CCIE Security Written Exam v4.0

Number: 350-018
Passing Score: 800
Time Limit: 120 min
File Version: 9.0

CCIE Security Written Exam v4.0

Version: 9.0
Cisco 350-018 Exam

Exam A

QUESTION 1
Which two of these Cisco Catalyst security features offer the best ways to prevent ARP cache poisoning? (Choose two.)

A. Dynamic ARP Inspection
B. port security
C. MAC address notification
D. DHCP snooping
E. PortFast
F. 802.1x authentication

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
Which one of the following is not a valid RADIUS packet type?

A. access-reject
B. access-response
C. access-challenge
D. access-reply
E. access-accept

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

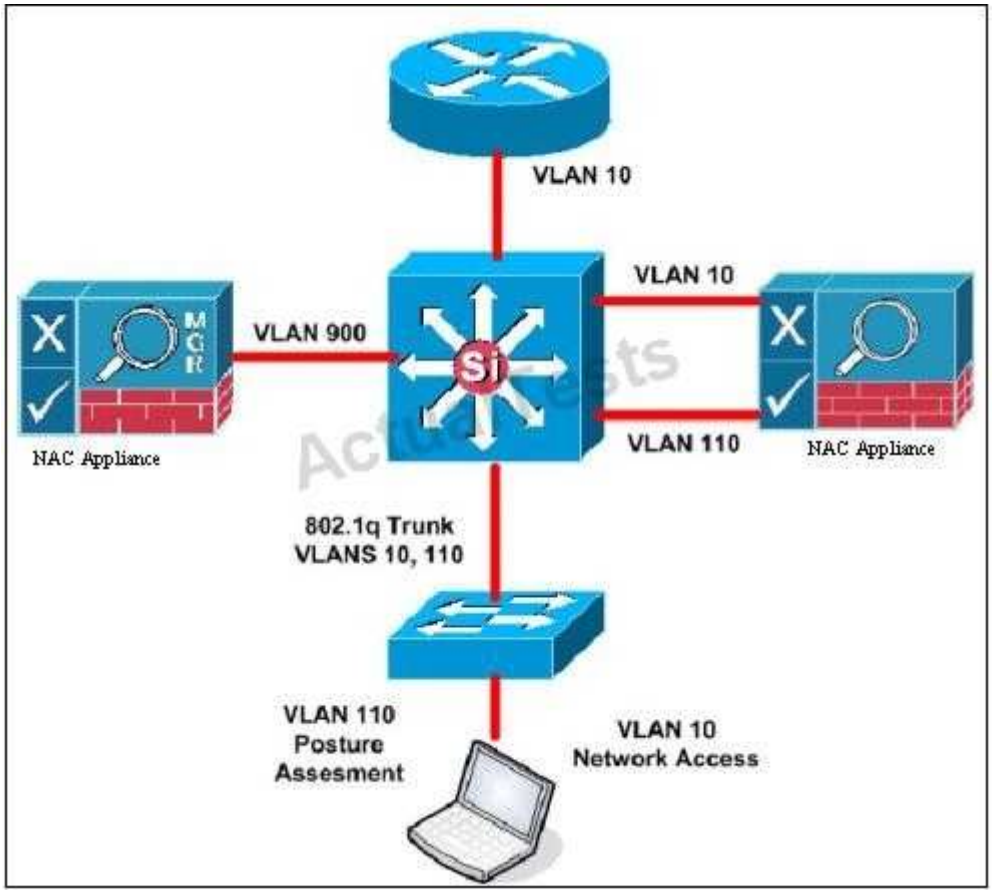
QUESTION 3
Which two of these statements about SMTP and ESMTP are the most correct? (Choose two.)

A. Open mail relays are often used for spamming.
B. ESMTP does not provide more security features than SMTP.
C. SMTP provides authenticated e-mail sending.
D. Worms often spread via SMTP.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
Refer to the exhibit. Which three of the following statements are correct? (Choose three.)



A. The exhibit shows an example of a NAC Framework network.
B. The exhibit shows an example of a NAC Appliance network.
C. The network utilizes in-band admission control.
D. The network utilizes out-of-band admission control.
E. Cisco NAC Appliance Agent is used to verify end-user PC compliance with the security policy
F. Cisco Trust Agent is used to verify end-user PC compliance with the security policy.

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
Referring to the partial debug output shown in the exhibit, which of these values is contained inside the brackets [4] in line 1?

```
router# debug radius

00:02:50: RADIUS: NAS-IP-Address [4] 6 10.0.0.1
00:02:50: RADIUS: Vendor, Cisco [26] 19 VT=02 TL=13 ISDN 0:D:23
00:02:50: RADIUS: NAS-Port-Type [61] 6 Async
00:02:50: RADIUS: User-Name [1] 12 "4085274206"
00:02:50: RADIUS: Called-Station-Id [30] 7 "52981"
00:02:50: RADIUS: Calling-Station-Id [31] 12 "4085554206"
00:02:50: RADIUS: Acct-Status-Type [40] 6 Start
00:02:50: RADIUS: Service-Type [6] 6 Login
```

A. RADIUS identifier field value
B. RADIUS attribute type value
C. RADIUS VSA number
D. RADIUS VSA length
E. vendor ID

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

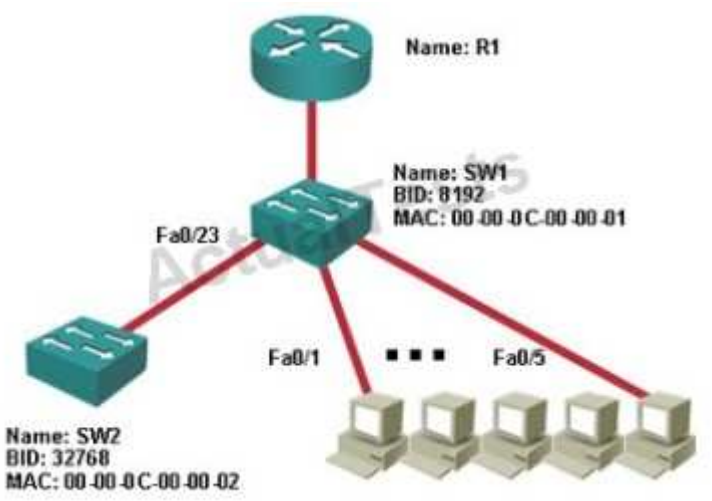
QUESTION 6
What is the net effect of using ICMP type 4 messages to attack RFC 1122-compliant hosts?

A. Hosts will perform a soft TCP reset and restart the connection.
B. Hosts will perform a hard TCP reset and tear down the connection.
C. Hosts will reduce the rate at which they inject traffic into the network.
D. Hosts will redirect packets to the IP address indicated in the ICMP type 4 message.
E. Hosts will retransmit the last frame sent prior to receiving the ICMP type 4 message.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
Refer to the exhibit. Switch SW2 has just been added to Fa0/23 on SW1. After a few seconds, interface Fa0/23 on SW1 is placed in the error-disabled state. SW2 is removed from port 0/23 and inserted into SW1 port Fa0/22 with the same result. What is the most likely cause of this problem?



A. The spanning-tree PortFast feature has been configured on SW1.
B. BPDU filtering has been enabled either globally or on the interfaces of SW1.
C. The BPDU guard feature has been enabled on the Fast Ethernet interfaces of SW1.
D. The Fast Ethernet interfaces of SW1 are unable to autonegotiate speed and duplex with SW2.
E. PAgP is unable to correctly negotiate VLAN trunk characteristics on the link between SWI and SW2.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
ASDM on the Cisco ASA adaptive security appliance platform is executed as which of the following?

A. an ActiveX application or a JavaScript application
B. a JavaScript application and a PHP application
C. a fully compiled .Net Framework application
D. a fully operational Visual Basic application
E. a Java applet or a standalone application using the Java Runtime Environment

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 9

After the client opens the command channel (port 21) to the FTP server and requests passive mode, what will be the next step?

A. The FTP server sends back an ACK to the client.
B. The FTP server allocates a port to use for the data channel and transmits that port number to the client.
C. The FTP server opens the data channel to the client using the port number indicated by the client.
D. The FTP client opens the data channel to the FTP server on port 20.
E. The FTP client opens the data channel to the FTP server on port 21.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
In ISO 27001 ISMS, which three of these certification process phases are required to collect information for ISO 27001? (Choose three.)

A. discover
B. certification audit
C. post-audit
D. observation
E. pre-audit
F. major compliance

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
How do TCP SYN attacks take advantage of TCP to prevent new connections from being established to a host under attack?

A. sending multiple FIN segments, forcing TCP connection release
B. filling up a host listen queue by failing to ACK partially opened TCP connections
C. taking advantage of the host transmit backoff algorithm by sending jam signals to the host
D. incrementing the ISN of each segment by a random number, causing constant TCP retransmissions
E. sending TCP RST segments in response to connection SYN+ACK segments, forcing SYN retransmissions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
For a router to obtain a certificate from a CA, what is the first step of the certificate enrollment process?

A. The router generates a certificate request and forwards it to the CA.
B. The router generates an RSA key pair.
C. The router sends its public key to the CA.
D. The CA sends its public key to the router.
E. The CA verifies the identity of the router.
F. The CA generates a certificate request and forwards it to the router.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
When a failover takes place on an adaptive security appliance configured for failover, all active connections are dropped and clients must reestablish their connections, unless the adaptive security appliance is configured in which two of the following ways? (Choose two.)

A. active/stand by failover
B. active/active failover
C. active/active failover and a state failover link has been configured
D. active/standby failover and a state failover link has been configured
E. to use a serial cable as the failover link
F. LAN-based failover

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
Which of these best represents a typical attack that takes advantage of RFC 792, ICMP type 3 messages?

A. blind connection-reset
B. large packet echo request
C. packet fragmentation offset
D. broadcast-based echo request
E. excessive bandwidth consumption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

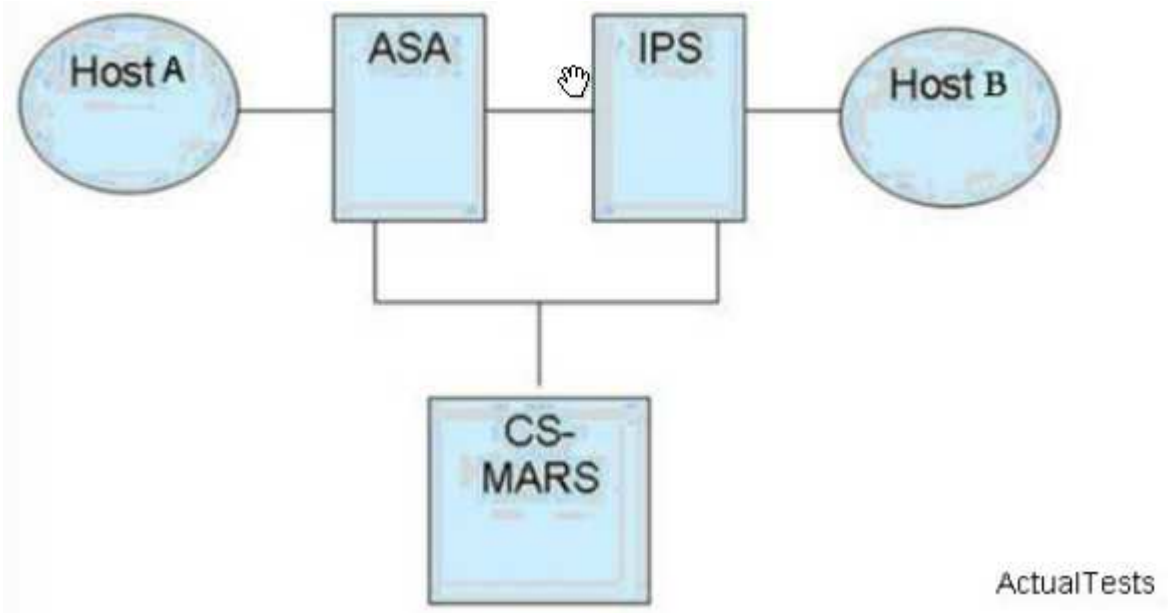
QUESTION 15
Which of these statements best describes the advantage of using Cisco Secure Desktop, which is part of the Cisco ASA VPN solution?

A. Cisco Secure Desktop creates a separate computing environment that is deleted when you finish, ensuring that no confidential data is left on the shared or public computer.
B. Cisco Secure Desktop is used to protect access to your registry and system files when browsing to SSL VPN protected pages.
C. Cisco Secure Desktop ensures that an SSL protected password cannot be exploited by a man- in-the-middle attack using a spoofed certificate
D. Cisco Secure Desktop hardens the operating system of the machines you are using at the time it is launched.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
In the example shown, Host A has attempted a DCOM attack using Metasploit from Host A to Host B. Which three statements best describe how event logs and IPS alerts can be used in conjunction with each other to determine if the attack was successful? (Choose three.)



A. Cisco Security MARS will collect the syslog and the IPS alerts based on time.
B. The IPS event will suggest that an attack may have occurred because a signature was triggered.
C. IPS and Cisco ASA adaptive security appliance will use the Unified Threat Management protocol to determine that both devices saw the attack
D. Cisco ASA adaptive security appliance will see the attack in both directions and will be able to determine if an attack was successful.
E. The syslog event will indicate that an attack is likely because a TCP SYN and an ACK followed the attempted attack.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 17
When using Cisco Easy VPN Remote (hardware client deployment) in the client-mode setup, all of the following statements are correct except which one?

A. Perform split tunneling on the Cisco Easy VPN Remote device.
B. Initiate a connection from a network behind the Cisco Easy VPN Server to the network behind the Cisco Easy VPN Remote client.
C. Set the Cisco Easy VPN Remote to allow an administrator or user to manually initiate a connection.
D. Set the Cisco Easy VPN Remote to automatically connect to the Cisco Easy VPN Server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
Which method is used by Cisco Security Agent to get user state information from the operating system?

A. secure SSL using HTTPS session
B. application (Layer 7)-based (Cisco proprietary) encryption
C. NetBIOS socket on TCP port 137-139 and UDP port 137-139
D. Win32 application binary interface (ABI)
E. Win32 application programming interface (API)

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
Which two of these commands are required to implement a Cisco Catalyst 6500 Series Firewall Services Module (FWSM) in a Catalyst 6500 running Cisco IOS? (Choose two.)

A. firewall multiple-vlan-interfaces
B. firewall module vlan-group y
C. module secure-traffic
D. firewall vlan-group <vlan-x>
E. firewall module secure-traffic

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
Cisco ASA 5500 Series Adaptive Security Appliance application layer protocol inspection is

implemented using which of these?

A. Protocol Header Definition File (PHDF)
B. Cisco Modular Policy Framework
C. Reverse Path Forwarding (RPF)
D. NetFlow version 9
E. Traffic Classification Definition File (TCDF)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
A DNS open resolver is vulnerable to which three of these malicious activities? (Choose three.)

A. cache poisoning attack
B. amplification attack
C. Ping of Death attack
D. Resource Utilization attack
E. Blue Screen of Death
F. Nachi worm attack

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
Which two of these are true about TFTP? (Choose two.)

A. TFTP includes a basic username/password authentication mechanism.
B. While "putting" files via TFTP is possible, it is good practice to disallow it, because TFTP lacks access control mechanisms.
C. TFTP uses a very basic "stop and wait" mechanism for flow control, for which each packet needs to be acknowledged before the next one is sent.
D. TFTP root directories need to be world-readable and -writable due to the lack of security controls in the protocol.
E. TFTP can list remote directory contents, but only if advanced options (as defined in RFC 2347) are negotiated between client and server at initial connection time.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
Which three of these protocols are supported when using TACACS+? (Choose three.)

A. AppleTalk
B. CHAP
C. NASI
D. NetBIOS
E. Kerberos

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
Refer to the exhibit.

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions		
						Alert and Log	Deny	Other
1108/0	IP Packet with Proto 11	☑	High	100	100	Alert		

Which of these statements is correct for the Fidelity Rating and Base RR values?

A. Both the Fidelity Rating and Base RR values are computed from the Severity Factor value.
B. The Fidelity Rating value is computed from the Base RR value.
C. The Severity Factor value is computed from the Fidelity Rating and Base RR values.
D. The Fidelity Rating value is computed from the Base RR and Severity Factor values.
E. The Base RR value is computed from the Fidelity Rating and Severity Factor values.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
The ARP functionality in IPv4 is accomplished using which type of messages, as defined in ICMPv6?

A. router solicitation and advertisement
B. neighbor solicitation and advertisement
C. redirect
D. neighbor solicitation and router advertisement
E. router solicitation and neighbor advertisement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26

Which two of these are valid TACACS+ Accounting packets? (Choose two.)

A. REQUEST
B. REPLY
C. RESPONSE
D. CONTINUE
E. START

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Accounting in TACACS+ works in a fashion fairly similar to how authorization works. Accounting takes place in TACACS+ in the form of various records being sent to the TACACS+ server from the NAS. These records use all the AV pairs described in the preceding section plus many more.
TACACS+ has three main types of accounting records:
· Start record- Indicates that a service is about to begin. Contains information used in the authorization records as well as other account-specific information. · Stop record- Indicates that a service is about to stop or has terminated. Contains information used in the authorization records as well as other account-specific information. · Continue record (also known as the Watchdog)- Sent while a service is still in progress. This type of record allows the NAS to periodically provide the AAA server with updated information Contains information used in the authorization records as well as other account-specific information.

QUESTION 27
To provide a separation of duties within Cisco Security Manager, which mode would the Cisco Security Manager administrator use?

A. Activity mode
B. Change Control mode
C. Workflow mode
D. Task-Based mode
E. Task Isolation mode

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
A DNS client that sends DNS messages to obtain information about the requested domain name space is known as which of these?

A. Resource Record
B. Resolver
C. Branch
D. Authoritative Client
E. Recursive Client

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
How does using DHCP Option 82 on a Cisco Wireless LAN Controller make a network more secure?

A. by preventing rogue DHCP servers from returning unauthorized addresses
B. by ensuring that DHCP addresses are parity-checked before being issued
C. by ensuring that clients receive proper routing information as part of their DHCP responses
D. by preventing DHCP address requests from untrusted relay agents
E. by adding fully qualified domain information that the client can use for SSL authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Which two of these statements regarding Authentication Header (AH) are true? (Choose two.)

A. AH requires the use of Encapsulating Security Payload (ESP) to work correctly.
B. AH provides authentication for most of the "outer" IP header, as well as the upper layer protocols.
C. AH can be deployed in tunnel mode only.
D. AH is not commonly used, because it can only encrypt the original packet using a DES encryption algorithm.
E. AH will work through a NAT (one-to-one) device, but not through a PAT (one-to-many) device.
F. AH uses an IP protocol number of 51.

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
If an administrator is unable to connect to a Cisco ASA adaptive security appliance via Cisco ASDM, all of these would be useful for the administrator to check except which one?

A. The HTTP server is enabled.
B. The administrator IP is permitted in the interface ACL.
C. The administrator IP is permitted in the HTTP statement.
D. The ASDM file resides on flash memory.
E. The asdm image command exists in the configuration.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32

All of these are phases of the Security Incident Response methodology except which one?

A. planning
B. preparation
C. identification
D. classification
E. reaction
F. restructuring
G. post-mortem

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 33
Routing loops can occur in distance vector routing protocols if the network has inconsistent routing entries. Which three of these methods can be used to avoid them? (Choose three.)

A. split horizon
B. route poisoning
C. route suppression
D. route splitting
E. hold-down timers

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 34
A bogon list (a list of reserved or unassigned IP addresses) that is applied to an access control list (ACL) can be best described as which of these?

A. content filter
B. packet filter
C. URL filter
D. application filter
E. stateful filter

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
All of these statements about the Cisco Configuration Professional tool are correct except which one?

A. It is a GUI-based device management tool for Cisco access routers.
B. It offers a one-click router lockdown feature.
C. It is installed in router flash memory.
D. It is free and can be downloaded from the Cisco website.
E. It simplifies routing, firewall, IPS, VPN, Cisco Unified Communications, WAN, and LAN configuration using easy-to-use GUI-based wizards.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 36
Which three of these Windows operating system services run automatically (are automatically started upon appliance power up) on the Cisco Secure ACS Solution Engine? (Choose three.)

A. Net Logon
B. RunAs Service
C. DHCP Client (only if the appliance is using DHCP)
D. DNS Client
E. Routing and Remote Access
F. Windows Time

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

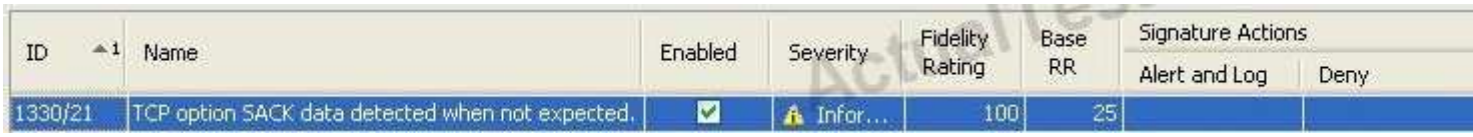
QUESTION 37
All of these Cisco security products provide event correlation capabilities except which one?

A. Cisco ASA adaptive security appliance
B. Cisco IPS
C. Cisco Security MARS
D. Cisco Guard/Detector
E. Cisco Security Agent

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 38
Refer to the exhibit. Which field can be modified using the signature action "Modify Packet" option?



ID	Name	Enabled	Severity	Fidelity Rating	Base RR	Signature Actions	
						Alert and Log	Deny
1330/21	TCP option SACK data detected when not expected.	☑	Infor...	100	25		

A. source IP address of TCP packet
B. TTL of TCP packet
C. SYN flag of TCP packet
D. destination port of TCP packet
E. ICMP type of ICMP packet

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 39
All of these security technologies use Rivest, Shamir, and Adleman (RSA) except which one?

A. SSH
B. IPsec using manual keying
C. IPsec using certificates
D. SSL
E. IPsec using encrypted nonces

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 40
If a BGP-enabled router receives multiple advertisements for the same route from multiple sources, the router selects only one path as the best path using which three of these criteria? (Choose three.)

A. prefer the path with the highest weight
B. prefer the path that has the highest metric
C. prefer the path with the highest local preference
D. prefer the path with the highest MED attribute
E. prefer an internal path over an external path
F. prefer the path with the lowest IP address, as specified by the BGP router ID

Correct Answer: ACF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 41

Which OSPF LSA type is generated by the ABR to describe a route to neighbors outside the area?

A. LSA Type 1
B. LSA Type 2
C. LSA Type 3
D. LSA Type 4
E. LSA Type 5
F. LSA Type 7

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 42
With proper Cisco Secure Desktop configuration, you can achieve which three of these goals? (Choose three.)

A. switch between Cisco Secure Desktop and the local desktop
B. launch an application after Cisco Secure Desktop has been installed
C. identify hosts by their IP addresses, active processes, and operating system versions
D. restrict hosts to sending traffic to devices on the local network
E. restrict hosts from modifying registry settings

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43
What will this configuration for an IDSM-2 module do?

```
intrusion-detection module 6 management-port access-vlan 36
intrusion-detection module 6 data-port 1 capture
intrusion-detection module 6 data-port 1 capture allowed-vlan 1-10, 36, 124
!
vlan access-map IDSM-2 10
match ip address 150
action forward capture
vlan access-map IDSM-2 20
match ip address 151
action forward
!
vlan filter IDSM-2 vlan-list 1 -10, 36, 124
!
access-list 150 permit tcp any 10.1.1.0 0.0.0.255
access-list 151 permit ip any any
```

A. forward all traffic to the IDSM-2 for inspection
B. forward only traffic destined to 10.1.1.0/24 to the IDSM-2 for inspection
C. forward only traffic destined to 10.1.1.0/24 and in VLANs 1-10, 36, and 124 to IDSM-2 for inspection

D. forward only traffic in VLAN 36 to the IDSM-2 for inspection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 44
Which of these Cisco IOS features implements a simple packet filter?

A. Cisco IPS
B. IPsec
C. IP routing
D. NBAR
E. access control list

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 45
You are trying to set up a site-to-site IPsec tunnel between two Cisco ASA adaptive security appliances, but you are not able to pass traffic. You try to troubleshoot the issue by enabling debug crypto isakmp and see the following messages:

CiscoASA# debug crypto isakmp
[IKEv1]: Group = 209.165.200.231, IP = 209.165.200.231, Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy
[IKEv1]: Group = 209.165.200.231, IP = 209.165.200.231, QM FSM error (P2 struct &0xb0cf31e8, mess id 0x97d965e5)!
[IKEv1]: Group = 209.165.200.231, IP = 209.165.200.231, Removing peer from correlator table failed, no match!

What could be the potential problem?

A. The policy group mapped to the site-to-site tunnel group is configured to use both IPsec and SSL VPN tunnels.
B. The policy group mapped to the site-to-site tunnel group is configured to use both IPsec and L2TP over IPsec tunnels.
C. The policy group mapped to the site-to-site tunnel group is configured to just use the SSL VPN tunnel.
D. The site-to-site tunnel group is configured to use both IPsec and L2TP over IPsec tunnels.
E. The site-to-site tunnel group is configured to just use the SSL VPN tunnel.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 46

Before you can configure devices using Cisco Configuration Professional, you must do what?

A. create a default password, and then attach it to the router list in the community map
B. create a community, and then add devices to that community
C. create a discovery map, and then bind this map to the community
D. create a hostname-to-IP-address mapping, and then add this map reference in the community

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47
All of these are task items that can be associated with the change management process except which one?

A. roles and responsibilities
B. rollback procedures
C. implementation schedule
D. risk analysis process
E. resource requirements

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 48
What is the main purpose of a denial of service attack?

A. unauthorized data manipulation
B. the gaining of system access
C. privilege escalation on a victim or compromised host
D. impeding of the availability of a resource to authorized users
E. unauthorized discovery and mapping of systems, services, or vulnerabilities

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 49
Which common FTP client command option can be used to monitor (denote) the transfer progress of a file?

A. ascii
B. binary
C. hash

D. quote
E. recv

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 50
Which of these is a core function of the risk assessment process?

A. performing regular network upgrades
B. performing network optimization
C. performing network posture validation
D. establishing network baselines
E. prioritizing network roll-outs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 51
When sending an e-mail message using Simple Mail Transfer Protocol (SMTP), the client must signal to the mail server that the message is complete by terminating the message with which of these?

A. END
B. SEND
C. <CR><LF>
D. <CR><LF> <CR><LF>
E. CTRL+C

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 52
The network administrator has created two network access control rules in Cisco Security Agent in order to block NetBIOS traffic; however, traffic is still passing and Cisco Security Agent is not filtering it. Which of these could be the issue?

A. Cisco Security Agent received those access control rules after the machine booted.
B. Cisco Security Agent received those access control rules before the machine booted.
C. NetBIOS ports open during the session connection and cannot be filtered beforehand.
D. Cisco Security Agent access control rules do not support NetBIOS filtering.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 53
ISAKMP phase 1 SA is part of a two-phase negotiation, using either the Main mode or Aggressive mode option. Which two of these identify the number of messages exchanged between the two peers in each of the two modes? (Choose two.)

A. Main mode (6 messages)
B. Main mode (5 messages)
C. Main mode (4 messages)
D. Aggressive mode (4 messages)
E. Aggressive mode (3 messages)
F. Aggressive mode (2 messages)

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 54
Management Frame Protection (MFP) works by doing all of these except which one?

A. adding a message integrity check to each frame
B. blocking management frames from known rogue access points
C. detecting flooding of management frames by a rogue access point
D. detecting rebroadcast of management frames
E. allowing encryption of management frames between access points and wireless clients

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 55
The Internet Engineering Task Force (IETF) is a collaborative effort (nonprofit) by the international community of Internet professionals to improve the design, use, and management of the Internet.

Which international organization charters the activity of IETF?

A. IANA (Internet Assigned Numbers Authority)
B. ISO (International Organization for Standardization)
C. ISOC (Internet Society)
D. RIR (Regional Internet Registry)
E. IEC (International Electrotechnical Commission)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 56
Which two of these correctly describe the following command? (Choose two.)

```
aaa authentication ppp user-radius if-needed group radius
```

A. RADIUS authentication will be used for lines using PPP with CHAP only
B. RADIUS authentication will be used for lines using PPP with CHAP or PAP
C. RADIUS authentication is not performed if the user has been authenticated/authorized
D. If the action returns an error, the user will be allowed access without authentication
E. The user radius keyword specifies that all RADIUS servers are to be used

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

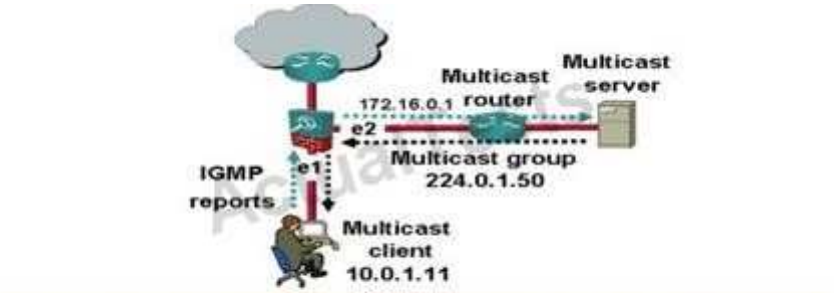
QUESTION 57
What does the "authoritative" flag in the show ip nhrp command output indicate?

A. It indicates that the information was learned from the source mapping information of an NHRP resolution request received by the local router, or from an NHRP resolution packet being forwarded through the local router.
B. It indicates an NHRP mapping entry for networks local to this router for which this router has answered an NHRP resolution request.
C. It indicates that the NHRP information was obtained from the next-hop server or router that maintains the NBMA-to-IP address mapping for a particular destination.
D. It indicates that this NHRP mapping entry must be unique; it cannot be overwritten with a mapping entry that has the same IP address but a different NBMA address.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 58
Refer To the Exhibit.



A company just completed the rollout of IP/TV. The first inside network multicast client to use the new feature claims that they cannot access the service. After reviewing the above ASA security appliance configuration and network diagram, which of the following was the administrator able to determine?

A. The access-list command was not correct and should be changed.
B. The ASA multicast configuration is correct, the configuration problem exists in the multicast client PC.
C. The igmp forward command should be changed to igmp forward interface inside and applied to interface Ethernet 2.
D. The igmp access-group command was not correct and should be changed.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 59
You have configured a DMVPN hub and spoke as follows (assume the IPsec profile "dmvpnprofile" is configured correctly):

Hub:
```
interface Tunnel0
ip address 172.16.1.1 255.255.255.0
no ip redirects
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 10
ip nhrp holdtime 600
ip nhrp redirect
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 10000
tunnel protection ipsec profile dmvpnprofile
```

Spoke 1:
```
interface Tunnel0
ip address 172.16.1.2 255.255.255.0
no ip redirects
ip nhrp authentication cisco
ip nhrp map multicast 1.1.1.2
ip nhrp map 172.16.1.1 1.1.1.2
ip nhrp network-id 20
ip nhrp holdtime 300
ip nhrp nhs 172.16.1.1
```

```
ip nhrp shortcut
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 1000
tunnel protection ipsec profile dmvpnprofile
```

With this configuration, you notice that the IKE and IPsec SAs come up between the spoke and the hub, but NHRP registration fails. Registration will continue to fail until you do which of these?

A. modify the NHRP hold times to match on the hub and spoke
B. modify the NHRP network IDs to match on the hub and spoke
C. modify the tunnel keys to match on the hub and spoke
D. configure the ip nhrp cache non-authoritative command on the hub's tunnel interface

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 60
You configured two routers for EBGP, but you see your BGP neighbor's state is Active after issuing the show ip bgp neighbor command. Which three of these could be reasons? (Choose three.)

A. The EBGP neighbor is two hops away, but the neighbor ttl-security command was not configured.
B. The EBGP neighbor is two hops away, but the neighbor ebgp-multihop command was not configured.
C. The EBGP neighbor is two hops away, but the neighbor disable connected-check command was not configured.
D. One router is configured for version 4, but the other router is configured for version 6.
E. The EBGP neighbor password is incorrect.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 61
A router has this configuration on one of its interfaces:

```
interface FastEthernet0/0
ip address 192.168.1.33 255.255.255.224
end
```

How would the router treat a packet with a destination address of 192.168.1.63?

A. directly connected unicast
B. remote subnet unicast
C. directed broadcast
D. directed multicast
E. limited broadcast

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 62
Prior to installing the Cisco IOS IPS version 5.0 signature package on a router for the first time, what must be done?

A. All signatures must be unretired.
B. All signatures must be enabled.
C. Cisco IOS IPS must be applied to an interface.
D. The Cisco IPS Public Crypto Key must be installed on the router.
E. The PostOffice parameters must be configured.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 63
Which four types of violations can be investigated using a security forensic process? (Choose four.)

A. Compliance
B. Intrusion
C. Asset
D. Access
E. Risk
F. Policy

Correct Answer: ABDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 64
A Cisco ASA adaptive security appliance configured in multiple context mode supports which three of these features? (Choose three.)

A. VPN
B. NAT
C. IPv6 traffic filtering
D. multicast
E. failover

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 65
The Control Plane Policing (CoPP) feature allows users to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets. The filter protects the control plane of Cisco IOS devices against reconnaissance and denial of service (DoS) attacks. The Control Plane Policing feature requires the Modular Quality of Service (QoS) Command-Line interface (CLI) (MQC) to configure packet classification and policing. Which two MQC actions are supported in policy maps?

A. police and transit
B. police and drop
C. cef-exception and drop
D. default and drop
E. police and transmit

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 66
Which of these authentication combinations would provide the highest level of security for an IPsec remote-access VPN client?

A. pre-shared key and xauth (RADIUS server)
B. certificate and xauth (local server)
C. certificate and xauth (RSA SecurID token)
D. pre-shared key and xauth (RSA SecurID token)
E. pre-shared key and xauth (local server)
F. certificate and xauth (RADIUS server)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 67
A customer has Cisco IOS Firewall deployed. Even though the customer has FTP inspection enabled, inspection does not appear to be working for FTP services running on a non-standard port of 21000. Which feature can the customer enable to help resolve this?

A. Extendable Static NAT Port Translation
B. Cisco IOS Flexible Packet Matching
C. Firewall Application Inspection and Control
D. Firewall Application Layer Gateway
E. Port-to-Application Mapping

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

Explanation:

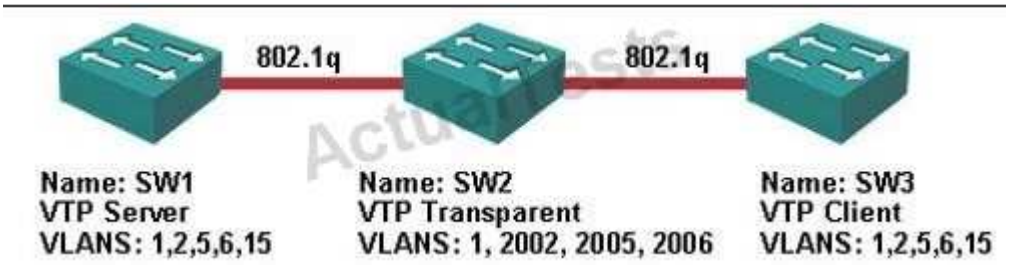
QUESTION 68
Which three of these situations warrant engagement of a Security Incident Response team? (Choose three.)

A. loss of data confidentiality/integrity
B. damage to computer/network resources
C. denial of service (DoS)
D. computer or network misuse/abuse
E. pornographic blogs/websites

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 69
Refer to the exhibit.



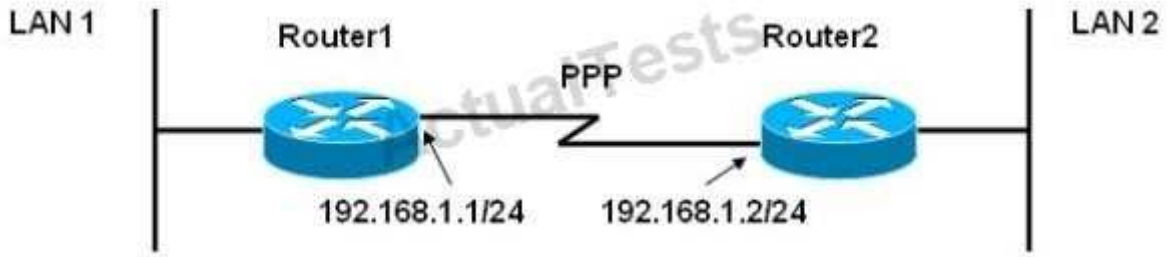
The Cisco IOS Software-based switches are configured with VTP and VLANs as shown. The network administrator wants to quickly add the VLANs defined on SW1 to the configuration of SW2. Therefore, the administrator copies the vlan.dat file from the flash memory on SW1 to the flash memory of SW2. After the file is copied to SW2, it is rebooted. What is the VLAN status of SW2 after the reboot?

A. The VLAN information on SW2 will remain the same because it has been configured for transparent VTP mode.
B. SW2 will clear the vlan.dat file and load its VLAN information from the configuration file stored in NVRAM.
C. A VTP mode mismatch will occur, causing the VLANS in the startup configuration to be ignored and all VLANs above 1005 to be erased.
D. The VLANs in the vlan.dat file will be copied to the running configuration and merged with the extended VLANs defined in the startup configuration.
E. All VLANs will be erased and all ports will be moved into the default VLAN 1.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 70
Refer to the exhibit.



If Router1 receives a packet from LAN 1 with a destination IP address of 192.168.1.10, what happens to the packet?

A. Router1 drops the packet due to ARP failure.
B. Router1 drops the packet due to inverse ARP failure.
C. Router1 drops the packet, because there is no route to the destination.
D. Router1 forwards the packet onto the PPP link, but the packet gets dropped on Router2 because there is no route to the destination.
E. The packet loops between Router1 and Router2 until the TTL expires.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 71
Which of these IPv6 messages should be filtered at the perimeter of your network if MIPv6 is not used?

A. ICMP Node Information Query (Type 139)
B. Type 2 Routing Header (RH2) (Type 43)
C. ICMPv6 Multicast Listener Report (Type 131)
D. Inverse Neighbor Discovery Solicitation Message (Type 141)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 72
Unicast Reverse Path Forwarding (Unicast RPF) is a protection mechanism that can be used against which of these?

A. TCP session hijacking attacks
B. brute-force attacks
C. teardrop attacks
D. password attacks
E. birthday attacks
F. spoofing attacks

Correct Answer: F

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 73
Which of these command sequences will send an email to holly@invalid.com using SMTP?

A. MAIL FROM:<david@invalid.com> RCPT TO:<holly@invalid.com> DATA
B. HELO invalid.comMAIL TO:<holly@invalid.com>MESSAGE END
C. HELO invalid.comMAIL FROM:<david@invalid.com> RCPT TO:<holly@invalid.com>BODY
D. MAIL FROM:<david@invalid.com> RCPT TO:<holly@invalid.com>MESSAGE

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 74
Which of these statements is true about the SSH login banner for SSHv1 and v2 connections?

A. It is not displayed.
B. It is displayed before you log into the device.
C. It is displayed after you log into the device.
D. It can be displayed only after the SSH client sends the username.
E. It is not supported.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 75
OSPF uses multicast addresses to send hello packets and routing updates using which of these protocols/ports?

A. IP protocol 17
B. TCP port 179
C. UDP port 520
D. TCP port 87
E. IP protocol 87
F. IP protocol 89

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 76
What is the default username and password set for Cisco Security Device Manager (SDM)?

A. sdm/sdm
B. sdm/cisco
C. cisco/sdm
D. cisco/cisco
E. cisco/cisco123

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 77
All of these are valid Cisco IOS AAA login authentication methods except which one?

A. none
B. kerberos
C. enable
D. local-case
E. group radius
F. group tacacs+

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 78
Communication between Cisco Security Device Manager (SDM) and a Cisco router is secured using which of these?

A. IPsec
B. SSL
C. AES
D. 3DES
E. Cisco proprietary encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 79
Which four of these are characteristics of a Cisco Network Intrusion Prevention System (IPS)? (Choose four.)

A. can provide the ability to drop the initial packet of an attack
B. analyzes a copy of the traffic on the network
C. can support TCP normalization
D. can change network traffic en route
E. cannot support TCP normalization
F. usually provides signature-based analysis

Correct Answer: ACDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 80
Which three of these are among the implicit IPv6 ACL rules in Cisco IOS allowing ICMPv6 neighbor discovery? (Choose three.)

A. permit icmp any any nd-na
B. deny icmp any any nd-na
C. permit icmp any any nd-ns
D. deny icmp any any nd-nn
E. permit ipv6 any any
F. deny ipv6 any any

Correct Answer: ACF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 81
Which three of these make use of a certificate as part of the protocol? (Choose three.)

A. EAP-MD5
B. EAP-TLS
C. EAP-TTLS
D. EAP-FAST
E. EAP-PEAP
F. LEAP

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 82
DNS Security Extension (DNSSEC) adds security functionality to the Domain Name System for which three purposes? (Choose three.)

A. origin authentication of DNS data

B. protection against denial of service (DoS) attacks
C. integrated data encryption using ESP
D. inclusion of the authorization flag in the DNS lookup
E. providing of confidentiality of data
F. data integrity

Correct Answer: ABF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 83
You run the show ipv6 port-map telnet command and you see that the port 23 (system-defined) message and the port 223 (user-defined) message are displayed. Which command is in the router configuration?

A. ipv6 port-map port telnet 223
B. ipv6 port-map port 23 port 23223
C. ipv6 port-map telnet port 23 233
D. ipv6 port-map telnet port 223

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 84
The Extension Mechanisms for DNS (EDNS0) header bit is now required to support larger DNS message sizes for which of these reasons?

A. to allow walking of the Resource Record Signature (RRSIG) for a domain name space
B. to ensure that the authority section is always present
C. to enable lookup for IPv6 AAAA records
D. to enable lookup for DNSSEC resource records
E. to provide a place for TXT resource records larger than 900 bytes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 85
The SSL VPN implementation on a Cisco ASA adaptive security appliance supports which three of these features? (Choose three.)

A. sending TCP and UDP traffic through a smart tunnel
B. sending TCP and UDP traffic through port forwarding
C. sending TCP-only traffic through a smart tunnel

D. sending TCP-only traffic through port forwarding
E. establishing a Winsock 2 connection between the client and the server through port forwarding
F. establishing a Winsock 2 connection between the client and the server through smart tunnels

Correct Answer: CDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 86
Which of these statements is true about EIGRP?

A. It conserves network bandwidth by using periodic, incremental updates to propagate network changes to its neighbors.
B. It can install up to eight equal-cost paths to a given destination in its routing table.
C. It is possible for two EIGRP routers to become neighbors even if the hello and hold timers do not match.
D. EIGRP updates can be sent between two discontiguous autonomous systems via a virtual link.
E. EIGRP packets can be both authenticated and encrypted to ensure that the information exchange is reliable and confidential.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 87
Which three of these are performed by both RADIUS and TACACS+ servers? (Choose three.)

A. login authentication
B. EXEC authorization
C. command authorization
D. EXEC accounting
E. command accounting

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 88
CustomerA wants to synchronize the time on all its routers using NTP. CustomerA knows the NTP master is at address 1.1.1.1, and is using MD5 authentication with a password of "cisco123." Assuming timezone settings are already configured, which four of these commands does the customer need to configure on each router to correctly synchronize the device with the NTP master? (Choose four.)

A. ntp encryption md5
B. ntp server 1.1.1.1 key 1
C. ntp authenticate
D. ntp trusted-key 1

E. ntp enable
F. ntp authentication-key 1 md5 cisco123

Correct Answer: BCDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 89
Which two statements about RADIUS are true? (Choose two.)

A. The RADIUS server must use TCP for its connection to the NAS.
B. The RADIUS server must use UDP for its connection to the NAS.
C. The NAS connection to the RADIUS server encrypts the entire packet, but the header is unencrypted.
D. The NAS connection to the RADIUS server encrypts the password in an Access-Request packet only.
E. The NAS connection to the RADIUS server encrypts the password in the Accounting-Request packet only

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 90
Which of these communications mechanisms can be used between Cisco Security Device Manager (SDM) and a Cisco router in addition to HTTP or HTTPS to read and write the router configurations?

A. Telnet/SSH
B. FTP/Telnet/SSH
C. SFTP/Telnet/SSH
D. FTP/SSH
E. SFTP/SSH

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 91
When configuring a Cisco adaptive security appliance in multiple context mode, which one of these capabilities is supported?

A. multicast
B. dynamic routing protocols
C. VPN configurations
D. static routes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 92
Hypertext Transfer Protocol (HTTP) version 1.1 introduced several improvements over HTTP 1.0, which resulted in improved performance (faster page displays) for end users. Which three of these of these enhancements were added to the HTTP 1.1 protocol over the HTTP1.0 protocol? (Choose three.)

A. GET requests
B. persistent connections
C. selective acknowledgements
D. chunked encoding
E. HTTP pipelining

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 93
The BPDU guard feature disables which kind of port when the port receives a BPDU packet?

A. any port
B. nonegotiate port
C. access port
D. PortFast port
E. root port

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 94
A DNS server that responds to query messages with information stored in Resource Records (RRs) for a domain name space stored on the server is known as which of these?

A. LDAP resolver
B. recursive resolver
C. zone
D. authoritative server
E. local server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 95
The Sarbanes-Oxley (SOX) act is a United States federal law that was enacted in July, 2002. SOX was introduced to provide which two of these? (Choose two.)

A. confidentiality and integrity of customer records and information
B. corporate fraud accountability
C. security standards that protect healthcare patient data
D. confidentiality of personal health information
E. assurance of the accuracy of financial records

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 96
Which of these standards replaced 3DES?

A. PKI
B. Blowfish
C. RC4
D. SHA-1
E. AES
F. MD5

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 97
The communication between Cisco Configuration Professional and a Cisco router is secured using which of these?

A. IPsec
B. ESP
C. SSL
D. GDOI
E. Cisco proprietary encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 98
What does this log message indicate?

```
4w6d: %PM-4-ERR_DISABLE: Psecure-Violation Error Detected on Gi3/2, Putting Gi3/2
```

```
in Err- Disable State
```

A. The port has been disabled because the traffic rate limit has been exceeded.
B. The port has been temporarily disabled because the broadcast packet limit has been exceeded.
C. The port has been disabled because the MAC address limit has been exceeded.
D. The port has been disabled due to a DHCP OFFER packet.
E. The port has been disabled due to detection of a gratuitous ARP packet.
F. The port has been disabled due to an invalid MAC address.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 99
LEAP authentication is provided by which of these?

A. hashing of the password before sending
B. user-level certificates
C. PAC exchange
D. modified MS-CHAP
E. TACACS+

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 100
Which IPv6 Interior Gateway Protocol (IGP) relies entirely on IPsec to secure communications between neighbors?

A. EIGRPv6
B. OSPFv3
C. RIPv6
D. IS-IS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Topic 2, Volume B

QUESTION 101
Identity NAT translates which of these?

A. the source IP address to the interface IP address
B. the local IP address to a global IP address

C. an IP address to itself
D. the destination IP address to an RFC 1918 address
E. the local IP address to a DNS-resolved IP address
F. the global IP address to a local IP address

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 102
Cisco Secure ACS server will forward the events for all of these log files to Cisco Security MARS except which one?

A. Failed Attempts
B. TACACS+ Accounting
C. RADIUS Accounting
D. Passed Authentications

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 103
CustomerA has set up a central syslog server to receive all syslog messages from its routers. The IP address of this central server is 1.1.1.1, and the customer wants all messages of level "error" and above to be sent there. In addition, it wants all messages of level "warning" and above to be stored locally on the router. Assuming logging is already enabled, which three commands on the router would accomplish these goals? (Choose three.)

A. logging host 1.1.1.1 level errors
B. logging buffered warnings
C. logging device 1.1.1.1
D. logging buffer enable
E. logging host 1.1.1.1
F. logging facility local-buffer
G. logging trap errors

Correct Answer: BEG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 104
What is the function of the `switch(config-if)# switchport port-security mac-address sticky` **command?**

A. allows the switch to restrict the MAC addresses on the switch port based on the static MAC addresses

configured in the startup configuration

B. allows the administrator to manually configure the secured MAC addresses on the switch port
C. allows the switch to permanently store the secured MAC addresses in the MAC address table (CAM table)
D. allows the switch to perform sticky learning, in which the dynamically learned MAC addresses are copied from the MAC address table (CAM table) to the startup configuration
E. allows the switch to dynamically learn the MAC addresses on the switch port and the MAC addresses will be added to the running configuration

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 105
What is the default TCP port used to remotely manage a Cisco Secure ACS v4.x software application server?

A. 2000
B. 2001
C. 2002
D. 2005
E. 2020

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 106
Refer to the exhibit.

A user located at the PC with IP address 198.51.100.2 is complaining that the PC is unable to access any web server, including cisco.com. As a network administrator, you may attempt to troubleshoot the problem by logging into the router, which is the user's default gateway, and attempting to access cisco.com. Which command or commands on the Cisco IOS router would you use to verify that the web server is working correctly?

A. connect 198.133.219.25
B. telnet 198.133.219.25GET /index.html HTTP/1.1
C. telnet 198.133.219.25 80GET /index.html HTTP/1.1
D. wget 198.133.219.25
E. wget 198.133.219.25 80

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 107
Which access control model provides access to system resources based on the job function of the user or the tasks that the user has been assigned?

A. Context Based Access Control
B. Rule Based Access Control
C. Mandatory Access Control
D. Discretionary Access Control
E. Role Based Access Control

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 108
Which type of attacks can be monitored and mitigated by CS-MARS using NetFlow data?

A. Spoof attack
B. Buffer Overflow
C. Man-in-the middle attack
D. Trojan Horse
E. Day zero attack
F. Land.C attack

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 109
Which two of the following are valid RADIUS packet flows? C indicates the user (such as a wireless laptop), N indicates the NAS, and S indicates an ACS server. (Choose two.)

A. N to S:RADIUS Access- ChallengeS to N: RADIUS Access-Accept
B. N to S:RADIUS Access-RequestS to N: RADIUS Access-RejectN to S:RADIUS Access- ChallengeS to N: RADIUS Access-Accept
C. C to N: RADIUS Access-RequestN to C: RADIUS Access- RejectC to N: RADIUS Access- ChallengeN to C: RADIUS Access-Accept
D. C to N: RADIUS Access-RequestN to C: RADIUS Access-Accept
E. N to S:RADIUS Access-RequestS to N: RADIUS Access-ChallengeN to S: RADIUS Access- RequestS to N: RADIUS Access-Accept

Correct Answer: DE
Section: (none)

Explanation

Explanation/Reference:
Explanation:

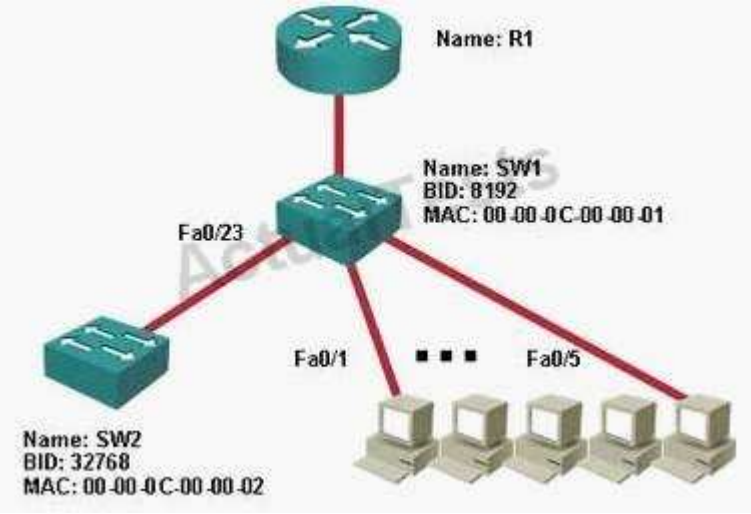
QUESTION 110
The key lengths for DES and 3DES, respectively, are:

A. 128 bits and 384 bits
B. 1024 bits and 3072 bits
C. 64 bits and 192 bits
D. 128 bytes and 384 bytes
E. 128 bits and 256 bits
F. 56 bits and 168 bits

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 111
Refer to the Exhibit. Switch SW2 has just been added to FastEthernet 0/23 on SW1. After a few seconds, interface Fa0/23 on SW1 is placed in the error-disabled state. SW2 is removed from port 0/23 and inserted into SW1 port Fa0/22 with the same result. What is the most likely cause of this problem?



A. PAgP is unable to correctly negotiate VLAN trunk characteristics on the link between SW1 and SW2.
B. BPDU filtering has been enabled either globally or on the interfaces of SW1.
C. The spanning-tree portfast feature has been configured on SW1.
D. The BPDU guard feature has been enabled on the FastEthernet interfaces of SW1.
E. The FastEthernet interfaces of SW1 are unable to auto-negotiate speed and duplex with SW2.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 112
CSA protects your host by:

A. Preventing browsers from acting as client to web servers.
B. Preventing buffer overflows.
C. Preventing users from entering unencrypted passwords.
D. Preventing browsers from opening network sockets in listening state.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 113
Referring to the ASDM screen shot shown in the exhibit, which of the following traffic is permitted based on the current Access Rules?

A. Any IP traffic from any host on the outside to the 172.16.10.2 server on the dmz2
B. Any IP traffic from any host on the inside to any host on the dmz or dmz2
C. Any IP traffic from any host on the dmz to any host on the outside

D. HTTP traffic from the 172.16.10.2 server to any host on the inside
E. Any IP traffic from the 172.16.1.2 host to any host on the inside
F. FTP traffic from any host on the outside to the 172.16.1.2 host on the dmz

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 114
Which one of the following is NOT a valid RADIUS packet type?

A. Access-reject
B. Access-accept
C. Access-reply
D. Access-response
E. Access-challenge

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 115
When an IPS device in single-interface VLAN-pairing mode fires a signature from the normalizer engine and TCP-based packets are dropped, which two of the following would be a probable cause? (Choose two.)

A. There was no information in the IPS state table for the connection.
B. There was a valid SYN ACK in the state table but the subsequent packets were fragmented and did not constitute a valid flow.
C. The IPS device identified an incorrect value in layer 7.
D. The IPS device identified an incorrect value in layer 6.
E. The IPS device identified an incorrect value in layer 5.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The IPS Normalizer takes place on layers 3 and 4, theirfore only B & D can be the correct answers.
The Normalizer engine deals with IP fragment reassembly and TCP stream reassembly. With the Normalizer engine you can set limits on system resource usage, for example, the maximum number of fragments the sensor tries to track at the same time. Note You cannot add custom signatures to the Normalizer engine. You can tune the existing ones.

· IP Fragmentation Normalization - Intentional or unintentional fragmentation of IP datagrams can hide exploits making them difficult or impossible to detect. Fragmentation can also be used to circumvent access control policies like those found on firewalls and routers. And different operating systems use different methods to queue and dispatch fragmented datagrams. If the sensor has to check for all possible ways that the end host can reassemble the datagrams, the sensor becomes vulnerable to DoS attacks. Reassembling all fragmented

datagrams inline and only forwarding completed datagrams, refragmenting the datagram if necessary, prevents this. The IP Fragmentation Normalization unit performs this function. · TCP Normalization - Through intentional or natural TCP session segmentation, some classes of attacks can be hidden. To make sure policy enforcement can occur with no false positives and false negatives, the state of the two TCP endpoints must be tracked and only the data that is actually processed by the real host endpoints should be passed on. Overlaps in a TCP stream can occur, but are extremely rare except for TCP segment retransmits. Overwrites in the TCP session should not occur. If overwrites do occur, someone is intentionally trying to elude the security policy or the TCP stack implementation is broken. Maintaining full information about the state of both endpoints is not possible unless the sensor acts as a TCP proxy. Instead of the sensor acting as a TCP proxy, the segments are ordered properly and the normalizer looks for any abnormal packets associated with evasion and attacks.

51

The association of VLANs in pairs on a physical interface is known as inline VLAN pair mode. Packets received on one of the paired VLANs are analyzed and forwarded to the other VLAN in the pair. Inline VLAN pairs are supported on all sensors that are compatible with IPS 5.1, except NMCIDS, AIPSSM10, and AIPSSM20.

QUESTION 116
Referring to the debug output shown below, what is causing the IKE Main Mode failure?

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0
1d00h: ISAKMP (0:1): no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with peer at
150.150.150.1
```

A. The Crypto ACL is not a mirror image of the peer.
B. The IKE Phase I policy does not match on both sides.
C. The IPSec transform set on the peers do not match.
D. The received IPsec packet specifies a Security Parameters Index (SPI) that does not exist in the security associations database (SADB).
E. The pre-shared keys on the peers do not match.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 117
ARP cache poisoning can be best prevented by using which two Catalyst security features? (Choose two.)

A. Dynamic ARP Inspection (DAI)
B. Port Fast
C. DHCP Snooping
D. MAC Address Notification
E. Port Security
F. 802.1x Authentication

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 118
Which access methods can CS-MARS use to get configuration information from an Adaptive Security Appliance (ASA)? (Choose 2)

A. Console
B. SSH
C. Telnet
D. FTP
E. HTTPS
F. SDEE

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 119
What of the following statements that describe Diffie Hellman Key exchange are correct? (Choose 4)

A. The DH key exchange is used to establish a shared secret over an insecure medium during an IPSec phase 1 exchange
B. A DH key exchange is an algorithm that utilizes asymmetric cryptographic keys
C. The DH exchange is used to authenticate the peer device during an IPSec phase 1 exchange
D. The DH exchange is susceptible to man-in-the-middle attacks
E. A DH exchange provides Perfect Forward Secrecy (PFS)

Correct Answer: ABDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 120
What is the most probable cause of the SSH debug messages?

```
00:26:51: SSH0: starting SSH control process
00:26:51: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
00:26:52: SSH0: protocol version id is - SSH-1.5-1.2.26
00:26:52: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:26:52: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH0: sending encryption confirmation
00:26:52: SSH0: keys exchanged and encryption on
00:26:52: SSH0: SSH_CMSG_USER message received
00:26:52: SSH0: authentication request for userid cisco
00:26:52: SSH0: SSH_SMSG_FAILURE message sent
00:26:54: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:26:54: SSH0: password authentication failed for cisco
00:26:54: SSH0: SSH_SMSG_FAILURE message sent
00:26:54: SSH0: authentication failed for cisco (code=7)
00:26:54: SSH0: Session disconnected - error 0x07
```

A. wrong user
B. bad password
C. SSH client not supported
D. Unsupported cipher

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 121
For a router to obtain a certificate from a CA, what is the first step of the certificate enrollment process?

A. the CA generates a certificate request and forwards it to the router.
B. the CA sends its public key to the router.
C. the router sends its public key to the CA.
D. the router generages a certificate request and forwards it to the CA.
E. the router generates an RSA key pair
F. the CA verifies the identity of the router.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 122
Which Cisco switch feature best protects against CAM table overflow attacks?

A. CAM table size definition
B. Storm Control
C. Port security
D. Network Based Application Recognition

E. IP spoof prevention

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 123
When configuring the Cisco Security Agent using preconfigured policies, what action should you take to customize the policy to fit your site's security needs? (choose two.)

A. The existing policy cannot cannot be edited.
B. Edit the existing policy
C. Clone and then edit the new policy
D. Add the existing poicy to the group and then edit the desired parameters.
E. Create and edit a new, similar policy.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 124
Refer to the Exhibit. A router running EIGRP with the "no ip classless" command contains the routing table as shown in the exhibit. What will happen to a packet destined for 172.16.254.1?

