire disk. They can also be a simple annoyance, such as popping up a window that says "Ha, ha, you are infected." Viruses cannot spread to a new computer without human assistance, for example, opening an infected file on a

removable media such as an e-mail attachment, or through file sharing.
* A worm executes arbitrary code and installs copies of itself in the memory of the infected computer. It can then infect other hosts from the infected computer. Like a virus, a worm is also a program that propagates itself. Unlike a virus, a worm can spread itself automatically over the network from one computer to the next. Worms are not clever or evil, they just take advantage of automatic file sending and receiving features found on many computers.
* Trojan horse is a general term, referring to programs that appear desirable, but actually contain something harmful. For example, a downloaded game could erase files. The contents could also hold a virus or a worm. A Trojan horse can attack on three levels. A virus known as the "Love Bug" is an example of a Trojan horse because it pretended to be a love letter when it actually carried a harmful program. The Love Bug was a virus because it infected all image files on the attacked disk, turning them into new Trojans. Finally, the Love Bug was a worm because it propagated itself over the Internet by hiding in the Trojan horses that it sent out using addresses in the attacked e-mail address book.

QUESTION 109:
The Certkiller security administrator needs to mitigate the effects of a recent worm attack that has affected the network. What are the four steps, in their correct order, to mitigate a worm attack?

A. Preparation, Identification, Traceback, and postmortem
B. Contain, Inoculate, Quarantine, and Treat
C. Identification, Inoculation, Postmortem, and Reaction
D. Preparation, Classification, Teaction, and Treat
E. Inoculate, Contain, Quarantine, and Treat
F. Quarantine, Contain, and Treat

Answer: B

Explanation:
The recommended steps for worm attack mitigation are:
Step 1 Containment: Contain the spread of the worm inside your network and within your network. Compartmentalize parts of your network that have not been infected.
Step 2 Inoculation: Start patching all systems and, if possible, scanning for vulnerable systems. Step 3 Quarantine: Track down each infected machine inside your network. Disconnect, remove, or block infected machines from the network.
Step 4 Treatment: Clean and patch each infected system. Some worms may require complete core system reinstallations to clean the system. Typical incident response methodologies can be subdivided into six major categories. These categories are based on the network service provider security incident response methodology:
Preparation: Acquire the resources to respond.
Identification: Identify the worm.
Classification: Classify the type of worm.
Traceback: Trace the worm back to its origin.

Reaction: Isolate and repair the affected systems.
Post mortem: Document and analyze the process used for the future.

QUESTION 110:
The Certkiller Security Administrator is concerned about network attacks. How can application layer attacks be mitigated?

A. Disable port redirection.
B. Implement traffic rate limiting.
C. Install the latest patches.
D. Implement Anti-DoS features.
E. Implement RFC 2827 filtering.

Answer: C

Explanation:
Application layer attacks can be implemented using several different methods:
* One of the most common methods of implementing application layer attacks is exploiting well-known weaknesses in software commonly found on servers, such as sendmail, PostScript, and FTP. By exploiting these weaknesses, attackers can gain access to a computer with the permission of the account running the application. The account is usually a privileged, system-level account.
* Trojan horse program attacks are implemented using programs that an attacker substitutes for common programs. These programs may provide all the functionality that the normal program provides, but may also include other features that are known to the attacker, such as monitoring login attempts to capture user account and password information. These programs can capture sensitive information and distribute it back to the attacker. They can also modify application functionality, such as applying a blind carbon copy to all e-mail messages so that the attacker can read all of the organization e-mail.
* One of the oldest forms of application layer attacks is a Trojan horse program that displays a screen, banner, or prompt that the user believes is the valid login sequence. The program then captures the information that the user enters and stores or e-mails it to the attacker. Next, the program either forwards the information to the normal login process (normally impossible on modern systems) or simply sends an expected error to the user (for example, Bad Username or Bad Password or a combination), exits, and starts the normal login sequence. The user believes that they have incorrectly entered the password, reenters the information and is allowed access.
* One of the newest forms of application layer attacks exploits the openness of several new technologies: the HTML specification, web browser functionality, and HTTP. These attacks, which include Java applets and ActiveX controls, involve passing harmful programs across the network and loading them through a user browser.
Application Layer Mitigation:
1. Read operating system and network log files or have them analyzed. It is important to review all logs and take action accordingly.
2. Subscribe to mailing lists that publicize vulnerabilities. Most application and operating

system vulnerabilities are published on the web by various sources.
3. Keep your operating system and applications current with the latest patches. Always test patches and fixes in a nonproduction environment. This practice prevents downtime and keeps errors from being generated unnecessarily.
4. Use IDS, IPS, or both to scan for known attacks, monitor and log attacks, and ultimately prevent attacks. Using these systems is essential to identifying security threats and mitigating some of these threats. In most cases, mitigation can be done automatically.

QUESTION 111:
You need to enhance the security of network management protocol traffic across the Certkiller WAN. Which procedure is recommended to protect SNMP from application layer attacks?

A. Use SNMP version 2.
B. Implement RFC 2827 filtering.
C. Configure SNMP with only read-only community strings.
D. Create an access list on the SNMP server.
E. None of the above.

Answer: C

Explanation:
SNMP is a network management protocol that you can use to retrieve information from a network device (commonly referred to as read-only access) or to remotely configure parameters on the device (commonly referred to as read-write access). SNMP version 1 and 2 uses passwords (called community strings) within each message as a simple form of security. Unfortunately, SNMPv1/v2 devices send the community string in plaintext along with the message. Therefore, SNMPv1/v2 messages may be intercepted by anyone with a packet sniffer located along the data path between the device and the management server. SNMPv3 overcomes these shortcomings by providing authentication and encryption to the message exchange.
1. Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the router.
To configure a community string, use the following command in global configuration mode:

Command	Purpose
snmp-server community *string* [**view** *view-name*] [**ro** | **rw**] [*number*]	Defines the community access string

---

QUESTION 112:
The Certkiller network administrator has enabled the AutoSecure feature on a new Certkiller router. What is one benefit of AutoSecure?

A. A multiuser logon screen is created with different privileges assigned to each member.

B. By default, all passwords are encrypted with level 7 encryption.
C. By default, a password is enabled on all ports.
D. Command line questions are created that automate the configuration of security features.
E. None of the above.

Answer: D

Explanation:
The AutoSecure feature is found in Cisco IOS software Release 12.3 and newer. AutoSecure is a single privileged EXEC program that allows you to quickly and easily eliminate many potential security threats. AutoSecure helps to make you more efficient at securing Cisco routers.
AutoSecure allows you to choose which router components to secure. You may want to secure the entire router functionality, or select individual planes or functions. The selectable components are the management plane, forwarding plane, firewall, login, NTP, and Secure Shell (SSH).

QUESTION 113:
In order to enhance the security of a Certkiller router, One-Step Lockdown was used. Which two actions will take place when One-Step Lockdown is implemented? (Select two)

A. A banner will be set.
B. Logging will be enabled.
C. Security passwords will be required to be a minimum of 8 characters.
D. CDP will be enabled.
E. Telnet settings will be disabled.
F. None of the above

Answer: A, B

Explanation:
Cisco SDM is an intuitive, web-based device-management tool for Cisco IOS software-based routers. Cisco SDM simplifies router and security configuration through smart wizards, which help you to quickly and easily deploy, configure, and monitor a Cisco router without requiring knowledge of the CLI. Cisco SDM simplifies firewall and Cisco IOS software configuration without requiring expertise about security or Cisco IOS software. Cisco SDM contains a Security Audit wizard that provides a comprehensive router security audit. Cisco SDM uses security configurations recommended by Cisco Technical Assistance Center (TAC) and International Computer Security Association (ICSA) as its basis for comparisons and default settings. The Security Audit wizard assesses the vulnerability of the existing router and provides quick compliance to best-practice security policies.
SDM can implement almost all of the configurations that AutoSecure offers with the One-Step Lockdown feature.

QUESTION 114:
To enhance the security of the Certkiller network, you have enabled the AutoSecure feature on every router. Which two statements about the AutoSecure feature are true? (Select two)

A. To enable AutoSecure, the "auto secure" global configuration command must be used.
B. AutoSecure automatically disables the CDP feature.
C. The auto secure full command automatically configures the management and forwarding planes without any user intervention.
D. If you enable AutoSecure, the minimum length of the login and enable passwords is set to 6 characters.
E. Once AutoSecure has been configured the user can launch the SDM Web interface to perform a security audit.

Answer: B, D

Explanation:
AutoSecure allows you to choose which router components to secure. You may want to secure the entire router functionality, or select individual planes or functions. The selectable components are the management plane, forwarding plane, firewall, login, NTP, and Secure Shell (SSH).
AutoSecure helps secure Cisco IOS networks by performing theserouter functions:
Disables insecure global services
Enables security-based global services
Disables insecure interface services
Enables appropriate security logging
Secures router administrative access
Secures the router management plane
Secures the router forwarding plane
The management plane includes management services, such as finger, PAD, UDP and TCP small servers, password encryption, TCP keepalives, CDP, BOOTP, HTTP, source routing, gratuitous ARP, proxy ARP, ICMP (redirects, mask-replies), directed broadcast, MOP, and banner. It also includes the login functions, such as password security and failed login attempt actions, as well as SSH access.

QUESTION 115:
In order to increase the security of the Certkiller network, the security administrator as enabled the AutoSecure feature in all the Certkiller routers. Which two statements about the Cisco AutoSecure feature are true? (Select two)

A. The auto secure command can be used to secure the router login as well as the NTP and SSH protocols.
B. For an interactive full session of AutoSecure, the auto secure login command should be used.
C. If the SSH server was configured, the 1024 bit RSA keys are generated after the auto

secure command is enabled.
D. Cisco123 would be a valid password for both the enable password and the enable secret commands.
E. All passwords entered during the AutoSecure configuration must be a minimum of 8 characters in length.

Answer: A, C

Explanation:
AutoSecure allows you to choose which router components to secure. You may want to secure the entire router functionality, or select individual planes or functions. The selectable components are the management plane, forwarding plane, firewall, login, NTP, and Secure Shell (SSH).
The management plane includes management services, such as finger, PAD, UDP and TCP small servers, password encryption, TCP keepalives, CDP, BOOTP, HTTP, source routing, gratuitous ARP, proxy ARP, ICMP (redirects, mask-replies), directed broadcast, MOP, and banner. It also includes the login functions, such as password security and failed login attempt actions, as well as SSH access.

QUESTION 116:
The following configuration was created automatically on a Certkiller router:

```
enable secret 5 $1$270i$BF/ftKAvuEzue3kfdikyP.
enable password 7 1414110209082722
username oeie password 7 08224F470C1A061E17
aaa new-mode
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
login block-for 60 attempts 3 within 5
hostname amos_eaton
ip domain-name amos_eaton.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
```

Based on the output shown above, What Cisco feature generated the configuration?

A. AAA
B. EZ VPN
C. IOS Firewall
D. IOS IPS
E. AutoSecure
F. TACACS+

G. None of the above

Answer: E

Explanation:
AutoSecure allows you to choose which router components to secure. You may want to secure the entire router functionality, or select individual planes or functions. The selectable components are the management plane, forwarding plane, firewall, login, NTP, and Secure Shell (SSH).

QUESTION 117:
A Certkiller router has been configured using the Authentication Proxy feature.
Which statement best describes this feature?

A. All traffic is permitted from the inbound to the outbound interface upon successful authentication of the user.
B. Prior to responding to a proxy ARP, the router will prompt the user for a login and password which are authenticated based on the configured AAA policy.
C. The proxy server capabilities of the IOS Firewall are enabled upon successful authentication of the user.
D. A specific access profile is retrieved from a TACACS+ or RADIUS server and applied to an IOS Firewall based on user provided credentials.

Answer: D

Explanation:
The authentication proxy feature allows a Cisco IOS router to intercept an HTTP or HTTPS session and prompt the user for authentication. The authentication is typically offloaded to an authentication, authorization, and accounting (AAA) server. In addition to just accepting or denying the connection, the router can download an authorization profile from the AAA server and apply that profile as an ACL to its interface. The profile includes information about the services that are accessible to the connecting user. Consequently all other traffic will be denied.

QUESTION 118:
Part of the Configuration file of an existing Certkiller router is shown below:

```
aaa new-model

username CertKiller password certkiller101

aaa authentication enable default group tacacs
```

Based on the information above, which two statements about the AAA configuration are true? (Select two)

A. If a TACACS+ server is not available, then the user Certkiller could be able to enter privileged mode as long as the proper enable password is entered.

B. Two authentication options are prescribed by the displayed aaa authentication command.
C. The aaa new-model command forces the router to override every other authentication method previously configured for the router lines.
D. A good security practice is to have the none parameter configured as the final method used to ensure that no other authentication method will be used.
E. To increase security, group radius should be used instead of group tacacs+.
F. If a TACACS+ server is not available, then a user connecting via the console port would not be able to gain access since no other authentication method has been defined.

Answer: B, C

Explanation:
You can manage user activity to and through a switch with authentication, authorization, and accounting (AAA) features. AAA uses standardized methods to challenge users for their credentials before access is allowed or authorized. Accounting protocols can also record user activity on a switch.
Switch(config)# aaa new-model
The new-model refers to the use of method lists, where authentication methods and sources can be grouped or organized. The new model is much more scalable than the "old model," where the authentication source was explicitly configured.
Use locally configured usernames and passwords as a last resort, when no other authentication servers are reachable or in use on the network. To define a username, use the following global configuration command:
Switch(config)# username username password password
RADIUS or TACACS+ servers are defined in groups. First, define each server along with its secret shared password. This string is known only to the switch and the server and provides a key for encrypting the authentication session. Use one of the following global configuration commands:
Switch(config)# radius-server host { hostname | ip-address} [key string]
Switch(config)# tacacs-server host { hostname | ip-address} [key string]
Then, define a group name that will contain a list of servers, using the following global configuration command:
Switch(config)# aaa group server {radius | tacacs+} group-name

---

QUESTION 119:
You have been tasked with setting up AAA services on a new Certkiller router.
Which command sequence is an example of a correctly configured AAA configuration that uses the local database?

A. Certkiller 3(config)# aaa new-model
Certkiller 3(config)# tacacs-server host 10.1.1.10
Certkiller 3(config)# tacacs-server key Certkiller 123
Certkiller 3(config)# aaa authentication login LOCAL_AUTH group tacacs+
Certkiller 3(config)# line con 0
Certkiller 3(config-line)# login authentication LOCAL_AUTH

B. Certkiller 3(config)# username Certkiller password Certkiller
Certkiller 3(config)# aaa new-model
Certkiller 3(config)# aaa authentication login LOCAL_AUTH local
Certkiller 3(config)# line con 0
Certkiller 3(config-line)# login authentication LOCAL_AUTH
C. Certkiller 3(config)# username Certkiller password Certkiller
Certkiller 3(config)# aaa new-model
Certkiller 3(config)# aaa authentication login LOCAL_AUTH local
Certkiller 3(config)# line con 0
Certkiller 3(config-line)# login authentication default
D. Certkiller 3(config)# aaa new-model
Certkiller 3(config)# tacacs-server host 10.1.1.10
Certkiller 3(config)# tacacs-server key Certkiller 123
Certkiller 3(config)# aaa authentication login LOCAL_AUTH group tacacs+
Certkiller 3(config)# line con 0
Certkiller 3(config-line)# login authentication default

Answer: B

Explanation:
You can manage user activity to and through a switch with authentication, authorization, and accounting (AAA) features. AAA uses standardized methods to challenge users for their credentials before access is allowed or authorized. Accounting protocols can also record user activity on a switch.
Switch(config)# aaa new-model
The new-model refers to the use of method lists, where authentication methods and sources can be grouped or organized. The new model is much more scalable than the "old model," where the authentication source was explicitly configured.
Switch(config)# aaa authentication login {default | list-name} method1 [method2 ...]
Here, the methods refer to these values:
tacacs+-Each of the TACACS+ servers configured on the switch will be tried, in the order that it was configured.
radius-Each of the RADIUS servers configured on the switch will be tried, in the order that it was configured.
local-The user's credentials will be compared against all of the username commands configured on the local switch.
line-The line passwords authenticate any connected user. No usernames can be used.
First, select a line (console or vty for Telnet access) using the
line line command. Then, trigger the user authentication on that line to use an AAA method list. Use the following line configuration command:
Switch(line)# login authentication {default | list-name}

QUESTION 120:
AAA has been configured on a Certkiller IOS firewall. Which firewall feature allows per-user policy to be downloaded dynamically to the router from a TACACS+ or RADIUS server using AAA services?

A. Port-to-Application Mapping (PAM)
B. Intrusion Prevention System
C. Lock-and-Key (dynamic ACLs)
D. Authentication Proxy
E. Reflexive ACLs
F. None of the above

Answer: D

Explanation:
The authentication proxy feature allows a Cisco IOS router to intercept an HTTP or HTTPS session and prompt the user for authentication. The authentication is typically offloaded to an authentication, authorization, and accounting (AAA) server. In addition to just accepting or denying the connection, the router can download an authorization profile from the AAA server and apply that profile as an ACL to its interface. The profile includes information about the services that are accessible to the connecting user. Consequently all other traffic will be denied.

QUESTION 121:
Router Certkiller 1 was configured as shown below:

```
Certkiller1# config t
Certkiller 1 (config) # username Certkiller password testking101
Certkiller 1 (config) # aaa new-model1
Certkiller 1 (config) # aaa authentication login LOCAL_AUTH local
Certkiller 1 (config) # line con 0
Certkiller1 (config-line)# login authentication LOCAL_AUTH
Certkiller1 (config-line)# line aux 0
Certkiller1 (config-line)# login authentication LOCAL_AUTH
Certkiller1 (config-line)# line vty 0 4
Certkiller1 (config-line)# login authentication LOCAL_AUTH
```

Based on the partial configuration shown above, which two statements are true? (Select two)

A. To make the configuration more secure, the none parameter should be added to the end of the aaa authentication login LOCAL_AUTH local command.
B. This is an example of a self-contained AAA configuration using the local database.
C. If configured, the enable password could also be used to log into the console port.
D. The command aaa authentication default should be issued for each line instead of the login authentication LOCAL_AUTH command.
E. The local parameter is missing at the end of each aaa authentication LOCAL-AUTH command.
F. To successfully establish a Telnet session with Certkiller 1, a user can enter the username Certkiller and password cisco.

Answer: B, F

Explanation:

You can manage user activity to and through a switch with authentication, authorization, and accounting (AAA) features. AAA uses standardized methods to challenge users for their credentials before access is allowed or authorized. Accounting protocols can also record user activity on a switch.
Switch(config)# aaa new-model
The new-model refers to the use of method lists, where authentication methods and sources can be grouped or organized. The new model is much more scalable than the "old model," where the authentication source was explicitly configured.
Switch(config)# aaa authentication login {default | list-name} method1 [method2 ...]
Here, the methods refer to these values:
tacacs+-Each of the TACACS+ servers configured on the switch will be tried, in the order that it was configured.
radius-Each of the RADIUS servers configured on the switch will be tried, in the order that it was configured.
local-The user's credentials will be compared against all of the username commands configured on the local switch.
line-The line passwords authenticate any connected user. No usernames can be used.
First, select a line (console or vty for Telnet access) using the line line command. Then, trigger the user authentication on that line to use an AAA method list. Use the following line configuration command:
Switch(line)# login authentication {default | list-name}

QUESTION 122:
The "aaa authentication enable default group radius enable" command was enabled on a Certkiller router. What is true regarding this command?

