TestKingdom

Premium Provider In IT Certification & Testing

Consider your-self **Certified**

Exam : 350-018

Title : CCIE Pre-Qualification Test for Security

Version : 6.0

Dated : 02/04/2010

Type : 232 Q & A with Explanation

QUESTION 1
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

Answer: E

QUESTION 2
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

Answer: E

QUESTION 3
Which 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 2)

A. N to S:RADIUS Access- Challenge
S to N: RADIUS Access-Accept

B. N to S:RADIUS Access-Request
S to N: RADIUS Access-Reject
N to S:RADIUS Access- Challenge
S to N: RADIUS Access-Accept

C. C to N: RADIUS Access-Request
N to C: RADIUS Access- Reject
C to N: RADIUS Access- Challenge
N to C: RADIUS Access-Accept

D. C to N: RADIUS Access-Request
N to C: RADIUS Access-Accept

E. N to S:RADIUS Access-Request
S to N: RADIUS Access-Challenge
N to S: RADIUS Access-Request
S to N: RADIUS Access-Accept

Answer: D,E

QUESTION 4
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.

Answer: F

QUESTION 5
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-treeportfast 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.

Answer: D

QUESTION 6
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.

Answer: D

QUESTION 7
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

Answer: D

QUESTION 8
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

Answer: D

QUESTION 9
When an IPS device in single interface VLAN-pairing mode fires a signature from the normalizer engine and TCP-based packets are dropped, which of the following would be a probable cause?

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.

Answer: A,B

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.
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 NM?CIDS, AIP?SSM?10, and AIP?SSM?20.

QUESTION 10
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 receivedIPsec 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.

Answer: B

QUESTION 11
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

Answer: A,C

QUESTION 12
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

Answer: B,C

QUESTION 13
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)

Answer: A,B,D,E

QUESTION 14
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
```

Testkingdom

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

Answer: B

QUESTION 15
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 routergenerages 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.

Answer: E

QUESTION 16
What 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

Answer: C

QUESTION 17
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 policycannot cannot be edited.
B. Edit the existing policy
C. Clone and then edit the new policy
D. Add the existingpoicy to the group and then edit the desired parameters.
E. Create and edit a new, similar policy.

Answer: C,E

QUESTION 18
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

Answer: B

QUESTION 19
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.

Answer: C

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 20
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

Answer: A

QUESTION 21
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 anda vulnerability used to run malicious software off of the stack.

Answer: B

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 22
Drop

Answer:

QUESTION 23
Asymmetric and symmetric ciphers differ in which of the following way(s)? (Choose 2)

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.

Answer: A,B

QUESTION 24
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.

Answer: B,C,D,E

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 25
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

Answer: C,D,E

QUESTION 26
Refer to 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 what two actions? (Choose 2)

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

Answer: A,D

QUESTION 27
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. ASAsyn protection
B. ASA ICMP application inspection.
C. CSA quarantine lists.
D. IPSsyn attack signatures.
E. Cisco Guard

Answer: C

QUESTION 28
What is Chain of Evidence in the context of security forensics?

A. The concept that evidence is controlled and accounted for as to not disrupt its authenticity and integrity
B. The concept that evidence is controlled in locked down, but not necessarily authenticated
C. 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
D. The concept that the general whereabouts of evidence is known

Answer: A

Explanation:
Forensic investigations typically consist of two phases. The first phase, known as the exploratory phase, is an attempt by the investigator to identify the nature of the problem at hand and to define what s/he thinks transpired at the scene of the incident. Once the investigator has determined what s/he thinks took place the induction ends and the deduction, i.e. the evidence phase, begins.

Fig. 1: Chain of Evidence Linking User to Crime

Testkingdom

Chain-of-Evidence Model
The Chain-of-Evidence Model illustrates the discrete sets of actions carried out by an insider attempting to inflict malicious damage in an intranet environment. One group of actions is separated from another, based on the level of authority required to execute them. Each group of actions has a different corresponding source of evidence that must be responsible for

documenting activity for forensic purposes. However each such source of evidence must be linked to the logs next to it (see above figure) in order to form a complete chain of evidence.
The figure above starts with physical access to computer systems that must precede any malicious activity. It is in this stage that the crucial link between physical recognition and computer recognition take place. Following log-on procedures the user proceeds to invoke the services of a network application that must be used as a vehicle to inflict damage on a remote system. The network application issues the malicious network traffic that reaches a remote computer and executes the intended behavior.

QUESTION 29
ASDM on the ASA platform is executed as:

A. A fully operational Visual Basicapplicaton.
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 frameworkapplicaton.

Answer: C

QUESTION 30
Which of the following is true for RFC 4301 - Security Architecture for the Internet Protocol (obsoletes RFC 2401) - (Select 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 forIPsec-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)

Answer: A,C

QUESTION 31
Which of the following is one way to configure the security appliance to protect against DoS attacks?

A. Using theemb_lim option in the acl command
B. Using thetcp_max_conns option in the nat command
C. Using theemb_lim option in the static command
D. Using theemb_conns argument in the global command

Answer: C

QUESTION 32
Which is a benefit of implementing RFC 2827?

A. Prevents Dos fromlegimate, 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

Answer: E

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 33
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.

Answer: C

QUESTION 34
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)

Answer: B

QUESTION 35
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.

Answer: E

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 IPSSupplied 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.

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 36
Which of these is the best way to provide sender non-repudiation?

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

Answer: D

QUESTION 37
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

Answer: A,D,E

QUESTION 38
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 BGPfixup configuration
C. Addnorandomseq 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

Answer: C

QUESTION 39
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 anEOUoUPD identity profile for clientless hosts.
C. Statically maps an access list to a NACAgentless Host (NAH)
D. Statically authorizes and maps devices to an access policy.

Answer: D

QUESTION 40
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.

Answer: C

QUESTION 41
Which two are correct functions of the Cisco Anomaly Guard and Detector for preventing DDOS attacks?(Choose two)

A. usesNetflow data for anomaly detections
B. using topology and configurationawareness,events from different devices are correlated and attacks mitgitations are performed at the optimal location
C. builds baseline profiles of normal operatingconditions,enabling rapid identification of unusual activity that indicates an attack
D. dynamic diversion redirects and cleans only traffic destined for targeteddevices,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 viasyslog,SDEE and SNMP

Answer: C,D

QUESTION 42
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

Answer: C

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 43
What 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.

Answer: C

QUESTION 44
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 version1operations.

Answer: A,D,E

QUESTION 45
Which of the following is the correct diagram for an IPsec Authentication Header?

A.

B.

C.

D.

E.

Testkingdom

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

Answer: C

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)			Testkingdom

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 46
An attacker is attempting to Telnet 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 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 (nodiscard)
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

Answer: C

QUESTION 47
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. Thereceipient 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

Answer: E

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 48
Refer to the Exhibit. Which of the following R1 router configurations will correctly prevent R3 from becoming a PIM neighor with rendezvous point R1?

A. access-list 1 deny 192.168.1.3 255.255.255.255
!
interface fa0/0
ip pim neighbor-filter 1

B. access-list 1permit 192.168.1.3 255.255.255.255
ip pim rp-announce-filter rp-list 1
C. access-list 1permit 192.168.1.2 255.255.255.255
access-list 1 deny any
!
interface fa0/0
ip pim bidir-neighbor-filter 1

D. access-list 1permit 192.168.1.2 255.255.255.255
!
interface fa0/0
ip multicast boundary 1 filter-autorop

E. access-list 1 deny 192.168.1.3 255.255.255.255
!
interface fa0/0
ip igmp access-group 1

Answer: A

QUESTION 49
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. encryptionaes
B. hashsha 1
C. cryptoisakmp policy 7
D. group 2
E. lifetime 86400
F. authenticationrsa-sig

Answer: B

QUESTION 50
What 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.

Answer: C

QUESTION 51
Which two IP multicast addresses belong to the group represented by the MAC address of 0x01-00-5E-15-6A-2C?

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

Answer: A,B

QUESTION 52
Which two of followings are correct regarding the Cisco Trust Agent (CTA)? (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 applyQoS 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.

Answer: A,B

QUESTION 53
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

Answer: A,B

QUESTION 54
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
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

Answer: E

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:
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 55
If you perform a network trace of a ping going through an IPSec/3-DES tunnel, what would be true with respect to the appearance of a tunneled/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.

Answer: A

QUESTION 56
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

Answer: E

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 57
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_

Answer: C

QUESTION 58
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 ismet, 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.

Answer: D

QUESTION 59
Drop

Answer:

QUESTION 60
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.

Answer: A

QUESTION 61
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 Attributeimplementation, 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.

Answer: B,C,D

QUESTION 62
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

Answer: D

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 63
What is NTP crucial for?

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

Answer: C,E,F

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 timespecific events occur.
http://www.cisco.com/en/US/tech/ CK6 48/ CK3 62/ CK4 61/tsd_technology_support_subprotocol_ 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 64
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

Answer: A,C,F

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 authproxy 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.

Testkingdom

QUESTION 65

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?