```
R1# show ip route
....
     172.16.0.0/16 is variably  subnetted, 2 subnets, 2 masks
D        172.16.32.0/20 [90/4879540] via  192.168.1.2
D       172.16.32.0/24  [90/25789217] via 192.168.1.1
S*   0.0.0.0/0 [1/0] via 192.168.1.3
```

A. The packet is forwarded to 192.168.1.1
B. The packet is dropped.
C. The packet is forwarded to 192.168.1.2
D. The packet is forwarded to 192.168.1.3

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 125
Which of the following describes the DHCP "starvation" attack?

A. Inject a DHCP server on the network for the purpose of overflowing DNS servers with bogus learned host names.
B. Saturate the network with DHCP requests preventing other network services working

C. Exhaust the address space available on the DHCP servers so an attacker can inject their own DHCP server to serve addresses for malicious reasons.
D. DHCP starvation is the act of sending DHCP-response packets for the purpose of overloading layer two CAM tables.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Explanation
DHCP Starvation
A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. This is easily achieved with attack tools such as gobbler. If enough requests are sent, the network attacker can exhaust the address space available to the DHCP servers for a period of time. This is a simple resource starvation attack just like a SYN flood is a starvation attack. The network attacker can then set up a rogue DHCP server on his or her system and respond to new DHCP requests from clients on the network. Exhausting all of the DHCP addresses is not required to introduce a rogue DHCP server, though.

QUESTION 126
When configuring an intrusion prevention sensor in promiscuous mode what type of malicious traffic can NOT be stopped?

A. Atomic attacks (single packet attacks)
B. Teardrop attacks
C. All of the above
D. Sweep reconnaissance (such as ICMP sweeps)
E. Flood attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 127
In most buffer overflow attacks, which of the following behavior should be expected?

A. Shell code to exploit the buffer.
B. A vulnerability used to overflow the buffer and an exploit used to run malicious software off of the stack.
C. A single crafted packet to overflow the buffer and run malicious software.
D. An exploit used to overflow the buffer and a vulnerability used to run malicious software off of the stack.

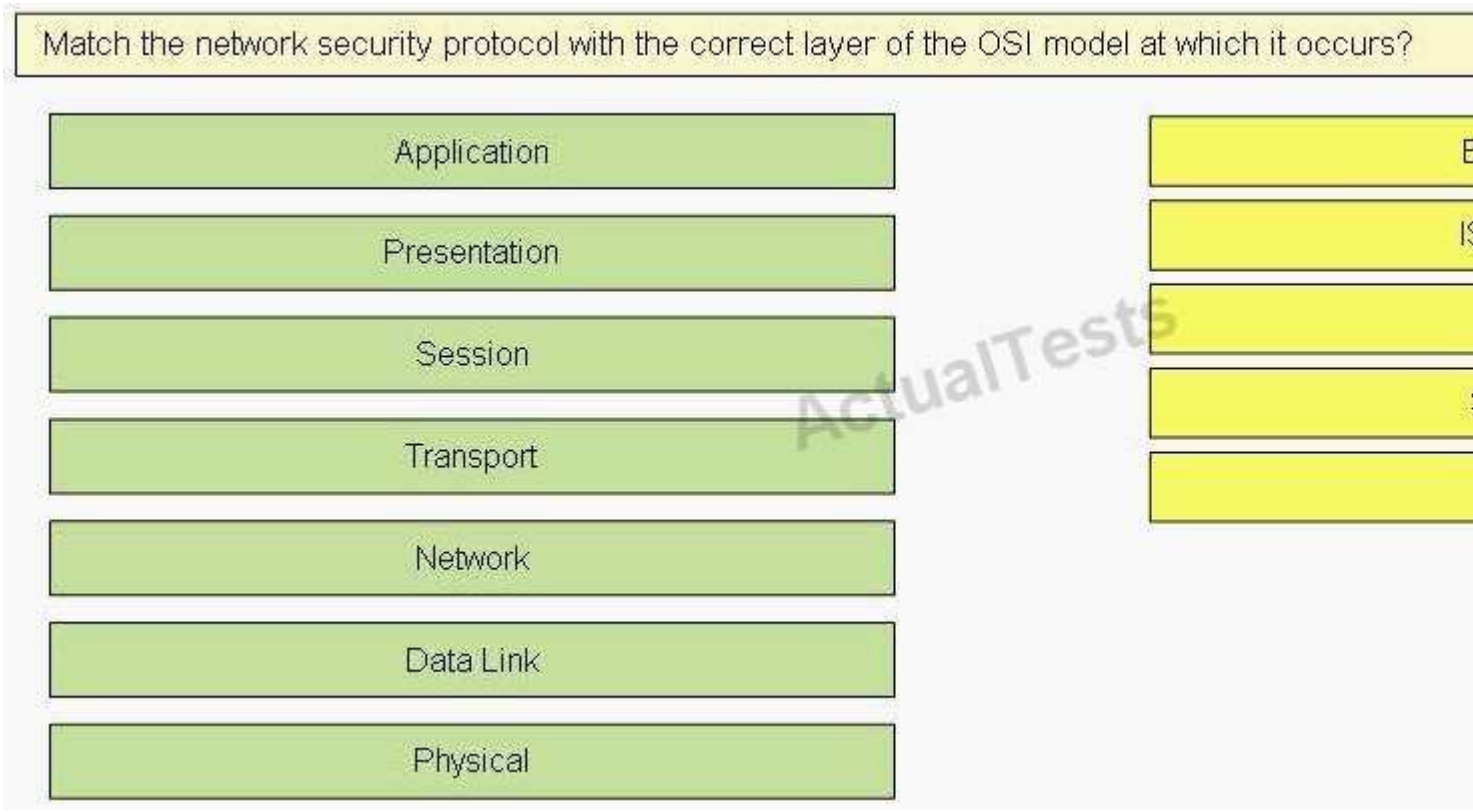
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
What causes the buffer overflow condition? Broadly speaking, buffer overflow occurs anytime the program writes more information into the buffer than the space it has allocated in the memory. This allows an attacker to overwrite data that controls the program execution path and hijack the control of the program to execute the attacker's code instead the process code.

QUESTION 128

DRAG DROP

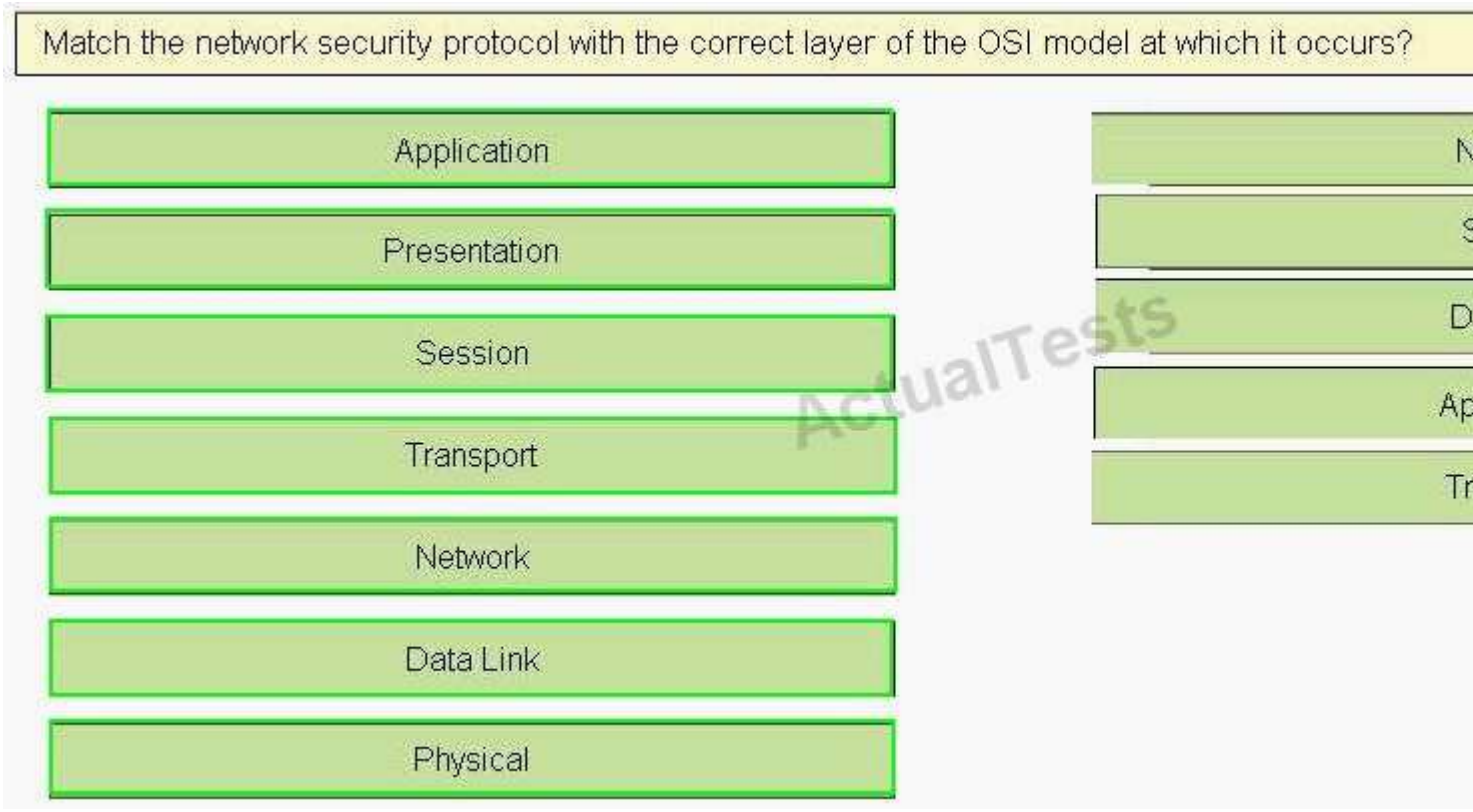
Drop



A.
B.
C.
D.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:



Explanation:

QUESTION 129
Asymmetric and symmetric ciphers differ in which two of the following ways? (Choose two.)

A. Asymmetric ciphers use public and private keys.
B. Symmetric ciphers are faster to compute.
C. Asymmetric ciphers are faster to compute.
D. Asymmetric ciphers use pre-shared keys.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 130
With NetFlow configured and several IPS, switches, routers and firewall devices imported into its database, CS-MARS will provide which of the following security features? (Choose 4)

A. Identify which hosts have CSA installed.
B. Draw a topology of your network.
C. Event correlation to help identify attacks
D. Make mitigation recommendations to stop attacks.
E. Identification of hosts that generate abnormal amounts of traffic.
F. Pull SNMP traps from different devices.

Correct Answer: BCDE

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cisco IOS NetFlow efficiently provides a key set of services for IP applications, including network traffic accounting, usage-based network billing, network planning, security, Denial of Service monitoring capabilities, and network monitoring. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing. Cisco invented NetFlow and is the leader in IP traffic flow technology.

NetFlow version 9, the latest Cisco IOS NetFlow innovation, is a flexible and extensible method to record network performance data. It is the basis of a new IETF standard. Cisco is currently working with a number of partners to provide customers with comprehensive solutions for NetFlow-based, planning, monitoring and billing.

NetFlow packet details:
NetFlow Analyzer accounts for the following details from the NetFlow Packets :
Source and destination IP address
Input and output interface number
Source and destination port number
Layer 4 Protocol
Number of packets in the flow
Total Bytes in the flow
Time stamp in the flow
Source and destination AS
TCP_Flag & TOS
Security Monitoring for Threat Control
Cisco Security Monitoring, Analysis and Response System (MARS) provides security monitoring for network security devices and host applications made by Cisco and other providers. Security monitoring greatly reduces false positives by providing an end-to-end view of the network, and can increase effective mitigation responses.
Other features and benefits of Cisco MARS:
· "Understands" the configuration and topology of your environment · Promotes awareness of environmental anomalies with Network Behavior Analysis using NetFlow

· Provides quick and easy access to audit compliance reports with more than 150 ready-to-use customizable reports
· Makes precise recommendations for threat removal, including the ability to visualize the attack path and identify the source of the threat with detailed topological graphs that simplify security response at Layer 2, and above
Security monitoring with Cisco Security MARS and Cisco Security Manager are part of the Cisco Security Management Suite, which delivers policy administration and enforcement for the Cisco Self-Defending Network.

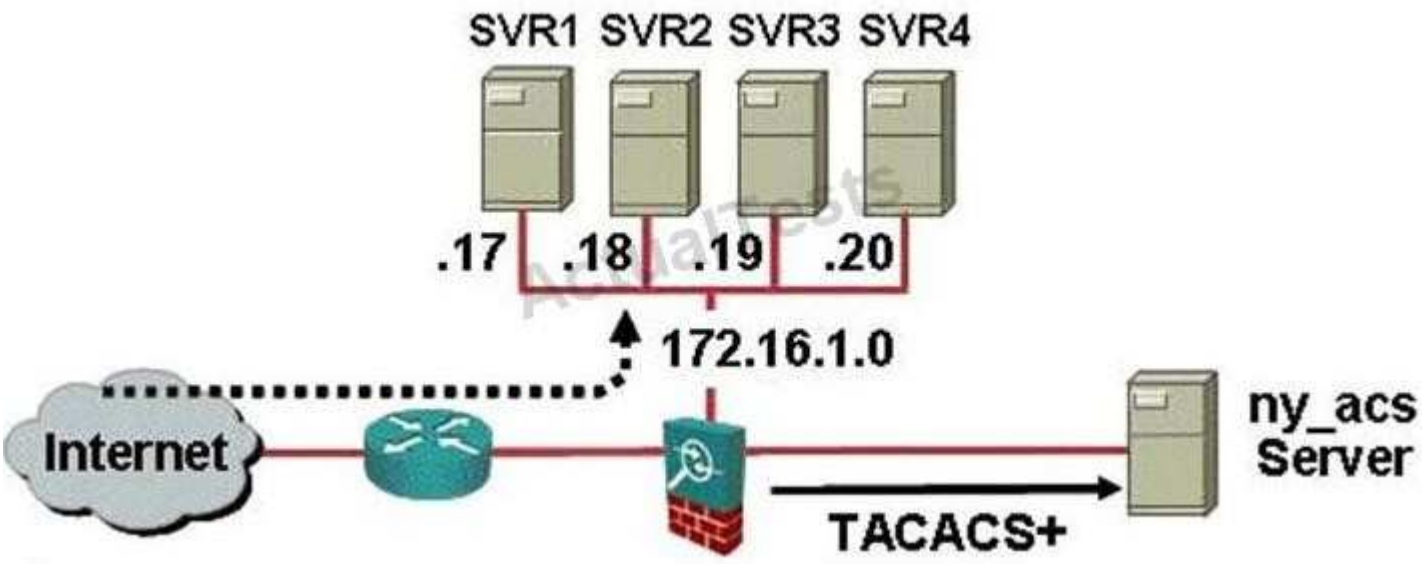
QUESTION 131
Which algorithms did TKIP add to the 802.11 specification? (Choose 3)

A. cyclic redundancy check
B. AES-based encryption
C. key mixing
D. message integrity check
E. anti-replay sequence counter

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 132
Refer to the network diagram in the exhibit. There are four servers on the DMZ. All servers are capable of supporting both FTP and HTTP applications. When a remote user accesses the security appliance and is authenticated, according to the group configuration in the ny_acs server, a remote user from this group is authorized to perform which two of the following actions? (Choose two.)



A. access any server on the DMZ
B. access any FTP server on the DMZ
C. access "SVR 2" only
D. use FTP and HTTP protocols
E. use HTTP only
F. use FTP only

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 133
Low and slow reconnaissance scans used to gain information about a system to see if it is vulnerable to an attack can be stopped with which of the following Cisco products?

A. ASA syn protection
B. ASA ICMP application inspection

C. CSA quarantine lists
D. IPS syn attack signatures
E. Cisco Guard

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 134
Which of the following best describes Chain of Evidence in the context of security forensics?

A. Evidence is locked down, but not necessarily authenticated.
B. Evidence is controlled and accounted for to maintain its authenticity and integrity.
C. The general whereabouts of evidence is known.
D. Someone knows where the evidence is and can say who had it if it is not logged.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 135
ASDM on the ASA platform is executed as:

A. A fully operational Visual Basic applicaton.
B. An active-x application or a java script application.
C. A java applet running in the context of your browser or a stand alone application using the java run-time environment.
D. A java script application and a PHP application
E. A fully compiled NET framework applicaton.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 136
Which two of the following are true for RFC 4301 - Security Architecture for the Internet Protocol (obsoletes RFC 2401)? (Choose two.)

A. Designed to provide security services for traffic at the IP layer, in both the IPv4 and IPv6 environments
B. Specifies the Security Architecture for the Internet.
C. Specifies the base architecture for IPsec-compliant systems.
D. Designed to provide security services for traffic at the IP layer, in the IPv4 environment only.
E. Specifies the base architecture for Key Management, the Internet Key Exchange (IKE)

Correct Answer: AC
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 137
Which of the following is one way to configure the security appliance to protect against DoS attacks?

A. Using the emb_lim option in the acl command
B. Using the tcp_max_conns option in the nat command
C. Using the emb_lim option in the static command
D. Using the emb_conns argument in the global command

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 138
Which is a benefit of implementing RFC 2827?

A. Prevents Dos from legimate, non-hostile end systems
B. Prevents disruption of "special services", such as Mobile IP
C. Allows DHCP or BOOTP packets to reach the relay agents as appropriate
D. Restricts directed broadcasts at the ingress router
E. Defeats Dos attacks which employ IP Source Address Spoofing

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
Recent occurrences of various Denial of Service (DoS) attacks which have employed forged source addresses have proven to be a troublesome issue for Internet Service Providers and the Internet community overall. This paper discusses a simple, effective, and straightforward method for using ingress traffic filtering to prohibit DoS attacks which use forged IP addresses to be propagated from 'behind' an Internet Service Provider's (ISP) aggregation point. While the filtering method discussed in this document does absolutely nothing to protect against flooding attacks which originate from valid prefixes (IP addresses), it will prohibit an attacker within the originating network from launching an attack of this nature using forged source addresses that do not conform to ingress filtering rules. All providers of Internet connectivity are urged to implement filtering described in this document to prohibit attackers from using forged source addresses which do not reside within a range of legitimately advertised prefixes. In other words, if an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.

QUESTION 139
Which of the following describes the DHCP "starvation" attack?

A. DHCP starvation is the act of sending DHCP-response packets for the purpose of overloading layer two CAM tables.
B. Inject a DHCP server on the network for the purpose of overflowing DNS servers with bogus learned host

names.

C. Exhaust the address space available on the DHCP servers so an attacker can inject their own DHCP server to serve addresses for malicious reasons.
D. Saturate the network with DHCP requests preventing other network services working.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 140
Which Cisco security software product mitigates Day Zero attacks on desktops and servers - stopping known and unknown attacks without requiring reconfigurations or updates on the endpoints?

A. Cisco Trust Agent (CTA)
B. Cisco Security Agent (CSA)
C. NAC Appliance Agent (NAA)
D. Cisco Secure Desktop (CSD)
E. SSL VPN Client (SVC)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 141
Which of the following signatures was created by an IPS adminisrator using the custom signature creation capability of IPS?

A. 2000 - ICMP Echo Reply
B. 3050 - Half-open SYN attack
C. 12000 - Gator Spyware Beacon
D. 9000 - TCP Backdoor Probe.
E. 6000- BitTorrent File Download.

Correct Answer: E
Section: (none)
Explanation

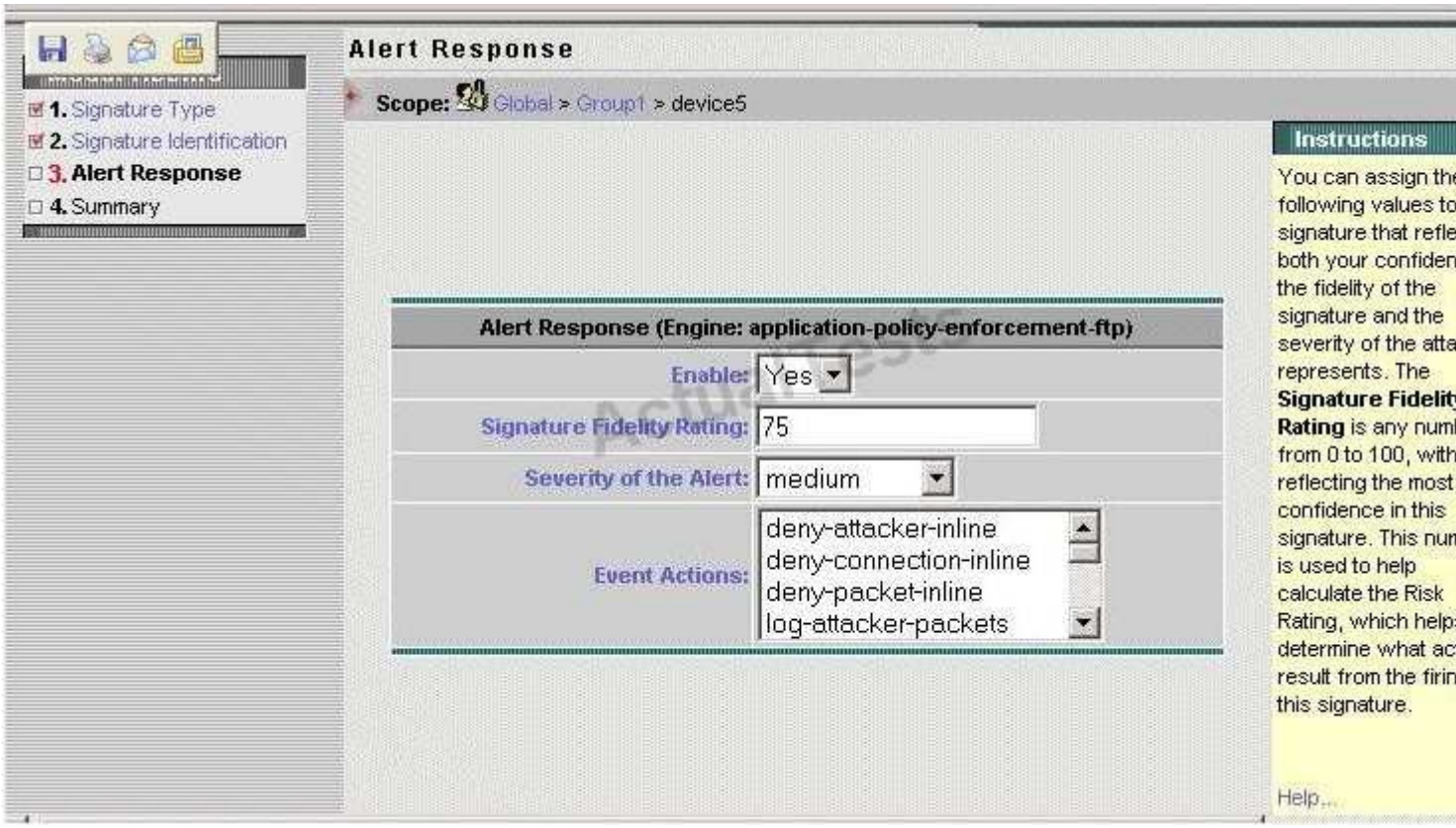
Explanation/Reference:
Explanation:

Signatures
Cisco IPS prevents intrusion by comparing traffic against the signatures of known attacks. Cisco IOS images that support Cisco IPS have built-in signatures that Cisco IPS can use, and you can also have Cisco IPS import signatures for the router to use when examining traffic. Imported signatures are stored in a signature definition file (SDF). This window lets you view the configured Cisco IPS signatures on the router. You can add customized signatures, or import signatures from SDFs downloaded from Cisco.com. You can also edit, delete, enable, and disable signatures.
Cisco IPS is shipped with an SDF that contains signatures that your router can accommodate. To learn more about the SDF shipped with Cisco IPS, and how to have Cisco IPS use it, click IPS- Supplied Signature Definition Files.

Adding a 5.x Custom Signature By Using the Signature Wizard You can create custom signatures using the Signature Wizard. The Signature Wizard creates custom signatures at the device level, not at the group level.
To use the Signature Wizard, follow these steps:
Step 1 Select Configuration > Settings.
Step 2 In the TOC, click the Object Selector handle.
Step 3 In the Object Selector, select the 5.x sensor for which you want to create a custom signature.
Step 4 In the TOC, select Signature Wizard > IPS 5.x.
The Signature Wizard welcome page appears.
Step 5 Click Start the Wizard.
a. Select either Engine Type or Protocol Type as the type of signature you want to create.
The Select Engine drop-down list appears.

65

b. Enter the signature name in the Signature Name field and then click Next>.
The Alert Response page appears.



d. Enter the signature fidelity rating in the Signature Fidelity Rating field. f. Select the action or actions that should be taken from the Event Action list. Then click Next>. You can press and hold the Ctrl key while selecting, to select more than one Event Action from the list.
The Summary page appears.
h. Click Finish>.
The system displays a message that notifies you that the signature has been succesfully created. j. Verify that the new custom signature has been specified correctly:
a. In the TOC, select Signatures.
c. In the Select Group list box, select Custom.
e. Confirm the appearance of the new custom signature in the list, which signifies that it was

added.

QUESTION 142
Which of these is the best way to provide sender non-repudiation?

A. secure hash
B. SSL
C. pre-shared key
D. RSA signature

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 143
Which algorithms did TKIP add to the 802.11 specification? (Choose 3)

A. key mixing
B. AES-based encryption
C. cyclic redundancy check
D. anti-replay sequence counter
E. message integrity check

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 144
Refer to the exhibit. A Cisco security appliance has been correctly configured and inserted between routers.R1 and R2.The security appliance allows Ibgp connectivity between R1 and R2 and BGP is fully functional. To increase security, MD5 neighbor authentication is correctly configured on R1 and R2. Unfortunately, BGP stops working after the MD5 configuration is added. What configuration task must be completed on the security appliance to restore BGP connectivity?

A. Configure the MD5 authentication key on the security appliance
B. Add the MD5 key to the security appliance BGP fixup configuration
C. Add norandomseq to the static NAT translation on the security appliance
D. Configure a GRE tunnel to allow authenticated BGP connections to traverse the security appliance
E. Configure authentication-proxy on the security appliance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 145
You are configuring a Cisco switch in a NAC Framework solution, what is the resulting action of issuing the `device authorize` **command have in the** `(config-identity-prof)#` **sub-configuration mode?**

A. Maps the NAD to clientless host for posture authorization.
B. Enables an EOUoUPD identity profile for clientless hosts.
C. Statically maps an access list to a NAC Agentless Host (NAH)
D. Statically authorizes and maps devices to an access policy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 146
How can Netflow be used to help identify a day-zero scanning worm?

A. Netflow tracks destination address.
B. Netflow protects against unknown virus attacks.
C. Netflow statistics can show a huge increase in traffic on a specific day.
D. Netflow makes sure that only the correct applications are using their designated ports.
E. Netflow prevents buffer overflow attacks.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 147
Which two are correct functions of the Cisco Anomaly Guard and Detector for preventing DDOS attacks?(Choose two.)

A. uses Netflow data for anomaly detections
B. using topology and configuration awareness, events from different devices are correlated and attacks mitgitations are performed at the optimal location
C. builds baseline profiles of normal operating conditions, enabling rapid identification of unusual activity that indicates an attack
D. dynamic diversion redirects and cleans only traffic destined for targeted devices, allowing unaffected traffic to flow freely and ensuring business continuity
E. pushes ACLs to network devices to only block the malicious traffic
F. accept events inputs from different network devices via syslog, SDEE and SNMP

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 148
Which ones are the two types of ciphers?

A. 3DES cipher and AES cipher
B. Blocker cipher and Streamer cipher

C. Block cipher and Stream cipher
D. Blocking cipher and non-blocking cipher.
E. CBC cipher and EBC cipher

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In cryptography, a block cipher is a symmetric key cipher which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation. When encrypting, a block cipher might take a (for example) 128-bit block of plaintext as input, and output a corresponding 128-bit block of ciphertext. The exact transformation is controlled using a second input -- the secret key. Decryption is similar: the decryption algorithm takes, in this example, a 128-bit block of ciphertext together with the secret key, and yields the original 128-bit block of plaintext. To encrypt messages longer than the block size (128 bits in the above example), a mode of operation is used.
Block ciphers can be contrasted with stream ciphers; a stream cipher operates on individual digits one at a time, and the transformation varies during the encryption. The distinction between the two types is not always clear-cut: a block cipher, when used in certain modes of operation, acts effectively as a stream cipher.
An early and highly influential block cipher design was the Data Encryption Standard (DES), developed at IBM and published as a standard in 1977. A successor to DES, the Advanced Encryption Standard (AES), was adopted in 2001.

QUESTION 149
Which statement is true concerning PAT?

A. PAT provides access control.
B. PAT is the preferred method to map servers to external networks.
C. PAT rewrites the source address and port.
D. PAT keeps ports but rewrites address.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 150
Which three statements regarding Cisco ASA multicast routing support are correct? (Choose three.)

A. The ASA supports both PIM-SM and bi-directional PIM.
B. When configured for stub multicast routing, the ASA can act as the Rendezvous Point (RP)
C. The ASA can be configured for IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring the multicast traffic to be forwarded only those interfaces associated with hosts requesting the multicast group.
D. Enabling multicast routing globally on the ASA automatically enables PIM and IGMP on all interfaces.
E. ASA supports both stub multicast routing and PIM multicast routing. However, you cannot configure both concurrently on a single security appliance.
F. If the ASA detects IGMP version 1 routers, the ASA will automatically switch to IGMP version 1 operations.

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 151
Which of the following is the correct diagram for an IPsec Authentication Header?

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Authentication header (AH)
The AH is intended to guarantee connectionless integrity and data origin authentication of IP datagrams. Further, it can optionally protect against replay attacks by using the sliding window technique and discarding old packets. AH protects the IP payload and all header fields of an IP datagram except for mutable fields, i.e. those that might be altered in transit. In IPv4, mutable (and therefore unauthenticated) IP header fields include TOS, Flags, Fragment Offset, TTL and Header Checksum. AH operates directly on top of IP, using IP protocol number 51. An AH packet diagram:

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Authentication data (variable)			

Field meanings:
Next header
Identifies the protocol of the transferred data.
Payload length
Size of AH packet.
RESERVED
Reserved for future use (all zero until then).
Security parameters index (SPI)
Identifies the security parameters, which, in combination with the IP address, then identify the security association implemented with this packet.
Sequence number
A monotonically increasing number, used to prevent replay attacks.
Authentication data
Contains the integrity check value (ICV) necessary to authenticate the packet; it may contain

padding.

QUESTION 152
An attacker is attempting to use a Telnet session to reach a specific host secured behind a firewall rule that only allows inbound connections on TCP port 25. How can the attacker exploit RFC 791 (IP) to perform this attack?

A. Send a SYN/ACK to the host on TCP port 23 indicating a response to a SYN request from the host on the secure side of the firewall
B. Send packets with a fragmentation offset of 20 and a TCP destination port 25. All subsequent packets will overwrite the IP header allowing a new IP header to be inserted
C. Send two packets, the first packet with the DF bit clear and the MF bit set, and the second packet with a fragmentation offset of 1 and a destination port of TCP 23
D. Set the TOS bits to 1111 1100 indicating a network control packet that should be forwarded to the host with high reliability (no discard)
E. Send packets destined for TCP port 23 with the DF and MF bits clear and the fragment offset to 0 since many firewalls will pass IP fragments with a 0 offset

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 153
With PGP, which of the following entity signs a users's public key?

A. The sender's administrator who provides the sender with the PGP program
B. The vendor of the PGP program
C. The sender of the message
D. The receipient of the message
E. A third party that belongs to what's often known as "web of trust", that can verify the relationship between the user and the key

Correct Answer: E
Section: (none)
Explanation

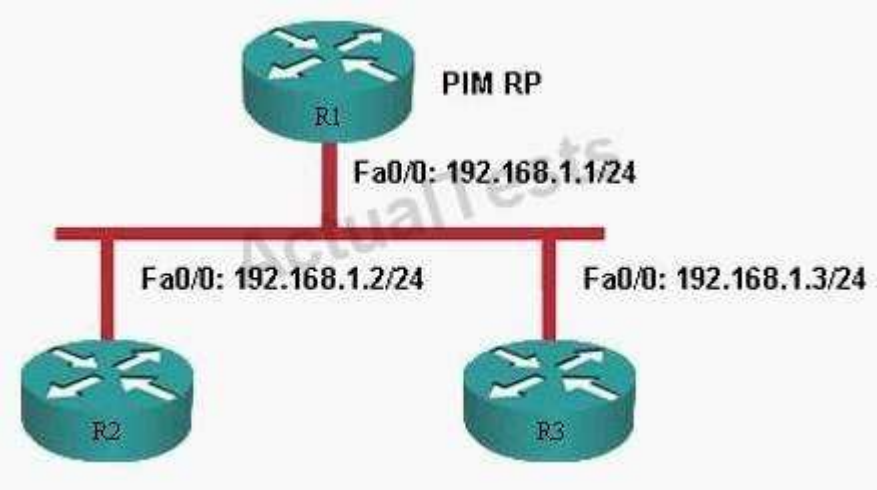
Explanation/Reference:
Explanation: Explanation
Pretty Good Privacy is a computer program that provides cryptographic privacy and authentication. It was originally created by Philip Zimmermann in 1991. PGP and other similar products follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data.

PGP encryption uses public-key cryptography and includes a system which binds the public keys to a user name. The first version of this system was generally known as a web of trust to contrast with the X.509 system which uses a hierarchical approach based on certificate authority and which was added to PGP implementations later. Current versions of PGP encryption include both alternatives through an automated key management server.

Web of trust
Both when encrypting messages and when verifying signatures, it is critical that the public key one uses to send messages to someone or some entity actually does 'belong' to the intended recipient. Simply downloading a public key from somewhere is not overwhelming assurance of that association; deliberate (or accidental) spoofing is possible. PGP has, from its first versions, always included provisions for distributing a user's public

keys in an 'identity certificate' which is so constructed cryptographically that any tampering (or accidental garble) is readily detectable. But merely making a certificate effectively impossible to modify undetectably is also insufficient. It can prevent corruption only after the certificate has been created, not before. Users must also ensure by some means that the public key in a certificate actually does belong to the person/entity claiming it. From its first release, PGP products have included an internal certificate 'vetting scheme' to assist with this; a trust model which has been called a web of trust. A given public key (or more specifically, information binding a user name to a key) may be digitally signed by a third party user to attest to the association between someone (actually a user name) and the key. There are several levels of confidence which can be included in such signatures. Although many programs read and write this information, few (if any) include this level of certification when calculating whether to trust a key.
The web of trust protocol was first described by Zimmermann in the manual for PGP version 2.0:
As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys.
The web of trust mechanism has advantages over a centrally managed PKI scheme such as that used by S/MIME, but has not been universally used. Users have been willing to accept certificates and check their validity manually, or to simply accept them. The underlying problem has found no satisfactory solution.

QUESTION 154
Refer to the exhibit. Which one of the following R1 router configurations will correctly prevent R3 from becoming a PIM neighbor with rendezvous point R1?



A. access-list 1 deny 192.168.1.3 255.255.255.255!interface fa0/0ip pim neighbor-filter 1
B. access-list 1 permit 192.168.1.3 255.255.255.255ip pim rp-announce-filter rp-list 1
C. access-list 1 permit 192.168.1.2 255.255.255.255access-list 1 deny any!interface fa0/0ip pim bidir-neighbor-filter 1
D. access-list 1 permit 192.168.1.2 255.255.255.255!interface fa0/0ip multicast boundary 1 filter- autorop
E. access-list 1 deny 192.168.1.3 255.255.255.255!interface fa0/0ip igmp access-group 1

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 155
Which of the following lines is incorrect in the following IOS IKE configuration?

```
crypto isakmp policy 7
encryption aes
hash sha 1
authentication rsa-sig
group 2
lifetime 86400
```

A. encryption aes
B. hash sha 1
C. crypto isakmp policy 7
D. group 2
E. lifetime 86400
F. authentication rsa-sig

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 156
Which one of these statements is true about a Pre-Block ACL configured when setting up your sensor to perform IP blocking?

A. The Pre-Block ACL is overwritten when a blocking action is initiatied by the sensor.
B. You can not configure a Pre-Block ACL when configuring IP Blocking on your sensor.
C. The Pre-Block ACL entries override the blocking ACL entries generated by the sensor.
D. The blocking ACL entries generated by the sensor override the Pre-Block ACL entries.
E. The Pre-Block ACL is replaced by the Post-Block ACL when a blocking action is initiated by the sensor.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 157
Which two IP multicast addresses belong to the group represented by the MAC address 0x01-00- 5E-15-6A-2C? (Choose two.)

A. 233.149.106.44
B. 224.21.106.44
C. 224.25.106.44
D. 236.25.106.44
E. 239.153.106.44

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 158
Which two of the following are correct regarding the Cisco Trust Agent? (Choose two.)

A. Includes both a Layer 3 communication component using EAP over UDP, as well as an 802.1x supplicant, allowing layer 2 EAP over LAN communications.
B. Can communicate the Cisco Security Agent (CSA) version, OS and patch version, as well as the presence, version, and other posture information of third-party applications that are part of the NAC initiative to the Authentication Server.
C. Provides the capability at the endpoint to apply QoS markings to application network traffic as specified by Cisco Trust Agent policy rules.
D. Resides between the applications and the Operating System Kernel to prevent day zero attacks.
E. Available on Windows operating systems only.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 159
When configuring IOS firewall (CBAC) operations on Cisco routers, the "inspectin rule" could be applied at which two locations? (Choose two.)

A. at the untrusted interface in the outbound direction
B. at the trusted interface in the inbound direction
C. at the trusted and untrusted interface in the inbound direction
D. at the trusted interface in the outbound direction
E. at the untrusted interface in the inbound direction
F. at the trusted and untrusted interface in the outbound direction

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 160
Using FTP passive mode, after the client opens the command channel (port 21) to the FTP server and requests passive mode, what will be the next step?

A. The FTP server opens the data channel to the client using the port number indicated by the client
B. The FTP client opens the data channel to the FTP server on Port 21 77

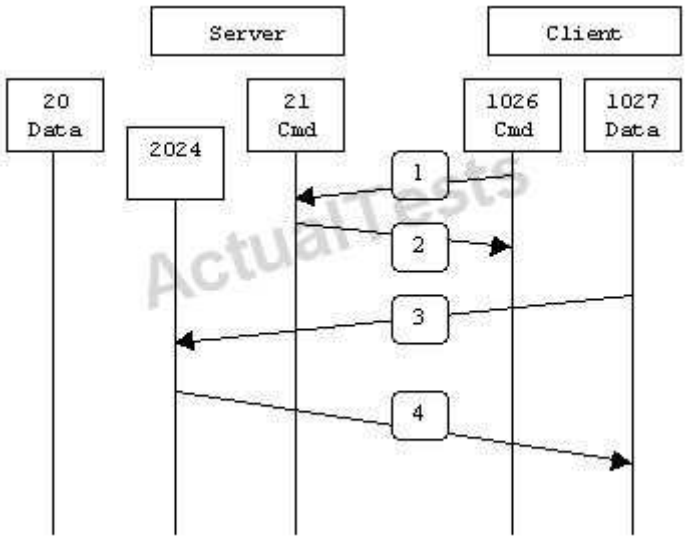
C. The FTP client opens the data channel to the FTP server on Port 20
D. The FTP server sends back an acknowledgment (ACK) to the client
E. The FTP server allocates a port to use for the data channel and transmit that port number to the client

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Passive FTP
In order to resolve the issue of the server initiating the connection to the client a different method for FTP connections was developed. This was known as passive mode, or PASV, after the command used by the client to tell the server it is in passive mode. In passive mode FTP the client initiates both connections to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server. When opening an FTP connection, the client opens two random unprivileged ports locally (N > 1023 and N+1). The first port contacts the server on port 21, but instead of then issuing a PORT command and allowing the server to connect back to its data port, the client will issue the PASV command. The result of this is that the server then opens a random unprivileged port (P > 1023) and sends the PORT P command back to the client. The client then initiates the connection from port N+1 to port P on the server to transfer data.
From the server-side firewall's standpoint, to support passive mode FTP the following communication channels need to be opened:
FTP server's port 21 from anywhere (Client initiates connection) FTP server's port 21 to ports > 1023 (Server responds to client's control port) FTP server's ports > 1023 from anywhere (Client initiates data connection to random port specified by server)
FTP server's ports > 1023 to remote ports > 1023 (Server sends ACKs (and data) to client's data port)
When drawn, a passive mode FTP connection looks like this:

78



In step 1, the client contacts the server on the command port and issues the PASV command. The server then replies in step 2 with PORT 2024, telling the client which port it is listening to for the data connection. In step 3 the client then initiates the data connection from its data port to the specified server data port. Finally, the server sends back an ACK in step 4 to the client's data port.

QUESTION 161
If you trace a ping through an IPsec or 3DES tunnel, which of these is true regarding the appearance of tunneled or encrypted packets?

A. The same key is used, but an index vector is used by IPSec to offset the key, resulting in a unique packet for each transmission.
B. The encryption key changes for each packet, resulting in a unique packet for each transmission.
C. The packets will likely be the same except for TTL and the sequence number.

D. A characteristic of 3-DES ensures that no two packets are alike.
E. The only way to ensure that packets are unique is to use AH as a header protocol.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 162
Cisco Clean Access ensures that computers connecting to your network have which of the following?

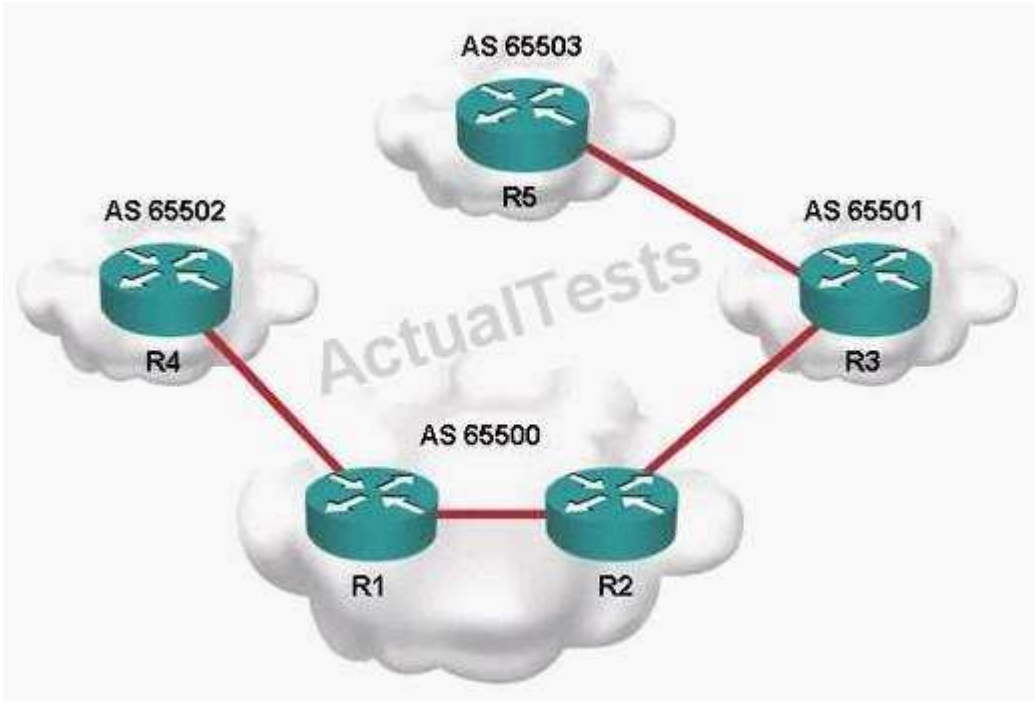
A. Current IPS signatures
B. No vulnerable applications or operating systems
C. Cisco Security Agent
D. No viruses or worms
E. Appropriate security applications and patch levels

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Immunize Networks with Policy Enforcement
Cisco NAC Appliance (formerly Cisco Clean Access) is an easily deployed Network Admission Control (NAC) product that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With NAC Appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access. It identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network's security policies and repairs any vulnerabilities before permitting access to the network. When deployed, Cisco NAC Appliance provides the following benefits:
· Recognizes users, their devices, and their roles in the network. This first step occurs at the point of authentication, before malicious code can cause damage. · Evaluates whether machines are compliant with security policies. Security policies can include specific antivirus or antispyware software, OS updates, or patches. Cisco NAC Appliance supports policies that vary by user type, device type, or operating system. · Enforces security policies by blocking, isolating, and repairing noncompliant machines. Noncompliant machines are redirected into a quarantine area, where remediation occurs at the discretion of the administrator.

QUESTION 163
Refer to the Exhibit. What as-path access-list regular expression should be applied no R2 as a neighbor filter-list to only allow updates with an origin of AS65503?



A. 65503
B. _65503$
C. ^65503.*
D. _65503.$
E. ^65503$
F. _65503_

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 164
When configuring system state conditions with the Cisco Security Agent, what is the resulting action when configuring more than one system state condition?

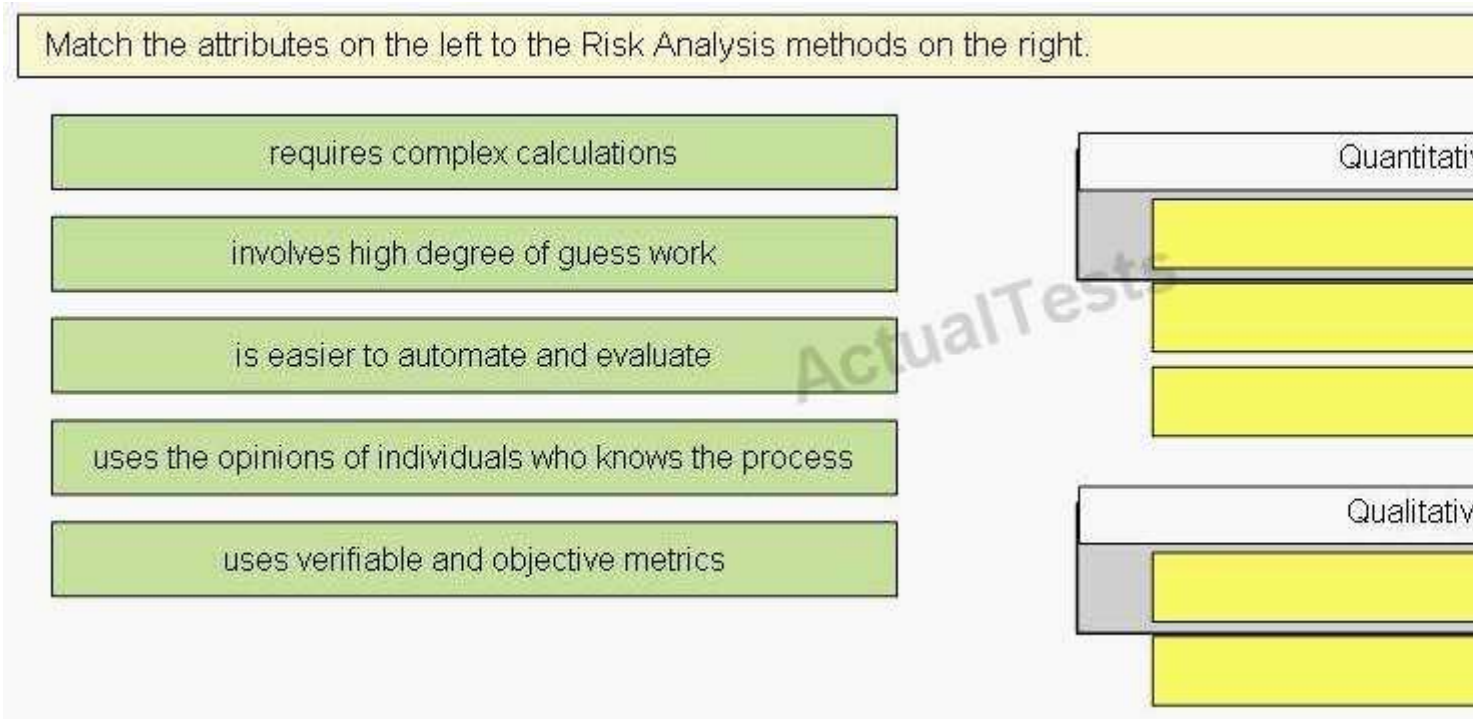
A. Any matching state condition will result with the state being triggered.
B. Once a state condition is met, the system ceases searching further conditions and will cause the state condition to trigger.
C. Once the state conditions are met, they become persistent and can only be removed using the Reset feature.
D. All specified state conditions are used as part of the requirements to be met to for the state to trigger.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 165
DRAG DROP

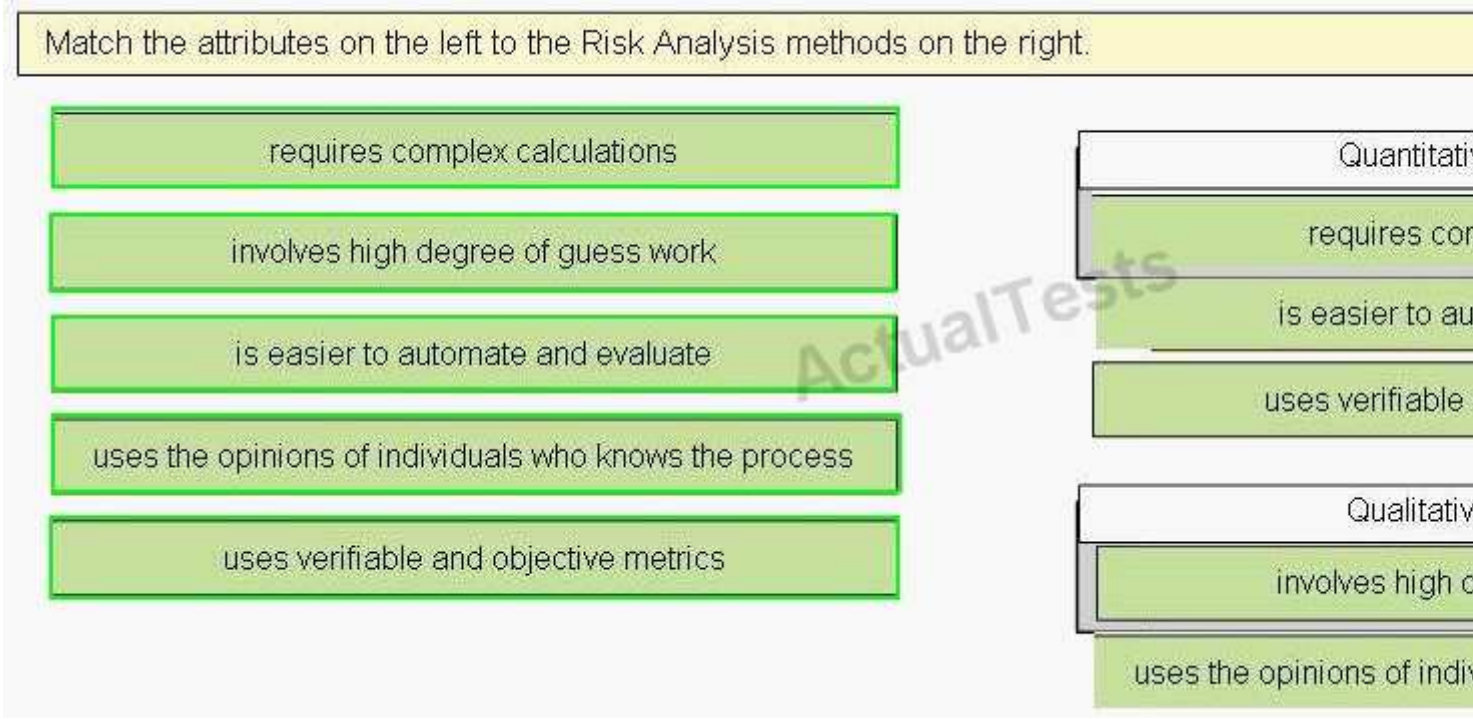
Drop



A.
B.
C.
D.

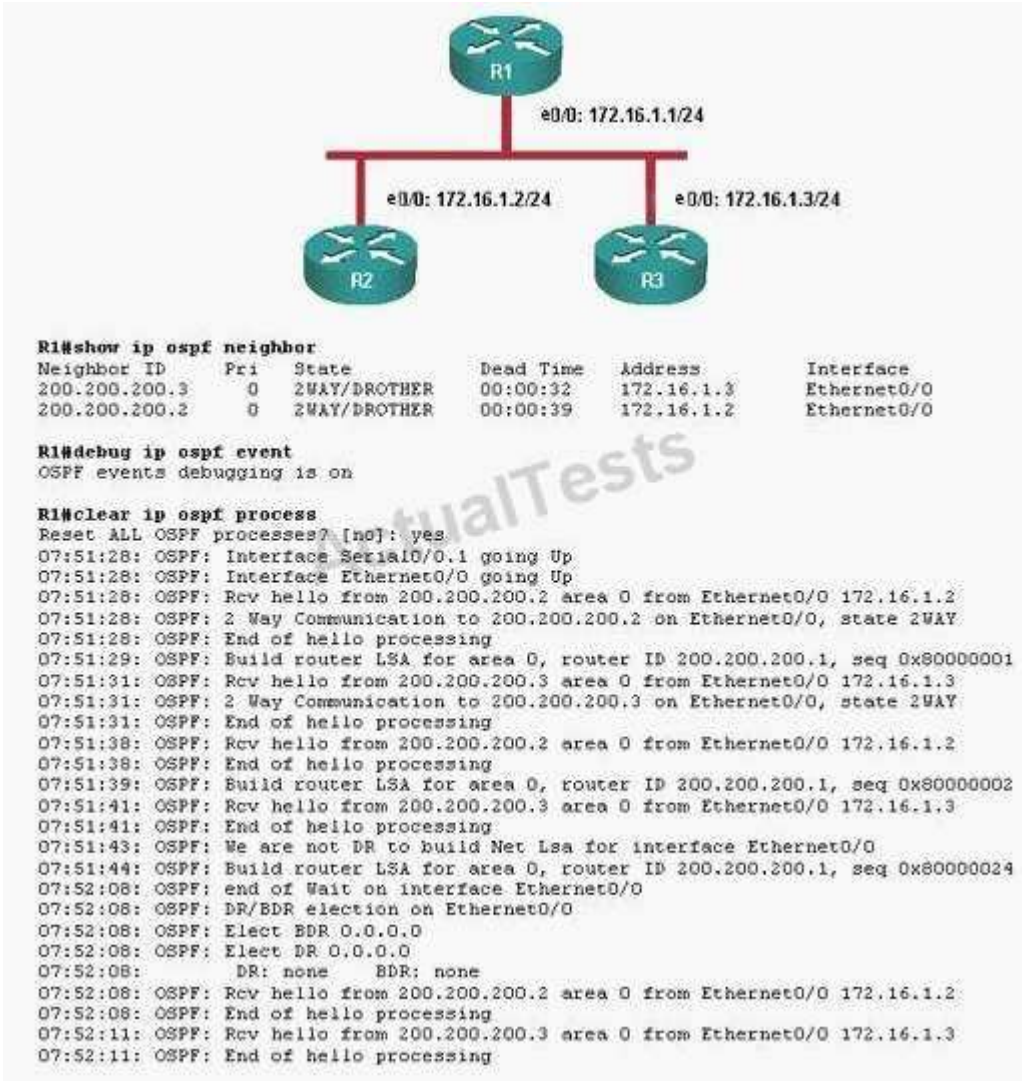
Correct Answer:
Section: (none)
Explanation

Explanation/Reference:



Explanation:

QUESTION 166
Refer to the Exhibit. Router R1 is stuck in 2-WAY state with neighbors R2 and R3. As a result R1 has an incomplete routing table. To troubleshoot the issue, the show and debug commands in the exhibit are entered on R1. Based on the output of these commands what is the most likely cause of this problem?



A. All the routers on the Ethernet segment have been configured with "ip ospf priority 0"
B. The Ethernet 0/0 interfaces on these routers are missing the "ip ospf network broadcast" command.
C. The hello timers on the segment between these routers do not match.
D. The Ethernet 0/0 interfaces on R1 has been configured with the command, "ip ospf network non-broadcast".
E. R1 can not form an adjacency with R2 or R3 because it does not have a matching authentication key.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 167
Which of the following is true about RADIUS Vendor Specific Attribute? (Choose 3)

A. A radius server that does not understand the vendor-specific information sent by a client must reject the authentication request
B. The RADIUS Vendor Specific Attribute type is decimal 26
C. Vendor Specific Attribute MUST include the Length field

D. In Cisco's Vendor Specific Attribute implementation, vendor-ID of 1 is commonly referred to as Cisco AV (Attribute Value) pairs.
E. Vendor Specific Attributes use a RADIUS attribute type between 127 and 255.
F. A vendor can freely choose the Vendor-ID it wants to use when implementing Vendor Specific Attributes as long as the same Vendor-ID is used on all of its products.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 168
What security reporting system is analogous to CS-MARS?

A. Security Reporting and Response System SRRS
B. Security Incident Response System SIRT
C. Security Information Management System SIM
D. Security Threat Mitigation System STM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: Explanation
The CS-MARS is most analogous or like a secuirty Threat Mitgation systems because MARS finds security risks and helps to mitigate or protect against them by all of the following:

Security Monitoring for Threat Control
Cisco Security Monitoring, Analysis and Response System (MARS) provides security monitoring for network security devices and host applications made by Cisco and other providers. Security monitoring greatly reduces false positives by providing an end-to-end view of the network, and can increase effective mitigation responses. Other features and benefits of Cisco MARS:
· "Understands" the configuration and topology of your environment · Promotes awareness of environmental anomalies with Network Behavior Analysis using NetFlow

· Provides quick and easy access to audit compliance reports with more than 150 ready-to-use customizable reports
· Makes precise recommendations for threat removal, including the ability to visualize the attack path and identify the source of the threat with detailed topological graphs that simplify security response at Layer 2, and above

QUESTION 169
What is NTP crucial for?

A. Clock
B. Routing Updates
C. Validating Certificates
D. Time Zone
E. Accurate Logging
F. Kerberos Tickets

Correct Answer: CEF
Section: (none)

Explanation

Explanation/Reference:
Explanation:
NTP (Network Time Protocol) is a protocol designed to synchronize the clocks of computers over a network. NTP version 3 is an internet draft standard, formalized in RFC 1305. NTP version 4 is a significant revision of the NTP standard, and is the current development version, but has not been formalized in an RFC. Simple NTP (SNTP) version 4 is described in RFC 2030.

Answer A is correct
NTP synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows events to be correlated when system logs are created and other time- specific events occur.
http://www.cisco.com/en/US/tech/tk648/tk362/tk461/tsd_technology_support_sub- protocol_home.html
C is correct
Proper validation of certificates typically requires checking to ensure the certificate has not yet expired. If devices have a real-time clock, they SHOULD verify the certificate validity dates. If no real-time clock is available, the device SHOULD attempt to determine the current time using NTP prior to certificate validation. If neither is available, devices SHOULD verify that the start validity date of its peer's certificate is less than its own certificate's expiration date, and its peer's expiration date is greater than its own start date. Note that failure to check a certificate's temporal validity can make a device vulnerable to man-in-the-middle attacks launched using compromised, expired certificates, and therefore devices should make every effort to perform this validation.
E is correct
Kerberos time sensitivity
Time is a critical service in Windows 2000 and Windows Server 2003. Timestamps are needed for directory replication conflict resolution, but also for Kerberos authentication. Kerberos uses timestamps to protect against replay attacks. Computer clocks that are out of sync between clients and servers can cause authentication to fail or extra authentication traffic to be added during the Kerberos authentication exchange.

QUESTION 170
With the Cisco's IOS Authentication Proxy feature, users can initiate network access via which three protocols? (Choose three.)

A. HTTP/HTTPS
B. L2TP
C. TELNET
D. IPSec
E. SSH
F. FTP

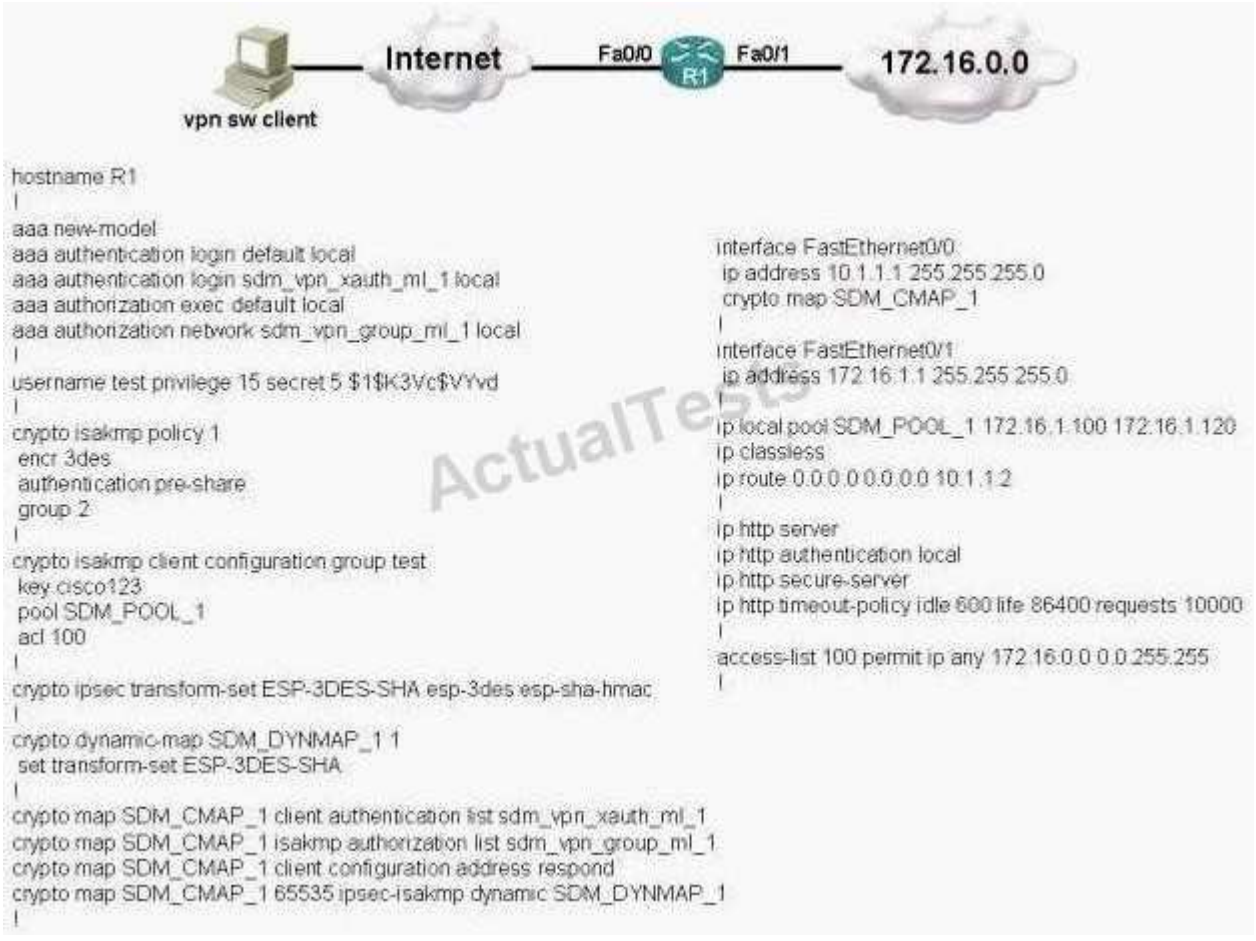
Correct Answer: ACF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

2651-1(config)#ip auth-proxy name test ?
ftp FTP Protocol
http HTTP Protocol
telnet Telnet Protocol
debug ip auth-proxy
To display the authentication proxy configuration information on the router, use the show ip auth- proxy configuration command in privileged EXEC mode.
debug ip auth-proxy {ftp | function-trace | http | object-creation | object-deletion | tcp | telnet | timer} Syntax Description

ftp	Display FTP events related to the authentication proxy.
function-trace	Display the authentication proxy functions.
http	Display HTTP events related to the authentication proxy.
object-creation	Display additional entries to the authentication proxy cache.
object-deletion	Display deletion of cache entries for the authentication proxy.
tcp	Display TCP events related to the authentication proxy.
telnet	Display Telnet related authentication proxy events.
timer	Displays authentication proxy timer-related events.

QUESTION 171
Referring to the network diagram and the R1 router configurations shown in the exhibit, why remote users using their Cisco VPN software client are not able to reach the 172.16.0.0 networks behind R1 once they successfully VPN into R1?



A. Reverse Route Injection (RRI) is not enabled on R1
B. The R1 configuration is missing the crypto ACL
C. The ACL 100 on R1 is misconfigured.

D. The Cisco VPN software client does not support DH group 2
E. The dynamic crypto map on R1 is misconfigured.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A is incorrect because the Cisco VPN client does support DH Group 2 B is incorrect because

Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities. Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote Virtual Private Network (VPN) router as the next hop, the traffic is forced through the crypto process to be encrypted. http:// www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gt_rrie.ht m

C is incorrect because the cyrpto ACL is not missing

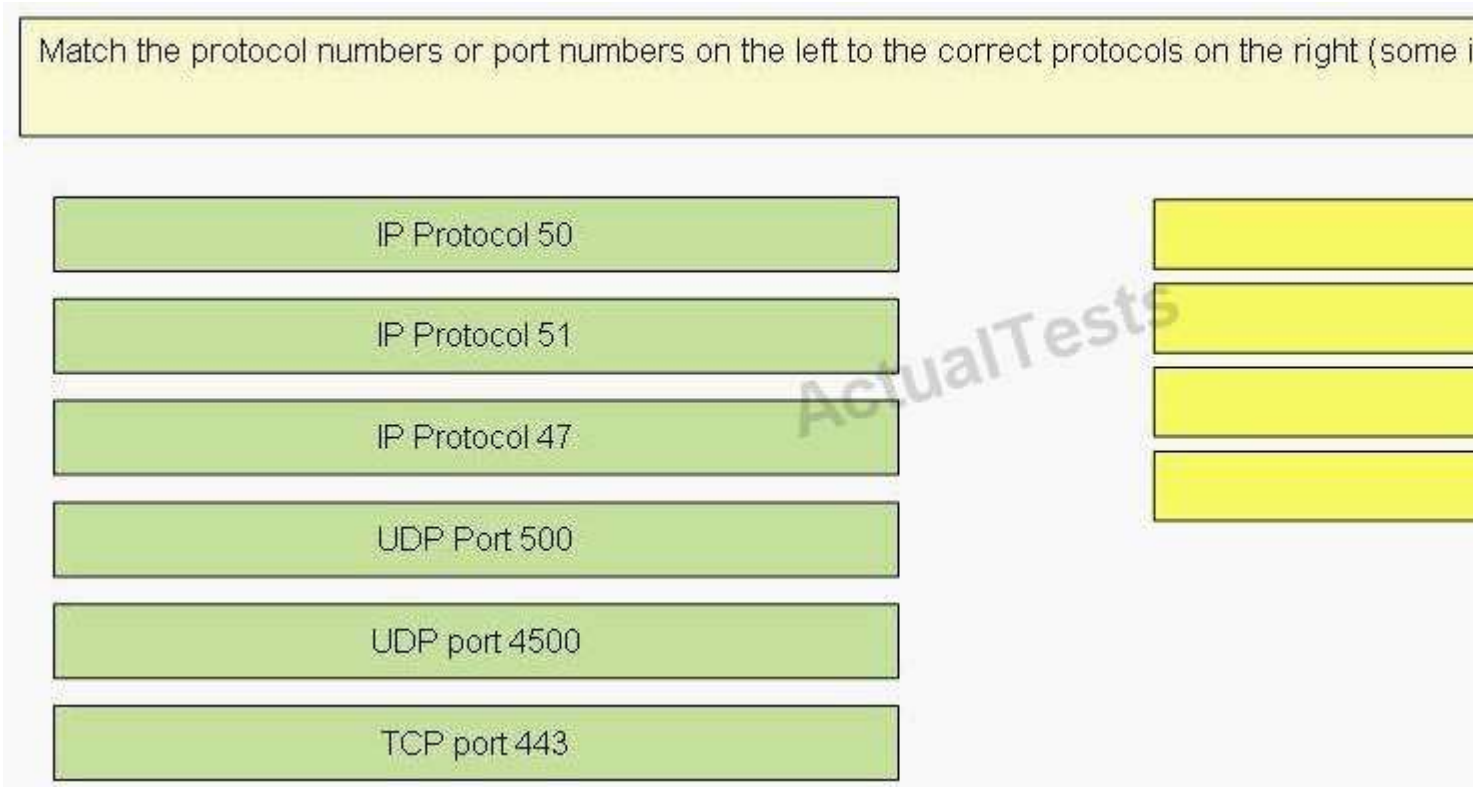
The Crypto Access Check on Clear-Text Packets feature removes the checking of clear-text packets that go through the IP Security (IPSec) tunnel just prior to encryption or just after decryption. The clear-text packets were checked against the outside physical interface access control lists (ACLs). This checking was often referred to as a double ACL check. This feature enables easier configuration of ACLs and eliminates the security risks that are associated with a double check when using dynamic crypto maps.
crypto map map-name seq-number
Example:
Router(config)# crypto map vpn1 10
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gt_crpks.h tm

D is incorrect because the dynamic crypto map is not misconfigured http://www.cisc.com/univercd/cc/td/doc/ product/iaabu/csvpnc/csvpnsg/icike.htm

E is correct because the ACL is not applied to an interface

QUESTION 172
DRAG DROP

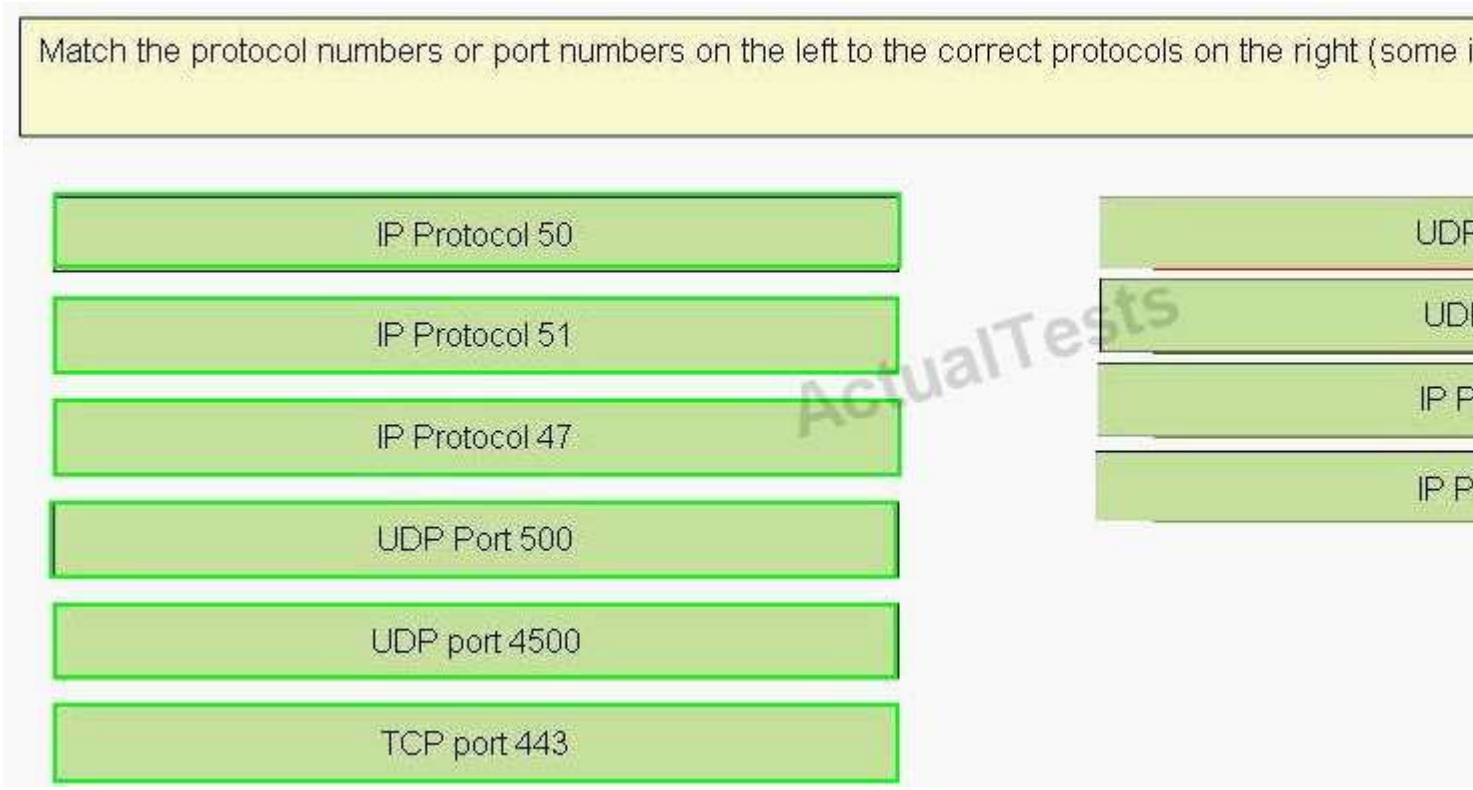
Drop



A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:



Explanation:

QUESTION 173
With the following GRE tunnel configuration, how many bytes of GRE overhead does encapsulation add to the original data packet?