A. If the radius server returns a 'failed' message, the enable password will be used.
B. If the radius server returns an error, the enable password will be used.
C. The command login authentication group will associate the AAA authentication to a specified interface.
D. If the group database is unavailable, the radius server will be used.
E. None of the above.

Answer: B

Explanation:
The authentication login command in global configuration mode enables the AAA authentication process.
RouterA(Config)# aaa authentication login {default | list-name} group {group-name | radius | tacacs+} [method2 [method3 [method4]]]

aaaauthentication login Parameters

default	This command creates a default that is automatically applied to *all* lines and interfaces, specifying the method or sequence of methods for authentication.
list-name	This command creates a list, with a name of your choosing, that is applied explicitly to a line or interface using the method or methods specified. This defined list overrides the default when applied to a specific line or interface.
group *group-name* **group radius** **group tacacs+**	These methods specify the use of an AAA server. The **group radius** and **group tacacs+** methods refer to previously defined RADIUS or TACACS+ servers. The *group-name* string allows the use of a predefined group of RADIUS or TACACS+ servers for authentication (created with the **aaa group server radius** or **aaa group server tacacs+** command).
method2 **method3** **method4**	This command executes authentication methods in the listed order. If an authentication method returns an error, such as a timeout, the Cisco IOS software attempts to execute the next method. If the authentication fails, access is denied. You can configure up to four methods for each operation. The method must be supported by the authentication operation specified. A general list of methods includes: **enable:** Uses the enable password for authentication **group:** Uses server-group **krb5:** Uses Kerberos Version 5 for authentication **line:** Uses the line password for authentication **local:** Uses the local username and password database for authentication **local-case:** Uses case-sensitive local username authentication **none:** Uses no authentication

---

QUESTION 123:

Your absent minded junior administrator has enabled AAA authentication on the Certkiller network, but forgot to set the authentication. What will happen when a user try's to login?

A. Disallow a user from access to all resources after login.
B. Allow any user to login without checking the authentication data.
C. Record all access of resources and how long the user accessed each resource.
D. Allow a user to access all resources after login.
E. Not to record any access of resources after login.
F. Disallow any user from logging in with or without a valid username and password.
\

Answer: F

Explanation:
The three parts of AAA are defined as follows:
Authentication: Authentication determines the identity of users and whether they should be allowed access to the network. Authentication allows network managers to bar intruders from their networks.
Authorization: Authorization allows network managers to limit the network services available to each user. Authorization also helps restrict the exposure of the internal network to outside callers. Authorization allows mobile users to connect to the closest local connection and still have the same access privileges as if they were directly connected to their local networks. You can also use authorization to specify which

commands a new system administrator can issue on specific network devices.
Accounting: System administrators might need to bill departments or customers for connection time or resources used on the network (for example, bytes transferred). Accounting tracks this kind of information. You can also use the accounting syslog to track suspicious connection attempts into the network and trace malicious activity.
To enable AAA on a router we would type:
Router(config)#aaa new-model
If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. To set the AAA authentication we must use the following command:
Router(config)#aaa authentication [login | enable | arap |
ppp | nasi] method
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 15-11

QUESTION 124:
What six types of accounting information does a TACACS+ / RADIUS server record?

A. Connection, protocol, system, network, command, and resource
B. Resource, interface, connection, system, command, and network
C. Command, system, exec, network, connection, and resource
D. Network, interface, exec, protocol, system, and resource
E. Crypto, system, network, protocol, command, and resource
F. None of the above

Answer: C

Explanation:
AAA Accounting - AAA accounting can supply information concerning user activity back to the database. This concept was especially helpful in the early days of Internet service when many ISPs offered 20 or 40 hours per week at a fixed cost and hourly or minute charges in excess of the specified timeframe. Today it is much more common for the ISP charge to be set for an unlimited access time. This does not, however, minimize the power of accounting to enable the administrator to track unauthorized attempts and proactively create security for system resources. In addition, accounting can be used to track resource usage to better allocate system usage.
Accounting is generally used for billing and auditing purposes and is simply turned on for those events that are to be tracked. The commands follow this general syntax:
aaaaccounting what-to-track how-to-track where-to-send-the-information
The what-to-track arguments are as follows:
network - With this argument, network accounting logs the information, on a user basis, for PPP, SLIP, or ARAP sessions. The accounting information provides the time of access and the network resource usage in packet and byte counts.
connection - With this argument, connection accounting logs the information about outbound connections made from the router or RAS device, including Telnet and rlogin

sessions. The key word is outbound; it enables the tracking of connections made from the RAS device and where those connections were established.
exec
- With this argument, EXEC accounting logs the information about when a user creates an EXEC terminal session on the router. The information includes the IP address and telephone number, if it is a dial-in user, and the time and date of the access. This information can be particularly useful for tracking unauthorized access to the RAS device.
system- With this argument, system accounting logs the information about system-level events. System-level events include AAA configuration changes and reloads for the device. Again, this information would be useful to track unauthorized access or tampering with the router.
command- With this argument, command accounting logs information regarding which commands are being executed on the router. The accounting record contains a list of commands executed for the duration of the EXEC session, along with the time and date information.
resource - Before AAA resource failure stop accounting, there was no method of providing accounting records for calls that failed to reach the user authentication stage of a call setup sequence. Such records are necessary for users employing accounting records to manage and monitor their networks and their wholesale customers.
This command was introduced in Cisco IOS Software Release 12.1(3)T.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 2-12
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#1014024

QUESTION 125:
On one of the Certkiller routers the following configuration command was issued:
Certkiller A(config)#aaa authentication login default group tacacs+
none
What is this command used for?

A. It uses the list of servers specified in group "TACACS+", if none are available, then no access is permitted.
B. It uses the list of TACACS+ servers for authentication, if TACACS+ fails then uses no authentication.
C. It uses the list of TACACS+ servers for authentication, if TACACS+ fails then no access is permitted.
D. No authentication is required to login.
E. It uses a subset of TACACS+ servers named "group" for authentication as defined by the aaa group servers tacacs+ command.
F. TACACS+ is the first default authentication method.

Answer: B

Explanation:
Once AAA has been enabled on the router, the administrator must declare the methods by

which authentication can take place. The aaa authentication login command answers this question: How do I authenticate the login dialog?
The declaration of default tells the router what to do if no listname has been declared on the interface. If a listname has been declared, that listname controls the login. In this statement the listname group is defined, It declares that listname group use TACACS+ by default, and if that fials no authentication is required because the none command has been entered at the end.
Additional methods for the aaa authentication command are:
* enable - Uses the enable password for authentication.
* line - Uses the line password for authentication.
* local - Uses the local username/password database for authentication.
* none - Uses no authentication.
* tacacs+ - Uses the TACACS+ authentication method.
* radius - Uses the RADIUS authentication method.
* guest - Allows guest logins without passwords. This option applies only to ARAP operations.
* auth-guest - Allows guest logins only if the user has already logged in to EXEC. This option only applies to ARAP operations.
* if-needed - Stops further authentication if the user has already been authenticated. This option only applies to PPP operations.
* krb5 - Uses Kerberos 5 for authentication, this option only applies to PPP operations.
Reference:
Cisco Press - Building Cisco Remote Access Networks Student Guide v1.1 Page 15-12
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8) Page 409 & 410

QUESTION 126:
You have just received a brand new Cisco router and need to configure auditing on it. What command would you use to enable auditing of the privileged mode access commands?

A. aaa accounting enable 15
B. ip audit enable
C. aaa accounting command 15
D. aaa accounting enable priv

Answer: C

Explanation:
AAA accounting can supply information concerning user activity back to the database. This concept was especially helpful in the early days of Internet service when many ISPs offered 20 or 40 hours per week at a fixed cost and hourly or minute charges in excess of the specified timeframe. Today it is much more common for the ISP charge to be set for an unlimited access time. This does not, however, minimize the power of accounting to enable the administrator to track unauthorized attempts and proactively create security for system resources. In addition, accounting can be used to track resource usage to better

allocate system usage.
Accounting is generally used for billing and auditing purposes and is simply turned on for those events that are to be tracked.
Syntax:
aaaaccounting {system | network | exec | connection | commands level} {default | list-name} {start-stop | stop-only | none} method1 [method2...]
Commands - Runs accounting for all commands at the specified privilege level.
Level - Specific command level to track for accounting. Valid entries are 0 through 15.
Command - With this argument, command accounting logs information regarding which commands are being executed on the router. The accounting record contains a list of commands executed for the duration of the EXEC session, along with the time and date information.
Reference:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8) Page 416.

QUESTION 127:
You are a senior network administrator and your junior administrator didn't arrive to work because he claimed he was sick. So you give him an assignment to do from home via Telnet. So from his home; he logged onto the companies router and entered the following command:
Router(config)#aaa new-model
Before entering anything else, the lazy junior administrator (with the intention of being cautious) thought it would be safe to save the configuration to NVRAM, log off from telnet and take a break for a few hours. Assuming that no local username or password exists on the router database, what will happen when the administrator tries to immediately establish another telnet session? (Choose two)

A. The session asks for a username that may not exist.
B. The router requires a reboot to so the administrator can login.
C. The administrator must access the router through the console port to login.
D. The administrator can log in without using a password.

Answer: A, C

Explanation:
Once AAA has been enabled on the router, the administrator must declare the methods by which authentication can take place. The key issue is to ensure that the administrator has a way to gain access to the router if the AAA server is down. Failure to provide a backdoor interface can result in lost communications to the router and the necessity to break in through the console port. Care should be taken to always configure a local access method during any implementation of AAA.
References:
Cisco Press - BCRAN - 642-821 - Exam Certification Guide 2004 (ISBN 1-58720-084-8) Page 408

CCNP Remote Access Exam Certification Guide, page 374, Brian Morgan & Craig Dennis, Cisco Press 2001, ISBN 1-58720-003-1

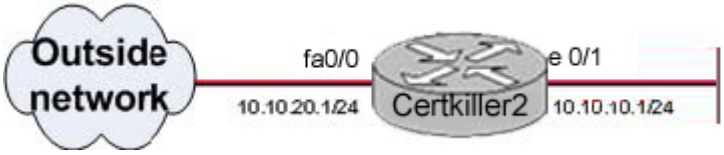
QUESTION 128:
Given the following configurationon a Certkiller router, which two statements about the router are true? (Choose two.)
Certkiller 1(config)# aaa authentication login default group tacacs+ none

A. No authentication is required to login.
B. It uses TACACS+ as the first default authentication method.
C. It uses the default local database for authentication. If authentication fails, then no access is permitted.
D. It uses the list of servers specified in group "TACACS+". If none are available, then no access is permitted.
E. It uses the list of TACACS+ servers for authentication. If the TACACS+ authentication servers are unavailable, then the router uses no authentication.
F. It uses a subset of TACACS+ servers named "group" for authentication as defined by the aaa group server tacacs+ command.

Answer: B, E

Explanation:
The Cisco IOS software uses the first method listed to authenticate users. If that method fails to respond (indicated by an ERROR), the Cisco IOS software selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method, or all methods defined in the method list are exhausted. From the configuration file shown above, the order of operation is to first check the tacacs+ server, and should that fail do not use any authentication method.

QUESTION 129:
A portion of the Certkiller network is shown below:



Part of the Certkiller router configuration is shown below:

```
Certkiller1 # conf t
Enter configuration commands, per line.  End with CNTL/Z.
Certkiller1 (config)# access-list 150 permit tcp any 10.10.10.0 0.0.0.255 established
Certkiller1 (config)# access-list 150 deny ip any any
Certkiller1 (config)# interface fa0/0
Certkiller1 (config-if)# ip access-group 150 in
Certkiller1 (config-if ) # ^Z
Certkiller1 #
```

Based on the information above, what is the result of the ACL configuration that is displayed?

A. TCP responses from the outside network for TCP connections that originated on the

inside network are allowed.
B. TCP responses from the inside network for TCP connections that originated on the outside network are denied.
C. Any inbound packet with the SYN flag set to be routed is permitted.
D. Inbound packets to request a TCP session with the 10.10.10.0/24 network are allowed.
E. None of the above

Answer: A

Explanation:
An access list is nothing more than an ordered list of permit and deny statements. Every time the router needs to refer to the list for some reason, it reads it at the top and works its way down.
Extended access lists Extended access lists can evaluate many of the other fields in the Layer 3 and Layer 4 header of an IP packet. They can evaluate source and destination IP addresses, the protocol field in the Network layer header, and the port number at the Transport layer header. This gives extended access lists the ability to make much more granular decisions when they are controlling traffic.
In Exhibit: Extended Access List is created: Syntax of Extended ACL is,
Access-list <Num> permit | deny <Protocol> <Source Address> <Destination Address> eq | lt | gt <Port Number>

QUESTION 130:
A Certkiller router interface is configured with an inbound access control list and an inspection rule. How will an inbound packet on this interface be processed?

A. The packet is processed by the inspection rule. If the packet does not match the inspection rule, the inbound ACL is invoked.
B. The packet is processed by the inspection rule. If the packet matches the inspection rule, the inbound ACL is invoked.
C. The packet is processed by the inbound ACL. If the packet is not dropped by the ACL, it is processed by the inspection rule.
D. The packet is processed by the inbound ACL. If the packet is dropped by the ACL, it is processed by the inspection rule.
E. None of the above.

Answer: C

Explanation:
Inbound access lists When an access list is applied to inbound packets on an interface, those packets are processed through the access list before being routed to the outbound interface. Any packets that are denied won't be routed because they're discarded before the routing process is invoked.
Outbound access lists When an access list is applied to outbound packets on an interface, those packets are routed to the outbound interface and then processed through the access list before they are queued.

QUESTION 131:
You need to add an access list to a Certkiller router in order to increase the security of the network. Which two statements are correct about mitigating attacks by the use of access control lists? (Select two)

A. Ensure that earlier statements in the ACL do not negate any statements that are found later in the list.
B. Denied packets should be logged by an ACL that traps informational (level 6) messages.
C. Each ACL that is created ends with an implicit permit all statement.
D. More specific ACL statements should be placed earlier in the ACL.
E. Extended ACLs on routers should always be placed as close to the destination as possible.
F. IP packets that contain the source address of any internal hosts or networks inbound to a private network should be permitted.

Answer: B, D

QUESTION 132:
While you were on your lunch break your apprentice trainee was busy configuring access lists. When you return to your workstation you find the following configuration:
access-list101 permit ip any any
access-list101 deny tcp any any eq ftp
dialer-list 2 protocol ip list 101
What is true about the configuration that your trainee entered? (Choose all that apply)

A. FTP traffic will be forwarded.
B. Since FTP uses two sockets, both must be defined to prevent packet forwarding.
C. FTP will cause the line to come up in a dialer or ISDN interface.
D. FTP traffic will not be forwarded.

Answer: A, C

Explanation:
The logic that IOS uses with a multiple-entry Access Control List can be summarized as follows:
1. The matching parameters of the access-list statement are compared to the packet.
2. If a match is made, the action defined in this access-list statement (permit or deny) is performed.
3. If a match is not made in Step 2, repeat Steps 1 and 2 using each successive statement in the ACL until a match is made.
4. If no match is made with an entry in the access list, the deny action is performed.
The access-list 101 permit ip any any command is used and the result is that every packet

will be permitted. So the second command "access-list 101 deny tcp any any eq ftp" is never read by the IOS since all IP traffic (including FTP) will match the first line.
The dialer-list 2 protocol ip list 101 command binds the Access Control List to the dialer list. Therefore the FTP traffic will be forwarded and it will bring up the line.
Reference:
Cisco Press - ICND - 640-811 - Exam Certification Study Guide 2004 (ISBN 1-58720-083-x) Page 430

QUESTION 133:
You need to configure NTP on a new Certkiller router. Which statement is true about a router configured with the "ntp trusted-key 10" command?

A. The IOS will not permit "10" as an argument to the ntp trusted-key command.
B. This router only synchronizes to a system that uses this key in its NTP packets.
C. This router will join an NTP multicast group where all routers share the same trusted key.
D. This command enables DES encryption of NTP packets.

Answer: B

Explanation:
NTP is used to synchronize the clocks in the entire network. Many features depend on it, such as accurate time information in syslog messages, certificate-based authentication in VPNs, ACLs with time range configuration, key rollover in routing protocol authentication (Enhanced Interior Gateway Routing Protocol [EIGRP], Routing Information Protocol [RIP]).
If you want to authenticate the associations with other systems for security purposes, use the commands that follow. The first command enables the NTP authentication feature. The second command defines each of the authentication keys. Each key has a key number, a type, and a value. Currently the only key type supported is md5. Finally, a list of trusted authentication keys is defined. If a key is trusted, this system will be ready to synchronize to a system that uses this key in its NTP packets.
Steps:
R1(config)#ntp authentication
R1(config)#ntp authentication-key 1 md5 aabbbcddee344
R1(config)#ntp trusted-key

NTP Authentication commands

Command	Description
`ntp authenticate`	Enables the NTP authentication feature. If this command is specified, the system will not synchronize to a system unless its NTP messages carry one of the authentication keys specified in the **ntp trusted-key** global configuration command.
`ntp authentication-key` *number* **md5** *value*	Defines an authentication key. Message authentication support is provided using the MD5 algorithm. The key type **md5** is currently the only key type supported. The key value can be any arbitrary string of up to eight characters.
`ntp trusted-key` *key-number*	Defines trusted authentication keys.

QUESTION 134:
You are configurig NTP on a new Certkiller router. Which global configuration mode command will configure a Cisco router as an authoritative NTP server?

A. ntp peer
B. ntp master
C. ntp broadcast
D. ntp server
E. None of the above

Answer: B

Explanation:
NTP is used to synchronize the clocks in the entire network. Many features depend on it, such as accurate time information in syslog messages, certificate-based authentication in VPNs, ACLs with time range configuration, key rollover in routing protocol authentication (Enhanced Interior Gateway Routing Protocol [EIGRP], Routing Information Protocol [RIP]).
Use the
ntp master command in global configuration mode if you want the system to be an authoritative NTP server (a master clock), even if the system is not synchronized to an outside time source or an external NTP source is not available. Stratum is an optional number from 1 to 15 that indicates the NTP stratum number that the system will claim. By default, the master clock function is disabled. When enabled, the default stratum is 8.

QUESTION 135:
You have been tasked with configuring security features on a new Cisco device. Which statement is true about the superview of Role-Based CLI?