```
hostname R1
!
aaa new-model
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authorization exec default local
aaa authorization network sdm_vpn_group_ml_1 local
!
username test privilege 15 secret 5 $1$K3Vc$VYvd
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group test
 key cisco123
 pool SDM_POOL_1
 acl 100
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
!
crypto dynamic-map SDM_DYNMAP_1 1
 set transform-set ESP-3DES-SHA
!
crypto map SDM_CMAP_1 client authentication list sdm_vpn_xauth_ml_1
crypto map SDM_CMAP_1 isakmp authorization list sdm_vpn_group_ml_1
crypto map SDM_CMAP_1 client configuration address respond
crypto map SDM_CMAP_1 65535 ipsec-isakmp dynamic SDM_DYNMAP_1
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 crypto map SDM_CMAP_1
!
interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.0
!
ip local pool SDM_POOL_1 172.16.1.100 172.16.1.120
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
ip http server
ip http authentication local
ip http secure-server
ip http timeout-policy idle 600 life 86400 requests 10000
!
access-list 100 permit ip any 172.16.0.0 0.0.255.255
!
```

Testkingdom

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 ismisconfigured.

Answer: C

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.htm
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.htm
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 66
Drop

Answer:

QUESTION 67

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

Answer: C

QUESTION 68
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
```

Testkingdom

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

Answer: A,D

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
Defaults
Debugging is disabled.
Command Modes
EXEC
Command History
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.
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
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 69
What 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

Answer: C

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 70
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

Answer: D

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 71
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

Answer: B,C,D

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_sheet0900aecd80225ae1.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 72
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. Thesyslog 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 thesyslog 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.

Answer: A,B,C

QUESTION 73
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 thevty lines
C. Configure the host name of the router
D. Enable AAA Authentication
E. Configure the SSH version that the router will use

Answer: A,C

QUESTION 74
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 $65104^
ip as-path access-list 1permit any
B. ip as-path access-list 1 deny_65104$

ip as-path access-list 1permit^$
C. ip as-path access-list 1 deny_65104$
ip as-path access-list 1permit.*
D. ip as-path access-list 1 deny_65104_
ip as-path access-list 1permit.*
E. ip as-path access-list 1 deny_65104_
ip as-path access-list 1permit any
F. ip as-path access-list 1 deny ^65104$
ip as-path access-list 1permit.*

Answer: C

QUESTION 75
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

Answer: D,E

QUESTION 76
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 ESPheader,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 confidentialityservice,but it does not provide data origin authentication.To achieve data origin authentication,AH must be used.