```
interface Tunnel0
ip address 1.1.1.1 255.255.255.252
tunnel source Ethernet0/0
tunnel destination 2.2.2.2
tunnel key 1234
```

A. 32 bytes
B. 24 bytes
C. 28 bytes
D. 20 bytes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 174
Referring to the debug output shown, which two statements are true? (Choose two.)

```
R1# debug ip ospf adj

23:48:06: OSPF: Interface OSPF_VL1 going Up
23:48:06: OSPF: Send with youngest Key 0
23:48:07: OSPF: Build router LSA for area 0, router ID 3.3.3.3, seq 0x80000001
23:48:07: OSPF: Build router LSA for area 2, router ID 3.3.3.3, seq 0x80000033
23:48:07: OSPF: Build router LSA for area 1, router ID 3.3.3.3, seq 0x80000030
23:48:14: OSPF: 2 Way Communication to 1.1.1.1 on OSPF_VL1, state 2WAY
23:48:14: OSPF: Send DBD to 1.1.1.1 on OSPF_VL1 seq 0x1EA opt 0x62 flag 0x7 len32
23:48:14: OSPF: Send with youngest Key 1
23:48:14: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x3FB opt 0x62 flag 0x7 len 32 mtu 0 state EXSTART
23:48:14: OSPF: First DBD and we are not SLAVE 23:48:16: OSPF: Send with youngest Key 1
23:48:19: OSPF: Send DBD to 1.1.1.1 on OSPF_VL1 seq 0x1EA opt 0x62 flag 0x7 len 32
23:48:19: OSPF: Send with youngest Key 1 23:48:19: OSPF: Retransmitting DBD to 1.1.1.1 on OSPF_VL1 [1]
23:48:19: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x3FB opt 0x62 flag 0x7 len 32 mtu 0 state EXSTART 2
3:48:19: OSPF: First DBD and we are not SLAVE
23:48:19: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x1EA opt 0x62 flag 0x2 len 172 mtu 0 state EXSTART
23:48:19: OSPF: NBR Negotiation Done. We are the MASTER
23:48:19: OSPF: Send DBD to 1.1.1.1 on OSPF_VL1 seq 0x1EB opt 0x62 flag 0x3 len 112
23:48:19: OSPF: Send with youngest Key 1
23:48:19: OSPF: Send with youngest Key 1
23:48:19: OSPF: Database request to 1.1.1.1
23:48:19: OSPF: sent LS REQ packet to 5.0.0.1, length 48
23:48:19: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x1EB opt 0x62 flag 0x0 len 32 mtu 0 state EXCHANGE
23:48:19: OSPF: Send DBD to 1.1.1.1 on OSPF_VL1 seq 0x1EC opt 0x62 flag 0x1 len 32
23:48:19: OSPF: Send with youngest Key 1
23:48:19: OSPF: Build router LSA for area 0, router ID 3.3.3.3, seq 0x80000030
23:48:19: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x1EC opt 0x62 flag 0x0 len 32 mtu 0 state EXCHANGE
23:48:19: OSPF: Exchange Done with 1.1.1.1 on OSPF_VL1
23:48:19: OSPF: Synchronized with 1.1.1.1 on OSPF_VL1, state FULL
23:48:19: %OSPF-5-ADJCHG: Process 2, Nbr 1.1.1.1 on OSPF_VL1 from LOADING to FULL, Loading Done
```

A. The OSPF neighbors are using MD5 Authentication
B. Both R1 (local) router and the remote OSPF neighbor are not directly connected to Area 0
C. The R1 (local) router is the DR
D. The OSPF neighbors are establishing a virtual link
E. The remote OSPF neighbor has an OSPF Router ID of 3.3.3.3

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation: Explanation
debug ospf flood
To display information about flood events such as acknowledgments and updates received, use the debug ospf flood command in EXEC mode. To disable debugging output, use the no form of this command.
debug ospf instance-name flood [access-list-name]
no debug ospf instance-name flood [access-list-name]

Syntax Description

instance-name	Name that uniquely identifies an OSPF routing process. The instance name is any alphanumeric string no longer than 40 characters. The instance name is defined by the router ospf command.
access-list-name	(Optional) Name of a particular access control list. The name cannot contain a space or quotation mark; it may contain numbers.

Defaults
Debugging is disabled.
Command Modes
EXEC
Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the Configuring AAA Services on Cisco IOS XR Software module of the Cisco IOS XR System Security Configuration Guide.
Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to Using Debug Commands on Cisco IOS XR Software. Use the debug ospf flood command to display messages containing information related to flood events.

91

The debug ospf flood command generates a substantial amount of output. Use the command only when traffic on the IP network is low so that other activity on the system is not adversely affected.

Task ID

Task ID	Operations
ospf	read, write

Examples
The following is sample output from the debug ospf flood command:

RP/0/RP0/CPU0:router# debug ospf 1 flood
RP/0/RP0/CPU0:33:19: ospf[239]: Rcv Update Type 2, LSID 192.168.20.207, Adv rtr 192.168.20.207, age 764, seq 0x80000001
RP/0/RP0/CPU0:33:19: ospf[239]: Mask 255.255.255.0
RP/0/RP0/CPU0:33:19: ospf[239]: %ROUTING-OSPF-5-ADJCHG : Process 1, Nbr 192.168.20.207 on GigabitEthernet0/2/0/0 from LOADING to FULL, Loading Done RP/0/RP0/CPU0:33:19: ospf[239]: Sending update on GigabitEthernet0/2/0/0 to 192.168.20.207 Area 0
RP/0/RP0/CPU0:33:19: ospf[239]: Send Type 1, LSID 1.1.1.1, Adv rtr 1.1.1.1, age 40, seq 0x80000001 (0)
RP/0/RP0/CPU0:33:19: ospf[239]: Inc retrans unit nbr count index 1 (0/1) to 1/1 RP/0/RP0/CPU0:33:19: ospf

[239]: Set Nbr 192.168.20.207 1 first flood info from 0 (0) to 0x81e1994 (18)
RP/0/RP0/CPU0:33:19: ospf[239]: Init Nbr 192.168.20.207 1 next flood info to 0x81e1994 RP/0/RP0/
CPU0:33:19: ospf[239]: Add Type 1 LSA ID 1.1.1.1 Adv rtr 1.1.1.1 Seq 80000002 to GigabitEthernet0/2/0/0
192.168.20.207 retransmission list RP/0/RP0/CPU0:33:19: ospf[239]: Start GigabitEthernet0/2/0/0
192.168.20.207 retrans timer RP/0/RP0/CPU0:33:19: ospf[239]: Set idb next flood info from 0 (0) to 0x81e1994
(18) RP/0/RP0/CPU0:33:19: ospf[239]: Add Type 1 LSA ID 1.1.1.1 Adv rtr 1.1.1.1 Seq 80000002 to
GigabitEthernet0/2/0/0 flood list
RP/0/RP0/CPU0:33:19: ospf[239]: Start GigabitEthernet0/2/0/0 pacing timer for 0.000001 msec
RP/0/RP0/CPU0:33:19: ospf[239]: Flooding update on GigabitEthernet0/2/0/0 to 224.0.0.5 Area 0
RP/0/RP0/CPU0:33:19: ospf[239]: Send Type 1, LSID 1.1.1.1, Adv rtr 1.1.1.1, age 1, seq

0x80000002 (0)
RP/0/RP0/CPU0:33:19: ospf[239]: Create retrans unit 0x81e0178/0x81df818 1 (0/1) 1 RP/0/RP0/CPU0:33:19:
ospf[239]: Set nbr 1 (0/1) retrans to 4976 count to 1 RP/0/RP0/CPU0:33:19: ospf[239]: Set idb next flood info
from 0x81e1994 (18) to 0 (0) RP/0/RP0/CPU0:33:19: ospf[239]: Remove Type 1 LSA ID 1.1.1.1 Adv rtr 1.1.1.1
Seq 80000002 from GigabitEthernet0/2/0/0 flood list
RP/0/RP0/CPU0:33:19: ospf[239]: Stop GigabitEthernet0/2/0/0 flood timer RP/0/RP0/CPU0:33:21: ospf[239]:
Sending delayed ACK on GigabitEthernet0/2/0/0 RP/0/RP0/CPU0:33:21: ospf[239]: Ack Type 1, LSID
192.168.20.207, Adv rtr 192.168.20.207, age 764, seq 0x80000003
RP/0/RP0/CPU0:33:21: ospf[239]: Ack Type 2, LSID 192.168.20.207, Adv rtr 192.168.20.207, age 764, seq
0x80000001
RP/0/RP0/CPU0:33:21: ospf[239]: Received ACK from 192.168.20.207 on GigabitEthernet0/2/0/0 RP/0/RP0/
CPU0:33:21: ospf[239]: Rcv Ack Type 1, LSID 1.1.1.1, Adv rtr 1.1.1.1, age 40, seq 0x80000001
RP/0/RP0/CPU0:33:24: ospf[239]: Retransmitting update on GigabitEthernet0/2/0/0 to 192.168.20.207 Area 0

QUESTION 175
Which Cisco technology protects against Spanning Tree Protocol manipulation?

A. Spanning tree protect.
B. MAC spoof guard.
C. Root Guard and BPDU Guard.
D. Port Security.
E. Unicast Reverse Path Forwarding

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Explanation
Network Security at the Data Link Layer (Layer 2) of LAN Every layer of communication has its own unique security challenges. The data link layer (layer 2) communication is a weak link in terms of security. Network security should be addressed at multiple layers to for different vulnerabilities. In this article, we focus on the security issues related to wired local area networks. Wireless LAN and the securities issues for wide area networks (WAN) are discussed in separate articles. Switches are key components at the layer 2 communications and they are also used for layer 3 communications. They are susceptible to many of the same Layer 3 attacks as routers, as well as many unique network attacks, which include:
· Content-Addressable Memory (CAM) table overflow: The CAM table in a switch contains information such as the MAC addresses available on a given physical port of a switch, as well as the associated VLAN parameters. CAM tables are limited in size. Typically a network intruder will flood the switch with a large number of invalid-source MAC addresses until the CAM table fills up. When that occurs the switch will flood all ports with incoming traffic because it cannot find the port number for a particular MAC address in the CAM table. CAM table overflow only floods traffic within the local VLAN so the intruder will see only traffic within the local VLAN to which he or she is connected.
· VLAN hopping: VLAN hopping is a network attack whereby an end system sends out packets destined for a system on a different VLAN that cannot normally be reached by the end system. This traffic is tagged with a

different VLAN ID to which the end system belongs. Or, the attacking system may be trying to behave like a switch and negotiate trunking so that the attacker can send and receive traffic between other VLANs.
· Spanning-Tree Protocol manipulation: Spanning-Tree Protocol is used in switched networks to prevent the creation of bridging loops in an Ethernet network topology. By attacking the Spanning- Tree Protocol, the network attacker hopes to spoof his or her system as the root bridge in the topology. To do this the network attacker broadcasts out Spanning-Tree Protocol Configuration/Topology Change Bridge Protocol Data Units (BPDUs) in an attempt to force spanning-tree recalculations. The BPDUs sent out by the network attacker's system announce that the attacking system has a lower bridge priority. If successful, the network attacker can see a variety of frames.
· Media Access Control (MAC) Address spoofing: MAC spoofing attacks involve the use of a known MAC address of another host to attempt to make the target switch forward frames destined for the remote host to the network attacker. By sending a single frame with the other host's source Ethernet address, the network attacker overwrites the CAM table entry so that the switch forwards packets destined for the host to the network attacker. Until the host sends traffic it will not receive any traffic. When the host sends out traffic, the CAM table entry is rewritten once more so that it moves back to the original port.
· Address Resolution Protocol (ARP) attack: ARP is used to map IP addressing to MAC addresses in a local area network segment where hosts of the same subnet reside. ARP attack happens when someone is trying to change the ARP table of MAC and IP addresses information without authorization. By doing so, hackers can spoof his/her MAC or IP address to launch the following two types of attacks: Denial of Service and Man-In-The-Middle attacks. · Private VLAN: Private VLANs work by limiting the ports within a VLAN that can communicate with other ports in the same VLAN. Isolated ports within a VLAN can communicate only with promiscuous ports. Community ports can communicate only with other members of the same community and promiscuous ports. Promiscuous ports can communicate with any port. One network attack capable of bypassing the network security of private VLANs involves the use of a proxy to bypass access restrictions to a private VLAN. · DHCP starvation: A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. This is easily achieved with attack tools such as gobbler. If enough requests are sent, the network attacker can exhaust the address space available to the DHCP servers for a period of time. This is a simple resource starvation attack just like a SYN flood. The network attacker can then set up a rogue DHCP server on his or her system and respond to new DHCP requests from clients on the network.
Mitigations of LAN Security Risks
The CAM table-overflow attack can be mitigated by configuring port security on the switch. This option provides for either the specification of the MAC addresses on a particular switch port or the specification of the number of MAC addresses that can be learned by a switch port. When an invalid MAC address is detected on the port, the switch can either block the offending MAC address or shut down the port.
Mitigating VLAN hopping attacks requires several modifications to the VLAN configuration. One of the more important elements is to use dedicated VLAN IDs for all trunk ports. Also, disable all unused switch ports and place them in an unused VLAN. Set all user ports to nontrunking mode by explicitly turning off DTP on those ports.
To mitigate Spanning-Tree Protocol manipulation use the root guard and the BPDU guard enhancement commands to enforce the placement of the root bridge in the network as well as enforce the Spanning-Tree Protocol domain borders. The root guard feature is designed to provide a way to enforce the root-bridge placement in the network. The Spanning-Tree Protocol BPDU guard is designed to allow network designers to keep the active network topology predictable. While BPDU guard may seem unnecessary given that the administrator can set the bridge priority to zero, there is still no guarantee that it will be elected as the root bridge because there might be a bridge with priority zero and a lower bridge ID. BPDU guard is best deployed towards user-facing ports to prevent rogue switch network extensions by an attacker.
Use the port security commands to mitigate MAC-spoofing attacks. The port security command provides the capability to specify the MAC address of the system connected to a particular port. The command also provides the ability to specify an action to take if a port-security violation occurs. However, as with the CAM table-overflow attack mitigation, specifying a MAC address on every port is an unmanageable solution. Hold-down timers in the interface configuration menu can be used to mitigate ARP spoofing attacks by setting the length of time an entry will stay in the ARP cache.
Configure access control lists (ACLs) on the router port to mitigate private VLAN attacks. Virtual ACLs can also be used to help mitigate the effects of private VLAN attacks. The techniques that mitigate CAM table flooding also mitigate DHCP starvation by limiting the number of MAC addresses on a switch port. As implementation of RFC 3118, Authentication for DHCP Messages, DHCP starvation attacks will become more difficult. In addition, IEEE 802.1X, a standard for passing the Extensible Authentication Protocol (EAP) framework over a wired or wireless network , acts as a gatekeeper for basic network access at the data link layer. By denying access to the network before authentication is successful, 802.1X can prevent many attacks against network infrastructure that depend on having basic IP connectivity. Originally written to be used within the Point-to-Point

Protocol (PPP) of dial-up and remote access networks, 802.1x allows for EAP to be used within the context of LANs, including wireless LAN.

The network security measures at the data link layer are complementary to the network layer (IPsec) measures to provide extra protection of the network and users, especially in the case of wireless LAN. The following table gives feature comparison of the network security at the data link layer and network layer.

QUESTION 176
Which of the following is an example of a security technology that could be enabled by Netflow?

A. SYN Cookies
B. Content filtering
C. Anti-X Protection
D. Anomaly Detection
E. Anti Virus
F. Application Inspection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
NetFlow is an embedded instrumentation within Cisco IOS Software to characterize network operation. Visibility into the network is an indispensable tool for IT professionals. In response to new requirements and pressures, network operators are finding it critical to understand how the network is behaving including:
· Application and network usage
· Network productivity and utilization of network resources · The impact of changes to the network
· Network anomaly and security vulnerabilities
· Long term compliance issues

QUESTION 177
What new features were added to the PIX in version 7.0? (Choose 3)

A. WebVPN
B. Support for multiple virtual firewalls.
C. Transparent firewall
D. Rate-Limiting

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Release Highlights
ADVANCED FIREWALL SERVICES
· Deep inspection firewall services for HTTP, FTP, ESMTP, and more
· Instant messaging, peer-to-peer, and tunneling application blocking
· Cisco Modular Policy Framework with flow-based security policies
· Virtual firewall services
· Layer 2 transparent firewall
· 3G Mobile Wireless security services
ROBUST IPSEC VPN SERVICES

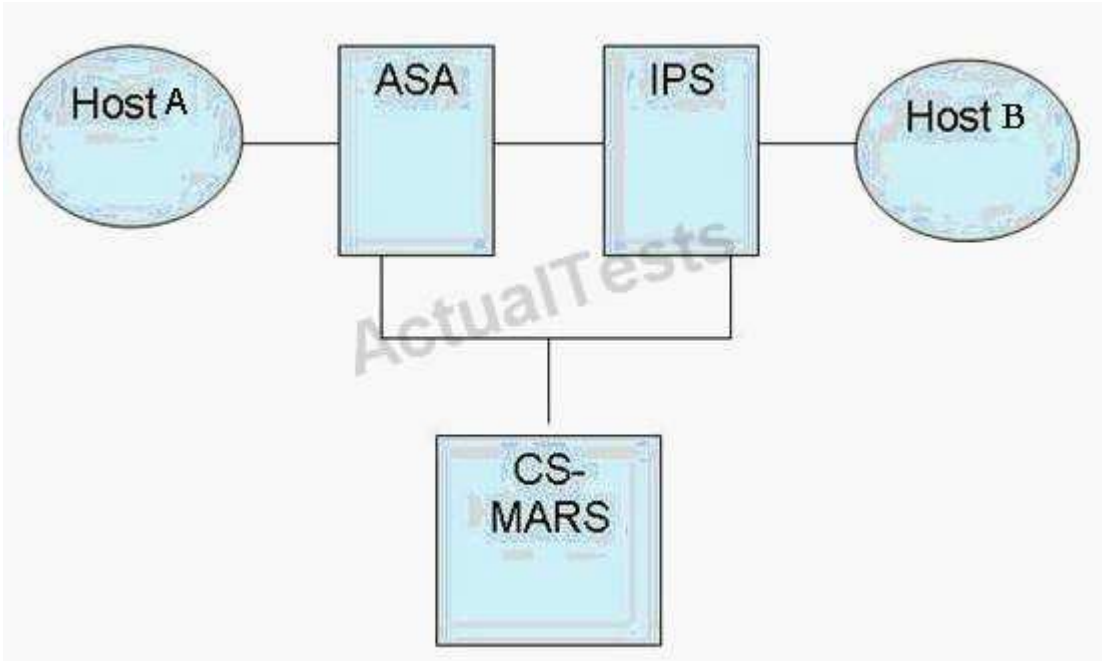
· VPN client security posture enforcement
· Automatic VPN client software updating
· OSPF dynamic routing over VPN tunnels
HIGH AVAILABILITY SERVICES
· Active/Active failover with asymmetric routing support · Remote-access and site-to-site VPN stateful failover · Zero-downtime software upgrades
INTELLIGENT NETWORK SERVICES
· PIM multicast routing
· Quality of service (QoS)
· IPv6 networking
FLEXIBLE MANAGEMENT SOLUTIONS
· SSHv2 and SNMPv2c
· Configuration rollback
· Usability enhancements

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet0900aecd80225ae 1.html

Rate-limiting is mention in version 7.0.4
http://www.cisco.com/en/US/docs/security/pix/pix70/release/notes/pix704rn.html#wp217692

The Web VPN client is not mention until verson 7.2
http://www.cisco.com/en/US/docs/security/pix/pix72/release/notes/pixrn72.html

QUESTION 178
In the example shown, Host A has attempted a D-COM attack using metasploit form Host A to Host B. Which answer best describes how event logs and IPS alerts can be used in conjunction with each other to determine if the attack was successful? (Choose 3)



A. The syslog connection built event will indicate that an attack is likely because a TCP syn and an ack followed the attempted attack.
B. The IPS event will suggest that an attack may have occurred because a signature was triggered.
C. CS-MARS will collect the syslog and the IPS alerts based on time.
D. ASA will see the attack in both directions and will be able to determine if an attack was successful.
E. IPS and ASA will use the Unified Threat Management protocol to determine that both devices saw the attack.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 179
What two things must you do on the router before generating an SSH key with the "crypto key generate rsa "IOS command ?

A. Configure the default IP domain name that the router will use
B. Enable SSH transport support on the vty lines
C. Configure the host name of the router
D. Enable AAA Authentication
E. Configure the SSH version that the router will use

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 180
Which AS-Path ACL is used to deny all the prefixes that originate in AS 65104 and permit all other prefixes?

A. ip as-path access-list 1 deny _65104_ ip as-path access-list 1 permit .* ip as-path access-list 1 deny _65104$ ip as-path access-list 1 permit .*
B. ip as-path access-list 1 deny ^65104$ ip as-path access-list 1 permit *
C. ip as-path access-list 1 deny $65104^ ip as-path access-list 1 permit any
D. ip as-path access-list 1 deny _65104_ ip as-path access-list 1 permit any
E. ip as-path access-list 1 deny _65104$ ip as-path access-list 1 permit ^$

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 181
Whenever a failover takes place on the ASA running in failover mode, all active connections are dropped and clients must re-establish their connections unless

A. the ASA is configured for Active-Active failover
B. the ASA is configured for LAN-Based failover
C. the ASA is configured to use a serial cable as the failover link
D. the ASA is configured for Active-Standby failover and a state failover link has been configured
E. the ASA is configured for Active-Active failover and a state failover link has been configured
F. the ASA is configured for Active-Standby failover

Correct Answer: DE

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 182
Select two statements that correctly describe the ESP protocol (Choose 2)

A. ESP can operate in either tunnel or transport mode
B. The following fields can be found in the ESP header, Security Parameters Index (SPI), Sequence number, crypto engine connection ID.
C. The complete ESP header is encrypted
D. ESP uses IP protocol 50
E. ESP can provide data confidentiality service, but it does not provide data origin authentication.To achieve data origin authentication, AH must be used.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 183
Which SSL protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment?

A. SSL Alert Protocol
B. SSL Change CipherSpec Protocol
C. SSL Record Protocol
D. SSL Handshake Protocol

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SSL Architecture
SSL is designed to make use of TCP to provide a reliable end-to-end secure service. SSL is not a single protocol but rather two layers of protocols.

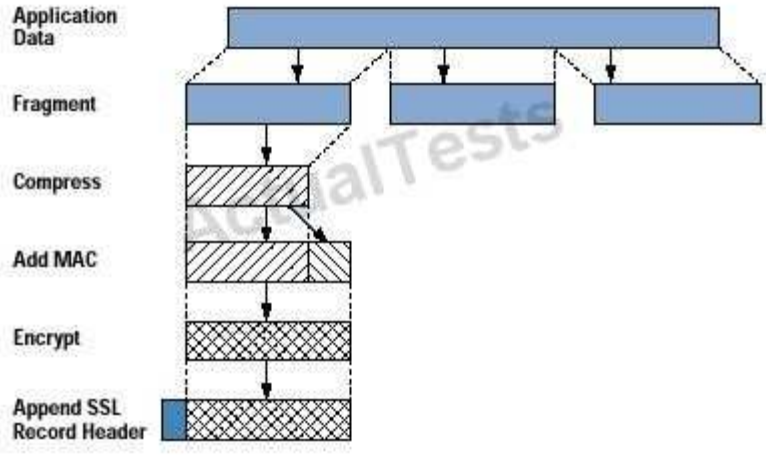
The SSL Record Protocol provides basic security services to various higher-layer protocols. In particular, the HTTP, which provides the transfer service for Web client/server interaction, can operate on top of SSL. Three higher-layer protocols are defined as part of SSL: the Handshake Protocol , the Change CipherSpec Protocol , and the Alert Protocol. These SSL-specific protocols are used in the management of SSL exchanges.

SSL Record Protocol
The SSL Record Protocol provides two services for SSL connections: confidentiality, by encrypting application data; and message integrity, by using a message authentication code (MAC). The Record Protocol is a base protocol that can be utilized by some of the upper-layer protocols of SSL. One of these is the handshake protocol which, as described later, is used to exchange the encryption and authentication keys. It is vital that this key exchange be invisible to anyone who may be watching this session.

Figure 1 indicates the overall operation of the SSL Record Protocol. The Record Protocol takes an application

message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment. Received data is decrypted, verified, decompressed, and reassembled and then delivered to the calling application, such as the browser.

Figure 1: SSL Record Protocol Operation



The first step is fragmentation. Each upper-layer message is fragmented into blocks of 2 14 bytes (16, 384 bytes) or less. Next, compression is optionally applied. In SLLv3 (as well as the current version of TLS), no compression algorithm is specified, so the default compression algorithm is null. However, specific implementations may include a compression algorithm.

The next step in processing is to compute a message authentication code over the compressed data. For this purpose, a shared secret key is used. In essence, the hash code (for example, MD5) is calculated over a combination of the message, a secret key, and some padding. The receiver performs the same calculation and compares the incoming MAC value with the value it computes. If the two values match, the receiver is assured that the message has not been altered in transit. An attacker would not be able to alter both the message and the MAC, because the attacker does not know the secret key needed to generate the MAC.

Next, the compressed message plus the MAC are encrypted using symmetric encryption. A variety

of encryption algorithms may be used, including the Data Encryption Standard (DES) and triple DES. The final step of SSL Record Protocol processing is to prepend a header, consisting of the following fields:
Content Type (8 bits): The higher-layer protocol used to process the enclosed fragment. Major Version (8 bits): Indicates major version of SSL in use. For SSLv3, the value is 3. Minor Version (8 bits): Indicates minor version in use. For SSLv3, the value is 0. Compressed Length (16 bits): The length in bytes of the plain-text fragment (or compressed fragment if compression is used).
The content types that have been defined are change_cipher_spec, alert, handshake, and application_data. The first three are the SSL-specific protocols, mentioned previously. The application-data type refers to the payload from any application that would normally use TCP but is now using SSL, which in turn uses TCP. In particular, the HTTP protocol that is used for Web transactions falls into the application-data category. A message from HTTP is passed down to SSL, which then wraps this message into an SSL record.

QUESTION 184
RFC 2827 ingress filtering is used to help prevent which type of attacks?

A. Land.C
B. Network Reconnaissance.
C. Syn Flood.

D. Tiny IP Fragments
E. Source IP address spoofing
F. Overlapping IP Fragments.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 185
Which three of these are important goals of NTP? (Choose three.)

A. accurate logging
B. time zone
C. validating certificates
D. routing updates
E. Kerberos tickets
F. clock

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 186
CS-MARS works with which IOS feature to accomplish anomaly detection?

A. CSA
B. Netflow
C. IOS Network Foundation Protection (NFP)
D. IOS IPS
E. IOS Firewall
F. Autosecure

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 187
Referring to the partial IOS configuration shown in the exhibit, which statements are true? (Choose three.)

```
!
interface Ethernet1
ip address 192.168.20.2 255.255.255.0
ip access-group 101 in
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.20.3
!
access-list 101 deny ip any any
```


A. Ethernet0 needs an outbound access-list to make the configuration work
B. ACL 101 needs to have at least one permit statement in it or it will not work properly
C. Ethernet0 needs an inbound access-list to make the configuration work
D. CBAC will create dynamic entries in ACL 101 to permit the return traffic
E. Ethernet0 is the trusted interface and Ethernet1 is the untrusted interface
F. All outbound ICMP traffic will be inspected by the IOS Firewall

Correct Answer: DEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 188
In an L2TP voluntary tunneling scenario, the VPDN tunnel is terminated between which of these elements?

A. The NAS and the LNS.
B. The client and the NAS.
C. The NAS and the LAC.
D. The client and the LNS.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 189
Which one of the following is NOT a supported IKE attribute?

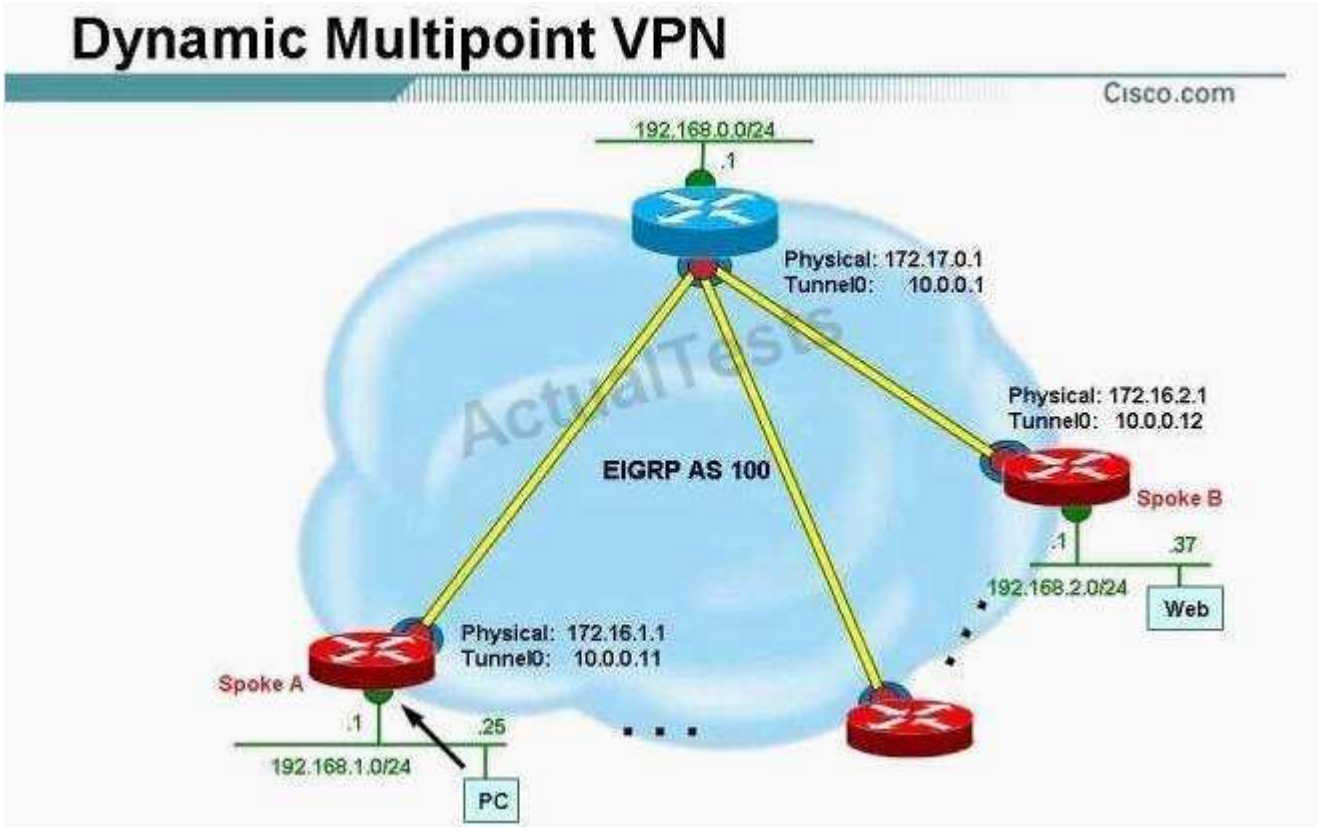
A. Hashing Algorithm

B. Authentication method.
C. Lifetime duration
D. Encryption algorithm
E. PFS group

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 190
Referring to the DMVPN topology diagram shown in the exhibit, which two statements are correct? (Choose two.)

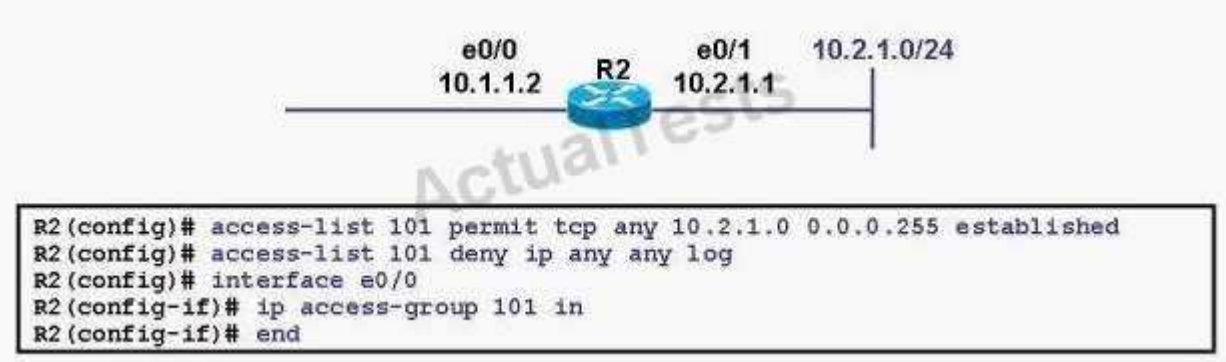


A. At the Spoke A router, the next-hop to reach the 192.168.0.0/24 network should be 172.17.0.1
B. Before a spoke-to-spoke tunnel can be built, the spoke router needs to send NHRP query to the hub to resolve the remote spoke router physical interface ip address
C. The spoke routers act as the NHRP servers for resolving the remote spoke physical interface ip address
D. At the Spoke A router, the next-hop to reach the 192.168.2.0/24 network should be 10.0.0.1
E. The hub router tunnel interface must have EIGRP next-hop-self enabled
F. The hub router needs to have EIGRP split horizon disabled

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 191
Referring to the network diagram and the partial router configuration shown, which packet will be permitted by ACL 101?



A. Any TCP packet with the ACK bit set destined to a host on the 10.2.1.0/24 subnet.
B. An ICMP echo-reply packet destined to a host on the 10.2.1.0/24 subnet
C. A HTTP packet with the SYN bit set destined to a host on the 10.2.1.0/24 subnet.
D. A TFTP packet with the RST bit set destined to a host on the 10.2.1.0/24 subnet.
E. Any TCP return traffic destined to a host on the 10.2.1.0/24 subnet that matches a corresponding outgoing TCP connection in the router's firewall state table.
F. Any TCP packets with the initial SYN or ACK bit set destined to a host on the 10.2.1.0/24 subnet.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 192
When enrolling a Cisco IOS router to a CA server using SCEP, which one of the following is not a required step?

A. Authenticate the CA server's certificate.
B. Configure an ip domain-name on the router
C. Generate the RSA key pairs on the router.
D. Import the server certificate to the router using TFTP.
E. Define the crypto pki trustpoint on the router.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 193
Which two steps does a receiver perform to validate a message using HMAC? (Choose two.)

A. look up the sender's public key.

B. compares the computed MAC vs. the MAC received.
C. decrypts the received MAC using a secret key.
D. authenticate the received message using the sender's public key.
E. extracts the MAC from the received message then encrypts the received message with a secret key to produce the MAC
F. Computes the MAC using the received message and a secret key as inputs to the hash function.

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 194
Figure 1 shows three security contexts sharing a common VLAN (VLAN 500). A single IP subnet corresponds to that VLAN. This is equivalent to connecting three security appliances using an Ethernet switch. A property of the FWSM makes all interfaces across the entire module use only one global MAC address ("M" in Figure 1). This is usually not a problem, until multiple contexts start sharing an interface. Which operational function within the FWSM handles this issue?

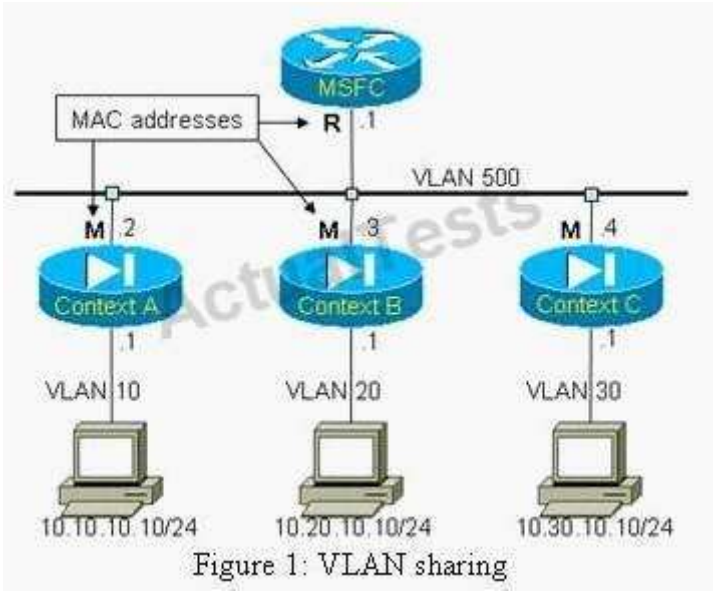


Figure 1: VLAN sharing

A. Session Manager
B. Classifier
C. Packetizer
107

D. Normalizer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 195

Which best represents a typical attack that takes advantage of RFC 792, ICMP Type 3 messages?

A. Broadcast-based echo request
B. Excessive bandwidth consumption
C. Blind connection-reset
D. Large packet echo request
E. Packet fragmentation offset

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

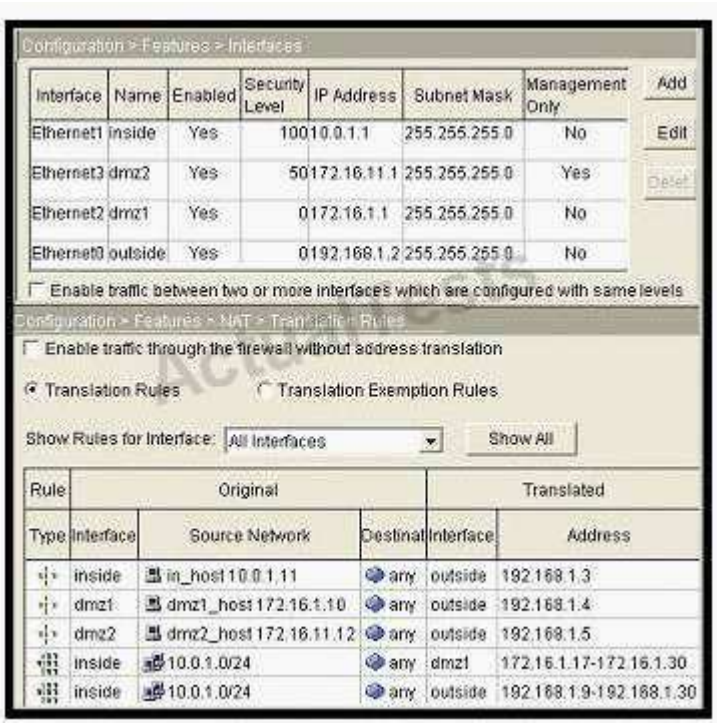
QUESTION 196
Which of the following statements describing the PPTP protocol is incorrect?

A. A single PPTP tunnel can carry multiple end-to-end ppp sessions
B. MPPE encryption to secure the tunnel is required for PPTP
C. The control session for PPTP runs over TCP port 1723
D. The data session uses a modified version of GRE as transport.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 197
An administrator is troubleshooting a new ASDM configured security appliance. A remote user is trying to establish a web session with the dmz1_host and the in_host from a PC on the outside network. The remote user is able to establish a FTP connection with the in_host successfully from the outside. However, they are unable to connect to the dmz1_host with an IP address of 192.168.1.4 from their outside PC. The administrator checked the access-lists and they were correct. The next step was to check the security appliance interfaces and NAT configuration screens. From information present on the ASDM screens, what appears to be the issue why the remote user can not create a web session with the dmz1_host?



A. With Nat-control disabled, the end user should target the real dmz1_host IP address.
B. If the remote user can not connect to dmz1_host using the 192.168.1.4, the administrator should check the remote user's PC configuration.
C. The administrator should enable Inter-interface routing.
D. The administrator should select "enable traffic through the firewall without address translation" checkbox.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Explanation
Configuring Inter-Interface Communication
Allowing communication between same security interfaces provides the following benefits:
You want protection features to be applied equally for traffic between two interfaces; for example, you have two departments that are equally secure.
For different security level interfaces, many protection features apply only in one direction, for example, inspection engines, TCP intercept, and connection limits. If you enable same security interface communication, you can still configure interfaces at different security levels as usual.