A. Commands cannot be directly configured for a superview.
B. Any user with level 15 privileges can create or modify views and superviews.
C. A CLI view cannot be shared by multiple superviews.
D. The maximum number of CLI views which can exist is limited only by the amount of flash available.
E. None of the above

Answer: A

Explanation:
A superview consists of one or more CLI views, which allow users to define which commands are accepted and what configuration information is visible. Superviews allow you to easily assign all users within configured CLI views to a superview instead of having to assign multiple CLI views to a group of users.
Superviews have these characteristics:
* A CLI view can be shared among multiple superviews.
* Commands cannot be configured for a superview; that is, you must add commands to

the CLI view and add that CLI view to the superview.
* Users who are logged into a superview can access all of the commands that are configured for any of the CLI views that are part of the superview.
* Each superview has a password that is used to switch between superviews or from a CLI view to a superview.
* If a superview is deleted, all CLI views associated with that superview will not also be deleted.
To configure a superview, use the parser view command and configure a password for that superview. Then, add a normal CLI view to the superview using the view command. Issue this command for each CLI view that is to be added to the superview.

QUESTION 136:
Part of the configuration file of a Certkiller router is shown in the exhibit below:

```
ip ssh time-out 60
ip ssh authentication-retries 2
!
line vty 04
transport input ssh
```

SDM has added the commands in the exhibit to the Certkiller router's configuration. What are three objectives that the commands above accomplish? (Select three)

A. Sets the maximum number of unsuccessful SSH login attempts to two before locking access to the router
B. Specifies SSH for remote management access
C. Inspects SSH packets across all enabled interfaces every 60 seconds
D. Prevents Telnet access to the device unless it is from the SDM workstation
E. Sets the SSH timeout value to 60 seconds, a value that causes incomplete SSH connections to shut down after 60 seconds
F. Forces the user to authenticate twice to prevent man-in-the-middle attacks

Answer: A, B, E

Explanation:
Secure Shell (SSH) is an application and a protocol that provide a secure replacement to the Berkeley r-tools. The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools. There are currently two versions of SSH available: SSHVersion 1 and SSHVersion

2. Only SSHVersion 1 is implemented in the CiscoIOS software.

Command	Purpose
Router(config)# **ip ssh** {[**timeout** *seconds*] | [**authentication-retries** *integer*]}	(Required) Configures SSH control variables on your router. • You can specify the timeout in seconds, not to exceed 120 seconds. The default is 120. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0-4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes. • You can also specify the number of authentication retries, not to exceed 5 authentication retries. The default is 3.

QUESTION 137:
A new Certkiller router is being configured for the Network Time Protocol (NTP).
Which statement is true about the global configuration command ntp server 198.133.219.25?

A. The command configures the router to be the NTP time source for a peer located at IP address 198.133.219.25.
B. Entering the command ntp server 198.133.219.26 would replace the original command ntp server 198.133.219.25.
C. The command configures the router to provide the date and clock setting for a host located at IP address 198.133.219.25.
D. The command configures the router to synchronize with an NTP time source located at IP address 198.133.219.25.
E. None of the above.

Answer: D

Explanation:
Although you may configure either a peer or a server association, NTP clients would be typically configured with a server association (meaning that only this system will synchronize to the other system, and not the other way around). If you want to allow the software clock to be synchronized by an NTP time server, use the ntp server command in global configuration mode.
RouterA(Config)#ntp server {ip-address | hostname} [version number] [key key-id] [source interface] [prefer]

NTP Server parameters:

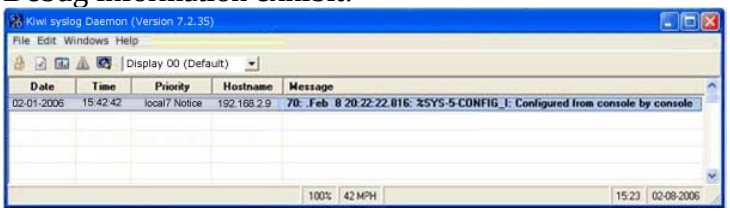
Parameter	Description
ip-address	IP address of the time server providing the clock synchronization.
hostname	Name of the time server providing the clock synchronization.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number (1 to 3). Default is 3.
key	(Optional) Defines the authentication key.
Key-id	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Identifies the interface from which to pick the IP source address. Default is to take the interface address.
interface	(Optional) Name of the interface from which to pick the IP source address.
prefer	(Optional) Specifies that the server referenced in this command is preferred over other configured NTP servers.

QUESTION 138:

Router Certkiller 2 is configured as shown below:

```
Certkiller2 # proof t
Certkiller2 (config) # logging host 192.168.2.7
Certkiller2 (config) # logging trap informational
Certkiller2 (config) # exit
Certkiller2 # debug ip ssh
   Incomming ssh debugging is on
Certkiller2
```

Debug information exhibit:



A user is unable to initiate an SSH session with Certkiller 2. To help troubleshoot the problem, Certkiller 2 has been configured as indicated in the exhibit. However, a second attempt to initiate an SSH connection to Certkiller 2 fails to generate debug information on the Syslog server. What configuration change would display the debug information on the Syslog server?

A. Router Certkiller 2 must be configured with the logging trap debugging global configuration command.
B. Router Certkiller 2 must be configured with the logging buffered informational global configuration command.
C. Router Certkiller 2 should be configured with the debug ip packet EXEC command.
D. Router Certkiller 2 must be configured with the correct Syslog IP address.
E. Router Certkiller 2 must be configured with the logging monitor debugging global configuration command.
F. None of the above.

Answer: A

Explanation:
Set the log severity (trap) level: Setting the log severity level limits the error messages sent to syslog servers to only those at the specified level. Default value is severity level 6. Use the logging trap command in global configuration mode to set the severity level. logging trap level.
Cisco Log Severity Levels

Level	Name	Description
0	Emergencies	Router unusable
1	Alerts	Immediate action required
2	Critical	Condition critical
3	Errors	Error condition
4	Warnings	Warning condition
5	Notifications	Normal but important event
6	Informational	Informational message
7	Debugging	Debug message

QUESTION 139:
The following output was shown on router Certkiller 2:

```
Certkiller2 # debug ip ssh
   Incomming ssh debugging is on
Certkiller2 #
    GMT   : 00:18:20   27: 351: Could not get a vty line for incoming session
```

On the basis of the information presented above, which configuration change would correct the Secure Shell (SSH) problem?

A. Configure router Certkiller 2 with the crypto key generate rsa general-keys modulus modulus-number global configuration command.
B. Configure router Certkiller 2 with the crypto key generate rsa usage-keys modulus modulus-number global configuration command.
C. Configure router Certkiller 2 with the ip domain name domain-name global configuration command.
D. Configure router Certkiller 2 with the no transport input telnet vty line configuration command.
E. Configure router Certkiller 2 with the transport input ssh vty line configuration command.
F. None of the above.

Answer: E

Explanation:
Secure Shell (SSH) is an application and a protocol that provide a secure replacement to the Berkeley r-tools. The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools. There are currently two versions of SSH available: SSHVersion 1 and SSHVersion 2. Only SSHVersion 1 is implemented in the CiscoIOS software.

1. Disable vty inbound Telnet sessions: Austin2(config)#line vty 0 4
2. R1(config-line)#no transport input telnet
1. Enable vty inbound SSH sessions: R1(config-line)#transport input ssh
1.
The SSH protocol is automatically enabled once you generate the SSH (RSA) keys, as shown in the figure. Once the keys are created, you may access the router SSH server using your SSH client software. The procedure for connecting to a Cisco router SSH server varies depending on the SSH client application that you are using. Generally, the SSH client passes your username to the router SSH server. The router SSH server prompts you for the correct password. Once the password has been verified, you can configure and manage the router as if you were a standard vty user.

QUESTION 140:
You need to configure a new Certkiller device using the Cisco SDM. What are three features in the SDM that role-based access provides? (Select three)

A. It provides dynamic update of new IPS signatures for administrator, firewall administrator, easy VPN client, and read-only users
B. It provides logical separation of the router between different router administrators and users
C. It provides secure access to the SDM user interface and Telnet interface specific to the profile of each administrator
D. It provides to end customers multiservice switching platforms (MSSPs) with a graphical, read-only view of the customer premises equipment (CPE) services
E. It provides advanced troubleshooting using debug output analysis
F. It provides configuration wizards for all routing protocols (like RIP, OSPF, EIGRP, BGP, IS-IS)

Answer: B, C, D

Explanation:
Cisco SDM is an intuitive, web-based device-management tool for Cisco IOS software-based routers. Cisco SDM simplifies router and security configuration through smart wizards, which help you to quickly and easily deploy, configure, and monitor a Cisco router without requiring knowledge of the CLI. Cisco SDM simplifies firewall and Cisco IOS software configuration without requiring expertise about security or Cisco IOS software.
Cisco SDM contains a Security Audit wizard that provides a comprehensive router security audit. Cisco SDM uses security configurations recommended by Cisco Technical Assistance Center (TAC) and International Computer Security Association (ICSA) as its basis for comparisons and default settings. The Security Audit wizard assesses the vulnerability of the existing router and provides quick compliance to best-practice security policies.
SDM can implement almost all of the configurations that AutoSecure offers with the One-Step Lockdown feature.

QUESTION 141:
Part of the configuration file of router Certkiller 3 is displayed below:

```
<Output omitted>

① hostname Certkiller3
  !
② aaa new-model
③ username Cisco Password 0 Certkiller101

④ ip domain-name rtp.certkiller.com
  !
⑤ crypto key generate rsa
⑥ ip ssh time-out 60
⑦ ip ssh authentication-retries 2
  !
⑧ line vty 0 4
⑨ transport input ssh
```

Refer to the numbers at the left of each configuration line. Of the numbered items in the exhibit, which combination is required to implement only SSH?

A. 1, 4, 5, and 9
B. 5, 6, and 7
C. 5, 6, 7, and 9
D. 2, 3, 5, and 9
E. 1, 3, 5, 6, 7, and 9

Answer: A

Explanation:
Secure Shell (SSH) is an application and a protocol that provide a secure replacement to the Berkeley r-tools. The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools. There are currently two versions of SSH available: SSHVersion 1 and SSHVersion 2. Only SSHVersion 1 is implemented in the CiscoIOS software.
To configure a host name and host domain, enter the following commands beginning in global configuration mode:

Command	Purpose
Router(config)# **hostname** *hostname*	Configures a host name for your router.
Router(config)# **ip domain-name** *domainname*	Configures a host domain for your router.

Generate an RSA key pair for your router, which automatically enables SSH.
To generate an RSA key pair, enter the following global configuration command:

Command	Purpose
Router(config)# **crypto key generate rsa**	Enables the SSH server for local and remote authentication on the router.

Command	Purpose
Router(config)# **ip ssh** {[**timeout** *seconds*] | [**authentication-retries** *integer*])	(Required) Configures SSH control variables on your router. • You can specify the timeout in seconds, not to exceed 120 seconds. The default is 120. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0-4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes. • You can also specify the number of authentication retries, not to exceed 5 authentication retries. The default is 3.

QUESTION 142:
You have been tasked with implementing SSH on a new Certkiller router. Which two steps must be taken for SSH to be implemented on a router? (Select two)

A. Ensure that the target routers are configured for AAA either locally or through a database
B. Ensure that each router is using the correct domain name for the network
C. Ensure that the Cisco IOS Firewall feature set is installed on the devices.
D. Ensure that an ACL is configured on the VTY lines to block Telnet access

Answer: A, B

Explanation:
Secure Shell (SSH) is an application and a protocol that provide a secure replacement to the Berkeley r-tools. The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools. There are currently two versions of SSH available: SSHVersion 1 and SSHVersion 2. Only SSHVersion 1 is implemented in the CiscoIOS software.
To configure a host name and host domain, enter the following commands beginning in global configuration mode:

Command	Purpose
Router(config)# **hostname** *hostname*	Configures a host name for your router.
Router(config)# **ip domain-name** *domainname*	Configures a host domain for your router.

Generate an RSA key pair for your router, which automatically enables SSH.
To generate an RSA key pair, enter the following global configuration command:

Command	Purpose
Router(config)# **crypto key generate rsa**	Enables the SSH server for local and remote authentication on the router.

Command	Purpose
Router(config)# **ip ssh** ([**timeout** *seconds*] | [**authentication-retries** *integer*])	(Required) Configures SSH control variables on your router. • You can specify the timeout in seconds, not to exceed 120 seconds. The default is 120. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0-4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes. • You can also specify the number of authentication retries, not to exceed 5 authentication retries. The default is 3.

Here is the sample Configuration:
In the following example, SSH is configured on a Cisco 7200 with a timeout that is not to exceed 60seconds, and no more than 2 authentication retries. Also, before configuring the SSH server feature on the router, TACACS+ is specified as the method of authentication.
aaa new-modelaaa authentication login default tacacs+aaa authentication login aaa7200kw noneenable password enable7200pwusername mcisco password 0 maryspw username jcisco password 0 johnspwip subnet-zerono ip domain-lookupip domain-name cisco.com! Enter the ssh commands.ip ssh time-out 60ip ssh authentication-retries 2

QUESTION 143:
You need to secure some of the management protocols and services used on a new Certkiller router. Which two statements about management protocols are true? (Select two)

A. NTP version 3 or above should be used because these versions support a cryptographic authentication mechanism between peers.
B. TFTP authentication (username and password) is sent in an encrypted format, and no additional encryption is required.
C. SNMP version 3 is recommended since it provides authentication and encryption services for management packets.
D. Syslog version 2 or above should be used because it provides encryption of the syslog messages.
E. SSH, SSL and Telnet are recommended protocols to remotely manage infrastructure devices.

Answer: A, C

Explanation:
SNMP is a network management protocol that you can use to retrieve information from a network device (commonly referred to as read-only access) or to remotely configure parameters on the device (commonly referred to as read-write access). SNMP version 1 and 2 uses passwords (called community strings) within each message as a simple form of security. Unfortunately, SNMPv1/v2 devices send the community string in plaintext along with the message. Therefore, SNMPv1/v2 messages may be intercepted by anyone with a packet sniffer located along the data path between the device and the management server. SNMPv3 overcomes these shortcomings by providing authentication and encryption to the message exchange.
Network Time Protocol (NTP) is used to synchronize the clocks of various devices across a network. Synchronization of the clocks within a network is critical for digital certificates and for correct interpretation of events within syslog data. A secure method of providing clocking for the network is for network administrators to implement their own master clocks for private networks synchronized, via satellite or radio, to Coordinated Universal Time (UTC). However, if network administrators do not wish to implement their own master clocks because of cost or other reasons, clock sources are available for synchronization via the Internet.
The current version of NTP is version 4. The latest version defined by an RFC is version 3, which is recommended from a security perspective.

QUESTION 144:
You have been tasked with enhancing the security of the management protocols used on the Certkiller routers. Which two management protocols provide security enhancements such as cryptographic authentication and packet encryption of management traffic? (Select two)

A. TFTP version 3
B. NTP version 3
C. Telnet version 3
D. SNMP version 3
E. Syslog version 3

Answer: B, D

Explanation:
SNMP is a network management protocol that you can use to retrieve information from a network device (commonly referred to as read-only access) or to remotely configure parameters on the device (commonly referred to as read-write access). SNMP version 1 and 2 uses passwords (called community strings) within each message as a simple form of security. Unfortunately, SNMPv1/v2 devices send the community string in plaintext along with the message. Therefore, SNMPv1/v2 messages may be intercepted by anyone with a packet sniffer located along the data path between the device and the management

server. SNMPv3 overcomes these shortcomings by providing authentication and encryption to the message exchange.
Network Time Protocol (NTP) is used to synchronize the clocks of various devices across a network. Synchronization of the clocks within a network is critical for digital certificates and for correct interpretation of events within syslog data. A secure method of providing clocking for the network is for network administrators to implement their own master clocks for private networks synchronized, via satellite or radio, to Coordinated Universal Time (UTC). However, if network administrators do not wish to implement their own master clocks because of cost or other reasons, clock sources are available for synchronization via the Internet.
The current version of NTP is version 4. The latest version defined by an RFC is version 3, which is recommended from a security perspective.

QUESTION 145:
The Certkiller security administrator wants to increase the security of all the routers within the network. Which three techniques should be used to secure management protocols in Cisco routers? (Select three)

A. Synchronize the NTP master clock with an Internet atomic clock.
B. Configure SNMP with only read-only community strings.
C. Implement RFC 2827 filtering at the perimeter router when allowing syslog access from devices on the outside of a firewall.
D. Encrypt TFTP and syslog traffic in an IPSec tunnel.
E. Use SNMP version 2.
F. Use TFTP version 3 or above because these versions support a cryptographic authentication mechanism between peers.

Answer: B, C, D

Explanation:
SNMP community strings act like passwords. An SNMP community string is a text string used to authenticate messages between a management station and an SNMP engine: If the manager sends one of the correct read-only community strings, it can get information, but not set information in an agent. If the manager uses one of the correct read-write community strings, it can get or set information in the agent. In effect, having read-write access is equivalent to having the enable password. SNMP agents accept commands and requests only from SNMP systems using the correct community string. By default, most SNMP systems use a community string of "public." If you configure your router SNMP agent to use this commonly known community string, anyone with an SNMP system is able to read the router MIB. Because router MIB variables can point to things like routing tables and other security-critical parts of the router configuration, it is important that you create your own custom SNMP community strings.
SNMP is a network management protocol that you can use to retrieve information from a network device (commonly referred to as read-only access) or to remotely configure parameters on the device (commonly referred to as read-write access). SNMP version 1 and 2 uses passwords (called community strings) within each message as a simple form

of security. Unfortunately, SNMPv1/v2 devices send the community string in plaintext along with the message. Therefore, SNMPv1/v2 messages may be intercepted by anyone with a packet sniffer located along the data path between the device and the management server. SNMPv3 overcomes these shortcomings by providing authentication and encryption to the message exchange.
TFTP and syslog traffic goes by default into plain text format, Using different packet sniffers can capture packets and read easily so it should encrypted or tunneled before sending the data.

QUESTION 146:
A Certkiller router was recently upgraded to the firewall feature set. Which two statements are true about Cisco IOS Firewall? (Select two)

A. It is implemented as a per-destination process.
B. It enhances security for TCP and UDP applications.
C. It enhances security for TCP applications only.
D. It is implemented as a per-application process.
E. It enhances security for UDP applications only.

Answer: B, D

Explanation:
Firewalls enforce access control between networks, which can be of different types and levels of trust. A common name for a group of networks reachable over a single firewall network interface is a security zone. A security zone is therefore an administratively separate domain, to or from which a firewall can filter incoming or outgoing traffic. The most notable security zones are inside and outside networks that are connected to firewalls over inside or outside interfaces, respectively.
Firewall operations are based on one of the three technologies:
Packet filtering: Packet filtering limits information entering a network based on static packet header information. Packet filtering is usually employed by a Layer 3 device to statically define access control lists (ACLs) that determine which traffic is permitted or denied. Packet filtering can examine protocol header information up to the transport layer to permit or deny certain traffic. Packets that make it through the filters are sent to the requesting system. All other packets are discarded.
ALGs work at the application layer. An ALG is a special piece of software designed to relay application-layer requests and responses between endpoints. An ALG acts as an intermediary between an application client, for which it acts as a virtual server, and a server, for which it acts as a virtual client. The client connects to the proxy server and submits an application layer request. The application layer request includes the true destination and the data request itself. The proxy server analyzes the request and may filter or change its contents, and then opens a session to the destination server. The destination server replies to the proxy server. The proxy server passes the response, which may be filtered and changed, back to the client.
Stateful packet filtering: Stateful packet filtering combines the best of packet filtering and proxy server technologies. Firewalls using stateful packet filtering are also called

hybrid firewalls. Stateful packet filtering is the most widely used firewall technology. Stateful packet filtering is an application-aware method of packet filtering that works on the connection, or flow, level. Stateful packet filtering maintains a state table to keep track of all active sessions crossing the firewall. A state table, which is part of the internal structure of the firewall, tracks all sessions and inspects all packets passing through the firewall. If packets have the expected properties, predicted by the state table, they are forwarded. The state table changes dynamically according to the traffic flow.

QUESTION 147:
A new Certkiller router with the IOS Firewall feature set needs to be configured.
Which three statements about IOS Firewall configurations are true? (Select three)

A. The ACL applied in the inbound direction on the unsecured interface should be an extended ACL.
B. The IP inspection rule can be applied in the inbound direction on the secured interface.
C. The IP inspection rule can be applied in the outbound direction on the unsecured interface.
D. For temporary openings to be created dynamically by Cisco IOS Firewall, the IP inspection rule must be applied to the secured interface.
E. For temporary openings to be created dynamically by Cisco IOS Firewall, the access-list for the returning traffic must be a standard ACL.
F. The ACL applied in the outbound direction on the unsecured interface should be an extended ACL.

Answer: A, B, C

Explanation:
You must decide whether to configure Cisco IOS Firewall on an internal or external router interface. If you configure the firewall in two directions, you should configure the inspection in one direction first, using the appropriate internal and external interface designations. When you configure the inspection in the other direction, the interface designations will be swapped.
Follow these general rules when evaluating your IP ACLs at the firewall:
* Start with a basic configuration. A basic initial configuration allows all network traffic to flow from protected networks to unprotected networks, while it blocks network traffic from any unprotected networks.
* Permit traffic that should be inspected by the Cisco IOS Firewall. For example, if Telnet will be inspected by the firewall, then Telnet traffic should be permitted on all ACLs that apply to the initial Telnet flow.
* Use extended ACLs to filter traffic entering the router from the unprotected networks. For temporary openings to be created dynamically by Cisco IOS Firewall, the access control list (ACL) for the returning traffic must be an extended ACL.
* Deny any inbound traffic (incoming on external interface) from a source address matching an address on the protected network. This is known as antispoofing protection, because it prevents traffic from an unprotected network from assuming the identity of a device on the protected network.

* Deny broadcast messages with a source address of 255.255.255.255. This entry helps to prevent broadcast attacks.
* By default, the last entry in an ACL is an implicit denial of all IP traffic not specifically allowed by other entries in the ACL. Optionally, you can add an entry to the ACL denying IP traffic with any source or destination address, thus making the denial rule explicit. This is especially useful if you want to log information about the denied packets.

QUESTION 148:
What should the Certkiller security administrator who uses SDM consider when configuring the firewall on an interface that is used in a VPN connection?

A. The firewall must permit encrypted traffic between the local and remote VPN peers.
B. The firewall must permit traffic to a VPN concentrator only.
C. The firewall must permit traffic going out of the local interface only.
D. The firewall cannot be configured in conjunction with a VPN.
E. None of the above

Answer: A

Explanation:
The Cisco IOS Firewall Feature Set is a security-specific option for Cisco IOS software available in security IOS images. It integrates robust firewall functionality, authentication proxy, and intrusion prevention for every network perimeter, and enriches existing Cisco IOS security capabilities. It adds more flexibility to existing Cisco IOS security solutions, such as authentication, encryption, and failover, by delivering application-based filtering; dynamic per-user authentication and authorization; defense against network attacks; Java blocking; and real-time alerts. When combined with Cisco IOS IPsec software and other Cisco IOS software-based technologies, such as Layer 2 Tunneling Protocol (L2TP) and quality of service (QoS), the Cisco IOS Firewall provides a complete, integrated virtual private network (VPN) solution.
The Cisco IOS Firewall features are designed to prevent unauthorized external individuals from gaining access to your internal network and to block attacks on your network, while at the same time allowing authorized users to access network resources.

QUESTION 149:
A Certkiller router was recently upgraded to the firewall feature set. Which two statements are true about the Cisco IOS Firewall set? (Select two)

A. Traffic originating within the router is not inspected.
B. protects against denial of service (DoS) attacks
C. An ACL entry is statically created and added to the existing, permanent ACL.
D. Temporary ACL entries are created and persist for the duration of the communication session.

Answer: B, D

Explanation:
Cisco IOS Firewall intelligently filters TCP and UDP packets based on application layer protocol session information. It inspects traffic for sessions that originate on any interface of the router and manages state information for TCP and UDP sessions. This state information is used to create temporary openings in the ACLs to allow return traffic and additional data connections for permissible sessions.
Inspecting packets at the application layer and maintaining TCP and UDP session information helps prevent certain types of network attacks, such as SYN flooding. Cisco IOS Firewall inspects packet sequence numbers in TCP connections to see if they are within expected ranges, and drops any suspicious packets. Additionally, Cisco IOS Firewall can detect unusually high rates of new connections and issue alert messages. The firewall inspection can help protect against certain denial of service (DoS) attacks involving fragmented IP packets.

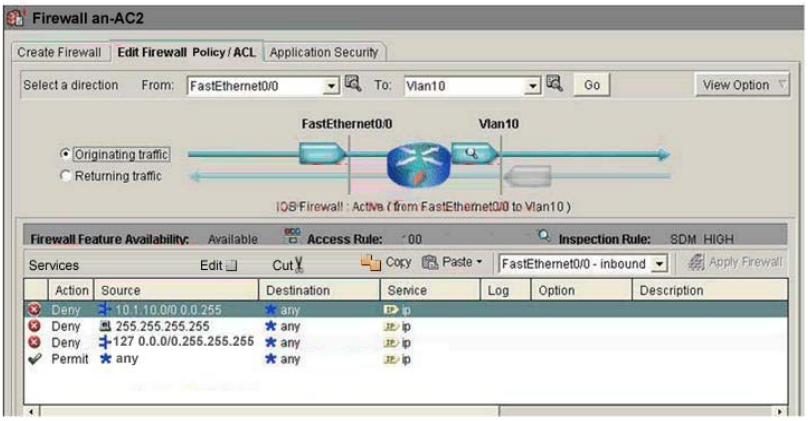
QUESTION 150:
You need to configure access rules on a new Certkiller router with the firewall feature set. Which three statements are true about a Cisco IOS Firewall? (Select three)

A. It can be configured to block Java traffic.
B. The inspection rules can be used to set timeout values for specified protocols.
C. It can be configured to detect and prevent SYN-flooding denial-of-service (DoS) network attacks.
D. The ip inspect cbac-name command must be configured in global configuration mode.
E. It can only examine network layer and transport layer information.
F. It can only examine transport layer and application layer information.

Answer: A, B, C

Explanation:
Cisco IOS Firewall intelligently filters TCP and UDP packets based on application layer protocol session information. It inspects traffic for sessions that originate on any interface of the router and manages state information for TCP and UDP sessions. This state information is used to create temporary openings in the ACLs to allow return traffic and additional data connections for permissible sessions. Inspecting packets at the application layer and maintaining TCP and UDP session information helps prevent certain types of network attacks, such as SYN flooding. Cisco IOS Firewall inspects packet sequence numbers in TCP connections to see if they are within expected ranges, and drops any suspicious packets. Additionally, Cisco IOS Firewall can detect unusually high rates of new connections and issue alert messages. The firewall inspection can help protect against certain denial of service (DoS) attacks involving fragmented IP packets.

QUESTION 151:
The Basic Firewall wizard has been used to configure a router as shown in the diagram below:

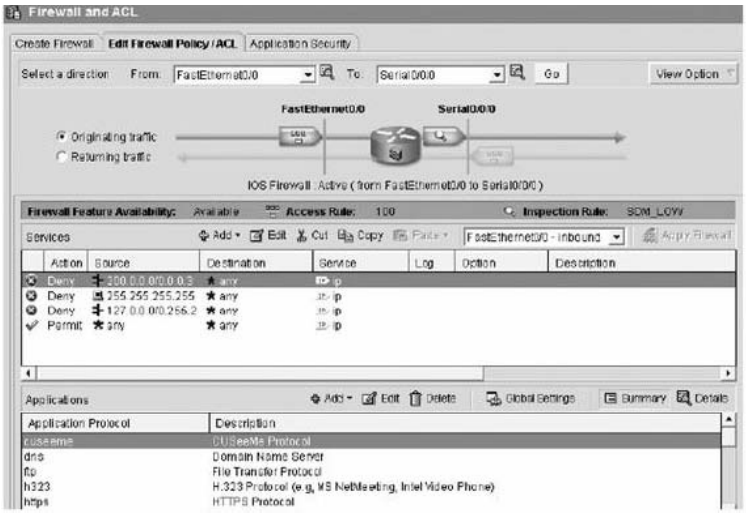


Based on the information above, what is the purpose of the highlighted access list statement?

A. to establish a DMZ by preventing traffic from interface VLAN10 being sent out interface Fa0/0
B. to prevent spoofing by blocking traffic entering interface Fa0/0 with a source address in the same subnet as interface VLAN10
C. to prevent spoofing by blocking traffic entering Fa0/0 with a source address in the RFC 1918 private address space
D. to establish a DMZ by preventing traffic from interface Fa0/0 being sent out interface VLAN10

Answer: B

Explanation:
SDM, a configuration and management tool for Cisco IOS routers using a GUI, offers a simple method to set up the Cisco IOS Firewall. Depending on the number of router interfaces, you will select either the Basic Firewall Configuration wizard, which supports only one outside interface and one or more inside interfaces, or the Advanced Firewall Configuration wizard, which, in addition to the inside and outside interfaces, also supports a DMZ interface.
When the firewall features are configured on the router, the wizard finishes and you are placed in the Edit Firewall Policy / ACL tab of the Firewall and ACL menu. In this window, you can review and modify the configured options. The figure illustrates how to view the ACL entries applied for the originating traffic (ACL 100 in this example); in other words, you examine the ACL that is applied to the inside interface in inbound direction.
Example:



ACL 100 is applied inbound to the inside interface. It prevents spoofing by denying packets sourced from 200.0.0.0/30 network, which is configured on the outside interface. The ACL also blocks packets sourced from the broadcast address and the 127.0.0.0/8 network and permits all other traffic. The inspection rule name in this example is SDM_LOW In this example, the firewall is active from the Fa0/0 to S0/0/0 direction, where Fa0/0 is in the inside (trusted) interface and S0/0/0 is the outside (untrusted) interface. You can also verify that the firewall is active by the firewall icon displayed inside the router icon.

QUESTION 152:

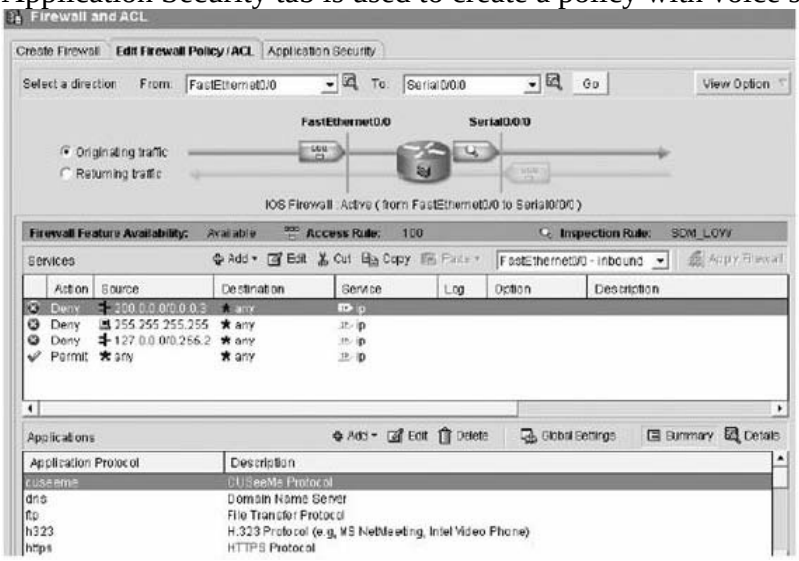
A Certkiller site using VOIP requires support for skinny and H.323 voice protocols. How is this configured on an IOS firewall using the SDM?

A. The Application Security tab is used to create a policy with voice support before the Firewall wizard is run.
B. The Application Security tab is used to modify the SDM_High policy to add voice support prior to the Firewall wizard being run.
C. The Advanced Firewall wizard is executed and a custom Application Security policy is selected in place of the default Application Security policies.
D. The Basic Firewall wizard is executed and the High Security Application policy is selected.
E. Noe of the above

Answer: C

Explanation:

Application Security tab is used to create a policy with voice support.



QUESTION 153:

A new Certkiller router needs to be configured using SDM. Which three statements are true when configuring Cisco IOS Firewall features using the SDM? (Select three)

A. An optional DMZ interface can be specified in the Advanced Firewall Interface Configuration dialog box.
B. Custom application policies for e-mail, instant messaging, HTTP, and peer-to-peer services can be created using the Intermediate Firewall wizard.
C. The SDM provides a basic, intermediate, and advanced firewall wizard.
D. Only the outside (untrusted) interface is specified in the Basic Firewall Interface Configuration dialog box.
E. The outside interface that SDM can be launched from is configured in the Configuring Firewall for Remote Access dialog box.
F. A custom application security policy can be configured in the Advanced Firewall Security Configuration dialog box.

Answer: A, E, F

Explanation:
SDM, a configuration and management tool for Cisco IOS routers using a GUI, offers a simple method to set up the Cisco IOS Firewall. Depending on the number of router interfaces, you will select either the Basic Firewall Configuration wizard, which supports only one outside interface and one or more inside interfaces, or the Advanced Firewall Configuration wizard, which, in addition to the inside and outside interfaces, also supports a DMZ interface. The Basic Firewall Configuration wizard applies default access rules to both inside and outside interfaces, applies default inspection rules to the outside interface, and enables IP unicast reverse-path forwarding on the outside interface. The Advanced Firewall Configuration wizard applies default or custom access rules, as well as default or custom inspection rules, to inside, outside, and DMZ interfaces.

Furthermore, the Advanced Firewall Configuration wizard enables IP unicast reverse-path forwarding on the outside

---

QUESTION 154:
A new Certkiller router needs to be configured using SDM. Which two commands will start services that should be enabled for SDM operations? (Select two)

A. ip http secure-server
B. ip http authentication local
C. service tcp-small-servers
D. service password-encryption
E. ip dhcp-client network-discovery

Answer: A, B

Explanation:
The CiscoIOS HTTP server provides authentication, but not encryption, for client connections. The data that the client and server transmit to each other is not encrypted. This leaves communication between clients and servers vulnerable to interception and attack.
The Secure HTTP (HTTPS) feature provides the capability to connect to the CiscoIOS HTTPS server securely. It uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption
Enabling HTTPS To enable HTTPS, enter the following command in global configuration mode:

Command	Purpose
Router(config)# **ip http secure-server**	Enables HTTPS.

Disabling HTTPSTo disable HTTPS, enter the following command in global configuration mode:

Command	Purpose
Router(config)# **no ip http secure-server**	Disables HTTPS.

Changing the HTTPS Port Number The default HTTPS port number is 443. To change the HTTPS port number, enter the following command in global configuration mode:

Command	Purpose
Router(config)# **ip http secure-port** *port_number*	Changes the secure HTTPS port number. The acceptable range is 1-65535.

The HTTPS server uses the same authentication configuration settings as the HTTP server. Configuring HTTP authentication using the ip http authentication command also configures authentication for HTTPS. Configuring authentication for the HTTP and HTTPS servers adds additional security to communication between clients and the HTTP and HTTPS servers on the device.

QUESTION 155:
You need to configure a new Certkiller router's firewall function via the SDM.

Which two statements are true about the configuration of the Cisco IOS Firewall using the SDM? (Select two)

A. The Advanced Firewall Configuration wizard applies access rules to the inside (trusted), outside (untrusted) and DMZ interfaces.
B. To simplify the Firewall configuration task, the SDM provides Basic Firewall, Intermediate Firewall, and Advanced Firewall wizards.
C. Cisco IOS Firewall features may be configured by choosing the Additional Tasks wizard.
D. The Basic Firewall Configuration wizard applies default access rules to the inside (trusted), outside (untrusted) and DMZ interfaces.
E. Firewall policies can be viewed from the Home screen of the SDM.

Answer: A, E

Explanation:
SDM, a configuration and management tool for Cisco IOS routers using a GUI, offers a simple method to set up the Cisco IOS Firewall. Depending on the number of router interfaces, you will select either the Basic Firewall Configuration wizard, which supports only one outside interface and one or more inside interfaces, or the Advanced Firewall Configuration wizard, which, in addition to the inside and outside interfaces, also supports a DMZ interface. The Basic Firewall Configuration wizard applies default access rules to both inside and outside interfaces, applies default inspection rules to the outside interface, and enables IP unicast reverse-path forwarding on the outside interface. The Advanced Firewall Configuration wizard applies default or custom access rules, as well as default or custom inspection rules, to inside, outside, and DMZ interfaces. Furthermore, the Advanced Firewall Configuration wizard enables IP unicast reverse-path forwarding on the outside

---

QUESTION 156:
You need to configure a new Certkiller router via the SDM firewall wizard. Which statement is true about the SDM Basic Firewall wizard?

A. The wizard permits the creation of a custom application security policy.
B. The wizard can configure multiple DMZ interfaces for outside users.
C. The wizard configures one outside interface and one or more inside interfaces.
D. The wizard applies predefined rules to protect the private and DMZ networks.
E. None of the above.

Answer: C

Explanation:
SDM, a configuration and management tool for Cisco IOS routers using a GUI, offers a simple method to set up the Cisco IOS Firewall. Depending on the number of router interfaces, you will select either the Basic Firewall Configuration wizard, which supports only one outside interface and one or more inside interfaces, or the Advanced Firewall Configuration wizard, which, in addition to the inside and outside interfaces, also supports a DMZ interface.

The Basic Firewall Configuration wizard applies default access rules to both inside and outside interfaces, applies default inspection rules to the outside interface, and enables IP unicast reverse-path forwarding on the outside interface.
The Advanced Firewall Configuration wizard applies default or custom access rules, as well as default or custom inspection rules, to inside, outside, and DMZ interfaces. Furthermore, the Advanced Firewall Configuration wizard enables IP unicast reverse-path forwarding on the outside

---

QUESTION 157:
You need to configure a new Certkiller router using the Cisco SDM. Which privilege level is required when configuring the SDM?

A. 1
B. 12
C. 0
D. 8
E. 10
F. 15
G. 255

Answer: F

Explanation:
SDM is an easy-to-use, browser-based device management tool that is used to configure single Cisco IOS routers. It is embedded within the Cisco IOS 800 through 3700 series routers at no additional cost. The SDM software files reside in the router's Flash Memory alongside other router operating system files.
SDM simplifies router and security configuration through the use of several intelligent wizards to enable efficient configuration of key router VPN and Cisco IOS Firewall parameters. This capability permits administrators to quickly and easily deploy, configure, and monitor Cisco access routers.
SDM is designed for resellers and network administrators of small- to medium-sized businesses who are proficient in LAN fundamentals and basic network design, but have little or no experience with the Cisco IOS CLI or may not be a security expert.
SDM is designed to help you secure your Cisco routers and their associated networks without having to memorize multiple CLI commands or having to be an expert in network security. For more advanced users, SDM provides several time-saving tools, such as an ACL Editor, a VPN Crypto Map Editor, and a preview of Cisco IOS CLI commands.
You can retain your existing configuration file and configure the router to be an HTTP/ HTTP Secure (HTTPS) router using local authentication. Configure a local user with a privilege level of 15. Configure vty connections to use local login with a privilege level of 15. An optional recommended step is to turn on local logging.

QUESTION 158:
Part of the configuration file for a Certkiller router is displayed below:

```
hostname  Certkiller
!
logging buffered 51200 warnings
!
username cisco privilege 15 secret 0 cisco
!
ip domain-name certkiller.com
!
interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
  ip address 10.10.10.1.255.255.255.248
   no shutdown
!
ip http server
ip http secure-server
ip http authentication local
ip http timeout-policy idle 5 life 86400 requests 10000
 <Output omitted>
line con 0
 login local
line vty 0 4
 privilege level 15
 login local
 transport input telnet
 transport input telnet ssh
line vty 5 15
 privilege level 15
 login local
 transport input telnet
 transport input telnet ssh
!
! End of SDM default config file
end
```

Based on this information, what is one of the objectives accomplished by the default startup configuration file created by the SDM?

A. Blocks both Telnet and SSH
B. Encrypts all HTTP traffic to prevent man-in-the-middle attacks
C. Prevents the router from ever being used as an HTTP server
D. Requires access authentication by a TACACS+ server
E. Enables local logging to support the log monitoring function
F. None of the above

Answer: E

Explanation:
By default, there are three privilege levels on the router.
* privilege level 1 = non-privileged (prompt is router>), the default level for logging in
* privilege level 15 = privileged (prompt is router#), the level after going into enable mode
* privilege level 0 = seldom used, but includes 5 commands: disable, enable, exit, help, and logout
Levels 2-14 are not used in a default configuration, but commands that are normally at level 15 can be moved down to one of those levels and commands that are normally at

level 1 can be moved up to one of those levels. Obviously, this security model involves some administration on the router
Example:
Privilege level 15 : Defines the privilege level
Login local : Method of Login

QUESTION 159:
A Certkiller router was configured as shown below:

```
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw tcp timeout 3600
ip inspect name myfw UDP timeout 3600
ip inspect name myfw ftp timeout 3600
interface Ethernet0/1
      ip address 172.16.1.2 255.255.255.0
      ip access-group 111 in
      ip inspect myfw out
access list 111 deny   Company 10.1.1.0 0.0.0.255 echo
access-list 111 permit icmp any 10.1.1.0 0.0.0.255
```

What is the configuration of this Certkiller router an example of?

A. infrastructure protection ACLs
B. Authentication Proxy
C. reflexive ACLs
D. turbo ACLs
E. distributed time-based ACLs
F. IOS firewall

Answer: F

Explanation:
The Cisco IOS Firewall, formerly known as CBAC, is the stateful packet filtering engine of a Cisco IOS router. Cisco IOS Firewall allows you to implement firewall intelligence as part of an integrated, single-box solution.
For example, sessions with an extranet partner involving Internet applications, multimedia applications, or Oracle databases no longer need to open a network doorway accessible via weaknesses in the network of a partner. The stateful engine enables tightly secured networks to run the basic application traffic as well as advanced applications, such as multimedia and videoconferencing, securely through a router.

QUESTION 160:
The following command was shown in the following exhibit:

```
Certkiller1 #show ip inspect session
Established sessions
Session 624C3 A4 (20.0.01.1:11006/->(150.150  .150.2:23) tcp SIS_OPEN
```

Based on the output shown above, what type of security configuration is being

verified?

A. Turbo ACLs
B. IOS Firewall
C. Authentication Proxy
D. Reflexive ACLs
E. Distributed Time-Based ACLs
F. Infrastructure Protection ACLs
G. None of the above

Answer: B

Explanation:
Use the show ip inspectEXEC command to display information about various components of Cisco IOS Firewall.
Show ip inspect session detail: Shows existing sessions that are currently being tracked and inspected by Cisco IOS firewall. The optional detail keyword shows additional details about these sessions.
Example:
Router#showipinspectsessiondetail
EstablishedSessions
Session80E87274(192.168.1.116:32956)=>(192.168.101.115:23)tcpSIS_OPEN
Created00:00:08,Lastheard00:00:04
Bytessent(initiator:responder)[140:298]aclcreated2
Outgoingaccess-list102appliedtointerfaceFastEthernet0/0
Inboundaccess-list101appliedtointerfaceFastEthernet0/1

QUESTION 161:
A Certkiller router was configured as show below:

```
ip inspect name myfw ftp timeout 3600
 ip inspect name myfw ftp timeout 3600
ip inspect name myfw tcp timeout 3600
ip inspect name myfw udp timeout 3600
ip inspect name myfw tftp timeout 3600
interface Ethernet0/1
      ip address 172. 16.1.2.255.255.0
      ip access-group 111 in
      ip inspect myfw out
access-list 111 deny icmp any 10.1.1.0 0.0.0.255 echo
access-list 111 permit icmp any 10.1.1.0 0.0.0.255
```

Based on the information shown above, what does this configuration accomplish?

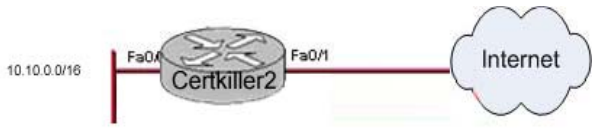
A. For the specified protocols, the configuration results in a timeout value of 3600 seconds for authentication of encrypted traffic.
B. The configuration creates temporary openings in the access lists of the firewall. These openings have an absolute timeout value.
C. The configuration permits ICMP outbound traffic, denies ICMP inbound traffic, and permits traffic that has been initiated from inside a router that has been synched with an

NTP server.
D. The configuration uses NTP synchronization to implement time-based ACLs.
E. The configuration permits ICMP inbound traffic, denies ICMP outbound traffic, and permits traffic that has been initiated from inside a router that has been synched with an NTP server.
F. The configuration creates temporary openings in the access lists of the firewall. These openings time out after the specified period of inactivity.
G. None of the above.

Answer: F

Explanation:
You must define inspection rules to specify which IP traffic (that is, which application layer protocols) will be inspected by Cisco IOS Firewall at an interface.
The inspection rule consists of a series of statements, each listing a protocol and specifying the same inspection rule name. Inspection rules include options for controlling alert and audit trail messages, and for checking IP packet fragmentation. In the figure, the IP inspection rule shown is named FWRULE. This rule will inspect the extended Simple Mail Transfer Protocol (SMTP) and FTP protocols with alert and audit trail enabled, and an idle timeout of 300 seconds. Use the ip inspectname command in global configuration mode to define a set of inspection rules. Use the no form of this command to remove the inspection rule for a protocol, or to remove the entire set of inspection rules.
ipinspect name inspection-name protocol [alert {on | off}] [audit-trail {on | off}] [timeout seconds]

QUESTION 162:
Router Certkiller 2 connects to the Internet as shown below:



Router Certkiller 2 is also configured as shown below:

```
Certkiller2# show running-config | include inspect
ip inspect name FIREWALL_ACL suseem  timeout 3600
ip inspect name FIREWALL_ACL rcmd timeout 3600
ip inspect name FIREWALL_ACL http timeout 3600
ip inspect name FIREWALL_ACL rcmd timeout 3600
ip inspect name FIREWALL_ACL realaudio timeout 3600
ip inspect name FIREWALL_ACL smtp timeout 3600
ip inspect name FIREWALL_ACL titp timeout 30
ip inspect name FIREWALL_ACL udp timeout 15
ip inspect name FIREWALL_ACL tcp timeout 3600
```

The Certkiller network administrator wishes to mitigate network threats. Given that purpose, which two statements about the IOS firewall configuration shown above

are true?

A. The command ip access-group FIREWALL_ACL in must be applied on interface FastEthernet 0/1.
B. The command ip inspect FIREWALL_ACL out must be applied on interface FastEthernet 0/0.
C. The configuration excerpt is an example of a reflexive ACL.
D. The command ip access-group FIREWALL_ACL in must be applied on interface FastEthernet 0/0.
E. The command ip inspect FIREWALL_ACL out must be applied on interface FastEthernet 0/1.
F. The configuration excerpt is an example of a CBAC list.

Answer: E, F

Explanation:
The inspection rule consists of a series of statements, each listing a protocol and specifying the same inspection rule name. Inspection rules include options for controlling alert and audit trail messages, and for checking IP packet fragmentation. In the figure, the IP inspection rule shown is named FWRULE. This rule will inspect the extended Simple Mail Transfer Protocol (SMTP) and FTP protocols with alert and audit trail enabled, and an idle timeout of 300 seconds. Use the ip inspectname command in global configuration mode to define a set of inspection rules. Use the no form of this command to remove the inspection rule for a protocol, or to remove the entire set of inspection rules.
ipinspect name inspection-name protocol [alert {on | off}] [audit-trail {on | off}] [timeout seconds]
After creating inspect rules you need to apply on interface.
Router(Config-if)#ip inspect inspect_rule { in | out}

QUESTION 163:
The Certkiller network administrator issued the "no ip inspect" command on a Cisco IOS firewall device. What are three objectives that this command achieves? (Select three)

A. It removes the entire CBAC configuration
B. It denies HTTP and Java applets to the inside interface but permits this traffic to the DMZ
C. It removes all associated static ACLs
D. It resets all global timeouts and thresholds to the defaults
E. It deletes all existing sessions
F. It turns off the automatic audit feature in SDM

Answer: A, D, E

Explanation:

The inspection rule consists of a series of statements, each listing a protocol and specifying the same inspection rule name. Inspection rules include options for controlling alert and audit trail messages, and for checking IP packet fragmentation. In the figure, the IP inspection rule shown is named FWRULE. This rule will inspect the extended Simple Mail Transfer Protocol (SMTP) and FTP protocols with alert and audit trail enabled, and an idle timeout of 300 seconds.
Use the ip inspect name command in global configuration mode to define a set of inspection rules. Use the no form of this command to remove the inspection rule for a protocol, or to remove the entire set of inspection rules.

QUESTION 164:
A Certkiller IOS firewall is configured as shown below:

```
!
ip inspect name voice skinny
ip inspect name voice h323
ip inspect name voice tcp
ip inspect name voice udp
!
interface FastEthernet0/0
 ip address 10.1.1.254 255.255.255.0
 ip access-group 100 in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.10.254 255.255.255.0
 ip access-group 101 in
 ip verify unicast reverse-path
 ip inspect voice in
!
!
ip http server
no ip http secure-server
!
access-list 100 deny   ip 10.1.10.0 0.0.0.255 any
access-list 100 deny   ip host 255.255.255.255 any
access-list 100 deny   ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip any any
!
access-list 101 permit icmp any host 10.1.10.254 echo-reply
access-list 101 permit icmp any host 10.1.10.254 time-exceeded
access-list 101 permit icmp any host 10.1.10.254 unreachable
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
access-list 101 deny   ip host 255.255.255.255 any
access-list 101 deny   ip host 0.0.0.0 any
access-list 101 deny   ip any any log
!
```

This firewall has been configured to support skinny and H.323. Voice traffic is not passing through the firewall as expected. Based on the configuration shown above, what needs to be corrected in this configuration?

A. Access list 101 needs to permit skinny and H.323.
B. The "ip inspect voice in" command on interface FastEthernet 0/1 should be applied in the outbound direction.
C. Access list 100 needs to permit skinny and H.323.
D. The "ip inspect voice out" command should be applied to interface FastEthernet 0/0.
E. None of the above.

Answer: B

Explanation:
The inspection rule consists of a series of statements, each listing a protocol and specifying the same inspection rule name. Inspection rules include options for controlling

alert and audit trail messages, and for checking IP packet fragmentation. In the figure, the IP inspection rule shown is named FWRULE. This rule will inspect the extended Simple Mail Transfer Protocol (SMTP) and FTP protocols with alert and audit trail enabled, and an idle timeout of 300 seconds.
Use the ip inspect name command in global configuration mode to define a set of inspection rules. Use the no form of this command to remove the inspection rule for a protocol, or to remove the entire set of inspection rules.
After creating inspect rule you need to apply on interface using:
Router(Config-if)#ip inspect voice { in | out }

QUESTION 165:
A new Cisco IDS was installed in the Certkiller network. Which two statements about an Intrusion Detection System are true? (Select two)

A. The IDS can send TCP resets to the source device.
B. Default operation is for the IDS to discard malicious traffic.
C. The IDS can send TCP resets to the destination device.
D. The IDS is in the traffic path.
E. The IDS listens promiscuously to all traffic on the network.

Answer: A, E

Explanation:
The IDS is a software- or hardware-based solution that passively listens to network traffic. The IDS is not in the traffic path, but listens promiscuously to all traffic on the network. Typically, only one promiscuous interface is required for network monitoring. Additional promiscuous interfaces can be used to monitor multiple networks.
When the IDS detects malicious traffic, it sends an alert to the management station.
The IDS has limited active response capabilities. When configured, the IDS can block further malicious traffic by actively configuring network devices (for example, security appliances or routers) in response to malicious traffic detection. However, the original malicious traffic has already passed through the network to its destination and cannot be blocked. Only subsequent traffic will be blocked. The IDS also has the capability of sending a TCP reset to the end host to terminate any malicious TCP connections.

QUESTION 166:
The Certkiller security administrator is concerned about network based intrusions and wants to implement an IDS solution. Which statement is true about signature-based intrusion detection?

A. It performs analysis that is based on a predefined network security policy.
B. It performs analysis that is based on known intrusive activities by matching predefined patterns in network traffic.
C. It performs analysis by intercepting the procedural calls to the operating system kernel.
D. It performs analysis that is based on anomalies in packets or packet sequences. It also

verifies anomalies in traffic behavior.
E. None of the above

Answer: B

Explanation:
Signature-based pattern matching refers to searching for a fixed sequence of bytes in a single packet, or predefined content. As its name suggests, it is an approach that is fairly rigid but simple to employ. In most cases, the signature pattern is matched only if the suspect packet is associated with a particular service or, more precisely, destined to or from a particular port. This method lessens the amount of inspection done on every packet. However, it tends to make it more difficult for systems to deal with protocols that do not reside on well-defined ports, and, in particular, Trojan horses and their associated traffic, which can usually be moved at will.
Initially, there might be many alerts, but which are no threat for the network. After the system is tuned and adjusted to the specific network parameters, there will be fewer false alerts than with the policy-based approach.

QUESTION 167:
What is the purpose of Security Device Event Exchange (SDEE) messages?

A. SDEE messages can be viewed in real time using SDM.
B. For SDEE messages to be viewed, the show ip ips all or show logging commands must be given first.
C. SDEE messages are the SDM version of syslog messages.
D. SDEE specifies the IPS/IDS message exchange format between an IPS/IDS device and IPS the management/monitoring station.
E. SDEE messages displayed at the SDM window cannot be filtered.
F. None of the above

Answer: D

Explanation:
The Cisco IOS IPS acts as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router, and scanning each packet to match any of the Cisco IOS IPS signatures. When the IPS detects suspicious activity, it responds before network security can be compromised, and logs the event through syslog or Security Device Event Exchange (SDEE) protocol.
SDEE is an application level communication protocol that is used to exchange IPS messages between IPS clients and IPS servers. It provides a secure communication path using Secure Socket Layer (SSL) (Secure HTTP [HTTPS]). SDEE replaced the Post Office Protocol (POP) on Cisco IOS routers.

QUESTION 168:
In order to mitigate the threat of intrusions within the Certkiller network, the Certkiller network administrator has implemented Cisco IDS/IPS devices. Which

three statements are true about Cisco Intrusion Detection System (IDS) and Cisco Intrusion Prevention System (IPS) functions? (Select three)

A. IPS can detect misuse, abuse, and unauthorized access to networked resources and respond before network security can be compromised.
B. IDS can detect misuse, abuse, and unauthorized access to networked resources but can only respond after an attack is detected.
C. IDS can deny malicious traffic from the inside network whereas IPS can deny malicious traffic from outside the network.
D. The signatures on the IDS devices are configured manually whereas the signature on the IPS devices are configured automatically.
E. Only IDS systems provide real-time monitoring that includes packet capture and analysis of network packets.
F. Both IDS and IPS systems provide real-time monitoring that involves packet capture and analysis of network packets.

Answer: A, B, F

Explanation:
The IDS is a software- or hardware-based solution that passively listens to network traffic. The IDS is not in the traffic path, but listens promiscuously to all traffic on the network. Typically, only one promiscuous interface is required for network monitoring. Additional promiscuous interfaces can be used to monitor multiple networks.
When the IDS detects malicious traffic, it sends an alert to the management station.
The IDS has limited active response capabilities. When configured, the IDS can block further malicious traffic by actively configuring network devices (for example, security appliances or routers) in response to malicious traffic detection. However, the original malicious traffic has already passed through the network to its destination and cannot be blocked. Only subsequent traffic will be blocked. The IDS also has the capability of sending a TCP reset to the end host to terminate any malicious TCP connections.
When the IPS detects malicious traffic, it sends an alert to the management station and blocks the malicious traffic immediately. The original and subsequent malicious traffic is blocked as the IPS proactively prevents attacks. Because network attack mechanisms are becoming more sophisticated, this proactive approach is required to protect against network viruses, worms, malicious applications, and vulnerability exploits.

QUESTION 169:
When a new IPS device is installed in the Certkiller network it must be tuned to reduce the number of false positives. What is meant by the attack classification of "false positive" on a Cisco IPS device?

A. A signature is not fired when non-offending traffic is captured and analyzed.
B. A signature is not fired when offending traffic is detected.
C. A signature is fired for nonmalicious traffic, benign activity.
D. A signature is correctly fired when offending traffic is detected and an alarm is generated.

E. None of the above.

Answer: C

Explanation:
The Cisco IOS IPS acts as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router, and scanning each packet to match any of the Cisco IOS IPS signatures. When the IPS detects suspicious activity, it responds before network security can be compromised, and logs the event through syslog or Security Device Event Exchange (SDEE) protocol.
Cisco IOS IPS offers configuration flexibility by providing these two functions:
* The administrator can load the built-in signature database (available in the IOS image itself), load a specific signature database file (sdf), or even merge different databases to extend the protection scope.
* Individual signatures can be disabled or tuned in case of false positives.
IPS signature files are dynamically updated and posted to Cisco.com on a regular basis. Thus, customers can access signatures that help protect their network from the latest known network attacks. Multiple definition sources are available, such as the default, built-in signatures that are shipped with the routers, or the SDF files named 64MB.sdf, 128MB.sdf, and 256MB.sdf. They differ in the number of configured signatures. The administrator should select the appropriate SDF file based on the amount of RAM memory in the router. The SDF files are dynamically updated and accessed from Cisco.com.

QUESTION 170:
A new Cisco IPS device was just installed in the Certkiller network. When packets in a session match a signature, what are three actions that the Cisco IOS Firewall IPS can take? (Select three)

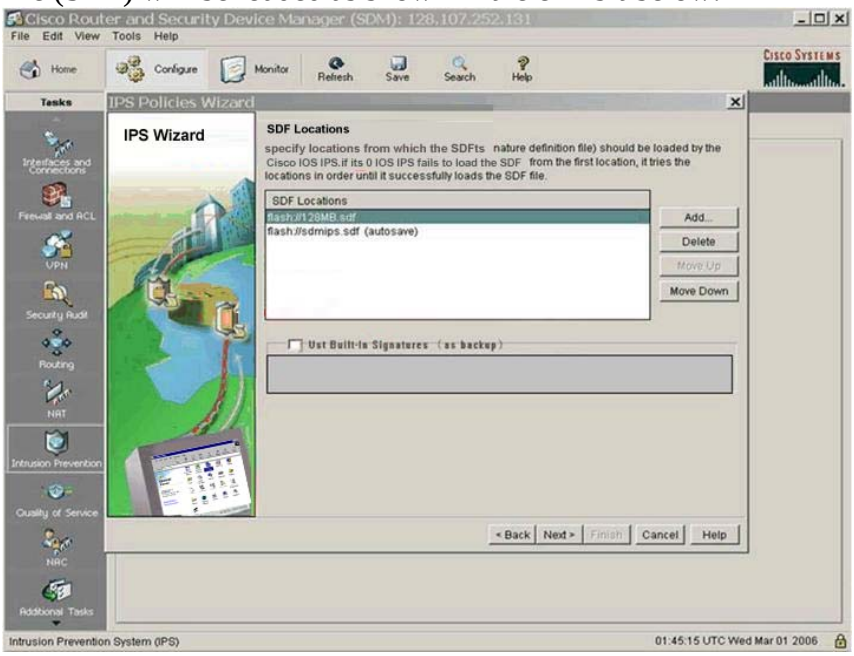
A. Drop the packets
B. Send an alarm to a syslog server
C. Reset the connection
D. Notify a centralized management interface of a false positive
E. Use the signature micro-engine to prevent a CAM Table Overflow Attack
F. Remove the virus or worm from the packets and forward the packet through

Answer: A, B, C

Explanation:
When a signature is matched, the IPS responds in real time, before network security can be compromised, and logs the event through Cisco IOS syslog messages or SDEE. You can configure IPS to choose the appropriate response to various threats. When packets in a session match a signature, IPS can take any of these actions, as appropriate:
1. Send an alarm to a syslog server or a centralized management interface. This action is typically combined with other preventive actions.
1. Drop the packet. This action is effective for all IP protocols and does not affect any

legitimate user if the source IP address was spoofed.
2. Reset the connection. This action works only for TCP sessions.

QUESTION 171:
SDM has been used to configure the locations from which the signature definition file (SDF) will be loaded as shown in the exhibit below:

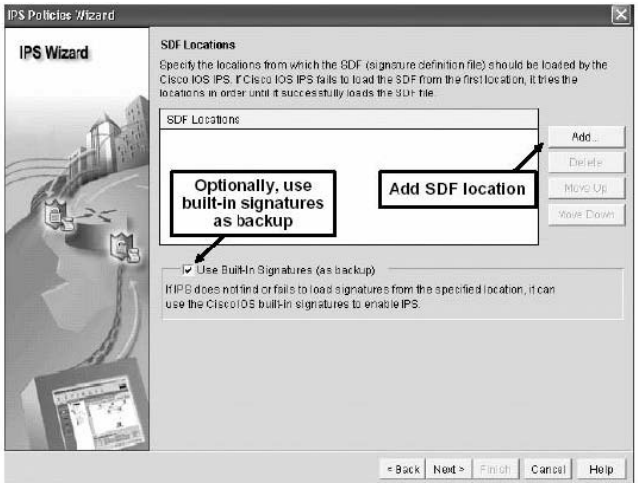


Based on the exhibit, what will happen if the SDF files in flash are not available at startup?

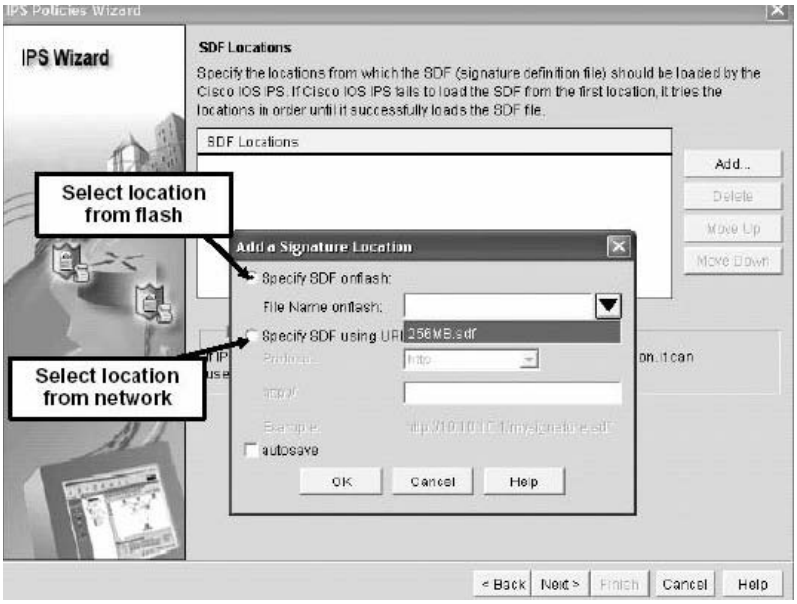
A. All traffic will be inspected by the pre-built signatures bundled in the attack-drop.sdf file.
B. All traffic will be marked as uninspected and will be checked after the signature file is loaded.
C. All traffic will be inspected by the built-in signatures bundled with Cisco IOS Software.
D. All traffic will flow uninspected or will be dropped.

Answer: D

Explanation:
You must specify which SDF should be used to load the signatures, and its location. Click the Add button to provide the information about the SDF location. Additionally, there is the Use Built-in Signatures (as backup) check box. If checked, the Cisco IOS built-in signature set will be used if the signatures cannot be loaded from the specified location or if no SDF location has been configured.



Here is the screen showing the currently configured SDF locations. You may configure more than one SDF location by clicking the Add button. If you configure more than one SDF location, Cisco IOS will try to load them, starting from the top of the list. If IOS fails to load the SDF from the first location in the list, it will try the subsequent locations one by one until it successfully loads the SDF file.



QUESTION 172:

You need to create policies on a new Certkiller IPS device. Which statement is true about the SDM IPS Policies wizard?

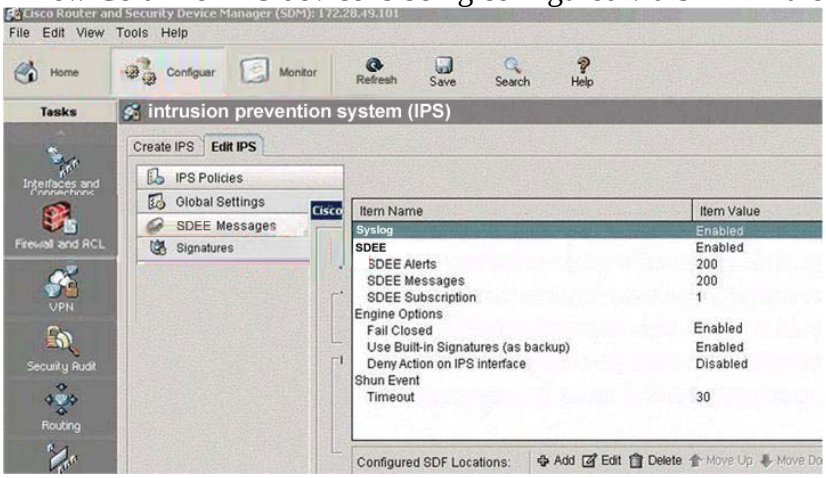
A. The IPS Policies wizard only allows the use of default signatures which cannot be modified.
B. When initially enabling the IPS Policies wizard, SDM automatically checks and downloads updates of default signatures available from CCO (cisco.com).
C. In order to configure the IPS, the wizard requires that customized signature files be created.
D. The wizard verifies whether the command is correct but does not verify available

router resources before the signatures are deployed to the router.
E. The IPS Policies wizard can be used to modify, delete, or disable signatures that have been deployed on the router.
F. None of the above.

Answer: E

Explanation:
The SDM provides a wide range of configuration capabilities for Cisco IOS IPS. All options are configurable through the IPS Edit menu.
Additionally, SDM offers the IPS Policies wizard, which expedites the deployment of default IPS settings. The wizard provides configuration steps for interface and traffic flow selection, SDF location, and signature deployment. The wizard also verifies the available router resources before the commands are sent to the router. The IPS Policies wizard configures IPS using default signature descriptions, as defined in the SDF files provided by Cisco, or the built-in signatures included in the Cisco IOS.
If you want to customize the signatures after the wizard deploys the default settings, you should use the IPS Edit menu available in SDM. Using the Edit menu, you can modify any signature parameter, as well as disable and delete the signatures.

QUESTION 173:
A new Certkiller IPS device is being configured via SDM in the following exhibit:

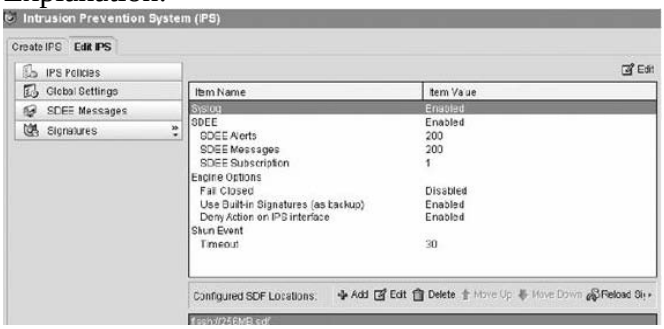


In this example, what are the ramifications of Fail Closed being enabled under Engine Options?

A. The router will drop all packets that arrive on the affected interface.
B. If the IPS detects any malicious traffic, it will cause the affected interface to close any open TCP connections.
C. The IPS engine is enabled to scan data and drop packets depending upon the signature of the flow.
D. If the IPS engine is unable to scan data, the router will drop all packets.
E. None of the above.

Answer: D

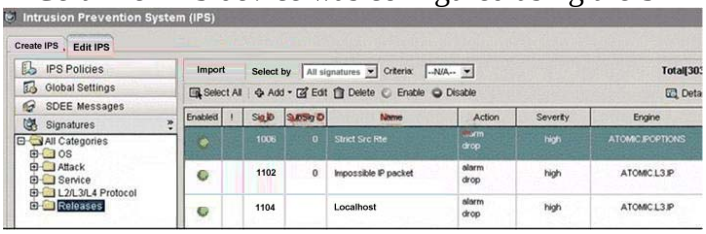
Explanation:



Click Global Settings in the menu of the Edit IPS tab to view and modify the general IPS settings configured on the router. These settings include reporting settings using two protocols: syslog and SDEE.
See the status of the fail-closed setting. SDM default is fail-closed disabled. If enabled, the router will drop all packets if the IPS engine is unable to scan data. Finally, you can verify if the built-in signatures have been enabled for backup purposes if the configured SDF is unavailable or cannot be loaded. If you want to modify any of these global settings, click the Edit button in the upper-right corner of the window to perform the desired changes.

QUESTION 174:

A Certkiller IPS device was configured using the SDM as shown below:



Assume that a signature can identify an IP address as the source of an attack.
Which action would automatically create an ACL that denies all traffic from an attacking IP address?

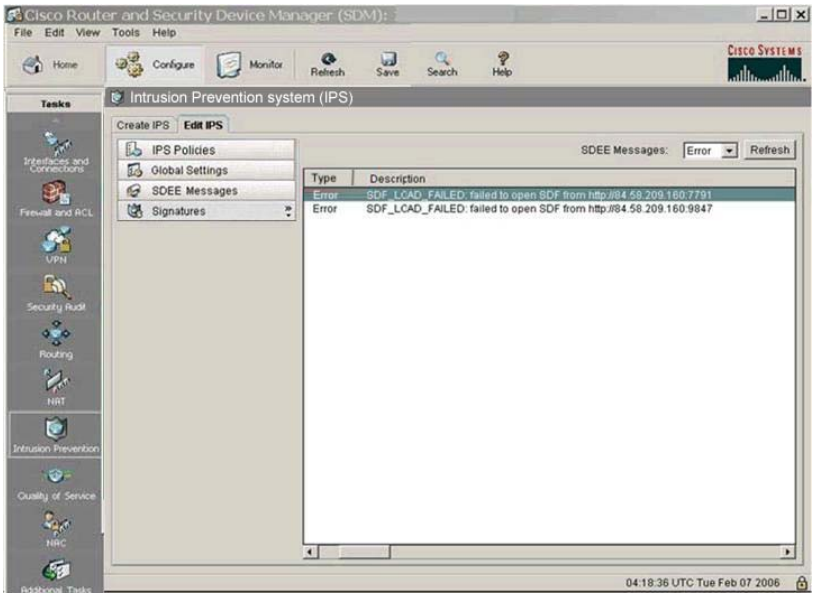
A. DenyAttackerInline
B. Alarm
C. Deny-connection-inline
D. Reset
E. Drop
F. DenyFlowInline
G. None of the above

Answer: A

Explanation:
The Cisco IOS IPS-enabled router uses this SDF to update the existing IPS configuration live, meaning that the number of running signatures and the way that the signatures are configured for actions to take when a signature match is made (alarm, drop, reset,

denyAttackerInline, and denyFlowInline) all can be changed without a Cisco IOS Software image update. Use of the SDF for signature selection is replaced by the selection of Cisco IOS Software signature categories or selection or deselection of individual signatures and tuning of their parameters through the command-line interface (CLI).

QUESTION 175:
The Certkiller network administrator used the Cisco SDM to manage the router as shown below:

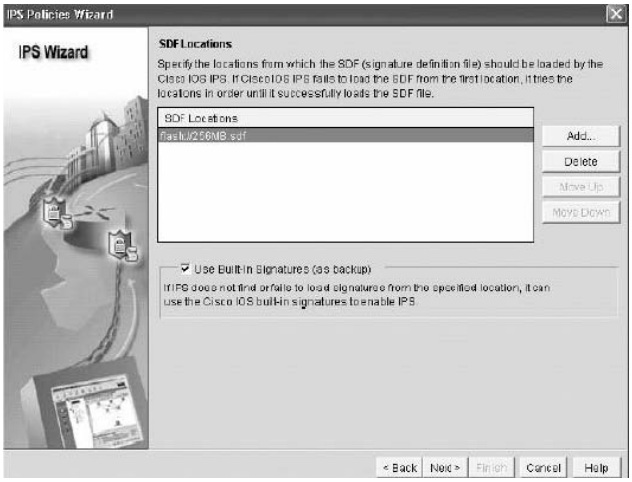


SDM has been used to configure IPS on the Certkiller router. While reviewing the Secure Device Event Exchange (SDEE) error messages, you noticed that SDM failed to load a signature definition file (SDF) from the specified URL locations. Which other location, if enabled, could the SDF be loaded from?

A. The RAM of a PC
B. The RAM of a router
C. The startup configuration file of a router
D. The flash memory of a router
E. The running configuration file of a router
F. None of the above

Answer: D

Explanation:
You may configure more than one SDF location by clicking the Add button. If you configure more than one SDF location, Cisco IOS will try to load them, starting from the top of the list. If IOS fails to load the SDF from the first location in the list, it will try the subsequent locations one by one until it successfully loads the SDF file. if SDM failed to load the signature file, it can load the signature from flash memory router.

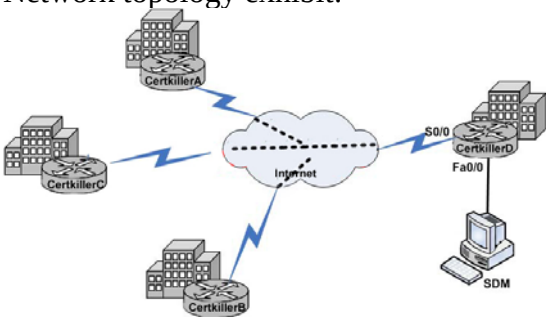


Topic 1, Certkiller Scenario, Scenario1

You work as a network administrator at Certkiller .com. You need to make retrieve some information from the Certkiller .com WAN being displayed in the network topology. You use the SDM (Cisco Router and Security Device Manager) to retrieve the information being presented in the other exhibits in this scenario.

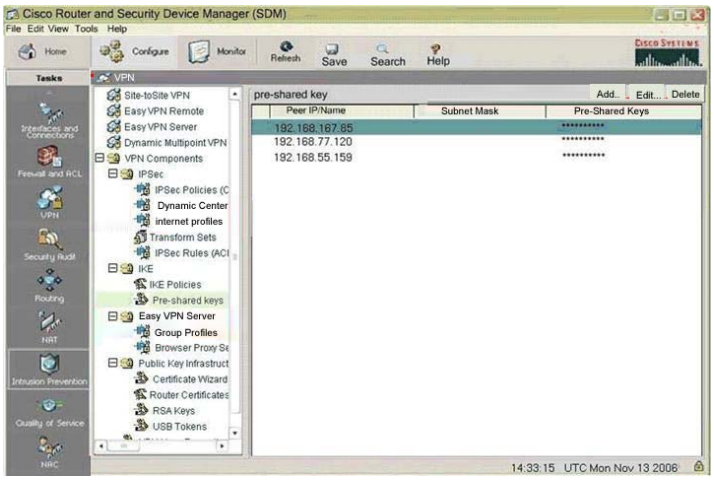
Use this information and answer the questions belonging to the scenario.

Network topology exhibit:

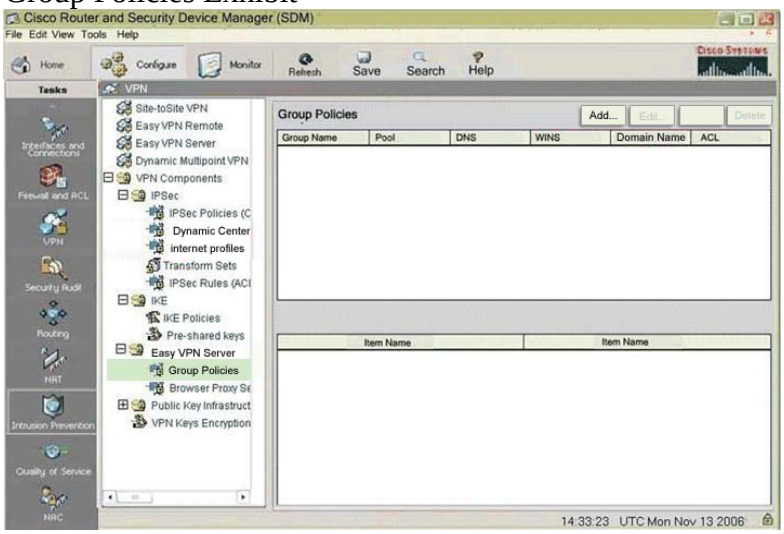


IKE Policies Exhibit

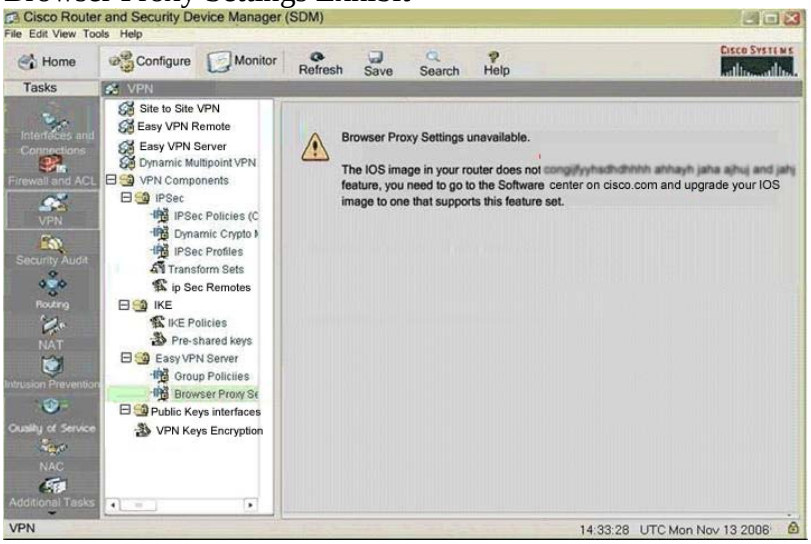
Pre-shared Exhibit



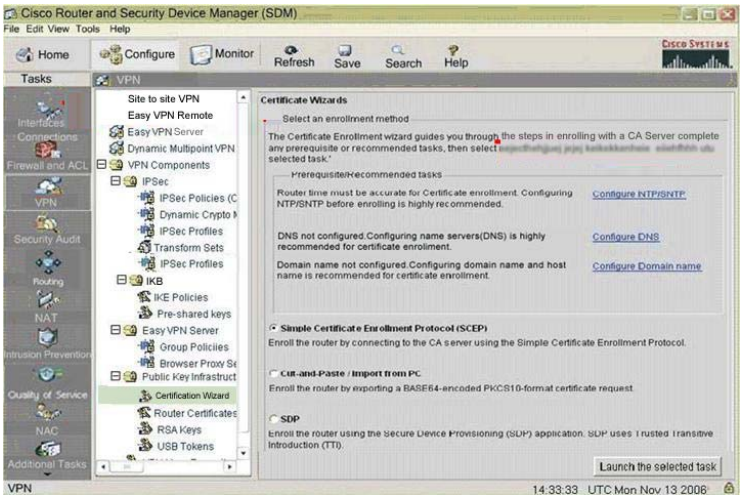
Group Policies Exhibit



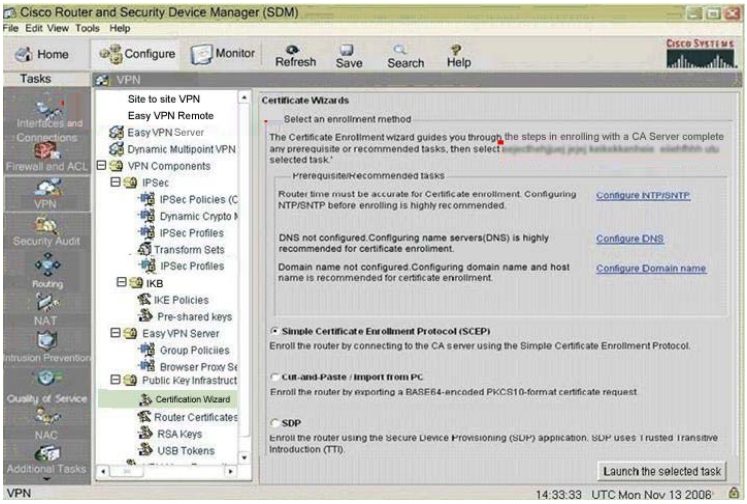
Browser Proxy Settings Exhibit



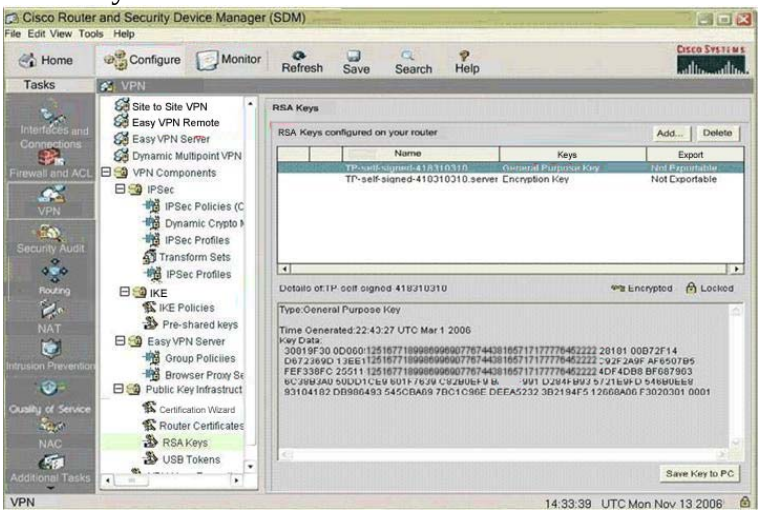
Certificate Wizards Exhibit



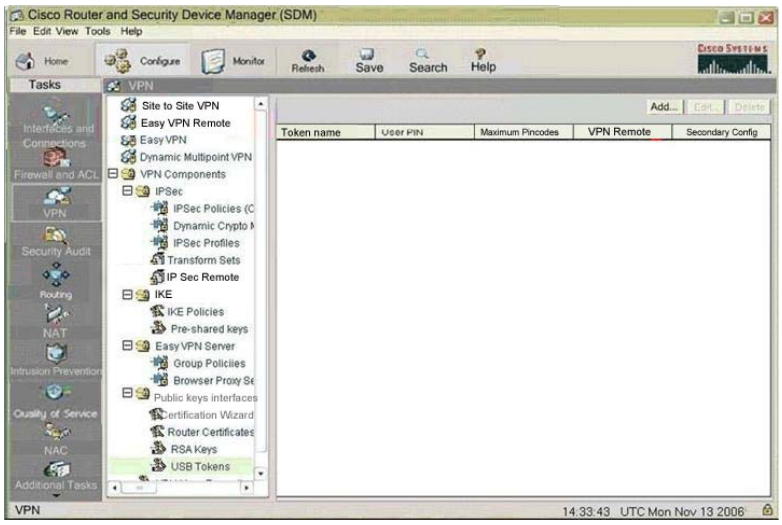
Router Certificates Exhibit



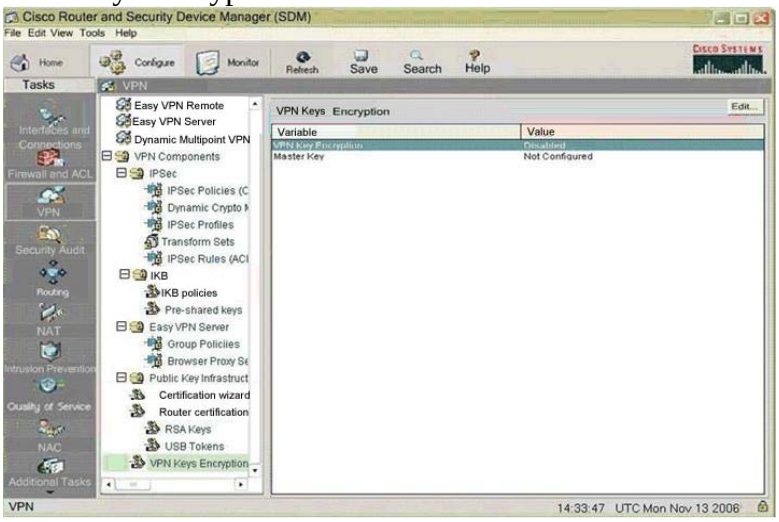
RSA Keys Exhibit



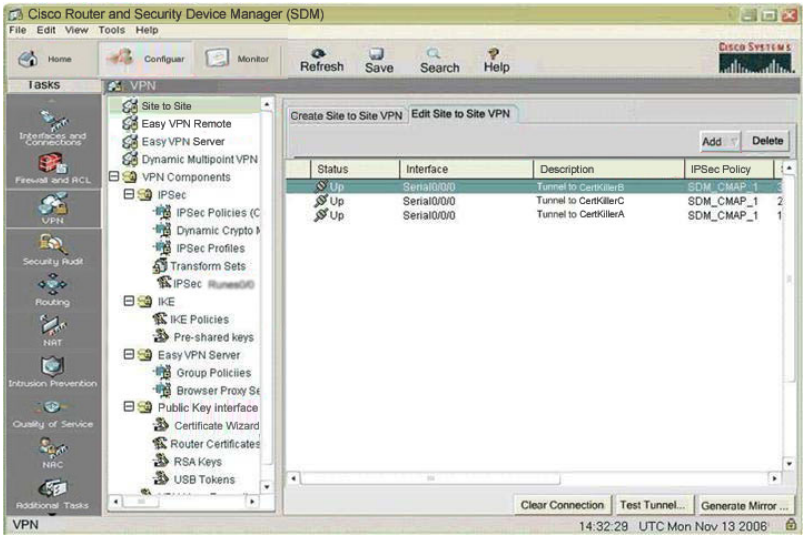
USB Tokens Exhibit



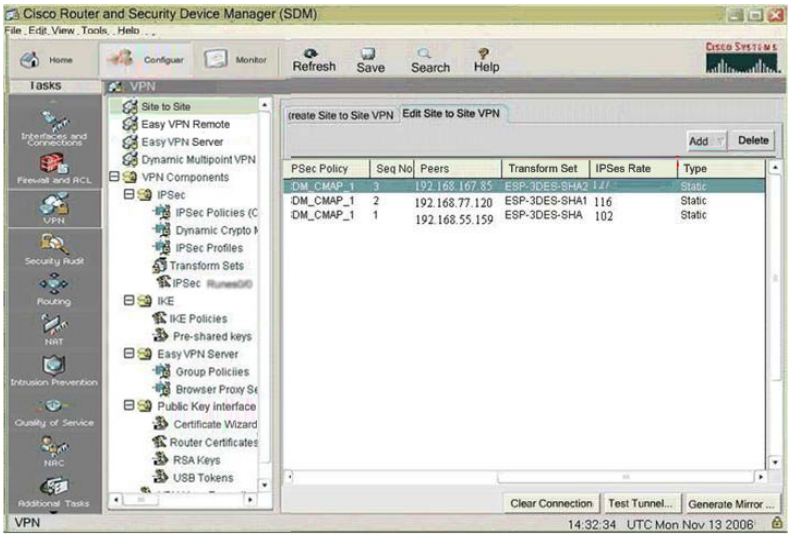
VPN Keys Encryption Exhibit



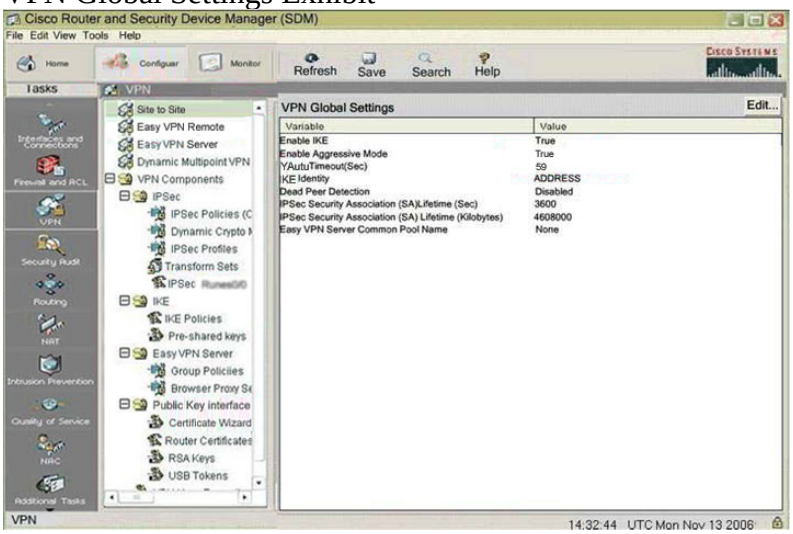
Edit Site to Site VPN Exhibit



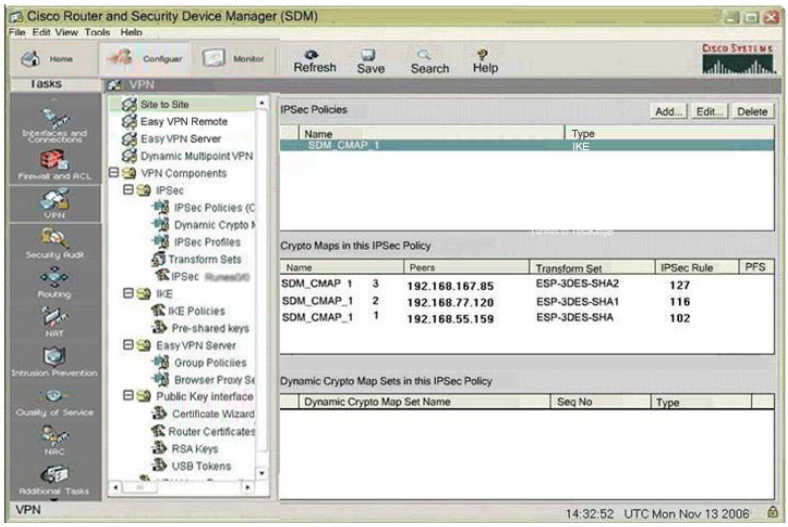
Edit Site to Site VPN Exhibit#2



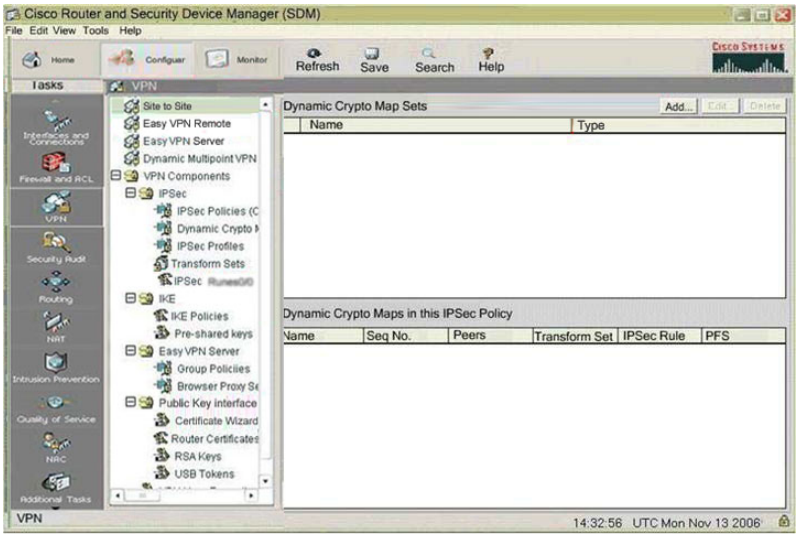
VPN Global Settings Exhibit



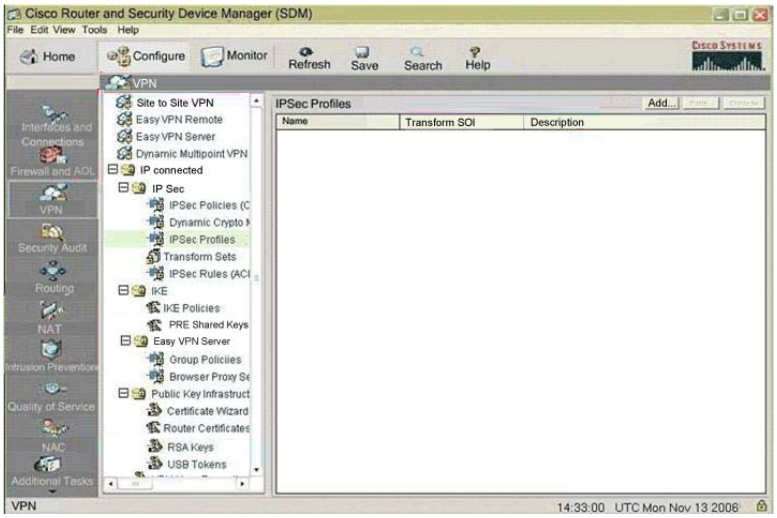
IPSec Policies Exhibit



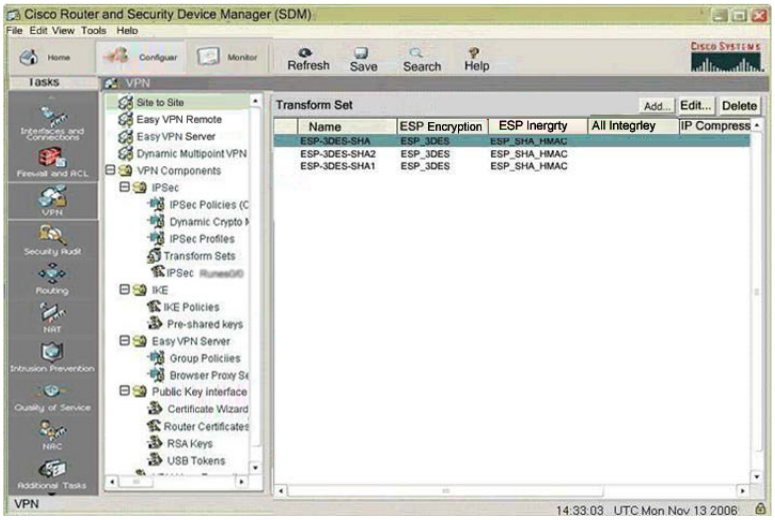
Dynamic Crypto Map Sets Exhibit



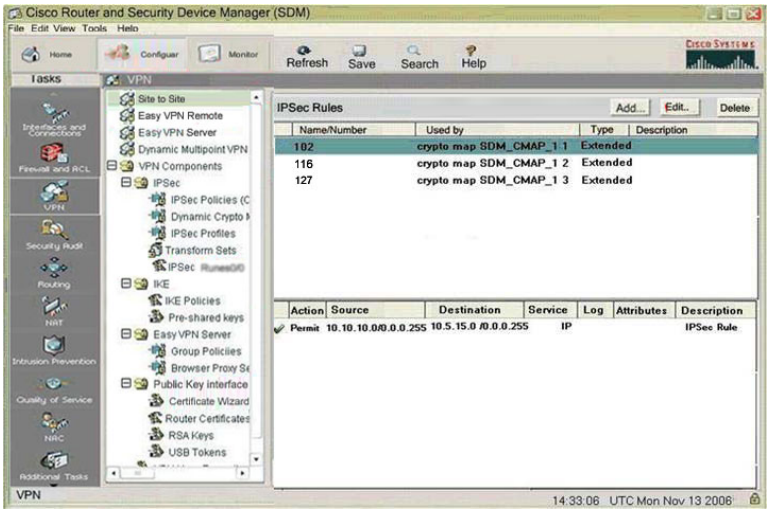
IPSec Profiles Exhibit



Transform Sets Exhibit



IPSec Rules Exhibit



Topic 1, Certkiller Scenario 1 Questions (4 Questions)

QUESTION 176:
Based on the information provided in the scenario, which algorithm as defined by the transform set is used for providing data confidentiality when connected to Certkiller B?

A. ESP-SHA-HMAC
B. ESP-3DES-SHA
C. ESP-3DES
D. ESP-3DES-SHA2
E. ESP-3DES-SHA1

Answer: D

QUESTION 177:
Based on the information provided in the scenario, which peer authentication method and which IPSEC mode is used to connect to the branch locations? (Select two)

A. Digital Certificate
B. GRE/IPSEC Transport Mode
C. Transport Mode
D. GRE/IPSEC Tunnel Mode
E. Tunnel Mode
F. Pre-Shared Key

Answer: F

QUESTION 178:
Based on the information provided in the scenario, which defined peer IP address

and local subnet belong to Certkiller A? (Select two)

A. Subnet 10.5.15.0/24
B. Subnet 10.3.33.0/24
C. Subnet 10.8.28.0/24
D. Peer address 192.168.167.85
E. Peer address 192.168.55.159
F. Peer address 192.168.77.120

Answer: A

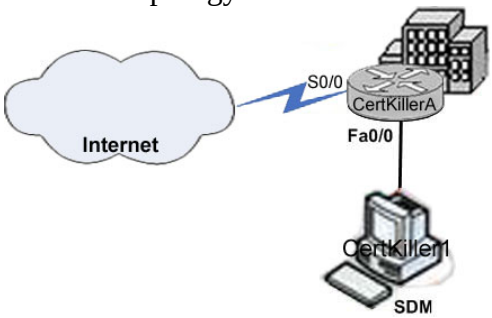
QUESTION 179:
Based on the information provided in the scenario, which IPSec rule is used for the Certkiller C branch and what does it define? (Select two)

A. IP traffic sourced from 10.10.10.0/24 destined to 10.8.28.0/24 will use the VPN.
B. 127
C. IP traffic sourced from 10.10.10.0/24 destined to 10.5.15.0/24 will use the VPN.
D. IP traffic sourced from 10.10.10.0/24 destined to 10.5.33.0/24 will use the VPN.
E. 102
F. 116

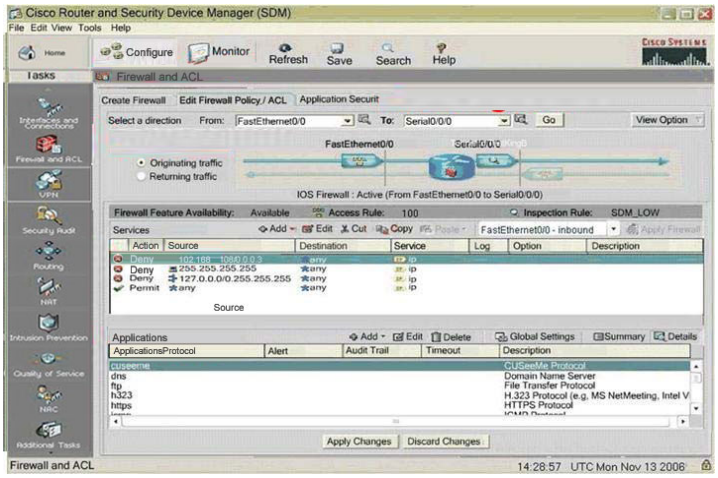
Answer: D

Topic 2, Certkiller Scenario, Scenario2

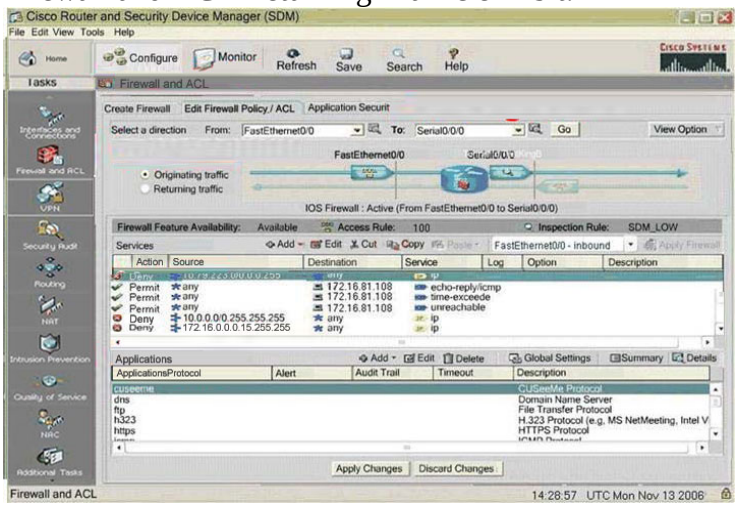
You work as a network engineer at Certkiller . Certkiller is large international company with offices in North America, Europe and Asia. Certkiller has made a recent Internet connectivity upgrade. The Certkiller boss, Miss Certkiller, has asked you personally to provide important documentation regarding this upgrade. In particular you would be required to document the active Firewall configuration on the Certkiller A router. You decided to use the SDM (Security Device Manager) tool. You retrieve the information being displayed in the exhibits of this scenario. Using this information you must then answer the questions belonging to this scenario to comply with Miss Bill's request.
Network topology exhibit:



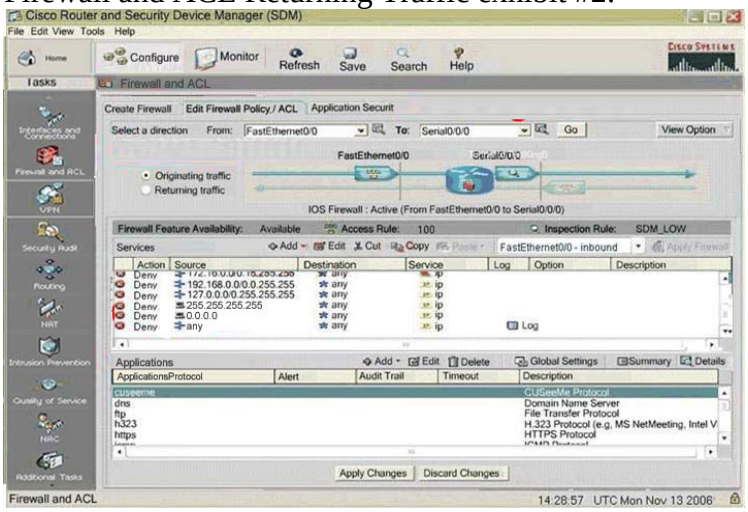
Firewall and ACL Originating Traffic exhibit:



Firewall and ACL Returning Traffic exhibit:

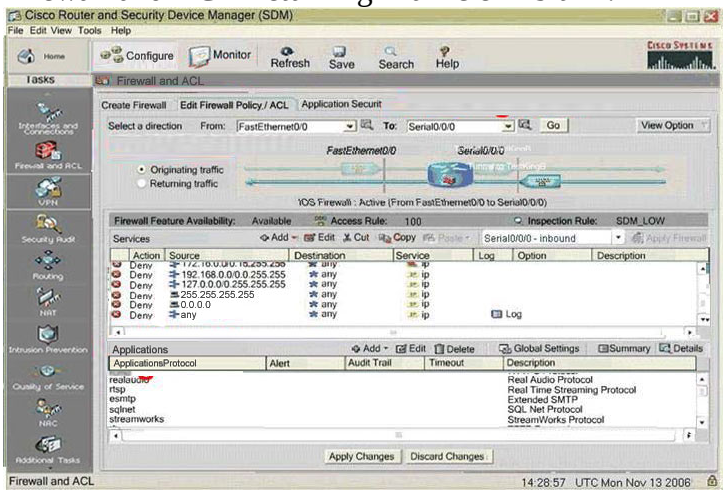


Firewall and ACL Returning Traffic exhibit #2:

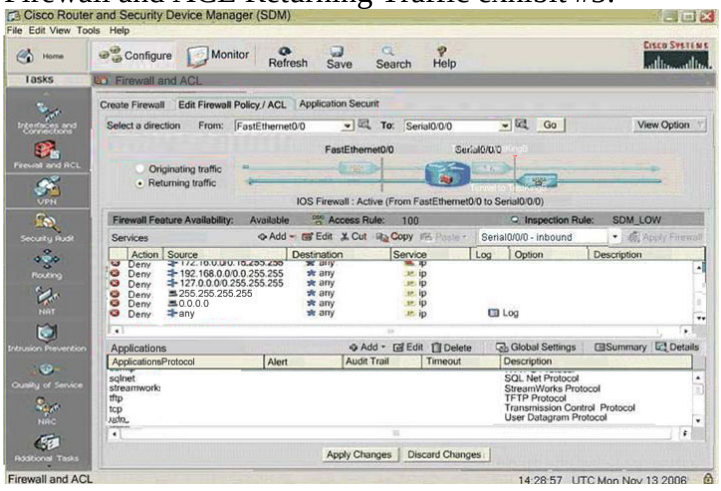


Firewall and ACL Returning Traffic exhibit #3:

Firewall and ACL Returning Traffic exhibit #4:



Firewall and ACL Returning Traffic exhibit #5:



Topic 2, Certkiller Scenario 2 Questions (3 Questions)

QUESTION 180:
Based on the information provided in the scenario, which two statements would be true for a permissible incoming TCP packet on an untrusted Interface in this configuration? (Select two)

A. The session originated from an untrusted interface
B. The packet has a source address of 198.133.219.135
C. The packedt has a source address of 10.79.233.186
D. The packet has a source address of 172.16.81.108
E. The application is not specified within the inspection rule SDM_LOW.
F. The session originated from a trusted Interface

Answer: B, F

Explanation:
Only sessions from the trusted source can return back.
Not E: The address is not in the ACL deny list.

QUESTION 181:
Based on the information provided in the scenario, which statement below is true?

A. FastEthernet 0/0 is an untrusted interface and Serial 0/0/0 is a trusted interface.
B. Both FastEthermet 0/0 and Serial 0/0/0 are trusted interface.
C. FastEthernet 0/0 is a trusted interface and Serial 0/0/0 is an untrusted interface.
D. Both FastEthernet 0/0 and Serial 0/0/0 are untrusted interfaces.

Answer: C

Explanation: Extended ACL is applied on the serial port. serial port is also on the WAN side.

QUESTION 182:
Based on the information provided in the scenario, which two statements would specify a permissible incoming TCP packet on a trusted interface in this configuration? (Select two)

A. The packet has a source address of 172.16.81.108
B. The packet has a source address of 198.133.219.40
C. The destination address is not specified within the inspection rule SDM_LOW.
D. The destination address is specified within the inspection rule SDM_LOW.
E. The packet has a source address of 10.79.233.107

Answer: A, C

Mixed (10 Questions)

QUESTION 183:

Exhibit:

```
CertKiller3(config)# ip route vrf cust1
CertKiller3(config-router)# address-family ipv4 vrf cust1
CertKiller3(config-router-af)# redistribute static
CertKiller3(config-router-af)# redistribute connected
```

Please study the exhibit carefully.
What is the purpose of the restribute commands?

A. to redistribute routes specifically intop EIGRP
B. to redistribute routes into the VRF BGP table
C. to redistribute routes specifically intop RIP
D. to define the MPLS labels to attach to packets by the CE router.
E. to redistribute routes into the local IGP routing table.
F. to redistribute routes specifically intop BGP
G. to redistribute routes specifically intop OSPF
H. to redistribute routes specifically intop IGP
I. to define the MPLS labels to attach to packets by the PE router.

Answer: B

QUESTION 184:
Your boss at Certkiller .com, Mrs. Certkiller, is interested in xDSL.
What can you tell her? Select two.

A. IDSL offers downstream and upstream rates of up to 1 Mbps over a maximum distance of 5.6 km (18,000 feet)
B. ADSL offers downstreet rates of up to 1 Mbps and upstream rates up to 8 Mbps over a maximum distance of 5.6 km (18,000 feet)
C. VDSL offers downstreet rates of up to 52 Mbps and upstream rates up to 13 Mbps over a maximum distance of 8.52 km (28,000 feet)
D. ADSL offers downstreet rates of up to 8 Mbps and upstream rates up to 1 Mbps over a maximum distance of 5.6 km (18,000 feet)
E. VDSL offers downstreet rates of up to 13 Mbps and upstream rates up to 52 Mbps over a maximum distance of 8.52 km (28,000 feet)
F. G.SHDSL offers downstream and upstream rates of up to 2.3 Mbps over a maximum distance of 8.52 km (18,000 feet)

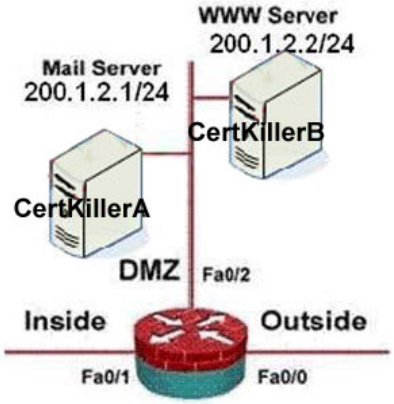
Answer: D,F

QUESTION 185:
Your boss at Certkiller .com, Mrs. Certkiller, is interested of ACLs IOS firewall configuration. What are two principles here? Select two.

A. Allow traffic that will be inspected by IOS firwall to leave the network through the firewall.
B. Prevent traffic that will be inspected by IOS Firewall from leaving the network through the firewall.
C. Permit broadcast messages with a source address of 255.255.255.255.
D. Configure ACL to deny traffic from the protected netwotk to the unprotected networks.
E. Configure extended ACLs to prvent IOS Firewall return traffic from entering the network throough the firewall.

Answer: A,E

QUESTION 186:
Network topology exhibit:



Configuration exhibit:

```
interface FastEthernet0/0
 ip inspect OUTSIDE in
 ip access-group OUTSIDEACL in
!
interface FastEthernet0/1
 ip inspect INSIDE in
 ip access-group INSIDEACL in
!
interface FastEthernet0/2
 ip access-group DMZACL in
!
ip inspect name INSIDE tcp
ip inspect name OUTSIDE tcp
!
ip access-list extended OUTSIDEACL
 permit tcp any host 200.1.2.1 eq 25
 permit tcp any host 200.1.2.2 eq 80
 permit icmp any any packet-too-big
 deny ip any any log
!
ip access list extended INSIDEACL
 permit tcp any any eq 80
 permit icmp any any packet-too-big
 deny ip any any log
!
ip access-list extended DMZACL
 permit icmp any any packet-too-big
 deny ip any any log
```

Please refer to two exhibits.
Your boss at Certkiller .com, Mrs. Certkiller, is interested of ACLs IOS firewall configuration. What is true in this scenario?

A. ICMP unreachable 'packet-too-big' messages are rejected on all interfaces to prevent DDOS attacks.
B. Inside users are not permitted to browse the Internet.
C. The TCP inspection will automatically allow return traffic of the outbound HTTP sessions and allow return traffic of the inbound SMTP and HTTP sessions.
D. Inbound SMTP and HTTP are permitted by the ACL OUTSIDEACL. OUTSIDEACL is applied to the inside interface in the outbound direction.
E. Outbound HTTP sessions are allowed by the ACL INSIDEACL. INSIDEACL is applied to the outside interface in the inbound direction.

Answer: C

QUESTION 187:
Which two Network Time Protocol (NTP) statements are true? Select two.

A. Whenever possible, configure NTP version 5 because it automatically provides authentication and encryption services.
B. A stratum 0 time server is required for NTP operation.
C. The ntp server global configuration is used to configure the NTP master clock to which other peers synchronize themselves.
D. NTP is enable on all interfaces by default, and all interfaces receive NTP packets.
E. The show ntp status command displays detailed association information of all NTP peers.
F. NTP operates on IP networks using User Datagram Protocol (UDP) port 123.

Answer: D,F

QUESTION 188:
What are three configurable parameters when editing signatures in Security Device Manager (SDM)? Select three.

A. EventAction
B. AlarmSeverity
C. EventMedia
D. AlarmKeepalive
E. EventAlarm
F. AlarmTraits

Answer: A,B,F,

QUESTION 189:
Your boss at Certkiller .com, Mrs. Certkiller, is interested IDS (intrusion detection

system). She asks you which two active response capabilities can be configured on an IDS in response to malicious traffic detection? Select 3.

A. the transmission of a TCP reset to the offending end host.
B. The ignition of dynamic access lists on the IDS to prevent further malicious traffic.
C. The invoking of SNMP-sourced controls
D. The shutdown of ports on intermediary devices
E. The configuration of network devices to prevent malicious traffic from passing through

Answer: A,E

QUESTION 190:
What are two possible actions an IOS IPS can take if a packet in a session matches a signature? Select 2.

A. drop the packet
B. reset the connections
C. check the packet agains an ACL
D. forward the packet

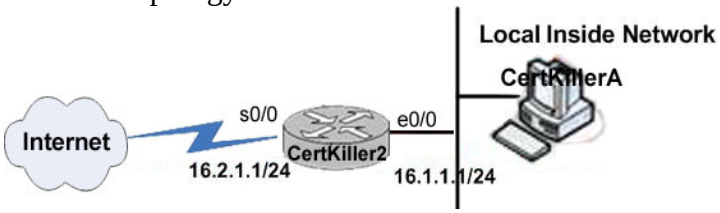
Answer: A,B

QUESTION 191:
How can virus and Trojan horse attacks be mitigated?

A. Enable trust levels.
B. Use antivirus software
C. Disable port scan
D. Implement RFC 2827 filtering
E. Deny echo replies on all edge routes.

Answer: B

QUESTION 192:
Network topology exhibit



Configuration exhibit:

```
CertKiller2 #show running-config
 <output omitted>
interface Serial0/0
 ip address 16.2.1.1 255.255.255.0
 ip access-group 100 in
 <output omitted>
access-list 100 permit tcp any 16.1.1.0 0.0.0.255 established
access-list 100 deny ip any any log
```

Please refer to the exhibits.
What is the purpose of the access list?
It allows TCP traffic from...

A. ...any destination to reach the 16.1.1.0/24 network if the request originated from the inside network.
B. ...any destination to reach the 16.1.1.0/24 network if the request originated from the Internet.
C. ...any destination to reach the 16.1.1.0/24 network if the request originated from the inside network and has a port number greater then 1024.
D. ...the 16.1.1.0/24 network to reach any destionation if the request originated from the inside network and has a port number greater less 1024.
E. ...the 16.1.1.0/24 network to reach any destionation if the request originated from the Internet.

Answer: C