Answer: A,D

QUESTION 77
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 ChangeCipherSpec Protocol
C. SSL Record Protocol
D. SSL Handshake Protocol

Answer: C

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 Reccrd 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 78
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.

Answer: E

QUESTION 79
What is NTP crucial for?

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

Answer: A,C,D

QUESTION 80
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

Answer: B

QUESTION 81
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
```

Testkingdom

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

Answer: D,E,F

QUESTION 82
In an L2TP voluntary tunneling scenario, the VPDN tunel is terminated between:

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

Answer: D

QUESTION 83
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

Answer: E

QUESTION 84
Referring to the DMVPN topology diagram shown in the exhibit, which two statements are correct? (Choose two)

A. At the Spoke Arouter,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 bebuilt, 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 interfaceip address
D. At the Spoke Arouter,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

Answer: B,F

QUESTION 85
Referring to the network diagram and the partial router's 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.

Answer: A

QUESTION 86
When enrolling a Cisco IOS router to a CA server using the SCEP protocol, which one of the following is NOT a required step?

A. Authenticate the CA server's certificate.
B. Configure anip 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 cryptopki trustpoint on the router.

Answer: D

QUESTION 87
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.

Answer: B,F

QUESTION 88
Figure 1 represents 3 security contexts all sharing a common 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
D. Normalizer

Answer: B

QUESTION 89
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

Answer: C

QUESTION 90
Which of the following statements that describe the PPTP protocol is incorrect?

A. A single PPTP tunnel can carry multiple end-to-endppp 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.

Answer: B

QUESTION 91
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.

Answer: C

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 92
When configuring a multipoint GRE (Mgre) 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. tunnelvrf

Answer: B

QUESTION 93
A network administrator is using a LAN analyzer to troubleshoot OSPF router exchange messages sent to ALL OSPF ROUTERS. To what MAC address 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

Answer: A

QUESTION 94
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

Answer: D

QUESTION 95
Which of the following is true about the Cisco IOS-IPS functionality? (Choose 2)

A. To activate new signatures you download a new SignatureDefition 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.

Answer: A,E

QUESTION 96
Drop

Answer:

QUESTION 97
Which of the following is one way to configure the security appliance to protect against DoS attacks?

A. Using theemb_lim option in the acl command.
B. Using thetcp_max_conns option in the nat command
C. Using theemb_lim option in the static command.
D. Using theemb_conns argument in the global command.

Answer: C

QUESTION 98
Referring to the partial IOS configuration shown in the exhibit,which two statements are

true?(Choose three)

```
ip inspect name test icmp alert on audit-trail on timeout 30
!
interface Ethernet0
ip address 192.168.10.2 255.255.255.0
ip inspect test in
!
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
```

Testkingdom

A. All outbound ICMP traffic will be inspected by the IOS Firewall
B. Ethernet0 is the trusted interface and Ethernet1 is theuntrusted 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

Answer: A,B,E

QUESTION 99
When implementing best practices for IP Source Address Spoofing and Defeating Denial of Service Attacks with IP Source Address Spoofing, what RFC is commonly used to protect your network?

A. RFC 2827
B. RFC 1918
C. RFC 1149
D. RFC 3704

Answer: A

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 100
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 VTPmuti-domain feature should be restricted to migration and temporary implementation.
E. When using secure modeVTP,only configure management domain passwords on VTP servers.

Answer: B,C

Explanation:
VTP has 3 protocol versions Version 1, 2, & 3. VTP Version 3 incorporates many changes from VTP V1 and V2.
VTP Messages in Detail
VTP packets are sent in either Inter-Switch Link (ISL) frames or in IEEE 802.1Q (dot1q) frames. These packets are sent to the destination MAC address 01-00-0C-CC-CC-CC with a logical link control (LLC) code of Subnetwork Access Protocol (SNAP) (AAAA) and a type of 2003 (in the SNAP header). This is the format of a VTP packet that is encapsulated in ISL frames:

Of course, you can have a VTP packet inside 802.1Q frames. In that case, the ISL header and cyclic redundancy check (CRC) is replaced by dot1q tagging.
Summary Advertisements
By default, Catalyst switches issue summary advertisements in five-minute increments. Summary advertisements inform adjacent Catalysts of the current VTP domain name and the configuration revision number.
When the switch receives a summary advertisement packet, the switch compares the VTP domain name to its own VTP domain name. If the name is different, the switch simply ignores the packet. If the name is the same, the switch then compares the configuration revision to its own revision. If its own configuration revision is higher or equal, the packet is ignored. If it is lower, an advertisement request is sent.

Summary Advert Packet Format:

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
Version	Code	Followers	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revision Number			
Updater Identity			
Update Timestamp (12 bytes)			
MD5 Digest (16 bytes)			

Testkingdom

This list clarifies what the fields means in the summary advertisement packet:
* The Followers field indicates that this packet is followed by a Subset Advertisement packet.
* The Updater Identity is the IP address of the switch that is the last to have incremented the configuration revision.
* The Update Timestamp is the date and time of the last increment of the configuration revision.
* Message Digest 5 (MD5) carries the VTP password, if MD5 is configured and used to authenticate the validation of a VTP update.

Subset Advertisements

When you add, delete, or change a VLAN in a Catalyst, the server Catalyst where the changes are made increments the configuration revision and issues a summary advertisement. One or several subset advertisements follow the summary advertisement. A subset advertisement contains a list of VLAN information. If there are several VLANs, more than one subset advertisement can be required in order to advertise all the VLANs.

Subset Advert Packet Format:

VTP Pruning
VTP ensures that all switches in the VTP domain are aware of all VLANs. However, there are occasions when VTP can create unnecessary traffic. All unknown unicasts and broadcasts in a VLAN are flooded over the entire VLAN. All switches in the network receive all broadcasts, even in situations in which few users are connected in that VLAN. VTP pruning is a feature that you use in order to eliminate or prune this unnecessary traffic.
http://www.cisco.com/warp/public/473/21.html#vtp_pruning
VLAN Pruning
VTP can prune unneeded VLANs from trunk links. VTP maintains a map of VLANs and switches, enabling traffic to be directed only to those switches known to have ports on the intended VLAN . This enables more efficient use of trunk bandwidth.
Each switch will advertise which VLAN's it has active to neighboring switches. The neighboring switches will then "prune" VLAN's that are not active across that trunk, thus saving bandwidth. If a VLAN is then added to one of the switches, the switch will then re-advertise it's active VLAN's so that pruning can be updated by its neighbors. For this to work, VLAN pruning must be enabled on both ends of the trunk. It is easiest to enable VLAN pruning for an entire VTP management domain by simply enabling it on one of the VTP servers for that domain. To enable VLAN pruning for a VTP domain, enter the following command on a VTP server for that domain...
VTP_Server_ Sw1(config)# vtp pruning
This will then propagate to all switches in the vtp domain.
Configure VLAN Pruning

QUESTION 101
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 proxyagent, 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

Answer: C

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.
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 102
Drop

Answer:

QUESTION 103

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.
```
+----+-------------+------------+
| AH | orig ip hdr | ip payload |
+----+-------------+------------+
```

B.
```
+------------+---+------------+-----------+
| New IP hdr |AH |orig ip hdr | ip payload|
+------------+---+------------+-----------+
```

C.
```
+------------+-----------+----+
|orig ip hdr | ip payload | AH |
+------------+-----------+----+
```

D.
```
+------------+----+------------+
|orig ip hdr | AH | ip payload |
-------------+----+------------+
```

Testkingdom

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

Answer: D

Explanation:
Not B: The question 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.