```
FWSM/contexta(config)# same-security-traffic permit inter-interface
```

QUESTION 198
When configuring a multipoint GRE tunnel interface, which one of the following is not a valid configuration option?

A. ip address
B. tunnel destination
C. tunnel key
D. tunnel source
E. tunnel vrf

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 199
A network administrator uses a LAN analyzer to troubleshoot OSPF router exchange messages sent to all OSPF routers. To which one of these MAC addresses are these messages sent?

A. 01-00-5E-00-00-05
B. 01-00-5E-EF-00-00
C. EF-FF-FF-00-00-05
D. EF-00-00-FF-FF-FF
E. 00-00-1C-EF-00-00
F. FF-FF-FF-FF-FF-FF

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 200
Using FTP passive mode, after the client opens the command channel (port 21) to the FTP server and requests passive mode, what will be the next step ?

A. The FTP server sends back an acknowledgment (ACK) to the client
B. The FTP server opens the data channel to the client using the port number indicated by the client
C. The FTP client opens the data channel to the FTP server on Port 21
D. The FTP server allocates a port to use for the data channel and transmit that port number to the client
E. The FTP client opens the data channel to the FTP server on Port 20

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 201
Which of the following is true about the Cisco IOS-IPS functionality? (Choose 2)

A. To activate new signatures you download a new Signature Defition File (SDF) from Cisco's web site
B. To update signatures you need to install a new IOS image.
C. The signatures available are built into the IOS code.
D. Cisco IOS only provides Intrusion Detection functionality.
E. Loading and enabling selected IPS signatures is user configurable.
F. Cisco IOS-IPS requires a network module installed in your router running sensor software.

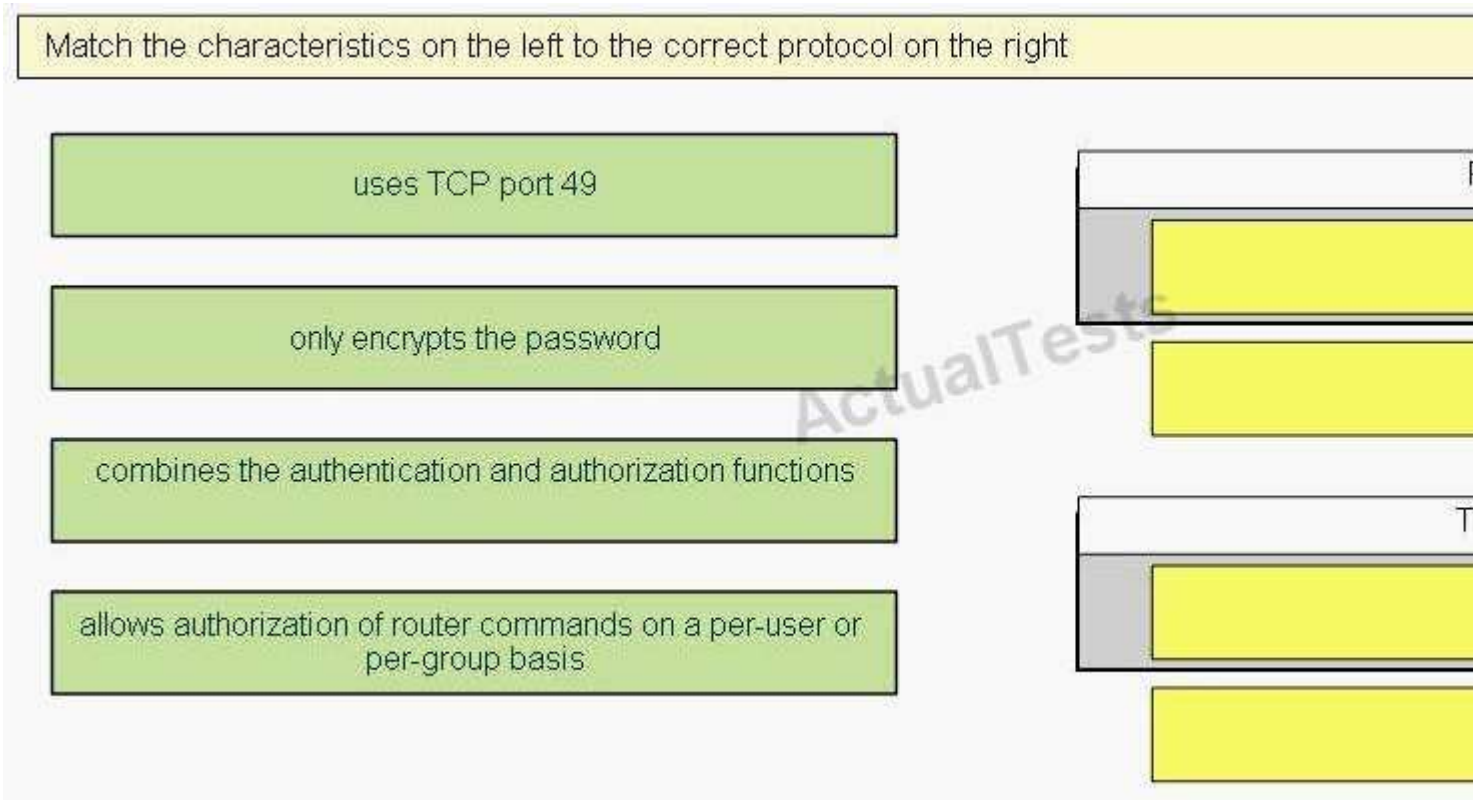
Correct Answer: AE
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 202
DRAG DROP

Drop

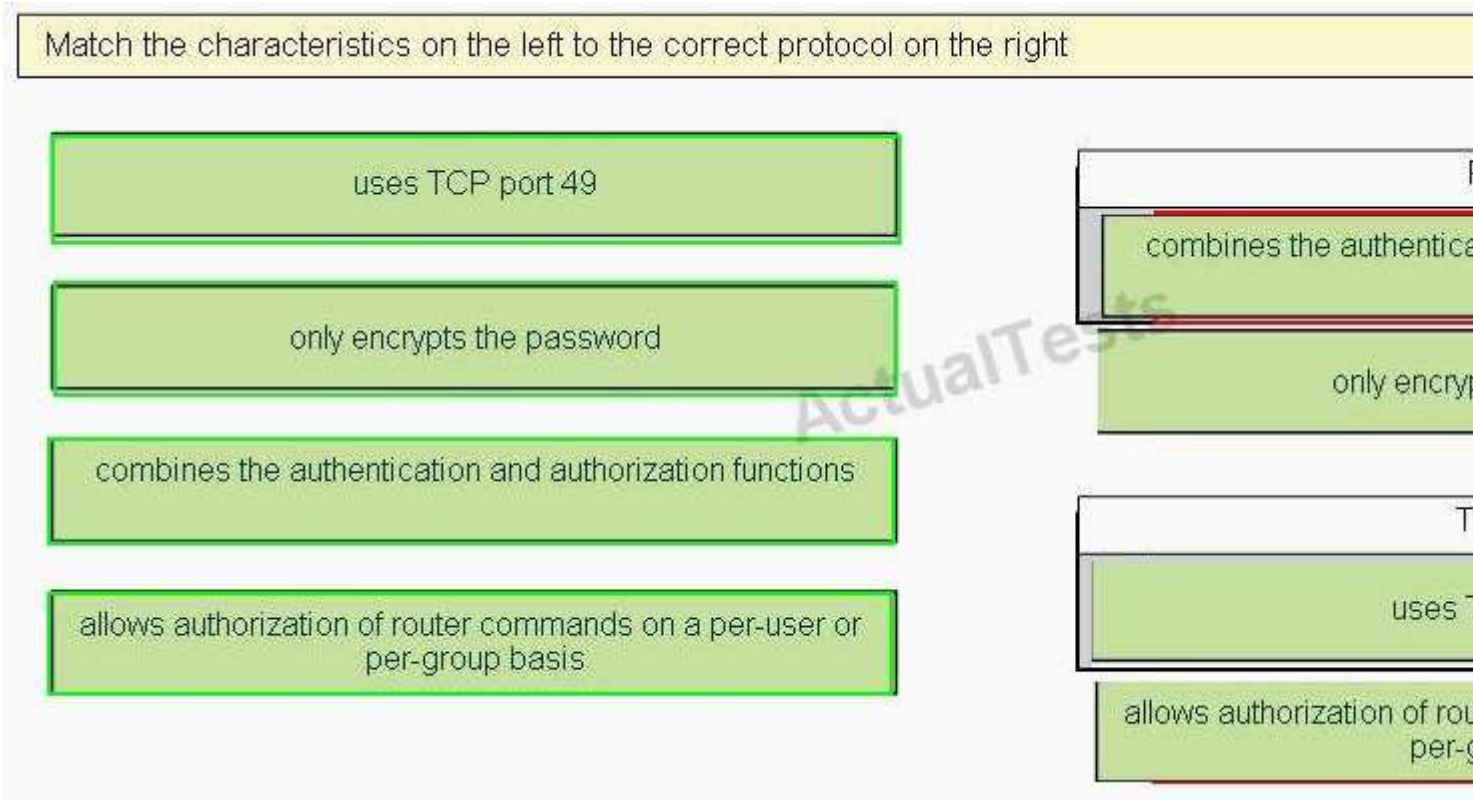


111

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:



Explanation:
RADIUS - combines the authentication and authorization functions, only encrpyts the passwordTACACS+ - uses TCP port 49, allows authorization of router commands on a per-user or per-group basis.Explanation:
RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, can be captured by a third party. RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization
TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. For debugging purposes, it is useful to have the body of the packets unencrypted. However, during normal operation, the body of the packet is fully encrypted for more secure communications. TACACS+ provides two methods to control the authorization of router commands on a per-user or per-group basis
Reference:
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml

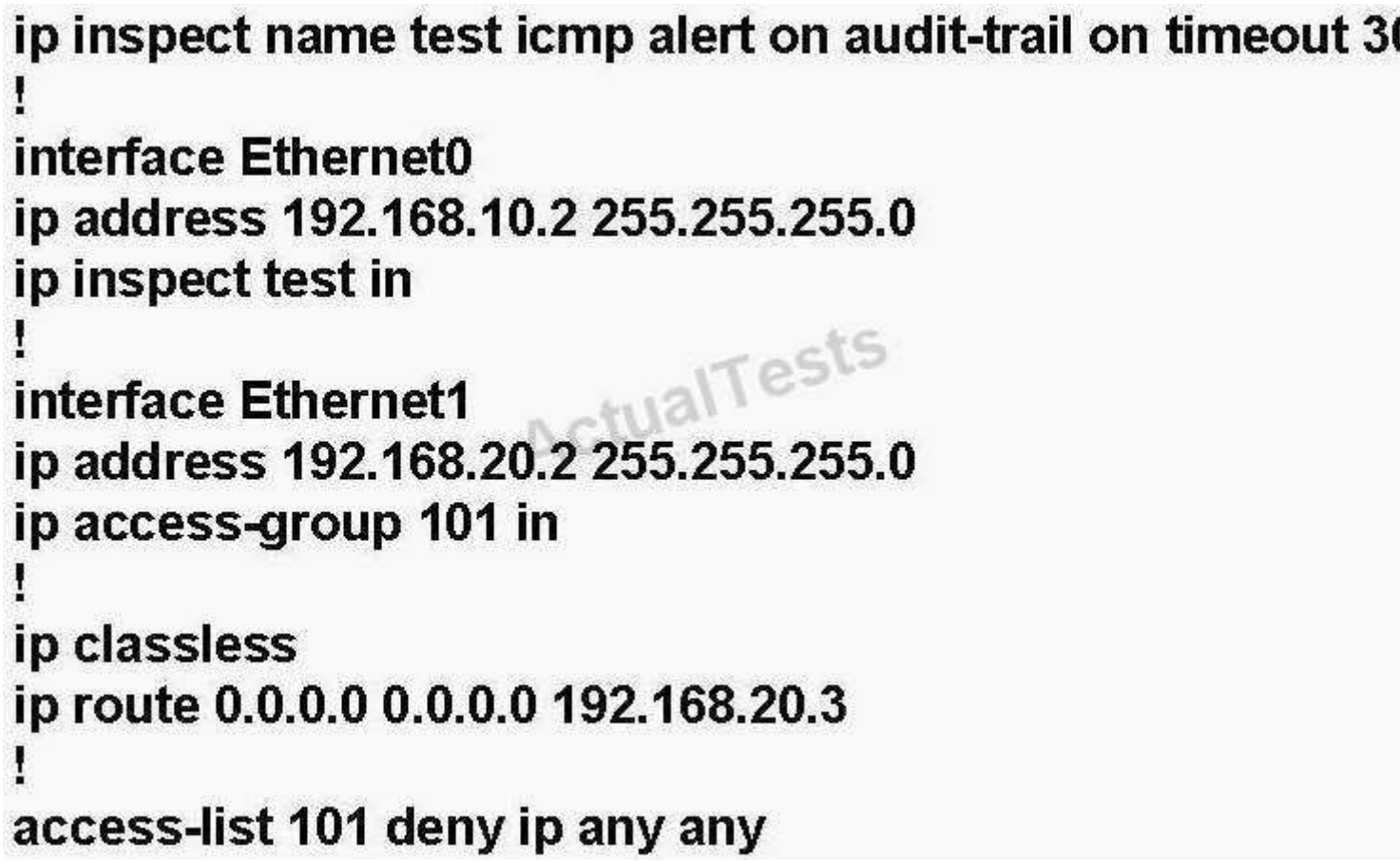
QUESTION 203
Which of the following is one way to configure the security appliance to protect against DoS attacks?

A. Using the emb_lim option in the acl command.
B. Using the tcp_max_conns option in the nat command
C. Using the emb_lim option in the static command.
D. Using the emb_conns argument in the global command.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 204
Referring to the partial IOS configuration shown in the exhibit, which two statements are true? (Choose three.)



A. All outbound ICMP traffic will be inspected by the IOS Firewall
B. Ethernet0 is the trusted interface and Ethernet1 is the untrusted interface
C. Ethernet0 needs an outbound access-list to make the configuration work
D. Ethernet0 needs an inbound access-list to make the configuration work
E. CBAC will create dynamic entries in ACL 101 to permit the return traffic
F. ACL 101 needs to have at least one permit statement in it or it will not work properly

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 205
When implementing best practices for IP source address spoofing and defeating denial of service attacks, which RFC is commonly used to protect your network?

A. RFC 2827
B. RFC 1918
C. RFC 1149

D. RFC 3704

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: Explanation
RFC 1149 - Standard for the transmission of IP datagrams on avian carriers http://www.faqs.org/rfcs/rfc1149.html
RFC 3704 - Ingress Filtering for Multihomed Networks
http://www.ietf.org/rfc/rfc3704.txt
RFC 1918 - Address Allocation for Private Internets
http://www.faqs.org/rfcs/rfc1918.html
RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
http://www.ietf.org/rfc/rfc2827.txt

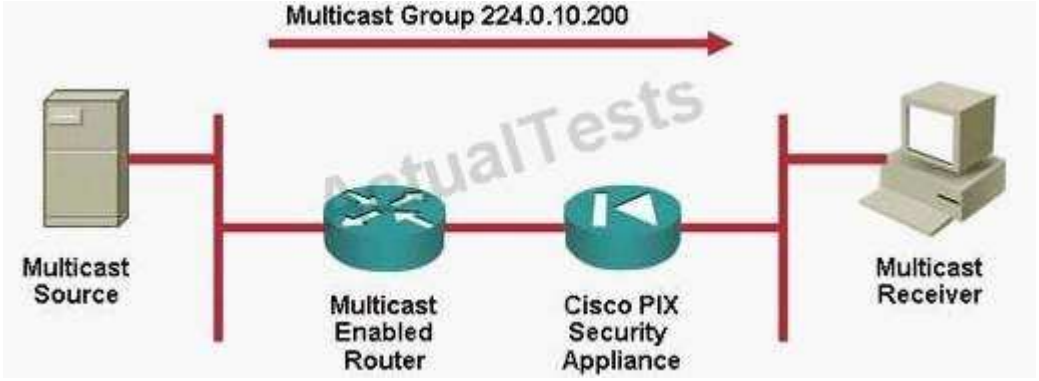
QUESTION 206
What are two important guidelines to follow when implementing VTP? (Choose 2)

A. CDP must be enabled on all switches in the VTP management domain
B. Enabling VTP pruning on a server will enable the feature for the entire management domain
C. All switches in the VTP domain must run the same version of VTP
D. Use of the VTP muti-domain feature should be restricted to migration and temporary implementation.
E. When using secure mode VTP, only configure management domain passwords on VTP servers.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 207
Refer to the Exhibit. A Cisco security appliance has been inserted between a multicast source and its receiver, preventing multicast traffic between them. What is the best solution to address this problem?



A. Create a static route on the multicast source and receiver pointing to the outside and inside interfaces of the security appliance respectively
B. Configure a GRE tunnel to allow the multicast traffic to bypass the security appliance
C. Configure SMR so the security appliance becomes an IGMP proxy agent, forwarding IGMP messages from hosts to the upstream multicast router

D. Configure the security appliance as an IGMP multicast client
E. Configure the security appliance as the rendezvous point of the multicast network so that (*, G) trees traverse it

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Explanation
A security appliance is nothing more than a Cisco PIX or an ASA.

A is wrong because

Multicast Support (IGMP v2 and Stub Multicast Routing) This release enables you to statically configure multicast routes or use an IGMP helper address for forwarding IGMP reports and leave announcements.
The following summarizes multicast support in this release:
· NAT and PAT can be performed on the multicast packet source addresses only. · IGMP packets for address groups within the 224.0.0.0-224.0.0.255 range are not forwarded because these addresses are reserved for protocol use. NAT is not performed on IGMP packets. When IGMP forwarding is configured, the adaptive security appliance forwards the IGMP packets (report and leave) with the IP address of the helper interface as the source IP address.
Multicast Support
PIM sparse mode was added to allow direct participation in the creation of a multicast tree using PIM-SM. This capability extends existing multicast support for IGMP forwarding and for Class D access control policies and ACLs. PIM-SM provides an alternative to transparent mode operation in multicast environments.

The pim commands and the multicast-routing command added support to the new functionality in addition to the show mrib EXEC command in this feature. For more information, see the "Configuring Multicast Routing" section in the Cisco Security Appliance Command Line Configuration Guide.
For a complete description of the command syntax, see the Cisco Security Appliance Command Reference.
http://www.cisco.com/en/US/docs/security/asa/asa70/release/notes/asa_rn.html#wp208194 B is incorrect because of the following:
As explained in the PIX documentation, the PIX Firewall does not pass multicast packets, even though many routing protocols use multicast packets to transmit their data. Cisco considers it inherently dangerous to send routing protocols across the PIX Firewall. If the routes on the unprotected interface are corrupted, the routes transmitted to the protected side of the firewall pollute routers there as well.

Note: At this time, you cannot terminate GRE tunnels on the PIX. In order to terminate a GRE tunnel, you need a virtual tunnel interface. At this time, however, PIX version 7.0 only supports physical and logicalinterfaces.

http://www.cisco.com/warp/public/707/tunnel_pix.pdf

C is incorrect because of the following:
Configuring a Static Rendezvous Point Address
All routers within a common PIM sparse mode or bidir domain require knowledge of the PIM RP address. The address is statically configured using the pim rp-address command. The security appliance does not support Auto-RP or PIM BSR; you must use the pim rp-address command to specify the RP address.
Answer D is incorrect because
Configuring a Static Multicast Route
When using PIM, the security appliance expects to receive packets on the same interface where it sends unicast packets back to the source. In some cases, such as bypassing a route that does not support multicast routing, you may want unicast packets to take one path and multicast packets to take another.
Static multicast routes are not advertised or redistributed. To configure a static multicast route for PIM, enter the following command:
hostname(config)# mroute src_ip src_mask {input_if_name | rpf_addr) [distance]

To configure a static multicast route for a stub area, enter the following command:
hostname(config)# mroute src_ip src_mask input_if_name [dense output_if_name] [distance]

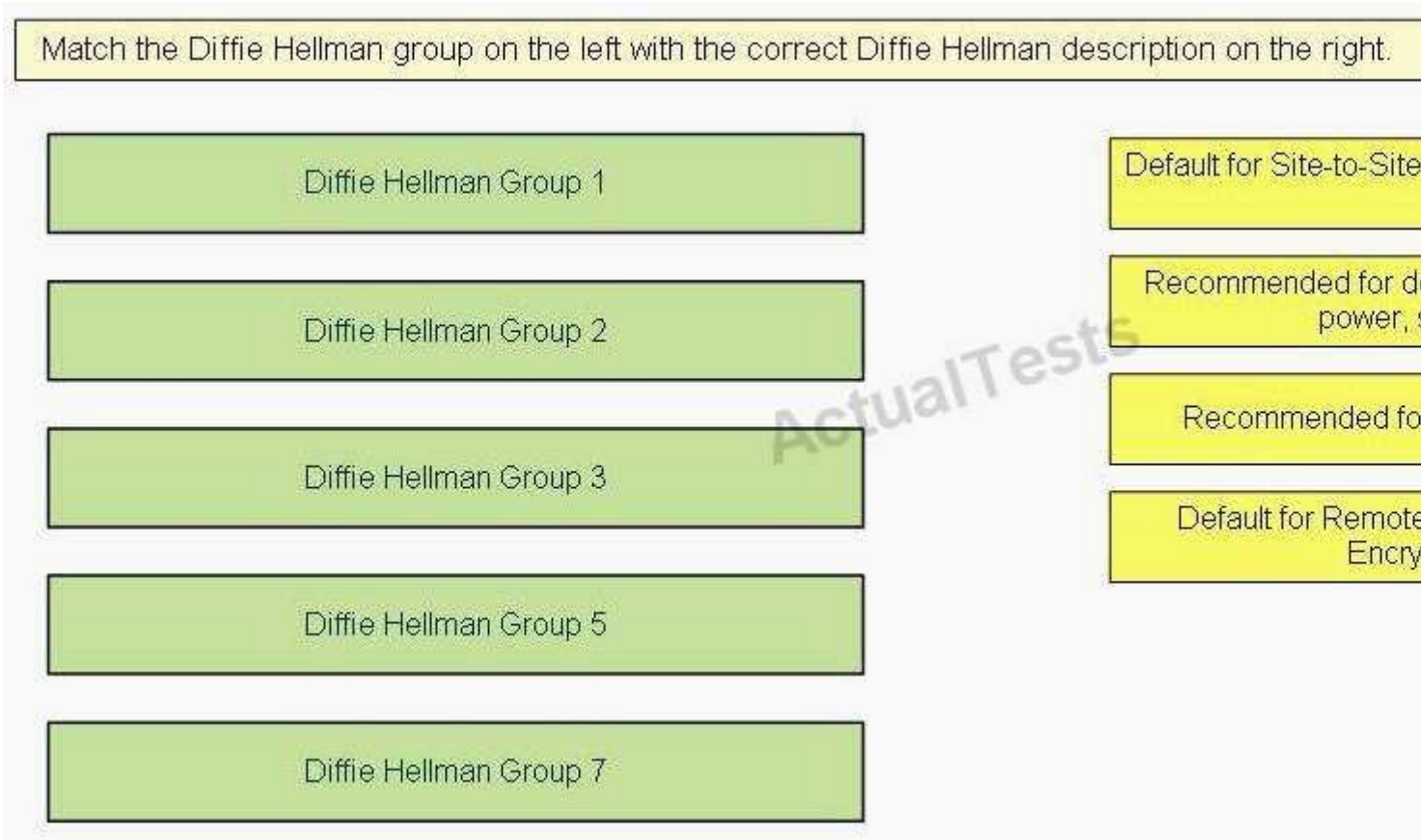
The dense output_if_name keyword and argument pair is only supported for stub multicast routing.

116

Answer E more information
For More Information about Multicast Routing
The following RFCs from the IETF provide technical details about the IGMP and multicast routing standards used for implementing the SMR feature:
· RFC 2236 IGMPv2
· RFC 2362 PIM-SM
· RFC 2588 IP Multicast and Firewalls
· RFC 2113 IP Router Alert Option
· IETF draft-ietf-idmr-igmp-proxy-01.txt

QUESTION 208
DRAG DROP

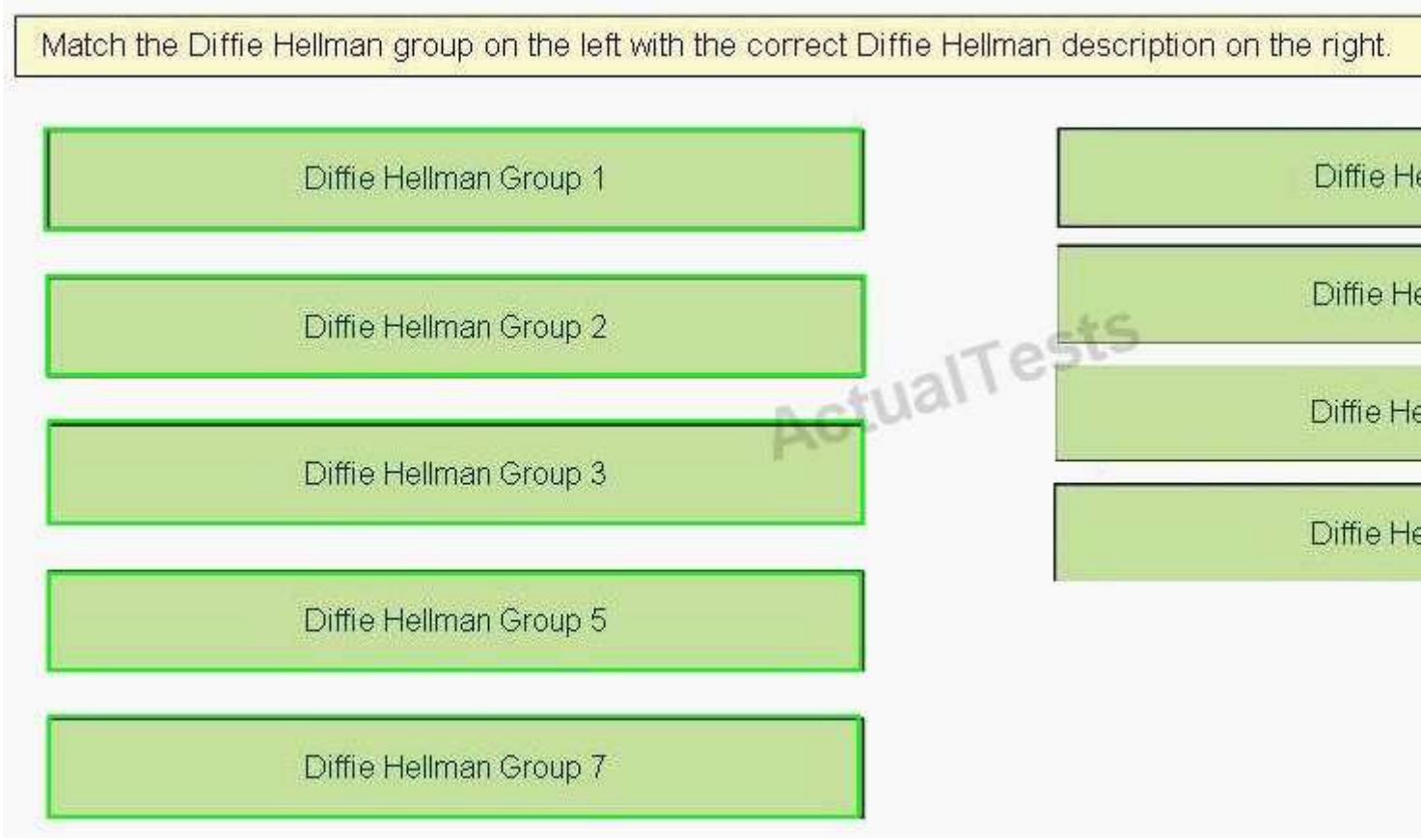
Drop



A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

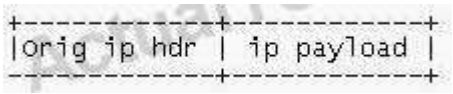
Explanation/Reference:

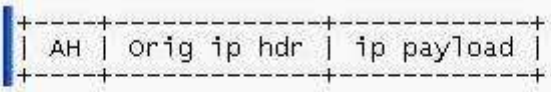


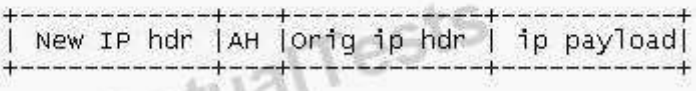
Explanation:

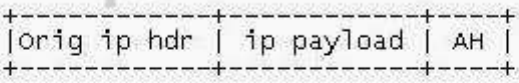
117

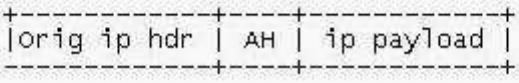
QUESTION 209
Assuming the shown data packet is to be protected by AH (Authentication Header) in transport mode, which of the following correctly describes the packet structure after AH is applied?



A.


B.


C.


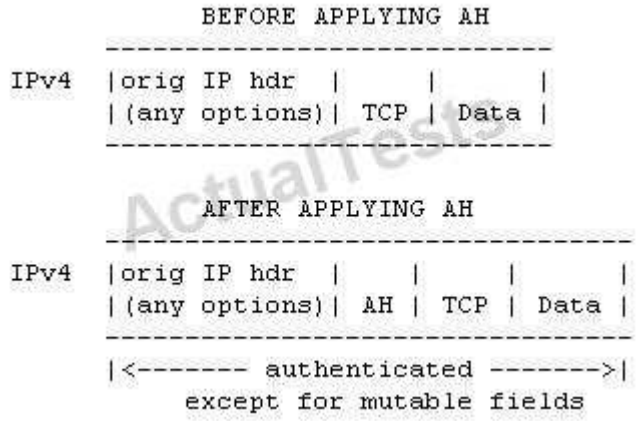
D.


A. Option A
B. Option B
C. Option C
D. Option D

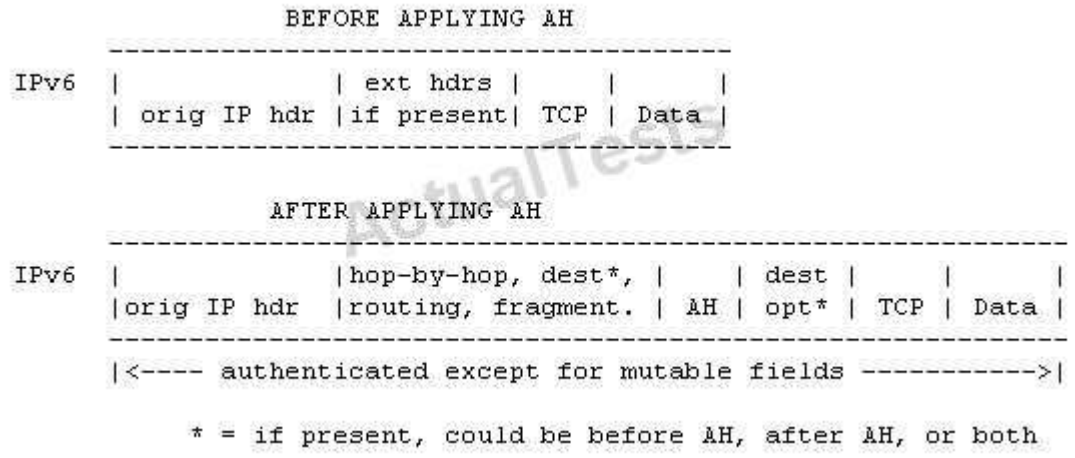
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Not B: The QUESTION NO: is about transport mode. In transport never a new IP hdr is put in front of the AH header.

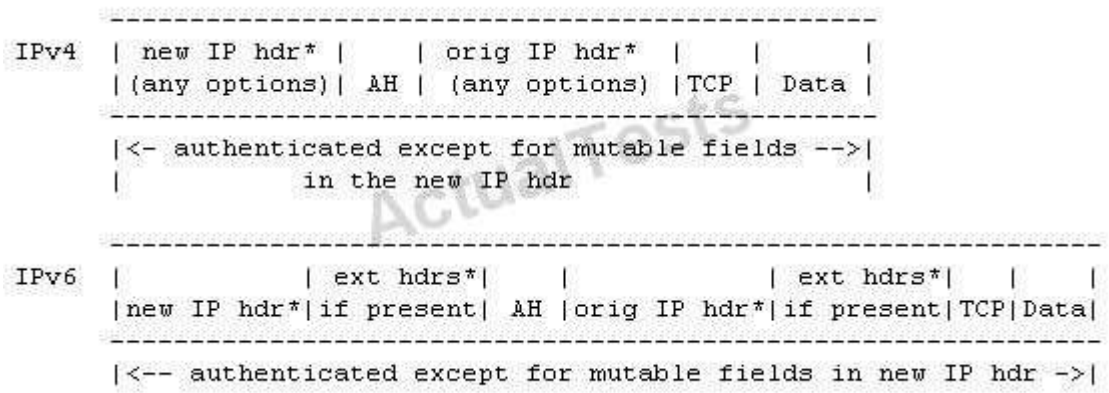
Note:
The following diagram illustrates AH transport mode positioning for a typical IPv4 packet, on a "before and after" basis.



The following diagram illustrates AH transport mode positioning for a typical IPv6 packet.



The following diagram illustrates AH tunnel mode positioning for typical IPv4 and IPv6 packets.

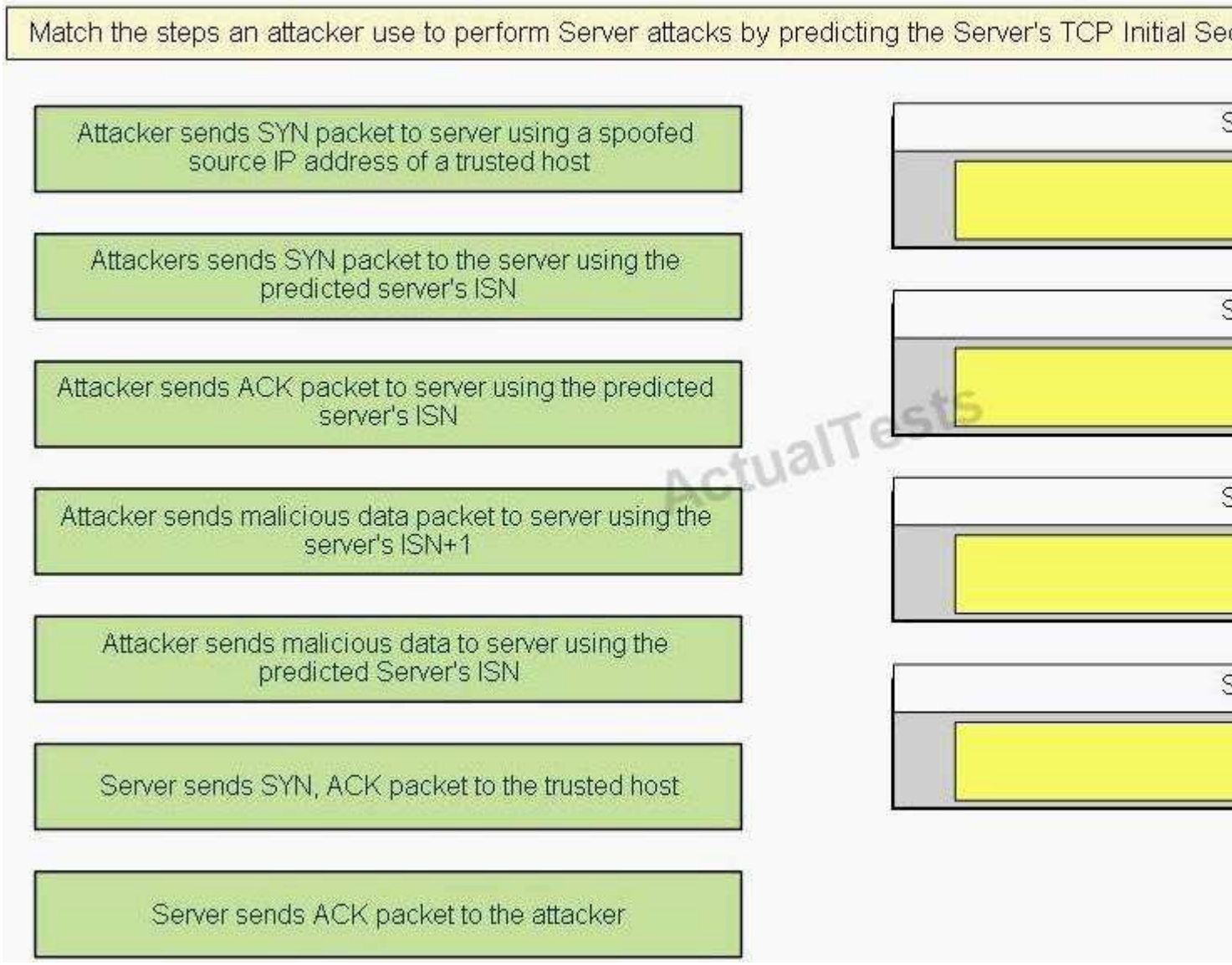


http://www.faqs.org/rfcs/rfc2402.html

See RFC 2402

QUESTION 210
DRAG DROP

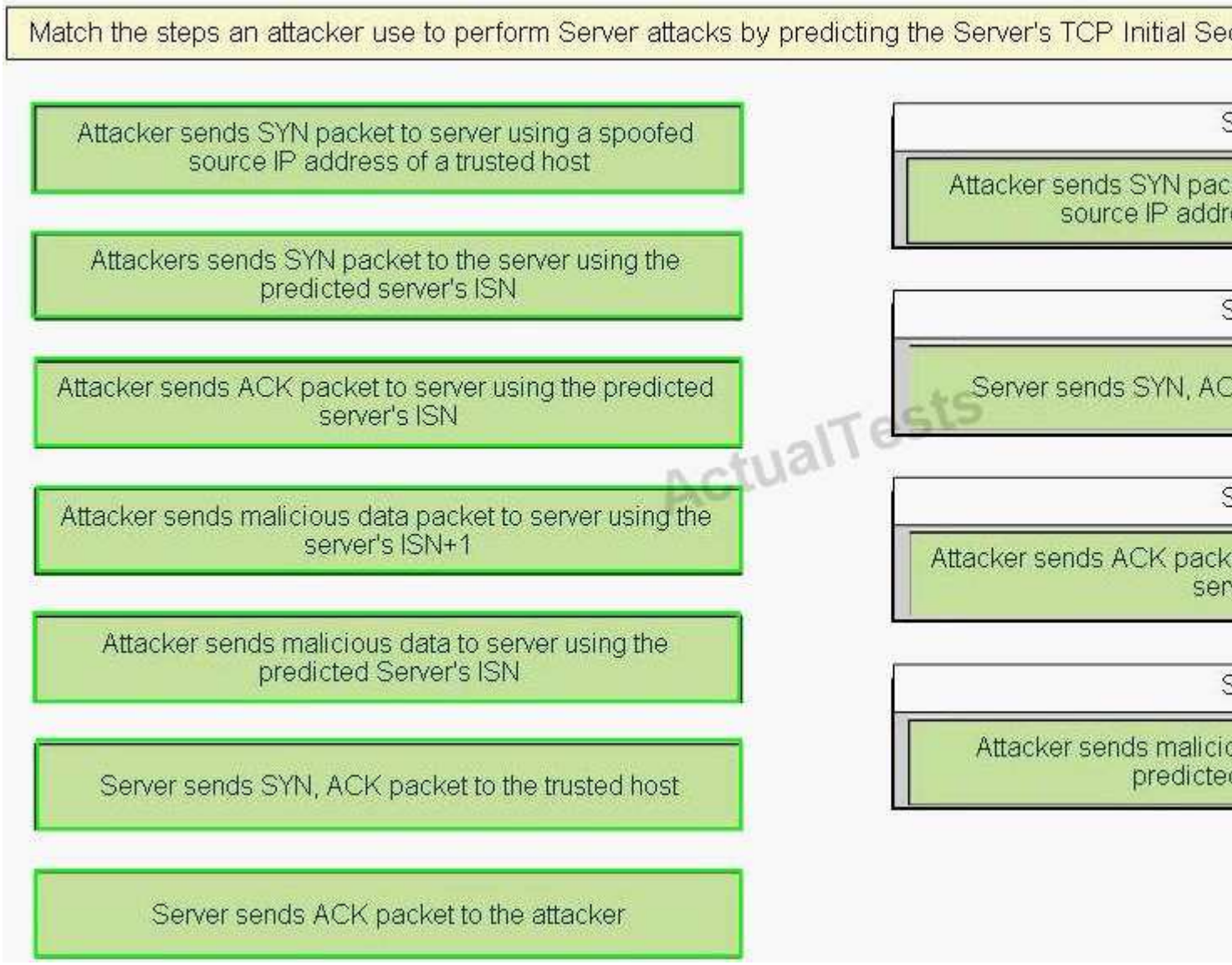
Drop



A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:



120

Explanation:

QUESTION 211
Which three technologies are included in anti-X? (Choose three.)

A. Intrusion Prevention
B. Content Caching
C. VPN
D. Virus and Phishing protection
E. Content and URL filtering

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 212
To increase security, MD5 authentication is added to an OSPF virtual link. Company security policies dictate that all passwords must be changed after 90 days. What will be the effect on the OSPF network of changing the MD5 key?

A. A second MD5-authenticated virtual link should be created. Once that is operational, the old virtual link can be removed.
B. Once a MD5 key is configured a hash is created. For security purposes, this hash can only be removed by clearing the MD5 configuration and resetting the OSPF adjacency.
C. A new MD5 key can be configured after removing the old one. This will momentarily disable MD5 authentication until the new key is learned in updated LSAs.
D. if a second MD5 key is configured OSPF will authenticated both keys allowing the first key to be removed with no effect on OSPF
E. if a new MD5 key is configured using the same key-id, it automatically replaces the existing one with no effect on OSPF

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 213
Which of the following are not steps in setting up a TLS session?

A. Client sends Hello to Server listing all of its supported cipher suites
B. Client calculates and sends encrypted pre_master_secret
C. Server sends-Hello to Client listing all of is supported cipher suites
D. Server sends Change Cipher Spec to indicate a shift to encrypted mode
E. Client and Server calculate keys from pre_master_secret

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Transport Layer Security (TLS) IETF RFC 4507 / RFC4507 These goals are achieved by the handshake protocol, which can be summarized as follows: The client sends a client hello message to which the server must respond with a server hello message, or else a fatal error will occur and the connection will fail. The client hello and server hello are used to establish security enhancement capabilities between client and server. The client hello and server hello establish the following attributes: Protocol Version, Session ID, Cipher Suite, and Compression Method. Additionally, two random values are generated and exchanged: ClientHello.random and ServerHello.random.
The client indicates that it supports this mechanism by including a SessionTicket TLS extension in the ClientHello message. The extension will be empty if the client does not already possess a ticket for the server. The extension is described in Section 3.2. If the server wants to use this mechanism, it stores its session state (such as ciphersuite and master secret) to a ticket that is encrypted and integrity-protected by a key known only to the server. The ticket is distributed to the client using the NewSessionTicket TLS handshake message described in Section 3.3. This message is sent during the TLS handshake before the ChangeCipherSpec message, after the server has successfully verified the client's Finished message.

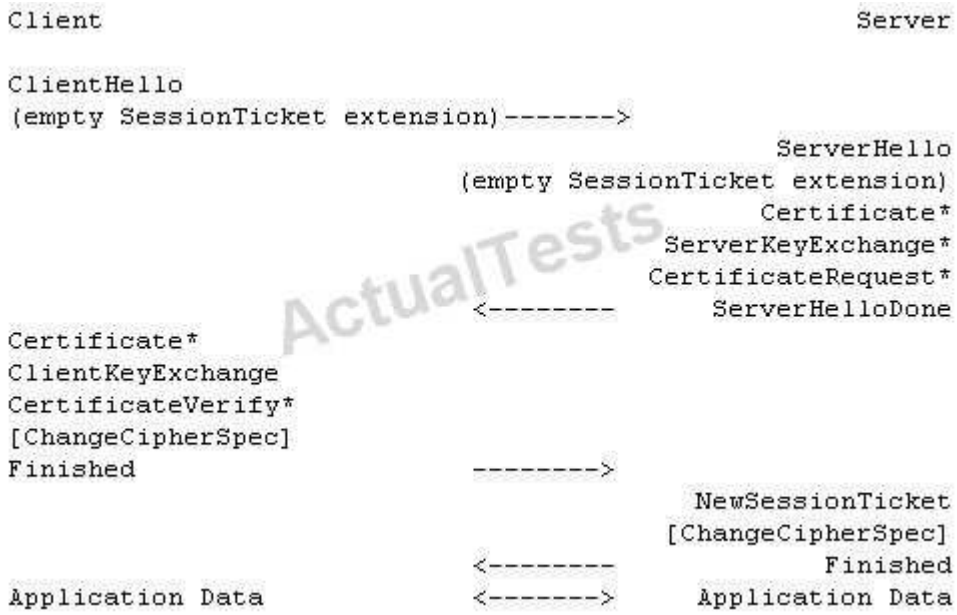


Figure 1: Message flow for full handshake issuing new session ticket The client caches this ticket along with the master secret and other parameters associated with the current session. When the client wishes to resume the session, it includes the ticket in the SessionTicket extension within the ClientHello message. The server then decrypts the received ticket, verifies the ticket's validity, retrieves the session state from the contents of the ticket, and uses this state to resume the session. The interaction with the TLS Session ID is described in Section 3.4. If the server successfully verifies the client's ticket, then it may renew the ticket by including a NewSessionTicket handshake message after the ServerHello.

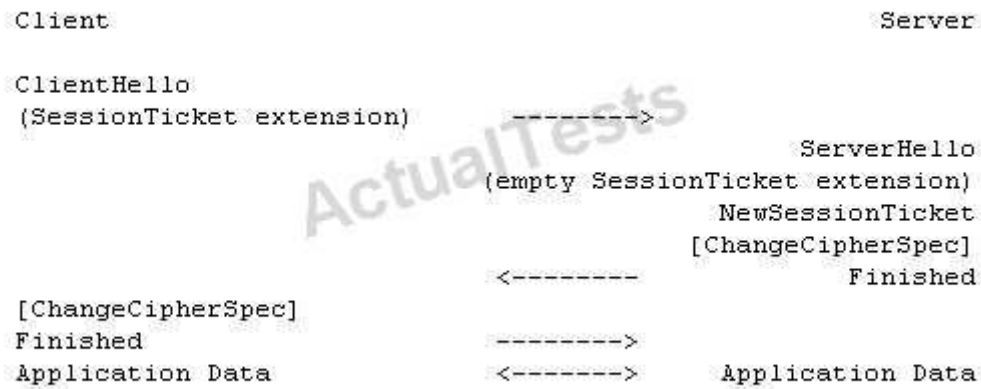


Figure 2: Message flow for abbreviated handshake using new session ticket

pre_master_secret This random value is generated by the client and is used to generate the master secret When RSA is used for server authentication and key exchange, a 48- byte pre_master_secret is generated by the client, encrypted under the server's public key, and sent to the server. The server uses its private key to decrypt the pre_master_secret. Both parties then convert the pre_master_secret into the master_secret, as specified above. If the client has a certificate containing fixed Diffie-Hellman parameters, its certificate contains the information required to complete the key exchange. Note that in this case the client and server will generate

the same Diffie-Hellman result (i.e., pre_master_secret) every time they communicate.

QUESTION 214
Which of the following is the most effective technique to prevent source IP Address spoofing?

A. RFC 1918 filtering
B. policy based routing (PBR)
C. IP source routing
D. unicast reverse path forwarding (uRPF)
E. lock and key ACL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 215
What does the Common Criteria (CC) standard define?

A. The U S standards for encryptions export regulations.
B. The current list of Common Vulnerabilities and Exposures (CVEs)
C. The international standards for privacy laws.
D. The standards for establishing a security incident response systems.
E. Tools to support the development of pirvotal, forward-looking information system technologies.
F. The international standards for evaluating trust in information systems and products.

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security. Unlike standards such as FIPS 140-2, Common Criteria does not provide a list of product security requirements or features that products must contain. Instead, it describes a framework in which computer system users can specify their security requirements, vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.

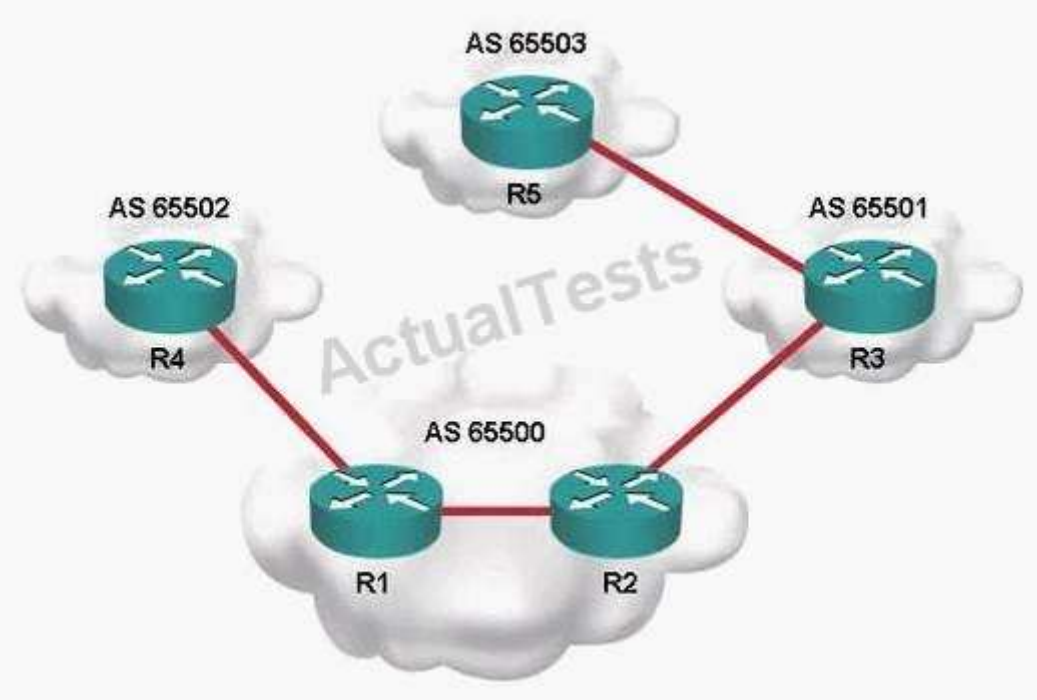
QUESTION 216
What is a stream cipher?

A. cipher that encrypts a byte at a time
B. cipher that encrypts a block at a time
C. Stream is not a valid type of cipher
D. cipher that encrypts one bit at a time

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 217
Refer the Exhibit. What as-path access-list regular expression should be applied on R2 to only allow updates originated from AS65501 or autonomous systems directly attached to AS65501?

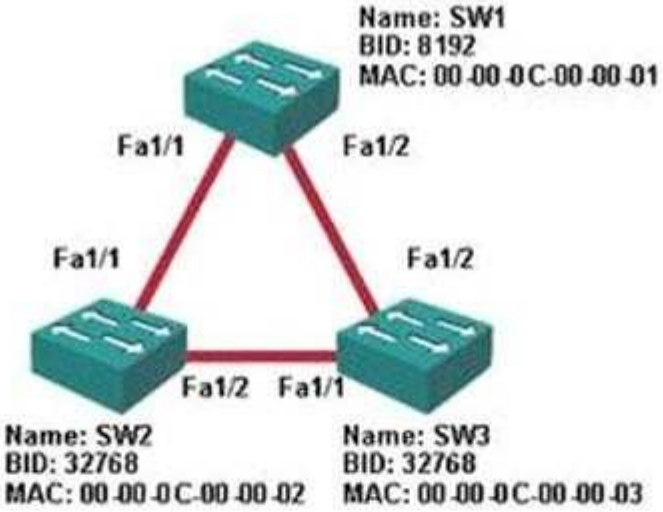


A. _65501+[0.9]$
B. ^65501_[0-9]*$
C. _65501_*$
D. _65501_.*
E. \[0-9]*+65501_+\[0-9]$
F. ^65501_*$

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 218
Refer to the Exhibit. Under normal conditions, SW1 is spanning tree root and the link between SW2 AND SW3 is in the blocking state. This network transports large amounts of traffic and is heavily loaded. After a software upgrade to these switches, users are complaining about slow performance. To troubleshoot, the commands shown in the exhibit are entered. What two are the most likely causes of this issue?




```
SW1> (enable) show port 1
Port  Name                 Status     Vlan       Level  Duplex Speed Type
----- -------------------- ---------- ---------- ------ ------ ----- ------------
 1/1                       connected  1          normal a-full a-100 10/100BaseTX
 1/2                       connected  1          normal a-half a-100 10/100BaseTX
```

```
SW1> show port counters 1
Port  Align-Err  FCS-Err     Xmit-Err    Rcv-Err     UnderSize
----- ---------- ---------- ---------- ---------- ---------
 1/1           0          0          0          0         0
 1/2           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts      Giants
----- ---------- ---------- ---------- ---------- --------- ---------- ---------
 1/1           0          0          0          0         0          0         -
 1/2       12566        660          0       2206         0          0         0
```

```
SW3> (enable) show spantree 1 active
VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled

Designated Root             00-00-0c-00-00-02
Designated Root Priority    32768
Designated Root Cost        19
Designated Root Port        1/1
Root Max Age   14 sec   Hello Time 2 sec   Forward Delay 10 sec

Bridge ID MAC ADDR          00-00-0c-00-00-03
Bridge ID Priority          32768
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port                 Vlan Port-State    Cost      Prio Portfast Channel_id
-------------------- ---- ------------ --------- ---- -------- ----------
 1/1                 1    forwarding          19   32 disabled 0
 1/2                 1    forwarding          19   32 disabled 0
```

A. Duplex mismatch on the link between SW1 and SW3 causing high rate of collisions
B. The bridge priority of SW1 was changed to be greater than 32768 allowing SW2 to become the new root of the spanning tree.
C. UDLD has not been configured between SW1 and SW3 so SW3 errantly sees its link to SW1 as up and operational.
D. Lack of BPDUs from high priority bridge SW1 causes SW3 to unblock Fa1/1 126

E. The Max Age timers on SW1 and SW2 have been changed and no longer match the MAX Age timer on SW3

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 219
Of the threats discussed below, what is the main advantage of using Cisco Secure Desktop which is part of the Cisco ASA VPN solution?

A. Secure desktop will create a completely separate computing environment that will be deleted when you are done. This ensures that no confidential data has been left on the shared/public computer.
B. Secure desktop is used to protect access to your registry and system files when browsing to SSL/VPN protected pages.
C. Secure Desktop ensures that an SSL protected password cannot be exploited by a main in the middle attack using a spoofed certificate.
D. Secure desktop hardens the operating system of the machines you are using at the time secure desktop is launched.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 220
Which of the following statements are true regarding hashing?

A. SHA-256 is an extension to SHA-1 with a longer output
B. SHA-1 is stronger than MD5 because it can be used with a key to prevent modification
C. MD5 takes more CPU cycles to compute than SHA-1
D. MD5 produces a 160-bit result
E. Changing 1 bit of the input to SHA-1 changes 1 bit of the output

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 221

Select the best answer to this QUESTION NO:. ASA/PIX Active/Active failover can be used to load-balance.

A. On a per-context basis only
B. All traffic passing through the appliance
C. Traffic from internal networks on a per IP basis
D. Based on protocol only

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 222
Which three steps are required to enable SSH Server on an IOS router? (Choose three.)

A. Configure a domain name
B. Configure a host name
C. Specifies a fingerprint that can be matched against the fingerprint of a CA certificate during authentication.
D. Generate an RSA key pair.
E. Configure the Crypto PKI trustpoint (CA)
F. Import the SSH client fingerprint.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 223
The following is an example of an IPSec error message:

```
IPSEC(validat_proposal): invalid local address 192.1.1.1
ISAKMP (0:3): atts not acceptable.
Next payload is 0
ISAKMP (0:3): SA not acceptable!
```

What is the most common problem that this message can be attributed to?

A. This is only an informational message, ipsec session will still succeed.
B. Crypto access-lists are not mirrored on each side.
C. Crypto map is applied to the wrong interface or is not applied at all.
D. Router is missing the crypto map map-name local-address command.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

This error message is attributed to one of these two common problems. · The crypto map map-name local-

address interface-id command causes the router to use an incorrect address as the identity because it forces the router to use a specified address. · Crypto map is applied to the wrong interface or is not applied at all. Check the configuration in order to ensure that crypto map is applied to the correct interface.

QUESTION 224
What is the function of the switch(config-if)# switchport port-security mac-address sticky command?

A. allows the switch to dynamically learn the MAC addresses on the switchport and the MAC addresses will be added to the running configuration.
B. allows the switch to perform sticky learning where the dynamically learned MAC addresses are copied from the MAC Address Table (CAM Table) to the startup configuration.
C. allows the switch to permanently store the secured MAC addresses in the MAC Address Table (CAM Table)
D. allows the administrator to manually configured the secured MAC addresses on the switchport.
E. allows the switch to restrict the MAC addresses on the switchport based on the static MAC addresses configured in the startup configuration.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: Explanation
The switch supports these types of secure MAC addresses:
· Static secure MAC addresses--These are manually configured by using the switchport port- security mac-address mac-address interface configuration command, stored in the address table, and added to the switch running configuration.
· Dynamic secure MAC addresses--These are dynamically configured, stored only in the address table, and removed when the switch restarts.
· Sticky secure MAC addresses--These are dynamically configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, when the switch restarts, the interface does not need to dynamically reconfigure them.

QUESTION 225
Referring to partial IOS router configuration shown in the exhibit, which statement is true?

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp key cisco123 address 10.3.3.1
!
!
crypto ipsec transform-set mytrans esp-3des esp-sha-hmac
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to10.3.3.1
 set peer 10.3.3.1
 set transform-set mytrans
 match address 103
!
!
interface FastEthernet0/1
 description $FW_INSIDE$
 ip address 172.16.4.2 255.255.255.0
 ip access-group 100 in
 ip inspect SDM_LOW in
 ip nat inside
!
interface Serial0/0/0
 description $FW_OUTSIDE$
 ip address 10.4.4.1 255.255.255.252
 ip access-group 102 in
 ip verify unicast reverse-path
 ip nat outside
 crypto map SDM_CMAP_1
!
ip nat inside source route-map rmap interface Serial0/0/0 overload
!
route-map rmap permit 1
 match ip address 104
```

```
access-list 100 deny   ip 10.4.4.0 0.0.0.3 any
access-list 100 deny   ip 172.16.14.0 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 102 permit ip 172.16.3.0 0.0.0.255 172.16.4.0 0.0.0.255
access-list 102 permit udp host 10.3.3.1 host 10.4.4.1 eq non500-isakmp
access-list 102 permit udp host 10.3.3.1 host 10.4.4.1 eq isakmp
access-list 102 permit esp host 10.3.3.1 host 10.4.4.1
access-list 102 permit ahp host 10.3.3.1 host 10.4.4.1
access-list 102 permit tcp any host 10.4.4.1 eq 1000
access-list 102 permit icmp host 10.3.3.1 host 10.4.4.1 echo
access-list 102 deny   ip 172.16.4.0 0.0.0.255 any
access-list 102 deny   ip 172.16.14.0 0.0.0.255 any
access-list 102 permit icmp any host 10.4.4.1 echo-reply
access-list 102 permit icmp any host 10.4.4.1 time-exceeded
access-list 102 permit icmp any host 10.4.4.1 unreachable
access-list 102 permit tcp any host 172.16.14.1 eq telnet
access-list 102 permit eigrp any any
access-list 102 deny   ip 10.0.0.0 0.255.255.255 any
access-list 102 deny   ip 172.16.0.0 0.15.255.255 any
access-list 102 deny   ip 192.168.0.0 0.0.255.255 any
access-list 102 deny   ip 127.0.0.0 0.255.255.255 any
access-list 102 deny   ip host 255.255.255.255 any
access-list 102 deny   ip host 0.0.0.0 any
access-list 102 deny   ip any any log
!
access-list 103 permit ip 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255
!
access-list 104 deny   ip 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255
access-list 104 permit ip 172.16.4.0 0.0.0.255 any
access-list 104 permit ip 172.16.14.0 0.0.0.255 any
```

A. Traffic from subnet 172.16.4. 0/24 to the 172.16.3.0/24 subnet will be protected by IPSec and will go through NAT
B. All traffic from subnet 172.16.4.0/24 to the 172.16.3.0/24 subnet will go through NAT
C. ACL 104 is the crypto ACL defining traffic that should be protected by IPSec
D. Traffic from subnet 172.16.4.0/24 to any destinations will be protected by IPSec and will bypass NAT
E. All IPSec protected traffic will bypass NAT

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reason being: NAT ACL is 104, Crypto ACL is 103.
The Crypto ACL says that any traffic from 172.16.4.0/24 going to 172.16.3.0/24 will be IPSec protected. No other traffic is listed.
The NAT ACL says that any traffic from 172.16.4.0/24 to 172.16.3.0 will not be matched and therefor will be ignored by the NAT process. All other traffic from the source 172.16.4.0/24 to ANY and all source 172.16.14.0/24 to ANY traffic will be processed by NAT.

QUESTION 226
How is the ACS server used in the NAC framework?

A. To verify the virus patch levels
B. To authenticate devices based on quarantine information

C. To authorize devices based on quarantine information
D. To verify that the device certificates are correct

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 227
During STP troubleshooting, you determine that the problem is caused by a user connecting a rogue switch to an access port, and that rogue switch becoming the root bridge. What can you do to prevent that kind of situation from happening in the future?

A. Lower the bridge priority on the desired Root Bridge
B. enable VACL to filter the traffic
C. enable IP Source Guard on the portfast access ports
D. enable BPDU Guard on the portfast access ports
E. Lower the port priority on the portfast access ports

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: Explanation
Answer A is wrong because
VACL is an acronym for VLAN Access Control Lists where VLAN stands for Virtual Local Area Network. Specifically created to filter and move VLAN traffic. May be used like a SPAN port or network tap it is a way to replicate computer network data that is coming and going from a computer or a network of computers. This is useful if you want to monitor that traffic to determine the health of the application(s) running on those computer (s) or health of the network itself. VACL or VACL Ports can be much more discriminating of the traffic they forward than a standard SPAN port. They may be set to only forward specific types or specific VLANS to the monitoring port. However, they forward all traffic that matches the criteria as they do not have the functionality to select from ingress or egress traffic like SPAN ports.
Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations.
Election of the Root Switch
All switches in an extended LAN participating in Spanning-Tree Protocol gather information on other switches in the network through an exchange of data messages. These messages are bridge protocol data units (BPDUs). This exchange of messages results in the following:
· The election of a unique root switch for the stable spanning-tree network topology. · The election of a designated switch for every switched LAN segment. · The removal of loops in the switched network by placing redundant switch ports in a backup state.

The Spanning-Tree Protocol root switch is the logical center of the spanning-tree topology in a switched network. All paths that are not needed to reach the root switch from anywhere in the switched network are placed in Spanning-Tree Protocol backup mode. Table C-1 describes the root switch variables, that affect the entire spanning-tree performance.

Table C-1: Root Switch Variables Affecting STP

Variable	Description
Hello Time	**Determines how often the switch broadcasts its hello message to other switches.**
Maximum Age Timer	Measures the age of the received protocol information recorded for a port and ensures that this information is discarded when its age limit exceeds the value to the maximum age parameter recorded by the switch. The timeout value for this timer is the maximum age parameter of the switches.
Forward Delay Timer	Monitors the time spent by a port in the learning and listening states. The timeout value is the forward delay parameter of the switches.

BPDUs contain information about the transmitting switch and its ports, including switch and port Media Access Control (MAC) addresses, switch priority, port priority, and port cost. The Spanning- Tree Protocol uses this information to elect the root switch and root port for the switched network, as well as the root port and designated port for each switched segment.

B is correct because
The STP PortFast BPDU guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are not able to influence the STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that has PortFast configured. The BPDU guard transitions the port into errdisable state, and a message appears on the console.

133

C is wrong because
IP source guard is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. You can use IP source guard to prevent traffic attacks caused when a host tries to use the IP address of its neighbor.
You can enable IP source guard when DHCP snooping is enabled on an untrusted interface. After IP source guard is enabled on an interface, the switch blocks all IP traffic received on the interface, except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.
The IP source binding table has bindings that are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.
IP source guard is supported only on Layer 2 ports, including access and trunk ports.You can configure IP source guard with source IP address filtering or with source IP and MAC address filtering.

D & E are wrong because neither is a perminate solution to the problem

QUESTION 228
Refer to the exhibit. In the sample configuration file what does the ip verify unicast reverse-path interface command accomplish?

```
ip cef distributed
!
interface Serial 1/0/0
 ip address 207.19.165.225 255.255.255.252
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reverse-path
 ip access-group 201 in
 ip access-group 101 out
!
access-list 101 permit ip 207.19.165.128 0.0.0.31 any
access-list 101 deny ip any any log
access-list 201 deny ip host 0.0.0.0 any log
access-list 201 deny ip 127.0.0.0 0.255.255.255 any log
access-list 201 deny ip 10.0.0.0 0.255.255.255 any log
access-list 201 deny ip 172.16.0.0 0.15.255.255 any log
access-list 201 deny ip 192.168.0.0 0.0.255.255 any log
access-list 201 deny ip 207.19.165.128 0.0.0.31 any log
access-list 201 permit ip any any
```


A. It verifies source address and source interface of all input traffic on an interface is in the routing table.
B. It verifies the route of incoming traffic is from an approved network.
C. It verifies the route of outgoing traffic is an approved network.
D. It verifies destination address and destination interface of all output traffic on an interface is in the routing table.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 229
Referring to partial IOS router configuration shown in the exhibit, which statement is true?

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp key cisco123 address 10.3.3.1
!
!
crypto ipsec transform-set mytrans esp-3des esp-sha-hmac
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to10.3.3.1
 set peer 10.3.3.1
 set transform-set mytrans
 match address 103
!
!
interface FastEthernet0/1
 description $FW_INSIDE$
 ip address 172.16.4.2 255.255.255.0
 ip access-group 100 in
 ip inspect SDM_LOW in
 ip nat inside
!
interface Serial0/0/0
 description $FW_OUTSIDE$
 ip address 10.4.4.1 255.255.255.252
 ip access-group 102 in
 ip verify unicast reverse-path
 ip nat outside
 crypto map SDM_CMAP_1
!
ip nat inside source route-map rmap interface Serial0/0/0 overload
!
route-map rmap permit 1
 match ip address 104
```

```
access-list 100 deny   ip 10.4.4.0 0.0.0.3 any
access-list 100 deny   ip 172.16.14.0 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 102 permit ip 172.16.3.0 0.0.0.255 172.16.4.0 0.0.0.255
access-list 102 permit udp host 10.3.3.1 host 10.4.4.1 eq non500-isakmp
access-list 102 permit udp host 10.3.3.1 host 10.4.4.1 eq isakmp
access-list 102 permit esp host 10.3.3.1 host 10.4.4.1
access-list 102 permit ahp host 10.3.3.1 host 10.4.4.1
access-list 102 permit tcp any host 10.4.4.1 eq 1000
access-list 102 permit icmp host 10.3.3.1 host 10.4.4.1 echo
access-list 102 deny   ip 172.16.4.0 0.0.0.255 any
access-list 102 deny   ip 172.16.14.0 0.0.0.255 any
access-list 102 permit icmp any host 10.4.4.1 echo-reply
access-list 102 permit icmp any host 10.4.4.1 time-exceeded
access-list 102 permit icmp any host 10.4.4.1 unreachable
access-list 102 permit tcp any host 172.16.14.1 eq telnet
access-list 102 permit eigrp any any
access-list 102 deny   ip 10.0.0.0 0.255.255.255 any
access-list 102 deny   ip 172.16.0.0 0.15.255.255 any
access-list 102 deny   ip 192.168.0.0 0.0.255.255 any
access-list 102 deny   ip 127.0.0.0 0.255.255.255 any
access-list 102 deny   ip host 255.255.255.255 any
access-list 102 deny   ip host 0.0.0.0 any
access-list 102 deny   ip any any log
!
access-list 103 permit ip 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255
!
access-list 104 deny   ip 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255
access-list 104 permit ip 172.16.4.0 0.0.0.255 any
access-list 104 permit ip 172.16.14.0 0.0.0.255 any
```

A. ACL 104 is the crypto ACL defining traffic that should be protected by IPSec.
B. All traffic from subnet 172.16.4.0/24 to the 172.16.3.0/24 subnet will go through NAT
C. All IPSec protected traffic bypass NAT
D. Traffic from subnet 172.16.4.0/24 to any destinations will be protected by IPSec and will bypass NAT
E. Traffic from subnet 172.16.4.0/24 to the 172.16.3.0/24 subnet will be protected by IPSEC and will go through NAT.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 230
CSA network shield does which of the following?

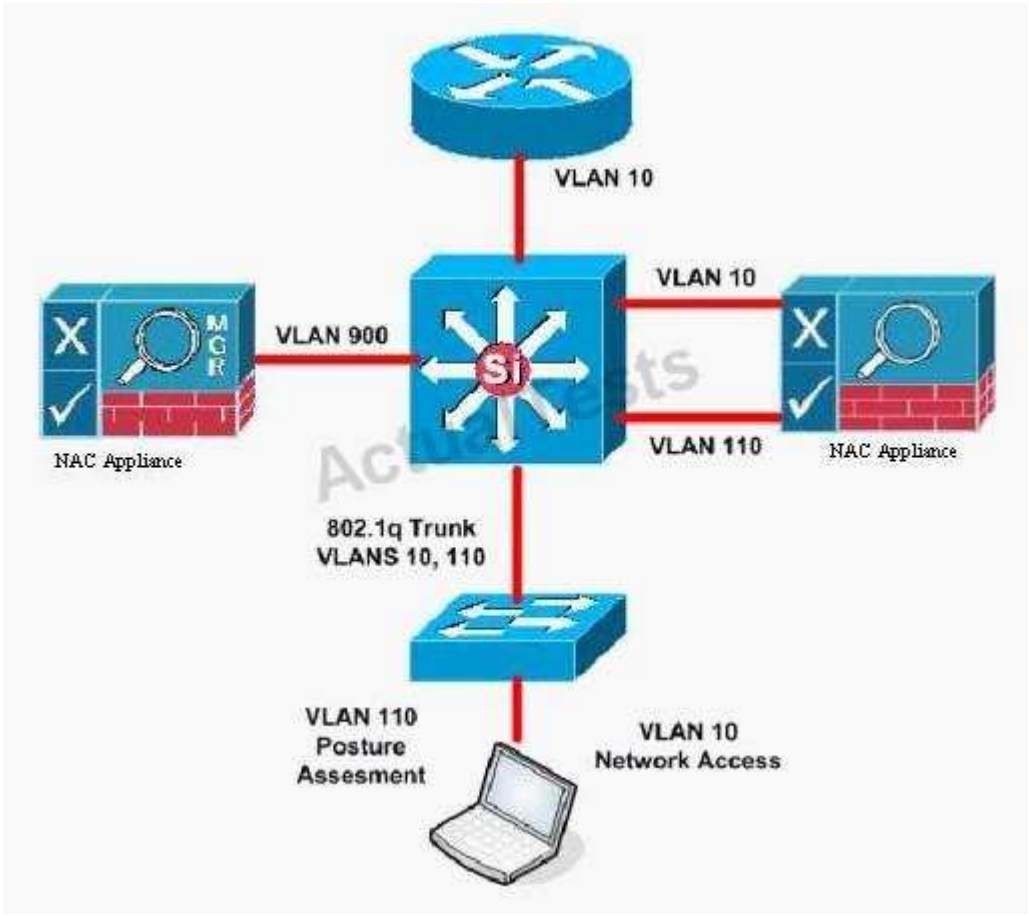
A. Prevents buffer overflows
B. Drops malformed IP packets
C. Stops your user-defined applications from responding to vulnerability scanners
D. Prevents open listening network sockets
E. Prevents users from entering unencrypted passwords

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 231
Refer to the exhibit. Which three of the following statements are correct? (choose 3)



A. In the exhibit is an example of a NAC appliance network
B. Cisco Trust Agent (CTA) is used to verify the end user's PC complies with the security policy
C. In the exhibit is an example of a NAC framework network
D. NAC Appliance Agent (NAA) is used to verify the end user's PC complies with the security policy
E. The network utilizes In-ban admission control
F. The network utilizes Out-of- ban admission control

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 232
Which of the following best describes what NTP ensures in the router when implementing IPsec VPN in a PKI environment?

A. The router has the correct time when generating its private and public key pairs.
B. The router has the correct time when checking certificate validity from the remote peers.
C. The router time is synchronized with the remote peers for encryption key generation.
D. The router time is synchronized with the remote peers during the DH exchange.
E. The router time is synchronized with the remote peers when generating the cookies during IKE Phase 1.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 233
Referring to the shown configuration, which type of attack is it trying to mitigate?

```
access-list 111 permit udp any any eq 1434
 class-map match-all bad_worm
  match access-group 111
  match packet length min 404 max 404
 policy-map drop-bad-worm
  class bad-worm
   police 1000000 22250 22250 conform-action drop exceed-action drop violate-actio
```


A. Smurf Attack
B. Code Red Worm
C. This is not valid configuration.
D. MSQL and JavaScript attack
E. SQL Slammer Worm

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 234
To enable TCP port-forwarding applications using Cisco IOS WebVPN, what needs to be downloaded to the client?

A. Cisco Security Agent
B. Cisco Trust Agent
C. Cisco Secure Desktop
D. a small Java applet
E. SSL VPN Client
F. SSL VPN Client and Cisco Secure Desktop

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 235
You want to establish Internet connectivity from a private office with the following conditions:

· 254 users
· only one IP address provided by your ISP
· dynamically assigned IP address
· CPE from the ISP is preprovisioned and working
· router changes are expected

Which three of the following RFCs can you use for this connectivity? (Choose three.)

A. IP Network Address Translator (NAT): Defined in RFC 1631
B. IP Network Address Translator (NAT) Terminology and Considerations: Defined in RFC 2663
C. Network Address Translator (NAT) - Friendly Application Design Guidelines: Defined in RFC
D. Address Allocation for Private Internets: Defined in RFC 1918
E. PPP and IPCP: Defined in RFC 1332
F. DHCP: Defined in RFC 2131

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 236
Whenever a failover takes place on the ASA (configured for failover), all active connections are dropped and clients must re-establish their connections unless:(Choose 2)

A. The ASA is configured for LAN-Based failover.
B. The ASA is configured for Active-Active failover and a state failover link has been configured.
C. The ASA is configured to use a serial cable as failover link.
D. The ASA is configured for Active-Standby failover and a state failover link has been configured.
E. The ASA is configured for Active-Active failover.
F. The ASA is configured for Active-Standby failover.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 237
Which of the following should be the key driver for a company security policy creation, implementation, and enforcement?

A. the company's business objectives
B. the company's network topology
C. the business knowledge of the IT staff
D. the technical knowledge of the IT staff

E. the IT future directions

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 238
Which statement is true about SYN cookies?

A. All TCP options are supported, such as large windows.
B. The server can have more than eight unique MSS values.
C. SYN cookies are not implemented as a method of defending against SYN floods.
D. SYN cookies are implemented as a method of defending against SYN floods.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 239
PEAP provides authentication for the EAP exchange using

A. SSH
B. RC4
C. 3DES
D. TLS
E. AES

Correct Answer: D
Section: (none)
Explanation

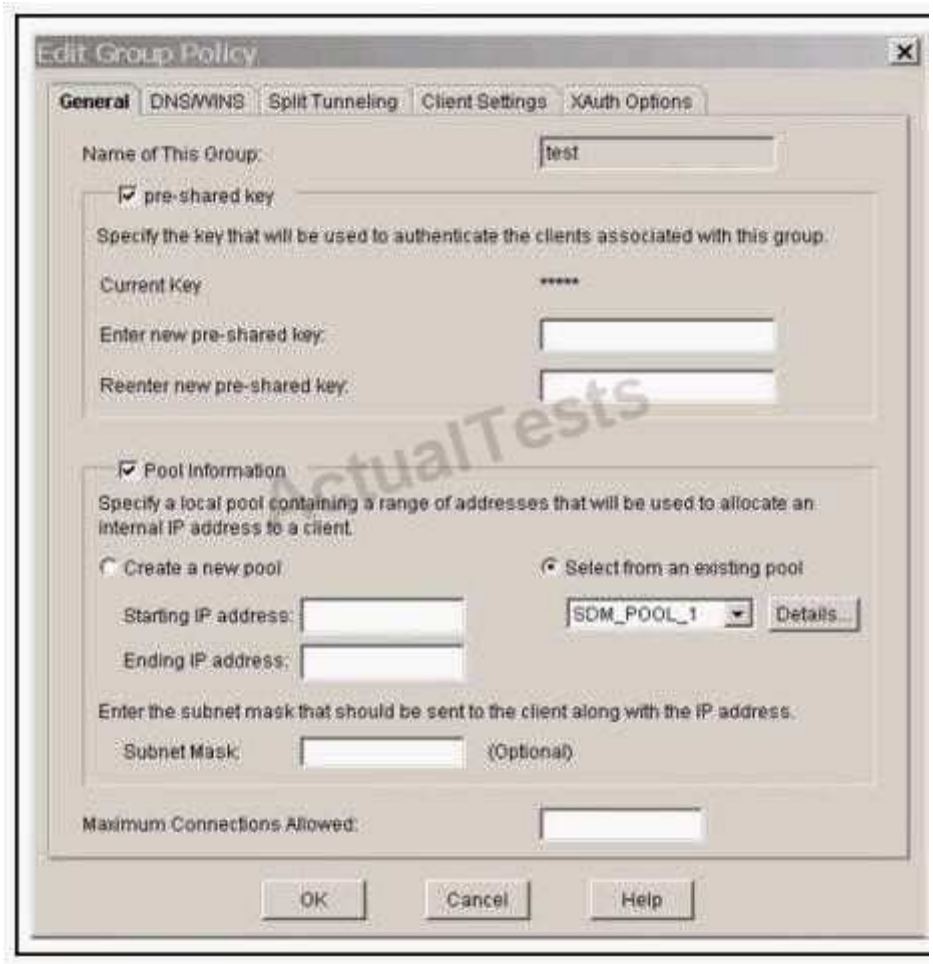
Explanation/Reference:
Explanation:
Protected Extensible Authentication Protocol, Protected EAP, or simply PEAP (pronounced "peep"), is a method to securely transmit authentication information, including passwords, over wired or wireless networks. It was jointly developed by Cisco Systems, Microsoft, and RSA Security. Note that PEAP is not an encryption protocol; as with other EAP types it only authenticates a client into a network.
PEAP uses only server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server. The ensuing exchange of authentication information is then encrypted and user credentials are safe from eavesdropping. PEAP is a joint proposal by Cisco Systems, Microsoft and RSA Security as an open standard. It is already widely available in products, and provides very good security. It is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication.

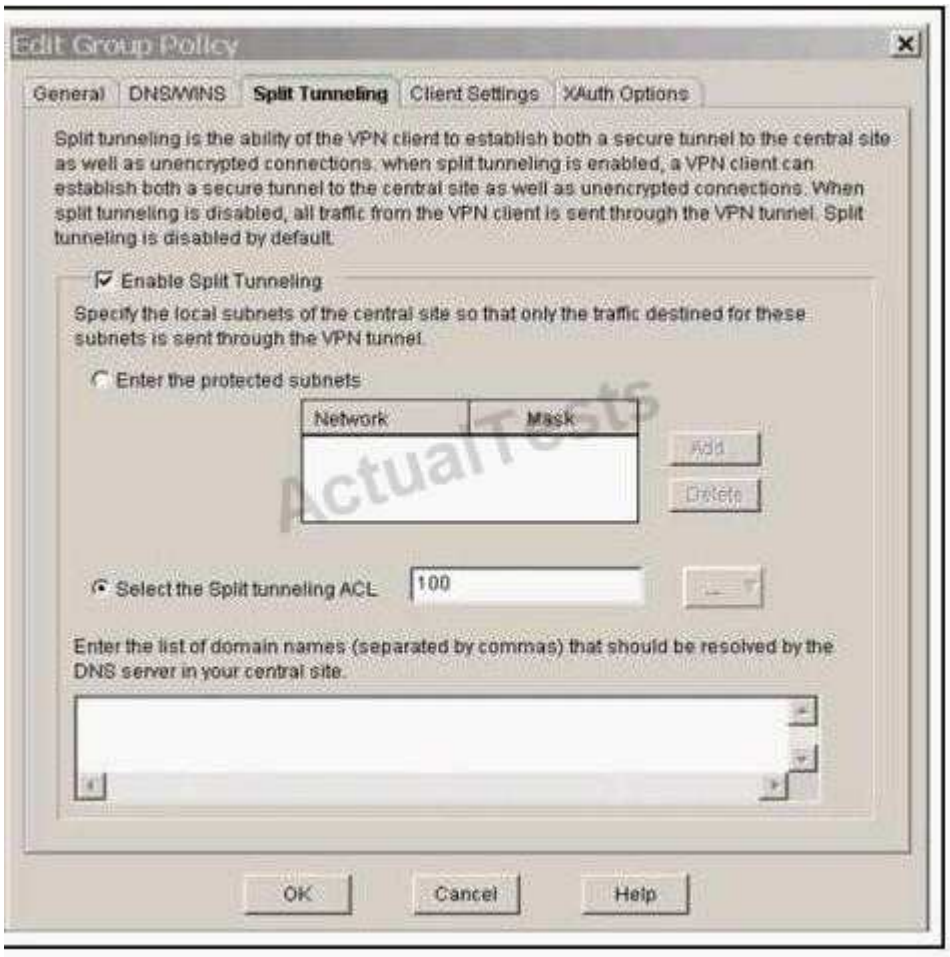
As of May of 2005, there were two PEAP sub-types certified for the updated WPA and WPA2 standard. They are:

· PEAPv0/EAP-MSCHAPv2
· PEAPv1/EAP-GTC

QUESTION 240

Refer to the Cisco SDM screens shown.





Which two statements are true about the Cisco IOS Easy VPN Server configuration? (Choose two.)

A. A digital certificate is used to authenticate the remote VPN client.
B. Split tunneling is enabled where traffic that matches ACL 100 will not be encrypted.
C. Split tunneling is disabled because no protected subnets have been defined.
D. To connect, the remote VPN client will use a groupname "test."
E. The remote VPN client will be assigned an internal IP address from the SDM_POOL_1 IP address pool.
F. Pre-shared key authentication will be used during the XAUTH phase.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 241
Cisco Clean Access ensures that computers connecting to your network have which of the following?

A. No viruses or worms
B. No vulnerable applications or operating systems
C. Appropriate security applications and patch levels.
D. Current ips signatures.

E. Cisco Security Agent

Correct Answer: C
Section: (none)
Explanation

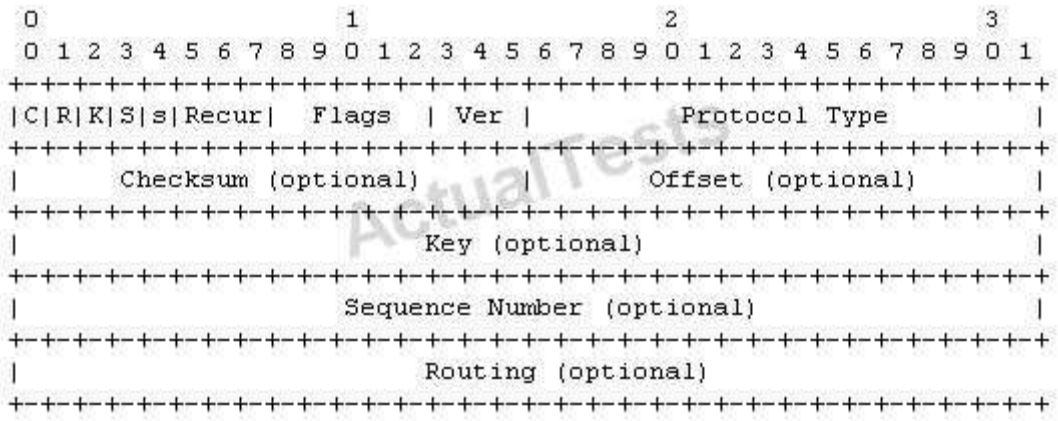
Explanation/Reference:
Explanation:

QUESTION 242
What is the size of a point-to-point GRE header, and Protocol number at IP layer?

A. 8 byte, and 74
B. 4 byte, and 47
C. 2 byte, and 71
D. 24 byte, and 1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Protocol suite: TCP/IP. Type: Transport layer encapsulation protocol. IP Protocol: 47.
Generic Routing Encapsulation (GRE)
Packet header The GRE packet header has the form:



Flags and version (2 octets)
The GRE flags are encoded in the first two octets. Bit 0 is the most significant bit, bit 15 is the least significant bit. Bits 13 through 15 are reserved for the Version field. Bits 5 through 12 are reserved for future use and MUST be transmitted as zero.

RFC 1701 Generic Routing Encapsulation (GRE) October 1994 Checksum Present (bit 0)
If the Checksum Present bit is set to 1, then the Checksum field is present and contains valid information. If either the Checksum Present bit or the Routing Present bit are set, BOTH the Checksum and Offset fields are present in the GRE packet. Routing Present (bit 1) If the Routing Present bit is set to 1, then it indicates that the Offset and Routing fields are present and contain valid information. If either the Checksum Present bit or the Routing Present bit are set, BOTH the Checksum and Offset fields are present in the GRE packet.

Key Present (bit 2) If the Key Present bit is set to 1, then it indicates that the Key field is present in the GRE header. Otherwise, the Key field is not present in the GRE header. Sequence Number Present (bit 3) If the Sequence Number Present bit is set to 1, then it indicates that the Sequence Number field is present.

Otherwise, the Sequence Number field is not present in the GRE header.
Strict Source Route (bit 4) The meaning of the Strict Source route bit is defined in other documents. It is recommended that this bit only be set to 1 if all of the the Routing Information consists of Strict Source Routes.
Recursion Control (bits 5-7) Recursion control contains a three bit unsigned integer which contains the number of additional encapsulations which are permissible. This SHOULD default to zero.
RFC 1701 & 2890

QUESTION 243
Based on the following partial configuration shown, which statement is true?

```
Interface FsaEthernet0/1
Switchport access vlan 100
Switchport mode access
Dot1x port-control auto
Dot1x guest-vlan 10
```

A. vlan 10, the guest vlan is also known as the restricted vlan
B. EAP over LAN frames will flow over VLAN 10
C. client connecting to port fa0/1 with an 802.1x supplicant but fails authentication will be assigned to the vlan 100
D. client without an 802.1x supplicant connecting to port fa0/1 will be assigned to the vlan 10
E. client connecting to port fa0/1 with an 802.1x supplicant but fails authentication will be assigned to the vlan 10

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
switchport access
Use the switchport access interface configuration command to configure a port as a static-access port. The port operates as a member of the configured VLAN. Use the no form of this command to reset the access mode to the default VLAN for the switch.
Syntax
switchport access vlan vlan-id
no switchport access vlan vlan-id
Syntax Description
vlan vlan-id
ID of the VLAN. Valid IDs are from 1 to 1005. Do not enter leading zeroes.
switchport mode
Use the switchport mode interface configuration command on the switch stack or on a standalone switch to configure the VLAN membership mode of a port. Use the no form of this command to reset the mode to the appropriate default for the device. switchport mode {access | dot1q-tunnel | dynamic {auto | desirable} | private-vlan | trunk} no switchport mode {access | dot1q-tunnel | dynamic | trunk} Syntax Description dot1x port-control

access	Set the port to access mode (either static-access or dynamic-access depending on the setting of the switchport access vlan interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN.
dot1q-tunnel	Set the port as an 802.1Q tunnel port.
dynamic auto	Set the interface trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link. This is the default switchport mode.
dynamic desirable	Set the interface trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
private-vlan	See the switchport mode private-vlan command.
trunk	Set the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.

Use the dot1x port-control interface configuration command to enable manual control of the authorization state of the port. Use the no form of this command to return to the default setting.

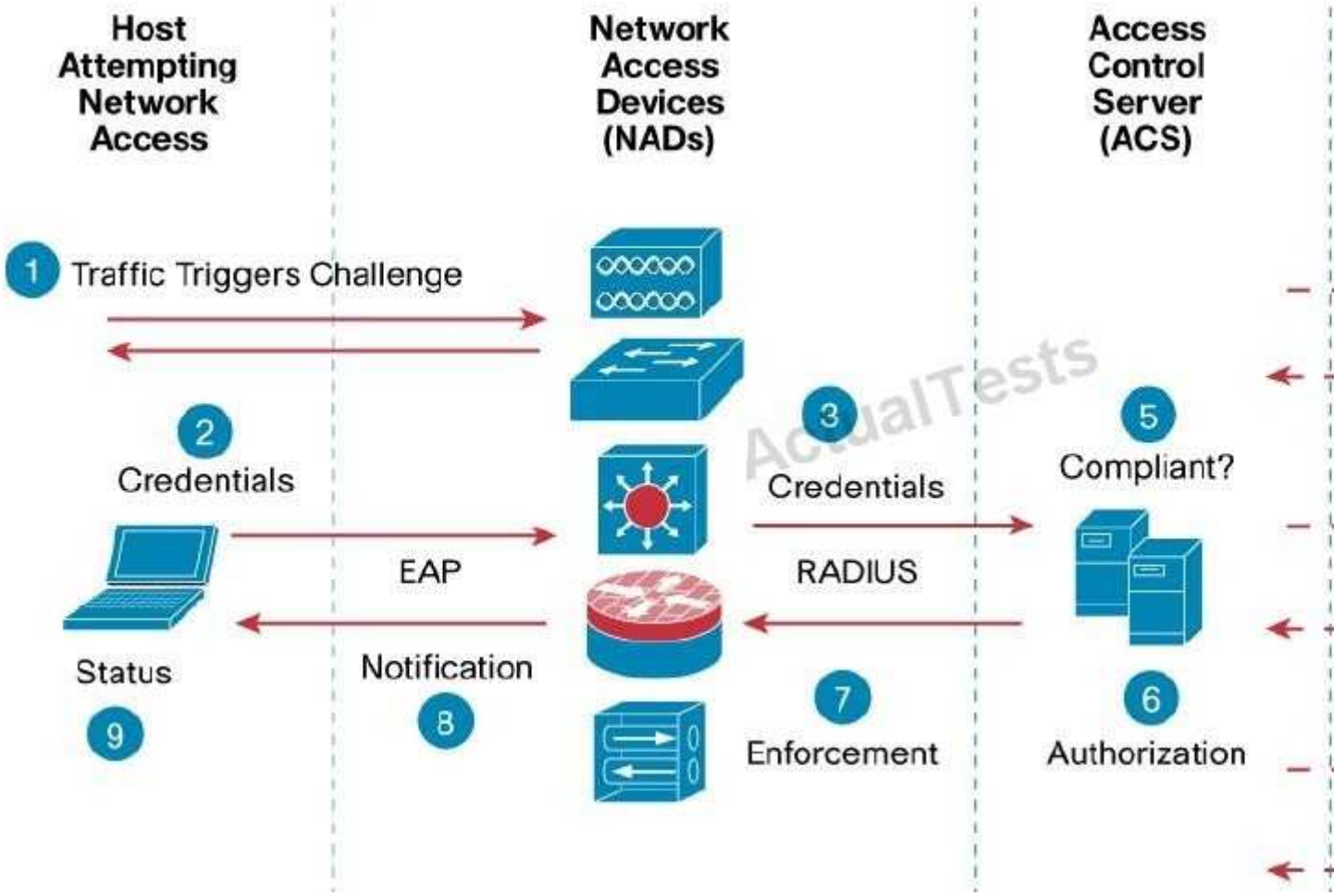
Syntax Description auto
Enable 802.1X authentication on the interface and cause the port to transition to the authorized or unauthorized state based on the 802.1X authentication exchange between the switch and the client.

QUESTION 244
Which is a function of a Cisco router acting as a Network Access Device (NAD) in a NAC Framework solution?

A. Communicates with the antivirus policy server using the HCAP protocol
B. Maps policy decisions to a network access profile
C. Sends and receives posture information to and from the policy server using the RADIUS protocol
D. Acts as a Posture Credentials Provider(PCP)

Correct Answer: C
Section: (none)
Explanation

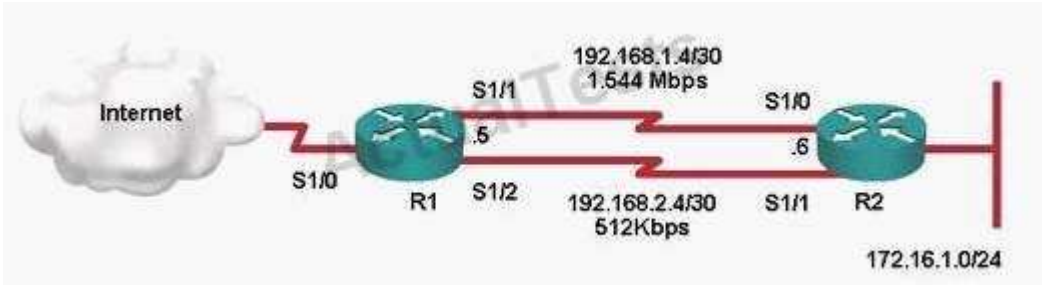
Explanation/Reference:
Explanation:
Network Access Device (NAD) -- Network devices acting as a NAC enforcement point. These can include Cisco access routers (800-7200), VPN Gateways (VPN3000 series), Catalyst Layer 2 and Layer 3 switches, and wireless access points.



Step 1. Posture validation occurs when a NAC-enabled network access device detects a host attempting to connect or use its network resources.
Step 2. Upon detection of a new endpoint, the NAD sets up a communication path between the AAA server (ACS) and the posture agent. After the communication path has been established, the AAA server requests the endpoint for posture credentials from one or more posture plugins. Step 3. The host responds to the request with its posture credentials from available posture plugins from NAC-compatible software components on the host. Step 4. The AAA server either validates the posture information locally, or it can in turn delegate parts of the decision to external posture validation servers. Step 5. The AAA server aggregates the individual posture results, or posture tokens, from all of the delegate servers to determine the overall compliance of the host, or system posture token. Step 6. The identity authentication and system posture token are then mapped to a network authorization in the network access profile, which
consists of RADIUS attributes for timers, VLAN assignments, or downloadable access control lists (ACLs).
Step 7. These RADIUS attributes are sent to the NAD for enforcement on the host. Step 8. The CTA on the host is then sent its posture status for notifying the respective plugins of their individual application posture as well as the entire system posture. Step 9. A message can be optionally sent to the end-user using the CTA's notification dialog so they know the host's current state on the network.

QUESTION 245
Refer to the Exhibit. Routers R1 and R2 are connected by two links, one primary (1.544Mbps) and one backup (512Kbps). For this network design, the backup link should only be used if the primary link is down, and it was decided only static routing be used. Therefore, a default route to the Internet and two static routes pointing to the 172.16.1.0/24 network are to be configured on R1. What primary static route

should be configured on R1, to ensure backup routing occurs (and the primary static route is removed) if the primary link between R1 and R2 fails?



A. ip route 172.16.1.0 255.255.255.0 serial 1/1 192.168.1.6
B. ip route 172.16.1.0 255.255.255.0 192.168.1.6
C. ip route 172.16.1.0 255.255.255.0 serial 1/1
D. ip route 172.16.1.0 255.255.255.0 serial 1/0
E. ip route 172.16.1.0 255.255.255.0 serial 1/0 200

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 246
When configuring the FWSM for multiple security contexts, in which context do you allocate interfaces?

A. Both b and c
B. System context
C. Admin context
D. Context A

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 247
An attacker is attempting to Telnet to a specific host secured behind a firewall rule that only allows inbound connections on TCP port 25. What aspect of RFC 791 (Internet Protocol) can the attacker exploit to perform this attack?

A. Send packets with a fragmentation offset of 20 and a TCP destination port 25. All subsequent packets will overwrite the IP header allowing a new IP header to be inserted.
B. Send a SYN/ACK to the host on TCP port 23 indicating a response to a SYN request from the host on the secure side of the firewall.
C. Send two packets, the first packet with the DF bit clear and the MF bit set, and the second packet with a fragmentation offset of 1 and a destination port of TCP 23.
D. Send packets destined for TCP port 23 with the DF and MF bits clear and the fragment offset to 0 since many firewalls will pass IP fragments with a 0 offset

E. Set the TOS bits to 1111 1100 indicating a network control packet that should be forwarded to the host with high reliability (no discard)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 248
Since HTTP is one of the most common protocols used in the internet, what should be done at a firewall level to ensure that the protocol is being used correctly?

A. Ensure that HTTP is always authenticated.
B. Ensure that a stateful firewall allows only HTTP traffic destined for valid web server IP address.
C. Ensure that your web server is in a different zone than your backend servers such as SQL and DNS.
D. Ensure that your firewall enforces HTTP protocol compliance to ensure that only valid flows are allowed in and out of your network.
E. Ensure that a firewall has SYN flood and DDoS protection applied specifically for valid web servers.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 249
What is the main reason for using the "ip ips deny-action ips-interface" IOS command?

A. To support load-balancing configurations in which traffic can arrive via multiple interfaces.
B. To selectively apply drop actions to specific interfaces.
C. This is not a valid IOS command.
D. To enable IOS to drop traffic for signatures configured with the Drop action.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 250
When implementing internet standards you are required to follow RFC's processes and procedures based on what RFC?

A. RFC 1669 real standards and mere publications.
B. RFC 1769 and mere publications.
C. None of the above.
D. Real standards and mere publications RFC 1769
E. Real standards of RFC 1918

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 251
What are two key characteristics of VTP? (Choose two.)

A. VTP messages are sent out all switch-switch connections.
B. VTP manages addition, deletion, and renaming of VLANs 1 to 4094.
C. VTPv2 can only be used in a domain consisting of VTPv2-capable switches.
D. VTP V2 performs consistency checks on all sources of VLAN information.
E. VTP pruning restricts flooded traffic, increasing available bandwidth.
F. VTP L2 messages are communicated to neighbors using CDP.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 252
With PGP, which of the following entity signs a user's public key?

A. The receipient of the message.
B. A third party that belong to what's often known as "web of trust", that can verify the relationship between the user and the key.
C. The sender of the message.
D. The vendor of the PGP program.
E. The sender's administrator who provides the sender with the PGP program.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

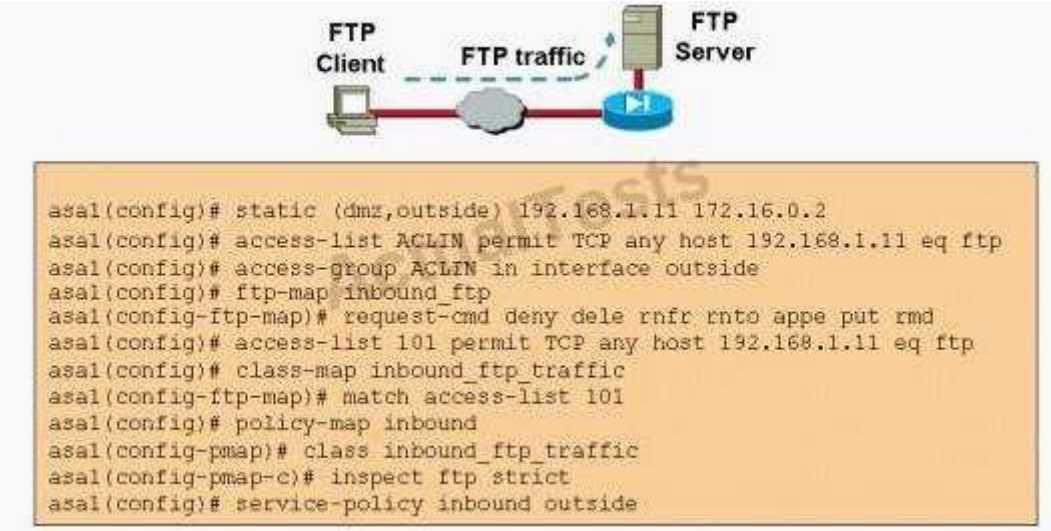
QUESTION 253
Which is a function of a Cisco router acting as a Network Access Device (NAD) in a NAC Framework solution ?

A. Sends and receives posture information to and from the policy server using the RADIUS protocol
B. Communicates with the antivirus policy server using the HCAP protocol
C. Maps policy decisions to a network access profile
D. Acts as a Posture Credentials Provider (PCP)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 254
Refer to the diagram and partial configuration. Based on the partial configuration, which of the following FTP application answers is correct?



A. If the FTP client is configured for active FTP, the ASA partial configuration will enable the remote user to "get" and "put" FTP files.
B. If the FTP client is configured for passive FTP, ASA FTP protocol inspection is required before FTP data traffic can be returned through the ASA to the FTP client.
C. If the FTP client is configured for passive FTP, the ASA partial configuration will enable remote user to "get" but not "put" FTP files.
D. If the FTP client is configured for active FTP, only the outside access-list and FTP server static statement are required before FTP data and control traffic can be passed through the ASA.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 255
What new features were added to the PIX in version 7.0? (Choose 3)

A. WebVPN
B. Support for multiple virtual firewalls
C. Rate-Limiting
D. Transparent firewall

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 256
What is the best way to mitigate Browser Helper Objects from being installed on your system?

A. Disable BHOs in your browser preferences.
B. A BHO is certificate-protected and therefore safe to install on your system.
C. A BHO is not a security concern.
D. A BHO is easily protected using default antivirus or IPS signatures.
E. A BHO installation can be stopped using Cisco Security Agent rules.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

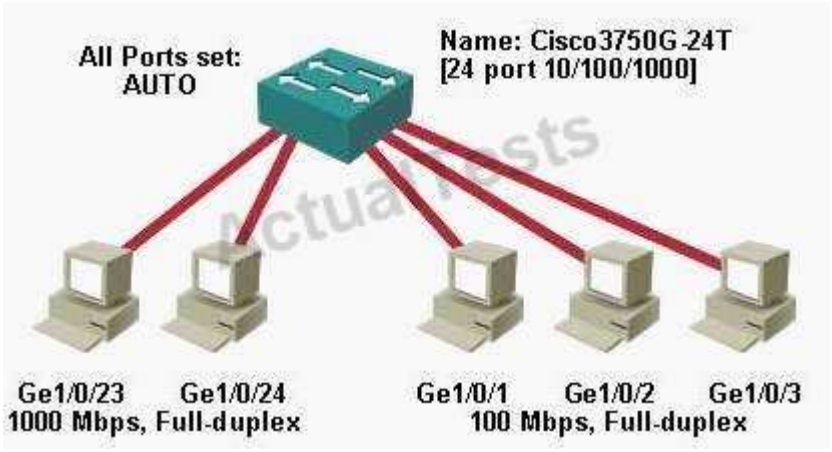
QUESTION 257
Referring to the ASDM screen shot shown in the exhibit, which of the following traffic is permitted based on the current Access Rules?

A. Any IP traffic from any host on the outside to the 172.16.10.2 server on the dmz2
B. HTTP traffic from the 172.16.10.2 server to any host on the inside
C. FTP traffic from any host on the outside to the 172.16.1.2 host on the dmz
D. Any IP traffic from the 172.16.1.2 host to any host on the inside
E. Any IP traffic from any host on the inside to any host on the dmz or dmz2
F. Any IP traffic from any host on the dmz to any host on the outside 155

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 258
Refer to the Exhibit. A Cisco 10/100/1000 Mbps switch is inserted in a small office network. The two servers and three user workstations are configured as shown in the diagram. After inserting the switch, server to server communication is fine, but performance and communication to/from user workstations is poor. What is the most likely cause of these problems?



A. Connections to user workstations improperly configured as Trunk ports
B. Auto negotiation failure causing duplex mismatches only on 100Mpbs interfaces
C. Bad or faulty Ethernet NICs on the user PCs
D. Bad or faulty Ethernet ports/controllers on the Cisco 10/100/1000 switch
E. Failure to configure user workstation interfaces for spanning tree portfast

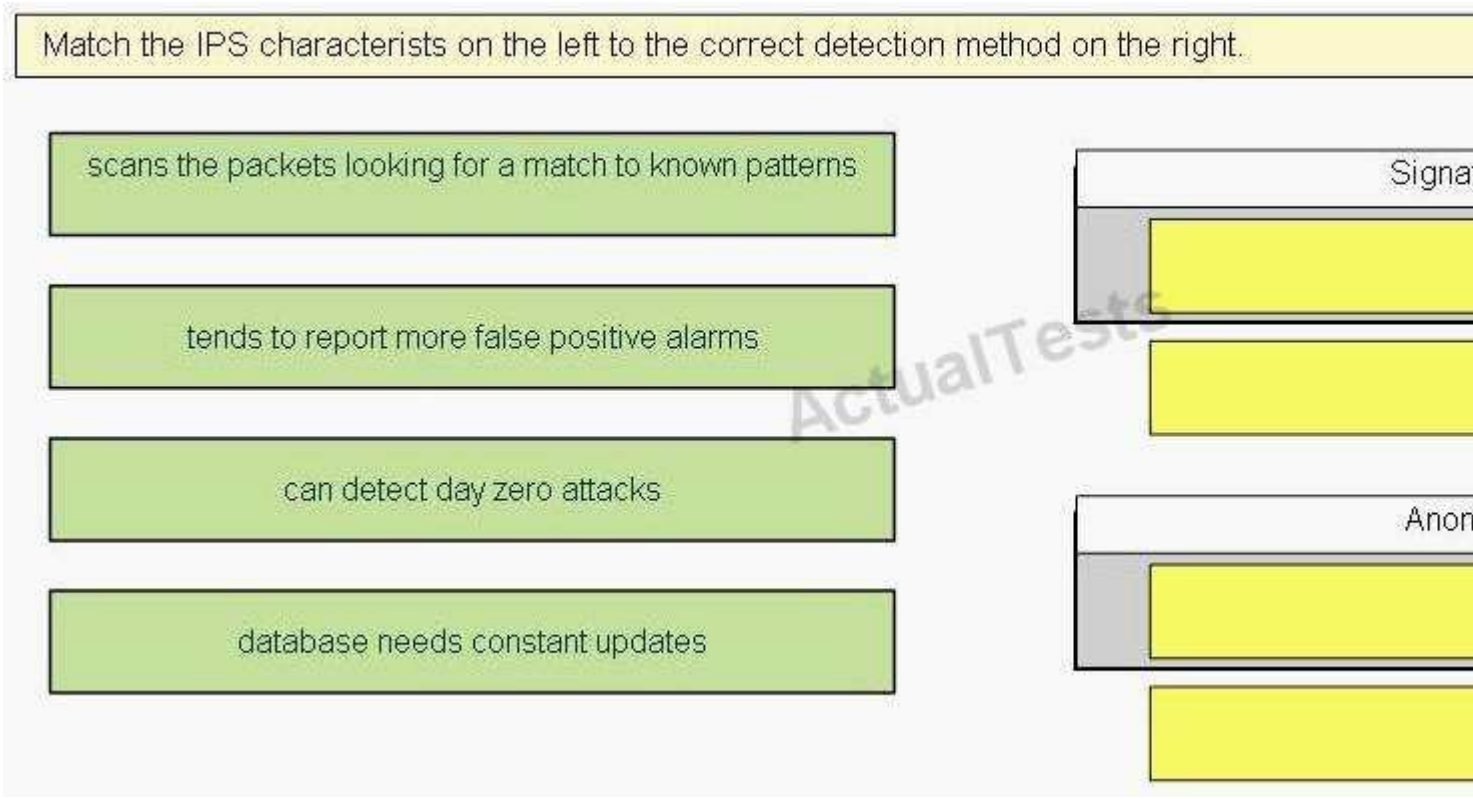
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A is incorrect because very rarely will mulitple NIC's fall on multiple PC's at the same time. The common denonator in this instance is the installation of the switch B is incorrect because no sign of wrong configuration is shown C is incorrect because it is also an extreamly rare occurance D is incorrect because user workstation ports do not participate in Spanning tree E is correct and can be a common occurance this reequires the port speed to be statically configured on the 100mbps switch ports

156

QUESTION 259
DRAG DROP

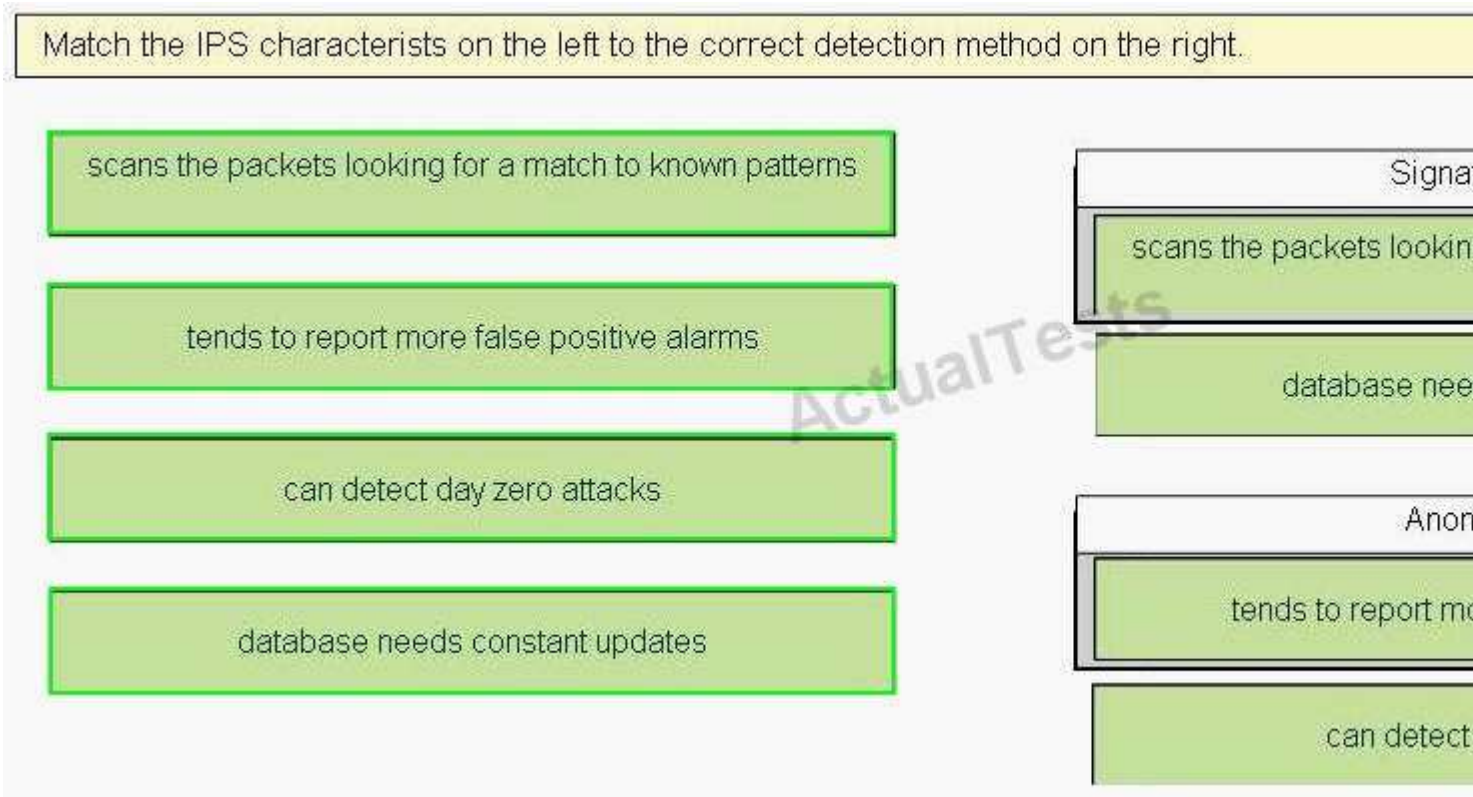
Drop



A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:



Explanation:

QUESTION 260
Which two of these security statements are correct about the HTTP protocol and its use? (Choose two.)

A. HTTP is often used to tunnel communication for insecure clients such as P2P.
B. HTTP can provide server identification.
C. HTTP is NOT often used to tunnel communication for insecure clients such as P2P.
D. Cookies can not provide information about where you have been.
E. Long URLs are not used to provoke buffer overflows.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 261
Based on the following partial configuration shown, which statement is true?

```
interface FastEthernet0/1
switchport access vlan 100
switchport mode access
dot1x port-control auto
dot1x guest-vlan 10
```

A. client connecting to port fa0/1 with an 802.1x supplicant but fails authentication will be assigned to the vlan 100
B. client without an 802.1x supplicant connecting to port fa0/1 will be assigned to the vlan 10

C. client connecting to port fa0/1 with an 802.1x supplicant but fails authentication will be assigned to the vlan 10.
D. EAP over LAN frames will flow over VLAN 10
E. vlan 10, the guest vlan is also known as the restricted vlan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 262
Which of the following IP protocols and ports are commonly used in IPsec protocols?

A. IP protocols 50 and 51, UDP ports 500 and 4500
B. UDP ports 50, 51, 500, and 4500
C. TCP ports 50, 51, 500, and 4500
D. IP protocols 50, 51, 500, and 4500
E. IP protocols 50 and 51, UDP port 500, and TCP port 4500

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
TCP and UDP exist on Layer 4 of the OSI model. At this layer of the OSI model ports are used but not on Layer 3 which is were IP is used and data is identified with IP Addresses. In addition no protocols are listed only port numbers. Because of this A, D, & E are wrong.

An ISAKMP message is the payload of a (User Datagram Protocol) UDP message with the source and destination UDP ports set to 500 (or 4500). An ISAKMP message has an ISAKMP header and one or more ISAKMP payloads as defined in RFC 2408.

QUESTION 263
What does the command qos pre-classify enable in regard to implementing QoS over GRE/IPsec VPN tunnels?

A. copying the ToS field from the inner (original) IP header to the outer tunnel IP header
B. making a copy of the inner (original) IP header and running a QoS classification before encryption, based on fields in the inner IP header
C. classifying packets based on the ToS field in the inner (original) IP header
D. classifying packets based on the ToS field in the outer tunnel IP header
E. for the Cisco IOS classification engine to only see a single encrypted and tunneled flow to reduce classification complexity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 264
What is the net effect of using ICMP Type 4 messages to attack RFC 1122 compliant hosts?

A. Hosts will perform a "hard" TCP reset and tear down the connection.
B. Hosts will reduce the rate at which they inject traffic into the network.
C. Hosts will redirect packets to the IP address indicated in the ICMP type 4 message.
D. Hosts will perform a "soft" TCP reset and restart the connection.
E. Hosts will retransmit the last frame sent prior to receiving the ICMP type 4 message.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: Explanation
The Internet Control Message Protocol (ICMP) has many messages that are identified by a "type" field.

Type	Name	Reference
0	Echo Reply	[RFC792]
1	Unassigned	[JBP]
2	Unassigned	[JBP]
3	Destination Unreachable	[RFC792]
4	Source Quench	[RFC792]
5	Redirect	[RFC792]
6	Alternate Host Address	[JBP]
7	Unassigned	[JBP]
8	Echo	[RFC792]
9	Router Advertisement	[RFC1256]
10	Router Solicitation	[RFC1256]
11	Time Exceeded	[RFC792]
12	Parameter Problem	[RFC792]
13	Timestamp	[RFC792]
14	Timestamp Reply	[RFC792]
15	Information Request	[RFC792]
16	Information Reply	[RFC792]
17	Address Mask Request	[RFC950]
18	Address Mask Reply	[RFC950]
19	Reserved (for Security)	[Solo]
20-29	Reserved (for Robustness Experiment)	[ZSu]
30	Traceroute	[RFC1393]
31	Datagram Conversion Error	[RFC1475]
32	Mobile Host Redirect	[David Johnson]
33	IPv6 Where-Are-You	[Bill Simpson]
34	IPv6 I-Am-Here	[Bill Simpson]
35	Mobile Registration Request	[Bill Simpson]
36	Mobile Registration Reply	[Bill Simpson]
37	Domain Name Request	[RFC1788]
38	Domain Name Reply	[RFC1788]
39	SKIP	[Markson]
40	Photuris	[RFC2521]
41	ICMP messages utilized by experimental mobility protocols such as Seamoby	[RFC4065]
42-255	Reserved	[JBP]

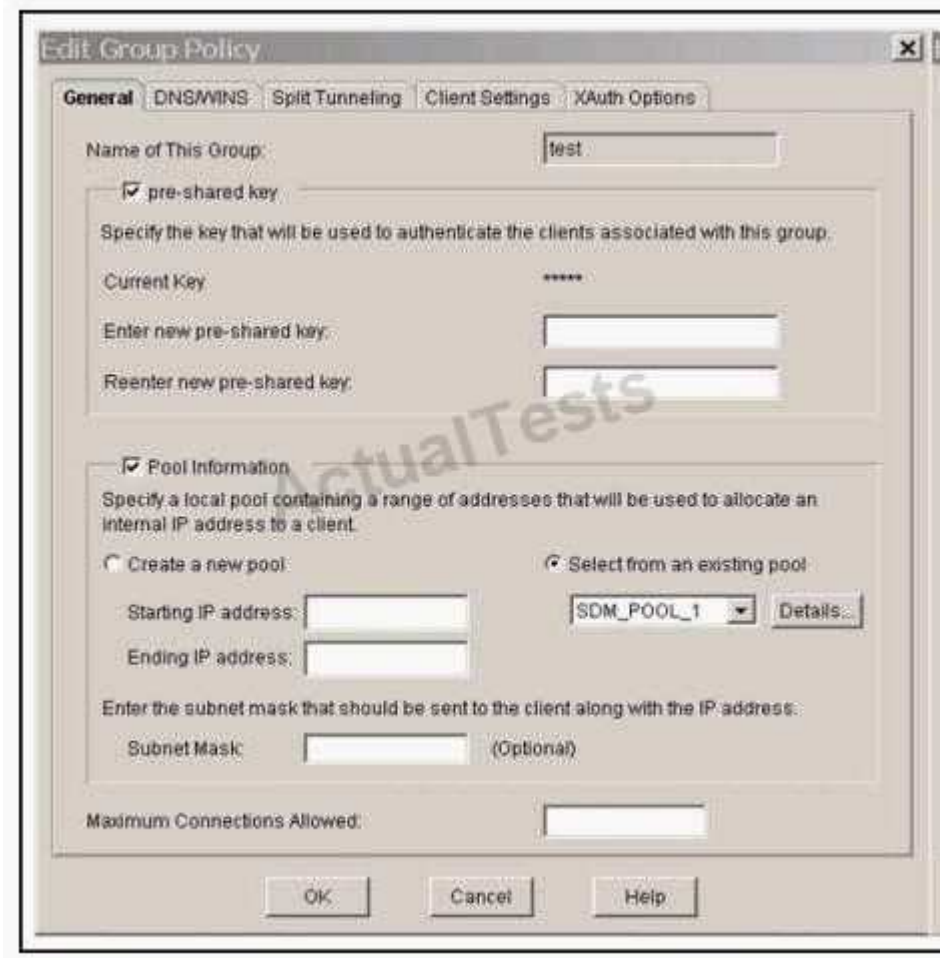
http://www.iana.org/assignments/icmp-parameters

1.1.1 Internet Hosts A host computer, or simply "host, " is the ultimate consumer of communication services. A host generally executes application programs on behalf of user(s), employing network and/or Internet communication services in support of this function. An Internet host corresponds to the concept of an "End-System" used in the OSI protocol suite [INTRO:13].

An Internet communication system consists of interconnected packet networks supporting communication among host computers using the Internet protocols. The networks are interconnected using packet-switching computers called "gateways" or "IP routers" by the Internet community, and "Intermediate Systems" by the OSI world [INTRO:13]. The RFC "Requirements for Internet Gateways" [INTRO:2] contains the official specifications for Internet gateways. That RFC together with
http://www.faqs.org/rfcs/rfc1122.html

The Source Quench is an Internet Control Message Protocol message which requests the sender to decrease the traffic rate of messages to a router or host. This message may be generated if the router or host does not have sufficient buffer space to process the request, or may occur if the router or host's buffer is approaching its limit.

QUESTION 265
Referring to the SDM screens shown, which two statements are true about the IOS Easy VPN Server configuration? (Choose two.)



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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 266
By default, to perform IPS deny actions, where is the ACL applied when using IOS-IPS?

A. To the ingress interface on which IOS-IPS is configured.
B. To the ingress interface of the offending packet.
C. To the egress interface on which IOS-IPS is configured.
D. To the egress interface of the offending packet

E. To the ingress interface of the offending packet and the ingress interface on which IOS-IPS is configured.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 267
The Risk Rating for an IPS signature is calculated using four primary components. Select the four components below.

A. Exploit Probability Rating
B. Attack Relevancy Rating
C. Target Value Rating
D. Alert Severity Rating
E. Signature Fidelity Rating

Correct Answer: BCDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 268
Which two statements are correct about the aaa authentication login default group tacacs+ local global configuration command? (Choose two.)

A. if the tacacs+ server fails to respond then the local database on the router will be used to authenticate the user
B. this login authentication method list is automatically applied to all lines except those that have a named method list explicitly defined.
C. "login" is the name of the method list being configured.
D. If the user fails the TACACS+ authentication then the local database on the router will be used to authenticate the user.
E. if the tacacs+ server is unavailable, authentication will succeed automatically by default.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 269
Which IOS QoS mechanism is used strictly to rate limit traffic destined to the router itself?

A. Single-Rate Policier.
B. Control Plane Policing
C. Dual-Rate Policier
D. Class-Based Policing

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 270
What is true about SYN cookies?

A. All TCP options are supported, such as large windows.
B. The server can have more than 8 unique MSS values
C. SYN cookies are implemented as a method of defending against SYN floods
D. SYN cookies are not implemented as a method of defending against SYN floods

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 271
You can view the number of packets (or flows) dropped because they do not conform to the Cisco ASA or PIX security policy by using which command?

A. show counters drop
B. show security-policy
C. show asp drop
D. show policy-map

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 272
Select the two correct statements from the list below that describe DES and 3DES :(Choose 2)

A. DES can only be used for encryption, whereas 3DES can also be used for authentication
B. The decryption operation for both DES and 3DES is the same as the encryption operation
C. 3DES is much more secure than DES
D. Both DES and 3DES are stream ciphers
E. DES uses 64 bit keys, although the effective key length is only 56 bits

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

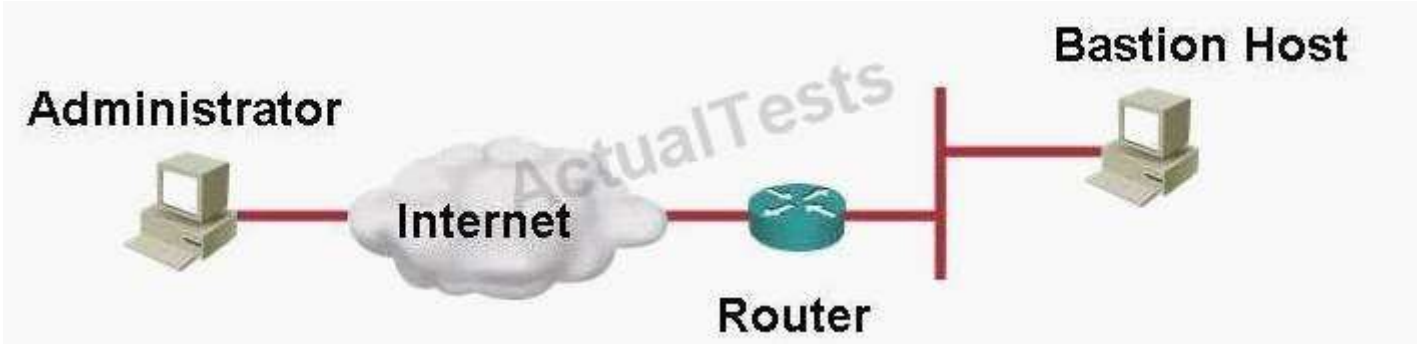
QUESTION 273
What is Chain of Evidence in the context of security forensics?

A. The concept that if a person has possession of evidence someone knows where the evidence is and can say who had it if it is not logged
B. The concept that evidence is controlled and accounted for as to not disrupt its authenticity and integrity.
C. The concept that the general whereabouts of evidence is known.
D. The concept that evidence is controlled in locked down, but not necessarily authenticated.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 274
Refer to the exhibit. The router in the exhibit only supports telnet access from the Bastion Host. The Bastion Host is running SSH. What option in SSH would allow the remote administrator to make a secure connection across the Internet to the route?

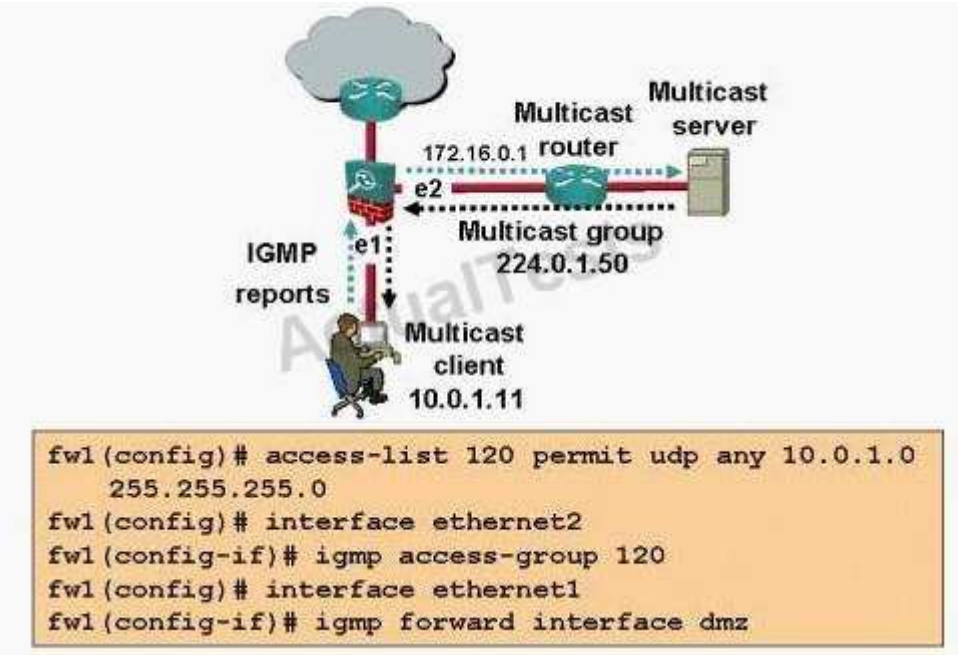


A. secure telnet option
B. port forwarding option
C. There are no options to accomplish this
D. telnet emulator option

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 275
A company just completed the rollout of IP/TV. The first inside network MC client to use the new feature claims they can not access the service. After re-viewing the above ASA Security appliance configuration and network diagram, the administrator was able to determine the following




```
fwl(config)# access-list 120 permit udp any 10.0.1.0
    255.255.255.0
fwl(config)# interface ethernet2
fwl(config-if)# igmp access-group 120
fwl(config)# interface ethernet1
fwl(config-if)# igmp forward interface dmz
```

A. The igmp access-group command was not correct and should be changed.
B. The access-list command was not correct and should be changed
C. The igmp forward command should be changed to igmp forward interface inside and applied to interface Ethernet 2
D. The ASA multicast configuration is correct, the configuration problem exists in the MC clients PC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
TCP/IP Access Lists
You can have up to 99 Standard IP Access Lists ranging in number from 1 to 99, the Extended IP Access Lists number range is assigned from 100 to 199. The most common use of the Extended IP access list to is create a packet filtering firewall. This is where you specify the allowed destinations of each packet from an allowed source.
UDP
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} udp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]]
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name]
In all software releases, the access-list-number can be 101 to 199. In Cisco IOS Software Release 12.0.1, extended ACLs begin to use additional numbers (2000 to 2699). These additional numbers are referred to as expanded IP ACLs. Cisco IOS Software Release 11.2 added the ability to use list name in extended ACLs.
The value of 0.0.0.0/255.255.255.255 can be specified as any. After the ACL is defined, it must be applied to the interface (inbound or outbound). In early software releases, out was the default when a keyword out or in was not specified. The direction must be specified in later software releases.
interface <interface>
ip access-group {number|name} {in|out}
This extended ACL is used to permit traffic on the 10.1.1.x network (inside) and to receive ping responses from the outside while it prevents unsolicited pings from people outside, permitting all other traffic.
interface Ethernet0/1
ip address 172.16.1.2 255.255.255.0
ip access-group 101 in
access-list 101 deny icmp any 10.1.1.0 0.0.0.255 echo

access-list 101 permit ip any 10.1.1.0 0.0.0.255

igmp access-group
To control the multicast groups that hosts on the subnet serviced by an interface can join, use the igmp access-group command in interface configuration mode. To disable groups on the interface, use the no form of this command.
igmp access-group acl
no igmp access-group acl

QUESTION 276
168

Which of the following is true with respect to active-active failover on the ASA ?

A. Active-active failover is available for systems running in multiple or single context mode
B. Active-active failover is available only for system running in multiple context mode
C. Active-active failover is available only for systems running in transparent mode
D. Active-active failover is available only for systems running in routed mode
E. Active-active failover is available only for systems running in single context mode

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 277
Choose the most correct statements about SMTP/ESMTP. (Choose 2)

A. ESMTP does NOT provide more security features than SMTP.
B. SMTP does provide authenticated email sending."
C. Open mail relays are often used for spamming.
D. Worms often spread via SMTP.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 278
Cisco IOS IPS sends IPS alert messages using which two protocols? (Choose two.)

A. FTP
B. SNMP
C. SYSLOG
D. LDAP
E. SMTP
F. SDEE

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 279
Which option describes the actions that can be taken when an IPS 5.x signature fires?

A. Deny Packet Inline - Produce Alert.
B. Produce Alert - Produce Detailed Alert
C. Drop Packet - Suppress Alert
D. Drop Connection - Drop Packet.
E. Block Connection - Generate SNMP Trap.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 280
Which statement below is true about the command "nat control" on the ASA?

A. It requires traffic passing through the firewall on interfaces of the security level to match a NAT translation rule.
B. It allows traffic originating from the inside interface to pass through the firewall on the outside interface without a NAT translation rule being matched.
C. It requires traffic originating from the inside interface to match a NAT translation rule to pass through the firewall on the outside interface.
D. It allows traffic originating from the outside interface to pass through the firewall on the inside interface without a NAT translation rule being matched.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 281
A server with IP address 209.165.202.150 is protected behind the inside interface of a Cisco ASA or PIX security appliance and the Internet on the outside interface. Users on the Internet need to access the server at any time, but the firewall administrator does not want to apply NAT to the address of the server because it is currently a public address. Which three of the following commands can be used to accomplish this? (Choose three.)

A. nat (inside) 1 209.165.202.150.255.255.255.255
B. static (inside, outside) 209.165.202.150.209.165.202.150 netmask 255.255.255.255
C. no nat-control
D. access-list no-nat permit ip host 209.165.202.150 anynat(inside) 0 access-list no-nat
E. nat (inside) 0 209.165.202.150.255.255.255.255

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 282
In ISO 27001 ISMS what are the main certification process phases required to collect information for ISO 27001?

A. Observation
B. Certification audit
C. Post-audit
D. Discover
E. Major compliance.
F. Pre-audit

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 283
What group in Cisco IOS does 1536-bit Diffie-Hellman prime modulus equivalent too?

A. group 1
B. group 5
C. group 7
D. group 3

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 284
Which can control the per-user authorization of commands on a company router?

A. RADIUS
B. TACACS+
C. IPSec
D. AAAA

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 285
How could you deny telnet access to the aux port of your router?

A. access-list 52 deny 0.0.0.0 255.255.255.255 line aux 0 access-class 52 in
B. access-list 52 deny 0.0.0.0 255.255.255.255 line aux 0 access-group 52 in
C. There is no telnet access to the aux port.
D. You cannot do this.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 286
Which one of the following Cisco ASA adaptive security appliance rule samples will send HTTP data to the AIP-SSM module to evaluate and stop HTTP attacks?

```
access-list inside_mpc_in extended permit tcp any any eq 80
class-map inside-class
    match access-list inside_mpc_in

policy-map inside-policy
  class inside-class
    deep-packet inline fail-open

service-policy inside-policy interface inside
```

```
access-list inside_mpc_in extended permit tcp any any eq 80
class-map inside-class
    match access-list inside_mpc_in

policy-map inside-policy
  class inside-class
    ips inline fail-open

service-policy inside-policy interface inside
```

```
access-list inside_mpc_in extended permit udp any any eq 80
class-map inside-class
    match access-list inside_mpc_in

policy-map inside-policy
  class inside-class
    ips inline fail-open

access-list inside_mpc_in extended permit tcp any any eq 80
class-map inside-class
    match access-list inside_mpc_in
```

```
policy-map inside-policy
  class inside-class
    ids inline fail-open

service-policy inside-policy interface inside
```

A. Exhibit A

B. Exhibit B
C. Exhibit C
D. Exhibit D

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 287
In Unix, where are failed super-user level access attempts stored?

A. /var/adm/sulog
B. /var/adm/wtmp
C. /etc/adm/sulog
D. /etc/wtmp

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 288
What Cisco IOS feature examines packets received to make sure that the source address and interface are in the routing table and match the interface that the packet was received on?

A. Unicast RPF
B. Dynamic access-lists
C. lock-and-key
D. ip audit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 289
You want to filter traffic using IOS firewall (CBAC). Your traffic is HTTP, TFTP, and TELNET. You create an inspection rule with the command "ip inspect name ccie tcp" and apply it to the Ethernet interface with the command "ip inspect ccie in". Which of the following are correct? (Select all that apply)

A. HTTP through the firewall is enabled.
B. IPP through the firewall is enabled.
C. TFTP through the firewall is enabled.
D. None of these are enabled. There is more to do.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 290
What command is used to set the TACACS+ server and its encryption key, in the Cisco IOS?

A. tacacs-server host; tacacs-server key
B. ip tacacs-server host; ip tacacs-server key
C. tacacs-server host; tacacs-server password
D. aaa tacacs-server host; aaa tacacs-server key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 291
Your BGP router receives two routes. Both of their next hops are reachable, neither has a weight set, RA has a larger local preference but a longer AS path than RB. Which route is the BEST BGP route?

A. RA, as it has a larger local preference.
B. RB, as it has a shorter AS path.
C. Neither route.
D. Both routes are best.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 292
During IKE negotiation, how do two peers compare policies? And what must policies match? (Select all that apply)

A. Remote compares its local from highest (smallest numbered) to lowest (highest numbered),
B. Remote compares its local from highest numbered to lowest numbered.
C. Policies must match encryption, hash, authentication, Diffie-Hellman values, and lifetime < or equal.
D. Policies must match hash, IPSec key, authentication, lifetime < or equal, and Diffie-Hellman values.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 293
What traffic is allowed through the following access-list (select the best answer)?