```
              BEFORE APPLYING AH
        ----------------------------
IPv4    |orig IP hdr  |     |      |
        |(any options)| TCP | Data |
        ----------------------------

              AFTER APPLYING AH
        ---------------------------------
IPv4    |orig IP hdr  |     |     |      |
        |(any options)| AH | TCP | Data |
        ---------------------------------
        |<------- authenticated -
             except for mutable fields
```

Testkingdom

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

```
                    BEFORE APPLYING AH
        ---------------------------------------
IPv6    |              | ext hdrs |      |      |
        | orig IP hdr  |if present| TCP  | Data |
        ---------------------------------------

                    AFTER APPLYING AH
        -------------------------------------------------------------
IPv6    |              |hop-by-hop, dest*, |     | dest |      |      |
        |orig IP hdr   |routing, fragment. | AH  | opt* | TCP  | Data |
        -------------------------------------------------------------
        |<---- authenticated except for mutable fields ----------->|
```

Testkingdom

```
             * = if present, could be before AH, after AH, or both
```

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

```
        ------------------------------------------------
IPv4    | new IP hdr* |     | orig IP hdr*  |     |      |
        |(any options)| AH  | (any options) |TCP  | Data |
        ------------------------------------------------
        |<- authenticated except for mutable fields -->|
        |            in the new IP hdr                 |

        ------------------------------------------------------------
IPv6    |            | ext hdrs*|     |             | ext hdrs*|    |     |
        |new IP hdr*|if present| AH |orig IP hdr*|if present|TCP|Data|
        -------------------------------------------------------
        |<-- authenticated except for mutable fields in new IP hdr -->|
```

Testkingdom

http://www.faqs.org/rfcs/rfc2402.html
See RFC 2402

QUESTION 104
Drop

Answer:

QUESTION 105
What technologies are included in Anti-X? (Choose 3)

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

Answer: A,D,E

QUESTION 106
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 becreated.Once that is operational,the old virtual link can be removed.
B. Once a MD5 key is configured a hash iscreated.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 oldone.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

Answer: D

QUESTION 107
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 encryptedpre_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 frompre_master_secret

Answer: C

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.

```
Client                                               Server

ClientHello
(empty SessionTicket extension)------->
                                              ServerHello
                             (empty SessionTicket extension)
                                             Certificate*
                                       ServerKeyExchange*
                                      CertificateRequest*
                              <--------      ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished                      -------->
                                         NewSessionTicket
                                       [ChangeCipherSpec]
                              <--------
Application Data              <------->     Application Data
```

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 .

```
RFC 4507              Stateless TLS Session Resumption              May 2006


      Client                                                  Server

      ClientHello
      (SessionTicket extension)       -------->
                                                         ServerHello
                                  (empty SessionTicket extension)
                                                   NewSessionTicket
                                                 [ChangeCipherSpec]
                                   <--------             Finished
      [ChangeCipherSpec]
      Finished                     -------->
      Application Data             <------->     Application Data

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

Testkingdom

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 108

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

Answer: D

QUESTION 109

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 establishinga security incident response systems.
E. Tools to support the development ofpirvotal, forward-looking information system technologies.
F. The international standards for evaluating trust in information systems and products.

Answer: F

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 110
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