```
access-list 2000 permit ip host 10.1.1.1 host 10.2.2.2
access-list 2000 deny ip any any
```

```
access-list 2000 permit ip any any log
```

A. All traffic is allowed through.
B. All traffic from host 10.1.1.1 to host 10.2.2.2 is allowed through.
C. All traffic from host 10.2.2.2 to host 10.1.1.1 is allowed through.
D. No traffic is allowed through.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 294
Without a CA, what would you have to configure on each router, whenever a new router was added to the network?

A. Keys between the new router and each of the existing routers.
B. RSA private keys.
C. Access-lists
D. Security associations.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 295
In Unix, what is syslogd? And what does it do?

A. The system logging facility daemon - takes log entries and performs the action configured in the /etc/syslog.conf file.
B. The network time protocol daemon - keep track of time synchronization between servers.
C. The synchronization protocol server - syncs files.
D. The system logging facility daemon - purges system log entries from the system log so that it doesn't grow too large.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 296
How many useable hosts can you get from a /30 subnet mask?

A. 2
B. 4
C. 8
D. 30

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 297
Crypto maps do which of the following? (Select all that apply)

A. Define whether sa's are manual or via IKE.
B. Define the transform set to be used.
C. Define who the remote peer is.
D. Define the local address.

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 298
How do you change EAP from running in its default mode?

A. ppp eap local
B. ppp eap proxy
C. eap local
D. ppp eap nas

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 299
Exhibit:

```
aaa new-model
aaa authentication login default group radius
aaa authorization exec default group radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Look at the attached exhibit. After this configuration is in place, you point your web browser to your router's IP address. What username password combination should you use?

A. The one from your RADIUS server.
B. The one from your TACACS+ server.
C. Your local authentication credentials.
D. There will be no authentication.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 300
Which of these access-lists allow DNS traffic?

A. access-list 101 permit udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53
B. access-list 101 permit udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 123
C. access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2049
D. access-list 101 permit tcp 0.0.0.0 255.255.255.255 B.B.13.2 0.0.0.0 eq 23

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 301
If you want to use RADIUS authentication, must you configure AAA?

A. RADIUS
B. No, AAA is not required to use RADIUS, just use the "ip auth radius" commands
C. Yes, you must configure AAA to use TACACS+, Kerberos, or RADIUS.
D. No, AAA is for authentication, authorization, and accounting. It is not required to configure

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 302
SWA has a priority of 8192 while SWB has a priority of 32768. Which switch will be root _why?

A. SWA, it has the lowest priority.
B. SWB, it has the highest priority.
C. Neither, it will be determined by the lowest MAC address.
D. Neither, it will be determined by the lowest cost to the root switch.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 303
What does a PIX do with tcp sequence number to minimize the risk of tcp sequence number attacks? (Select all that apply)

A. Randomize them.
B. Make sure they are within an acceptable range.
C. Doesn't use them.
D. Uses the same numbers over and over again

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 304
Traffic is flowing from the inside to the outside. You are using an output access-list (outbound access-list) along with NAT. What IP addresses should be referenced in the access-list?

A. Outside (global) addresses
B. Inside (local) addresses
C. Encrypted addresses
D. Private addresses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 305
Which of the following are valid av-pairs on a RADIUS server?

A. rte-fltr-out#0="router igrp 60"
B. user = georgia {login = cleartext labservice = ppp protocol = ip {addr-pool=bbb} }
C. cisco-avpair = "ip:addr-pool=bbb"
D. route#1 = "3.0.0.0 255.0.0.0 1.2.3.4"

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 306
What is RADIUS? (Select all that apply)

A. Remote Authentication Dial-In User Services
B. "A distributed client/server system that secures networks against unauthorized access"
C. A secret-key network authentication protocol.
D. A modular security application that provides centralized validation of users attempting to gain access to a router or network access server

Correct Answer: AB
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 307
In RFC 2138 (RADIUS), vendor specific attributes (VSA) are specified. Specifically, this is called VSA 26 (attribute 26). These allow vendors to support their own extended options. Cisco's vendor ID is 9. Which of the following commands tell the Cisco IOS to use and understand VSA's? (Select all that apply)

A. radius-server vsa send
B. radius-server vsa send authentication
C. radius-server vsa send accounting
D. ip radius-server vsa send

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 308
In your company's network, a Cisco adaptive security appliance is running in multiple context mode. Multiple contexts are associated with the ingress interface. As a network technician of your company, can you tell me which three actions will be taken by the security appliance to classify packets into a context? (Choose three.)

A. looking at the destination interface IP address for traffic destined to an interface
B. looking at the source interface IP address for traffic sourced from an interface
C. looking at static commands where the global interface matches the ingress interface of the packet
D. looking at IP addresses identified by a global pool for the ingress interface by use of the global command

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 309
Your RADIUS server is at IP address 172.22.53.201 and the authentication key is "Cisco". AAA has not yet been configured on your router. What is the minimum number of commands you can type to tell your router about your RADIUS server? (Select all that apply)

A. aaa new-model radius-server host 172.22.53.201 auth-port 1545 acct-port 1546 key Cisco
B. radius-server host 172.22.53.201 key cisco
C. aaa new-model
D. radius-server host 172.22.53.201 auth-port 1545 acct-port 1546 key cisco

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 310
When a Cisco Secure Intrustion Detection System Sensor communicates with a Cisco Secure Instrustion Detection System Director, what statement is FALSE?

A. If the preferred route is down, up to 255 alternate listed routes can be attempted
B. When the sensor to director is detected as "down", packets lost during this time are buffered and retransmitted. The packets are dropped only when the buffer is full.
C. The communication occurs via the postofficed system
D. When no keepalives are detected, eventd on the sensor e-mails the administrator.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 311
The main reason the NFS protocol is not recommended for use across a firewall or a security domain is that.

A. it is UDP based. As a result, its state is difficult to track.
B. This protocol uses a range of ports, and firewalls have difficulty opening the proper entry points to allow traffic.
C. File permissions are easily modified in the requests, and the security of the protocol is not stringent.
D. Industry technicians do not understand NFS well, but is actually appropriate to run across various security domains.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 312
Why it is important to delete IPSec Security Associations (SAs) frequently and then re-key and reestablish the SA's?

A. To reduce the chance that another IPSec machine on the network will generate the same random SPIf which will cause confusion as to which machine is the endpoint of a tunnel.
B. To reduce the risk of a brute force attack where your key can be compromised if it stays the same for too long period of a time.
C. Each time a SA is regenerated, the integrity of the link is checked. This is the only way to establish if the tunnel is still active.
D. To reduce the potential problems of counters exceeding their allocated size, which will cause them to wrap back to zero and display invalid results.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 313
What command sequence should be used to turn on RADIUS in a router?

A. aaa new-modelaaa authen login default radius radius-server host #.#.#.# radius-server key <key>
B. aaa new-modelaaa authen login default radius radius-server host #.#.#.#
C. radius-server host #.#.#.# radius-srever key <key> aaa authen login default radius aaa new- model
D. radius-server host #.#.#.# radius-server use-extended login radius

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 314
Routers running OSPF and sharing a common segment become neighbors on that segment. What statement regarding OSPF neighbors is FALSE?

A. The Primary and Secondary addresses on an interface allow the router to belong to different areas at the same time.
B. All routes must agree on the stub area flag in the ISPF Hello Packets.
C. Neighbors will fail to form an adjaceny if thei Hello and Dead intervals differ, .
D. Two routers will not become neighbors if the Area-ID and Authentication password do not mathc.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 315
If the read community is known and there is SNMP connectivity to a device (without an access-list limiting this):

A. The System Description (sysDescr), which includes the full name and version identification of the system's hardware type, software operating-system, and networking software, can be ascertained through and SNMP query.
B. The entire configuration of the router can be read but not modified.
C. The passwords on the router can be modified.
D. The passwords on the router can be read, not modified. This enables the attacker to access the router as a base of operations for other attacks.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 316
IPS signatures are stored in which format?

A. Post Office

B. RDEP
C. IDCONF
D. SDEE

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 317
Which of the following aptly describes the Unix file /etc/shadow?

A. The Unix file/etc/shadow is referenced by login when the /etc/passwd file contains an asterisk in the third field.
B. The Unix file/etc/shadow is referenced by NIS when the /etc/passwd file contains a line with the first character of '+'.
C. The Unix file/etc/shadow is a place to store encrypted passwords without referencing the /etc/passwd file.
D. The Unix file/etc/shadow is a read-protected file referenced by login when the /etc/passwd file contains a special character in the second field.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 318
What statement about AH and ESP is FALSE?

A. ESP encapsulates the IP header, while AH does not.
B. ESP uses protocol 50.
C. AH uses protocol 51.
D. AH does not lent itself to a NAT environment becayse of IP header encapsulation.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 319
A switch has been configured to support MuitiLayer Switching (MLS). In addition, Access Control Lists on the MLS-Route Processor have been configured to block all FTP traffic destined to the Internet. What flow mask will be used to create each shortcut?

A. Application flow mask
B. Full flow mask
C. Destination-Source flow mask
D. Destination flow mask

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
185

Explanation:

QUESTION 320
What is the term used to describe an attack that falsifies a broadcast ICMP echo request and includes a primary and secondary victim?

A. Fraggle Attack
B. Man in the Middle Attack
C. Trojan Horse Attack
D. Smurf Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 321
When configuring IPSec with IKE, if the transform set includes an ESP cipher algorithm, specify the cipher keys. In a Cisco IOS IPsec transform set, which two of the following items are valid for ESP cipher algorithms?(Choose two.)

A. esp-null, esp-seal
B. esp-aes 256, esp-aes null
C. esp-null, esp-aes 512
D. esp-aes 192, esp-des, esp-3des

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 322
If the result of an attack left an ARP table in the state below, what address would you suspect of launching the attack?

```
Internet 171.16.1.100 - 000c.5a35.3c77 ARPA FastEthernet0/0
Internet 171.16.1.111 0 00bc.d1f5.f769 ARPA FastEthernet0/0
Internet 171.16.1.112 0 00bc.d1f5.f769 ARPA FastEthernet0/0
Internet 171.16.1.113 3 00bc.d1f5.f769 ARPA FastEthernet0/0
Internet 171.16.1.114 0 00bc.d1f5.f769 ARPA FastEthernet0/0
```

A. 171.16.1.100
B. 171.16.1.111
C. 171.16.1.112
D. 171.16.1.113

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 323
What would be a reason to decrease the security association lifetime on a router?

A. To ease the workload on the router CPU and RAM
B. To give a potential hacker less time to decipher the keying
C. To improve Perfect Forward Secrecy (PFS)
D. If the lifetime of the peer router on the other end of the tunnel is shooter, the lifetime on the local router must be decreased so that the SA lifetime of both routers is the same.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 324
The no ip directed-broadcast command is useful in preventing SMURF style attacks for the following reason:

A. It prevents your network device from being a target
B. It prevents your network device from launching an attack.
C. It prevents your network device from being a reflector in an attack
D. It prevents your network device from being traced as the source of an attack.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 325
IDS tuning requires a step-by-step methodology in order to successfully tuje ISD signatures effectively. Put the following tuning steps for a new sensor into their proper order.

A. Identify critical assets that require monitoring and protection.
B. Update sensors with new signatures.
C. Let sensors operate for a period of time generating alarms using the default configuration.
D. Apply initial configuration.
E. Selectively implement response actions.
F. Connect sensors to network.
G. Analyze alarms and tune out false positives.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 326
The newly appointed trainee technician wants to know what the purpose of Lock _Key is. What will your reply be?

A. Lock _Key secures the console port of the router so that even users with physical access to the router cannot gain access without entering the proper sequence.
B. Lock _Key permits Telnet to the router and have temporary access lists applied after issuance of the access-enable command.
C. Lock _Key require additional authentication for traffic traveling through the PIX for TTAP compliance.
D. Lock _Key is to prevent users from getting into enable mode.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 327
The company network administrator has forgotten the enable password of the router. There are no users logged into the router, but all passwords on the router are encrypted.

What can the administrator do to recover the enable secret password?

A. The administrator can reboot the router, press the BREAK key during boot up, and boot the router into ROM Monitor mode to erase the configuration, and re-install the entire configuration as it was saved on a TFTP server.
B. The administrator can call the Cisco Technical Assistance Center (TAC) for a specific code that will erase the existing password.
C. The administrator can reboot the router, press the BREAK key during boot up, boot the router into ROM Monitor mode to either erase or replace the existing password, and reboot the router as usual.
D. The administrator should erase the configuration, boot the router into ROM Monitor mode, press the BREAK key, and overwrite the previous enable password with a new one.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 328
The newly appointed trainee technician wants to know what the definition of exploit signatures is in the context of Intrustion detection. What will your reply be?

A. Exploit Signatures are policies that prevent hackers from your network.
B. Exploit Signatures are security weak points in your network that are open to exploitation by intruders.
C. Exploit Signatures are identifiable patterns of attacks detected on your network.
D. Exploit Signatures are digital graffiti from malicious users.

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 329
Which of the following services would you advice the new trainee technician to enable on ISO firewall devices?

A. SNMP with community string public.
B. TCP small services.
C. UDP small services
D. Password-encryption.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 330
The newly appointed trainee technician wants to know what PFS (Perfect Forward Security) requires. What will your reply be?

A. AH
B. ESP
C. Another Diffie-Hellman exchange when an SA has expired
D. Triple DES

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 331
Using Ciscos' Security Device manager on an IOS router, what functions could you expect the security audit option to do for you?

A. Scan for and report open ports.
B. Report IOS vulnerabilities.
C. List identiflcable configuration problems and suggest recommendations for fixing them.
D. Configure LAN and WAN interfaces with IP addresses and security related commands

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 332
The comapny network is using Cisco Secure Intrustion Detection System and the network traffic pattern appears ordinary. However, numerous false positives for a particular alarm are received. What

can you do to avoid the quantity of "noise" in the future?

A. Click the unmanage for the alarm in QUESTION NO: in the HP OpenView/NR GUI interface.
B. Click the acknowledge for the alarm in QUESTION NO: in the HPOV/NR GUI interface.
C. You can use ventd to decrease the alarm level severity
D. You could configure a decreases alarm level severity through nrconfigure.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 333
What does "counting to infinity" mean in a Distance Vector protocol environment?

A. "counting to infinity" means calculating the time taken for a protocol to converge.
B. "counting to infinity" means checking that the number of route entries do not exeed a set upper limit.
C. "counting to infinity" can occur when Split Horizon is not enabled.
D. "counting to infinity" means setting an upper limit for hop count, to break down routing loops if this limit is reached.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 334
Which network management software installation is a prerequisite for the Cisco Secure Intrustion Detection System Director software?

A. CiscoWorks 2000 on Unix
B. SunNetManager on Solaris
C. Microsoft Internet Information Server on Windows NT
D. NetSonar on Linux

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 335
The newly appointed trainee technician wants to know if one can change the situation where every time a typing mistake is made at the exec prompt of a router, the message from the router indicates a lookup is being performed. Also, there is a waiting period of several seconds before the next command can be typed. What will your reply be?

A. No, this is a default feature of Cisco IOS software.
B. Yes, by using the no ip domain-lookup command
C. Yes, by using the no ip helper-address command.

D. Yes, by using the no ip multicast helper-map command

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 336
How does Cisco Secure Intrustion Detection System sensor behave when it detects unauthorized activity?

A. Cisco Secure Intrustion System sensor will send an e-mail to the network administrator.
B. Cisco Secure Intrustion System sensor will send an alarm to Cisco Secure Intrustion Detection System Director.
C. Cisco Secure Intrustion System sensor will shut down the interface where the traffic arrived, if device management is configured.
D. Cisco Secure Intrustion System sensor will perform a traceroute to the attacking device.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 337
Why do scanning tools may report a root Trojan Horse compromise when it is run against an IOScomponent?

A. IOS is based on BSD UNIX and is thus subject to a Root Trojan Horse compromise.
B. The scanning software is detecting the hard-coded backdoor password in IOS.
C. Some IOS versions are crashable with the telnet option vulnerability.
D. The port scanning package mis-parses the IOS error messages.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 338
The PIX firewall allows users to block Java when using what combination of keywords and implementation?

A. "no cafebabe" in a static
B. "no Java" in a static
C. "no cafebabe" in an outbound list
D. "filter Java" in an outbound list

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 339
What can be used to solve a problem situation where a user's PC is unable to ping a server located on a different LAN connected to the same router?

A. Ensure routing is enabled.
B. A default gateway from the router to the server must be defined
C. Check to see if both the PC and the server have properly defined default gateways
D. Both the server and the PC must have defined static ARP entries.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 340
What happens when one experiences a ping of death?

A. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP) and the "type" field in the ICMP header is set to 18 (Address Mask Reply).
B. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP), the Last Fragment bit is set, and (IP offset' 8) + (IP data length) >65535. In other words, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8-byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
C. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP) and the source equal to destination address.
D. This is when an the IP header is set to 1 (ICMP) and the "type" field in the ICMP header is set to 5 (Redirect).

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 341
What response will a RADIUS server send to a client to indicate the client's user name or password is invalid?

A. Authentication Denied
B. Access-Reject
C. Access-Deny
D. Access-Fasil

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 342
Mail Server A is trying to contact Mail Server B behind a firewall. Mail Server A makes the initial connection, but there is a consistent long delay (1 minute) before the queued mail is actually sent. A reason for this might be:

A. Mail Server A does not have a default route.
B. Mail Server B does not have a default route
C. The firewall is blocking TCP port 113.
D. A third Mail Server is delaying the traffic.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 343
What would be the biggest challenge to a hacker writing a man-in-the-middle attack aimed at VPN tunnels using digital certificates for authentication?

A. Programmatically determining the private key so they can proxy the connection between the two VPN endpoints.
B. Determining the ISAKMP credentials when passed to establish the key exchange.
C. Determining the pase two credentials used to establish the tunnel attributes.
D. Decrypting and encrypting 3DES once keys are known.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 344
Which best describes a common method used for VLAN hopping?

A. Using VTP to configure a switchport to sniff all VLAN traffic
B. Appending an additional tag to an 802.1Q frame such that the switch forwards to packet to the embedded VLAN ID
C. Flooding the VLAN with traffic containing spoofed MAC addresses in an attempt to cause the CAM table to overflow
D. Spoofing the IP address of the host to that of a host in the target VLAN

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 345
The newly appointed trainee technician wants to know where Kerberos is mainly used. What will your reply be?

A. Session-layer protocols, for data integrity and checksum verification.
B. Application-layer protocols, like Telnet and FTP.
C. Presentation-layer protocols, as the implicit authentication system for data stream or RPC.
D. Transport and Network-layer protocols, for host to host security in IP, UDP, or TCP.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 346
Which of the following statements regarding Certificate Revocation List (CRL) is valid when using PKI?

A. The CRL resides on the CA server and is built by querying the router or PIX to determine which clients' certificate status in the past.
B. The CRL is used to check presented certificates to determine if they are revoked.
C. A router or PIX will not require that the other end of the IPSec tunnel have a certificate if the crl optional command is in place.
D. The router's CRL includes a list of clients that have presented invalid certificates to the router in the past.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 347
What is the rationale behind a Network Administrator wanting to use Certificate Revocation Lists (CRLs) in their IPSec implementations?

A. CRLs allow netwotk administrators the ability to do "on the fly" authentication of revoked certificates.
B. They help to keep a record of valid certificates that have been issued in their network
C. CRLs allow network administrators to deny devices with certain certificates from being authenticated to their network.
D. Wildcard keys are much more efficient and secure. CRLs should only be used as a last resort.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 348
What sets the FECN bit in Frame Relay?

A. The Frame Relay network, to inform the DTE receiving the frame that congestion was experienced in the path form source to destination.
B. The Frame Relay network, in frames traveling in the opposite direction from those frames that encountered congestion.
C. The receiving DTE, to inform the Frame Relay network that it is overloaded and that the switch should throttle back.

D. The sending DTE, to inform the Frame Relay network that it is overloaded and that the switch should throttle back

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

196

QUESTION 349
Under which of the following circumstances will Network Address Translation (NAT) not work well?

A. With outbound HTTP when AAA authentication is involved.
B. With traffic that carries source and/or destination IP addresses in the application data stream.
C. With ESP Tunnel mode IPSec traffic.
D. When PAT (Port Address Translation) is used on the same firewall.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 350
Generally speaking which of the following could be done to mitigate a Day Zero host or server attack?

A. Install software that prevents actions such as buffer overflows and writes to the system directory.
B. Deploy Intrustion Detection on all switches that directly connect to hosts or servers. C. Install Virus scanning software.
C. Ensure that your hosts and servers all have the latest security patches.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 351
The newly appointed company trainee technician wants to know how a route running Certificate Enrollment Protocol (CEP) obtains a certificate. What will your reply be?

A. The router administrator should send an e-mail message to 'sysadmin@icsa.net'. This message should request a certificate and include the FQDN of the device.
B. If using Cisco IDS version 11.3 or 12.0, the router administrator should enter the following configuration: crypto ca identity <registered_ca_name> enrollment ftp:// <cetificate_authority>
C. The router administrator has to copy the certificate from the peer router at the other end of the tunnel and then paste it onto the local router.
D. If using Cisco IOS version 11.3 or 12.0, the router administrator should enter the following configuration: crypto ca identify <registered_ca_name> enrollment http:// <certificate authority>

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 352
The addresses on the inside of a packet-filtering router are configured from the network 10.0.0.0/8. Which of the following access-list entries on the outside gateway router would prevent spoof attacks to this network?

A. access-list 101 deny ip 10.0.0.0 0.0.0.255 0.0.0.0 255.255.255.255
B. access-list 101 deny ip 10.0.0.0 255.0.0.0 0.0.0.0 0.0.0.0
C. access-list 101 deny ip any 10.0.0.0 255.255.255
D. access-list 101 deny ip 10.0.0.0 0.255.255.255 any

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 353
Below are four "out" access-lists, configured on an interface.

What list will block an IP packet with source address 144.23.67.94, destination address 197.55.34.254, destination TCP port 23 from leaving the routr?

A. access-list 100 deny ip tcp 144.23.67.0 0.0.0.7 eq telnet 197.55.34.240 0.0.0.15 eq telnet access-list 100 permit ip any any
B. access-list 100 deny tcp 144.23.67.94 0.0.0.7 any eq telnetaccess-list 100 permit ip 197.55.34.240 0.0.0.15 eq telnet any
C. access-list 100 deny tcp 144.23.67.96 0.0.0.7 eq telnet 197.55.34.240 0.0.0.15access-list 100 permit ip any any
D. access-list 100 deny ip 144.23.67.94 0.0.0.7 host 144.23.67.94access-list 100 permit ip any any

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 354
A router is connected to a serial link with a protocol MTU of 512 bytes.

If the router receives an IP packet containing 1024 bytes, it will: (Select two)

A. Always drop the packet.
B. Fragment the packet, also, the router at the other side of the serial link will reassemble the packet.
C. Drop the packet if the DF bit is set.
D. Fragment the packet and sent it, also, the destination will reassemble the packet when it arrives.

Correct Answer: CD

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 355
The primary benefit of RSA encrypted nonces over RSA signatures is:

A. The do not require a certificate authority.
B. The offer repudiation.
C. They are not subject to export control
D. There is better scalability for multiple peers.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 356
The CEO of a tech company want to know which security programs can effectively protect your network against password sniffer programs? (Choose three.)

A. IPSec, due to it encrypting data.
B. RLOGIN, because it does not send passwords.
C. Kerberos, due to encrypt password abilities.
D. One time passwords, because the passwords always change.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 357
Which of the following is a description of the principle on which a Denial of Service (DoS) attack works?

A. MS-DOS and PC-DOS operating systems using a weak security protocol.
B. Overloaded buffer systems can easily address error conditions and respond appropriately.
C. Host systems are incapable of responding to real traffic, if they have an overwhelming number of incomplete connections (SYN/RCVD State).
D. All CLIENT systems have TCP/IP stack compromisable implementation weaknesses and permit them to launch an attack easily.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 358

When using a sniffer directly connected to an access switch, the sniffer sees an excessive amount of BPDUs with the TCA bit set. Which are the most likely explanations?

A. There are no problems in the network.
B. Ports connecting to workstations do not have spanning tree portfast configured.
C. Bad cabling is being used in the network.
D. The CPU utilization on the root switch is getting up to 99% and thus not sending out any BPDUs.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 359
Which three methods best describe a secure wireless LAN implementation? (Choose three.)

A. Deploy WEP using a static 128 bit key.
B. Deploy dynamic key management.
C. Deploy mutual authentication between access point and client.
D. Deploy mutual authentication between authentication server and client.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 360
You are performing device management with a Cisco router. Which of the following is true?

A. The Cisco Secure Intrustion Detection System sensor can apply access-list definition 198 and 199 (default) to the router in response to an attack signature.
B. The Cisco Secure Intrustion Detection System sensor can shut down the router interface in response to an attack signature.
C. The Cisco Secure Intrustion Detection System sensor can emit an audible alarm when the Cisco router is attached.
D. The Cisco Secure Intrustion Detection System sensor can modify the routing table to divert the attacking traffic.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 361
The network administrator was requested to make a script with the following criteria:

- Must be owned by the root and executable by a group of users other than the root.
- Must not give other users root privileges other than execution of the script.
- Must not allow the users to modify the script.

Which of the following would be the best way to accomplish this task?

A. Having the root use 'chmod 4755 <name_of_script>' to make it readable and executable by non-root users or the use 'chmod u-s <name_of_script>'.
B. By having the users logged in under their own ID's, typing 'su' and inputting the root password after they have been given the root password, then executing the script.
C. Changing permissions to read-write and changing ownership of the script to the group.
D. By having root use 'chmod u-s <name_of_script>'.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 362
Multicast addresses in the range of 224.0.0.0 through 224.0.0.244 are reserved for:

A. Administratively Scoped multicast traffic that is intended to reamin inside of a private network and is never intended to be transmitted into the Internet.
B. Global Internet multicast traffic intended to travel throughout the Internet.
C. Link-local multicast traffic consiting of network control messages that never leave the local subnet.
D. Any valid multicast data stream.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 363
You are the network administrator of the company. Can you tell me, which is the first step to establish PPP communications over a link?

A. The switch sends NCP frames to negotiate parameters such as data compression and address assignment.
B. The originating node sends configuration request packets to negotiate the LCP layer.
C. One or more Layer 3 protocols are configured.
D. The originating node sends Layer 3 data packet to inform the receiving node's Layer 3 process.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 364
Which of the following commands must be present on the router (exact syntax would depend on the version) for the user with priviledge level 15 (as defined in their TACACS+ profile) to be dropped into enabled mode immediately when that user telnets into a Cisco router?

A. The global command: aaa authorization exec [default] [group] tacacs- 202

B. The line command: logon authorization tacacs+
C. The global command: privilege 15 enable
D. The global command: aaa authentication enable default tacacs+

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

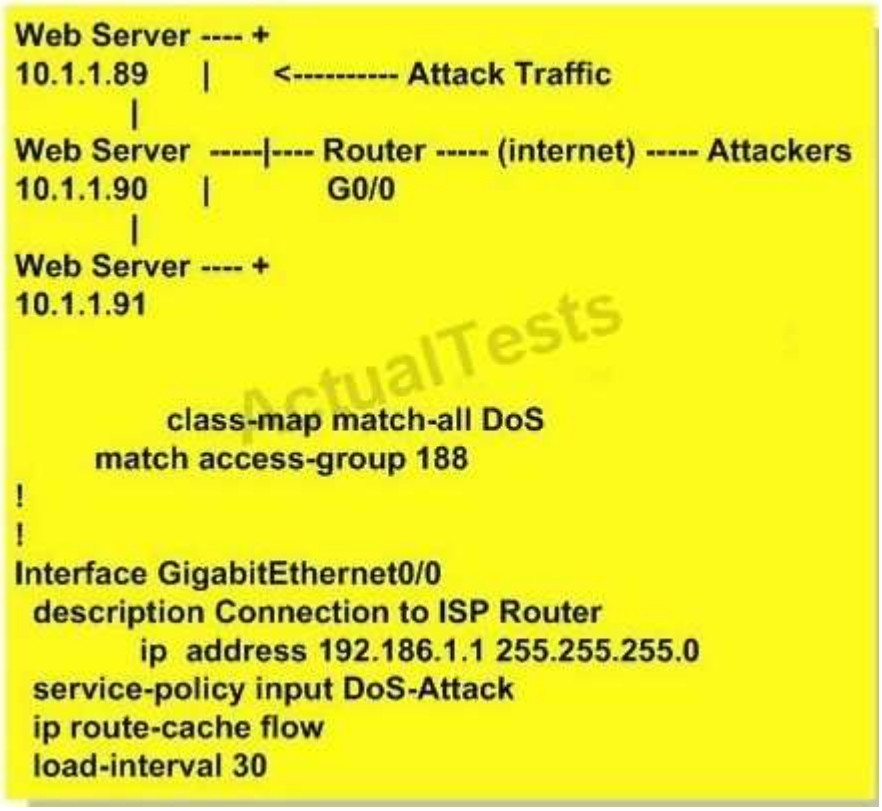
QUESTION 365
Under which circumstances will the Diffie-Hellman key exchange allows two parties to establish a shared secret key? (Choose all that apply.)

A. Over an insecure medium.
B. After the termination of a secure session.
C. Prior to the initiation of a secure session.
D. After a session has been fully secured.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 366
Based on the displayed network diagram and configuration. You are hosting a web server at 10.1.1.90, which is under a denial of service attack. Use NBAR to limit web traffic to that server at 200 kb/s. Which configuration is true to complete the NBAR configuration?



A. policy-map DoS-Attackclass DoSpolice cir 200 bc 200 be 200conform-action transmit exceed- action dropviolate-action drop!access-list 188 permit tcp any host 10.1.1.90 eq www
B. policy-map dropclass DoSpolice conform-action transmit exceed-action drop
C. policy-map dropclass DoSpolice cir 200000 bc 37500 be 75000conform-action transmitexceed- action dropviolate-action drop!access-list 188 permit tcp any host 10.1.1.90 eq www
D. policy-map DoS-Attackclass DoSpolice cir 200000 bc 37500 be 75000conform-action transmitexceed-action dropviolate-action drop!access-list 188 permit tcp any host 10.1.1.90 eq www

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 367
When a user initiales a dailup PPP logon to a Cisco router running RADIUS, what attributes are sent to the RADIUS server for authentication? (assume a PAP password)

A. Username (1), user service (7), PAP Password (8)
B. Username (1), user service (7), Filter ID (11), Login port(16), reply message (18), Vendor Specific Attribute (26)
C. Username (1), CHAP password (3)
D. Username (1), PAP Password (2), NAS-ip (4), NAS-port (5), NAS port type (61), user service (7), framed protocol (6)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 368
You are the network administrator. Two remote LANs connected via a serial connection are exchanging routing updates via RIP. An alternate path exists with a higher hop count. When the serial link fails, you receive complaints of users regarding the time it takes to transfer to the alternate path. How will you ameliorate this situation?

A. You could change the hop count on an alternate path to be the same cost.
B. You could reduce or disable the holdown timer by making use of the timers basic command.
C. You could increase the bandwidth of the alternate serial connection.
D. You could configure a static route with the appropriate administratice cost via the alternate route.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 369
When using MD5 authentication in BGP where is the hash passed in the IP packet?

A. The payload packet of a BGP request and response.
B. In a TCP header flagged with an option 19.
C. A specially defined BGP authentication packet.
D. In a UDP header flagged with an option 16.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 370
Which of the following statements is NOT accurate regarding frame Relay?

A. Frame Relay does not provide error recovery.
B. Frame Relay provides error detection.
C. Frame Relay is high-speed, shared bandwidth protocol.
D. Frame Relay is based on a "packet-over-circuit" architecture.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 371
Which of the following represents the correct ways of releasing IBGP from the condition that all IBGP neighbors need to be fully meshed? (Choose all that apply.)

A. Configure route reflectors
B. Configure IBGP neighbors several hops away
C. Configure confederations
D. Configure local preference

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 372
A security System Administrator is reviewing the network system log files. He notes the following:

- Network log files are at 5 MB at 12:00 noon.
- At 14:00 hours, the log files at 3 MB.

What should he assume has happened and what should he do about the situation?

A. He should contact the attacker's ISP as soon as possible and have the connection disconnected.
B. He should log the event as suspicious activity, continue to investigate, and take further steps according to site security policy.
C. He should log the file size, and archive the information, because the router crashed.
D. He should run a file system check, because the Syslog server has a self correcting file system problem.
206

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 373
What reaction can be expected from the host when a router sends an ICMP packet, with the Type 3 (host unreachable) and Code 4 (DF bit set) flags set, back to the originating host?

A. The host should reduce the size of future packets it may send to the router.
B. This scenario is not possible because the packet will be fragmented and sent to the original destination.
C. The sending station will stop sending packets, due to the router not expecting to see the DF bit in the incoming packet.
D. The sending station will clear the DF bit and resend the packet.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 374
Suppose a client calls and advises you that an FTP data transaction is not allowing him to view the host??s directory structure. What are the most likely causes of the problem? (Choose all that apply.)

A. The client??s username/password is wrong.
B. The client??s FTP data port is not connected.
C. The host machine has denied him access because the password is wrong.
D. An access list is stopping port 20 from detailing the directory list.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 375
Which of the following statements is true regarding SSL?

A. Every packet sent between host and client is authenticated.
B. Encryption is used after a simple handshake is completed.
C. SSL uses port 2246.
D. SSL is not a predefined standard.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 376
In IPSec, what encapsulation protocol only encrypts the data and not the IP header?

A. ESP
B. AH
C. MD5
D. HASH

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 377
What can be drawn from the following syslog message receive by an administrator from his adaptive security appliance?

```
%ASA-6-201010 Embryonic connection limit exceeded 200/200 for inbound packet from
209.165.201. 10/1026 to 10. 1. 1. 1.20/80 on interface outside
```

A. The client at 209.165.201.10 has been infected with a virus.
B. The server at 10.1.1.20 is under a SYN attack.
C. The server at 10.1.1.20 is under a smurf attack.
D. The server at 209.165.201.10 is under a smurf attack.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 378
Birthday attacks are used against which one of the following?

A. symmetric ciphering
B. asymmetric ciphering
C. hash algorithms
D. digital signatures

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

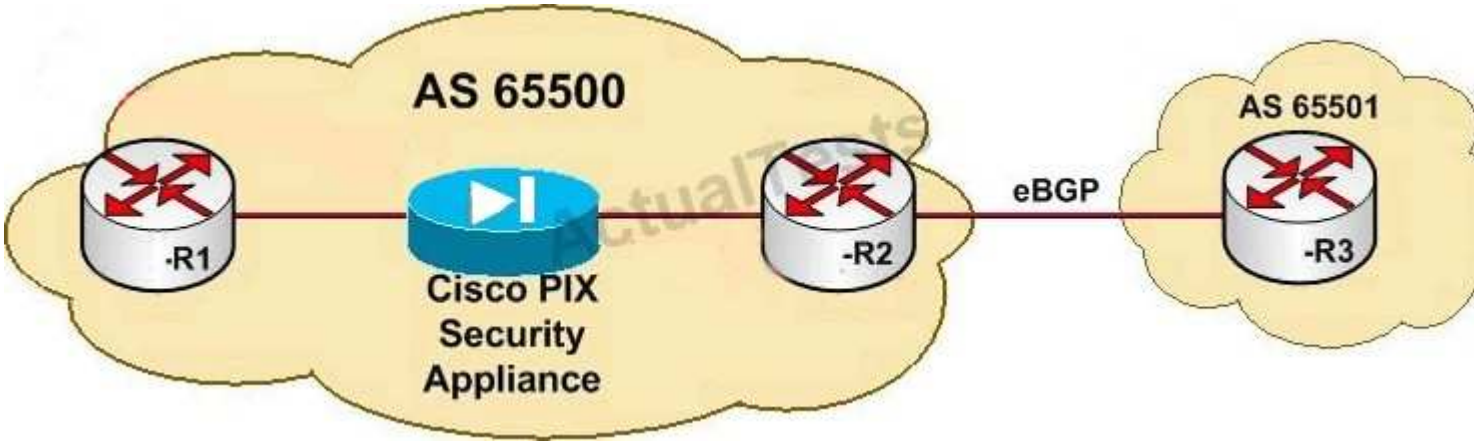
QUESTION 379
Which of the following is AH??s destination IP port?

A. 23
B. 21
C. 50
D. 51

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 380
You work as a network engineer, study the exhibit carefully. Your company has just configured Cisco security appliance between R1 and R2 to enhance security and apply advanced protocol inspection. Unluckily, BGP stopped working after inserting the appliance in the network. How to restore BGP connectivity? (Choose three.)



A. Configure BGP on the security appliance as an IBGP peer to R1 and R2 in AS 65500.
B. Configure a static NAT translation to allow inbound TCP connections from R2 to R1.
C. Configure an ACL on the security appliance allowing TCP port 179 between R1 and R2.
D. Configure a static route on R1 and R2 using the appliance inside and outside interfaces as 209

gateways.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 381
In Cisco PIX Firewall Software version 7.0 and later, which command replaced the fixup protocol commands?

A. secure <protocol>
B. fixup protocol commands did not change in version 7.0
C. inspect <protocol>
D. audit <protocol>

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

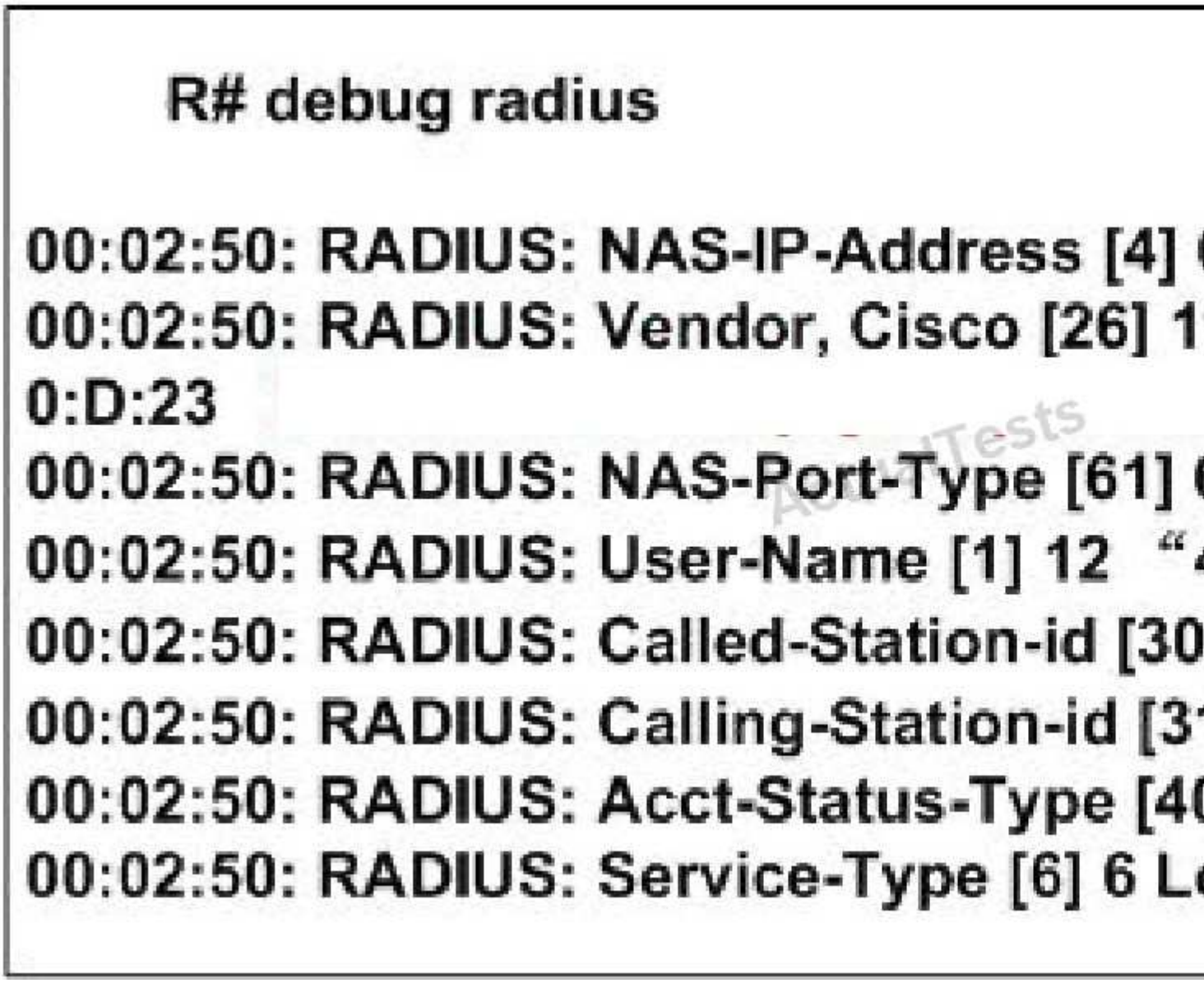
QUESTION 382
Certificate Enrollment Process (CEP) runs over what TCP port number? (Choose the best two answers.)

A. Same as HTTP
B. Port 80
C. Port 50
D. Port 51

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 383
On the basis of the partial debug output displayed in the exhibit, which value is contained inside the brackets [4] in line 1?



A. RADIUS VSA number
B. RADIUS attribute type value
C. RADIUS VSA length
D. RADIUS identifier field value

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 384
What definition best describes Kerberized?

A. A general term that refers to authentication tickets
B. An authorization level label for Kerberos principals

C. Applications and services that have been modified to support the Kerberos credential infrastructure
D. A domain consisting of users, hosts, and network services that are registered to a Kerberos server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 385
Which three statements best describe how DNSSEC prevents DNS cache poisoning attacks from succeeding? (Choose three.)

A. DNSSEC utilizes DS records to establish a trusted hierarchy of zones.
B. DNSSEC signs all records with domain-specific keys.
C. DNSSEC introduces KEY records that hold domain-specific public keys
D. DNSSEC deprecates CNAME records and replaces them with DS records.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 386
Which two of the following can you configure an IPS sensor with three sniffing interfaces as? (Choose two.)

A. three promiscuous sensors
B. two inline sensors, one promiscuous sensors
C. one inline sensor, one promiscuous sensor
D. three inline sensors

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 387
What definition best describes a key distribution center when Kerberos is applied to a network?

A. A general term that refers to authentication tickets
B. An authorization level label for Kerberos principals
C. Applications and services that have been modified to support the Kerberos credential infrastructure
D. A Kerberos server and database program running on a network host

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 388
Examine the following items, what are the header sizes for point-to-point and multipoint GRE with tunnel key?

A. 8 bytes for both
B. 4 bytes and 8 bytes respectively
C. 24 bytes for both
D. 4 bytes for both

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 389
Which three statements are correct concerning private address space? (Choose three.)

A. Private address space is defined in RFC 1918.
B. These IP addresses are considered private:10.0.0.0 172.15.0.0 192.168.0.0
C. Private address space is not supposed to be routed over the Internet.
D. Using only private address space and NAT to the Internet is not considered as secure as having a stateful firewall.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 390
Which of the following protocols does TACACS+ support?

A. PPP
B. AppleTalk
C. NetBIOS
D. All the above

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 391
What is SDEE?

A. a queuing mechanism to store alerts
B. a protocol used by multiple vendors to transmit IDS events across the network
C. a mechanism to securely encode intrusion events in an event store

D. a Cisco proprietary protocol to transfer IDS events across the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 392
Which two statements are true concerning NAT? (Choose two.)

A. NAT is only useful for TCP/UDP and ICMP traffic.
B. NAT provides one-to-one address mapping.
C. NAT provides one-to-many address mapping.
D. NAT can be used for all IP traffic.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 393
What versions of TACACS does Cisco IOS support? (Select the best three answers.)

A. TACACS+
B. TACACS
C. Extended TACACS
D. Extended TACACS+

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 394
Which command can be used to globally disable the requirement that a translation rule must exist before packets can pass through the firewall?

A. access-list
B. no nat-control
C. global <interface> 0
D. nat <interface> 0

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 395
Which two statements are attributed to stateless filtering? (Choose two.)

A. It can look at sequence numbers to validate packets in flow
B. It must process every packet against the inbound ACL filter
C. The first TCP packet in a flow must be a SYN packet.
D. It can be used in asymmetrical traffic flows.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 396
What algorithm initiates and encrypts a session between two routers?? exchange keys between two encryption devices?

A. Routing algorithm
B. Diffie-Hellman algorithm
C. The switching engine

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 397
You are a network engineer, can you tell me how do TCP SYN attacks take advantage of TCP to prevent new connections from being established to a host under attack?

A. taking advantage of the host transmit backoff algorithm by sending jam signals to the host
B. filling up a host listen queue by failing to ACK partially opened TCP connections
C. incrementing the ISN of each segment by a random number, causing constant TCP retransmissions
D. sending multiple FIN segments, forcing TCP connection release

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 398
Select three RFC 1918 addresses. (Choose three.)

A. 0.0.0.0/8
B. 10.0.0.0/8
C. 172.16.0.0/12
D. 192.168.0.0/16

Correct Answer: BCD

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 399
An administrator notices a router??s CPU utilization has jumped from 2 percent to 100 percent, and that a CCIE engineer was debugging. What IOS command can the network administrator enter to stop all debugging output to the console and vty lines without affecting users on the connected router?

A. no logging console debugging
B. undebug all
C. line vty 0 4 no terminal monitor
D. reload the router

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 400
When implementing WLAN security, what are three benefits of using the TKIP instead of WEP? (Choose three.)

A. TKIP uses an advanced encryption scheme based on AES.
B. TKIP provides authentication and integrity checking using CBC-MAC.
C. TKIP provides per-packet keying and a rekeying mechanism.
D. TKIP provides message integrity check.
E. TKIP reduces WEP vulnerabilities by using a different hardware encryption chipset.
F. TKIP uses a 48-bit initialization vector.

Correct Answer: CDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Topic 5, Volume E

QUESTION 401
SSL stands for Secure Sockets Layer, though IETF has renamed it TLS (Transport Layer Security). TLS is documented in RFC 2246 and identifies itself in the protocol version field as SSL 3.1. When initiating a new SSL/TLS session, the client receives the server SSL certificate and validates it. What does the client use the certificate for after validating it?

A. The server creates a separate session key and sends it to the client. The client has to decrypt the session key using the server public key from the certificate.
B. The client creates a separate session key and encrypts it with the server public key from the certificate before sending it to the server.
C. Nothing, the client and server switch to symmetric encryption using IKE to exchange keys.
D. The client generates a random string, encrypts it with the server public key from the certificate, and sends it

to the server. Both the client and server derive the session key from the random data sent by the client.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 402
After entering debug ip packet, no messages appear on your Telnet session. What is the likely cause?

A. OSPF routing is required.
B. The console port does not support debug output.
C. The terminal monitor command is required.
D. IP packets are not supported with the debug command.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 403
Comparing symmetric ciphers to asymmetric ciphers, which statement is not correct?

A. Symmetric ciphers are less computationally intensive.
B. Asymmetric ciphers are in general more difficult to break.
C. Asymmetric ciphers require a shared secret called the private key.
D. Symmetric ciphers are faster.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 404
Which two statements indicate how Cisco IPS Sensor Software Version 5.0 differs from Version 4.0? (Choose two.)

A. The sensor pushes events to the monitoring system.
B. The sensor supports intrusion prevention functionality
C. The monitoring system pulls events from the sensor.
D. The sensor software calculates a risk rating for alerts to reduce false positives.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 405
On the basis of the Cisco ASA Software Version 7.x configuration. Which scenario best describes the reason you would deploy this configuration on your Cisco ASA adaptive security appliance?

A. to ensure that any HTTP session that has a URL with the string "X-Counter" or "X-Session" is reset and logged
B. to ensure that HTTP traffic follows RFC compliance
C. to ensure that any HTTP session that has a URL with the string "X-Counter" or "X-Session" is blocked and logged
D. to ensure that connections from any custom web applications that use "X-Counter" or "X- Session" are reset and logged

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 406
When managing a Cisco IOS device by use of Cisco SDM, which configuration statement is necessary to be able to use Cisco SDM?

A. ip http server
B. ip http secure-server sdm location X.X.X.X
C. ip http secure-server
D. ip http serversdm location X.X.X.X

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 407
SNMP is restricted on Cisco routers by what IOS command?

A. snmp-server enable
B. snmp-server community string
C. snmp-server ip-address
D. snmp-server no access permitted

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 408
Which two statements best describe the reason that TACACS+ is more desirable from a security standpoint than RADIUS? (Choose two.)

A. It encrypts the password field with a unique key between server and requester.
B. It uses TCP as its transport
C. It uses UDP as its transport.
D. Encrypting the whole data payload is optional.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 409
Which three statements are correct concerning AES? (Choose three.)

A. AES is faster to compute than 3DES.
B. AES is not subject to known-plaintext attacks, while DES is subject to them.
C. AES is a block cipher, while 3DES and DES are stream ciphers.
D. AES can be used with longer keys than 3DES.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 410
The AS5300 series router can support which of the following incoming connections?

A. Voice
B. Dialup users via PSTN
C. ISDN
D. All the above

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 411
Which statement is true about a hash function?

A. a reversible value computed from a piece of data and used to detect modifications
B. an irreversible fast encryption method
C. a reversible fast encryption method
D. an irreversible value computed from a piece of data and used to detect modifications

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 412
If an administrator can't use Cisco ASDM to connect to a Cisco ASA or PIX security appliance, which items must be checked? (Choose four.)

A. The user IP address is permitted in the interface ACL.
B. The HTTP server is enabled.
C. The HTTPS server is enabled.
D. The user IP address is permitted in the HTTP statement.
E. The ASDM file resides in flash memory
F. The asdm image command exists in the configuration

Correct Answer: BDEF
Section: (none)
Explanation

Explanation/Reference:
221

Explanation:

QUESTION 413
Place the following steps in the correct order for PPP callback, as specified in RFC 1570.

1. A PC user (client) connects to the Cisco access server.
2. The Cisco IOS Software validates callback rules for this user/line and disconnects the caller for callback.
3. PPP authentication is performed.
4. Callback process is negotiated in the PPP link control protocol (LCP) phase.
5. The Cisco Access Server dials the client.

A. 1, 2, 3, 4, 5
B. 1, 3, 2, 5, 4
C. 1, 4, 5, 3, 2
D. 5, 4, 3, 2, 1

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 414
The Cisco Security MARS appliance offers attack mitigation using which two methods? (Choose two.)

A. automatically pushing ACLs to Layer 3 devices to block attacker traffic
B. automatically pushing commands to Layer 2 switches to shut down attacker ports
C. automatically resetting attacker TCP connections
D. recommending ACLs to be manually pushed to Layer 3 devices such as routers and firewalls
E. operating as an inline appliance, it automatically blocks malicious traffic inline
F. working in conjunction with CSM to block attacker traffic inline

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 415
TACACS+ authentication uses which three packet types? (Choose three.)

A. ACCESS REQUEST
B. ACCESS ACCEPT
C. CONTINUE
D. CHALLENGE
E. REPLY
F. START

Correct Answer: CEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 416
If two Cisco routers are configured for HSRP and one router has a default priority of 100 and the other 99, which router assumes the role of active router?

A. The default priority cannot be 100.
B. The router with a higher priority.
C. The router with the lowest priority.
D. Neither router because Cisco routers do not support HSRP; only clients do.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 417
Which statement correctly describes a hybrid crypto system?

A. uses symmetric crypto for proof of origin
B. uses asymmetric crypto for message confidentiality
C. uses symmetric crypto for fast encryption and decryption
D. uses symmetric crypto for key distribution

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 418
Which two commands are needed to implement a Cisco Catalyst 6500 Series FWSM? (Choose two.)

A. module x secure-traffic
B. firewall module x vlan-group y
C. firewall multiple-vlan-interfaces
D. firewall vlan-group

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 419
Which of the following are the four possible states of spanning tree?

A. Listening, learning, blocking, broadcasting
B. Listening, learning, blocking, connecting
C. Discovering, learning, blocking, connecting
D. Listening, learning, blocking, forwarding

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 420
When applying MD5 route authentication on routers running RIP or EIGRP, which two important key chain considerations should be accounted for? (Choose two.)

A. The lifetimes of the keys in the chain should overlap.
B. Key 0 of all key chains must match for all routers in the autonomous system.
C. Routers should be configured for NTP to synchronize their clocks.

D. No more than three keys should be configured in any single chain

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 421
Why should a Route Reflector be used in a BGP environment?

A. Route Reflector is used to overcome issues of split-horizon within BGP.
B. Route Reflector is used to reduce the number of External BGP peers by allowing updates to reflect without the need to be fully meshed.
C. Route Reflector is used to allow the router to reflect updates from one Internal BGP speaker to another without the need to be fully meshed.
D. Route Reflector is used to divide Autonomous Systems into mini-Autonomous Systems, allowing the reduction in the number of peers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 422
Which of the following statements are true? (Choose two.)

A. RC4 is a stream cipher.
B. DES and 3DES are stream ciphers.
C. AES is a block cipher
D. Stream ciphers require padding

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 423
Which of the following types of traffic is NOT subject to inspection in the 105 Firewall Feature Set?

A. ICMP
B. FTP
C. TFTP
D. SMTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 424
Which two statements best describe the SSH protocol? (Choose two.)

A. SSH version 1 supports DSA public key algorithm but not RSA.
B. There are structural weaknesses in SSH version 1 which leave it open to attacks.
C. SSH version 1 only supports DES or 3DES.
D. SSH version 2 also supports Secure FTP

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 425
What functionality best defines the use of a 'stub' area within an OSPF environment?

A. A stub area appears only on remote areas to provide connectivity to the OSPF backbone.
B. A stub area is used to inject the default route for OSPF.
C. A stub area uses the no-summary keyword to explicitly block external routes, defines the non- transit area, and uses the default route to reach external networks.
D. A stub area is used to reach networks external to the sub area.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 426
Cisco Security Agent can protect a host from which three attack points according to its default policy? (Choose three.)

A. a buffer overflow followed by an attempt to run code off of the stack on the Cisco Security Agent-protected host
B. a new application that is attempting to run for the first time after being downloaded from the Internet on a Cisco Security Agent-protected host
C. a process trying to create a new file on a Cisco Security Agent-protected host
D. vulnerability scanning against the host running the Cisco Security Agent

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 427
According to RFC 3180, what is the correct GLOP address for AS 456?

A. 224.4.86.0
B. 239.2.213.0
C. 233.1.200.0
D. 224.0.4.86

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 428
Which three of the following are attributes of the RADIUS protocol? (Choose three.) Select 3 response (s).

A. encrypts the password
B. hashes the password
C. uses UDP as the transport
D. uses TCP as the transport
E. combines authentication and authorization in a single request
F. commonly used to implement command authorization

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 429
Which two of the following statements are true about Cisco IOS IPS functionality?

A. The signatures available are built into the Cisco IOS code.
B. To update signatures, you need to install a new Cisco IOS image.
C. To activate new signatures, you can download a new signature definition file from the Cisco website.
D. Loading and enabling selected IPS signatures is user-configurable.
E. Cisco IOS Software only provides intrusion detection functionality.
F. Cisco IOS IPS requires a network module running sensor software to be installed in your router.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 430
What is the main reason for using the ip ips deny-action ips-interface Cisco IOS command?

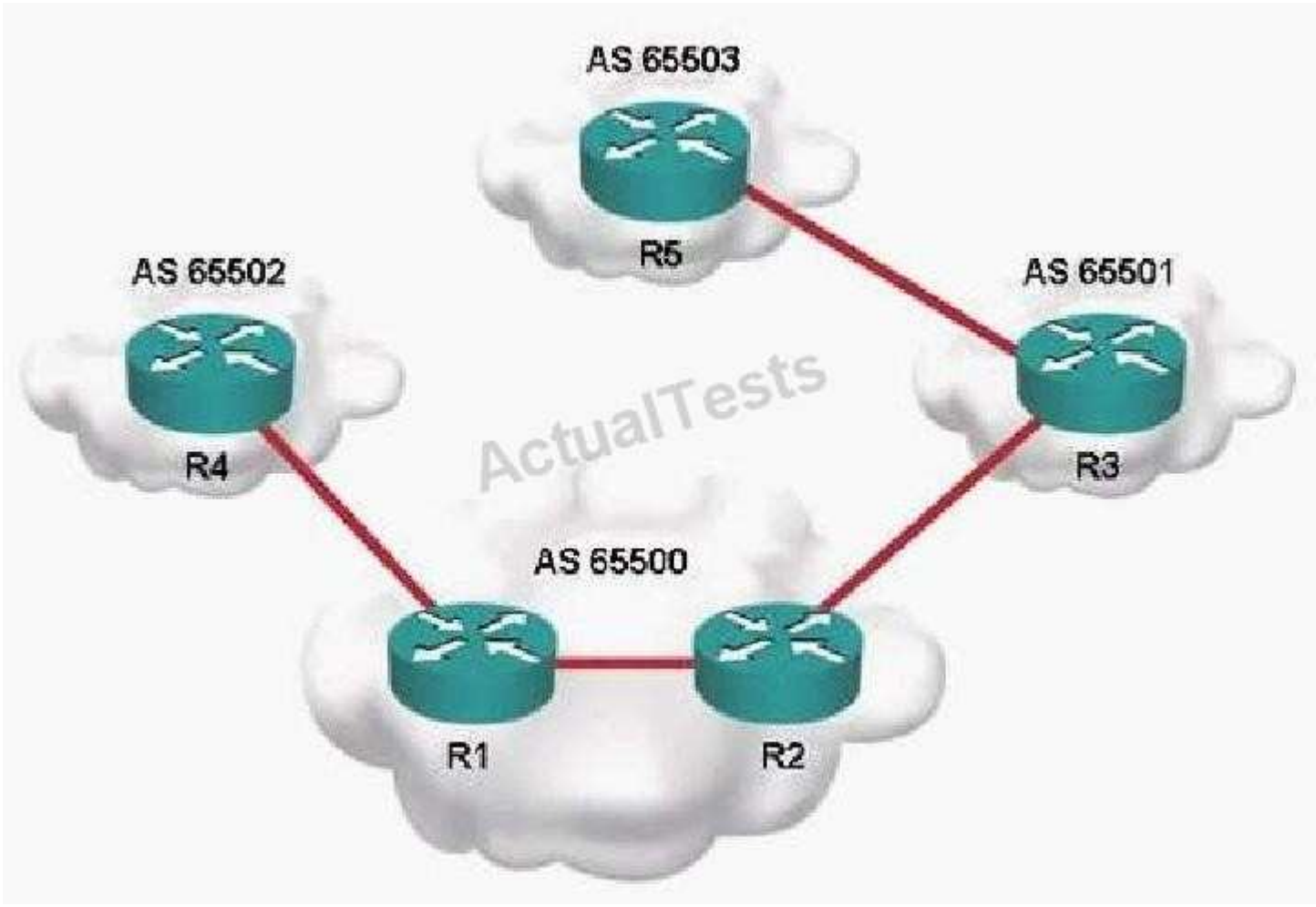
A. to selectively apply drop actions to specific interfaces
B. to enable Cisco IOS to drop traffic for signatures configured with the drop action
C. to support load-balancing configurations in which traffic can arrive via multiple interfaces

D. not a valid Cisco IOS command

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 431
Refer to the exhibit.



Which as-path access-list regular expression should be applied on R2 as a neighbor filter list to only allow updates with an origin of AS 65503? Select the best response.

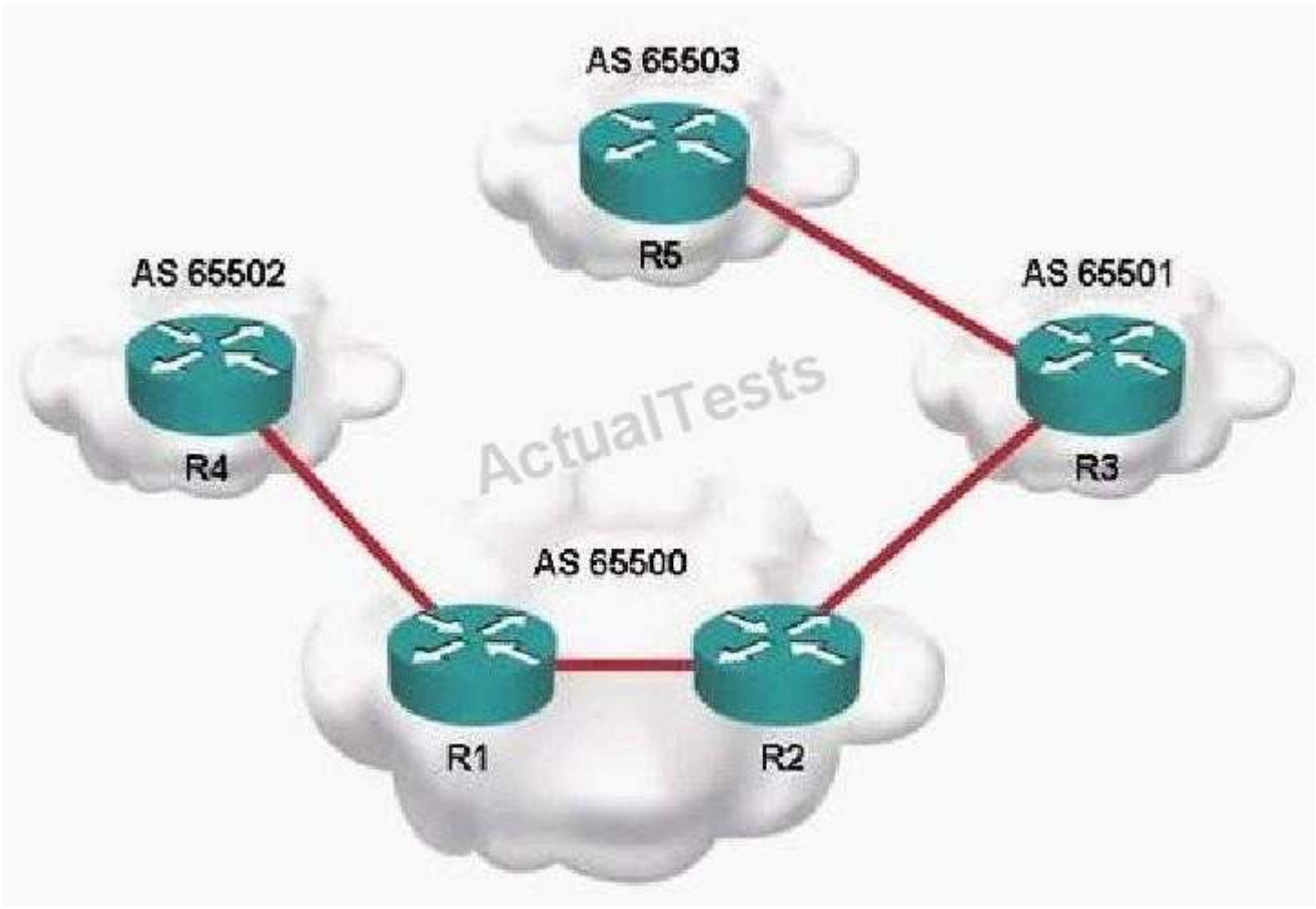
A. 65503
B. _65503_
C. ^65503$
D. _65503$
E. ^65503 .*
F. _65503.?$

Correct Answer: E

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 432
Refer to the exhibit.



Which as-path access-list regular expression should be applied on R2 to only allow updates originating from AS 65501 or autonomous systems directly attached to AS 65501?

Select the best response.

A. _65501_.*
B. _65501_*$
C. ^65501_*$
D. _65501+[0.9]$
E. ^65501_[0-9]*$
F. \[0-9]*+65501_+\[0-9]$

Correct Answer: E
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 433
Cisco ASA or PIX security appliance software version 7.0 introduced Modular Policy Framework as an extensible way to classify traffic, and then apply policies (or actions) to that traffic. MPF, at a minimum, requires which three commands? Select the best response.

A. http-map, tcp-map, class-map
B. class-map, tcp-map, policy-map
C. class-map, policy-map, service-map
D. class-map, service-policy, policy-map

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 434
With active/active failover in a load-balanced environment, which of the following optional failover commands is needed to ensure that traffic is automatically load-balanced after a reload of either appliance?

Select the best response.

A. join-failover-group x
B. preempt
C. failover group x
D. No additional command is needed.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 435
Two routers running Cisco IOS Software are failing to negotiate the IPsec tunnel. Crypto debugs reveal the following messages:

```
1d00h: IPSec(validate_transform_proposal): proxy identities not supported 1d00h:
ISAKMP: IPSec policy invalidated proposal 1d00h: ISAKMP (0:2): SA not acceptable!
```

What is the most likely cause of the error message? Select the best response.

A. Crypto access lists are not mirrored on each side.
B. The crypto-map is incomplete.
C. ISAKMP policies have attributes that do not match.
D. This is not an error message, but an indication that proxy IDs are not supported.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 436
Which addresses below would be valid IP addresses of hosts on the Internet? (Multiple answer)

A. 235.1.1.1
B. 223.20.1.1
C. 10.100.1.1
D. 127.0.0.1
E. 24.15.1.1

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 437
On an Ethernet LAN, a jam signal causes a collision to last long enough for all other nodes to recognize that:

A. A collision has occurred and all nodes should stop sending.
B. Part of a hash algorithm was computed, to determine the random amount of time the nodes should back off before retransmitting.
C. A signal was generated to help the network administrators isolate the fault domain between two Ethernet nodes.
D. A faulty transceiver is locked in the transmit state, causing it to violate CSMA/CD rules.
E. A high-rate of collisions was caused by a missing or faulty terminator on a coaxial Ethernet network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 438
A Network Administrator is trying to configure IPSec with a remote system. When a tunnel is initiated from the remote end, the security associations (SAs) come up without errors. However, encrypted traffic is never send successfully between the two endpoints. What is a possible cause?

A. NAT could be running between the two IPSec endpoints
B. A mismatched transform set between the two IPSec endpoints
C. There is a NAT overload running between the two IPSec endpoints
D. Mismatched IPSec proxy between the two IPSec endpoints

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 439
A SYN flood attack is when:

A. A target machine is flooded with TCP connection requests with randomized source address & ports for the TCP ports.
B. A target machine is sent a TCP SYN packet (a connection initiation), giving the target host's address as both source and destination, and is using the same port on the target host as both source and destination.
C. A TCP packet is received with the FIN bit set but with no ACK bit set in the flags field.
D. A TCP packet is received with both the SYN and the FIN bits set in the flags field.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 440
What kind of interface is not available on the Cisco Secure Intrusion Detection System sensor?

A. Ethernet
B. Serial
C. Token Ring
D. FDDI

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 441
How is data between a router and a TACACS+ server encrypted?

A. CHAP Challenge responses
B. DES encryption, if defined
C. MD5 has using secret matching keys
D. PGP with public keys

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 442
A gratuitous ARP is used to: (Multiple answer)

A. Refresh other devices' ARP caches after reboot.
B. Look for duplicate IP addresses.

C. Refresh the originating server's cache every 20 minutes.
D. Identify stations without MAC addresses.
E. Prevent proxy ARP from becoming promiscuous.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 443
To restrict SNMP access to a router, what configuration command could be used?

A. snmp-server community
B. snmp-server public
C. snmp-server password
D. snmp-server host

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 444
TFTP security is controlled by: (Multiple answer)

A. A default TFTP directory.
B. A username/password.
C. A TFTP file.
D. A pre-existing file on the server before it will accept a put.
E. File privileges.

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 445
Which statements are true about RIP v1? (Multiple answer)

A. RIP v1 is a classful routing protocol.
B. RIP v1 does not carry subnet information in its routing updates.
C. RIP v1 does not support Variable Length Subnet Masks (VLSM).
D. RIP v1 can support discontiguous networks.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 446
Exhibit:

```
S* 0.0.0.0/0 [1/0] via 172.31.116.65
D 172.16.0.0/24 [90/48609] via 10.1.1.1
R 172.16.0.0/16 [120/4] via 192.168.1.4
```

A router has the above routers listed in its routing table and receives a packet destined for 172.16.0.45. What will happen?

A. The router will not forward this packet, since it is destined for the 0 subnet.
B. The router will forward the packet though 172.31.116.65, since it has the lowest metric.
C. The router will forward the packet through 10.1.1.1.
D. The router will forward the packet through 172.31.116.65, since it has the lowest administrative distance.
E. The router will forward the packet through 192.168.1.4.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 447
In the Cisco Secure Intrusion Detection System/HP OpenView interface, a "yellow" sensor icon would mean:

A. A "yellow" sensor icon means that a sensor daemon had logged a level 4 or 5 alarm.
B. A "yellow" sensor icon means that the director that the sensor reports to is operating in degraded mode.
C. A "yellow" sensor icon means that a sensor daemon had logged a level 3 alarm.
D. A "yellow" sensor icon means that the device that the sensor detected being attacked is inoperative due to the attack.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 448
What is the first thing that must be done to implement network security at a specific site?

A. Hire a qualified consultant to install a firewall and configure your router to limit access to known traffic.
B. Run software to identify flaws in your network perimeter.
C. Purchase and install a firewall to protect your network.
D. Install access-control lists in your perimeter routers, so you can ensure that only known traffic is getting through your router.
E. Design a security policy.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 449
What would be the best reason for selecting L2TP as a tunnel protocol for a VPN Client?

A. L2TP uses TCP as a lower level protocol so the transmissions are connected oriented, resulting in more reliable delivery.
B. L2TP uses PPP so address allocation and authentication is built into the protocol instead of relying on IPSecextended functions, like mode config and a-auth.
C. L2TP does not allow the use of wildcard pre-shared keys, which is not as secure as some other methods.
D. L2TP has less overhead than GRE.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 450
In the IOS Firewall Feature Set, which network layers are examined by CBAC to make filtering decisions? (Multiple answer)

A. Transport
B. Application
C. Network
D. Presentation
E. Data Link

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 451
In the realm of email security, "message repudiation" refers to what concept?

A. A user can validate which mail server or servers a message was passed through.
B. A user can claim damages for a mail message that damaged their reputation.
C. A recipient can be sure that a message was sent from a particular person.
D. A recipient can be sure that a message was sent from a certain host.
E. A sender can claim they did not actually send a particular message.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 452

A RARP is sent:

A. To map a hostname to an IP address.
B. To map an IP address to a hostname.
C. To map an MAC address to an IP address.
D. To map a MAC address to a hostname.
E. To map and IP address to a MAC address.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 453
Exhibit:

```
aaa authentication login default local tacacs
aaa authorization exec default tacacs
aaa authentication login vty tacacs local
aaa authorization exec vty tacacs if-authenticated username abc password xuz
line vty 0 4
exec-timeout 0 0
```

If a router running IOS 11.3 is configured as shown in the TACACS server is down, what will happen when someone Telnets into the router?

A. Using the local username, the user will pass authentication but fail authorization.
B. The user will be bale to gain access using the local username and password, since list vty will be checked.
C. Using the local username, the user will bypass authentication and authorization since the server is down.
D. The user will receive a message saying "The TACACS+ server is down, please try again later".

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 454
When an IPSec authentication header (AH) is used in conjunction with NAT on the same IPSec endpoint, what is the expected result?

A. NAT has no impact on the authentication header.
B. IPSec communicates will fail because the AH creates a hash on the entire IP packet before NAT.
C. AH is only used in IKE negotiation, so only IKE will fail.
D. AH is no a factor when used in conjunction with NAT, unless Triple DES is included in the transform set.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 455
Which of the following statements regarding Routing Information Protocol (RIP) is valid?

A. RIP runs on TCP port 520.
B. RIP runs directly on top of IP with the protocol ID 89.
C. RIP runs on UDP port 520.
D. RIP does not run on top of IP.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 456
A remote user tries to login to a secure network using Telnet, but accidentally types in an invalid username or password. Which response would NOT be preferred by an experienced Security Manager? (Multiple answer)

A. Invalid Username
B. Invalid Password
C. Authentication Failure
D. Logon Attempt Failed
E. Access Denied

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 457
Some packet filtering implementations block Java by finding the magic number 0xCAFEBABE at the beginning of documents returned via HTTP.How can this Java filter be circumvented?

A. By using Java applets in zipped or tarred archives.
B. By using FTP to download using a web browser.
C. By using Gopher.
D. By using non-standard ports to enable HTTP downloads.
E. All of the above.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 458
User_A and User_B are logged into Windows NT Workstation Host_A and Host_B respectively.

All users are logged in to the domain"CORP".
All users run a logon script with the following line: "net useD:\\CORPSVR\data"

- User_A and User_B are both members of the local group "USERS".
- Local group "USERS" is includes in global group "DOMAIN USERS".
- All users, hosts, and groups are in the domain "CORP".
- The directory \\CORPSVR\data has the share permission for local group "USERS" set to "No Access".
- The Microsoft Word document \\CORPSVR\data\word.doc has file permissions for local group "USERS" set to "Full Control".
- The Microsoft Word document \\CORPSVR\data\word.doc is owned by User_B. Given this scenario on a

Windows NT 4.0 network, what is the expected behavior when User_A attempts to edit D:\word.doc?

A. Local groups cannot be placed into global groups. The situation could not exist.
B. There is not enough information. Permissions on Microsoft Word are set within the application and are not subject to file and share level permissions.
C. Access would be denied. Only the owner of a file can edit a document.
D. Access would be denied. "No access" overrides all other permissions unless the file is owned by the user.
E. User_A has full control and can edit the document successfully.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 459
Which of the following is an invalid Cisco Secure Intrusion Detection System function?

A. Cisco Secure Intrusion Detection System sets off an alarm when certain user-configurable strings are matched.
B. Cisco Secure Intrusion Detection System sends e-mail messages at particular alarm levels via eventd.
C. Cisco Secure Intrusion Detection System performs a traceroute to the intruding system.
D. Cisco Secure Intrusion Detection System sends a TCP reset to the intruder when operating in packet sniffing mode.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 460
Under normal circumstances, after a single IPSec tunnel has been established, how many IPSec security associations should be active on the system?

A. One per protocol (ESP and AH)
B. Two per protocol (ESP and AH)
C. Three per protocol (ESP and AH)
D. Four per protocol (ESP and AH)
E. Five total (either ESP or AH)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 461
Which of the following does NOT qualify to be an example of a supported ISAKMP keying mechanism?

A. Pre-shared
B. Perfect Forward Secrecy
C. RSA
D. Certificate authority

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 462
Exhibit:

```
10.1.1.0/24 through OSPF
10.1.0.0/16 through EIGRP
10.1.0.0&16 static
```

If a router had the three routers listed, which one of the routers would forward a packet destined for 10.1.1.1?

A. 10.1.0.0/16 though EIGRP, because EIGRP routes are always preferred over OSPF or static routes.
B. 10.1.0.0/16 static, because static routes are always preferred over OSPF or EIGRP routes.
C. 10.1.1.0/24 through OSPF because the route with the longest prefix is always chosen.
D. Whichever route appears in the routing table first.
E. The router will load share between the 10.1.0.0/16 route through EIGRP and the 10.1.0.0/16 static route.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 463
The purpose of Administrative Distance, as used by Cisco routers, is:

A. To choose between routes from different routing protocols when receiving updates for the same network.
B. To identify which routing protocol forwarded the update.
C. To define the distance to the destination used in deciding the best path.
D. To be used only for administrative purposes.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 464
A network manager issues an RCP (Remote Copy) when copying a configuration from a router to a Unix system. What file on the Unix system would need to be modified to allow the copying to occur?

A. rcmd
B. rcmd.allow
C. allow.rcmd
D. hosts.allow
E. .rhosts

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 465
In the context of intrusion detection, what is the definition of exploit signatures?

A. Policies that prevent hackers from your network.
B. Security weak points in your network that can be exploited by intruders.
C. Identifiable patterns of attack detected on your network.
D. Digital graffiti from malicious users.
E. Certificates that authenticate authorized users.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 466
According to RFC 1700, what well-known ports are used for DNS?

A. TCP and UDP 23.
B. UDP 53 only.
C. TCP and UDP 53.
D. UDP and TCP 69.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 467
Besides Kerberos port traffic, what additional service does the router and the Kerberos server use in implementing Kerberos authentication on the router?

A. TCP
B. Telnet

C. DNS
D. FTP
E. ICMP
F. None of the above.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 468
Identify the default port(s) used for web-based SSL (Secure Socket Layer) Communication:

A. TCP and UDP 1025.
B. TCP 80.
C. TCP and UDP 443.
D. TCP and UDP 1353.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 469
In the TACACS+ protocol, the sequence number is: (Multiple answer)

A. An identical number contained in every packet.
B. A number that must start with 1 (for the fist packet in the session) and increment each time a request orresponse is sent.
C. Always an odd number when sent by the client.
D. Always an even number when sent by the client and odd when sent by the daemon.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 470
The Company network administrator is troubleshooting a problem with FTP services. What will the administrator encounter if a device blocks the data connection?

A. The administrator will experience very slow connect times.
B. Incomplete execution, when issuing commands like "pwd" or "cd".
C. User login problems will occur.
D. Failure when listing a directory.
E. No problems at all.

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 471
What return status will cause a AAA statement to look to next defined method for authentication?

A. Fail
B. Error
C. Access-reject
D. All of the above

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 472
Global deployment of RFC 2827 (ingress and egress filtering) would help mitigate what classification of attack?

A. Sniffing attack
B. Denial of service attack
C. Spoofing attack
D. Reconnaissance attack
E. Port Scan attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 473
What is the primary reason for using NAT translation on a firewall?

A. To translate RFC 1918 addresses for access to the Internet.
B. To increase the number of registered IP addresses used.
C. To increase firewall performance.
D. To improve security.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 474
The ultimate target of a smurf attack should:

A. Contact the reflectors, either to ask them to reconfigure their networks to shut down the attack, or to ask for their assistance in tracing the stimulus stream.
B. Launch a retaliatory attack on the reflector network.
C. Ask the reflector network administrator to quench the attack by allowing directed broadcasts.
D. Use the access-list logging command on the inside interface of the router of the ultimate target network todetermine the station inside the network launching the attack.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 475
A Security Manager needs to allow L2TP traffic through the firewall into the Internet network. What ports generally need to be opened to allow this traffic to pass?

A. TCP/UDP 1207
B. TCP/UDP 500
C. IP 50, IP 51
D. TCP 49
E. UDP 1701
F. TCP 1072

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 476
Protocols are protected by an authentication.

What range can Cisco Secure Intrusion Detection System user-definable string-matches have?

A. Signatures 1000
B. Signatures 3000
C. Signatures 8000
D. Any signature range

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 477
NTP (Network Time Protocol) or the clock set command must be set up when which features or services are employed on a router? (Multiple answer)

A. L2TP
B. Intusion Detection

C. Kerkeros
D. PKI

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 478
What command in the IOS Firewall Feature Set is used to turn off CBAC?

A. no ip inspect cbac
B. no enable ip inspect
C. no enable cbac
D. no ip inspect
E. no ip inspect all

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 479
CiscoWorks VMS consists of several management consoles or MCs. The IDS is used to control the configuration of the IDS sensors and IDSM blades deployed in an enterprise. Which parameters must be unique when in a given PostOffice domain?

A. IP address and PostOffice ID
B. Host ID and PostOffice domain name
C. Host ID and IP address
D. Organization ID and Host ID
E. Organization name and Organization ID
F. Organization ID and PostOffice ID

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 480
What effect do these configuration commands have?

```
Line vty 0 4
no login Password cisco
```

A. The VTY password is cisco
B. The login password is login
C. The VTY password is required but not set
D. No password is required for VTY access

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

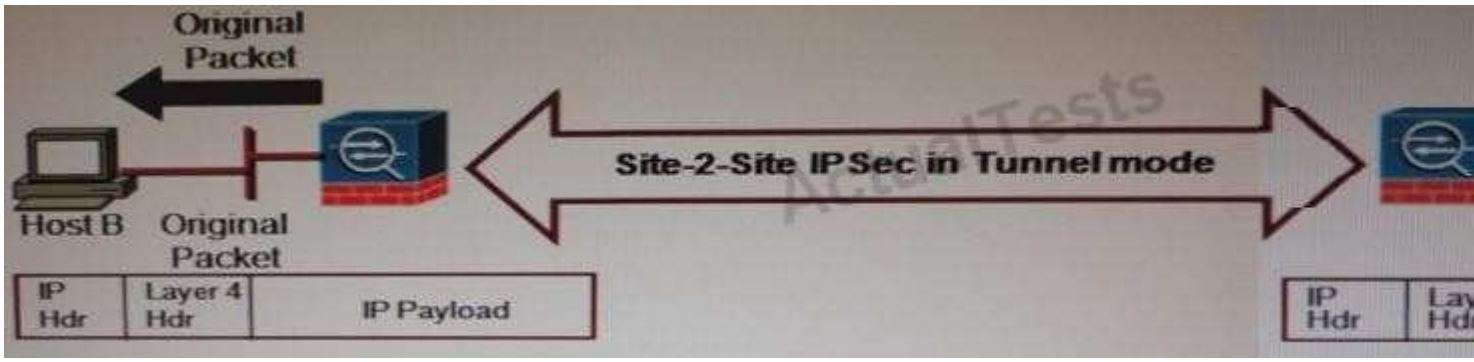
QUESTION 481
The SSL protocol provides "channel security, " but lacks what property?

A. A private channel. Encryption is used for all messages after a simple handshake is used to define a secret key.
B. An authenticated channel. The server endpoint of the conversation is always authenticated, while the client endpoint is optionally authenticated.
C. A reliable channel. The message transport includes a message integrity check (using a MAC).
D. An independent authentication where each transmission requires authentication by the server endpoint.

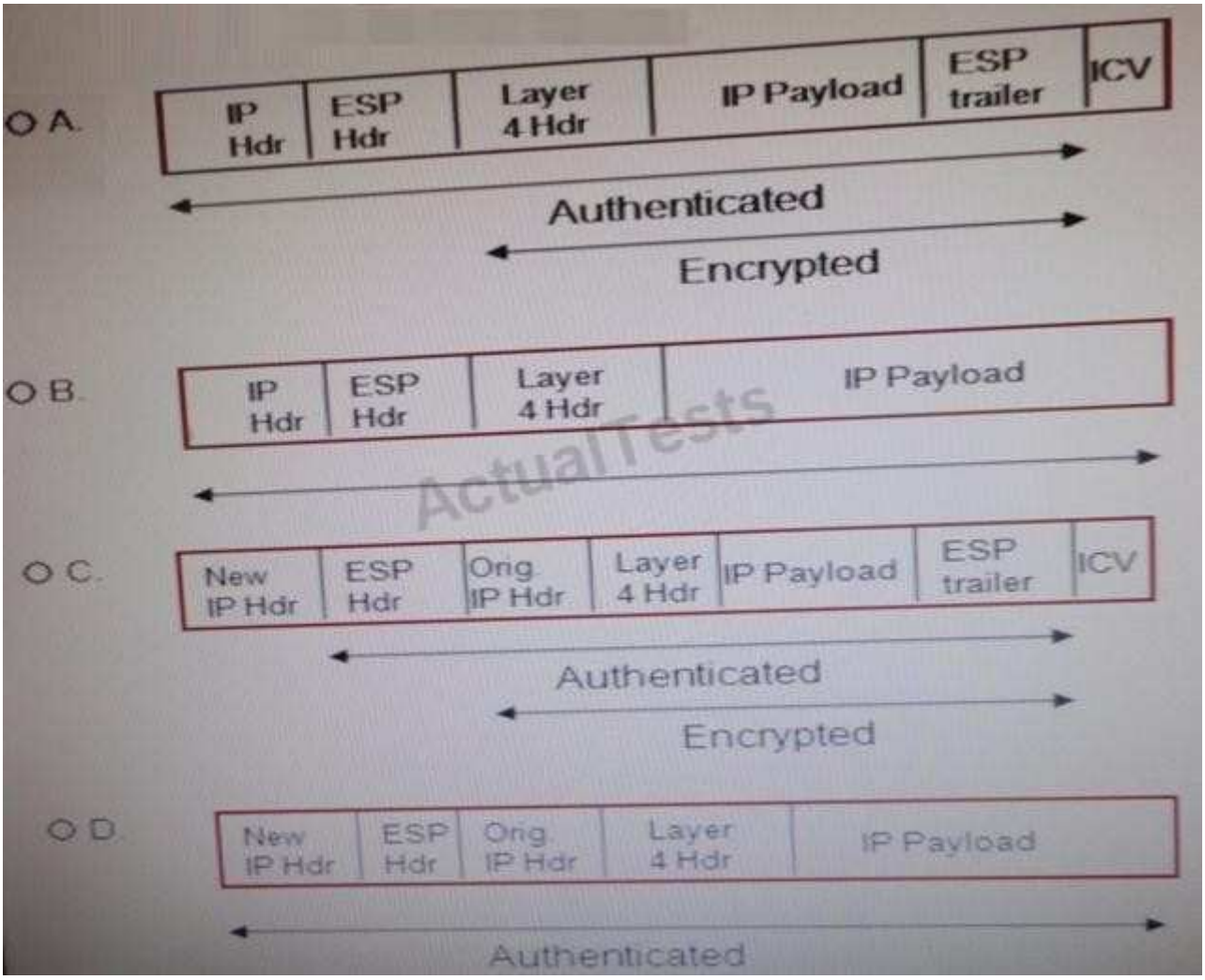
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 482
Refer to exhibit.



An IPSec site-to-site tunnel is set up between two Cisco ASA adaptive security appliances. When Host A sends a packet to Host B, what is the correct ESP packet format if tunnel mode is used?



A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 483
What are three benefits of Cisco IPS Manager Express (Cisco IME) compared to Cisco IPS Device Manager (Cisco IDM)? (Choose three.)

A. Advanced Cisco IPS signatures can be configured with Cisco IME, while only basic Cisco IPS signatures can be configured with Cisco IDM.
B. Cisco IME can manage up to 10 Cisco IPS devices while Cisco IDM can only manage a single Cisco IPS device.
C. A live RSS feed for Cisco security alerts can be set up on Cisco IME, but not on Cisco IDM.

D. The sensor health dashboard can only be viewed on Cisco IME, not on Cisco IDM.
E. Email notification can be sent form Cisco IME if an event is being triggered by Cisco IPS, but cannot be sent from Cisco IDM.
F. Automatic signature updating can only be provisioned from Cisco IDM.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

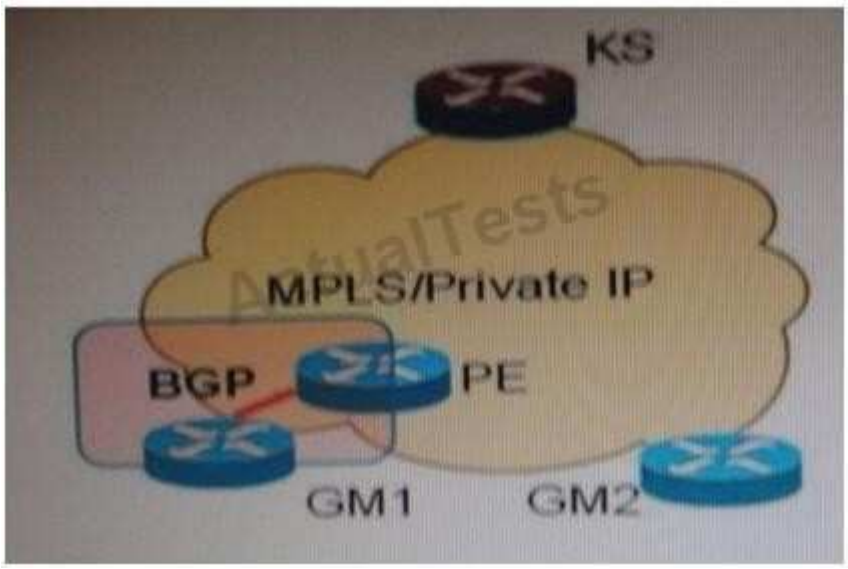
QUESTION 484
Which method is used by Cisco Security Agent to get user information from the OPrtating System?

A. State secure SSL using HTTPS session
B. Application (Layer 7)-based (Cisco proprietary) encryption
C. NetBIOS socket on TCP port 137-139 and UDP port 137-139
D. Win32 application binary interface (ABI)
E. Win32 application programming interface (API)

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 485
Refer to the exhibit.



In this GETVPN setup, as soon as GM1 successfully registers with the key server "KS," the BGP session between GM1 and its peering router in the provider network goes down. With the KS configuration listed below, what could be the reason for the BGP problem?

```
crypto gdoi group group1
identity number 3333
server local
rekey authentication mypubkey rsa getvpn-rsa-key
rekey transport unicast
sa ipsec 1
profile gdoi-ip
match address ipv4 ENCRYPT-POLICY
!
ip access-list extend ENCRYPT-POLICY
deny ospf any any
deny eigrp any any
deny ip 224.0.0.0 0.0.0.255 any
deny ip any 224.0.0.0 0.0.0.255
deny udp any eq 848 any eq 848
permit ip any any
!
```

A. GETVPN cannot run over MPLS provider backbone.
B. The key server should exclude BGP from its encryption policy.
C. GETVPN does support BGP running between CE and PE links, so IGP must be used.
D. The key server should be configured as a BGP reflector.
E. The rekey method should be configured as multicast on key server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 486
Which four of these hash functions are part of the SHA-2 family, named after their digests length? (Choose four)

A. SHA-168
B. SHA-224
C. SHA-256
D. SHA-384
E. SHA-448
F. SHA-512

Correct Answer: BCDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 487
A customer just deployed Cisco IOS firewall, and it has started to experience issues with applications timing out and overall network slowness during peak hours. The network administrator noticed the following syslog message around the time of the problem.

```
%FW-4-ALET_ON: getting aggressive, count (501/500) current 1-min rate: 200
```

What could the problem could be, and how might it be migrated?

A. The DoS max half-open session threshold has been reached. Increase the threshold IP inspect max-incomplete high configuration.
B. The Cisco IOS firewall session license limit has been exceeded. Obtain an new license with more sessions.
C. The router system resource limit threshold has been reached. Replace the router with one that has more memory and CPU power.
D. The aggregate virus detection threshold has been reached. Identify the affected host and accordingly.
E. The per-host new session establishment rate has been reached. Increase the threshold with IP inspect tcp max incomplete host configuration.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 488
Which two of these are the components of a Certificate Signing Request (CSR)? (Choose two.)

A. Private key
B. Information identifying the applicant
C. Public key
D. Pre-shared key
E. Host key

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 489
Which three of these are properties of Encapsulating Security Payload (ESP) protocol (in non- tunnel mode)? (Choose three.)

A. uses IP protocol 50
B. provides confidentiality of the IP header
C. provides data integrity
D. provides data confidentiality
E. uses IP protocol 51
F. provides data integrity of the IP header static fields

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 490
When Cisco IOS IPS matches a signature against a packet stream, it can perform all of these actions except which one?

A. send an SDEE event
B. send an SNMP Trap event
C. deny all packets from an attacker
D. send TCP reset packets to both ends of the connection
E. drop a malicious packet

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 491
Which three functions can be performed by an event correlation system such as Cisco Security MARS? (Choose three.)

A. network behavioral analysis
B. topological awareness
C. route optimization
D. risk assessment
E. policy management
F. address translation

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 492
When a client that is configured for DHCP is powered on and requests an IP address, what is the first DHCP message the client sends?

A. DHCP Acknowledgement
B. DHCP Request
C. DHCP Discover
D. DHCP Inform
E. DHCP Offer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 493
Which program is used to resolve a DNS name to an IP address?

A. ipconfig
B. ndc
C. whois
D. nslookup
E. netstat

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 494
Which three of these are properties of RC4? (Choose three.)

A. It is a stream cipher
B. It is a block cipher
C. It is used in SSL
D. It is a symmetric cipher
E. It is an asymmetric cipher
F. It is used in AES

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 495
Which three of these are security properties that TLS V1.2 provides? (Choose three.)

A. Confidentiality
B. Integrity
C. Authentication
D. Authorization
E. Non-repudiation

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 496
Which three of these are properties of the Authentication Header (AH) protocol? (Choose three.)

A. Provides data integrity

B. Provides data confidentiality
C. Provides data origin authentication
D. Uses IP protocol number 50
E. Optionally provides replay Protection

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 497
Which process entails thoughtful planning and sensitive implementation, clear definition of roles and responsibilities, definition of rollback procedures, as well as consultation with, and involvement of, the people affected by the modifications?

A. Incident response process
B. Change management process
C. Risk assessment process
D. Security Audit Process
E. Forensic analysis process

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 498
Handshake protocol is the most complex part of SSL. Which two of these statements are true of SSL handshake protocol? (Choose two.)

A. This protocol allows the server and client t o authenticate each other.
B. This protocol is used after any application data is transmitted.
C. This is not a single protocol but rather two layers of protocol
D. This protocol is used to exchange cryptographic keys using DH
E. This protocol consists of a series of message exchanged by t he client and server.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 499
What is the name of the unique tool/feature in Cisco Security Manager that is used to merge an access list based on the source/destination IP address, service, or combination of these to provide a manageable view of access policies?

A. merge rule tool
B. policy simplification tool

C. rule grouping tool
D. combine rule tool
E. object group tool

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 500
In order for a user to perform a reverse DNS lookup for a web server, which type of record must be stored in the DNS server for that web server?

A. type "A" record
B. PTR record
C. MX record
D. CNAME record
E. NS record

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 501
Which three global correlation features can be enabled from Cisco IPS Device Manager (Cisco IDM)? (Choose three.)

A. Network Reputation
B. Data Contribution
C. Reputation Assignment
D. Signature Correlation
E. Global Data Integration
F. Reputation Filtering
G. Global correlation infection

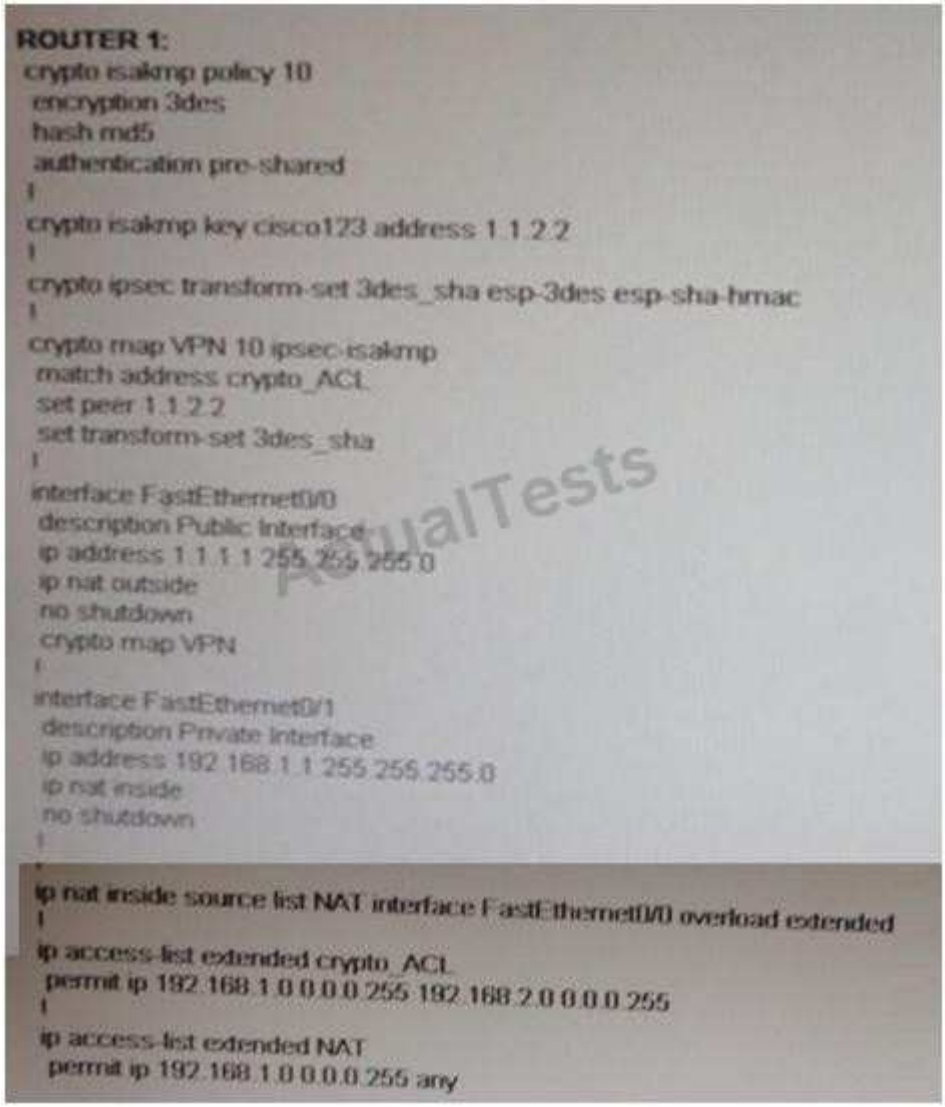
Correct Answer: AFG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Global Correlation Features and Goals
There are three main features of global correlation:
· Global Correlation Inspection--We use the global correlation reputation knowledge of attackers to influence alert handling and deny actions when attackers with a bad score are seen on the sensor.
· Reputation Filtering--Applies automatic deny actions to packets from known malicious sites. · Network Reputation--Sensor sends alert and TCP fingerprint data to the SensorBase Network.

QUESTION 502

You are responsible for bringing up an IPsec tunnel between two Cisco IOS routers in Site A and Site B, and, at the same time, allowing them to access to the Internet from their local sites. You applied these configurations to the routers:



ROUTER 1:

```
crypto isakmp policy 10
 encryption 3des
 hash md5
 authentication pre-shared
!
crypto isakmp key cisco123 address 1.1.2.2
!
crypto ipsec transform-set 3des_sha esp-3des esp-sha-hmac
!
crypto map VPN 10 ipsec-isakmp
 match address crypto_ACL
 set peer 1.1.2.2
 set transform-set 3des_sha
!
interface FastEthernet0/0
 description Public Interface
 ip address 1.1.1.1 255.255.255.0
 ip nat outside
 no shutdown
 crypto map VPN
!
interface FastEthernet0/1
 description Private Interface
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 no shutdown
!
ip nat inside source list NAT interface FastEthernet0/0 overload extended
!
ip access-list extended crypto_ACL
 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
!
ip access-list extended NAT
 permit ip 192.168.1.0 0.0.0.255 any
```

You issue the show crypto ipsec sa command and see that tunnel is up, but no packets are encrypted or decrypted on either side. To test connectivity, you sourced a ping from the private interface of the each router, destined to the private interface of the far-end router. You ask a VPN expert to help you trouble shoot. The expert has verified that ESP is not being blocked, and the routing is correct.

After troubleshooting, the expert makes which of these determinations?

A. The problem is with the encryption ACL. As you were testing with ICMP, you needed to allow ICMP in both encryption ACLs.Router 1: permit ICMP 192.168.1.0.0.0.0.255.192.168.2.0.0.0.0.255Router 2: permit ICMP 192.168.1.0.0.0.0.255.192.168.2.0.0.0.0.255

B. The problem is with the NAT ACL. VPN traffic should be denied in the NAT ACL so that the ACL, looks likes the following.Router 1: Ip access list ext NATdeny IP 192.168.1.0.0.0.0.255.192.168.2.0.0.0.0.255permit ip 192.168.1.0 anyRouter 2:Ip access list ext NATdeny IP 192.168.1.0.0.0.0.255.192.168.2.0.0.0.0.255permit ip 192.168.1.0 any

C. The problem is that is not possible to do NAT along with VPN on a Cisco IOS router.

D. The problem is the NAT transparency is enabled. Disable NAT Transparency using the following global command on both routers. No crypto ipsec nat-transparency udp-encapsulation.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 503
When you define the BGP neighbor ttl-security command, you must consider which two of these restrictions? (Choose two.)

A. This feature is supported for internal BGP (IBGP) peer groups.
B. This feature is not supported for internal BGP (IBGP) peers.
C. This feature cannot be configured for a peer that is configured with the neighbor next-hop-self command.
D. This feature cannot be configured for a peer that is configured with the neighbor ebgp-multihop command.
E. This feature cannot be configured for a peer that is configured with the neighbor send- community command.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 504
Which five of these are criteria for rule-based rogue classification of access points by the Cisco Wireless LAN Controller? (Select five.)

A. minimum RSSI
B. open authentication
C. MAC address range
D. whether it matches a managed AP SSID
E. whether it matches a user-configured SSID
F. whether it operates on an authorized channel
G. time of day the rogue operates
H. number of clients it has

Correct Answer: ABEGH
Section: (none)
Explanation

Explanation/Reference:

QUESTION 505
Which four routing protocols are supported when using Cisco Configuration Professional? (Choose four.)

A. RIPv1
B. RIPv2
C. IGRP
D. EIGRP
E. OSPF
F. BGP

Correct Answer: ABDE
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 506
Application layer protocol inspection is available for the Cisco ASA 5500 Series Adaptive Security Appliance. This feature performs which type of action on traffic traversing the firewall?

A. Classification and policing (for QoS)
B. Deep packet inspection
C. Flexible packet matching
D. Reverse path forwarding
E. Remote triggering of a black hole.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

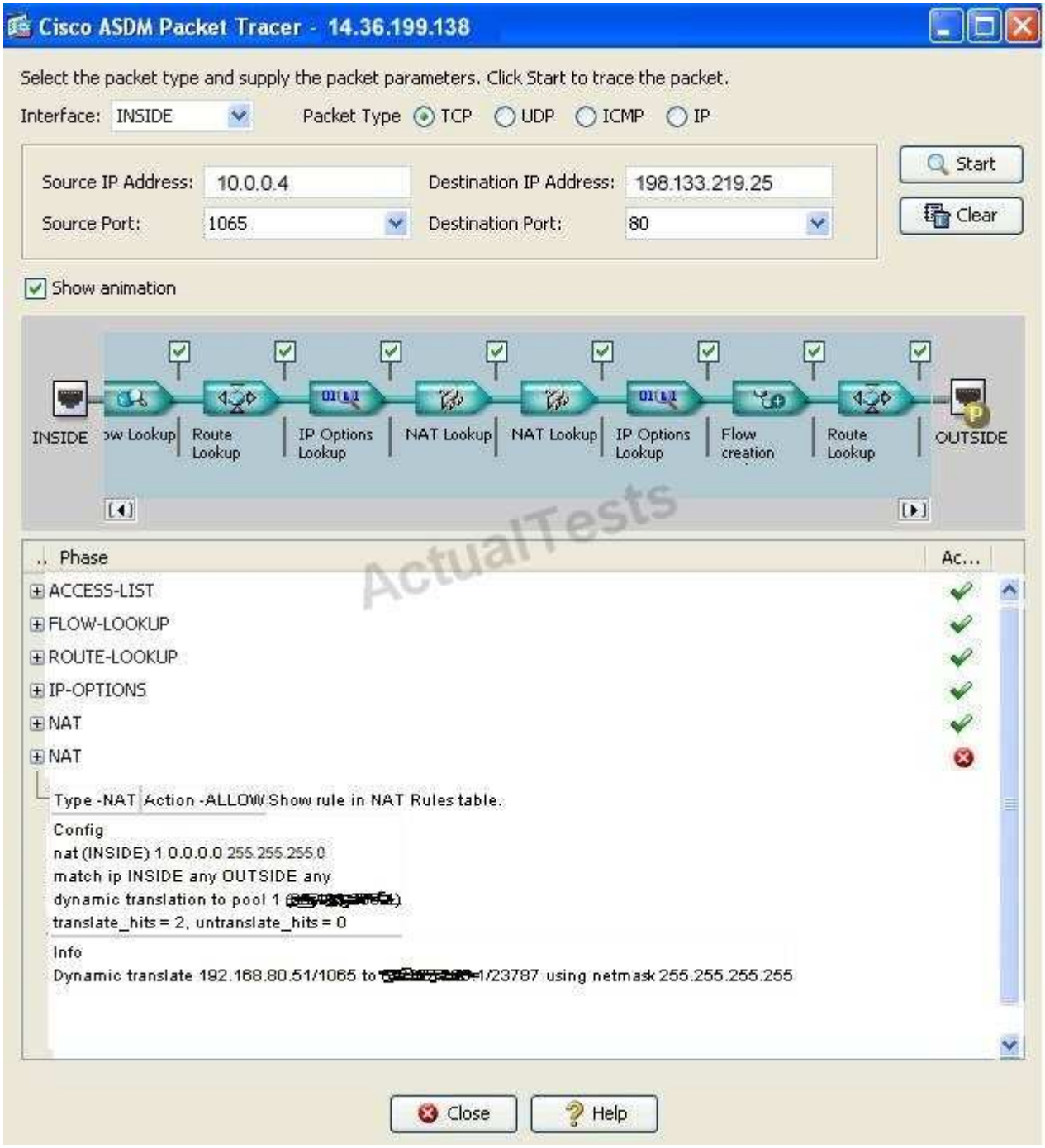
QUESTION 507
EIHRP functionality is very similar to which of these protocols?

A. TCP
B. ARP
C. IP
D. RDP
E. DHCP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 508
Refer to the exhibit.



Which command is required to fix the issue identified by Cisco ASDM Packet Tracer in the image?

A. nat (inside) 1 10.0.0.4
B. global (outside) 1 203.0.113.100
C. global (outside) 1 203.0.113.110
D. access-list outside permit tcp host 10.0.0.4 host 198.133.219.25 eq www
E. nat (outside) 10 198.133.219.25

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

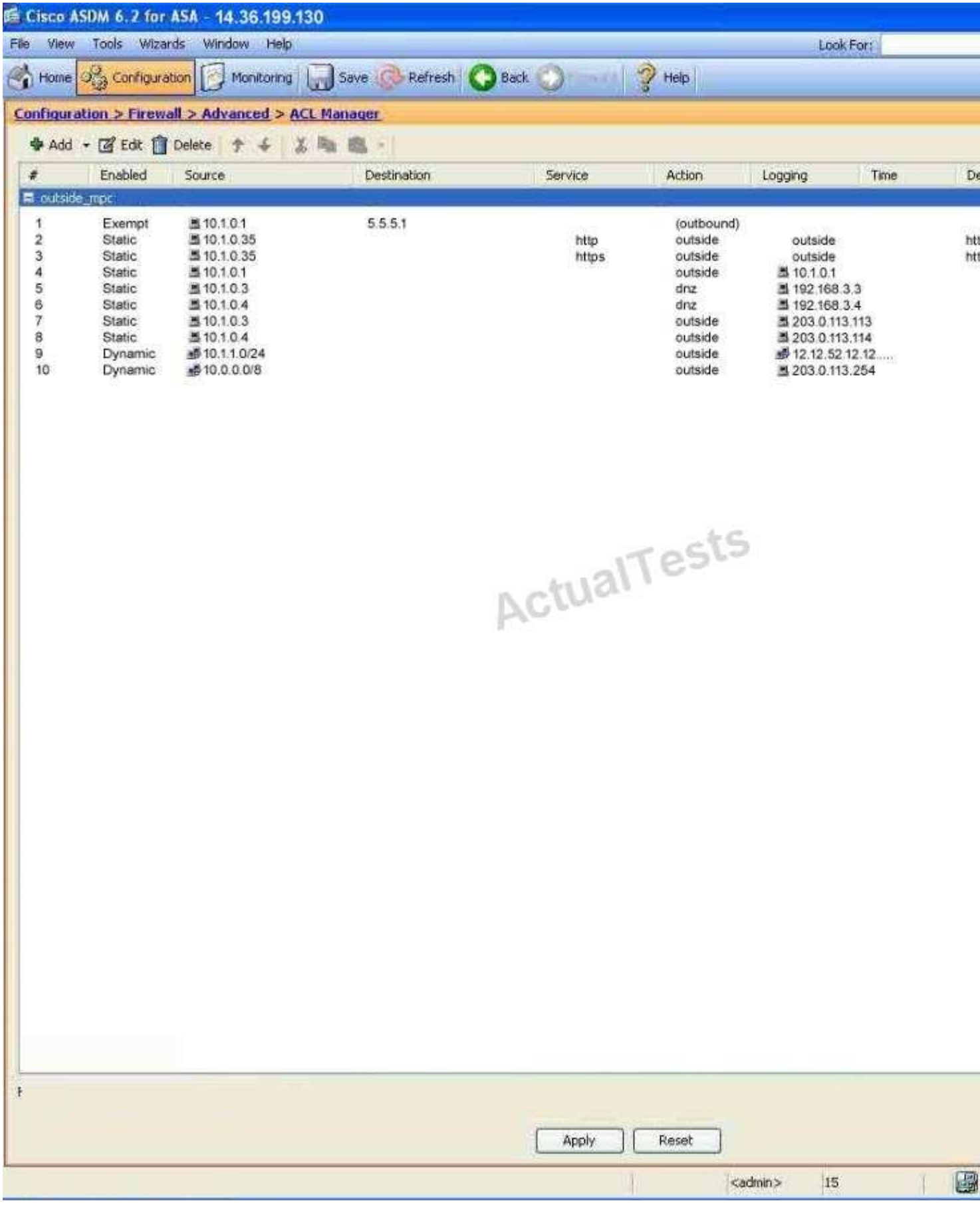
QUESTION 509
Which four of these areas can be characterized for network risk assessment testing methodology? (Choose four)

A. Router hostname and IP addressing scheme
B. Router filtering rules
C. Route optimization
D. Database connectivity and RTT
E. Weak authentication mechanisms
F. Improperly configured email servers
G. Potential web server exploits

Correct Answer: BEFG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 510
Refer to the exhibit


Cisco ASDM 6.2 for ASA - 14.36.199.130
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Help
Configuration > Firewall > Advanced > ACL Manager
Add Edit Delete
Enabled Source Destination Service Action Logging Time
outside_mpc
1 Exempt 10.1.0.1 5.5.5.1 (outbound)
2 Static 10.1.0.35 http outside outside
3 Static 10.1.0.35 https outside outside
4 Static 10.1.0.1 outside 10.1.0.1
5 Static 10.1.0.3 dnz 192.168.3.3
6 Static 10.1.0.4 dnz 192.168.3.4
7 Static 10.1.0.3 outside 203.0.113.113
8 Static 10.1.0.4 outside 203.0.113.114
9 Dynamic 10.1.1.0/24 outside 12.12.52.12.12....
10 Dynamic 10.0.0.0/8 outside 203.0.113.254
ActualTests
Apply
Reset
<admin>
15

From the ASDM NAT Rules table, inside host 10.1.0.4 is translated to which IP address on the outside interface?

A. 203.0.113.254
B. 192.168.3.3
C. 192.168.3.4
D. 203.0.113.113
E. 203.0.113.114

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 511
In the context of Cisco Configuration Professional, to "discover" a router means to establish a session to the router using either secure or nonsecure means, do which of the following, and populate a screen with the information obtained?

A. read the configuration present in the router
B. read the IOS version in the router
C. read the interface(s) information in the router
D. read the CPU information in the router
E. check if the router is UP or Down

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 512
When a failover takes place on an adaptive security appliance configured for failover, all active connections are dropped and clients must reestablish their connections, unless the adaptive security appliance is configured in which two of the following ways?(Choose two.)

A. active/standby failover
B. active/active failover
C. active/active failover and a state failover link has been configured
D. active/standby failover and a state failover link has been configured
E. to use a serial cable as the failover linkF LAN-based failover

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 513
What is the main purpose of FlexConfig in Cisco Security Manager?

A. to share configuration between multiple devices
B. to configure device commands that are not supported by Cisco Security Manager
C. to duplicate/clone basic configuration of a device
D. to merge multiple policies into a simplified view
E. to configure complex commands for a device

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

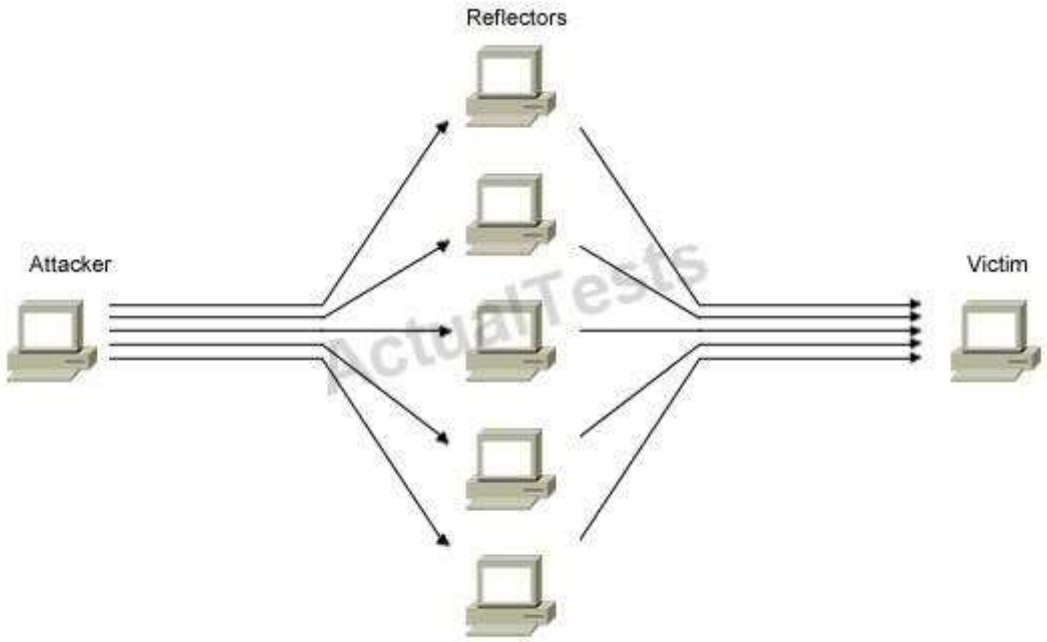
QUESTION 514
All of these correctly describe SNMPv3 except which one?

A. does not provide any protection against denial of service attacks
B. provides a mechanism for verification that messages have not been altered in transit
C. requires the use of NTP to correctly synchronize timestamps and generate public/private key pairs used for encryption of messages
D. provides a mechanism for verification of the identity of the device that generated the message
E. includes timeliness indicators in each message so the receiving SNMP engine can determine if it was sent recently

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 515
Refer to the Exhibit.



The exhibit illustrates which type of attack?

A. virus infection
B. worm propagation
C. port scanning
D. denial of service (Dos)
E. distributed Dos (DDos)

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 516
All of these are available from Cisco IPS Device Manager (Cisco IDM) except which one?

A. Interface Status
B. Global Correlation Reports
C. Sensor Information
D. CPU, Memory and Load
E. Top Signatures
F. Top Applications

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 517
Which two of these properties does the UDP protocol itself provide? (Choose two.)

A. reliable delivery of data
B. data rate negotiation
C. checksum to prevent data errors
D. prevention of data interception
E. efficient data transfer

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 518
Which two U.S. government entities are authorized to execute and enforce the penalties for violations of the Sarbanes-Oxley (SOX) act? (Choose two.)

A. Federal Trade Commission (FTC)
B. Federal Reserve Board
C. Securities and Exchange Commission (SEC)

D. Office of Civil Rights (OCR)
E. United States Citizenship and Immigration Services (USCIS)
F. Internal Revenue Service (IRS)

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 519
NHRP functionality is very similar to which of these protocols?

A. TCP
B. ARP
C. IP
D. RDP
E. DHCP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 520
You have recently deployed DMVPN Phase 3 for your WAN. Each of the spokes has a static IP assigned

to it by the ISP, except one, which gets a dynamic IP. After a recent power loss during the day, the router rebooted, but was unable to bring the tunnel up to the hub immediately. The log on the spoke shows an NHRP registration reply from the hub indication an error.

```
%NHRP-3-PAKREPLY: Receive Registration Reply packet with error  unique address
registered already (14)

interface Tunnel0
ip address 17216.1.1.255.255.255.255.0
no ip redirects
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 10
ip nhrp holdtime 3600
ip nhrp redirect
tunnel source FastEthermet0/0
tunnel mode gre multipoint
```

Below is the configuration of the tunnel interface of Spoke 1

```
Interface Tunnel 0
ip address 17216.1.2.255.255.255.255.0
no ip redirects
ip nhrp authentication cisco
ip nhrp map multicast 1.1.1.2
ip nhrp map 172.16.1.1 1.1.1.2
ip nhrp network-id 20
ip nhrp holdtime 3600
ip nhrp nhs 172.16.1.1
ip nhrp shortcut
tunnel source FastEthermet0/0
tunnel mode gre multipoint
```

Which of these actions could solve this problem?

A. Configure tunnel protection, with the appropriate cryptographic configuration on the hub and spokes
B. Configure the no ip nhrp registration unique command on the hub, Hub 1
C. Configure the ip nhrp registration no-unique command on the spoke, Spoke 1
D. Remove the ip nhrp shortcut command from the spoke, Spoke 1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 521
The Cisco IPsec VPN Shared Port Adapter (SPA) operates in which mode of IPsec implementation?

A. bump in the wire (BITW)
B. bump in the network (BITN)
C. bump in the stack (BITS)
D. hardware-assisted tunnel mode (HATM)
E. hardware-assisted transport mode (HATM)

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 522
A Layer 2 switch forwards traffic based on which of these?

A. IP layer addresses
B. ARP layer addresses
C. MAC layer addresses
D. Forwarding information Base (FIB)
E. Hardware-Assisted Forwarding (HAF)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 523
A 1200-byte packet arrives on the LAN segment and needs to be fragmented before being forwarded to the egress interface. Which of these identifies the correct IP header fields for the IP fragments after fragmentation (where MF is the More Fragment flag bit, and FO is the Fragment Offset in the IP header)?

A. fragment1: id=1, length=1000, MF=0, FO=980; fragment2: id=2, length=220, MF=0, FO=980
B. fragment1: id=1, length=996, MF=1, FO=0; fragment2: id=1, length=224, MF=0, FO=122
C. fragment1: id=1, length=600, MF=1, FO=0, fragment2: id=2, length=620, MF=0, FO=75
D. fragment1: id=1, length=1000, MF=1, FO=0; fragment2: id=1, length=220, MF=0, FO=980
E. fragment1: id=1, length=600, MF=0, FO=580; fragment2: id=1, length=620, MF=0, FO=0

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 524
All of these correctly describe advantages of GETVPN compared to traditional IPsec except which one?

A. Eliminates the need for tunnels, and therefore scales better
B. Provides always-on full mesh encryption capability
C. Provides native multicast encryption
D. Allows all members to dynamically discover each either with no static peer configuration required
E. Can take advantage of the existing routing infrastructure, and does not require overlay routing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 525
Hypertext Transfer Protocol Secure (HTTPS) was created to provide which of these?

A. a secure connection over a secure network
B. a secure connection over an insecure network
C. an authenticated connection over a secure network
D. an authenticated connection over an insecure network
E. an authorized connection over an insecure network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 526
Which three of these statements about a zone-based policy firewall are correct? (Choose three.)

A. An interface can be assigned to only one security zone.
B. Traffic cannot flow between a zone member interface and any interface that is not a zone member.
C. By default, all traffic to and from an interface that belongs to a security zone is dropped unless explicitly allowed in the zone-pair policy.
D. In order to pass traffic between two interfaces that belong to the same security zone, you must 272

   configure a pass action using class-default
E. Firewall policies, such as the pass, inspect, and drop actions, can only be applied between two zones.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

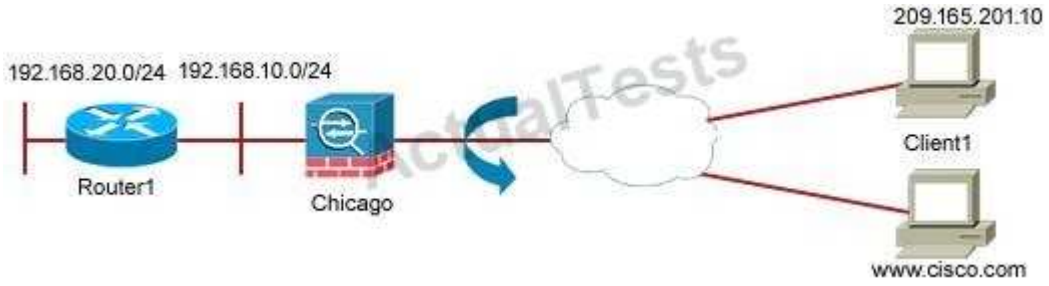
QUESTION 527
The Rivest, Shamir, and Adleman (RSA) algorithm can be used to create digital signatures for authentication. Suppose Alice wants to sign a message using RSA and send it to Bob. Which one of the following statements most accurately describes this operation?

A. Alice creates a hash of her messages, and then encrypts this hash with her public key to create the signature to be sent along with the message to Bob
B. Alice creates a hash of her message, and then encrypts this hash with her private key to create the signature to be sent along with the message to Bob
C. Alice creates a hash based on her message combined with her public key, and then uses this hash to create the signature to be sent along with the message to Bob
D. Alice creates a hash based on her message combined with her private key, and then uses this hash to create the signature to be sent along with the message to Bob
E. Alice encrypts her message with her public key, creates a signature by hashing this encrypted message. Then sends it along with the message to Bob

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 528
Refer to the Exhibit.



Refer to the exhibit. Client1 has an IPsec VPN tunnel established to a Cisco ASA adaptive security appliance in Chicago. The remote access VPN client wants to access www.cisco.com, but split tunneling is disabled. Which of these is the appropriate configuration on the Cisco ASA adaptive security appliance if the VPN client's public IP address is 209.165.201.10 and it is assigned a private address from 192.168.1.0/24?

A. same-security-traffic permit intra-interfaceIp local pool ippool 192.168.1.1-192.168.1.254Global (outside) 1 209.165.200.230Nat (inside) 1 192.168.1.0 255.255.255.0
B. same-security-traffic permit intra-interfaceIp local pool ippool 192.168.1.1-192.168.1.254Global (outside) 1 209.165.200.230Nat (outside) 1 192.168.1.0 255.255.255.0
C. same-security-traffic permit intra-interfaceIp local pool ippool 192.168.1.1-192.168.1.254Global (inside) 1 209.165.200.230Nat (inside) 1 192.168.1.0 255.255.255.0
D. same-security-traffic permit intra-interfaceIp local pool ippool 192.168.1.1-192.168.1.254Global (outside) 1 209.165.200.230Nat (outside) 1 209.165.201.10 255.255.255.255
E. same-security-traffic permit intra-interfaceIp local pool ippool 192.168.1.1-192.168.1.254Global (outside) 1 209.165.200.230Nat (inside) 1 209.165.201.10 255.255.255.255
F. same-security-traffic permit intra-interfaceIp local pool ippool 192.168.1.1-192.168.1.254Global (inside) 1 209.165.200.230Nat (inside) 1 209.165.201.10 255.255.255.255

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 529
One of the main security issues with the WEP protocol stems from?

A. lack of any integrity checking
B. having a maximum key of 40 bits
C. use of Open System authentication
D. use of RC4
E. lack of standardization of the WEP protocol itself

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 530
How can you configure Cisco Easy VPN Server on a Cisco IOS router in order to allow you to apply various QoS policies to different VPN groups?

A. Configure the command qos pre-classify under the crypto map that references each VPN group.
B. Configure Cisco Easy VPN using IPsec Dynamic Virtual Tunnel Interface (DVTI) and apply service policies on the VTI that are referenced by the ISAKMP profiles matching the respective VPN groups
C. It is not currently possible to apply QoS to different VPN groups
D. Configure s static VTI that allows configuration of QoS service policies with each VTI referenced by the respective VPN groups

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 531
Which three of these are considered TCP/IP protocols? (Choose three.)

A. ICMP
B. DOCSIS
C. IGMP
D. Ethernet
E. ATM
F. DNS

Correct Answer: ACF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 532
All of these are application layer protocols based on the OSI model except which one?

A. SMTP
B. FTP
C. DNS
D. Telnet
E. SNMP
F. OSPF

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:

QUESTION 533
Which of these notification protocols are supported in Cisco Security MARS?