Answer: D

QUESTION 111
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_*$

Answer: B

QUESTION 112
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
```

Testkingdom

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

Answer: A,D

QUESTION 113
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.

Answer: A

QUESTION 114
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

Answer: A,E

Explanation:
Answer A is incorret because, in cryptography , MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128- bit hash value. As an Internet standard (RFC 1321). It is easy to generate MD5 collisions, it is possible for the person who created the file to create a second file with the same checksum, so this technique cannot protect against some forms of malicious tampering
The SHA hash functions are five cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard . SHA stands for Secure Hash Algorithm. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length. They are called "secure" when (in the words of the standard), "it is computationally infeasible to:

find a message that corresponds to a given message digest, or
find two different messages that produce the same message digest.
Any change to a message will, with a very high probability, result in a different message digest ."
B is correct and C is incorrect because of the following
The five algorithms are denoted SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. The latter four variants are sometimes collectively referred to as SHA-2. SHA-1 produces a message digest that is 160 bits long; the number in the other four algorithms' names denote the bit length of the digest they produce.
SHA-1 is employed in several widely used security applications and protocols, including TLS and SSL , PGP , SSH , S/MIME , and IPsec . It was considered to be the successor to MD5 , an earlier, widely-used hash function.
E is incorroct because of the following
The security of SHA-1 has been somewhat compromised by cryptography researchers [1] . Although no attacks have yet been reported on the SHA-2 variants, they are algorithmically similar to SHA-1 and so efforts are underway to develop improved alternative hashing algorithms. [2] HYPERLINK \ l "_note-2"[3] An open competition for a new SHA-3 function was formally announced in the Federal Register on November 2, 2007. [4] "NIST is initiating an effort to develop one or more additional hash algorithms through a public competition, similar to the development process for the Advanced Encryption Standard (AES)." [5] Submissions are due October 31, 2008 and the proclamation of a winner and publication of the new standard are scheduled to take place in 2012.

QUESTION 115
Select the best answer to this question. ASA/PIX Active/Active failover can be used to loadbalance.

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

Answer: A

QUESTION 116
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 PKItrustpoint (CA)
F. Import the SSH client fingerprint.

Answer: A,B,D

QUESTION 117
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.

Answer: C

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 118
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 theswitchport 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 manuallyconfigured the secured MAC addresses on the switchport.
E. allows the switch to restrict the MAC addresses on theswitchport based on the static MAC addresses configured in the startup configuration.

Answer: A

Explanation:
The switch supports these types of secure MAC addresses:
Static secure MAC addresses- These are manually configured by using the switchport portsecurity 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 119
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
```

Testkingdom

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

Answer: B

QUESTION 120
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

Answer: B

QUESTION 121
During STP troubleshooting , you determined 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 theportfast access ports

Answer: D

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.

Testkingdom

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.
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 122
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
```

Testkingdom

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.

Answer: A

QUESTION 123
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 ´000
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
```

Testkingdom

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.

Answer: C

QUESTION 124
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

Answer: B

QUESTION 125
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 utilizesOut-of- ban admission control

Answer: A,D,F

QUESTION 126
Why is NTP an important component when implementing IPSec VPN in a PKI environment?

A. To ensure the router has the correct time when generating its private/public key pairs.
B. To ensure the router time is sync with the remote peers for encryption keys generation.
C. To ensure the router time is sync with the remote peers during the DH exchange
D. To ensure the router time is sync with the remote peers when generating the cookies during IKE phase 1.
E. To ensure the router has the correct time when checking certificate validityform the remote peers.

Answer: E

QUESTION 127
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-action drop
Taking into consideration the shown configuration, what kind of attack are we attempting to mitigate?

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

Answer: E

QUESTION 128
To enable TCP Port Forwarding applications using IOS WebVPN,what needs to be downloaded to the client?

A. Cisco Security Agent (CSA)
B. SSL VPN Client (SVC) and Cisco SecureDesktop(CSD)
C. A small Java Applet
D. SSL VPN Client (SVC)
E. Cisco Trust Agent (CTA)
F. Cisco Security Desktop (CSD)

Answer: C

QUESTION 129
Which RFCs are used to establish internet connectivity from a private office with the following requirements?
1. 254 users
2. Only one IP address provided by your ISP.
3. Your IP address is assigned dynamically.
4. The CPE from the ISP is pre-provisioned and working.
5. You are expected to make changes on your router.

A. Network Address Translator (NAT) - Friendly Application Design Guidelines: Defined in RFC 3235.
B. DHCP: Defined in RFC 2131
C. IP Network Address Translator (NAT): Defined in RFC 1631.
D. IP Network Address Translator (NAT) Terminology and Considerations: Defined in RFC 2663.
E. PPP and IPCP: Defined in RFC 1332.
F. Address Allocation for Private Internets: Defined in RFC 1918

Answer: B,C,F

Explanation:

NAT will be required if the ISP has only provide 1 IP Address for all users to access the internet.
NAT is defined in both A & B. A expains CIDR and B explains NAT IP Address mappings.
Internally a private IP Address will be used these are defined in answer C RFC 1918.
The IP Addresses have to provided dynamically this is defined in F

QUESTION 130
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.

Answer: B,D

QUESTION 131
Which should be the key driver for a company security policy's 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.

Answer: A

QUESTION 132
Which statement is true about SYN cookies?

A. SYN cookies do not help to protect against SYN flood attacks.
B. State is kept on the server machine TCP stack.
C. A system has to check every incoming ACK against state tables.
D. No State is kept on the server machine state and is embedded in the systems Initial Sequence Number (ISN).

Answer: D

QUESTION 133
PEAP provides authentication for the EAP exchange using

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

Answer: D

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 134
Referring to the SDM screens shown, which two statements are true about the IOS Easy VPN Server configuration? (Choose two)

A. Pre-sharedkey(PSK) authentication will be used during the X-Auth phase
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 addresspool
D. Split tunneling is disabled because no protected subnets have been defined
E. Split tunneling is enabled where traffic that matches ACL 100 will not be encrypted
F. Toconnect, the remote VPN client will use a groupname of "test"

Answer: C,F

QUESTION 135
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. Currentips signatures.
E. Cisco Security Agent

Answer: C

QUESTION 136
What is the size of a point-to-point GRE header, and Protocol number at IP layer?

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

Answer: B

Explanation:
Explaination
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:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|R|K|S|s|Recur|  Flags  | Ver |         Protocol Type         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Checksum (optional)      |       Offset (optional)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Key (optional)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Sequence Number (optional)                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Routing (optional)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Testkingdom

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 137

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 thevlan 100
D. client without an 802.1x supplicant connecting to port fa0/1 will be assigned to thevlan 10
E. client connecting to port fa0/1 with an 802.1x supplicant but fails authentication will be assigned to thevlan 10

Answer: D

Explanation:
Explaination
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
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 138
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 CredentialsProvider(PCP)

Answer: C

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.

Refer to the numbers in Figure 2 above for each step described in the NAC authorization process.
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 139
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

Answer: A

QUESTION 140
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

Answer: B

QUESTION 141
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 anda 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 twopackets, 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)

Answer: C

QUESTION 142
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 astateful 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 andDDoS protection applied specifically for valid web servers.

Answer: D

QUESTION 143
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.

Answer: A

QUESTION 144
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

Answer: C

QUESTION 145
What are two key characteristics of VTP? (Choose 2)

A. VTP messages are sent out all switch-switch connections.
B. VTP manages addition, deletion, and renaming of VLANs 1 to 4094.
C. VTP V2 can only be used in a domain consisting of V2 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.

Answer: C,E

QUESTION 146
With PGP, which of the following entity signs a user's public key?

A. Thereceipient 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.

Answer: B

QUESTION 147
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)

Answer: A

QUESTION 148
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.

Answer: A

QUESTION 149
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

Answer: B,C,D

QUESTION 150
What is the best way to mitigate Browser Helper Objects (BHO) from being installed on your system?

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

Answer: C

QUESTION 151
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 thedmz.
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 thedmz or dmz2
F. Any IP traffic from any host on thedmz to any host on the outside.

Answer: C

QUESTION 152
Refer the 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 treeportfast

Answer: B

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

QUESTION 153
Drop

Answer:

QUESTION 154
Choose the correct security statements about the HTTP protocol and its use. (Choose 2)

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.

Answer: A,B

QUESTION 155
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 thevlan 100
B. client without an 802.1x supplicant connecting to port fa0/1 will be assigned to thevlan 10
C. client connecting to port fa0/1 with an 802.1x supplicant but fails authentication will be assigned to thevlan 10.
D. EAP over LAN frames will flow over VLAN 10
E. vlan 10, the guest vlan is also known as the restricted vlan

Answer: B

QUESTION 156
The following ip protocols and ports are commonly used in IPSec protocols.

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

Answer: A

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 157
What does qos pre-classify provides in regard to implementing QoS over GRE/IPSec VPN tunnels?

A. enables IOS to make a copy of the inner (original) IP header and to run aQoS classification before encryption, based on fields in the inner IP header.
B. enables IOS to classify packets based on theToS field in the inner (original) IP header.
C. enables IOS to classify packets based on theToS field in the outer tunnel IP header.
D. enables IOS to copy theToS field from the inner (original) IP header to the outer tunel IP header.
E. enables the IOS classification engine to only see a single encrypted and tunneled flow to reduce classification complexity.

Answer: A

QUESTION 158
What is the net effect of using ICMP Type 4 messages to attack RFC 1122 compliant hosts?

A. Hosts will perform a "hard" TCPreset 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 4message.
D. Hosts will perform a "soft" TCPreset and restart the connection.
E. Hosts will retransmit the last frame sent prior to receiving the ICMP type 4 message.

Answer: B

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]

Testkingdom

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 159
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 agroupname of "test."
F. Split tunneling is disabled because no protected subnets have been defined.

Answer: C,E

QUESTION 160
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.

Answer: B

QUESTION 161
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

Answer: B,C,D,E

QUESTION 162
Which two statements are correct about the aaa authentication login default group tacacs+ local global configuration command? (Choose two)

A. if thetacacs+ 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 thetacacs+ server is unavailable, authentication will succeed automatically by default.

Answer: A,B

QUESTION 163
Which IOS QoS mechanism is used strictly to rate limit traffic destined to the router itself?

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

Answer: B

QUESTION 164
What is true about SYN cookies?

A. All TCP options aresupported,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

Answer: C

QUESTION 165
The number of packets (or flows) dropped because they do not conform to the ASA/PIX security policy can be viewed using what command?

A. show counters drop

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

Answer: C

QUESTION 166
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

Answer: B,E

QUESTION 167
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.

Answer: B

QUESTION 168
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

Answer: B

QUESTION 169
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

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

Answer: B

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 170
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 contextmode
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

Answer: B

QUESTION 171
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.

Answer: C,D

QUESTION 172
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

Answer: C,F

QUESTION 173
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.

Answer: A

QUESTION 174
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 interfaceto 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 ruletopass through the firewall on the outside interface.
D. It allows traffic originating from the outside interfacetopass through the firewall on the inside interface without a NAT translation rule being matched.

Answer: C

QUESTION 175
Given the topology of a server (with IP 209.165.202.150) protected behind the inside interface of an ASA/PIX, and the Internet on the outside interface. Users on the Internet need to access the server at any time, but the firewall administrator does no want to NAT the address of the server since it is currently a public address. Which of the following commands can be used to accomplish this? (Choose 3)

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. nonat-control
D. access-list no-nat permit ip host 209.165.202.150 any
nat(inside) 0 access-list no-nat
E. nat (inside) 0 209.165.202.150.255.255.255.255

Answer: B,C,D

QUESTION 176
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

Answer: B,C,F

QUESTION 177
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

Answer: B

QUESTION 178
Which can control the per-user authorization of commands on a company router?

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

Answer: B

QUESTION 179
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.

Answer: A

QUESTION 180
Assume that you are a network technician of your company. Look at the following Cisco ASA adaptive security appliance rule samples, which one 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
```

Testkingdom

Answer: B

QUESTION 181
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

Answer: A

QUESTION 182
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

Answer: A

QUESTION 183
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.

Answer: A,B

QUESTION 184
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

Answer: A

QUESTION 185
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.

Answer: A

QUESTION 186
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.

Answer: A,C

QUESTION 187
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.

Answer: B

QUESTION 188
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.

Answer: A

QUESTION 189
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.

Answer: A

QUESTION 190
How many useable hosts can you get from a /30 subnet mask?

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

Answer: A

QUESTION 191
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.

Answer: A,B,C,D

QUESTION 192
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

Answer: A

QUESTION 193
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.

Answer: A

QUESTION 194
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

Answer: A

QUESTION 195
If you want to use RADIUS authenticatfon, 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

Answer: C

QUESTION 196
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.

Answer: A

QUESTION 197
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

Answer: A,B

QUESTION 198
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

Answer: A

QUESTION 199
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 lab
service = 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"

Answer: C

QUESTION 200
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.

Answer: A,B

QUESTION 201
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

Answer: A,B,C

QUESTION 202
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

Answer: A,C,D

QUESTION 203
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

Answer: B,C

QUESTION 204
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.

Answer: D

QUESTION 205
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.

Answer: C

QUESTION 206
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.

Answer: B

QUESTION 207
What command sequence should be used to turn on RADIUS in a router?

A. aaa new-model
aaa authen login default radius
radius-server host #.#.#.#
radius-server key <key>
B. aaa new-model
aaa 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

Answer: A

QUESTION 208
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.

Answer: A

QUESTION 209
What is the best argument for installing a stateful firewall to protect your network?

A. By default, stateful firewalls block all incoming traffic.
B. Stateful firewalls ensure that traffic returning through the router must originate from the inside (unless a static policy on the firewall overrides this behavior).
C. Stateful firewalls are the latest in security architecture and cannot be compromised.
D. Stateless firewalls are more effective than stateful ones, but are more expensive.

QUESTION 210
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.

Answer: A

QUESTION 211
Simply put, an IPS signature is any distinctive characteristic that identifies something. Using this definition, all IPS products use signatures of some kind, regardless of what the product

descriptions claim. In which format are IPS signatures stored?

A. Post Office
B. RDEP
C. IDCONF
D. SDEE

Answer: C

QUESTION 212
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.

Answer: D

QUESTION 213
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.

Answer: A

QUESTION 214
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

Answer: B

QUESTION 215
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

Answer: D

QUESTION 216
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

Answer: A,D

QUESTION 217
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

Answer: D

QUESTION 218
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.

Answer: B

QUESTION 219
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.

Answer: C

QUESTION 220
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.
H. A, F, D, C, G, E, B
I. A, C, F, D, G, E, B
J. A, B, C, D, E, G, F
K. F, E, G, A, B, C, D

Answer: A

QUESTION 221
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.

Answer: B

QUESTION 222
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.

Answer: A

QUESTION 223
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.

Answer: C

QUESTION 224
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.

Answer: D

QUESTION 225
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

Answer: C

QUESTION 226
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

Answer: C

QUESTION 227
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 in the HP OpenView/NR GUI interface.
B. Click the acknowledge for the alarm in question 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.

Answer: D

QUESTION 228
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.

Answer: D

QUESTION 229
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.

Answer: D

QUESTION 230
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

Answer: B

QUESTION 231
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.

Answer: B

QUESTION 232
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.

Answer: D

QUESTION 233
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

Answer: D

QUESTION 234
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.

Answer: C

QUESTION 235
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).

Answer: B

QUESTION 236
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

Answer: B

QUESTION 237
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.

Answer: C

QUESTION 238
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.

Answer: A

QUESTION 239
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

Answer: B

QUESTION 240
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.

Answer: B

QUESTION 241
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.

Answer: B

QUESTION 242
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.

Answer: C

QUESTION 243
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

Answer: A

QUESTION 244
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.

Answer: B

QUESTION 245
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.
D. Ensure that your hosts and servers all have the latest security patches.

Answer: A

QUESTION 246
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> enrollmentftp:// <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> enrollmenthttp:// <certificate authority>

Answer: D

QUESTION 247
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

Answer: D

QUESTION 248
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 telnet
access-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 0.0.0.15
access-list 100 permit ip any any
D. access-list 100 deny ip 144.23.67.94 0.0.0.7 host 144.23.67.94
access-list 100 permit ip any any

Answer: B

QUESTION 249
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.

Answer: C,D

QUESTION 250
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.

Answer: A

QUESTION 251
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.

Answer: A,C,D

QUESTION 252
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.

Answer: C

QUESTION 253
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.

Answer: B

QUESTION 254
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.

Answer: A,B,D

QUESTION 255
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.

Answer: A

QUESTION 256
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>'.

Answer: A

QUESTION 257
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.

Answer: C

QUESTION 258
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.

Answer: B

QUESTION 259
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-
B. The line command: logon authorization tacacs+
C. The global command: privilege 15 enable
D. The global command: aaa authentication enable default tacacs+

Answer: D

QUESTION 260
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 insurance medium.
B. After ther terminiation of a secure session.
C. Prior to the initiation of a secure session.
D. After a session has been fully secured.

Answer: A,B,C

QUESTION 261
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?

```
Web Server ---- +
10.1.1.89     |      <---------- Attack Traffic
          |
Web Server  -----|---- Router ----- (internet) ----- Attackers
10.1.1.90     |           G0/0
          |
Web Server ---- +
10.1.1.91


            class-map match-all DoS
       match access-group 188
!
!
Interface GigabitEthernet0/0
  description Connection to ISP Router
           ip  address 192.186.1.1 255.255.255.0
  service-policy input DoS-Attack
  ip route-cache flow
  load-interval 30
```

Testkingdom

A. policy-map DoS-Attack
class DoS
police cir 200 bc 200 be 200
conform-action transmit
exceed-action drop
violate-action drop
!
access-list 188 permit tcp any host 10.1.1.90 eq www

B. policy-map drop
class DoS
police conform-action transmit exceed-action drop

C. policy-map drop
class DoS
police cir 200000 bc 37500 be 75000
conform-action transmit
exceed-action drop
violate-action drop
!
access-list 188 permit tcp any host 10.1.1.90 eq www

D. policy-map DoS-Attack
class DoS
police cir 200000 bc 37500 be 75000
conform-action transmit
exceed-action drop
violate-action drop
!
access-list 188 permit tcp any host 10.1.1.90 eq www

Answer: D

QUESTION 262
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)

Answer: D

QUESTION 263
You are the network administrator. Two remote LANs connected via a serial connection are exchanging routing updates via RJP. 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.

Answer: B

QUESTION 264
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.

Answer: B

QUESTION 265
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.

Answer: C

QUESTION 266
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

Answer: A,C

QUESTION 267
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.

Answer: B

QUESTION 268
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.

Answer: D

QUESTION 269
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.

Answer: B,D

QUESTION 270
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.

Answer: B

QUESTION 271
In IPSec, what encapsulation protocol only encrypts the data and not the IP header?

A. ESP
B. AH
C. MD5
D. HASH

Answer: A

QUESTION 272
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.

Answer: B

QUESTION 273
Birthday attacks can protest against which of the following?

A. symmetric ciphering
B. asymmetric ciphering
C. hash algorithms
D. digital signatures

Answer: C

QUESTION 274
Which of the following is AH??s destination IP port?

A. 23
B. 21
C. 50
D. 51

Answer: D

QUESTION 275
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 gateways.

Answer: B,C,D

QUESTION 276
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>

Answer: C

QUESTION 277
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

Answer: A,B

QUESTION 278
On the basis of the partial debug output displayed in the exhibit, which value is contained inside the brackets [4] in line 1?

```
R# 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
```

Testkingdom

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

Answer: B

QUESTION 279
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

Answer: C

QUESTION 280
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.

Answer: A,B,C

QUESTION 281
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

Answer: A,C

QUESTION 282
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

Answer: D

QUESTION 283
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

Answer: B

QUESTION 284
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.

Answer: A,C,D

QUESTION 285
Which of the following protocols does TACACS+ support?

A. PPP
B. AppleTalk
C. NetBIOS
D. All the above

Answer: D

QUESTION 286
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

Answer: B

QUESTION 287
Which two statements correctly describe 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.

Answer: B,D

QUESTION 288
What versions of TACACS does Cisco IOS support? (Select the best three answers.)

A. TACACS+
B. TACACS
C. Extended TACACS
D. Extended TACACS+

Answer: A,B,C

QUESTION 289
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

Answer: B

QUESTION 290
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.

Answer: B,D

QUESTION 291
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

Answer: B

QUESTION 292
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

Answer: B

QUESTION 293
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

Answer: B,C,D

QUESTION 294
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

Answer: B

QUESTION 295
While implementing WLAN security, which three benefits can be obtained by using the TKIP instead of WEP? (Choose three.)

A. TKIP uses an advanced encryption scheme based on AES.
B. TKIP uses a 48-bit initialization vector
C. TKIP provides per-packet keying and a rekeying mechanism.
D. TKIP provides message integrity check

Answer: B,C,D

QUESTION 296
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.

Answer: D

QUESTION 297
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.

Answer: C

QUESTION 298
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.

Answer: C

QUESTION 299
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.

Answer: B,D

QUESTION 300
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?

```
regex_xcounte  "X-Counter"
regex_xsession  "X-Session"
regex_any  " "


class-map type inspect http match-anyfireside
match request header regex_xsession regex_any
match request header regex_xcounter regex_any


policy-map type inspect http xx
description Fireside
class fireside
reset log
```

Testkingdom

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 "XSession" are reset and logged

Answer: D

QUESTION 301
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 server
sdm location X.X.X.X

Answer: A

QUESTION 302
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

Answer: B

QUESTION 303
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.

Answer: B,D

QUESTION 304
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.

Answer: A,B,D

QUESTION 305
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

Answer: D

QUESTION 306
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

Answer: D

QUESTION 307
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

Answer: B,D,E,F

QUESTION 308
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

Answer: D

QUESTION 309
Which two methods will be used by the Cisco Security MARS appliance to offer attack mitigation? (Choose two.)

A. automatically resetting attacker TCP connections
B. automatically pushing commands to Layer 2 switches to shut down attacker ports
C. automatically pushing ACLs to Layer 3 devices to block attacker traffic
D. recommending ACLs to be manually pushed to Layer 3 devices such as routers and firewalls

Answer: B,D

QUESTION 310
Which three packet types will be used by TACACS+ authentication? (Choose three.)

A. ACCESS REQUEST
B. START
C. CONTINUE
D. REPLY

Answer: B,C,D

QUESTION 311
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.

Answer: B

QUESTION 312
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

Answer: C

QUESTION 313
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

Answer: B,D

QUESTION 314
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

Answer: D

QUESTION 315
When using 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

Answer: A,C

QUESTION 316
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.

Answer: C

QUESTION 317
For the following items, which two statements are correct? (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

Answer: A,C
9

QUESTION 318
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

Answer: A

QUESTION 319
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

Answer: B,D

QUESTION 320
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 nontransit area, and uses the default route to reach external networks.
D. A stub area is used to reach networks external to the sub area.

Answer: C

QUESTION 321
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

Answer: A,B,D

QUESTION 322
Which is the correct GLOP address for AS 456 according to RFC 3180?

A. 224.4.86.0
B. 239.2.213.0
C. 233.1.200.0
D. 224.0.4.86

Answer: C

QUESTION 323
Choose the statement that best describes the correct characteristics pertinent to symmetric or asymmetric keys.

A. Symmetric key cryptography uses two distinct and separate keys for encryption and decryption.
B. Symmetric key cryptography uses a single, shared key for encryption and decryption. C. Asymetric key cryptography uses the same key for both encryption and decryption.
D. Asymetric key cryptography can only be used for decryption of information.
E. Both asymmetrivc and symmetric key cryptography can only encrypt information.

Answer: B