A. SNMP trap only
B. syslog only
C. email (Sendmail) adn SMS only
D. SNMP trap and syslog only
E. syslog email (Sendmail), SMS, and SNMP trap

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 534
The Network Participation feature of Cisco IPS gathers all of these when it collects real-time data from IPS sensors except which one?

A. signature ID
B. signature name
C. attacker port
D. reputation score
E. signature version
F. victim port

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 535
Assessing your network for potential security risks (risk assessment) should be an integral element of your network architecture. Which four task items need to be performed for an effective risk assessment and to evaluate network posture? (Choose four.)

A. Notification
B. Discovery
C. Profiling
D. Scanning
E. Base lining
F. Validation
G. Mitigation

Correct Answer: BCDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 536
Which two of these devices can be used as Cisco Easy VPN Remote hardware clients?

A. ASA5510 Adaptive Security Appliance
B. 800 Series Router
C. ASA5505 Adaptive Security Appliance
D. PIX 515E Security Appliance
E. 7200 Series Router

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 537
If single sign-on (SSO) is not working for a Layer 2 out-of-band (OOB) virtual gateway implementation, which two of these can you check to troubleshoot the issue? (Choose two.)

A. The clock between the NAC server and the Active Directory server is synchronized.
B. The KTPass.exe command was executed on the domain controller with the /RC4Only option.
C. The adkernel.exe process on the domain controller is accepting requests from the Cisco Clean Access Server.
D. The Active Directory domain definition was defined in upper case on the Cisco Clean Access Manager.
E. The ports are open to the appropriate domain controller in the guest role on Cisco Clean Access Manager.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 538
The major difference between VTP version 1 and VTP version 2 is which of these?

A. Extended VLAN range support
B. Gigabit Ethernet Support
C. VTP domain and password support
D. Token Ring support
E. Transparent mode support

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 539
Which two of these statements are true about the Host Scan capabilities of Cisco ASA adaptive security appliances? (Choose two.)

A. Endpoint assessment functionality within Host Scan requires you to purchase an"Endpoint Assessment

"license

B. Host Scan functionality occurs after Cisco Secure Desktop goes through the preiogin assessment and before DAP enforces its polices
C. You must use the advanced endpoint Host Scan to collect end-host information such as the end-no suppuration system, registry, files, or actively running processes.
D. The Host Scan database must be updated every 60 days to ensure that the antivirus and antispyware database is accurate.
E. Host Scan is a modular component of Cisco Secure Desktp

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 540
Which four of these attacks or wireless tools can the standard IDS signatures on a wireless LAN controller detect? (Choose four)

A. Association flood
B. SYN flood
C. NetStumbler
D. Fragment Overlap attack
E. Deautheorization flood
F. Long HTTP request
G. AirSnort
H. Wellenreiter

Correct Answer: ACEH
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 541
The Gramm-Leach-Bliley Act (GLBA), was enacted by the United States Congress in 1999. This act is used primarily for which two of these? (Choose two.)

A. Organizations in the financial sector
B. Assurace of the accuracy of financial records
C. Confidentility of personal healthcare information
D. Organizations tha offer loans
E. Organizations in the education sector

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 542

Which of these standards replaced 3DES?

A. PKI
B. Blowfish
C. RC4
D. SHA-1
E. AES
F. MD5

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 543
Which two of these multicast addresses does OSPF use? (Choose two.)

A. 224.0.0.5 to send hello packets to discover and maintain neighbor relationships
B. 224.0.0.6 to send hello packets to discover and maintain neighbor relationships
C. 224.0.0.10 to send hello packets to discover and maintain neighbor relationships
D. 224.0.0.5 to send OSPF routing information to designated routers on a network segment
E. 224.0.0.6 to send OSPF routing information to designated routers on a network segment
F. 224.0.0.10 to send OSPF routing information to designated routers on a network segment

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 544
What is the highest target value rating that you can assign to an ip address in Cisco IPS?

A. Medium
B. High
C. Mission-Critical
D. Serve
E. Important

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 545
LEAP authentication is provided by which of these?

A. Hashing of the password before sending
B. User-level certificates

C. PAC exchange
D. Modified MS-CHAP
E. TACAS+

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 546
Which three of these are true statements about TLS? (Choose three.)

A. It is a secure protocol encapsulated within SSL
B. It is a more recent version of SSL
C. It allows for client authentication via certificates
D. If a third-party (man i-the-middle) observes the entire handshake between client and server, the third-party can decrypt the encrypted data the passes between them
E. It can be used to secure SIP
F. It cannot be used for HTTPS

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 547
All of these tools are available from the Cisco IPS manager Express (Cisco IME) GUI except which one?

A. WHOIS
B. Traceroute
C. Telnet
D. DNS lookup
E. ping

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 548
Which of these is true of the NHRP network ID (specified by the command ip nhrp network-id)?

A. It needs to be the same on all routers within the DMVPN cloud for the tunnels to come up.
B. It is locally significant, and is not sent as part of the NHRP packet.
C. It is not required for the DMVPN to come up, only the tunnel key is required.
D. It is only required on the hub with multiple DMVPN clouds, in order to segregate the clouds on the hub.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 549
All of these are layers in the OSI model except which one?

A. presentation layer
B. physical layer
C. application layer
D. service layer
E. transport layer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 550
On a Cisco Catalyst switch, which three modes can a port be set to for trunking? (Choose three.)

A. dynamic auto
B. off
C. on
D. nonegotiate
E. dynamic desirable
F. negotiate
G. trunk

Correct Answer: AEG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 551
What are IKE Phase 1 Exchange (Main Mode) messages 3 and 4 used for?

A. generate SKEYID_e, which is used to encrypt IKE messages
B. generate SKEYID_a, which is used to provide data integrity and authentication to IKE messages
C. exchange authentication information (pre-shared key)
D. exchange information that is required for key generation using Diffie-Hellman (DH)
E. authenticate the digital signature (certifications)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 552
With GETVPN, if a key server is configured to use multicast as the rekey transport mechanism, then under which of these conditions will the key server retransmit the rekey message?

A. It never retransmits the rekey message.
B. It only retransmits the rekey message when it does not receive the rekey acknowledgement from at least one group member.
C. It only retransmits the rekey message when it does not receive the rekey acknowledgement from all group members.
D. It only retransmits the rekey message when DPD to the group member fails.
E. It always retransmits the rekey message.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 553
Which two of these are things an attacker can do with an encrypted RC4 data stream? (Choose two.)

A. use XOR to match the encrypted stream to itself, in order to retrieve the key
B. filter out the keystream if the attacker gets two streams encrypted with the same RC4 key
C. calculate the checksum of the encrypted stream
D. retrieve the private key if the attacker has access to the public key
E. flip a bit of the encrypted text, which will flip a corresponding bit in the cleartext once it is decrypted

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 554
When a DHCP server offers an IP address to a client, which field is populated with the client's IP address?

A. CIADDR
B. YIADDR
C. SIADDR
D. GIADDR
E. CHADDR

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 555
Which four of these support mutual authentication? (Choose four.)

A. EAP-TTLS
B. PEAP
C. EAP-FAST
D. EAP-MD5
E. EAP-SHA1
F. EAP-TLS

Correct Answer: ABCF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 556
Which two of these statements are true about the Cisco Clean Access solution? (Choose two.)

A. When two Cisco Clean Access Managers (Cisco CAMs) are set up in failover, the "service IP address" is the IP address of the primary Cisco CAM.
B. If a single Cisco Clean Access Server (Cisco CAS) operating in in-band device mode dies, the traffic cannot pass through the hardware.
C. When a Cisco Clean Access Server (Cisco CAS) is unable to communicate with the Cisco CAM, users who are already connected will not be affected, but new users will not be able to log in.
D. When a Cisco Clean Access Server (Cisco CAS) is unable to communicate with the Cisco CAM, all users (previously authenticated users and new users) will pass traffic due to its default behavior of Fail Open.
E. The clock between the Cisco Clean Access Server (Cisco CAS) and the Cisco Clean Access Manager (Cisco CAM) must be synchronized for Active Directory single sign-on to work.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 557
Which statement in reference to IPv6 multicast is true?

A. PIM dense mode is not part of IPv6 multicast.
B. The first 12 bits of an IPv6 multicast address are always FF.
C. IPv6 multicast uses Multicast Listener Discovery (MLD).
D. IPv6 multicast requires Multicast Source Discovery Protocol (MSDP).

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 558
What is the DNS transaction ID (TXID) used for?

A. tracking anomalous behaviors of name servers

B. tracking queries and responses to queries
C. Message Tracking Query Protocol (MTQP)
D. tracking queries on behalf of another DNS resolver
E. tracking Time To Live (TTL) set in the RR

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 559
A customer just deployed Cisco IOS firewall, and it has started to experience issues with applications timing out and overall network slowness during peak hours. The network administrator noticed the following syslog messages around the time of the problem:

```
%FW-4-ALERT_ON: getting aggressive, count (501/500) current 1-min rate: 200
```

What could the problem be, and how might it be mitigated?

A. The DoS max half-open session threshold has been reached. Increase the threshold with the ip inspect max-incomplete high configuration.
B. The Cisco IOS Firewall session license limit has been exceeded. Obtain a new license with 285 more sessions.
C. The router system resource limit threshold has been reached. Replace the router with one that has more memory and CPU power.
D. The aggregate virus detection threshold has been reached. Identify the affected host and patch accordingly.
E. The per-host new session establishment rate has been reached. Increase the threshold with the ip inspect tcp max-incomplete host configuration.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 560
All of these are predefined reports in the Cisco IPS Manager Express (Cisco IME) GUI except which one?

A. Attacks Overtime Report
B. Top Victims Report
C. Top Attacker Report
D. Top Application Report
E. Top Signature Report

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 561
A false negative represents which of these scenarios?

A. when an intrusion system generates an alarm after processing traffic that it is designed to detect
B. when an intrusion system generates an alarm after processing normal user traffic
C. when an intrusion system fails to generate an alarm after processing traffic that it is designed to detect
D. when an intrusion system fails to generate an alarm after processing normal user traffic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 562
During a computer security forensic investigation, a laptop computer is retrieved that requires content analysis and information retrieval. Which file system is on it, assuming it has the default installation of Microsoft Windows Vista operating system?

A. HSFS
B. WinFS
C. NTFS
D. FAT
E. FAT32

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 563
Which of the following is used in PEAP to provide authentication for the EAP exchange?

A. RC4
B. TLS
C. SSH
D. AES
E. 3DES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 564
During a DoS attack, all of the data is lost from a user's laptop, and the user must now rebuild the system. Which tool can the user use to extract the Outlook PST file from the Microsoft Exchange server database?

A. NTbackup.exe
B. Exmerge.exe
C. Eseutil.exe
D. Ost2pst.exe

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 565
In order to reassemble IP fragments into a complete IP datagram, which three IP header fields are referenced by the receiver? (Choose three.)

A. don't fragment flag
B. packet is fragmented flag
C. IP identification field
D. more fragment flag
E. number of fragments field
F. fragment offset field

Correct Answer: CDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 566
Which multicast routing mechanism is optimal to support many-to-many multicast applications?

A. PIM-SM
B. MOSPF
C. DVMRP
D. BIDIR-PIM
E. MSDP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 567
Which VTP mode allows the Cisco Catalyst switch administrator to make changes to the VLAN configuration that only affect the local switch and are not propagated to other switches in the VTP domain?

A. transparent
B. server
C. client

D. local
E. pass-through

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 568
Which three statements regarding VLANs are true? (Choose three.)

A. To create a new VLAN on a Cisco Catalyst switch, the VLAN name, VLAN ID and VLAN type must all be specifically configured by the administrator.
B. A VLAN is a broadcast domain.
C. Each VLAN must have an SVI configured on the Cisco Catalyst switch for it to be operational.
D. The native VLAN is used for untagged traffic on an 802.1Q trunk.
E. VLANs can be connected across wide-area networks.

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 569
Which type of VPN is based on the concept of trusted group members using the GDOI key management protocol?

A. DMVPN
B. SSLVPN
C. GETVPN
D. EzVPN
E. MPLS VPN
F. FlexVPN

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 570
Based on RFC 4890, what is the ICMP type and code that should never be dropped by the firewall to allow PMTUD?

A. ICMPv6 Type 1 Code 0 no route to host
B. ICMPv6 Type 1 Code 1 communication with destination administratively prohibited
C. ICMPv6 Type 2 Code 0 packet too big
D. ICMPv6 Type 3 Code 1 fragment reassembly time exceeded
E. ICMPv6 Type 128 Code 0 echo request

F. ICMPv6 Type 129 Code 0 echo reply

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 571
Which technology, configured on the Cisco ASA, allows Active Directory authentication credentials to be applied automatically to web forms that require authentication for clientless SSL connections?

A. one-time passwords
B. certificate authentication
C. user credentials obtained during authentication
D. Kerberos authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 572
A firewall rule that filters on the protocol field of an IP packet is acting on which layer of the OSI reference model?

A. network layer
B. application layer
C. transport layer
D. session layer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 573
Which layer of the OSI model is referenced when utilizing http inspection on the Cisco ASA to filter Instant Messaging or Peer to Peer networks with the Modular Policy Framework?

A. application layer
B. presentation layer
C. network layer
D. transport layer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 574
When a Cisco IOS Router receives a TCP packet with a TTL value less than or equal to 1, what will it do?

A. route the packet normally
B. drop the packet and reply with an ICMP Type 3, Code 1 (Destination Unreachable, Host Unreachable)
C. drop the packet and reply with an ICMP Type 11, Code 0 (Time Exceeded, Hop Count Exceeded)
D. drop the packet and reply with an ICMP Type 14, Code 0 (Timestamp Reply)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 575
In an 802.11 WLAN, which option is the Layer 2 identifier of a basic service set, and also is typically the MAC address of the radio of the access point?

A. BSSID
B. SSID
C. VBSSID
D. MBSSID

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 576
What term describes an access point which is detected by your wireless network, but is not a trusted or managed access point?

A. rogue
B. unclassified
C. interferer
D. malicious

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 577
Which two security measures are provided when you configure 802.1X on switchports that connect to corporate-controlled wireless access points? (Choose two.)

A. It prevents rogue APs from being wired into the network.

B. It provides encryption capability of data traffic between APs and controllers.
C. It prevents rogue clients from accessing the wired network.
D. It ensures that 802.1x requirements for wired PCs can no longer be bypassed by disconnecting the AP and connecting a PC in its place.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 578
In what subnet does address 192.168.23.197/27 reside?

A. 192.168.23.0
B. 192.168.23.128
C. 192.168.23.160
D. 192.168.23.192
E. 192.168.23.196

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 579
A router has four interfaces addressed as 10.1.1.1/24, 10.1.2.1/24, 10.1.3.1/24, and 10.1.4.1/24. What is the smallest summary route that can be advertised covering these four subnets?

A. 10.1.2.0/22
B. 10.1.0.0/22
C. 10.1.0.0/21
D. 10.1.0.0/16

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 580
Which two address translation types can map a group of private addresses to a smaller group of public addresses? (Choose two.)

A. static NAT
B. dynamic NAT
C. dynamic NAT with overloading
D. PAT
E. VAT

Correct Answer: CD

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 581
Given the IPv4 address 10.10.100.16, which two addresses are valid IPv4-compatible IPv6 addresses? (Choose two.)

A. :::A:A:64:10
B. ::10:10:100:16
C. 0:0:0:0:0:10:10:100:16
D. 0:0:10:10:100:16:0:0:0

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 582
Which authentication mechanism is available to OSPFv3?

A. simple passwords
B. MD5
C. null
D. IKEv2
E. IPsec AH/ESP

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 583
Which two IPv6 tunnel types support only point-to-point communication? (Choose two.)

A. manually configured
B. automatic 6to4
C. ISATAP
D. GRE

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 584
Which two EIGRP packet types are considered to be unreliable packets? (Choose two.)

A. update
B. query
C. reply
D. hello
E. acknowledgement

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 585
Before BGP update messages may be sent, a neighbor must stabilize into which neighbor state?

A. active
B. idle
C. connected
D. established

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 586
What is the size of a point-to-point GRE header, and what is the protocol number at the IP layer?

A. 8 bytes, and protocol number 74
B. 4 bytes, and protocol number 47
C. 2 bytes, and protocol number 71
D. 24 bytes, and protocol number 1
E. 8 bytes, and protocol number 47

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 587
Which three statements are correct when comparing Mobile IPv6 and Mobile IPv4 support? (Choose three.)

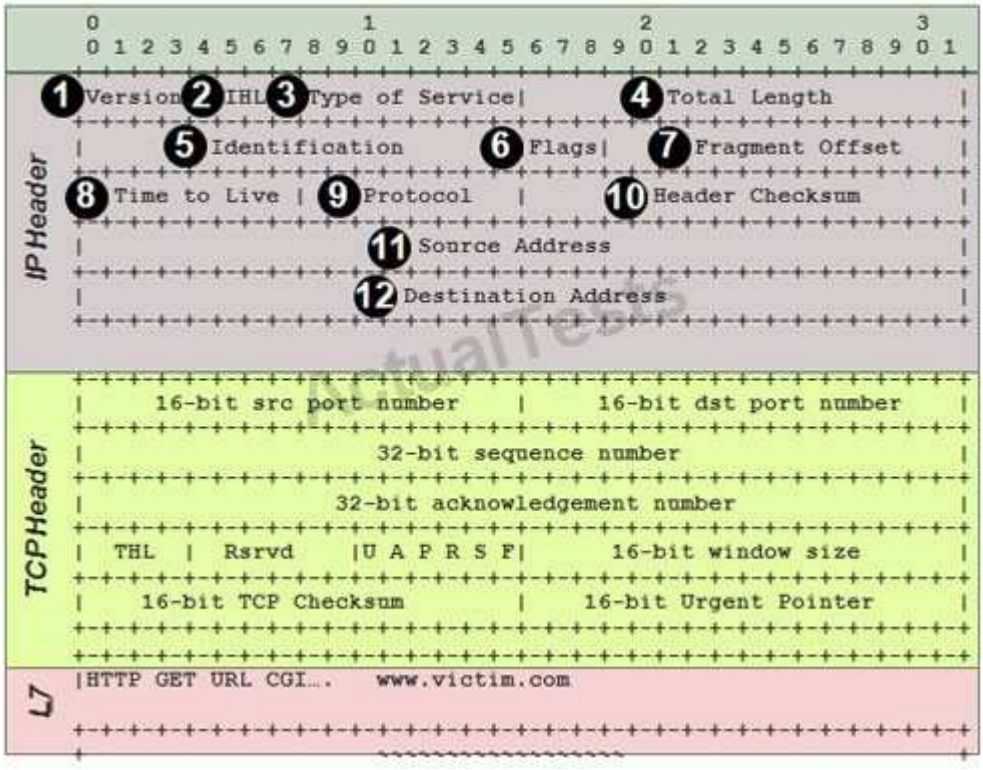
A. Mobile IPv6 does not require a foreign agent, but Mobile IPv4 does.
B. Mobile IPv6 supports route optimization as a fundamental part of the protocol; IPv4 requires extensions.
C. Mobile IPv6 and Mobile IPv4 use a directed broadcast approach for home agent address discovery.
D. Mobile IPv6 makes use of its own routing header; Mobile IPv4 uses only IP encapsulation.
E. Mobile IPv6 and Mobile IPv4 use ARP for neighbor discovery.

F. Mobile IPv4 has adopted the use of IPv6 ND.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 588
Refer to the exhibit.



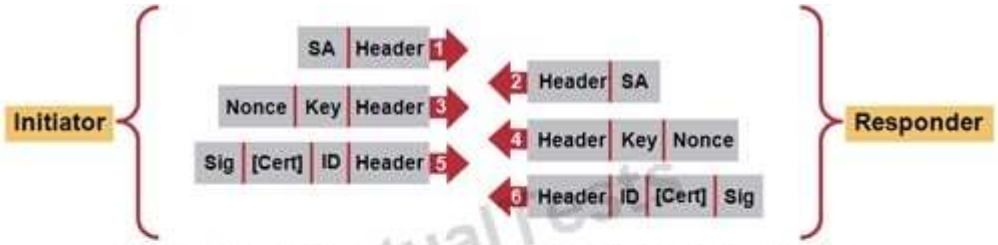
Which three fields of the IP header labeled can be used in a spoofing attack? (Choose one.)

A. 6,7,11
B. 6,11,12
C. 3,11,12
D. 4,7,11

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 589
Refer to the exhibit.



- MSG 1: Initiator offers acceptable encryption and authentication algorithms (3DES, MD5, and RSA, which is also called the transform-set)
- MSG 2: Responder presents acceptance of the proposal (or it might not)
- MSG 3: Initiator Diffie-Helman key and nounce (the key value is usually a number of 1024-bit length)
- MSG 4: Responder Diffie-Helman key and nounce
- MSG 5: Initiator signature, ID, and keys (maybe cert), which is also known as authentication data
- MSG 6: Responder signature, ID, and keys (maybe cert)

Which message could contain an authenticated initial_contact notify during IKE main mode negotiation?

A. message 3
B. message 5
C. message 1
D. none, initial_contact is sent only during quick mode
E. none, notify messages are sent only as independent message types

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 590
Which two answers describe provisions of the SOX Act and its international counterpart Acts? (Choose two.)

A. confidentiality and integrity of customer records and credit card information
B. accountability in the event of corporate fraud
C. financial information handled by entities such as banks, and mortgage and insurance brokers
D. assurance of the accuracy of financial records
E. US Federal government information
F. security standards that protect healthcare patient data

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 591
Which protocol does 802.1X use between the supplicant and the authenticator to authenticate users who wish to access the network?

A. SNMP
B. TACACS+
C. RADIUS
D. EAP over LAN
E. PPPoE

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 592
Which two statements are correct regarding the AES encryption algorithm? (Choose two.)

A. It is a FIPS-approved symmetric block cipher.
B. It supports a block size of 128, 192, or 256 bits.
C. It supports a variable length block size from 16 to 448 bits.
D. It supports a cipher key size of 128, 192, or 256 bits.
E. The AES encryption algorithm is based on the presumed difficulty of factoring large integers.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 593
What are two benefits of using IKEv2 instead of IKEv1 when deploying remote-access IPsec VPNs? (Choose two.)

A. IKEv2 supports EAP authentication methods as part of the protocol.
B. IKEv2 inherently supports NAT traversal.
C. IKEv2 messages use random message IDs.
D. The IKEv2 SA plus the IPsec SA can be established in six messages instead of nine messages.
E. All IKEv2 messages are encryption-protected.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 594
DNSSEC was designed to overcome which security limitation of DNS?

A. DNS man-in-the-middle attacks
B. DNS flood attacks
C. DNS fragmentation attacks
D. DNS hash attacks

E. DNS replay attacks
F. DNS violation attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 595
Which two statements about SHA are correct? (Choose two.)

A. Five 32-bit variables are applied to the message to produce the 160-bit hash.
B. The message is split into 64-bit blocks for processing.
C. The message is split into 512-bit blocks for processing.
D. SHA-2 and MD5 both consist of four rounds of processing.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 596
Which three statements about IKEv2 are correct? (Choose three.)

A. INITIAL_CONTACT is used to synchronize state between peers.
B. The IKEv2 standard defines a method for fragmenting large messages.
C. The initial exchanges of IKEv2 consist of IKE_SA_INIT and IKE_AUTH.
D. Rekeying IKE and child SAs is facilitated by the IKEv2 CREATE_CHILD_SA exchange.
E. NAT-T is not supported.
F. Attribute policy push (via the configuration payload) is only supported in REQUEST/REPLY mode.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 597
Which three statements about LDAP are true ? (Choose three.)

A. LDAP uses UDP port 389 by default.
B. LDAP is defined in terms of ASN.1 and transmitted using BER.
C. LDAP is used for accessing X.500 directory services.
D. An LDAP directory entry is uniquely identified by its DN.
E. A secure connection via TLS is established via the UseTLS operation.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 598
Which two EAP methods may be susceptible to offline dictionary attacks? (Choose two.)

A. EAP-MD5
B. LEAP
C. PEAP with MS-CHAPv2
D. EAP-FAST

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 599
Which PKCS is invoked during IKE MM5 and MM6 when digital certificates are used as the authentication method?

A. PKCS#7
B. PKCS#10
C. PKCS#13
D. PKCS#11
E. PKCS#3

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 600
Which three statements are true about MACsec? (Choose three.)

A. It supports GCM modes of AES and 3DES.
B. It is defined under IEEE 802.1AE.
C. It provides hop-by-hop encryption at Layer 2.
D. MACsec expects a strict order of frames to prevent anti-replay.
E. MKA is used for session and encryption key management.
F. It uses EAP PACs to distribute encryption keys.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Topic 7, Volume G

QUESTION 601
Which option is a benefit of implementing RFC 2827?

A. prevents DoS from legitimate, non-hostile end systems
B. prevents disruption of special services such as Mobile IP
C. defeats DoS attacks which employ IP source address spoofing
D. restricts directed broadcasts at the ingress router
E. allows DHCP or BOOTP packets to reach the relay agents as appropriate

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 602
IPsec SAs can be applied as a security mechanism for which three options? (Choose three.)

A. SeND
B. Mobile IPv6
C. site-to-site virtual interfaces
D. OSPFv3
E. CAPWAP
F. LWAPP

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 603
Which four options are valid EAP mechanisms to be used with WPA2? (Choose four.)

A. PEAP
B. EAP-TLS
C. EAP-FAST
D. EAP-TTLS
E. EAPOL
F. EAP-RADIUS
G. EAP-MD5

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 604
Which three features describe DTLS protocol? (Choose three.)

A. DTLS handshake does not support reordering or manage loss packets.
B. DTLS provides enhanced security, as compared to TLS.
C. DTLS provides block cipher encryption and decryption services.
D. DTLS is designed to prevent man-in-the-middle attacks, message tampering, and message forgery.
E. DTLS is used by application layer protocols that use UDP as a transport mechanism.
F. DTLS does not support replay detection.

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 605
Which three statements are true about the SSH protocol? (Choose three.)

A. SSH protocol runs over TCP port 23.
B. SSH protocol provides for secure remote login and other secure network services over an insecure network.
C. Telnet is more secure than SSH for remote terminal access.
D. SSH protocol runs over UDP port 22.
E. SSH transport protocol provides for authentication, key exchange, confidentiality, and integrity.
F. SSH authentication protocol supports public key, password, host based, or none as authentication methods.

Correct Answer: BEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 606
Which statement regarding TFTP is not true?

A. Communication is initiated over UDP port 69.
B. Files are transferred using a secondary data channel.
C. Data is transferred using fixed-size blocks.
D. TFTP authentication information is sent in clear text.
E. TFTP is often utilized by operating system boot loader procedures.
F. The TFTP protocol is implemented by a wide variety of operating systems and network devices.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 607
Which two statements are true when comparing ESMTP and SMTP? (Choose two.)

A. Only SMTP inspection is provided on the Cisco ASA firewall.
B. A mail sender identifies itself as only able to support SMTP by issuing an EHLO command to the mail server.

C. ESMTP mail servers will respond to an EHLO with a list of the additional extensions they support.
D. SMTP commands must be in upper case, whereas ESMTP can be either lower or upper case.
E. ESMTP servers can identify the maximum email size they can receive by using the SIZE command.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 608
How does a DHCP client request its previously used IP address in a DHCP DISCOVER packet?

A. It is included in the CIADDR field.
B. It is included as DHCP Option 50 in the OPTIONS field.
C. It is included in the YIADDR field.
D. It is the source IP address of the UDP/53 wrapper packet.
E. The client cannot request its last IP address; it is assigned automatically by the server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 609
Which two statements about an authoritative server in a DNS system are true? (Choose two.)

A. It indicates that it is authoritative for a name by setting the AA bit in responses.
B. It has a direct connection to one of the root name servers.
C. It has a ratio of exactly one authoritative name server per domain.
D. It cannot cache or respond to queries from domains outside its authority.
E. It has a ratio of at least one authoritative name server per domain.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 610
User A at Company A is trying to transfer files to Company B, using FTP. User A can connect to the FTP server at Company B correctly, but User A cannot get a directory listing or upload files.
The session hangs.

What are two possible causes for this problem? (Choose two.)

A. Active FTP is being used, and the firewall at Company A is not allowing the returning data connection to be initiated from the FTP server at Company B.
B. Passive FTP is being used, and the firewall at Company A is not allowing the returning data connection to be initiated from the FTP server at Company B.
C. At Company A, active FTP is being used with a non-application aware firewall applying NAT to the source

address of User A only.

D. The FTP server administrator at Company B has disallowed User A from accessing files on that server.
E. Passive FTP is being used, and the firewall at Company B is not allowing connections through to port 20 on the FTP server.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 611
Refer to the exhibit. Which three statements are true? (Choose three.)

A. Because of a "root delay" of 0ms, this router is probably receiving its time directly from a Stratum 0 or 1 GPS reference clock.
B. This router has correctly synchronized its clock to its NTP master.
C. The NTP server is running authentication and should be trusted as a valid time source.
D. Specific local time zones have not been configured on this router.
E. This router will not act as an NTP server for requests from other devices.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 612
Which three security features were introduced with the SNMPv3 protocol? (Choose three.)

A. Message integrity, which ensures that a packet has not been tampered with in-transit
B. DoS prevention, which ensures that the device cannot be impacted by SNMP buffer overflow
C. Authentication, which ensures that the message is from a valid source
D. Authorization, which allows access to certain data sections for certain authorized users
E. Digital certificates, which ensure nonrepudiation of authentications
F. Encryption of the packet to prevent it from being seen by an unauthorized source

Correct Answer: ACF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 613
Which common Microsoft protocol allows Microsoft machine administration and operates over TCP port 3389?

A. remote desktop protocol
B. desktop mirroring
C. desktop shadowing
D. Tarantella remote desktop

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 614
To prevent a potential attack on a Cisco IOS router with the echo service enabled, what action should you take?

A. Disable the service with the no ip echo command.
B. Disable the service with the no echo command.
C. Disable tcp-small-servers.
D. Disable this service with a global access-list.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 615
Which three new capabilities were added to HTTP v1.1 over HTTP v1.0? (Choose three.)

A. chunked transfer encoding
B. HTTP pipelining
C. POST method
D. HTTP cookies
E. keepalive mechanism

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 616
Which query type is required for an nslookup on an IPv6 addressed host?

A. type=AAAA
B. type=ANY
C. type=PTR
D. type=NAME-IPV6

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 617
According to OWASP guidelines, what is the recommended method to prevent cross-site request forgery?

A. Allow only POST requests.
B. Mark all cookies as HTTP only.
C. Use per-session challenge tokens in links within your web application.
D. Always use the "secure" attribute for cookies.
E. Require strong passwords.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 618
Which option is used to collect wireless traffic passively, for the purposes of eavesdropping or information gathering?

A. network taps
B. repeater Access Points
C. wireless sniffers
D. intrusion prevention systems

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 619
Which traffic class is defined for non-business-relevant applications and receives any bandwidth that remains after QoS policies have been applied?

A. scavenger class
B. best effort
C. discard eligible
D. priority queued

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 620
In the context of a botnet, what is true regarding a command and control server?

A. It can launch an attack using IRC or Twitter.
B. It is another name for a zombie.
C. It is used to generate a worm.

D. It sends the command to the botnets via adware.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 621
Which option is used for anti-replay prevention in a Cisco IOS IPsec implementation?

A. session token
B. one-time password
C. time stamps
D. sequence number
E. nonce

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 622
Which three Cisco security product features assist in preventing TCP-based man-in-the-middle attacks? (Choose three.)

A. Cisco ASA TCP initial sequence number randomization?
B. Cisco ASA TCP sliding-window conformance validation?
C. Cisco IPS TCP stream reassembly?
D. Cisco IOS TCP maximum segment size adjustment?

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 623
Which would be the best method to deploy on a Cisco ASA to detect and prevent viruses and worms?

A. deep packet inspection
B. content security via the Control Security Services Module
C. Unicast Reverse Path Forwarding
D. IP audit signatures

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 624
Refer to the exhibit.

```
regex domainlist1 "\.facebook\.com"
regex domainlist2 "\.youtube\.com"
regex domainlist3 "\.twitter\.com"

class-map type regex match-any DomainBlockList
 match regex domainlist1
 match regex domainlist3

class-map type inspect http match-all BlockDomainsClass
 match request header host regex class DomainBlockList

policy-map type inspect http http_inspection_policy
 parameters
  protocol-violation action drop-connection
 class BlockDomainsClass
  reset log

policy-map inside-policy
 class httptraffic
  inspect http http_inspection_policy

service-policy inside-policy interface inside
```


What will be the default action?

A. HTTP traffic to the Facebook, Youtube, and Twitter websites will be dropped.
B. HTTP traffic to the Facebook and Youtube websites will be dropped.
C. HTTP traffic to the Youtube and Twitter websites will be dropped.
D. HTTP traffic to the Facebook and Twitter websites will be dropped.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 625
Which Cisco ASA feature can be used to update non-compliant antivirus/antispyware definition files on an AnyConnect client?

A. dynamic access policies
B. dynamic access policies with Host Scan and advanced endpoint assessment
C. Cisco Secure Desktop

D. advanced endpoint assessment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 626
Refer to the exhibit.

When configuring a Cisco IPS custom signature, what type of signature engine must you use to block podcast clients from accessing the network?

A. service HTTP
B. service TCP
C. string TCP
D. fixed TCP
E. service GENERIC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 627
An attacker configures an access point to broadcast the same SSID that is used at a public hot- spot, and launches a deauthentication attack against the clients that are connected to the hot-spot, with the hope that the clients will then associate to the AP of the attacker.

In addition to the deauthentication attack, what attack has been launched?

A. man-in-the-middle
B. MAC spoofing
C. Layer 1 DoS
D. disassociation attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 628
Which four IPv6 messages should be allowed to transit a transparent firewall? (Choose four.)

A. router solicitation with hop limit = 1
B. router advertisement with hop limit = 1
C. neighbor solicitation with hop limit = 255
D. neighbor advertisement with hop limit = 255
E. listener query with link-local source address
F. listener report with link-local source address

Correct Answer: CDEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 629
Which statement best describes the concepts of rootkits and privilege escalation?

A. Rootkits propagate themselves.
B. Privilege escalation is the result of a rootkit.
C. Rootkits are a result of a privilege escalation.
D. Both of these require a TCP port to gain access.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 630
Refer to the exhibit of an ISAKMP debug.

```
ISAKMP (62): processing SA payload. message ID = 0
ISAKMP (62): Checking ISAKMP transform 1 against priority 10 policy
                    encryption DES-CBC
                    hash SHA
                    default group 1
                    auth pre-share
ISAKMP (62): atts are acceptable. Next payload is 0
ISAKMP (62): SA is doing pre-shared key authentication
ISAKMP (62): processing KE payload. message ID = 0
ISAKMP (62): processing NONCE payload. message ID = 0
ISAKMP (62): SKEYID state generated
ISAKMP (62); processing vendor id payload
ISAKMP (62): speaking to another Cisco IOS box!
ISAKMP: reserved not zero on ID payload!
%CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 172.16.100.201
 failed its sanity check or is malformed
```

Which message of the exchange is failing?

A. main mode 1
B. main mode 3
C. aggressive mode 1
D. main mode 5
E. aggressive mode 2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 631
Which multicast capability is not supported by the Cisco ASA appliance?

A. ASA configured as a rendezvous point
B. sending multicast traffic across a VPN tunnel
C. NAT of multicast traffic
D. IGMP forwarding (stub) mode

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 632
Refer to the exhibit.

```
regex App_regex_1
"[uU][nN][iI][oO][nN]([%]2[0bB]|[+])([aA][lL][lL]([%]2[0bB]|[+]))?
[sS][eE][lL][eE][cC][tT]"
regex App_regex_2 "[Ss][Ee][Ll][Ee][Cc][Tt](%2[0bB]|+)[^\r\x00-
\x19\x7f-\xff]+(%2[0bB]|+)[Ff][Rr][Oo][Mm](%2[0bB]|+)"
!
class-map WebServers
 match port tcp eq www
class-map type inspect http match-any App-map
 match request body regex App_regex_1
 match request body regex App_regex_2
!
policy-map type inspect http drop-Protocol
parameters
  body-match-maximum  3000
class App-map
  drop-connection log
policy-map protocol-traffic
class WebServers
  inspect http drop-Protocol
!
service-policy protocol-traffic interface  outside
```

What type of attack is being mitigated on the Cisco ASA appliance?

A. HTTPS certificate man-in-the-middle attack
B. HTTP distributed denial of service attack
C. HTTP Shockwave Flash exploit
D. HTTP SQL injection attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 633
Which method of output queuing is supported on the Cisco ASA appliance?

A. CBWFQ
B. priority queuing
C. MDRR
D. WFQ
E. custom queuing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 634
Which statement is true regarding Cisco ASA operations using software versions 8.3 and later?

A. The global access list is matched first before the interface access lists.
B. Both the interface and global access lists can be applied in the input or output direction.
C. When creating an access list entry using the Cisco ASDM Add Access Rule window, choosing "global" as the interface will apply the access list entry globally.
D. NAT control is enabled by default.
E. The static CLI command is used to configure static NAT translation rules.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 635
Which four values can be used by the Cisco IPS appliance in the risk rating calculation? (Choose four.)

A. attack severity rating
B. target value rating
C. signature fidelity rating
D. promiscuous delta
E. threat rating
F. alert rating

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 636
Which three authentication methods does the Cisco IBNS Flexible Authentication feature support? (Choose three.)

A. cut-through proxy
B. dot1x
C. MAB
D. SSO
E. web authentication

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 637
Troubleshooting the web authentication fallback feature on a Cisco Catalyst switch shows that clients with the 802.1X supplicant are able to authenticate, but clients without the supplicant are not able to use web authentication. Which configuration option will correct this issue?

A. switch(config)# aaa accounting auth-proxy default start-stop group radius
B. switch(config-if)# authentication host-mode multi-auth
C. switch(config-if)# webauth
D. switch(config)# ip http server
E. switch(config-if)# authentication priority webauth dot1x

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 638
Which option on the Cisco ASA appliance must be enabled when implementing botnet traffic filtering?

A. HTTP inspection
B. static entries in the botnet blacklist and whitelist
C. global ACL
D. NetFlow
E. DNS inspection and DNS snooping

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 639
Refer to the exhibit.

To configure the Cisco ASA, what should you enter in the Name field, under the Group Authentication option for the IPSec VPN client?

A. group policy name
B. crypto map name
C. isakmp policy name
D. crypto ipsec transform-set name
E. tunnel group name

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 640
Refer to the exhibit.

```
!other commands omitted
switch(config-if)# switchport access vlan 10
switch(config-if)# switchport mode access
switch(config-if)# switchport voice vlan 20
switch(config-if)# dot1x pae authenticator
switch(config-if)#authentication port-control auto
switch(config-if)#authentication host-mode multi-domain
switch(config-if)#authentication order mab dot1x
switch(config-if)#authentication priority dot1x mab
switch(config-if)#mab
!other commands omitted
```

Which statement about this Cisco Catalyst switch 802.1X configuration is true?

A. If an IP phone behind the switch port has an 802.1X supplicant, MAC address bypass will still be used to authenticate the IP Phone.
B. If an IP phone behind the switch port has an 802.1X supplicant, 802.1X authentication will be used to authenticate the IP phone.
C. The authentication host-mode multi-domain command enables the PC connected behind the IP phone to bypass 802.1X authentication.
D. Using the authentication host-mode multi-domain command will allow up to eight PCs connected behind the IP phone via a hub to be individually authentication using 802.1X.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 641
Which C3PL configuration component is used to tune the inspection timers such as setting the tcp idle-time and tcp synwait-time on the Cisco ZBFW?

A. class-map type inspect
B. parameter-map type inspect
C. service-policy type inspect
D. policy-map type inspect tcp
E. inspect-map type tcp

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 642
Which signature engine is used to create a custom IPS signature on a Cisco IPS appliance that triggers when a vulnerable web application identified by the "/runscript.php" URI is run?

A. AIC HTTP
B. Service HTTP
C. String TCP
D. Atomic IP
E. META
F. Multi-String

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 643
Which Cisco IPS appliance feature can automatically adjust the risk rating of IPS events based on the reputation of the attacker?

A. botnet traffic filter
B. event action rules
C. anomaly detection
D. reputation filtering
E. global correlation inspection

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 644
The ASA can be configured to drop IPv6 headers with routing-type 0 using the MPF. Choose the correct configuration.

A. policy-map type inspect ipv6 IPv6_PMAP
match header routing-type eq 0
drop log
B. policy-map type inspect icmpv6 ICMPv6_PMAP
match header routing-type eq 0
drop log
C. policy-map type inspect ipv6-header HEADER_PMAP
match header routing-type eq 0
drop log
D. policy-map type inspect http HEADER_PMAP
match routing-header 0
drop log
E. policy-map type inspect ipv6 IPv6_PMAP
match header type 0
drop log
F. policy-map type inspect ipv6-header HEADER_PMAP

match header type 0
drop log

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 645
Refer to the exhibit.

```
Client
|
|
(inside)
ZBFW
(outside)
|
|
Server

zone security inside
zone security outside

 interface inside
     zone-member security inside

interface outside
     zone-member security outside

class-map type inspect match-all HTTP_CMAP
     match protocol HTTP
class-map type inspect match-all TCP_CMAP
     match protocol TCP

policy-map type inspect IN-OUT_PMAP
     class type inspect TCP_CMAP
          inspect
     class type inspect HTTP_CMAP
          pass
     class class-default
          drop

zone-pair IN-OUT_ZP source inside destination outside
     service-policy type inspect IN-OUT_PMAP
```


With the client protected by the firewall, an HTTP connection from the client to the server on TCP port 80 will be subject to which action?

A. inspection action by the HTTP_CMAP
B. inspection action by the TCP_CMAP

C. drop action by the default class
D. inspection action by both the HTTP_CMAP and TCP_CMAP
E. pass action by the HTTP_CMAP
F. drop action due to class-map misclassification

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 646
Which mode of operation must be enabled on CSM to support roles such as Network Administrator, Approver, Network Operator, and Help Desk?

A. Deployment Mode
B. Activity Mode
C. Workflow Mode
D. User Roles Mode
E. Administration Mode
F. Network Mode

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 647
Which two ISE Probes would be required to distinguish accurately the difference between an iPad and a MacBook Pro? (Choose two.)

A. DHCP or DHCPSPAN
B. SNMPTRAP
C. SNMPQUERY
D. NESSUS
E. HTTP
F. DHCP TRAP

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 648
Which configuration option will correctly process network authentication and authorization using both 802.1X and MAB on a single port?

A.
```
interface FastEthernet1/0/9
 switchport access vlan 200
 switchport mode access
 switchport voice vlan 40
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication event server dead action authorize vlan 200
 authentication event server alive action reinitialize
 authentication host-mode multi-domain
 authentication open
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
 ip dhcp snooping information option allow-untrusted
end
```

B.
```
interface FastEthernet1/0/9
 switchport access vlan 200
 switchport mode access
 switchport voice vlan 40
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication event server dead action authorize vlan 200
 authentication event server alive action reinitialize
 authentication host-mode multi-domain
 authentication open
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
 ip dhcp snooping information option allow-untrusted
end
```

C.
```
interface FastEthernet1/0/9
 switchport access vlan 200
 switchport mode access
 switchport voice vlan 40
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication event server dead action authorize vlan 200
 authentication event server alive action reinitialize
 authentication host-mode multi-domain
 authentication open
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
 ip dhcp snooping information option allow-untrusted
end
```

D.
```
interface FastEthernet1/0/9
 switchport access vlan 200
 switchport mode access
 switchport voice vlan 40
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication event server dead action authorize vlan 200
 authentication event server alive action reinitialize
 authentication host-mode multi-domain
 authentication open
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control force-unauthorized
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
 ip dhcp snooping information option allow-untrusted
end
```

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 649
Which statement regarding the routing functions of the Cisco ASA is true?

A. The translation table can override the routing table for new connections.
B. The ASA supports policy-based routing with route maps?.
C. In a failover pair of ASAs, the standby firewall establishes a peer relationship with OSPF neighbors.
D. Routes to the Null0 interface can be configured to black-hole traffic.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 650
Refer to the exhibit.

```
!
access-list routemapacl standard deny host 10.66.42.215
access-list routemapacl standard deny 10.40.29.0 255.255.255.0
access-list routemapacl standard deny 10.39.24.0 255.255.255.0
access-list routemapacl standard permit any
!
route outside 10.39.23.0 255.255.255.0 192.168.1.1 1
route outside 10.39.24.0 255.255.255.0 192.168.1.1 1
route outside 10.39.27.0 255.255.255.0 192.168.1.1 1
route outside 10.40.29.0 255.255.255.0 192.168.1.1 1
route outside 10.40.30.0 255.255.255.0 192.168.1.1 1
route outside 10.66.42.215 255.255.255.255 192.168.1.1 1
!
route-map static_route_map permit 10
 match ip address routemapacl
!
router ospf 90
 network 192.168.1.0 255.255.255.0 area 0
 log-adj-changes
 redistribute static subnets route-map static_route_map
```


Which route will be advertised by the Cisco ASA to its OSPF neighbors?

A. 10.39.23.0/24
B. 10.40.29.0/24
C. 10.66.42.215/32
D. 10.40.29.0/24

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 651

Which three statements are true about the Cisco ASA object configuration below? (Choose three.)

```
object network vpnclients
range 10.1.100.4 10.1.100.10
object network vpnclients
nat (outside,outside) dynamic interface
```

A. The NAT configuration in the object specifies a PAT rule?.
B. This configuration requires the command same-security-traffic inter-interface for traffic that matches this NAT rule to pass through the Cisco ASA appliance.
C. The NAT rule of this object will be placed in Section 1 (Auto-NAT) of the Cisco ASA NAT table?.
D. This configuration is most likely used to provide Internet access to connected VPN clients.
E. Addresses in the range will be assigned during config-mode.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 652
Which three options can be configured within the definition of a network object, as introduced in Cisco ASA version 8.3(1)? (Choose three.)

A. range of IP addresses
B. subnet of IP addresses
C. destination IP NAT translation
D. source IP NAT translation
E. source and destination FQDNs
F. port and protocol ranges

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 653
Which three attributes may be configured as part of the Common Tasks panel of an authorization profile in the Cisco ISE solution? (Choose three.)

A. VLAN
B. voice VLAN
C. dACL name
D. voice domain permission
E. SGT

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 654
Which two statements describe the Cisco TrustSec system correctly? (Choose two.)

A. The Cisco TrustSec system is a partner program, where Cisco certifies third-party security products as extensions to the secure infrastructure.
B. The Cisco TrustSec system is an approach to certifying multimedia and collaboration applications as secure.
C. The Cisco TrustSec system is an Advanced Network Access Control System that leverages enforcement intelligence in the network infrastructure.
D. The Cisco TrustSec system tests and certifies all products and product versions that make up the system as working together in a validated manner.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 655
Which option is the correct definition for MAB?

A. MAB is the process of checking the mac-address-table on the local switch for the sticky address. If the mac-address of the device attempting to access the network matches the configured sticky address, it will be permitted to bypass 802.1X authentication.
B. MAB is a process where the switch will send an authentication request on behalf of the endpoint that is attempting to access the network, using the mac-address of the device as the credentials. The authentication server evaluates that MAC address against a list of devices permitted to access the network without a stronger authentication.
C. MAB is a process where the switch will check a local list of MAC addresses to identify systems that are permitted network access without using 802.1X.
D. MAB is a process where the supplicant on the endpoint is configured to send the MAC address of the endpoint as its credentials.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 656
Regarding VSAs, which statement is true?

A. VSAs may be implemented on any RADIUS server.
B. VSAs are proprietary, and therefore may only be used on the RADIUS server of that vendor. For example, a Cisco VSA may only be used on a Cisco RADIUS server, such as ACS or ISE.
C. VSAs do not apply to RADIUS; they are a TACACS attribute.
D. Each VSA is defined in an RFC and is considered to be a standard.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 657
Which four items may be checked via a Cisco NAC Agent posture assessment? (Choose four.)

A. Microsoft Windows registry keys
B. the existence of specific processes in memory
C. the UUID of an Apple iPad or iPhone
D. if a service is started on a Windows host
E. the HTTP User-Agent string of a device
F. if an Apple iPad or iPhone has been "jail-broken"
G. if an antivirus application is installed on an Apple MacBook

Correct Answer: ABDG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 658
Which three statements are true about the Cisco NAC Appliance solution? (Choose three.)

A. In a Layer 3 OOB ACL deployment of the Cisco NAC Appliance, the discovery host must be configured as the untrusted IP address of the Cisco NAC Appliance Server.
B. In a Cisco NAC Appliance deployment, the discovery host must be configured on a Cisco router using the "NAC discovery-host" global configuration command.
C. In a VRF-style OOB deployment of the Cisco NAC Appliance, the discovery host may be the IP address that is on the trusted side of the Cisco NAC Appliance Server.
D. In a Layer 3 IB deployment of the Cisco NAC Appliance, the discovery host may be configured as the IP address of the Cisco NAC Appliance Manager.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 659
Refer to the exhibit.

```
R1# show crypto engine connection active

  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
   1 <none>          <none>          set    HMAC_SHA+3DES_56_C      0        0
2000 FastEthernet0/1 172.16.1.10     set    HMAC_MD5+3DES_56_C      0        0
2001 FastEthernet0/1 172.16.1.10     set    HMAC_MD5+3DES_56_C      9        0
```

```
R2# show crypto engine connection active

  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
   1 FastEthernet0/0 172.16.1.20     set    HMAC_SHA+3DES_56_C      0        0
2000 FastEthernet0/0 172.16.1.20     set    HMAC_MD5+3DES_56_C      0        9
2001 FastEthernet0/0 172.16.1.20     set    HMAC_MD5+3DES_56_C      0        0
```

On R1, encrypt counters are incrementing. On R2, packets are decrypted, but the encrypt counter is not being incremented. What is the most likely cause of this issue?

A. a routing problem on R1
B. a routing problem on R2
C. incomplete IPsec SA establishment
D. crypto engine failure on R2
E. IPsec rekeying is occurring

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 660
Refer to the exhibit, which shows a partial output of the show command.

```
sslvpn1#show webvpn context
Codes: AS - Admin Status, OS - Operation Status
       VHost - Virtual Host
Context Name          AS   OS
------------          ---- --------
vpn1                  down down
```


Which statement best describes the problem?

A. Context vpn1 is not inservice.
B. There is no gateway that is configured under context vpn1.
C. The config has not been properly updated for context vpn1.
D. The gateway that is configured under context vpn1 is not inservice.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 661
Which three statements are true about the transparent firewall mode in Cisco ASA? (Choose three.)

A. The firewall is not a routed hop.
B. The firewall can connect to the same Layer 3 network on its inside and outside interfaces.
C. Static routes are supported.
D. PAT and NAT are not supported.
E. Only one global address per device is supported for management.
F. SSL VPN is supported for management.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 662
Which three statements about Cisco IOS RRI are correct? (Choose three.)

A. RRI is not supported with ipsec-profiles.
B. Routes are created from ACL entries when they are applied to a static crypto map.
C. Routes are created from source proxy IDs by the receiver with dynamic crypto maps.
D. VRF-based routes are supported.
E. RRI must be configured with DMVPN.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 663
Review the exhibit.

With inline VLAN pairs on a sensor:

A. You cannot pair a VLAN with itself.

B. For a given sensing interface, an interface used in a VLAN pair can be a member of another inline interface pair.

C. For a given sensing interface, a VLAN can be a member of only one inline VLAN pair; however, a given VLAN can be a member of an inline VLAN pair on more than one sensing interface.

D. The order in which you specifiy the VLANs in a inline pair is significant.

E. A sensing interface in inline VLAN pair mode can have from 1 to 255 inline VLAN pairs.

Which three statements about the Cisco IPS sensor are true? (Choose three.)

A. A
B. B
C. C
D. D
E. E

Correct Answer: ACE

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 664
An internal DNS server requires a NAT on a Cisco IOS router that is dual-homed to separate ISPs using distinct CIDR blocks. Which NAT capability is required to allow hosts in each CIDR block to contact the DNS server via one translated address?

A. NAT overload
B. NAT extendable
C. NAT TCP load balancing
D. NAT service-type DNS
E. NAT port-to-application mapping

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 665
Refer to the exhibit.

```
ip routing

crypto isakmp policy 1
 authentication pre-share
!
crypto isakmp key myPreshareKey0 address ipv6
3FFE:2002::A8BB:CCFF:FE01:2C02/128
!
crypto ipsec transform-set 3des ah-sha-hmac esp-3des
!
crypto ipsec profile profile0
 set transform-set 3des
!
ipv6 cef
!
interface Tunnel0
 ipv6 address 3FFE:1001::/64 eui-64
 ipv6 cef
 tunnel source Ethernet2/0
 tunnel destination 3FFE:2002::A8BB:CCFF:FE01:2C02
 tunnel protection ipsec profile profile0
```


Which three command sets are required to complete this IPv6 IPsec site-to-site VTI? (Choose three.)

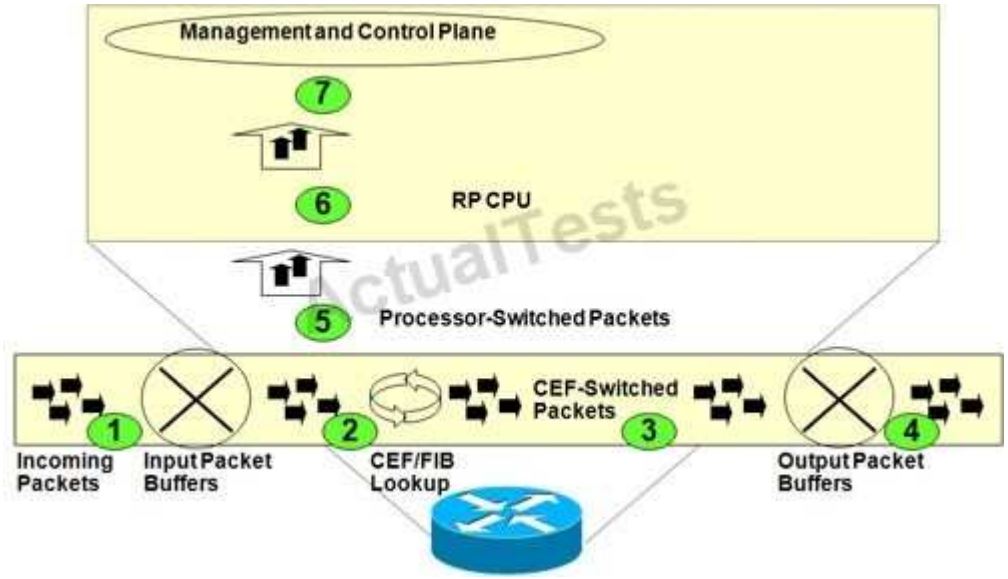
A. interface Tunnel0
   tunnel mode ipsec ipv6
B. crypto isakmp-profile
   match identity address ipv6 any
C. interface Tunnel0
   ipv6 enable
D. ipv6 unicast-routing

E. interface Tunnel0
ipv6 enable-ipsec

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 666
Refer to the exhibit.



Which option correctly identifies the point on the exhibit where Control Plane Policing (input) is applied to incoming packets?

A. point 6
B. point 7
C. point 4
D. point 1
E. points 5 and 6

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 667
Which three types of information could be used during the incident response investigation phase? (Choose three.)

A. netflow data
B. SNMP alerts

C. encryption policy
D. syslog output
E. IT compliance reports

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 668
Which three statements about the IANA are true? (Choose three.)

A. IANA is a department that is operated by the IETF.
B. IANA oversees global IP address allocation.
C. IANA managed the root zone in the DNS.
D. IANA is administered by the ICANN.
E. IANA defines URI schemes for use on the Internet.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 669
Refer to the exhibit.

```
vtp mode transparent
!
vlan 600
 private-vlan community
vlan 400
 private-vlan isolated
vlan 200
 private-vlan primary
 private-vlan association 400,600
!
interface FastEthernet 5/1
 switchport mode private-vlan host
 switchport private-vlan host-association 200 400
!
interface FastEthernet 5/2
 switchport mode private-vlan host
 switchport private-vlan host-association 200 600
!
interface FastEthernet 5/3
 switchport mode private-vlan host
 switchport private-vlan host-association 200 600
!
Interface FastEthernet 5/4
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 200 400,600
!
```


Which two statements about this Cisco Catalyst switch configuration are correct? (Choose two.)

A. The default gateway for VLAN 200 should be attached to the FastEthernet 5/1 interface.
B. Hosts attached to the FastEthernet 5/1 interface can communicate only with hosts attached to the FastEthernet 5/4 interface.
C. Hosts attached to the FastEthernet 5/2 interface can communicate with hosts attached to the FastEthernet 5/3 interface.
D. Hosts attached to the FastEthernet 5/4 interface can communicate only with hosts attached to the FastEthernet 5/2 and FastEthernet 5/3 interfaces.
E. Interface FastEthernet 5/1 is the community port.
F. Interface FastEthernet 5/4 is the isolated port.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 670
Which three configuration components are required to implement QoS policies on Cisco routers using MQC? (Choose three.)

A. class-map
B. global-policy
C. policy-map
D. service-policy
E. inspect-map

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 671
Which QoS marking is only locally significant on a Cisco router?

A. MPLS EXP
B. DSCP
C. QoS group
D. IP precedence
E. traffic class
F. flow label

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 672
Which three control plane subinterfaces are available when implementing Cisco IOS Control Plane Protection? (Choose three.)

A. CPU
B. host
C. fast-cache
D. transit
E. CEF-exception
F. management

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 673
Which type of PVLAN ports can communicate among themselves and with the promiscuous port?

A. isolated
B. community

C. primary
D. secondary
E. protected

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 674
Which statement is true about the Cisco NEAT 802.1X feature?

A. The multidomain authentication feature is not supported on the authenticator switch interface.
B. It allows a Cisco Catalyst switch to act as a supplicant to another Cisco Catalyst authenticator switch.
C. The supplicant switch uses CDP to send MAC address information of the connected host to the authenticator switch.
D. It supports redundant links between the supplicant switch and the authenticator switch.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 675
Which additional configuration component is required to implement a MACSec Key Agreement policy on user-facing Cisco Catalyst switch ports?

A. PKI
B. TACACS+
C. multi-auth host mode
D. port security
E. 802.1x

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 676
With the Cisco FlexVPN solution, which four VPN deployments are supported? (Choose four.)

A. site-to-site IPsec tunnels?
B. dynamic spoke-to-spoke IPSec tunnels? (partial mesh)
C. remote access from software or hardware IPsec clients?
D. distributed full mesh IPsec tunnels?
E. IPsec group encryption using GDOI?
F. hub-and-spoke IPsec tunnels?

Correct Answer: ABCF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 677
Which four techniques can you use for IP management plane security? (Choose four.)

A. Management Plane Protection
B. uRPF
C. strong passwords
D. RBAC
E. SNMP security measures
F. MD5 authentication

Correct Answer: ACDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 678
Which three statements about remotely triggered black hole filtering are true? (Choose three.)

A. It filters undesirable traffic.
B. It uses BGP or OSPF to trigger a network-wide remotely controlled response to attacks.
C. It provides a rapid-response technique that can be used in handling security-related events and incidents.
D. It requires uRPF.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 679
Which three statements about Cisco Flexible NetFlow are true? (Choose three.)

A. The packet information used to create flows is not configurable by the user.
B. It supports IPv4 and IPv6 packet fields.
C. It tracks all fields of an IPv4 header as well as sections of the data payload.
D. It uses two types of flow cache, normal and permanent.
E. It can be a useful tool in monitoring the network for attacks.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 680
Management Frame Protection is available in two deployment modes, Infrastructure and Client. Which three statements describe the differences between these modes? (Choose three.)

A. Infrastructure mode appends a MIC to management frames.
B. Client mode encrypts management frames.
C. Infrastructure mode can detect and prevent common DoS attacks.
D. Client mode can detect and prevent common DoS attacks.
E. Infrastructure mode requires Cisco Compatible Extensions version 5 support on clients.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 681
Which three object tracking options are supported by Cisco IOS policy-based routing? (Choose three.)

A. absence of an entry in the routing table
B. existence of a CDP neighbor relationship
C. existence of an entry in the routing table
D. results of an SAA operation
E. state of the line protocol of an interface

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 682
Which four protocols are supported by Cisco IOS Management Plane Protection? (Choose four.)

A. Blocks Extensible Exchange Protocol (BEEP)
B. Hypertext Transfer Protocol Secure (HTTPS)
C. Secure Copy Protocol (SCP)
D. Secure File Transfer Protocol (SFTP)
E. Secure Shell (SSH)
F. Simple Network Management Protocol (SNMP)

Correct Answer: ABEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 683
Which four Cisco IOS features are used to implement First Hop Security in IPv6? (Choose four.)

A. IPv6 First-Hop Security Binding Table

B. IPv6 Device Tracking
C. IPv6 RA Guard
D. SeND
E. IPv6 Selective Packet Discard
F. IPv6 Source Guard

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 684
Which two identifiers are used by a Cisco Easy VPN Server to reference the correct group policy information for connecting a Cisco Easy VPN Client? (Choose two.)

A. IKE ID_KEY_ID
B. OU field in a certificate that is presented by a client
C. XAUTH username
D. hash of the OTP that is sent during XAUTH challenge/response
E. IKE ID_IPV4_ADDR

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 685
According ISO27001 ISMS, which of the following are mandatory documents? (Choose 4)

A. ISMS Policy
B. Corrective Action Procedure
C. IS Procedures
D. Risk Assessment Reports
E. Complete Inventory of all information assets

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 686
Which current RFC made RFCs 2409, 2407, and 2408 obsolete?

A. RFC 4306
B. RFC 2401
C. RFC 5996
D. RFC 4301
E. RFC 1825

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: