Exam: 350-018

Title : CCIE Pre-Qualification Test for Security

Ver : 12.11.03

Section A

QUESTION .1 Which addresses below would be valid IP addresses of hosts on the Internet? (Multiple answer)
A. 235.1.1.1
B. 223.20.1.1
C. 10.100.1.1
D. 127.0.0.1
E. 24.15.1.1
Answer: B, E
Explanation: When you create an internal network, we recommend you use one of the following address groups reserved by the Network Working Group (RFC 1918) for private network addressing: Class A: 10.0.0.0 to 10.255.255.255 Class B: 172.16.0.0 to 172.31.255.255 Class C:192.168.0.0 to 192.168.255.255 class D address start with the 1110 bit so the 223.20.1.1 is a legal class C address

QUESTION .2 On an Ethernet LAN, a jam signal causes a collision to last long enough for all other nodes to recognize that:
A. A collision has occurred and all nodes should stop sending.
B. Part of a hash algorithm was computed, to determine the random amount of time the nodes should back off before retransmitting.
C. A signal was generated to help the network administrators isolate the fault domain between two Ethernet nodes.
D. A faulty transceiver is locked in the transmit state, causing it to violate CSMA/CD rules.
E. A high-rate of collisions was caused by a missing or faulty terminator on a coaxial Ethernet network.
Answer: A
Explanation: When a collision is detected the device will "transmit a jam signal" this will inform all the devices on the network that there has been a collision and hence stop them initiating the transmission of new data. This "jam signal" is a sequence of 32 bits that can have any value as long as it
does not equal the CRC value in the damaged frame's FCS field. This jam signal is normally 32 1's as this only leaves a 1 in 2^32 chance that the CRC is correct by chance. Because the CRC value is incorrect all devices listening on the network will detect that a collision has occurred and hence will
not create further collisions by transmitting immediately. "Part of a hash algorithm was computed, to determine the random amount of time the nodes should back off before retransmitting." WOULDSEEM CORRECT BUT IT IS NOT After transmitting the jam signal the two nodes involved in the
collision use an algorithm called the "truncated BEB (truncated binary exponential back off)" to determine when they will next retransmit. The algorithm works as follows: Each device will wait a multiple of 51.2us (minimum time required for signal to traverse network) before retransmitting. 51.2us
is known as a "slot". The device will wait a certain number of these time slots before attempting to retransmit. The number of time slots is chosen from the set {0,.....,2^k-1} at random where k= number of collisions. This means k is initialized to 1and hence on the first attempt k will be chosen at random from the set {0,1} then on the second attempt the set will be {0,1,2,3} and so on. K will stay at the value 10 in the 11, 12, 13, 14, 15 and 16th attempt but on the 17th attempt the MAC unit stops trying to transmit and reports an error to the layer above.

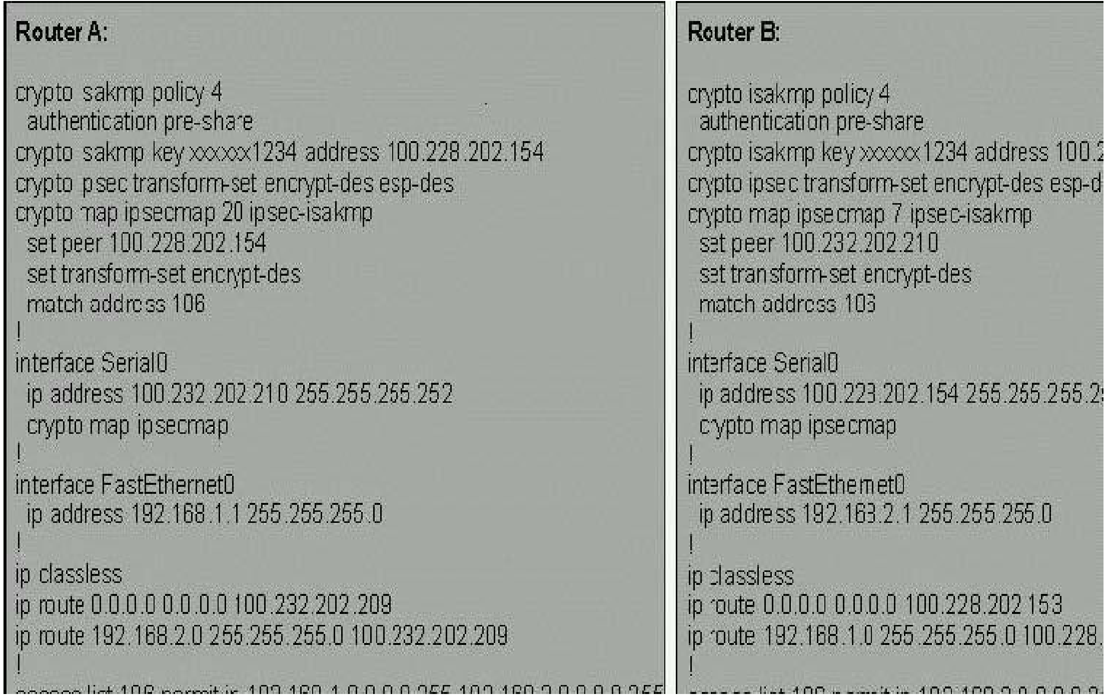
QUESTION .3 Which statements about TACACS+ are true? (Multiple answer)
A. If more than once TACACS+ server is configured and the first one does not respond within a given timeout

period, the next TACACS+ server in the list will be contacted.
B. The TACACS+ server's connection to the NAS encrypts the entire packet, if a key is used at both ends.
C. The TACACS+ server must use TCP for its connection to the NAS.
D. The TACACS+ server must use UDP for its connection to the NAS.
E. The TACACS+ server may be configured to use TCP or UDP for its connection to the NAS.
Answer: A, B, C
Explanation: PIX Firewall permits the following TCP literal names: bgp, Chargen, cmd, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, ident, IRC, klogin, kshell, lpd, nntp, pop2, pop3, pptp, rpc, smtp, sqlnet, sunrpc, TACACS, talk, telnet, time, uucp,
whois, and www. To specify a TACACS host, use the tacacs-server host global configuration command. Use the no form of this command to delete the specified name or address. timeout=(Optional) Specify a timeout value. This overrides the global timeout value set with the tacacs-server timeout command for this server only. tacacs-server key To set the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon, use the tacacs-server key global configuration command. Use the no form of this command to disable the key.
key = Key used to set authentication and encryption. This key must match the key used on the TACACS+ daemon.

QUESTION .4 A Network Administrator is trying to configure IPSec with a remote system. When a tunnel is initiated from the remote end, the security associations (SAs) come up without errors. However, encrypted traffic is never send successfully between the two endpoints. What is a possible cause?
A. NAT could be running between the twp IPSec endpoints.
B. NAT overload could be running between the two IPSec endpoints.
C. The transform set could be mismatched between the two IPSec endpoints.
D. The IPSec proxy could be mismatched between the two IPSec endpoints.
Answer: B
Explanation: This configuration will not work with port address translation (PAT). Note: NAT is a one-to-one address translation, not to be confused with PAT, which is a many (inside the firewall)-to-one translation. IPSec with PAT may not work properly because the outside tunnel endpoint device cannot handle multiple tunnels from one IP address. You will need to contact your vendor to determine if the tunnel endpoint devices will work with PAT Question- What is PAT, or NAT overloading? Answer- PAT, or NAT overloading, is a feature of Cisco IOS NAT and can be used to translate internal (inside local) private addresses to one or more outside (inside global-usually registered) IP addresses. Unique source port numbers on each translation are used to distinguish between the conversations. With NAT overload, a translation table entry containing full address and source port information is created.

QUESTION .5 Which are the principles of a one way hash function? (Multiple answer)
A. A hash function takes a variable length input and creates a fixed length output.
B. A hash function is typically used in IPSec to provide a fingerprint for a packet.
C. A hash function cannot be random and the receiver cannot decode the hash.
D. A hash function must be easily decipherable by anyone who is listening to the exchange.
Answer: A. B
Explanation: Developers use a hash function on their code to compute a diges, which is also known as a one-way hash .The hash function securely compresses code of arbitrary length into a fixed-length digest result.

QUESTION .6 Exhibit:



```
Router A:

crypto sakmp policy 4
  authentication pre-share
crypto sakmp key xxxxxx1234 address 100.228.202.154
crypto psec transform-set encrypt-des esp-des
crypto map ipsecmap 20 ipsec-isakmp
  set peer 100.228.202.154
  set transform-set encrypt-des
  match address 106
!
interface Serial0
  ip address 100.232.202.210 255.255.255.252
  crypto map ipsecmap
!
interface FastEthernet0
  ip address 192.168.1.1 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.232.202.209
ip route 192.168.2.0 255.255.255.0 100.232.202.209
!
```

```
Router B:

crypto isakmp policy 4
  authentication pre-share
crypto isakmp key xxxxxx1234 address 100.2
crypto ipsec transform-set encrypt-des esp-d
crypto map ipsecmap 7 ipsec-isakmp
  set peer 100.232.202.210
  set transform-set encrypt-des
  match address 103
!
interface Serial0
  ip address 100.223.202.154 255.255.255.2
  crypto map ipsecmap
!
interface FastEthernet0
  ip address 192.163.2.1 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.228.202.153
ip route 192.168.1.0 255.255.255.0 100.228.
!
```

What is the expected behavior of IP traffic from the clients attached to the two Ethernet subnets?

A. Traffic will successfully access the Internet, but will not flow encrypted between the router's Ethernet subnets.

B. Traffic between the Ethernet subnets on both routers will not be encrypted.

C. Traffic will be translated by NAT between the Ethernet subnets on both routers.

D. Traffic will successfully access the Internet fully encrypted.

E. Traffic bound for the Internet will not be routed because the source IP addresses are private.

Answer: A

Explanation: NOT ENOUGH OF THE EXHIBIT TO MAKE A REAL CHOICE. THE EXHIBIT ISONE OF IPSEC TAKE YOUR BEST SHOT.

QUESTION .7 A ping of death is when:

A. 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. 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. 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. The IP header is set to 1 (ICMP) and the "type" field in the ICMP header is set to 5 (Redirect).

Answer: B

Explanation: "A hacker can send an IP packet to a vulnerable machine such that the last fragment contains an offset where (IP offset *8) + (IP data length)>65535. This means that when the packet is reassembled, its total length is larger than the legal limit, causing buffer overruns in the machine's OS (because the buffer sizes are defined only to accommodate the maximum allowed size of the packet based on RFC 791)...IDS can generally recognize such attacks by looking for packet fragments that have the IP header's protocol field set to 1 (ICMP),

the last bit set, and (IP offset *8) +(IP
data length)>65535" CCIE Professional Development Network Security Principles and Practices by Saadat Malik pg 414 "Ping of Death" attacks cause systems to react in an unpredictable fashion when receiving oversized IP packets. TCP/IP allows for a maximum packet size of up to 65536 octets (1 octet= 8 bits of data), containing a minimum of 20 octets of IP header information and zero or more octets of optional information, with the rest of the packet being data. Ping of Death attacks can cause crashing, freezing, and rebooting.

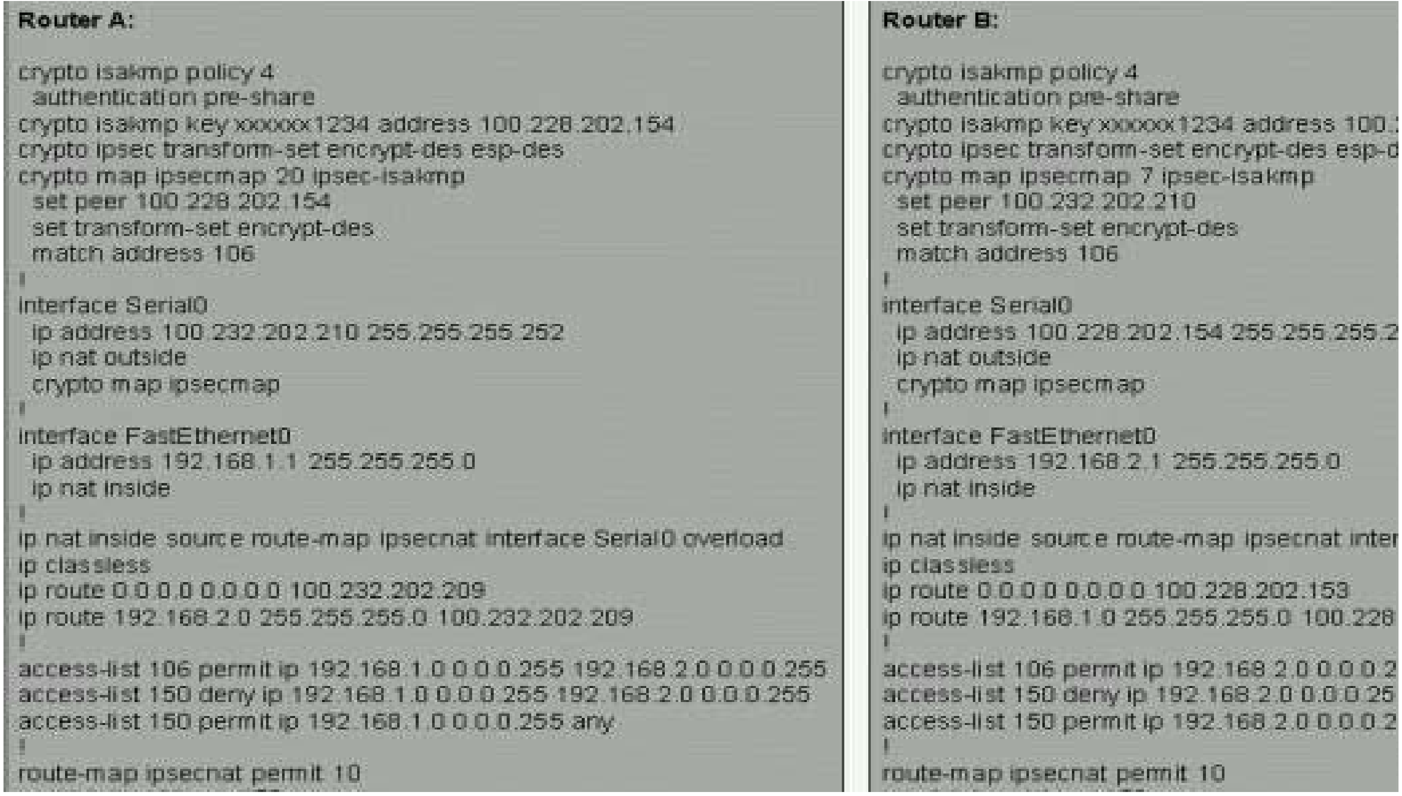
QUESTION .8 Why would a Network Administrator want to use Certificate Revocation Lists (CRLs) in their IPSec implementations?
A. They allow the ability to do "on the fly" authentication of revoked certificates.
B. They help to keep a record of valid certificates that have been issued in their network.
C. They allow them 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
Explanation: A method of certificate revocation. A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPSec peers on a regular periodic basis (for example, hourly, daily, or weekly). Each revoked certificate is identified in a
CRL by its certificate serial number. When a participating peer device uses a certificate, that system not only checks the certificate signature and validity but also acquires a most recently issued CRL and checks that the certificate serial number is not on that CRL.

QUESTION .9 A SYN flood attack is when:
A. A target machine is flooded with TCP connection requests with randomized source address &ports for the TCP ports.
B. A target machine is sent a TCP SYN packet (a connection initiation), giving the target host's address as both source and destination, and is using the same port on the target host as both source and destination.
C. A TCP packet is received with the FIN bit set but with no ACK bit set in the flags field.
D. A TCP packet is received with both the SYN and the FIN bits set in the flags field.
Answer: A
Explanation: to a server that requires an exchange of a sequence of messages. The client system begins by sending a SYN message to the server. The server then acknowledges the SYN message by sending a SYNACK message to the client. The client then finishes establishing the connection by responding with an ACK message and then data can be exchanged. At the point where the server system has sent an acknowledgment (SYN-ACK) back to client but has not yet received the ACK message, there is a half-open connection. A data structure describing all pending connections is in
memory of the server that can be made to overflow by intentionally creating too many partially open connections. Another common attack is the SYN flood, in which a target machine is flooded with TCP connection requests. The source addresses and source TCP ports of the connection request packets are randomized; the purpose is to force the target host to maintain state information for many connections that will never be completed. SYN flood attacks are usually noticed because the target host (frequently an HTTP or SMTP server) becomes extremely slow, crashes, or hangs. It's also possible for the traffic returned from the target host to cause trouble on routers; because this return traffic goes to the randomized source addresses of the original packets, it lacks the locality properties of "real" IP traffic, and may overflow route caches. On Cisco routers, this problem often manifests itself in the router running out of memory

QUESTION .10 What kind of interface is not available on the Cisco Secure Intrusion Detection System sensor?
A. Ethernet
B. Serial
C. Token Ring
D. FDDI
Answer: B
Explanation: Sensors are optimized for specific data rates and are packaged in Ethernet, Fast Ethernet (100BaseT), Token Ring, and FDDI configurations

---

QUESTION .11 Exhibit:



```
Router A:

crypto isakmp policy 4
 authentication pre-share
crypto isakmp key xxxxxx1234 address 100.228.202.154
crypto ipsec transform-set encrypt-des esp-des
crypto map ipsecmap 20 ipsec-isakmp
 set peer 100.228.202.154
 set transform-set encrypt-des
 match address 106
!
interface Serial0
 ip address 100.232.202.210 255.255.255.252
 ip nat outside
 crypto map ipsecmap
!
interface FastEthernet0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
!
ip nat inside source route-map ipsecnat interface Serial0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 100.232.202.209
ip route 192.168.2.0 255.255.255.0 100.232.202.209
!
access-list 106 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 150 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 150 permit ip 192.168.1.0 0.0.0.255 any
!
route-map ipsecnat permit 10
```

```
Router B:

crypto isakmp policy 4
 authentication pre-share
crypto isakmp key xxxxxx1234 address 100.
crypto ipsec transform-set encrypt-des esp-d
crypto map ipsecmap 7 ipsec-isakmp
 set peer 100.232.202.210
 set transform-set encrypt-des
 match address 106
!
interface Serial0
 ip address 100.228.202.154 255.255.255.2
 ip nat outside
 crypto map ipsecmap
!
interface FastEthernet0
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
!
ip nat inside source route-map ipsecnat inter
ip classless
ip route 0.0.0.0 0.0.0.0 100.228.202.153
ip route 192.168.1.0 255.255.255.0 100.228
!
access-list 106 permit ip 192.168.2.0 0.0.0.2
access-list 150 deny ip 192.168.2.0 0.0.0.25
access-list 150 permit ip 192.168.2.0 0.0.0.2
!
route-map ipsecnat permit 10
```

Given the configuration shown, what is the expected behavior of IP traffic traveling from the attached clients to the two Ethernet subnets? (Multiple answer)
A. Traffic bound for the Internet will be translated by NAT and will not be encrypted.
B. Traffic between the Ethernet subnets on both routers will be encrypted.
C. Traffic bound for the Internet will not be routed because the source IP addresses are private.
D. Traffic will not successfully access the Internet or the subnets of the remote router's Ethernet interface.
E. Traffic will be translated by NAT between the Ethernet subnets on both routers.
Answer: B Explanation:

QUESTION .12 How is data between a router and a TACACS+ server encrypted?
A. CHAP Challenge responses
B. DES encryption, if defined
C. MD5 has using secret matching keys
D. PGP with public keys

Answer: C
Explanation: "The hash used in TACACS+ is MD5"CCIE Professional Development Network Security Principles and Practices by Saadat Malik pg 497

QUESTION .13 A gratuitous ARP is used to: (Multiple answer)
A. Refresh other devices' ARP caches after reboot.
B. Look for duplicate IP addresses.
C. Refresh the originating server's cache every 20 minutes.
D. Identify stations without MAC addresses.
E. Prevent proxy ARP from becoming promiscuous.
Answer: A, B
Explanation: NOT SURE ABOUT THIS QUESTION- Refresh the originating server's cache every 20 minutes. could be answer but the test wants only 2Gratuitous ARP [23] is an ARP packet sent by a node in order to spontaneously cause other nodes to update an entry in their ARP cache. A gratuitous ARP MAY use either an ARP Request or an ARP reply packet. In either case, the ARP Sender Protocol Address and ARP Target Protocol Address are both set to the IP address of the cache entry to be updated, and the ARP Sender Hardware Address is set to the link-layer address to which this cache entry should be updated. When using an ARP Reply packet, the Target Hardware Address is also set to the link-layer address to which this cache entry should be updated (this field is not used in an ARP Request packet).Most hosts on a network will send out a Gratuitous ARP when they are initializing their IP stack. This Gratuitous ARP is an ARP request for their own IP address and is used to check for a duplicate IP address. If there is a duplicate address then the stack does not complete initialization.

QUESTION .14 Within OSPF, what functionality best defines the use of a 'stub' area?
A. It appears only on remote areas to provide connectivity to the OSPF backbone.
B. It is used to inject the default route for OSPF.
C. It uses the no-summary keyword to explicitly block external routes, defines the non-transit area, and uses the default route to reach external networks.
D. To reach networks external to the sub area.
Answer: B
Explanation: These areas do not accept routes belonging to external autonomous systems(AS); however, these areas have inter-area and intra-area routes. In order to reach the outside networks, the routers in the stub area use a default route which is injected into the area by the Area Border Router(ABR). A stub area is typically configured in situations where the branch office need not know about all the routes to every other office, instead it could use a default route to the central office and get to other places from there. Hence the memory requirements of the leaf node routers is reduced, and so is the size of the OSPF database.

QUESTION .15 What is the best explanation for the command aaa authentication PPP default if-neededtacacs+?
A. If authentication has been enabled on an interface, use TACACS+ to perform authentication.
B. If the user requests authentication, use TACACS+ to perform authentication.
C. If the user has already been authenticated by some other method, do not run PPP authentication.
D. If the user is not configured to run PPP authentication, do not run PPP authentication.
E. If the user knows the enable password, do not run PPP authentication.
Answer: C
Explanation: if-needed (Optional) Used with TACACS and extended TACACS. Does not perform CHAP or

PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces.

QUESTION .16 To restrict SNMP access to a router, what configuration command could be used?
A. snmp-server community
B. snmp-server public
C. snmp-server password
D. snmp-server host
Answer: A
Explanation: Configure the community string (Optional) For access-list-number, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999.

QUESTION .17 TFTP security is controlled by: (Multiple answer)
A. A username/password.
B. A default TFTP directory.
C. A TFTP file.
D. A pre-existing file on the server before it will accept a put.
E. File privileges.
Answer: B, D, E
Explanation: username/password- is for FTP a default TFTP directory - one has to be in your tftp server and the location listed in the tftp command In uploading code you need to have a file but some programs like solar winds will download the running config via tftp and make the file

---

QUESTION .18 Which statements are true about RIP v1? (Multiple answer)
A. RIP v1 is a classful routing protocol.
B. RIP v1 does not carry subnet information in its routing updates.
C. RIP v1 does not support Variable Length Subnet Masks (VLSM).
D. RIP v1 can support discontiguous networks.
Answer: A, B, C
Explanation: RIP and IGRP are classful protocols Why Doesn't RIP or IGRP Support Discontiguous Networks?

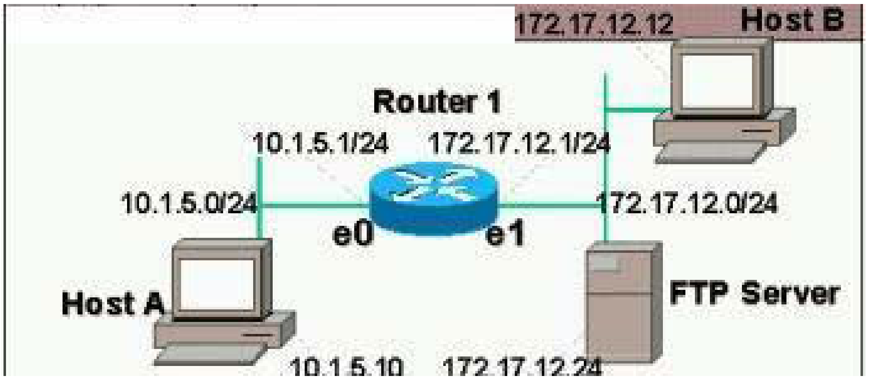
QUESTION .19 In the IOS Firewall Feature Set, what kind of traffic is NOT subject to inspection?
A. FTP
B. TFTP
C. ICMPD
D. SMTP
Answer: C
Explanation: CBAC-Supported applications (Deployable on a modular basis):

QUESTION .20 Exhibit:
S* 0.0.0.0/0 [1/0] via 172.31.116.65D 172.16.0.0/24 [90/48609] via 10.1.1.1R 172.16.0.0/16 [120/4] via192.168.1.4
A router has the above routers listed in its routing table and receives a packet destined for 172.16.0.45.What will happen?
A. The router will not forward this packet, since it is destined for the 0 subnet.

B. The router will forward the packet though 172.31.116.65, since it has the lowest metric.
C. The router will forward the packet through 10.1.1.1.
D. The router will forward the packet through 172.31.116.65, since it has the lowest administrative distance.
E. The router will forward the packet through 192.168.1.4.
Answer: C
Explanation: D= EIGRP and the lowest metric of the routing protocols R= Rip AD of 120 S*default route The 0.0.0.0 is a default route for packets that don't match the other routes is to be forwarded to 172.31.116.65

QUESTION .21 In the Cisco Secure Intrusion Detection System/HP Open View interface, a "yellow" sensor icon would mean:
A. A sensor daemon had logged a level 3 alarm.
B. A sensor daemon had logged a level 4 or 5 alarm.
C. The director that the sensor reports to is operating in degraded mode.
D. The device that the sensor detected being attacked is inoperative as a result of the attack.
Answer: A
Explanation: Alarm level 3 and 4 are medium. Medium severity is displayed in yellow, then icon medium severity is a yellow flag. by default events at level 1 and 2 are low, events at level 3 and 4 are medium, level 5 and higher are high. Cisco Secure intrusion detection system by Earl Carter p. 148,
213, 214

QUESTION .22 Symptoms: -Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)-Console logging: level warning, 0 messages logged-Monitor logging: level informational, 0 messages logged-Buffer logging: level informational, 0 message lines logged
Note: Router 1's CPU is normally above 25% busy switching packets Scenario: Host A cannot reach the FTP Server, but can reach Host B. The network administrator suspects that packets are traveling from network 10.1.5.0 to the FTP Server, but packets are not returning. The administrator logs into the console port of Router 1. When Host A sends a ping to the FTP Server, the administrator executes a "debug ip packet" command on the router. Exhibit:



The administrator does not see any output. What additional commands could be used to see the packets flowing from Ethernet 0 to Ethernet 1?
A. terminal monitor
B. configure terminal
logging console debug
interface ethernet1
no ip route-cache
C. configure terminal

logging console debug
D. configure terminal
no logging buffered
E. configure terminal
interface ethernet0
no ip route-cache
Answer: B
Explanation: By default, the network server sends the output from debug commands and system error messages to the console. If you use this default, monitor debug output using a virtual terminal connection, rather than the console port. To redirect debug output, use the logging command options within configuration mode as described 7 debugging messages. LOG_DEBUG. When multicast fast switching is enabled (like unicast routing), debug messages are not logged. If you want to log debug messages, disable fast switching. To limit the types of messages that are logged to
the console, use the logging console router configuration command. Use the ip route-cache interface configuration command to control the use of high-speed switching caches for IP routing. To disable any of these switching modes, use the no form of this command.

QUESTION .23 What is the first thing that must be done to implement network security at a specific site?
A. Hire a qualified consultant to install a firewall and configure your router to limit access to known traffic.
B. Run software to identify flaws in your network perimeter.
C. Purchase and install a firewall to protect your network.
D. Install access-control lists in your perimeter routers, so you can ensure that only known traffic is getting through your router.
E. Design a security policy.
Answer: E
Explanation: A Network security policy defines a framework to protect the assets connected to a network based on a risk assessment analysis. A network security policy defines the access limitations and rules for accessing various assets connected to a network. It is the source of information
for users and administrators as they set up, use, and audit the network. CCIE Professional Development Network Security Principles and Practices by Saadat Malik pg 8

QUESTION .24 What would be the best reason for selecting L2TP as a tunnel protocol for a VPN Client?
A. L2TP uses TCP as a lower level protocol so the transmissions are connected oriented, resulting in more reliable delivery.
B. L2TP uses PPP so address allocation and authentication is built into the protocol instead of relying on IPSec extended functions, like mode config and a-auth.
C. L2TP does not allow the use of wildcard pre-shared keys, which is not as secure as some other methods.
D. L2TP has less overhead than GRE.
Answer: B
Explanation: L2TP uses UDP which is connectionless protocol CCIE Professional Development Network Security Principles and Practices by Saadat Malik pg 243 L2TP, which stands for Layer 2 Tunneling Protocol, is an IETF standard emerging that combines Layer 2 Forwarding protocol(L2F) and Point-to-Point Tunneling protocol (PPTP). L2TP has all the security benefits of PPP, including multiple per user authentication options (CHAP, PAP, and MS-CHAP). It also can authenticate the tunnel end points, which prevents potential intruders from building a tunnel and accessing precious corporate data. To ensure further data confidentiality, Cisco recommends adding IPSec to any L2TP implementation. Depending on the corporation's specific network

security requirements, L2TP can be used in conjunction with tunnel encryption, end-to-end data encryption, or2661) 24 (bit) for the GRE overhead

---

QUESTION .25 In the IOS Firewall Feature Set, which network layers are examined by CBAC to make filtering decisions? (Multiple answer)
A. Transport
B. Application
C. Network
D. Presentation
E. Data Link
Answer: A, B, C
Explanation: CBAC intelligently filters TCP and UDP packets based on application layer protocol session information and can be used for intranets, extranets and the Internet. You can configure CBAC to permit specified TCP and UDP traffic through a firewall only when the connection is initiated from within the network you want to protect. (In other words, CBAC can inspect traffic for sessions that originate from the external network.) However, CBAC examines not only network layer and transport layer information but also examines the application-layer protocol information (such as FTP connection information) to learn about the state of the TCP or UDP session.

QUESTION .26 In BGP, why should a Route Reflector be used?
A. To overcome issues of split-horizon within BGP.
B. To reduce the number of External BGP peers by allowing updates to reflect without the need to be fully meshed.
C. To allow the router to reflect updates from one Internal BGP speaker to another without the need to be fully meshed.
D. To divide Autonomous Systems into mini-Autonomous Systems, allowing the reduction in the number of peers.
E. None of the above.
Answer: C
Explanation: "Route reflectors are useful when an AS contains a large number of IBGP peers. Unless EBGP routes are redistributed into the autonomous systems' IGP, all IBGP peers must be fully meshed. Route reflectors offer an alternative to fully meshed IBGP peers." CCIE Professional
Development Routing TCP/IP Volume II by Jeff Doyle and Jennifer Dehaven Carroll

---

QUESTION .27 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. What is the expected action of the host?
A. The host should reduce the size of future packets it may send to the router.
B. This scenario cannot occur, since the packet will be fragmented and sent to the original destination.
C. The sending station will stop sending packets, because the router is not expecting to see the DF bit in the incoming packet.
D. The sending station will clear the DF bit and resend the packet.
E. If the router has an Ethernet interface, this cannot occur because the MTU is fixed at 1500 bytes. Any other interface may legally generate this packet.
Answer: D
Explanation: Another ICMP message warns that a desired host is unreachable because of a problem with

fragmenting a datagram sending.host.net:icmp:tagret.host unreachable - need to frag (mtu1500) Network Intrusion Detection third edition by Stephen Northcutt and Judy Novak pg 67

QUESTION .28 In the realm of email security, "message repudiation" refers to what concept?
A. A user can validate which mail server or servers a message was passed through.
B. A user can claim damages for a mail message that damaged their reputation.
C. A recipient can be sure that a message was sent from a particular person.
D. A recipient can be sure that a message was sent from a certain host.
E. A sender can claim they did not actually send a particular message.
Answer: E
Explanation: A quality that prevents a third party from being able to prove that a communication between two other parties ever took place. This is a desirable quality if you do not want your communications to be traceable. Non-repudiation is the opposite quality-a third party can prove that a communication between two other parties took place. Non-repudiation is desirable if you want to be able to trace your communications and prove that they occurred. Repudiation - Denial of message submission or delivery.

QUESTION .29 A RARP is sent:
A. To map a hostname to an IP address.
B. To map an IP address to a hostname.
C. To map an MAC address to an IP address.
D. To map a MAC address to a hostname.
E. To map and IP address to a MAC address.
Answer: C
Explanation: RARP is used to translate hardware interface addresses to protocol addresses

---

QUESTION .30 Exhibit:
aaa authentication login default local tacacsaaa authorization exec default tacacs aaa authentication login vty tacacs local aaa authorization exec vty tacacs if-authenticated username abc password xuzline vty 04exec-timeout 0 0
If a router running IOS 11.3 is configured as shown in the TACACS server is down, what will happen when someone Telnets into the router?
A. Using the local username, the user will pass authentication but fail authorization.
B. The user will be bale to gain access using the local username and password, since list vty will be checked.
C. Using the local username, the user will bypass authentication and authorization since the server is down.
D. The user will receive a message saying "The TACACS+ server is down, please try again later".
Answer: B
Explanation: aaa authentication login vty tacacs local aaa authorization exec vty tacacs if authenticated. This lines in the config mean that the vty lines are to use tacacs first but the timeout expires and authentication then goes to the local database If-authenticated states that if authenticated before do not authenticate again.

QUESTION .31 When an IPSec authentication header (AH) is used in conjunction with NAT on the same IPSec endpoint, what is the expected result?
A. NAT has no impact on the authentication header.
B. IPSec communicates will fail because the AH creates a hash on the entire IP packet before NAT.
C. AH is only used in IKE negotiation, so only IKE will fail.
D. AH is no a factor when used in conjunction with NAT, unless Triple DES is included in the transform set.

Answer: B
Explanation: AH runs the entire IP packet, including invariant header fields such as source and destination IP address, through a message digest algorithm to produce a keyed hash. This hash is used by the recipient to authenticate the packet. If any field in the original IP packet is modified, authentication will fail and the recipient will discard the packet. AH is intended to prevent unauthorized modification, source spoofing, and man-in-the-middle attacks. But NAT, by definition, modifies IP packets. Therefore, AH + NAT simply cannot work.

QUESTION .32 Routing Information Protocol (RIP):
A. Runs on TCP port 520.
B. Runs directly on top of IP with the protocol ID 89.
C. Runs on UDP port 520.
D. Does not run on top of IP.
Answer: C
Explanation:

QUESTION .33 A security System Administrator is reviewing the network system log files. The administrator notes that: -Network log files are at 5 MB at 12:00 noon. -At 14:00 hours, the log files at 3 MB. What should the System Administrator assume has happened and what should they do?
A. Immediately contact the attacker's ISP and have the connection disconnected, because an attack has taken place.
B. Log the file size, and archive the information, because the router crashed.
C. Run a file system check, because the Syslog server has a self correcting file system problem.
D. Disconnect from the Internet discontinue any further unauthorized use, because an attack has taken place.
E. Log the event as suspicious activity, continue to investigate, and take further steps according to site security policy.
Answer: E
Explanation: This question os much like one from vconsole (see reference)"You should never assume a host has been compromised without verification. Typically, disconnecting a server is an extreme measure and should only be done when it is confirmed there is a compromise or the server contains such sensitive data that the loss of service outweighs the risk. Never assume that any administrator or automatic process is making changes to a system. Always investigate the root cause of the change on the system and follow your organizations security policy." Cisco Certified Internet work Expert Security Exam V1.7/Vconsole update questions by John Kaberna See ccbootcamp.com

---

QUESTION .34 When using PKI, what is true about Certificate Revocation List (CRL):
A. The CRL is used to check presented certificates to determine if they are revoked.
B. 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.
C. The router's CRL includes a list of clients that have presented invalid certificates to the router in the past.
D. It resides on the CA server and is built by querying the router or PIX to determine which clients have presented invalid certificates in the past.
Answer: A
Explanation: 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 --THIS SEEMS A RESONABLE ANSWER BUT HERE IS WHYI DISCOUNT IT--"will not require that the other end of the IPSec tunnel have a certificate" -- The PIX allows the Certificate

even if the CA DOES NOT RESPOND. I have not seen it stated that it will allow NO certificate. To allow other peers' certificates to still be accepted by your router even if the appropriate Certificate Revocation List (CRL) is not accessible to your router, use the crl optional configuration command. If the PIX Firewall does not receive a certificate from the CA within 1 minute(default) of sending a certificate request, it will resend the certificate request. The PIX Firewall will continue sending a certificate request every 1 minute until a certificate is received or until 20 requests have been sent. With the keyword crl optional included within the command statement, other peer’s certificates can still be accepted by your PIX Firewall even if the CRL is not accessible to your PIX Firewall.

QUESTION .35 A remote user tries to login to a secure network using Telnet, but accidentally types in an invalid username or password. Which response would NOT be preferred by an experienced Security Manager?(Multiple answer)
A. Invalid Username
B. Invalid Password
C. Authentication Failure
D. Logon Attempt Failed
E. Access Denied
Answer: A, B
Explanation: I think there are only two answers for this question. "Authentication failure” and "Logon attempt failed" does reveal some information, in that authentication and logon - both messages about login have failed. The BEST is Access Denied and Invalid user and password are CLEARLY WRONG.

QUESTION .36 Some packet filtering implementations block Java by finding the magic number 0xCAFEBABE at the beginning of documents returned via HTTP. How can this Java filter be circumvented?
A. By using Java applets in zipped or tarred archives.
B. By using FTP to download using a web browser.
C. By using Gopher.
D. By using non-standard ports to enable HTTP downloads.
E. All of the above.
Answer: E
Explanation: NOT SURE ABOUT THIS ANSWER BUT THE NON-STANDARD PORTAND ZIPPED/TARRED ANSWERS ARE CORRECT. Java blocking can be configured to filter or completely deny access to Java applets that are not embedded in an archive or compressed file. Java applets may be downloaded when you permit access to port 80 (http) (so the non-standard port answer seems logical) Cisco secure PIX firewall Advanced 2.0 9-16 Applets that are transmitted as embedded archives are not recognized and therefore cannot be blocked. CCIE Professional Development Network Security Principles and Practices by Saadat Malik pg 203 also see Cisco Certified Internet work Expert
Security Exam v1.7 by John Kaberna pg 404

QUESTION .37 An attack that falsifies a broadcast ICMP echo request and includes a primary and secondary victim is known as a:
A. Fraggle Attack
B. Smurf Attack
C. Man in the Middle Attack
D. Trojan Horse Attack
E. Back Orifice Attack

Answer: B

Explanation: Trojan and Back orifice are Trojan horse attacks. Man in the middle spoofs the Ip and redirects the victims packets to the cracker The infamous Smurf attack. preys on ICMP's capability to send traffic to the broadcast address. Many hosts can listen and respond to a single ICMP
echo request sent to a broadcast address. Network Intrusion Detection third Edition by Stephen North cutt and Judy Novak pg 70 The "smurf" attack's cousin is called "fraggle", which uses UDP echo packets in the same fashion as the ICMP echo packets; it was a simple re-write of "smurf".

QUESTION .38 User_A and User_B are logged into Windows NT Workstation Host_A and Host_B respectively.

All users are logged in to the domain " CORP ".

All users run a logon script with the following line: "net useD:\\CORPSVR\data"

-User_A and User_B are both members of the local group "USERS".

-Local group "USERS" is includes in global group "DOMAIN USERS".

-All users, hosts, and groups are in the domain "CORP".

-The directory \\CORPSVR\data has the share permission for local group "USERS" set to "No Access".

-The Microsoft Word document \\CORPSVR\data\word.doc has file permissions for local group "USERS" set to "Full Control".

-The Microsoft Word document \\CORPSVR\data\word.doc is owned by User_B. Given this scenario on a Windows NT 4.0 network, what is the expected behavior when User_A attempts to edit D:\word.doc?

A. Local groups cannot be placed into global groups. The situation could not exist.

B. There is not enough information. Permissions on Microsoft Word are set within the application and are not subject to file and share level permissions.

C. Access would be denied. Only the owner of a file can edit a document.

D. Access would be denied. "No access" overrides all other permissions unless the file is owned by the user.

E. User_A has full control and can edit the document successfully.

Answer: A

Explanation: Based on the name of each group, you might think that you'd add local groups to global groups. This isn't the case. You assign users or global groups to local groups to give access to local resources

---

QUESTION .39 Identify the invalid Cisco Secure Intrusion Detection System function:

A. It sets off an alarm when certain user-configurable strings are matched.

B. It sends e-mail messages at particular alarm levels via eventd.

C. It sends a TCP reset to the intruder when operating in packet sniffing mode.

D. It performs a traceroute to the intruding system.

Answer: D

Explanation: Traceroute is not done.

QUESTION .40 Kerberos is mainly used in:

A. Session-layer protocols, for data integrity and checksum verification.

B. Presentation-layer protocols, as the implicit authentication system for data stream or RPC.

C. Transport and Network-layer protocols, for host to host security in IP, UDP, or TCP.

D. Data link-layer protocols, for cryptography between bridges and routers.

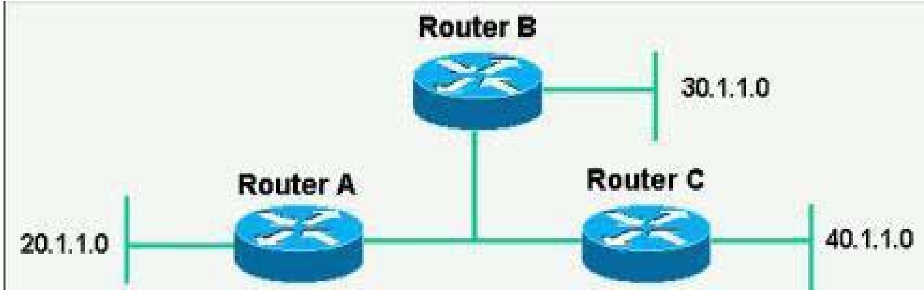
E. Application-layer protocols, like Telnet and FTP.

Answer: E

Explanation: Type Application layer protocol. Ports: 88 (UDP) 464 (TCP, UDP) change/setpassword.

QUESTION .41 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.
E. NFS does not have the concept of users and permissions, so it is not secure.
Answer: C
Explanation: NOT SURE ABOUT THIS ONE Another use of RPC is with the following command to see the exports of 204.31.17.25 if you want to allow NFS mounting from outside in.
Note: RPC is a very nonsecure protocol and should be used with caution. Type Application layer file transfer protocol. Port 2049 (TCP, UDP).

QUESTION .42 Exhibit:

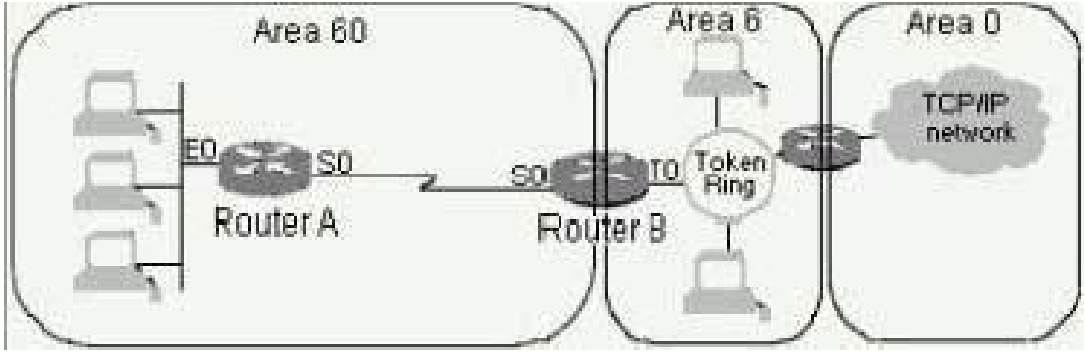


In order to allow IPSec to handle multiple peers from Router A, which crypto map and access list commands should be used?
A. crypto map foo 10 ipsec-isakmpset peer B match address 101 set trans bar crypto map foo 20 ipsecisakmpset peer C match address 102 set trans bar access-list 101 permit ip 20.1.1.0 0.0.255 30.1.1.0 0.0.0.255access-list 102 permit ip 20.1.1.0 0.0.255 401.1.0 0.0.0.255
B. crypto map foo 10 ipsec-isakmpset peer B set peer C match address 101 set trans bar access-list 101permit ip 20.1.1.0 0.0.0.255 30.1.1.0 0.0.0.255access-list 101 permit ip 20.1.1.0 0.0.0.255 40.1.1.0 0.0.0.255
C. crypto map foo 10 ipsec-isakmpset peer B match address 101 set trans bar crypto map foo 20 ipsectisakmpset per C match address 101 set trans bar access-list 101 permit ip 20.1.1.0 0.0.0.255 30.1.1.0 0.0.0.255access-list 101 permit ip 20.1.1.0 0.0.0.255 40.1.1.0 0.0.0.255
D. crypto map foo 10 ipsec-isakmpset peer B match address 101 set trans bar crypto trans bar crypto mapfoo 20 ipsec-isakmpset peer C match address 102 set trans bar access-list 101 permit ip 20.1.1.0 0.0.0.255 any access-list 102 permit ip 20.1.1.0 0.0.0.255 any
E. crypto map foo 10 ipsec-isakmpset peer B match address 101 set trans bar crypto map foo 10 ipsecisakmpset peer C match address 102 set trans bar
access-list 101 permit ip 20.1.1.0 0.0.0.255 any
access-list 102 permit ip 20.1.1.0 0.0.0.255 any
Answer: A

QUESTION .43 The Unix file /etc/shadow is:
A. A place to store encrypted passwords without referencing the /etc/passwd file.

B. Referenced by login when the /etc/passwd file contains an asterisk in the third field.
C. Referenced by NIS when the /etc/passwd file contains a line with the first character of '+'.
D. A read-protected file referenced by login when the /etc/passwd file contains a special character in the second field.
Answer: A
Explanation: One of these is the shadow password scheme, which is used by default. The encrypted password is not kept in /etc/passwd, but rather in /etc/shadow. /etc/passwd has a placeholder, x, in this field. passwd is readable by everyone, whereas shadow is readable only by root. The shadow
file also contains password aging controls. * or !! in the password field of /etc/shadow indicates that the account is disabled.

QUESTION .44 Exhibit:



In a reorganization, OSPF areas are realigned. In order to make this a valid network design, which changes could be made to the network and/or router configurations? (Multiple answer)
A. A virtual link could be configured between Area 60 and Area 0.
B. A serial line or other physical connection could be installed between devices in Area 60 and Area 0.
C. Router B could be configured as an Area Border Router between Area 60 and area 6.
D. This is not a valid design, and no changes can make it work.
Answer: A. B

QUESTION .45 Two remote LANs connected via a serial connection are exchanging routing updates via RIP. An alternate path exists with a higher hop count. When the serial link fails, users complain of the time it takes to transfer to the alternate path. What can be done to improve this?
A. Change the hop count on an alternate path to be the same cost.
B. Increase the bandwidth of the alternate serial connection.
C. Configure a static route via the alternate route with an appropriate administrative cost.
D. Reduce or disable the hold own timer using the timers basic command.
Answer: D

QUESTION .46 Network Address Translation (NAT) may not work well:
A. With outbound HTTP when AAA authentication is involved.
B. When PAT (Port Address Translation) is used on the same firewall.
C. When used in conjunction with static IP addresses assignment to some devices.
D. With traffic that carries source and/or destination IP addresses in the application data stream.
E. With ESP Tunnel mode IPSec traffic.
Answer: D
Explanation: AH does not work with NAT

QUESTION .47 Inside addresses = 131.108.0.0 Outside global addresses = 198.108.10.0Serial 0 is connected to the outside world Given the information above, what Network Address Translation (NAT) configuration is correct?

A. ip nat pool CCIE-198 198.108.10.0 198.108.10.255 prefix-length 24.ip nat inside source list 1 pool

```
interface serial 0
ip address 131.108.1.1 255.255.255.0
ip nat outside
interface Ethernet0
ip address 198.108.10.1 255.255.255.0
ip nat inside
access-list 1 permit 131.108.0.0 0.0.255.255
```

B. ip nat pool CCIE-198 198.108.10.0 198.108.10.255 prefix-length 24ip nat inside source list 1 pool

```
interface serial 0
ip address 198.108.10.1 255.255.255.0
ip nat outside
interface Ethernet0
ip address 131.108.1.1 255.255.255.0
ip nat inside
access-list 1 permit 131.108.0 0.0.255.255
```

C. ip nat pool CCIE-198 198.108.10.0 198.108.10.255 prefix-length 24.ip nat inside source list 1 pool

```
interface serial 0
ip address 198.108.10.1 255.255.255.0
ip nat outside
interface Ethernet0
ip address 131.108.1.1 255.255.255.0
ip nat inside
access-list 1 permit 198.108.10.0 0.0.0.255
```

D. ip nat pool CCIE-131 131.108.1.0 131.108.1.255 prefix-length 24.ip nat inside source list 1 pool

```
interface serial 0
ip address 198.108.10.1 255.255.255.0
ip nat inside
interface Ethernet0
ip address 131.108.1.1 255.255.255.0
ip nat outside
access-list 1 permit 198.108.10.0 0.0.0.255
```

Answer: B

Explanation: ip nat inside source list 1 pool CCIE-198 calls access list 1 to state which ip address are to be nated

QUESTION .48 PFS (Perfect Forward Security) requires:

A. Another Diffie-Hellman exchange when an SA has expired
B. Triple DES
C. AH
D. ESP
E. A discrete client

Answer: A
Explanation: crypto map my map 10 set pfs group2 This example specifies that PFS should be used whenever a new security association is negotiated for the crypto map "my map 10." The 1024-bitDiffie-Hellman prime modulus group will be used when a new security association is negotiated using the Diffie-Hellman exchange.

QUESTION .49 What service SHOULD be enabled on ISO firewall devices?
A. SNMP with community string public.
B. TCP small services.
C. UDP small services.
D. Password-encryption.
E. CDP
Answer: D
Explanation: To encrypt passwords, use the SERVICE password-encryption global configuration command The answer of TCP small-services and UDP are TCP and UDP small-servers

---

QUESTION .50 SNMP v1 community strings:
A. Are encrypted across the wire.
B. Can be used to gain unauthorized access into a device if the read-write string is known.
C. Are always the same for reading & writing data.
D. Are used to define the community of devices in a single VLAN.
Answer: B
Explanation: SNMP is also capable changing the configurations on the host, allowing the remote management of the network device.

QUESTION .51 Under normal circumstances, after a single IPSec tunnel has been established, how many IPSec security associations should be active on the system?
A. One per protocol (ESP and AH)
B. Two per protocol (ESP and AH)
C. Three per protocol (ESP and AH)
D. Four per protocol (ESP and AH)
E. Five total (either ESP or AH)
Answer: B
Explanation: Once established, the set of security associations (outbound, to the remote peer)is then applied to the triggering packet as well as to subsequent applicable packets as those packets exit the PIX Firewall. "Applicable" packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound security associations are used when processing the incoming traffic from that peer. If IKE is used to establish the security associations, the security associations will have lifetimes so that they will periodically expire and require renegotiation. (This provides an additional level of security.) Multiple IPSec tunnels can exist between two peers to secure different data streams, with each tunnel using a separate set of security associations. For example, some data streams might be just authenticated while other data streams must be both encrypted and authenticated. You can change the global lifetime values that are used when negotiating new IPSec security associations. (These global lifetime values can be overridden for a particular crypto map entry.)These lifetimes only apply to security associations established via IKE. Manually established security associations do not expire. There are two lifetimes: a "timed" lifetime and a "traffic-

volume" lifetime. A security association expires after the respective lifetime is reached and negotiations will be initiated for a new one.

QUESTION .52 What is NOT an example of a supported ISAKMP keying mechanism?
A. Pre-shared
B. RSA
C. Certificate authority
D. Perfect Forward Secrecy
Answer: D
Explanation: The three main mechanisms of devices authentication are - Preshared keys, Digital signatures, encrypted nonces CCIE Professional Development Networks Security Principles and Practices by Saadat Malik pg 306 The two entities must agree on a common authentication protocol
through a negotiation process using either RSA signatures, RSA encrypted nonces, or pre-shared keys. To specify that IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for this crypto map entry, or that IPSec requires PFS when receiving requests for new security associations

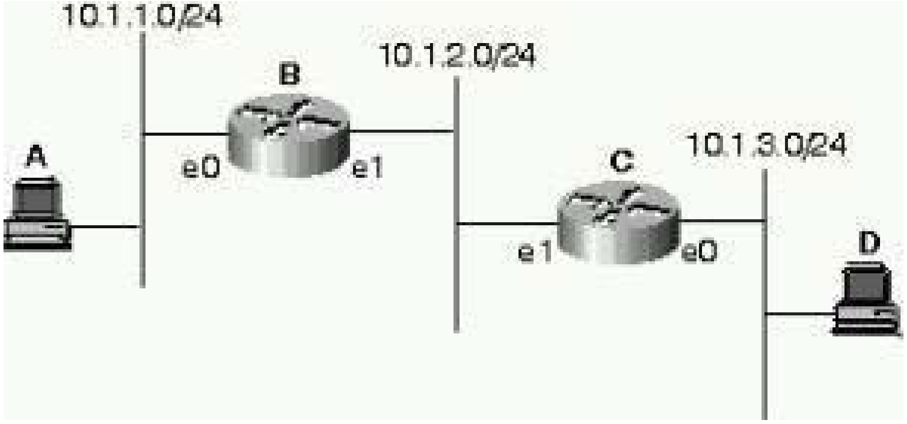
---

QUESTION .53 Exhibit:
10.1.1.0/24 through OSPF10.1.0.0/16 through EIGRP10.1.0.0&16 static
If a router had the three routers listed, which one of the routers would forward a packet destined for10.1.1.1?
A. 10.1.0.0/16 though EIGRP, because EIGRP routes are always preferred over OSPF or static routes.
B. 10.1.0.0/16 static, because static routes are always preferred over OSPF or EIGRP routes.
C. 10.1.1.0/24 through OSPF because the route with the longest prefix is always chosen.
D. Whichever route appears in the routing table first.
E. The router will load share between the 10.1.0.0/16 route through EIGRP and the 10.1.0.0/16 static route.
Answer: C
Explanation: This is a tricky question. If you look at the AD the 0/1 for static/default routes would be chosen first then (90) EIGRP then (110) OSPF So pick your option. I think it is OSPF because all static and default routes would be the chosen route.

QUESTION .54 Describe the correct authentication sequence for the IOS Firewall Authentication Proxy:
A. The user authenticates by FTP, and route maps are downloaded from the proxy server.
B. The user authenticates locally to the router.
C. The user authenticates by Telnet, and access lists are downloaded from the AAA server.
D. The user authenticates by HTTP, or Telnet, and access lists are downloaded from the AAA server.
E. The user authenticates by HTTP, and access lists are downloaded from the AAA server.
Answer: E
Explanation: When a user initiates an HTTP session through the firewall, the authentication proxy is triggered

---

QUESTION .55 Exhibit:



Host A is attempting to send a packet through Router B to Host D. There are not routing protocols configured nor are there any static routes for router B or C. However, Router B does have a default gateway configured to the IP address of Router C using the configuration ip default-gateway 10.1.2.2.Will Host A's packet reach Host D?

A. This will work of the routers are configured to bridge.

B. This will work because Router B will forward the packets destined to 10.1.3.0/24 to Router C through its IP default-gateway configuration.

C. The packets will reach Host D, but Host D will not be able to communicate back to Host A, so the session will fail.

D. This will work if CDP is enabled on the routers.

E. Routers only route packets to routes in the routing table, not their IP default-gateway so Host A's packets will never reach Router C or Host D.

Answer: B

Explanation: This is a tricky question because it does not say that C has ip default-gateway. SO it wont be able to send the packet back but the packet will reach D. Pick your option The ip default gateway command differs from the other two commands in that it should only be used when ip routing is disabled on the Cisco router

QUESTION .56 **T**he purpose of Administrative Distance, as used by Cisco routers, is:

A. To choose between routes from different routing protocols when receiving updates for the same network.

B. To identify which routing protocol forwarded the update.

C. To define the distance to the destination used in deciding the best path.

D. To be used only for administrative purposes.

Answer: A

Explanation: Administrative distance is the feature used by routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized
in order of most to least reliable (believable) using an administrative distance value.

QUESTION .57 -User_A and User_B are both members of the global group "DOMAIN USERS". -Global group" DOMAIN USERS" is included in local group "USERS".

-All users and groups are in the domain "CORP".

-The directory D:\data has the share permission for local group "USERS" set to "Read".

-The Microsoft Word document D:\data\word.doc has file permissions for local group "USERS" set to "Full Control".

-The Microsoft Word document D:\data\word.doc is owned by User_B. Given this scenario on a Windows NT 4.0 network, what is the expected behavior when User_A attempts to edit D:\data\word.doc?
A. User_A has full control and can edit the document successfully.
B. There is not enough information. Permissions for Microsoft Word are set within the application and are not subject to file and share level permissions.
C. Access would be denied. Only the owner of a file can edit a document.
D. Global groups can not be placed into local groups. The situation could not exist.
E. Edit access would be denied. The "Read" permission is least permissive so it would apply in this situation.
Answer: E
Explanation: Based on the name of each group, you might think that you'd add local groups to global groups. This isn't the case. You assign users or global groups to local groups to give access to local resources

---

QUESTION .58 A network manager issues an RCP (Remote Copy) when copying a configuration from a router to a Unix system. What file on the Unix system would need to be modified to allow the copying to occur?
A. rcmd
B. rcmd.allow
C. allow.rcmd
D. hosts.allow
E. .rhosts
Answer: D
Explanation: NOT SURE OF THIS ANSWER I AM SAYING .RHOSTS The$HOME/.rhosts file defines which remote hosts (computers on a network) can invoke certain commands on the local host without supplying a password. This file is a hidden file in the local user's home directory and must be owned by the local user

---

QUESTION .59 In the context of intrusion detection, what is the definition of exploit signatures?
A. Policies that prevent hackers from your network.
B. Security weak points in your network that can be exploited by intruders.
C. Identifiable patterns of attack detected on your network.
D. Digital graffiti from malicious users.
E. Certificates that authenticate authorized users.
Answer: C

QUESTION .60 The network administrator has forgotten the enable password of the router. Luckily, no one is currently logged into the router, but all passwords on the router are encrypted. What should the administrator do to recover the enable secret password?
A. Call the Cisco Technical Assistance Center (TAC) for a specific code that will erase the existing password.
B. 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.
C. 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.
D. 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: C
Explanation: The other possible answer is not correct in my view as you still need to put the config back onto the router after Rommon mode (normally in nvram but TFTP is a valid storage place as well)

QUESTION .61 According to RFC 1700, what well-known ports are used for DNS?
A. TCP and UDP 23.
B. UDP 53 only.
C. TCP and UDP 53.
D. UDP and TCP 69.
Answer: C
Explanation: Type Application layer name space translation protocol. Port 53 (TCP, UDP)server.

QUESTION .62 The purpose of Lock & Key is:
A. To secure 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. To allow a user to Telnet to the router and have temporary access lists applied after issuance of the access-enable command.
C. To require additional authentication for traffic traveling through the PIX for TTAP compliance.
D. To prevent users from getting into enable mode.
Answer: B
Explanation: Lock-and-key access allows you to set up dynamic access lists that grant access per user to a specific source/destination host through a user authentication process. You can allow user access through a firewall dynamically, without compromising security restrictions. The following
process describes the lock-and-key access operation A user opens a Telnet session to a border router configured for lock-and-key access. The Cisco IOS software receives the Telnet packet and performs a user authentication process. The user must pass authentication before access is allowed. The
authentication process can be done by the router or a central access server such as a TACACS+ or RADIUS server.

QUESTION .63 In addition to Kerberos port traffic, what additional service is used by the router and the Kerberos server in implementing Kerberos authentication on the router?
A. TCP
B. DNS
C. FTP
D. ICMP
E. Telnet
Answer: E
Explanation: The following network services are supported by the Kerberos authentication capabilities in Cisco IOS software Telnet, rlogin, rsh, rcp

---

QUESTION .64 Identify the default port(s) used for web-based SSL (Secure Socket Layer) Communication:
A. TCP and UDP 1025.
B. TCP 80.
C. TCP and UDP 443.
D. TCP and UDP 1353.
Answer: C
Explanation: Secure Sockets Layer (SSL) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates, public keys, and private keys. Use 443 (generally used for SSL transactions) as the SSL TCP service port and 443 as the clear text port. Configure the server to not use SSL and to monitor port 443. TCP service port 80requests are serviced

normally. Use 443 as the SSL TCP service port and 81 (or another unused port) for the clear text port. Configure the server to monitor port 81. TCP service port 80 requests are serviced normally.

QUESTION .65 In the TACACS+ protocol, the sequence number is: (Multiple answer)
A. An identical number contained in every packet.
B. A number that must start with 1 (for the fist packet in the session) and increment each time a request or response is sent.
C. Always on odd number when sent by the client.
D. Always an even number when sent by the client and odd when sent by the daemon.
Answer: B, C
Explanation: Seq_no - The sequence number of the current packet for the current session. The first TACACS+ packet is a session must have the sequence number 1, and each subsequent packet increments the sequence number by 1. Thus, clients (such as the NAS) send only packets containing odd sequence numbers, and TACACS+ daemons send only packets containing even sequence numbers. The sequence number must never wrap. In other words, if the sequence number 2^8-1 is ever reached, that session must terminate and be restarted with a sequence number of 1. CCIE Professional Development Network Security Principles and Practices by Saadat Malik pg 496

QUESTION .66 A network administrator is troubleshooting a problem with FTP services. If a device blocks the data connection, the administrator should expect to see:
A. Very slow connect times.
B. Incomplete execution, when issuing commands like "pwd" or "cd".
C. No problems at all.
D. User login problems.
E. Failure when listing a directory.
Answer: E
Explanation: Below is a caption from a cert advisory about FTP. FTP can have problems when the data channel is blocked. In FTP PASV mode, the client makes a control connection to the FTP server (typically port 21/tcp) and requests a PASV data connection. The server responds by listening for client connections on a specified port number, which is supplied to the client via the control connection. An active open is done by the server, from its port 20 to the same port on the client machine as was used for the control connection. The client does a passive open. For better or worse, most current FTP clients do not behave that way.

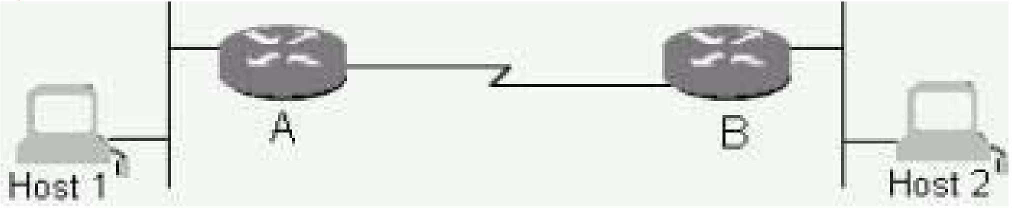
QUESTION .67 A Denial of Service (DoS) attack works on the following principle:
A. MS-DOS and PC-DOS operating systems utilize a weak security protocol.
B. All CLIENT systems have TCP/IP stack implementation weaknesses that can be compromised and permit them to launch an attack easily.
C. Overloaded buffer systems can easily address error conditions and respond appropriately.
D. Host systems cannot respond to real traffic, if they have an overwhelming number of incomplete connections (SYN/RCVD State).
E. A server stops accepting connections from certain networks, once those networks become flooded.
Answer: B
Explanation: Some of these answers are true examples of types of dos but in itself does not define a dos Denial-of-service (DOS) attacks might attempt o starve a host of resources needed to function correctly. Network

Intrusion Detection third edition by Stephen Northcutt and Judy Novak pg 93

QUESTION .68 Global deployment of RFC 2827 (ingress and egress filtering) would help mitigate what classification of attack?
A. Sniffing attack
B. Denial of service attack
C. Spoofing attack
D. Reconnaissance attack
E. Port Scan attack
Answer: C
Explanation: Network Ingress Filtering- Defeating Denial of Service Attacks which employ IP Source Address Spoofing

QUESTION .69 Which security programs can effectively protect your network against password sniffer programs?(Multiple answer)
A. IPSec, because it encrypts data.
B. One time passwords, because the passwords always change.
C. RLOGIN, because it does not send passwords.
D. Kerberos, because it encrypts passwords.
E. Use of POP e-mail, because it is better than using SMTP.
Answer: A, B

QUESTION .70 Exhibit:



Host 1 and Host 2 are on Ethernet LANs in different building. A serial line is installed between two Cisco routers using Cisco HDLC serial line encapsulation. Routers A and B are configured to route IPtraffic. Host 1 sends a packet to Host 2. A line hit on the serial line causes an error in the packet. When this is detected, the retransmission is sent by:
A. Host 1
B. Host 2
C. Router A
D. Router B
E. Protocol analyzer
Answer: C

QUESTION .71 The Diffie-Hellman key exchange allows two parties to establish a shared secret key: (Multiple answer)
A. Over an insurance medium.
B. After a secure session has been terminated.
C. Before a secure session has been initiated.

D. After a session has been fully secured.
E. During a secure session over a secure medium.
Answer: A, C Explanation: DH is used over a insecure medium

QUESTION .72 Exhibit:
aaa new-model aaa authentication login default local aaa authentication exec default local username abc privilege 5 password xyz privilege exec level 3 debug ip icmp.
If a router is configured as shown, what will happen when user ABC Telnets to the router and tries to debug ICMP? (Multiple answer)
A. The user will be locked out because the aaa new-model command is enabled and no TACACS server is defined.
B. The user can gain entry with the local username/password, but will not be able to use any debug commands because command authorization will fail.
C. The user can gain entry with the local username/password at Level 5, but cannot use any commands because none are assigned at Level 5.
D. The user can gain entry with a local username/password at Level 5 and run debug ip icmp unchallenged.
Answer: D
Explanation: To understand this example, it is necessary to understand privilege levels. By default, there are three command levels on the router. privilege level 0 - includes the disable, enable, exit, help, and logout commands privilege level 1 - normal level on Telnet; includes all user-level
commands at the router> prompt privilege level 15 - includes all enable-level commands at the router# prompt username john privilege 9 password 0 doe - He can configure snmp-server community because configure terminal is at level 8 (at or below level 9), and snmp-server community is level-8 command.

QUESTION .73 When the Cisco Secure Intrusion Detection System sensor detects unauthorized activity:
A. It sends e-mail to the network administrator.
B. It sends an alarm to Cisco Secure Intrusion Detection System Director.
C. It shuts down the interface where the traffic arrived, if device management is configured.
D. It performs a traceroute to the attacking device.
Answer: B
Explanation: CSIDS does a lot of these things, but the sensor is more specified. It sends the alarm to the full CSIDS director

QUESTION .74 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. Can this behavior be changed?
A. No, this is built in feature of Cisco IOS software.
B. Yes, use the no ip domain-lookup command.
C. Yes, use the no ip helper-address command.
D. Yes, use the no ip multicast helper-map command.
E. Yes, use the no exec lookup command.
Answer: B
Explanation: You can disable IP domain lookup using the no ip domain-lookup command under the router's global configuration mode. This will stop the IP domain lookup and speed up the show command output.

QUESTION .75 What network management software must be installed prior to the Cisco Secure Intrusion Detection System Director software?
A. Cisco Works 2000 on Unix.
B. SunNet Manager on Solaris.
C. HP Open View on HPUX or Solaris.
D. Microsoft Internet Information Server on Windows NT.
E. NetSonar on Linux.
Answer: C
Explanation: The following software must be installed on your workstation: HP-UX HP-UX10.20 HP Open View 4.1, 5.01, or 6.0 Web browser (for NSDB and help file) Sun Solaris 2.5.1 or2.6 HP Open View 4.1, 5.01, or 6.0 Web browser (for NSDB and help file)

QUESTION .76 In the IPSec protocol suite, transport mode & tunnel mode describe:
A. AH header and datagram layouts.
B. Diffie-Hellman keying.
C. SHA security algorithm.
D. ESP header and datagram layouts.
Answer: D
Explanation: OK I don't get this question ESP or AH can be used in tunnel or transport mode.316 In Transport Mode ESP, the ESP header is inserted into the IP datagram immediately prior to the transport-layer protocol header (such as TCP, UDP, or ICMP). In Tunnel Mode ESP, the original IP datagram is placed in the encrypted portion of the ESP and that entire ESP frame is placed within a datagram having unencrypted IP headers.

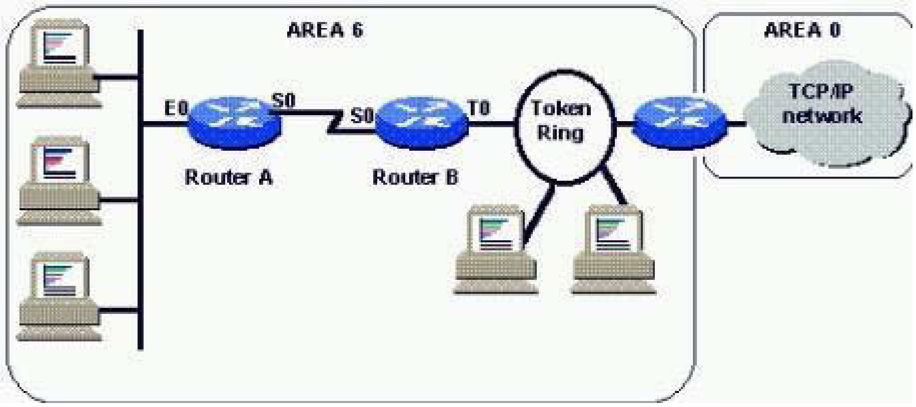
QUESTION .77 What well known port is commonly used for TFTP?
A. TCP 23
B. UDP 23
C. UDP 161
D. UDP 69
Answer: D
Explanation: Abbreviation of Trivial File Transfer Protocol, a simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP)and provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers.

QUESTION .78 What is RPF?
A. Reverse Path Forwarding
B. Reverse Path Flooding
C. Router Protocol Filter
D. Routing Protocol File
E. None of the above.
Answer: A
Explanation: This chapter describes Unicast Reverse Path Forwarding (Unicast RPF)commands.

QUESTION .79 IKE Phase 1 policy does not include negotiation of the:
A. Encryption algorithm
B. Authentication method.
C. Diffie-Hellman group.

D. Lifetime
E. Crypto-map access-list
Answer: E
Explanation: "Ike Phase 1 Policy Parameters - Encryption, Hash, Authentication method, Key exchange, Ike SA lifetimes" Cisco Secure PIX Firewall Advanced 2.0 14-14 "IKE's responsibilities in the IPSEC protocol include Negotiating protocol parameters, Exchanging public keys, authenticating both sides, managing keys after the exchange...In Phase 1 exchange, peers negotiate a secure, authenticated channel with which to communicate." CCIE Professional Development Network Security Practices and Principles by Saadit Malik pg 276, 278 "The first two messages in IKE main mode negotiation are used to negotiate the various values, hash mechanisms, and encryption mechanisms to use for the later half of the IKE negotiations." CCIE Professional Development Network Security Practices and Principles by Saadit Malik pg 280

QUESTION .80 Exhibit:



In a move to support standards-based routing, the decision is made to use the OSPF routing protocol throughout the entire network. The areas are shown as in the exhibit, and the subnets are:
Ethernet on Router A: 108.3.1.0 Serial line between Router A and Router B: 108.3.100.0 Token ring on Router B: 108.3.2.0
How should OSPF be configured on Router B?
A. router ospf
network 108.3.0.0
B. router ospf 1
network 108.3. 100.0 0.0.0.255 area 6
network 108.3.2.0 0.0.0.255 area 6
C. router ospf 1
network 108.3. 100.0 0.0.0.255 area 6
network 108.3.2.0 0.0.0.255 area 0
D . router ospf 1
network 108.3. 100.0 255.255.255.0 area 6
network 108.3.2.0 255.255.255.0 area 6
E. router ospf 1
network 108.3. 1.0 0.0.0.255 area 6
network 108.3.100.0 0.0.0.255 area 6
network 108.3.2.0 0.0.0.255 area 6
Answer: D configured in area 6. the Ethernet network on router A will be given to router B by router A

so there is no need to insert the network statement for it.
Explanation: Networks 108.3.100.0 and 108.3.2.0 using a /24 need to be put into the ospf statement.

QUESTION .81 Exhibit:
/etc/hosts.equiv:2.2.2.2 /etc/passwd:user_B:x:1003:1:User B:/export/home/user_B:/bin/kshuser_C:x:1004:1:UserC:/export/home/user_C:/bin/kshwith Host_B having the ip 2.2.2.2 & host C having the ip 3.3.3.3
What policy would be enforced given the files shown?
A. Allow User_B on Host_B to access Host_A via rlogin, rsh, rcp, & rcmd without a password.
B. Allow User_B to access Host_A via rlogin, rsh, rcp, & rcmd with a password but to prevent access from unlisted hosts including Host_C
C. Allow users to telnet from Host_B to Host_A but prevent users from telneting from unlisted hosts including Host_C
D. Allow users on Host_A to telnet to Host_B but not to unlisted hosts including Host_C
Answer: B
Explanation:

QUESTION .82 Given: Two routers have their SA lifetime configured for 86399 seconds and 2 million kilobytes. After 24 hours have passed and 500 KB of traffic have been tunneled, what happens?
A. If pre-shared keys are being used, traffic will stop until new keys are manually obtained and inputted.
B. The SA will be renegotiated.
C. The SA will not be renegotiated until 2 MB of traffic have been tunneled.
D. Traffic will be sent unencrypted.
Answer: C
Explanation: more or less 86399 seconds is 23.9 hours however 86400 is 24 hours so the SA need to be renegotiated

---

QUESTION .83 Why is authentication NOT used with TFTP?
A. TFTP protocol has no hook for a username/password.
B. TFTP uses UDP as a transport method.
C. TFTP is initiated by a server.
D. TFTP is already secure.
E. All of the above.
Answer: A
Explanation: FTP requires a username and password. TFTP does not.

QUESTION .84 If a network manager believes security has been compromised on a router or PC client, and he/she wishes to have the CA certificate revoked, the manager would:
A. Contact the CA administrator and be prepared to provide the challenge password chosen upon installation.
B. If a router is involved, type: configure terminal crypto ca revoke <name>
C. Uninstall the IPSec software on the PC, erase the router configuration and reconfigure the router, and request the certificate in the same way as the initial installation (Issuance of the new certificate will revoke the old one automatically).
D. Send e-mail to 'sysadmin@icsa.net' with the hostname and IP of the compromised device requesting certificate revocation.
Answer: A

Explanation: If you lose the password, the CA administrator may still be able to revoke the PIX Firewall's certificate, but will require further manual authentication of the PIX Firewall administrator identity.

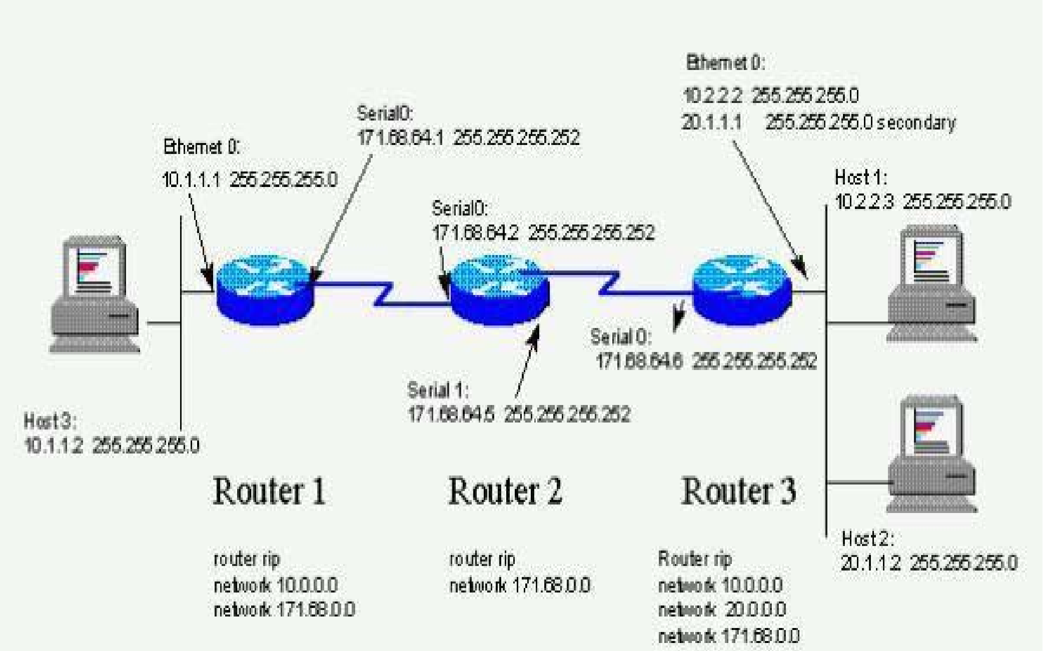
QUESTION .85 Scanning tools may report a root Trojan Horse compromise when run against an IOS component. Why does this happen?
A. The port scanning package mis-parses the IOS error messages.
B. IOS is based on BSD UNIX and is subject to a Root Trojan Horse compromise.
C. The scanning software is detecting the hard-coded backdoor password in IOS.
D. Some IOS versions can be crashed with the telnet option vulnerability.
E. IOS will not respond to vulnerability scans.
Answer: A

QUESTION .86 Which statement regarding the RADIUS authentication protocol are true? Multiple answer)
A. UDP 1812 is specified in RFC 2138.
B. UDP 1645 is commonly used by many vendors.
C. UDP 1647 is specified in RFC 2139.
D. UDP 48 is commonly used by many vendors.
Answer: A, B
Explanation: Exactly one RADIUS packet is encapsulated in the UDP Data field [2],where the UDP Destination Port field indicates 1812 (decimal). When a reply is generated, the source and destination ports are reversed. This memo documents the RADIUS protocol. There has been some
confusion in the assignment of port numbers for this protocol. The early deployment of RADIUS was done using the erroneously chosen port number 1645, which conflicts with the "data metrics" service. The officially assigned port number for RADIUS is 1812.

QUESTION .87 A Security Manager needs to configure an IPSec connection using ISAKMP with routers from mixed vendors. What information is NOT needed to configure the local security device to communicate with the remote machine?
A. Remote peer address.
B. Main mode attributes.
C. Quick mode attributes.
D. Addresses that need to be encrypted.
E. Peer gateway subnet.
F. Encryption authentication method.
Answer: E
Explanation: The peers gateway subnet is not needed. The address is needed.

QUESTION .88 An ISAKMP NOTIFY message is used between IPSec endpoints for what purpose?
A. To let the other side know that a failure has occurred.
B. To let the other side know the status of an attempted IPSec transaction.
C. To let the other side know when a physical link with an applied SA has been torn down.
D. To let the other side know that an SA has been bought up on an unstable physical connection; potential circuit flapping can cause problems for SPI continuity.
Answer: C

QUESTION .89 Exhibit:



If Host 1 cannot ping Host 2 and Host 2 cannot ping Host 1, what is most likely the cause?
A. Split horizon issue.
B. Default gateway on hosts.
C. Routing problem with RIP.
D. All of the above.
Answer: D

QUESTION .90 When building a non-passive FTP data connection, the FTP client:
A. Indicates the port number to be used for sending data over the command channel via the PORT command.
B. Receives all data on port 20, the same port the FTP server daemon sends data from.
C. Uses port 20 for establishing the command channel and port 21 for the data channel.
D. Initiates the connection from an ephemeral port to the RFC specified port of the server.
Answer: D
Explanation: Standard mode FTP uses two channels for communications. When a client starts an FTP connection, it opens a standard TCP channel from one of its higher-order ports to port 21on the server. This is referred to as the command channel. Cisco Secure PIX firewall Advanced 2.0 10-
5

QUESTION .91 The RADIUS attribute represented by the value 26 is used for:
A. Specifying accounting data specific to a particular vendor service.
B. Specifying the vendor name of the NAS.
C. Allowing vendors to define out-of-band RADIUS timeouts.
D. Transmitting vendor-specific attributes.
Answer: D
Explanation: Vendor-specific - allows vendors to support their own extended attributes that are unsuitable for general use. Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Network Security Principles and Practices, Saadat Malik p 524

QUESTION .92 A Hash (such as MD5) differs from an Encryption (such as DES) in what manner?
A. A hash is easier to break.
B. Encryption cannot be broken.
C. A hash is reversible.
D. A hash, such as MD5, has a final fixed length.
E. Encryption has a final fixed length.
Answer: D
Explanation: The MD5 algorithm takes as input a message of arbitrary length and produces as output infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.' Message hashing is an encryption technique that can be used to ensure that a message has not been altered. The MD5 algorithm takes as input a clear text message of arbitrary length...The MD5 algorithm is run on the input, which produces as output a fixed-length,128-bit "message digest" or "hash" of the input.' "It is considered computationally infeasible to reverse the hash process or to produce two message having the same message digest" Managging Cisco Network Security by Michael Wenstrom pg 464

QUESTION .93 Which statement about the Diffie-Hellman key exchange is false?
A. The two routers involved in the key swap generate large random integers (i), which are exchanged in private.
B. The local secret key is combined with known prime numbers n and g in each router to generate a Public key.
C. Each router combined the private key received from the opposite router with its own public key to create a shared secret key.
D. Each router uses the received random integer to generate a local secret (private) crypto key.
Answer: D
Explanation: more or less XvA=G^A mod P Network Security Principles and Practices, Saadat Malik p 284

QUESTION .94 Exhibit:
Configuration of Router A: crypto map tag 1 ipsec-isakmpset security-association lifetime seconds 240set security-association lifetime kilobytes 10000
Configuration of Peer Host Router B: crypto map tag 1 ipsec-isakmpset security-association lifetime seconds 120set security-association lifetime kilobytes 20000
Router A is configured as shown. Predict and explain what will happen after 110 seconds and 1500kilobytes of traffic:
A. Router A will not talk to Router B because the security association lifetimes were misconfigured; they should be the same.
B. The security association will not be renegotiated until 20000 kilobytes have traversed the link, because the interval will be the greater of 2 parameters - time and kilobytes.
C. Security association renegotiation will have started.
D. Assuming the same traffic pattern and rate, the present security associations will continue until almost 240 seconds have elapsed.
Answer: A
Explanation: I have heard different answers to this question. 1 is that the lesser of the values will be used. But the SA need to match which these don't.

QUESTION .95 What encryption algorithm is used for Microsoft Point-to-Point Encryption?
A. DES CBC
B. RSA RC4
C. RSA CBC
D. DES RC4
Answer: B
Explanation: MPPE uses the RSA RC4 [3] algorithm to provide data confidentiality.

QUESTION .96 The TFTP protocol:
A. Uses the UDP transport layer and requires user authentication.
B. Uses the TCP transport layer and does not require user authentication.
C. Uses the UDP transport layer and does not require user authentication.
D. Used TCP port 69.
E. Prevents unauthorized access by doing reverse DNS lookups before allowing a connection.
Answer: C
Explanation: TFTP does not require password authentication, and uses UDP port 69. this rules out all answers except C

QUESTION .97 What type of crypto maps and keying mechanism would be the most secure for a router connecting to a dial PC IPSec client?
A. Static crypto maps with pre-shared keys.
B. Static crypto maps with RSA.
C. Dynamic crypto maps with CA.
D. Dynamic crypto maps with pre-shared keys.
Answer: B
Explanation: Dynamic crypto maps are not recommend as the required matches are very small.

QUESTION .98 What is true about the DLCI field in the Frame Relay header?
A. It consists of two portions, source and destination, which map data to a logical channel.
B. It generally has significance only between the local switch and the DTE device.
C. It is an optional field in the ITU-T specification.
D. It present only in data frames sent through the network.
Answer: B
Explanation: DLCI is only locally significant

QUESTION .99 A user dials into the ISP router of a VPDN network as 'jsmith@abc.xzy'. The router is using TACACS+ or RADIUS authentication and authorization. At minimum, what information will be received from the ISP authentication server?
A. The tunnel-id and IP address of the Home Gateway (HGW) router based on domain abc.xzy.
B. The tunnel-id, IP address of the HGW router, and the IP address of outgoing ISP router interface based on domain abc.xzy.
C. The IP address of the HGW router and IP address of the outgoing ISP router interface based on domain abc.xzy.
D. An access-accept or access-reject (if RADIUS) or a PASS or FAIL (if TACACS) for useridjsmith@abc.xzy.
Answer: D

Explanation: The user must be authenticated first before any thing can happen (like the downloading of Access-lists)

QUESTION .100 What are the only two part found in a RADIUS user profile?
A. Reply attributes, check attributes
B. Reply items, check items
C. Check items, reply attributes
D. Check attributes, reply items
Answer: D
Explanation: Table 3-1: Standard User Profile Attributes Attribute Usage Password Specifies the user's password(check attribute). NAS-IP-Address IP address of the NAS1 (check attribute). Service_Type Specifies the level of service the user is requesting (check attribute). Session-Timeout Specifies, in seconds, the maximum length of the user's session (reply attribute). Idle-Timeout Specifies, in seconds, the maximum time a connection can remain idle (reply attribute).

Section B - Practice Questions.

QUESTION .1 IPSec supports encryption of broadcasts and multicasts, true or false?
A. True
B. False
Answer: B
Explanation: Much IP voice and video traffic is transmitted in multicast. IPsec does not natively support multicast traffic, which means voice and video traffic will be dropped when traversing the IPsec VPN. Restrictions---At this time, IPSec can be applied to unicast IP Datagrams only. Because the IPSec Working Group has not yet addressed the issue of group key distribution, IPSec does not currently work with multicasts or broadcast IP datagram

QUESTION .2 Will CBAC support stateful inspection of IPSec traffic?
A. No, CBAC does not support this.
B. Yes, CBAC can be configured to support IPSec.
C. Yes, use the inspection rule "ip inspect name ccie ipsec".
D. None of the above.
E. All of the above.
Answer: A
Explanation: CBAC does not inspect ipsec traffic therefore you need to allow the traffic in the inbound ACL. Be sure to allow esp protocol and udp port 500. Cisco IOS 12.0 Network Security", the authors state that CBAC is compatible with IPSec provided the tunnel end-point is on the router, and not a "pass-through" config.

QUESTION .3 Which of the following do not support local authentication?
A. authentication proxy
B. lock-and-key
C. login local
D. pptp VPN
Answer: A
Explanation: Use Lock-and-key in network environments that might benefit from local authentication and a limited number of router-based access control policies based on host addresses

QUESTION .4 Which Cisco security filtering method can "intelligently filter based on application-layer protocol session information"?
A. CBAC
B. ACL
C. IDS
D. Auth-proxy
E. PAM
F. Asec
Answer: A
Explanation: PAM=port adapter module (PAM) To configure CBAC inspection for an application-layer protocol, use one or both of the following global configuration commands:

QUESTION .5 The routing protocol on your non-broadcast frame-relay interface isn't functioning correctly with all of its neighbors on the frame-relay network. What could be one issue that should come to mind?
A. Split-horizon
B. Discontiguous networks
C. Classful network
D. VLSM
E. Default routing
Answer: A
Explanation: IP split horizon checking is disabled by default for Frame Relay encapsulation so routing updates will come in and out the same interface An exception is the Enhanced Interior Gateway Routing Protocol(EIGRP) for which split horizon must be explicitly disabled. Configuring Frame Relay subinterfaces ensures that a single physical interface is treated as multiple virtual interfaces. This capability allows you to overcome split horizon rules so packets received on one virtual interface can be forwarded to another virtual interface, even if they are configured on the same physical interface.

QUESTION .6 What is the decimal equivalent of 10101100 01100000 00010011 10000101 ?
A. 172.96.19.133
B. 192.96.19.133
C. 172.96.19.132
D. 172.96.18.133
E. 172.192.19.133
Answer: A
Explanation:128 64 32 16 8 4 2 1 128 64 32 16 8 4 2 1 128 64 32 16 8 4 2 1 128 64 32 16 8 4 2 11 0 1 0 11 0 0 0 1 1 0 0 0 0 0 0 0 0 1 0 0 1 1 1 0 0 0 0 1 0 1172 9619 133

QUESTION .7 Which of the following are CBAC supported protocols? (Select all that apply)
A. FTP
B. RealAudio
C. RTSP
D. SMTP
E. SQL*NET
F. TFTP
Answer: A, B, C, D, E, F Explanation: You can configure CBAC to inspect the following types of sessions: All

TCP sessions, regardless of the application-layer protocol (sometimes called "single channel" or "generic" TCP inspection) All UDP sessions, regardless of the application-layer protocol(sometimes called "single-channel" or "generic" UDP inspection) You can also configure CBAC to specifically inspect certain application-layer protocols. The following application-layer protocols can all be configured for CBAC CU-See Me (only the White Pine version) FTP H 323 (such as NetMeeting, Pro Share) Java UNIX R-commands (such as rlogin, rexec, and rsh) RealAudio RPC (Sun RPC, not DCERPC or Microsoft RPC) SMTP SQL*Net Stream Works TFTP VDO Live In the case of RTSP inspection, session output can vary based on the multimedia protocol and the transport mode.

QUESTION .8 You want to filter routing updates. What are three possibilities that should come to mind? (Select all that apply)
A. route-map
B. distribute-list
C. filter-list
D. policy-map
E. route-filter
F. distribute-filter
Answer: A, B, C
Explanation: Use the policy-map command to specify the name of the policy map to be created, added to, or modified before you can configure policies for classes whose match criteria are defined in a class map. Entering the policy-map command enables QoS policy-map configuration mode
in which you can configure or modify the class policies for that policy map. Route filters, along with route patterns, use dialed-digit strings to determine how a call is handled. You can only use route filters with North American Numbering Plan (NANP) route patterns; that is, route patterns that use an at
symbol (@) wildcard.

QUESTION .9 Exhibit:

```
Signature audit statistics [process switch: fast switch]
signature 2000 packets audited: [0:43]
signature 2001 packets audited: [558:2281]
signature 2004 packets audited: [1112:8803]
signature 2005 packets audited: [6:136]
signature 2006 packets audited: [1:2]
signature 2151 packets audited: [0:99]
signature 3040 packets audited: [0:1]
signature 3101 packets audited: [0:1100]
signature 3103 packets audited: [0:1]
Interfaces configured for audit 0
Session creations since subsystem startup or last reset 9712
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [14:12:2]
Last session created 5w5d
Last statistic reset never
Host ID:2, Organization ID:1234, SYN pkts sent:749422,ACK pkts sent:0, Heartbeat pkts sent:0, Heartbeat
ACK pkts sent:0,Duplicate ACK pkts
received:0, Retransmission:0, Queued pkts:0
```

Look at the attached exhibit. What command is this output

generated by?
A. show ip audit statistics
B. show ip verify statistics
C. show ip ids statistics
D. show audit statistics
E. show ids statistics
Answer: A
Explanation: The following displays the output of the show ip audit statistics command: Signature audit statistics[process switch: fast switch] signature 2000 packets audited: [0:2] signature 2001 packets audited: [9:9]signature 2004 packets audited: [0:2] signature 3151 packets audited: [0:12] Interfaces configured for audit 2 Session creations since subsystem startup or last reset 11 Current session counts (estab/halfopen/terminating) [0:0:0] Maxever session counts (estab/half-open/terminating) [2:1:0] Last session created 19:18:27 Last statistic reset never HID:1000 OID:100 S:218 A:3 H:14085 HA:7114 DA:0 R:0The Following show commands are not real commands show ip verify statistics show ip ids statistics show audit statistics show ids statistics

---

QUESTION .10 Your internal users cannot access hosts in the Internet, by name, through the PIX. What command is probably missing?
A. alias
B. conduit
C. dns
D. route
Answer: A
Explanation: The alias command has two possible functions: It can be used to do "DNS Doctoring" of DNS replies from an external DNS server. In DNS Doctoring, the PIX "changes" the DNS response from a DNS server to be a different IP address than the DNS server actually answered for a given name. This process is used when we want the actual application call from the internal client to connect to an internal server by its internal IP address. It can be used to do "Destination NAT" (dnat) of one destination IP address to another IP address. The DNS answer has some merit but it is not a command

---

QUESTION .11 What is the command that was run, resulting in the output in the attached exhibit?
A. crypto key generate rsa usage-keys
B. crypto key generate rsa
C. show crypto key mypubkey rsa
D. crypto isakmp identity address
Answer: A
Explanation: crypto key generate rsa usage-keys The name for the keys will be:myrouter.example.com Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus[512]? Generating RSA keys.... [OK]. Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus[512]? Generating RSA keys.... [OK]. The following example
generates general-purpose RSA keys.
(Note, you cannot generate both special-usage and general purpose keys; you can generate only one or the other.) NOTICE the difference crypto key generate rsa The name for the keys will be: myrouter.example.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key

modulus greater than 512 may take a few minutes. How many bits in the modulus[512]? Generating RSA keys.... [OK].

QUESTION .12 With PIX OS version 6.2, how many levels of command authorization are there?
A. 1
B. 16
C. 255
D. 15
E. 2, exec and enable.
Answer: B
Explanation: Most commands in the PIX are at level 15, although a few are at level 0. To show current settings for all commands, issue the following command show privilege all

---

QUESTION .13 What product allows you to administer user authentication, accounting, and authorization?
A. ACS
B. PDM
C. CSPM
D. RADIUS
Answer: A
Explanation: ACS offers centralized command and control for all user authentication, authorization, and accounting PDM Cisco PIX Device Manager (PDM) offers enterprise and service provider users the features they need to easily manage Cisco PIX Firewalls. CSPM managing policy through your Managed Devices is the goal of using CSPM button Remote Authentication Dial-In User Service is a distributed client/server system that secures networks against unauthorized access. (it is a protocol like tacacs+, not an application)

QUESTION .14 What is recommended file, accessible only by root, where hashed UNIX passwords are stored?
A. passwd
B. /etc/shadow
C. /etc/shadow/passwd
D. /etc/password
E. /var/adm/shpass
F. /etc/passwd
Answer: B
Explanation: One of these is the shadow password scheme, which is used by default. The encrypted password is not kept in /etc/passwd, but rather in /etc/shadow. /etc/passwd has a placeholder, x, in this field. passwd is readable by everyone, whereas shadow is readable only by root. The shadow file also contains password aging controls.

QUESTION .15 Which of these best describe IPSec? (Select all that apply)
A. confidentiality
B. integrity
C. origin authentication
D. anti-replay
E. CA
Answer: A, B, C, D

Explanation: IPSec provides the following network security services. These services are optional. In general, local security policy will dictate the use of one or more of these services: Data Confidentiality-The IPSec sender can encrypt packets before transmitting them across a network. Data Integrity-The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission. Data Origin Authentication-The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service. Anti-Replay-The IPSec receiver can detect and reject replayed packets

---

QUESTION .16 On a PIX firewall, which level is considered least secure?
A. 0
B. 100
C. 1
D. 99
E. 255
Answer: A
Explanation: Either 0 for the outside network or 100 for the inside network. Perimeter interfaces can use any number between 1 and 99. By default, PIX Firewall sets the security level for the inside interface to security100 and the outside interface to security0. The first perimeter interface is initially set to security10, the second to security15, the third to security20, and the fourth perimeter interface to security25 (a total of 6 interfaces are permitted, with a total of 4 perimeter interfaces permitted). For access from a higher security to a lower security level, nat and global commands or static commands must be present. For access from a lower security level to a higher security level, static and access-list commands must be present. Interfaces with the same security level cannot communicate with each other. We recommend that every interface have a unique security level.

QUESTION .17 What is the purpose of a CA? (Select all that apply)
A. Manage and issue certificates.
B. Simplify administration of IPSec devices.
C. Define traffic flow.
D. Help IPSec configurations to scale.
E. Monitor IPSec statistics between sa's.
Answer: A, B
Explanation: Unlike RADIUS and TACACS+ authentication servers, Certificate Authority servers rely on a third-party authority to establish the trust relationship between two network objects that communicate

---

QUESTION .18 You are trying to browse the Internet and your connection is going through routers communicating via a GRE tunnel. The connections between the routers and GRE tunnels are up but accessing the Internet still doesn't work. What is the most likely cause of the problem? (Select all that apply)
A. Change the maximum segment size.
B. Use different IP addresses.
C. You are using incorrect IP addresses.
D. Hackers
E. You need to use the command "ip tcp adjust-mss".
F. Your link is down.
Answer: A, E
Explanation: When GRE tunnels are created, the default Maximum Transfer Unit (MTU)size is 1,514 bytes;

this size is fixed regardless of the physical interfaces. Physical interfaces have different MTU sizes When the OSPF routing protocol runs over GRE tunnels with different physical interfaces having different MTU sizes, initialization fails due to an MTU mismatch. Change the TCPMSS option value on SYN packets that traverse through the router (available in IOS 12.2(4)T and higher). This reduces the MSS option value in the TCP SYN packet so that it's smaller than the value in
the ip tcp adjust-mss value command, in this case 1436 (MTU minus the size of the IP, TCP, and GRE headers). The end hosts now send TCP/IP packets no larger than this value.

QUESTION .19 What are the three components that the Cisco Secure IDS consists of? (Select all that apply)
A. sensor
B. director
C. post office
D. log server
E. encryption
F. firewall
Answer: A, B, C

QUESTION .20 When going from the outside network to the inside network, what occurs first, encryption or NAT translation?
A. NAT translation
B. encryption
Answer: A

QUESTION .21 Which command would enable OSPF on your router?
A. router ospf {process-id}
B. router ospf
C. enable router ospf {process id}
D. ip router ospf {as number}
E. router ospf interface e0/0
Answer: A
Explanation: To configure an OSPF routing process, use the router ospf global configuration command. To terminate an OSPF routing process, use the no form of this command. router ospf process id router ospf 1 network 4.0.0.0 0.255.255.255 area 0

QUESTION .22 What command or commands will set a password that must be entered to access the router command mode with the prompt "Router#" (Select all that apply)
A. enable password
B. enable secret
C. enable secret password
D. secret password
E. password enable-mode
Answer: A, B
Explanation: By default, the router ships without password protection. Because many privileged EXEC commands are used to set operating parameters, you should password-protect these commands to prevent unauthorized use. You can use two commands to do this: enable secret password(a secure, encrypted password)

enable password (a less secure, unencrypted password) You must enter an enable secret password to gain access to privileged EXEC mode commands. router#

QUESTION .23 Which of the following are common guidelines to consider when configuring a firewall? (Select all that apply)
A. Disable cdp.
B. Set console, line, and enable passwords.
C. Restrict telnet access.
D. Turn off NTP.
E. No ip source-route.
F. Enable directed broadcasts.
Answer: A, B, C, D, E
Explanation: Don't enable any local service (such as SNMP or NTP) that you don't use. Cisco Discovery Protocol(CDP) and Network Time Protocol (NTP) are on by default, and you should turn these off if you don’t need them. You should also disable source routing. For IP, enter the no ip source-route global configuration command. Disabling source routing at all routers can also help prevent spoofing. Normally, you should disable directed broadcasts for all applicable interfaces on your firewall and on all your other routers. For IP, use the no ip directed-broadcast command. Rarely, some IP networks do require directed broadcasts; if this is the case, do not disable directed broadcasts.

QUESTION .24 What can Unicast RPF help prevent? (Select all that apply)
A. Smurf
B. Tribe Flood Network
C. Snoop
D. Packet ARP Smacking
Answer: A, B
Explanation: The Unicast RPF feature helps mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. The two main components to the smurf denial-of-service attack are the
use of forged ICMP echo request packets and the direction of packets to IP broadcast addresses. button TFN has the capability to generate packets with spoofed source IP addresses

---

QUESTION .25 Which of these commands might tell you if ssh has been configured on your router? (Select all that apply)
A. show ip ssh
B. show crypto ssh
C. show ssh
D. show crypto ip ssh
Answer: A, C
Explanation: To display the version and configuration data for Secure Shell (SSH), use the show ip ssh privileged EXEC command. To display the status of Secure Shell (SSH) server connections, use the show ssh privileged EXEC command.

QUESTION .26 If you don't want a third party to be able to prove your communication occurred, what should you use as your IKE authentication method?
A. encrypted nonces

B. signatures
C. CA
D. Diffie-Hellman Group 1
Answer: A
Explanation: RSA signatures and RSA encrypted nonces-RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA signatures provides non-repudiation while RSA encrypted nonces provide repudiation. In general terms, the term "non-repudiation" crypto technically means: In authentication, a service that provides proof of the integrity and origin of data, both in an unforgivable relationship, which can be verified by any third party at any time; or, In authentication, an authentication that with high assurance can be asserted to be genuine, and that can not subsequently be refuted. (Emphasis added) [14]

QUESTION .27 What is Unicast RPF?
A. Unicast RPF provides a secure command line interface for connections between host and remote.
B. Unicast RPF allows per user authentication, policies, and access privileges.
C. Unicast RPF provides 16 levels of security for assigning IOS commands and usernames.
D. Unicast RPF provides a solution to DoS attacks.
E. Unicast RPF provides a problem concerning DoS attacks.
Answer: D
Explanation: The Unicast RPF feature helps mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address.

QUESTION .28 Which encryption method has a 168 bit encryption key?
A. DES
B. ssh
C. MD5
D. IPSec
E. 3DES
Answer: E
Explanation: 56-bit Data Encryption Standard (DES) 168-bit 3DES algorithms

---

QUESTION .29 Routers operate on what layer?
A. 3
B. 2
C. 1
D. 4
E. 5
F. 7
Answer: A
Explanation: Network Layer

QUESTION .30 In Solaris 7, where are failed login attempts stored?
A. /var/adm/loginlog
B. /var/adm
C. /etc/adm/loginlog

D. /etc/wtmp
E. /var/adm/sulog
Answer: A

QUESTION .31 What allows clients to use authentication methods not supported by the NAS?
A. PPP
B. EAP
C. LCP
D. NAS
E. BGP
F. AAA
Answer: B
Explanation: LCP, BGP, AAA really don't apply

QUESTION .32 What are Dynamic access-lists also known as (select the best answer)?
A. lock-and-key
B. reflexive access-lists
C. access-lists
D. firewalls
E. acls
Answer: A
Explanation: Configuring Lock-and-Key Security (Dynamic Access Lists)

QUESTION .33 Which command would enable login authentication using a local password?
A. aaa authentication login default enable
B. aaa authentication login default krb5
C. aaa authentication login default line
D. aaa authentication login default local
Answer: D
Explanation: Set login authorization to default to local. aaa authentication login default local

QUESTION .34 What feature of a PIX firewall allows for "user-based authentication of inbound or outbound connections but then allows the traffic to flow quickly and directly"?
A. proxy
B. nat
C. pat
D. ASA
E. cut-through-proxy
F. ip audit
Answer: E
Explanation: Cut-Through proxies let the PIX Firewall perform dramatically faster than proxy-based servers while maintaining session state. Cut-Through proxy also lowers the cost of ownership by reusing the existing authentication database.

QUESTION .35 What provides integrated intrusion detection and firewall support at every perimeter of the network?

A. IOS Firewall
B. CSPM
C. ACS
D. PDM
E. IOS IDS Host
F. IDS Host Sensor
Answer: A
Explanation:

QUESTION .36 Which of the following are used to encrypt packet data?
A. DES
B. MD5
C. HMAC
D. SHA
E. AH
Answer: A Explanation: Data Encryption Standard. Standard cryptographic algorithm developed by the U.S. National Bureau of Standards.

QUESTION .37 With non-repudiation, what can be proven and what applies? (Select all that apply)
A. Communication took place.
B. Communication never took place.
C. Your connection can be traced.
D. Your connection cannot be traced.
Answer: A, C
Explanation: In general terms, the term "non-repudiation" crypto-technically means: In authentication, a service that provides proof of the integrity and origin of data, both in an unforgeable relationship, which can be verified by any third party at any time; or, In authentication, an authentication
that with high assurance can be asserted to be genuine, and that can not subsequently be refuted. (Emphasis added) [14]

QUESTION .38 IPSec can provide which of the following services? (Select all that apply)
A. Data Confidentiality
B. Data Integrity
C. Data Origin Authentication
D. Anti-Replay
E. Certificate Authority
F. IKE
Answer: A, B, C, D
Explanation: IPSec provides the following network security services. These services are optional. In general, local security policy will dictate the use of one or more of these services: Data Confidentiality-The IPSec sender can encrypt packets before transmitting them across a network. Data
Integrity-The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission. Data Origin Authentication-The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity
service. Anti-Replay-The IPSec receiver can detect and reject replayed packets

---

QUESTION .39 What are two good reasons to use RIP V2? (Select all that apply)
A. MD5 authentication
B. VLSM
C. FLSM
D. IGRP
E. clear-text authentication
Answer: A, B
Explanation: FLSM is RIP 1and IGRP is a routing protocol (like rip)

QUESTION .40 Which of these features of the PIX OS will help prevent DoS attacks on AAA servers?
A. Flood Guard
B. Flood Defender
C. AAA Defender
D. Flood AAA Defender
E. FragGuard
Answer: A
Explanation: The Flood Guard feature controls the AAA service's tolerance for unanswered login attempts. This helps to prevent a denial of service (DoS) attack on AAA services in particular. This feature optimizes AAA system use. It is enabled by default and can be controlled with the flood guard 1 command. The Flood Defender feature protects inside systems from a denial of service attack perpetrated by flooding an interface with TCP SYN packets FragGuard and Virtual Re-assembly is a feature that provides IP fragment protection. This feature uses syslog to log any fragment overlapping and small fragment offset anomalies, especially those caused by a teardrop.c attack.

QUESTION .41 Exhibit:
aaa new-model aaa authentication login default local enable password Cisco username backup privilege 7password 0 backup username root privilege 15 password 0 router privilege exec level 7 ping Look at the attached exhibit. The root user forgets his login password but still knows the enable password and the username/password combination for the backup account.
What can the root user do to fix his password problem?
A. Login with the backup account and use the enable password to view or change his password.
B. There is nothing he can do.
C. He will have to get the backup user to do it for him.
D. The enable password and the root password are the same so this is a moot point.
E. There is no login enabled on the console port so no one can get in.
Answer: A
Explanation: username backup states that there is an account called backup. Enable password allowed him to entry to privileged mode

---

QUESTION .42 What is this describing? Lets you securely interconnect geographically distributed users and sites
over an unsecure network"
A. VPN
B. IPSEC
C. IKE
D. TUNNEL

E. GRE
Answer: A
Explanation: Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

QUESTION .43 What are the three actions possible for the Cisco IOS IDS to take when a signature match occurs?(Select all that apply)
A. alarm
B. drop
C. reset

D. deny
E. permit
F. warning
Answer: A, B, C
Explanation: When one or more packets in a session match a signature, Cisco IOS IDS may perform the following configurable actions: Alarm: sends an alarm to a syslog server or Net Ranger Director Drop: drops the packet Reset: resets the TCP connection

---

QUESTION .44 What are triggered updates?
A. When a router waits until the hold-down is over before sending an update to another router.
B. When a router sends an update out all interfaces as soon as the route is unavailable.
C. Waiting for the next update before sending out an "unreachable" message.
Answer: B
Explanation:

QUESTION .45 Crypto access lists are used to do what?
A. Determine what traffic will and will not be protected by IPSec.
B. Determine what traffic will not be protected by Crypto.
C. Determine what traffic is allowed in and out of your interface.
D. As a firewall.
Answer: A
Explanation: Crypto access lists are used to define which IP traffic will be protected by crypto and which traffic will not be protected by crypto. The access lists themselves are not specific to IPSec. It is the crypto map entry referencing the specific access list that defines whether IPSec processing is applied to the traffic matching a permit in the access list. Crypto access lists associated with IPSec crypto map entries have four primary functions: Select outbound traffic to be protected by IPSec (permit = protect). Indicate the data flow to be protected by the new security associations (specified by a single permit entry) when initiating negotiations for IPSec security associations. Process inbound traffic to filter out and discard traffic that should have been protected by IPSec. Determine whether or not to accept requests for IPSec security associations on behalf of the requested data flows when processing IKE negotiation from the peer. (Negotiation is only done for ipsecisakmp crypto map entries.) In order for the peer's request to be accepted during negotiation, the peer must specify a dataflow that is "permitted" by a crypto access list associated with an ipsec-isakmp crypto map command entry. If you want certain traffic to receive one combination of IPSec protection (for example, authentication only) and other traffic to receive a different combination of IPSec protection (for example, both authentication and

encryption), you need to create two different crypto access lists to define the two different types of traffic. These different access lists are then used in different crypto map entries which specify different IPSec policies.

QUESTION .46 Select the AAA protocols that offer multiprotocol support.
A. TACACS+
B. RADIUS
C. AAA
D. IPSec
E. PPP
Answer: A
Explanation: TACACS+ offers multiprotocol support. RADIUS does not support the following protocols: -AppleTalk Remote Access (ARA) protocol -NetBIOS Frame Protocol Control protocol -Novell Asynchronous Services Interface (NASI) -X.25 PAD connection

---

QUESTION .47 What is the new access-list enhancement available in version 6.2 of the PIX OS ?
A. TurboACL
B. SuperACL
C. Extended ACL
D. Reflexive ACL
E. EACL+
Answer: A
Explanation: Turbo Access Control List-A feature introduced with PIX Firewall version 6.2 that improves the performance of large ACLs.

QUESTION .48 If you have authentication through RADIUS configured and configure the following command, what AV-Pair must you also configure on the RADIUS server for the user to go directly into enable mode?
aaa authorization exec default group radius local
A. shell:priv-lvl=15
B. shell:priv:lvl=7
C. shell:priv:lvl=15
D. shell-priv-lvl=7
Answer: A
Explanation: shell:priv-lvl=15 User will be in enable mode after login (show privilege will be 15).

QUESTION .49 What features are available on PIX firewalls to enhance security? (Select all that apply)
A. Unicast Reverse Path Forwarding
B. Flood Guard
C. Flood Defender
D. Flood Fender
E. FragGuard and Virtual Re-Assembly
F. URL Filtering
Answer: A, B, C, E, F
Explanation: No such thing in the PIX as Flood Fender

QUESTION .50 Which of these are considered IGP's ? (Select all that apply)
A. BGP
B. OSPF
C. RIP
D. EIGRP
Answer: B, C, D
Explanation: BGP is a EGP

QUESTION .51 Concerning about Cisco IOS features, what does PAM do?
A. Non-stick cooking spray.
B. Allows you to customize TCP or UDP port numbers.
C. Provides per port security to prevent DoS attacks.
D. Performs application layer security.
E. Encrypts packets to the session level.
Answer: B
Explanation: PAM enables CBAC-supported applications to be run on nonstandard ports

QUESTION .52 An ISDN PRI in North America and Japan has which of the following? (Select all that apply)
A. 1 D
B. 23 B
C. 1 D
D. 30 B
E. 23 D
F. 2 B
Answer: A, B
Explanation: PRI (Primary Rate Interface): A larger aggregate than a BRI, a PRI will consist of 24 channels (T1) or 31 channel's (E1). In either case one channel is reserved for call signaling. For T1s, the D-channel is the 24th channel while the E1s use the 16th channel for signaling.

QUESTION .53 Your router sends a frame-relay frame to your frame-relay provider. The frame-relay switch sees that the port or DLCI that your frame is going to is congested. The frame-relay switch sends a frame back to your router to notify your router of the congestion ahead (of it) in the network. What is marked in this frame-relay frame sent to your router?
A. FECN
B. BECN
C. DE
D. PVC
E. DLCI
Answer: B
Explanation: backward explicit congestion notification. Bit set by a Frame Relay network in frames traveling in the opposite direction of frames encountering a congested path. DTE receiving frames with the BECN bit set can request that higher-level protocols take flow control action as
appropriate. Compare with FE.

QUESTION .54 Which of these commands will control smurf attacks? Choose the best answer.
A. no ip directed-broadcasts

B. ip verify
C. ip rpf verify
D. ip inspect
E. no ip subnet-zero
Answer: A
Explanation: A smurf reflector has more options than the ultimate target of a smurf attack. If a reflector chooses to shut down the attack, appropriate use of no ip directed-broadcast (or equivalent

---

QUESTION .55 What if the TACACS+ server is unavailable and you have the following command configured?(Select all that apply)
tacacs-server last-resort succeed
A. The router will wait for the TACACS+ server to come up before allowing the request.
B. The router will request the enable password before the access-request is granted.
C. The router will be allowed to login with no password.
D. This command does not exist.
E. The user will be denied access.
Answer: A, C
Explanation: To cause the network access server to request the privileged password as verification, or to allow successful login without further input from the user, use the tacacs-server last resort global configuration command. Use the no form of this command to deny requests when the server does not respond. Password-- Allows the user to access the EXEC command mode by entering the password set by the enable command. Succeed-- Allows the user to access the EXEC command mode without further question.

QUESTION .56 Which protocol uses the diffusing update algorithm?
A. IGRP
B. EIGRP
C. BGP
D. OSPF
E. RIP
F. IRDP
Answer: B
Explanation: The Diffusing Update Algorithm (DUAL) is the algorithm used to obtain loop freedom at every instant throughout a route computation. This allows all routers involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in the recomputation.

QUESTION .57 What are the default interfaces on a two interface PIX firewall and what are their security levels?
A. outside (0) and inside (100)
B. outside (0) and inside (255)
C. e0 (0) and e1 (100)
D. outside (1000) and inside (0)
E. e0 (0) and e1 (255)
Answer: A
Explanation: The PIX Firewall default configuration supplies name if commands for the inside and outside interfaces. Use the show name if command to view these commands. They will appearas: nameif ethernet0 outside security0 name if ethernet1 inside security100

QUESTION .58 What is the administrative distance of EIGRP?
A. 90
B. 100
C. 120
D. 1
E. 0
F. 110
Answer: A
Explanation: Internal EIGRP 90
IGRP 100 OSPF 110 Intermediate System-to-Intermediate System (IS-IS) 115 Routing Information Protocol (RIP) 120

QUESTION .59 What are the six AAA Accounting types? (Select all that apply)
A. Network
B. Connection
C. EXEC
D. System
E. Command
F. Resource
Answer: A, B, C, D, E, F
Explanation: AAA supports six different accounting types: Network Accounting Connection Accounting EXEC Accounting System Accounting Command Accounting Resource Accounting

QUESTION .60 When applied with the "ip access-group 2000 in" command, on an interface, what traffic does the following access-list block (select the best answer)?
access-list 2000 remark deny IPX any
A. None
B. Any IP traffic.
C. Invalid access-list.
D. All IPX traffic.
Answer: B
Explanation: 2000-2699 IP extended access list (expanded range) remark Access list entry comment R1(config)#access-list 2000 deny IPX any ^ Invalid input detected at '^' marker. R1(config)#access-list 2000 deny ip any I don’t agree with the question/answer here is it is not a supported command. The question has IPX and you cant insert it in the 2000 range as it is an IP access-list range. I think the question should have been "access-list 2000 remark deny IP any" If it were to have been about IPX then it would have been a different range (900-999 IPX extended access list) Depending on how it is shown on real test the answer could be B if the X is dropped to be just IP (not IPX)

QUESTION .61 An OSPF router that connects two areas is known as the what?
A. ABR
B. ASBR
C. NSSA
D. stub
E. ABRS

F. ARB
Answer: A
Explanation: area border router. Router located on the border of one or more OSPF areas that connects those areas to the backbone network. ABRs are considered members of both the OSPF backbone and the attached areas. They therefore maintain routing tables describing both the backbone
topology and the topology of the other areas

QUESTION .62 ISDN routers in the United States provide which interface?
A. U
B. R
C. S
D. T
E. NT2
Answer: A
Explanation:

QUESTION .63 What does split horizon do?
A. Keeps the router from sending routes out the same interface they came in .
B. Sends a "route delete" back down the same interface that the route came in .
C. Ignores routing updates.
D. Waits for the next update to come in before declaring the route unreachable.
Answer: A the gateway from which they were learned. The "simple split horizon" scheme omits routes learned from one neighbor in updates sent to that neighbor. "Split horizon with poisoned reverse" includes such routes in updates, but sets their metrics to infinity.
Explanation: "Split horizon" is a scheme for avoiding problems caused by including routes in updates sent to

---

QUESTION .64 What port number is HTTP over SSL?
A. 443
B. 80
C. 993
D. 3269
Answer: A
Explanation: If a web browser is not explicitly configured for a proxy, then the browser will initiate an Content Engine.

QUESTION .65 What port number does LDAP use?
A. 389
B. 3389
C. 398
D. 1812
E. 53
F. 79
Answer: A
Explanation: LDAP port 389

QUESTION .66 BGP runs over what protocol & port? (Select all that apply)
A. TCP
B. UDP
C. PVC
D. port 178
E. port 179
F. port 53
Answer: A, E
Explanation: Since BGP uses unicast TCP packets on port 179 to communicate with its peers, we can configure a PIX 1 and PIX 2 to allow unicast traffic on TCP port 179 between Routers 11and 12 and Routers 21 and 22.

QUESTION .67 What is the Kerberos KDC command to add new users to the KDC database?
A. ank
B. ark
C. ack
D. add new key
E. Kerberos add key
F. ip Kerberos ank
Answer: A
Explanation: Use the ank (add new key) command to add a user to the KDC. This command prompts for a password, which the user must enter to authenticate to the router. ank username@REALMUse the ank command to add a privileged instance of a user. ank username/instance@REALM

QUESTION .68 Your router will receive two routes to the same destination. Which route will it place in your routing table, the RIP route or the EIGRP route?
A. RIP
B. EIGRP
C. Both
D. Neither
Answer: B
Explanation: Lower Administrative Distance for Eigrp Internal EIGRP 90 Routing Information Protocol (RIP) 120

QUESTION .69 What would you do to prevent your routing tables being poisoned by rogue routing updates from another network?
A. Use routing protocol authentication.
B. Use ssh.
C. Encrypt your data.
D. AAA
Answer: A
Explanation: All routing protocols should be configured with the corresponding authentication. This prevents attackers from spoofing a peer router and introducing bogus routing information.

QUESTION .70 Exhibit:
r1#sh line Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int
0 CTY - - - - - 0 0 0/0 -

```
65 AUX 9600/9600- - - - - 0 0 0/0 -
66 VTY - - - - - 5 0 0/0 -
67 VTY - - - - - 0 0 0/0 -
68 VTY - - - - - 0 0 0/0 -
69 VTY - - - - - 0 0 0/0 -
70 VTY - - - - - 0 0 0/0 -
```

Line (s) nor in async made - or with no hardware support :1-64r1#You want to restrict access to vty's such that only IP 1.1.1.1 can connect to them. Look at the attached exhibit.

What configuration do you apply to do this?

A. access-list 1 permit 1.1.1.1 line vty 0 4access-class 1 in

B. You cannot do this.

C. access-list 1 permit 1.1.1.1 0.0.0.0line vty 66 70access-class 1 in

D. access-list 1 permit 1.1.1.1 255.255.255.255line vty 0 4access-class 1 in

Answer: A

Explanation: Look at the exhibit and notice that the vty lines start at 66 and go through

---

QUESTION .71 Due to Perfect Forward Secrecy (PFS), if one key is compromised so are subsequent as each key is derived from the previous. (True or False)

A. False

B. True

Answer: A

Explanation: During negotiation, this command causes IPSec to request PFS when requesting new security associations for the crypto map entry. PFS adds another level of security because if one key is ever cracked by an attacker then only the data sent with that key will be compromised. Without PFS, data sent with other keys could also be compromised. With PFS, every time a new security association is negotiated, a new Diffie-Hellman exchange occurs. This exchange requires additional processing time

---

QUESTION .72 Which routing protocols support MD5 authentication? (Select all that apply)

A. BGP

B. OSPF

C. RIPV2

D. EIGRP

E. IGRP

F. IS-IS

Answer: A, B, C, D

Explanation: VERY TRICKY QUESTION !!!! IN CODE 12.1 ISIS is NOT SUPPORTED. IN CODE 12.2T IT IS SUPPORTED MD5 authentication works similarly to plain text authentication, except that the key is never sent over the wire. Instead, the router uses the MD5
algorithm to produce a "message digest" of the key (also called a "hash"). The message digest is then sent instead of the key itself. This ensures that nobody can eavesdrop on the line and learn keys during transmission. These protocols use MD5 authentication: OSPF, RIP version 2, BGP, IP Enhanced IGRPCISCO IOS RELEASE 12.2 T---The IS-IS HMAC-MD5 authentication feature adds an HMAC-MD5digest to each Intermediate System-to-Intermediate System (IS-IS) protocol data unit (PDU). The digest allows authentication at the IS-IS routing protocol level, which prevents unauthorized routing message from being injected into the network routing domain. IS-IS clear text (plain text) authentication is enhanced so that passwords are encrypted when the software configuration is displayed and passwords are easier to manage and change.

QUESTION .73 Which security server feature will allow you to "customize TCP or UDP port numbers for network services"?
A. PAM
B. Asec
C. Bbal
D. auth-proxy
E. ACL
F. CBAC
Answer: A
Explanation: PAM enables CBAC-supported applications to be run on nonstandard ports

QUESTION .74 Routers, instead of bridges, are used to limit network traffic by dropping what?
A. broadcasts
B. BPDU
C. Novell services
D. chatter
Answer: A
Explanation: Routers are layer 3 and Bridges are layer 2. Layer 3 defines broadcast domains.

QUESTION .75 Your OSPF adjacency won't come up. You run the "show ip ospf neighbor" command and are returned to the command prompt. What are some of the possible causes? (Select all that apply)
A. The IGRP process is not properly configured.
B. Access-list preventing hellos.
C. Ospf is configured as passive.
D. Different OSPF area types (like stub or NSSA).
E. You are trying to form an adjacency over a secondary network.
F. ICMP is being denied.
Answer: B, C, D, E
Explanation: IGRP has nothing to do with OSPF interfaces. Access-lists cannot block the multicast addresses that are needed OSPF passive interface with listened but not actively be apart of Difference area types can cause adjacencies not to form ICMP has nothing to do with it as well

QUESTION .76 What is the administrative distance of RIP Version 2?
A. 90
B. 120
C. 100
D. 20
E. 170
F. 200
Answer: B
Explanation: Internal EIGRP 90 IGRP 100 OSPF 110 Intermediate System-to-Intermediate System (IS-IS) 115 Routing Information Protocol (RIP) 120

QUESTION .77 What port number does RADIUS use?
A. 1812

B. 1645
C. 1813
D. 110
E. 25
F. 1821
Answer: A
Explanation: Default Setting of RADIUS server on UDP authentication port 1812. radius server host command The default port for accounting requests is 1646. The default port for authentication requests is 1645 [UG_ACCT], port Proxy accepts accounting messages from the universal gateway at this port. 1813 Post Office Protocol (POP) 3 (port 110) port 25 (SMTP)

QUESTION .78 The Cisco Secure IDS provides protection for which of the following? (Select all that apply)
A. Unauthorized network access
B. Worms
D. Virus signatures
E. Spam
F. Bandwidth over utilization
Answer: A, B, C
Explanation:

QUESTION .79 What ports does TACACS+ use?
A. 49
B. 1812
C. 490
D. 940
E. 53
F. 149
Answer: A
Explanation: The TACACS+ (TCP port 49, not XTACACS UDP port 49) DNS (53)

QUESTION .80 What is the command that was run, resulting in the output in the attached exhibit?
A. crypto key generate rsa usage-keys
B. crypto key generate rsa
C. show crypto key mypubkey rsa
D. crypto isakmp identity address
E. show key generate rsa
Answer: C
Explanation: To check VeriSign CA enrollment, study the commands below. These commands show the public keys you are using for RSA encryption and signatures. dt1-45a#show crypto key mypubkey rsa % Key pair was generated at: 11:31:59 PDT Apr 9 1998 Key name: dt1-45a.cisco.com Usage: Signature Key Key Data:305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C1185439A9C75C 4E34C987 B4D7F36C A058D697 13172767 192166E1 661483DD0FDB907B F9C10B7ACB5A034F A41DF385 23BEB6A7 C14344BE E6915A12 1C86374F 83020301 0001 % Key pair was generated at: 11:32:02 PDT Apr 9 1998 Key name: dt1-45a.cisco.com Usage: Encryption Key Key Data:305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DCF5AC 360DD5A6

C69704CF47B2362D 65123BD4 424B6FF6 AD10C33E 89983D08 16F1EA58 3700BCF91EF17E71 5931A9FC 18D60D9A E0852DDD 3F25369C F09DFB75 05020301 0001

QUESTION .81 What is the PIX features that eliminates the need for a mail relay (or bastion host) outside the firewall?
A. Mail Guard
B. Right Guard
C. Guard Mail
D. SMTP Guard
E. Flood Guard
F. Frag Guard
Answer: A
Explanation: The Mail Guard feature provides safe access for Simple Mail Transfer Protocol(SMTP) connections from the outside to an inside messaging server. This feature allows a single mail server to be deployed within the internal network without it being exposed to known security problems with some SMTP server implementations. Avoids the need for an external mail relay (or bastion host)system. Mail Guard enforces a safe minimal set of SMTP commands to avoid an SMTP server system from being compromised. This feature also logs all SMTP connections.

QUESTION .82 Configuration: aaa new-model aaa authentication login default local enable password Cisco username backup privilege 7 password 0 backup username root privilege 15 password 0 router privilege exec level 7 ping What can the "backup" user do when he/she logs into the router with the attached configuration? (Select all that apply)
A. ping
B. sh run
C. wrt
D. sh ver
E. sh ip int brie
Answer: A, D, E
Explanation: Not sure about this answer as "privilege exec level 7 ping" is the only one listed here. Be sure to look for more exec level 7 commands.

QUESTION .83 What type of access-list is used to catch new TCP or UDP sessions, initiating from your inside network to your outside network, then dynamically create filters to allow those back in?
A. access-lists with the "established" keyword
B. reflexive access-lists
C. lock-any-key
D. dynamic access-lists
Answer: B
Explanation: Reflexive access lists are similar in many ways to other access lists. Reflexive access lists contain condition statements (entries) that define criteria for permitting IP packets. These entries are evaluated in order, and when a match occurs, no more entries are evaluated. However, reflexive access lists have significant differences from other types of access lists. Reflexive access lists contain only temporary entries; these entries are automatically created when a new IP session begins (for example, with an outbound packet), and the entries are removed when the session ends. Reflexive access lists are not themselves applied directly to an interface,

but are "nested" within an extended named IP access list that is applied to the interface. (For more information about this, see the section "Reflexive Access Lists Configuration Task List" later in this chapter

---

QUESTION .84 What is "infinity" in RIP V1 ?
A. 16
B. 255
C. infinity = infinity, forever
D. 12
E. 15
F. 65536
Answer: A
Explanation: Neighbor updates of the routes with a metric of 16 (infinity) mean the route is unreachable, and those routes are eventually removed from the routing table.

QUESTION .85 RADIUS encrypts what part of the packet?
A. username
B. password
C. entire packet
D. none
Answer: B
Explanation: RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, could be captured by a third party.

QUESTION .86 How many privilege levels are available to be assigned?
A. 16
B. 15
C. 7
D. 255
E. 16384
F. 64
Answer: A
Explanation: Below shows that 0 - 15 (=16 privilege levels) To understand this example, it is necessary to understand privilege levels. By default, there are three command levels on the router. privilege level 0 - includes the disable, enable, exit, help, and logout commands privilege level 1 -normal level on Telnet; includes all user-level commands at the router> prompt privilege level 15 -includes all enable-level commands at the router# prompt

---

QUESTION .87 You configure the OSPF routing process and networks that it will run on. You have non-broadcast frame-relay interfaces. What important OSPF command must you use to get the OSPF up?
A. neighbor
B. ip ospf network broadcast
C. ip ospf network point-to-multipoint
D. area X stub
E. nssa
F. network

Answer: A

Explanation: The reason that NEIGHBOR is correct is that the question as you to configure OSPF routing process and networks [you are in the router(config-router)#] There are two ways to simulate a broadcast model on an NBMA network: define the network type as broadcast with the ip ospf network broadcast interface sub-command or configure the neighbor statements using the router ospf command.

QUESTION .88 What does the following command do?

aaa authentication PPP MIS-access group tacacs+ none

A. Tells the router to not authenticate if the user has already been authenticated via tacacs+.

B. Tells the router to use RADIUS authentication for PPP if the local authentication fails.

C. Tells the router to use local authentication for PPP.

D. Tells the router to not authenticate if the user has already been authenticated via tacacs+ and deny access.

Answer: A

QUESTION .89 What command enables AAA?

A. aaa new-model

B. ip aaa enable

C. enable aaa

D. it is enabled by default

Answer: A

Explanation: To enable the AAA access control model, use the aaa new-model global configuration command.

QUESTION .90 How do reflexive access-lists determine when a UDP connection has ended? (Select all that apply)

A. When no packets of that session have passed after a timeout period, the session is considered as ended and, then, terminated.

B. When the configured timeout has ended.

C. 5 seconds after two FIN bits have passed.

D. When the RST bit has passed.

Answer: A, B

Explanation: Because it is multiple choice these are the correct answers. Because FIN and RST are TCP Temporary reflexive access list entries are removed at the end of the session. For TCP sessions, the entry is removed 5 seconds after two set FIN bits are detected, or immediately after matching a TCP packet with the RST bit set. (Two set FIN bits in a session indicate that the session is about to end; the 5-second window allows the session to close gracefully. A set RST bit indicates an abrupt session close.) Or, the temporary entry is removed after no packets of the session have been detected for a configurable length of time (the timeout period). For UDP and other protocols, the end of the session is determined differently than for TCP. Because other protocols are considered to be connectionless (session less) services, there is no session tracking information embedded in packets. Therefore, the end of a session is considered to be when no packets of the session have been detected for a configurable length of time (the timeout period).

QUESTION .91 The locally-significant value that identifies the virtual connection between the frame-relay switch and the frame-relay router is called what?

A. DLCI

B. PVC

C. FECN
D. BECN
E. DE
F. DTE
Answer: A
Explanation: data-link connection identifier. Value that specifies a PVC or an SVC in a Frame Relay network. In the basic Frame Relay specification, DLCIs are locally significant (connected devices might use different values to specify the same connection). In the LMI extended specification,
DLCIs are globally significant (DLCIs specify individual end devices).

QUESTION .92 Which of these should be addressed to have a well designed security policy?
A. Know your enemy.
B. Identify assumptions.
C. Control secret.
D. Know your weaknesses.
E. Understand your environment.
F. All of these.
Answer: F
Explanation:

QUESTION .93 Configuration: aaa new-model aaa authentication login default radius local aaa authorization exec default radius enable password Cisco radius-server 1.1.1.1 radius-server key password username root privilege 15 password 0routerline con 0 login authentication default Look at the attached configuration. If the RADIUS server is unavailable, what will happen when the root user tries to login?
A. He will be authenticated locally.
B. Login will succeed through RADIUS.
C. Login will fail.
D. Router will crash.
Answer: C
Explanation: Tricky question! It asks if the radius server FAILS. Then login fails. If it errors then it looks at local. The aaa authentication login default radius local command specifies that the username and password are verified by RADIUS or, if RADIUS returns an error, by the router's local
user database.

QUESTION .94 In STP, which switch is the root?
A. With the lowest priority.
B. The largest BPDU.
C. The ASBR.
D. The ABR.
E. The DR switch.
Answer: A
Explanation: Note: Even if the administrator sets the root bridge priority to zero in an effort to secure the root bridge position, there is still no guarantee, as there might be a bridge with priority zero and a lower bridge ID.

QUESTION .95 What is the primary features used to protect your network from SYN-Flood attacks?
A. tcp intercept

B. reflexive access-lists
C. dynamic access-lists
D. ip verify
Answer: A
Explanation: The TCP intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks, which are a type of denial-of-service attack. SYN flood attacks are usually noticed because the target host (frequently an HTTP or SMTP server) becomes extremely slow, crashes, or hangs. It's also possible for the traffic returned from the target host to cause trouble on routers; because this return traffic goes to the randomized source addresses of the original packets, it lacks the locality properties of "real" IP traffic, and may overflow route caches. On Cisco routers, this problem often manifests itself in the router running out of memory.

QUESTION .96 What product allows network administrators to apply per-user security policies?
A. auth proxy
B. ip verify
C. lock-and-key
D. ip rpf
E. ios firewall
F. username/password
Answer: A
Explanation: Authentication proxy (auth-proxy), available in Cisco IOS(r) Software Firewall version 12.0.5.T and later, is used to authenticate inbound or outbound users, or both. These users would normally be blocked by an access list, but with auth-proxy the users bring up a browser to go through the firewall and authenticate on a Terminal Access Controller Access Control System Plus (TACACS+)or RADIUS server.

QUESTION .97 Which are recommended steps to developing effective security policies? (Select all that apply)
A. Identify your network assets to protect.
B. Determine points of risk.
C. Remember physical security.
D. Make assumptions.
E. Keep policy to network security only.
Answer: A, B, C
Explanation: In Security policy you don't make assumptions. Security policy cover a huge range of topics from acceptable use to applications.

QUESTION .98 Command output: router1#sh ip inspect config Session audit trail is disabled one-minute (sampling period) thresholds are
[400:500]connections max-incomplete sessions thresholds are [400:500]max-incomplete tcp connections per host is 50.Block-time 0 minute. tcp syn wait-time is 30 sec -- tcp fin wait-time is 5 sectcp idle-time is3600 sec -- udp idle-time is 30 secdns-timeout is 5 sec Inspection Rule Configuration Inspection namely site ftp timeout 3600smtp timeout 3600tcp timeout 3600Look at the attached command output. What protocols is CBAC currently configured to inspect? (Select all that apply)
A. ftp
B. vdolive
C. smtp
D. udp

E. sqlnet
F. all protocols
Answer: A, C
Explanation: ftp timeout 3600, smtp timeout 3600 tell what CBAC is inspecting.

QUESTION .99 What are the two "modes" of tcp intercept? (Select all that apply)
A. watch
B. intercept
C. aggressive
D. open
E. connect
F. monitor
Answer: A, B
Explanation: The TCP intercept can operate in either active intercept mode or passive watch mode. The default is intercept mode.

QUESTION .**100** What IP address class is the address 223.255.253.1 located in?
A. A
B. B
C. C
D. D
E. E
F. F
Answer: C
Explanation:

QUESTION .101 To encrypt passwords stored on your Cisco router, what command must you run?
A. service password-encryption
B. service encryption-password
C. password-encryption
D. encrypt service-passwords
E. password hash
F. no service password-clear text
Answer: A
Explanation: To encrypt passwords, use the service password-encryption global configuration command. Use the no form of this command to disable this service.

QUESTION .102 What is the skinny protocol?
A. SCCP
B. SSCP
C. SIP
D. H.323
E. RTSP
Answer: A
Explanation: SKINNY-Skinny Client Control Protocol.

QUESTION .103 What command, or commands, will disable connections to the echo and discard ports?
A. no service tcp-small-servers
B. no ip tcp-small-servers
C. access-list 101 deny ip any eq echo access-list 101 deny ip any eq discard int lo0access-group 101 in
D. no service tcp-small-services
Answer: A
Explanation: To access minor TCP/IP services available from hosts on the network, use the service tcp-small-servers global configuration command. Use the no form of the command to disable these services.

QUESTION .104 What could connect two VLANs together? (Select all that apply)
A. 802.1q
B. ISL
C. trunking
D. VTP
E. DLS
F. RSRB
Answer: A, B, C
Explanation:

QUESTION .105 Which of the following commands would be used in configuring pptp access through a router from a PC? (Select all that apply)
A. vpdn enable
B. protocol pptp
C. no ip http server
D. no ip directed-broadcasts
E. pptp enable
F. protocol vpdn
Answer: A, B
Explanation: To enable virtual private dialup networking on the router and inform the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present, use the vpdn enable global configuration command.

QUESTION .106 What two commands, used together, on a PIX would configure inbound connections. (Choose two)
A. static
B. inbound
C. nat
D. global
E. passwd
Answer: A, B
Explanation: The Answer in this question is wrong. They stated that it is static and inbound. Inbound is not a command in PIX OS 6.2 However, I don't see a conduit command or access list command. SO TAKE YOUR BEST GUESS I THINK IT MAY BE STATIC AND NAT Set
password for Telnet access to the PIX Firewall console. (Privileged mode.) Create or delete entries from a pool of global addresses If the external network is connected to the Internet, each global IP address must be registered with the Network Information Center (NIC). Associate a network with a pool of global IP addresses

The nat command lets you enable or disable address translation for one or more internal addresses. Address translation means that when a host starts an outbound connection, the IP addresses in the internal network are translated into global addresses. Network Address Translation (NAT) allows your network to have any IP addressing scheme and the PIX Firewall protects these addresses from visibility on the external network. When an inbound packet arrives at an external interface such as the outside interface, it first passes the PIX Firewall Adaptive Security criteria. If the packet passes the security tests, the PIX Firewall removes the destination IP address, and the internal IP
address is inserted in its place. The packet is forwarded to the protected interface. In the CSPFA course book it does state that DYNAMIC translations use global and Nat but it is used for INSIDE to OUTSIDE "Dynamic Translations are used for local hosts and their outbound connections"

QUESTION .107 How can you tell what hosts are on your local network?
A. The IP address of your host.
B. The subnet mask of your host.
C. The remote router's IP address.
D. Your hub's IP address.
Answer: B
Explanation:

QUESTION .108 Which of these are a path vector routing protocol?
A. BGP
B. OSPF
C. RIP
D. EIGRP
E. RIPV2
F. IGRP
Answer: A
Explanation: BGP is classified as a path vector routing protocol by RFC 1322 The Border Gateway Protocol (BGP) (see [BGP91]) and the Inter Domain Routing Protocol (IDRP) (see [IDRP91])are examples of path vector (PV) protocols [Footnote: BGP is an inter-autonomous system routing
protocol for TCP/IP internets. IDRP is an OSI inter-domain routing protocol that is being progressed toward standardization within ISO.

QUESTION .109 Which are valid AAA authentication login methods? (Select all that apply)
A. enable
B. krb5
C. krb5-telnet
D. line
E. local-case
F. none
Answer: A, B, C, D, E, F
Explanation:

QUESTION .110 By default, what is a peer router's ISAKMP identity?
A. hostname
B. IP Address

C. pubkey
D. keystring
E. MAC Address
Answer: B
Explanation: To define the identity the router uses when participating in the IKE protocol, use the crypto isakmp identity global configuration command. Set an ISAKMP identity whenever you specify pre-shared keys. Address ets the ISAKMP identity to the IP address of the
interface that is used to communicate to the remote peer during IKE negotiations. Hostname sets the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.domain.com).

QUESTION .111 Type the command that you would enter on a vty line to enable lock-and-key
Answer: access-enable
Explanation: To enable the router to create a temporary access list entry in a dynamic access list, use the access-enable EXEC command. Use the auto command command with the access-enable command to cause the access-enable command to execute when a user opens a Telnet session into the router.

QUESTION .112 Which of these best describes PDM?
A. Lets you manage your PIX firewalls and their configurations.
B. Lets you manage your IPSec configuration.
C. Provides a certification authority.
D. Delivers geographical load balancing based on network topology and traffic patterns.
E. Enable service providers to lay the foundation for delivering differentiated New World services.
F. Cisco router configuration.
Answer: A
Explanation: PIX device manager

QUESTION .113 Your OSPF neighbors are not forming adjacencies. What might be the problem? (Select all that apply)
A. Network type mismatch.
B. Hello mismatch.
C. Dead mismatch.
D. ABR ASBR mismatch.
Answer: A, B, C

QUESTION .114 You do an "enable 0" and press enter. What commands can you now perform? (Select all that apply)
A. disable
B. enable
C. help
D. sh ver
E. logout
F. None, as you are at level ZERO.
Answer: A, B, C, E
Explanation: privilege level 0 - includes the disable, enable, exit, help, and logout commands privilege level 1 - normal level on Telnet; includes all user-level commands at the router>prompt privilege level 15 - includes all enable-level commands at the router# prompt

QUESTION .115 Your RADIUS server is at IP address 172.22.53.201and 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 1645 acct-port 1646 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 1645 acct-port 1646 key Cisco
Answer: B, C
Explanation:

QUESTION .116 Which of the following will help to prevent network data interception? (Select all that apply)
A. Data Confidentiality
B. Data Integrity
C. Data Origin Authentication
D. Anti-Replay
E. Accounting
Answer: A, B, C, D
Explanation: Accounting wont prevent data interception

QUESTION .117 Which of the following commands configured CAR?
A. ip car
B. rate-limit
C. ip rate-limit
D. car rate-limit
E. ip traffic-limit car
Answer: B
Explanation: To configure committed access rate (CAR) and distributed CAR (DCAR) policies, use the rate-limit interface configuration command

QUESTION .118 To what address are OSPF hellos sent?
A. 224.0.0.5
B. 224.0.0.6
C. 192.168.0.5
D. 10.1.1.1
E. 225.1.1.5
F. 224.0.0.2
Answer: A
Explanation: Open Shortest Path First (OSPF) uses the IP addresses 224.0.0.5 and 224.0.0.6 to exchange link-state information

QUESTION .119 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 vendorID 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
E. None, this is enabled by default.
F. All of the above.
Answer: A, B, C
Explanation: To configure the network access server to recognize and use vendor specific attributes, use the radius-server vsa send global configuration command. accounting (Optional)Limits the set of recognized vendor-specific attributes to only accounting attributes. authentication(Optional) Limits the set of recognized vendor-specific attributes to only authentication attributes.

QUESTION .120 At what point between two hosts, connected via the Internet, would a hacker have to be at to perform a "man in the middle" attack?
A. On your network.
B. On the remote network.
C. On your host.
D. On the remote host.
E. At some intermediate network between your host and the remote host.
Answer: E

QUESTION .121 You want to have the denials to your access-list sent to the router's log. What two commands do you need? (Select all that apply)
A. log buff 4096
B. access-list 101 deny any log-input
C. logging monitor
D. terminal monitor
E. logging trap
F. aaa accounting
Answer: A, B
Explanation: logging buffered To log messages to an internal buffer, use the logging buffered global configuration command. The no logging buffered command cancels the use of the buffer and writes messages to the console terminal, which is the default. States what traffic is going to the
buffer

QUESTION .122 In dialup technologies, interesting traffic will do which of the following? (Select all that apply)
A. Reset the idle timer to zero.
B. Trigger a call.
C. Increase the idle timer.
D. Disconnect a call.
Answer: A, B
Explanation: This Answer is correct. Dialup traffic is interesting it brings up the line and resets the idle timer.

QUESTION .123 What is a AAA POD?
A. Packet of Disconnect
B. Point of Disconnection
C. Place of Destruction

D. Packet of Determination
Answer: A
Explanation: To enable inbound user sessions to be disconnected when specific session attributes are presented, use the aaa pod server command in global configuration mode.

QUESTION .124 Will CBAC's tcp inspection enable support for FTP?
A. Yes, CBAC's tcp inspect support FTP and most other applications.
B. No, tcp inspect does not support FTP as FTP uses multiple channels to support data transmission between client and host.
C. No, tcp inspect does not support FTP as FTP uses IPSec and IPSec is not supported via the Cisco A. IOS firewall.
D. Yes, this is enabled by default.
Answer: A
Explanation: CBAC also has the ability to handle multiple channels and dynamic ports that are dynamically created when using multimedia applications and other protocols such as FTP, RPC, and SQLNet." Cisco Certified Internet work Expert Security Exam v1.7 by John J. Kaberna pg

---

QUESTION .125 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
Explanation: Remote Authentication Dial-In User Services and A distributed client/server system that secures networks against unauthorized access are correct answers

---

QUESTION .126 RADIUS uses what as its transport protocol?
A. UDP
B. TCP
C. ARP
D. IPSec
E. IPX
F. SSH
Answer: A

QUESTION .127 If you had to choose one command in global-config mode to disable CDP on interface e0/0, which would it be? Choose the best answer.
A. no cdp run
B. no cdp enable
C. no cdp
D. no ip cdp
Answer: A
Explanation: VERY TRICKY! Notice it says global config (router-config)# not (routerconfig-if)# normally you would use the cdp enable/no cdp enable to control interface cdp but the question calls for a global command. The normal global command is cdp run cdp run --To enable Cisco

Discovery Protocol (CDP), use the cdp run global configuration command. To disable CDP, use the no form of this command. cdp enable -- To enable Cisco Discovery Protocol (CDP) on an interface, use the cdp enable interface configuration command. To disable CDP on an interface, use the no form of this command.

QUESTION .128 If you run the "show ip ospf neighbor" command, which of the following are a possible output?
A. init
B. exstart/exchange
D. loading
E. nothing at all
F. all of the above
Answer: F
Explanation:

QUESTION .129 The Cisco IOS supports which versions of SSH?
A. 1
B. 2
C. 3
D. 4
Answer: A
Explanation: Secure Shell (SSH) is a protocol that provides a secure, remote connection to a router. There are currently two versions of SSH available, SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS software.

QUESTION .130 What is the STP cost for a 10Mb Ethernet link?
A. 1
B. 10
C. 100
D. 1000
E. 64
F. 250
Answer: C
Explanation:

QUESTION .131 Which of the following are valid av-pairs on a RADIUS server?
A. rte-fltr-out#0="router igrp 60"
B. user = georgia {login = clear text lab service = PPP protocol = ip {}}
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 .132 What bits must a class D IP address always begin with?
A. 10
B. 100
C. 110
D. 1110

E. 1111
F. 101
Answer: D
Explanation: Class D must always start with 1110 C 110 B 100 A 10 Binary Notation Decimal Notation
xxxx xxxx. 0000 0000.0000 0000.0000 0000/10 ------> X.0.0.0/10
xxxx xxxx. 0100 0000.0000 0000.0000 0000/10 ------> X.64.0.0/10
xxxx xxxx. 1000 0000.0000 0000.0000 0000/10 ------> X.128.0.0/10
xxxx xxxx. 1100 0000.0000 0000.0000 0000/10 ------> X.192.0.0/10

QUESTION .133.OSPF area 12 is not connected to area 0. What do you need to do? (Select all that apply)
A. Nothing, there is no problem with doing this.
B. Configure a virtual link.
C. All areas must be connected to the backbone.
D. Use the area X virtual-link command.
E. Use the default-information originate command.
Answer: B, C, D
Explanation: All areas in an OSPF autonomous system must be physically connected to the backbone area (area 0). In some cases where this is not possible, you can use a virtual link to connect to the backbone through a non-backbone area. As mentioned above, you can also use virtual links to connect two parts of a partitioned backbone through a non-backbone area. The area through which you configure the virtual link, known as a transit area, must have full routing information. The transit area cannot be a stub area. area <area-id> virtual-link <router-id>

QUESTION .134 What is the command to disable IKE?
Answer: no crypto isakmp enable

QUESTION .135 What two commands do you configure, together, on a PIX firewall, to configure outbound NAT translation? (Select all that apply)
A. nat
B. global
C. ip route
D. conduit
E. route inside
Answer: A, B
Explanation: In the CSPFA course book it does state that DYNAMIC translations use global and Nat but it is used for INSIDE to OUTSIDE "Dynamic Translations are used for local hosts and their outbound connections"

QUESTION .136 Which of the following commands would apply a CBAC rule to an interface?
Answer: ip inspect {inspection name} in

QUESTION .137 Cisco recommends configuring a backup authentication method, what is required to configure a backup authentication method?
A. AAA
B. RADIUS
C. TACACS+
D. Local authentication

E. Kerberos
Answer: A Explanation:

QUESTION .138 If you want no more than 4 useable host IP addresses, what subnet mask would you use? (Select all that apply)
A. /30
B. /32
C. /29
D. 255.255.255.248
E. 255.255.255.240
F. 255.255.255.0
Answer: C, D
Explanation: 29 and 255.255.255.248 are the same thing IP Mask Notes
192.27.200.0 255.255.255.248 Subnet Address
192.27.200.1 255.255.255.248
192.27.200.2 255.255.255.248
192.27.200.3 255.255.255.248
192.27.200.4 255.255.255.248
192.27.200.5 255.255.255.248
192.27.200.6 255.255.255.248
192.27.200.7 255.255.255.248 Broadcast Address

QUESTION .139 What command would begin the creation of the highest priority IKE policy?
A. crypto isakmp policy 1
B. crypto isakmp policy 10000
C. crypto ike policy 1
D. crypto ike policy 10000
Answer: A
Explanation: The following example shows two policies with policy 20 as the highest priority, policy 30 as the next priority, and the existing default policy as the lowest priority

---

QUESTION .140 Exhibit:
interface Serial1/0:0.254 point-to-point ip address 10.0.100.1 255.255.255.252no ip proxy-arp access group 155 out no cdp enable frame-relay class 1544Kfrkeepalivefram-relay interface-dlci 45access-list 155 permit ip any 10.254.0.0 0.0.255.255 eq telnet time-range time list time-range time list periodic daily 6:00 to 21:00
Based on the attached exhibit, when would telnet traffic to the 10.253.0.0 network function?
A. It would not function, it is denied.
B. It would always function, it is permitted in the access-list 155.
C. From 6am to 9pm each day.
D. The remote router would deny the telnet.
Answer: A
Explanation: This is a tricky question. Look at the config and the thing that jumps out is the time range. The time range is setup correctly but the access-list is not. "access-list 155 permit ip any10.254.0.0 0.0.255.255 eq telnet time-range" Notice the question asks for 10.253.0.0 network but the
access-list only allows 10.254.0.0

QUESTION .141 Which of the following are associated with SNMP V3 ? (Select all that apply)
A. Integrity
B. MD5 authentication
C. Encryption
D. Clear-text
E. Only security based on community strings and access-lists.
Answer: A, B, C
Explanation: Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are: Message integrity---Ensuring that a packet has not been tampered with in-transit. Authentication---Determining the message is from a valid source. Encryption---Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

QUESTION .142 What are the current commands used to apply access-lists on a PIX firewall?
A. access-list & access-group
B. conduit and outbound
C. access-class and access-group
D. map-list and route-map
Answer: A
Explanation: To maximize security when implementing a Cisco Secure PIX Firewall, it is important to understand how packets are passed from and to higher security interfaces from lower security interfaces by using the nat, global, static, and conduit commands, or access-list and access group commands in PIX software versions 5.0 and later.

QUESTION .143 What layer of the OSI model does ASCII run at?
A. 6
B. 2
C. 3
D. 4
E. 5
F. 7
Answer: A
Explanation: Layer 6: The Presentation Layer The presentation layer ensures that the information that the application layer of one system sends out is readable by the application layer of another system. If necessary, the presentation layer translates between multiple data formats by using a common format. If you want to think of Layer 6 in as few words as possible, think of a common data format.

QUESTION .144 Which of these routing protocols support discontiguous networks? (Select all that apply)
A. OSPF
B. RIP
C. IGRP
D. EIGRP
Answer: A, D
Explanation: RIP and IGRP are classful protocols, thus don’t allow discontiguous networks

QUESTION .145 In order, what ports do the following use- IKE, ESP, and AH
A. 500, 50, 51
B. 50, 51, 52
C. 51, 52, 500
D. 5000, 500, 501
E. 105, 150, 151
Answer: A
Explanation:500 IKE Internet Key Exchange [RFC 2409]50 ESP Encap Security Payload for IPv6 [RFC2406] 51 AH Authentication Header for IPv6 [RFC2402]

QUESTION .146 Which of the following are reflexive access-lists
A. None of these.
B. access-list 101 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 established
C. access-list 101 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 reflect
D. access-list 101 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 dynamic
Answer: A
Explanation: permit protocol any reflect name [timeout seconds] Defines the reflexive access list using the reflexive permit entry. Repeat this step for each IP upper-layer protocol; for example, you can define reflexive filtering for TCP sessions and also for UDP sessions. You can use the same name for multiple protocols. EXAMPLE: permit tcp any reflect tcp traffic Define the reflexive access list tcp traffic. This entry permits all outbound TCP traffic and creates a new access list named tcp traffic. Also, when an outbound TCP packet is the first in a new session, a corresponding temporary entry will be automatically created in the reflexive access list tcp traffic. The "access-list 101 permit tcp 0.0.0.0255.255.255.255 0.0.0.0 255.255.255.255 reflect" is not a complete statement. It needs to call a name and none is given

QUESTION .147 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
E. Both inside and outside addresses.
F. This will not work.
Answer: A

QUESTION .148 What are the four possible responses that the NAS could receive from the TACACS+ server?(Select all that apply)
A. ACCEPT
B. REJECT
C. ERROR
D. CONTINUE
E. DENY
F. FAIL
Answer: A, B, C, D
Explanation: The network access server will eventually receive one of the following responses from the

TACACS+ daemon: ACCEPT--The user is authenticated and service may begin. If the network access server is configured to requite authorization, authorization will begin at this time .REJECT--The user has failed to authenticate. The user may be denied further access, or will be prompted to retry the login sequence depending on the TACACS+ daemon. ERROR--An error occurred at some time during authentication. This can be either at the daemon or in the network connection between the daemon and the network access server. If an ERROR response is received, the network access server will typically try to use an alternative method for authenticating the user. CONTINUE-- The user is prompted for additional authentication information. A FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list. Access-Request---sent by the client (NAS) requesting access Access-Reject---sent by the RADIUS server rejecting access Access-Accept---sent by the RADIUS server allowing access Access-Challenge---sent by the RADIUS
server requesting more information in order to allow access. The NAS, after communicating with the user, responds with another access request.

QUESTION .149 SSH encrypts what, between server and client? (Select all that apply)
A. username/passwords
B. commands
C. Ipsec and IKE
D. IP source and destination addresses
Answer: A,B
Explanation:

QUESTION .150 What dose 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.
E. Denies them.
Answer: A, B
Explanation: Always in operation monitoring return packets to ensure they are valid. Actively randomizes TCP sequence numbers to minimize the risk of TCP sequence number attack. The sequences need to be within a valid range of each other to be allowed through the PIX

QUESTION .151 What is an atomic attack signature?
A. Detects simple patterns.
B. Detects compound patterns.
C. Detects complex patterns.
D. Detects distributed attacks.
Answer: A
Explanation: Atomic signatures (seventy-four): detect simple patterns (i.e.: attempt on a specific host) Compound signatures (twenty-seven): detect complex patterns (i.e.: attack on multiple hosts, over extended

time periods with multiple packets) Info signatures (forty): detect information gathering activities (i.e.: port sweep) Attack signatures (sixty-one): detect malicious activity (i.e.: illegal ftp commands)

QUESTION .152 Switch A has a priority of 8192 while Switch B has a priority of 32768. Which switch will be root & why?
A. Switch A, it has the lowest priority.
B. Switch B, 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
Explanation: Note: Even if the administrator sets the root bridge priority to zero in an effort to secure the root bridge position, there is still no guarantee, as there might be a bridge with priority zero and a lower bridge ID.

QUESTION .153 IKE provides which of the following benefits? (Select all that apply)
A. Allow encryption keys to change during IPSec sessions.
B. Anti-replay.
C. Enables you to specify a lifetime for security associations.
D. Enable you to have certification authority (CA) support.
E. Data integrity.
F. Provides data integrity.
Answer: A, B, C, D
Explanation: Specifically, IKE provides these benefits: Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
Allows you to specify a lifetime for the IPSec security association.
Allows encryption keys to change during IPSec sessions.
Allows IPSec to provide anti-replay services. Permits CA support for a manageable, scalable IPSec implementation.
Allows dynamic authentication of peers

QUESTION .154 According to the Cisco IOS documentation, what four things does CBAC do? (Select all that apply)
A. Traffic filtering.
B. Traffic inspection.
C. Alerts and audit trails.
D. Intrusion detection.
E. None of the above.
Answer: A, B, C, D
Explanation: CBAC intelligently filters TCP and UDP packets CBAC can inspect traffic Real-time alerts and audit trails

---

QUESTION .155 How would you see the default IKE policy?
A. show running
B. wr t
C. show crypto isakmp policy
D. show crypto ike policy
E. wrm

Answer: C
Explanation: To view the parameters for each IKE policy, use the show crypto isakmp policy EXEC command.

QUESTION .156 If you are using certificates, what is required? (Select all that apply)
A. Set a hostname and domain
B. Hostname {router hostname}
ip domain-name {domain name}
C. Configure and enable password.
D. Enable DHCP.
E. Crypto ca certificate query
Answer: A, B

QUESTION .157 What is a limitation of Unicast RPF?
A. Cisco express switching (CES) must be enabled.
B. Multiple access-lists must be configured.
C. A CA is required.
D. Symmetrical routing is required.
Answer: D
Explanation: Internal interfaces are likely to have routing asymmetry, meaning multiple routes to the source of a packet. Unicast RPF should be applied only where there is natural or configured symmetry. Hence, it is not recommended that you apply Unicast RPF where there is a chance of asymmetric routing.

QUESTION .158 RIP is at what OSI layer?
A. 1
B. 2

C. 3
D. 4
E. 5
F. 6
Answer: C
Explanation: Routing, error notification, etc., are considered layer management. There is nothing” above" them; they are part of the infrastructure for a given layer. So, all of them are logically layer 3.The issue of the mechanism they use to transfer information between them is independent of the layer
they manage. In Chuck's table below, EIGRP and OSPF do have transport functions that are part of their own design--which have a TCP-like flavor. For that matter, ISIS runs directly over data link. justice to his words.

QUESTION 159. If you want to use RADIUS authentication, must you configure AAA?
A. No, AAA is for authentication, authorization, and accounting. It is not required to configure
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.
Answer: C

QUESTION .160 How many of the most common attack "signatures" does the Cisco IOS IDS support?
A. 59

B. 256
C. 12
D. 95
Answer: A
Explanation: The Cisco IOS Firewall IDS feature identifies 59 of the most common attacks using "signatures" to detect patterns of misuse in network traffic. The intrusion-detection signatures included in the Cisco IOS Firewall were chosen from a broad cross-section of intrusion-detection signatures. The signatures represent severe breaches of security and the most common network attacks and information-gathering scans.

QUESTION .161 What are the two modes of BGP?
A. classless & classful
B. FLSM & VLSM
C. IBGP & EBGP
D. ABGP & BBGP
E. aggressive & quick mode
F. UDP & TCP
Answer: C

QUESTION .162 Why should you use SNMPV3 ? (Select all that apply)
A. It can use MD5 authenticate communications.
B. It can use DES for encrypting information.
C. It sends passwords in clear-text.
D. It supports ip audit.
E. Its security is based on using public and private as the community strings.
F. It is the most secure of the SNMP versions.
Answer: A, B, F
Explanation: Version 3 auth No Priv MD5 or SHA Provides authentication based on the authentication based on the HMACMD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. SNMPv3 provides for both
security models and security levels Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are: Message integrity---Ensuring that a packet has not been tampered with in-transit. Authentication---Determining the message is from a valid source. Encryption---Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

QUESTION .163 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
E. access-list 101 permit tcp 0.0.0.0 255.255.255.255 B.B.13.100 0.0.0.0 eq 21
Answer: A
Explanation: DNS Port: 53 (TCP, UDP) server.

QUESTION .164 Exhibit:
aaa new-model aaa authentication login default group radius aaa authorization exec default group radius ip http serve rip http authentication aaa radius-server host 171.68.118.101 auth-port 1645 acct-port1646radius-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.
E. The configuration is invalid.
F. The enable password.
Answer: A
Explanation: "aaa authentication login default group radius" states that you will login using the credit als in the RADIUS server.

QUESTION .165 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
E. no PPP eap local
F. no PPP eap proxy
Answer: A
Explanation: To authenticate locally instead of using the RADIUS back-end server, use the PPP eap local command in interface configuration mode. To re enable proxy mode (which is the default),use the no form of this command By default, Extensible Authentication Protocol (EAP) runs in proxy
mode. This means that EAP allows the entire authentication process to be negotiated by the network access server (NAS) to a back-end server that may reside on or be accessed via a RADIUS server. To disable proxy mode (and thus to authenticate locally instead of via RADIUS), use the PPP eap local command. In local mode, the EAP session is authenticated using the MD5 algorithm and obeys the same authentication rules as does Challenge Handshake Authentication Protocol (CHAP).

QUESTION .166 Which of the following security server protocols provides separate facilities for each of the A, A,& A ?
A. RADIUS
B. TACACS+
C. Kerberos
D. ssh
E. IPSec
F. IKE
Answer: B
Explanation:

QUESTION .167 What is the binary equivalent of 172.96.19.133 ?
A. 10101100 01100000 00010011 10000101

B. 10101100 01100000 00010111 10000101
C. 10101100 01100001 00010011 10000101 D. 10101100 01100000 00010011 10000111
Answer: A
Explanation:
128 64 32 16 8 4 2 1 128 64 32 16 8 4 2 1 128 64 32 16 8 4 2 1 128 64 32 16 8 4 2 1 1 0 1 0 1 1 0 0 0 1 1 0 0 0 0 0 0 0 0 1 0 0 1 1 1 0 0 0 0 1 0 1172 9619 133

QUESTION .168 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.
E. Define which IP source addresses, destination addresses, ports, and protocols are to be encrypted.
Answer: A, B, C, D
Explanation: Although there is only one peer declared in this crypto map, you can have multiple peers within a given crypto map The set transform-set command is where we associate the transforms with the crypto map ipsec-isakmp Indicate that IKE will be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry. ipsec-manual Indicate that IKE will not be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry. set peer Specify an IPSec peer in a crypto map entry. -- hostname Specify a peer by its hostname. This is the peer's hostname concatenated with its domain name. For example,myhost.example.com. -- ip-address Specify a peer by its IP address. set transform-set Specify which transform sets can be used with the crypto map entry.

QUESTION .169 Which of the following does CBAC do?
A. Recognize traffic at the application layer.
B. Provide intelligent filtering for all protocols.
C. Protect against attacks originating from the internal network.
D. Protect against every kind of attack.
Answer: A
Explanation: The reason that "Provide intelligent filtering for all protocols." is wrong is that it states ALL CBAC intelligently filters TCP and UDP packets CBAC can inspect traffic Real-time alerts and audit trails

---

QUESTION .170 How many useable hosts can you get from a /30 subnet mask?
A. 2
B. 4
C. 8
D. 30
E. 252
F. 0
Answer: A Explanation: IP Mask Notes ...
172.27.0.0 255.255.255.252 Subnet Address
172.27.0.1 255.255.255.252
172.27.0.2 255.255.255.252
172.27.0.3 255.255.255.252 Broadcast Address

QUESTION .171 ISAKMP defines the IKE framework (True or False)
A. True
B. False
Answer: A
Explanation: Identify the policy to create. Each policy is uniquely identified by the priority number you assign.isakmp policy priority

---

QUESTION .172 You want to create an access-list to allow only ssh to your RFC1918 network. Which one is correct?
A. access-list 100 permit tcp any host 10.0.0.0 0.255.255.255 eq 22
B. access-list 100 permit tcp any host 10.0.0.0 0.255.255.255 eq 22
access-list 100 permit any any
C. access-list 100 permit tcp any host 100.0.0.0 0.255.255.255 eq 23
D. access-list 100 permit tcp any host 100.0.0.0 0.0.0.255 eq 22
Answer: A
Explanation: SSH port 22 10.0.0.0 network is an RFC 1918 network

---

QUESTION .173 What can you do if storing large certificate revocation lists in your routers NVRAM becomes a problem? (Select all that apply)
A. crypto ca certificate query
B. crypto ca query
C. Turn on query mode so that certificate revocation lists are not stores locally but instead queried from the CA when necessary.
D. crypto key generate rsa
Answer: A, C
Explanation: "Turn on query mode so that certificate revocation lists are not stores locally but instead queried from the CA when necessary" really defines crypto ca certificate query To specify that certificates and Certificate Revocation Lists (CRLs) should not be stored locally but retrieved from
the CA when needed, use the crypto ca certificate query global configuration command.

QUESTION .174 On a PIX firewall, which of these rules are part of the ASA, by default? (Select all that apply)
A. All ICMP packets denied.
B. All inbound connections denied.
C. All outbound connections allowed.
D. No packets can traverse the PIX without a connection and state.
E. All packets are allowed in unless specifically denied.
Answer: A, B, C, D
Explanation:

QUESTION .175 Which of these are distance-vector routing protocols and support VLSM? (Select all that apply)
A. RIP
B. IGRP
C. BGP
D. OSPF

E. IS-IS
Answer: D,
E Explanation: THIS IS A MESSED UP QUESTION O SPF AND IS-IS ARE NOT DISTANCE-VECTOR YET THE ANSWER SAYS IT IS!! SO MAYBE THE ANSWER IS RIP (v2) and BGP (if thinking it is an advanced distance-vector instead of path vector) IF THE QUESTIOCALLS FOR LINK-STATE OSPF AND ISIS ARE CORRECT The Interior Gateway Routing Protocol(IGRP) is a distance vector interior-gateway routing protocol developed by Ciscohttp://www.cisco.com/en/US/products/hw/switches/ps663/products_configuration_guide_chapter09186a00800e 47dc.html The Enhanced Interior Gateway Routing Protocol (EIGRP) is a version of IGRP that combines the advantages of link-state protocols with distance vector protocols. EIGRP incorporates the Diffusing Update Algorithm (DUAL).The newer IP routing protocols, EIGRP and OSPF, support
VLSM, and they should be preferred in your network design Benefits: Customers choosing to implement RIP can now make more efficient use of their allocated address space by implementing Variable Length Subnet Masks (VLSM) within their networks. Until JJ Garcia-Luna-Alceves and then
Cisco started calling EIGRP "advanced distance vector" or "hybrid," distance vector was a term used for IGPs, and path vector was the term used for BGP.

QUESTION .176 What command is this output from?
name if ethernet0 outside security0
name if ethernet1 inside security100
A. show name if
B. show name
C. show interfaces
D. show ip int brief
E. show run
Answer: A

QUESTION .177 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
Explanation: Syslogd (8) is a collecting mechanism for various logging messages generated by the kernel and applications running on UNIX operating systems Prepare the configuration file for local hosts. The configuration file /etc/syslog.conf is as follows:

QUESTION .178 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 .179 What protocol does TACACS+ use to communicate?
A. TCP
B. UDP
C. IPX
D. TAC
E. RADIUS F. IPSec
Answer: A
Explanation:

QUESTION .180 What traffic is allowed through the following access-list (select the best answer)?
Access-list 2000 permit ip host 10.1.1.1 host 10.2.2.2Access-list 2000 deny ip any Access-list 2000permit ip 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.
E. This access-list is invalid as 2000 is the range for IPX access-lists.
Answer: B
Explanation: Access-list 2000 deny ip any Access-list 2000 permit ip any log THISIS IN THE WRONG ORDER! YOU DENY BUT THEN YOU ARE PERMITING ALL BUTLOGGING IT source to destination

QUESTION .181 What command will show the security levels, configured for interfaces, on a PIX firewall?
A. show name if
B. show interfaces
C. show ip interface brief
D. show name interfaces
E. show run
Answer: A
Explanation:

QUESTION .182 Which of these are based on the Bellman-Ford algorithm? (Select all that apply)
A. Distance vector routing protocols
B. Link-State routing protocols
C. OSPF
D. RIP
E. IGRP
Answer: A, D, E
Explanation: Distance-vector work off of Bellman-Ford algorithm and RIP and IGRP are Examples of DISTANCE-VECTOR

QUESTION .183 What is the easiest way to clear your router of RSA keys that have been generated?
A. no crypto key zeroes rsa
B. no crypto key generate rsa usage-keys
C. no crypto key generate rsa usage-keys
D. write erase & reload

Answer: A

Explanation: To delete all of your router's RSA keys, use the crypto key zeroes rsa global configuration command

---

QUESTION .184 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.

E. Policies must match exactly.

Answer: A, C

Explanation: IKE negotiations must be protected, so each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations. After the two peers agree upon a policy, the security parameters of the policy are identified by a security association established at each peer, and these security associations apply to all subsequent IKE traffic during the negotiation. There are five parameters to define in each IKE policy encryption algorithm 56-bit DES-CBC 168-bit Triple DES hash algorithm SHA-1 (HMAC variant) MD5 (HMAC variant) authentication method RSA signatures pre-shared keys Diffie-Hellman group identifier 768-bit Diffie-Hellman or 1024-bit Diffie-Hellman security association's lifetime can specify any number of seconds

---

QUESTION .185 With a CA, what do you have to do when adding a new router to your existing IPSec network?

A. Enroll the new router with the CA and request a certificate for the router.

B. Make multiple key entries on the routers in the network.

C. Enter the public key of the new router on each of the existing routers.

D. Configure a TA between each router.

Answer: A

QUESTION .186 Which of these use store-and-forward & cut-through?

A. switch

B. bridge

C. router

D. multiplexor

E. BPDU

F. PIX

Answer: A

Explanation: Switch uses store-and-forward and cut-through methods of send a packet through the switch. Remember it has to do with the packet length read before transmitted.

QUESTION .187 With a 10Mb Ethernet link, what is the formula for calculating OSPF cost?

A. 100 Mbps/10 Mbps = 10

B. 100 Mbps/10 Mbps = 1

C. 1000 Mbps/10 Mbps = 100

D. 100 Bbps/10 Mbps / Cost = .10

E. 10

F. 100 Mbps/10 Mbps * delay = 10
Answer: A
Explanation: In general, the path cost is calculated using the following formula: (10^8) ÷Bandwidth Asynchronous-Default cost is 10,000 X25-Default cost is 5208 56-kbps serial link-Default cost is 1785 64-kbps serial link-Default cost is 1562 T1 (1.544-Mbps serial link)-Default cost is 64 E1 (2.048-Mbps serial link)-Default cost is 48 4-Mbps Token Ring-Default cost is 25Ethernet-Default cost is 10 16-Mbps Token Ring-Default cost is 6 FDDI-Default cost is 1 ATM-Default cost is 1

QUESTION .188 Once a user enters their username and password, which are valid responses that a RADIUS server might provide? (Select all that apply)
A. ACCEPT
B. REJECT
C. CHALLENGE
D. CHANGE PASSWORD
E. DENY
F. REDIRECT
Answer: A, B, C, D
Explanation: Access-Request---sent by the client (NAS) requesting access Access-Reject---sent by the RADIUS server rejecting access Access-Accept---sent by the RADIUS server allowing access Access-Challenge---sent by the RADIUS server requesting more information in order to
allow access. The NAS, after communicating with the user, responds with another access request.

QUESTION .189 What does CSPM do that PDM does not? (Select all that apply)
A. Supports IOS routers.
B. Runs on Windows 2000.
C. Runs only on a web interface.
D. Part of Cisco works.
E. Supports only PIX.
Answer: A, B, D

QUESTION .190 Your BGP router receives two routes. Both of their next hops are reachable, neither has a weight set, route A has a larger local preference but a longer AS path than route B. Which route is the BEST BGP route?
A. Route A, as it has a larger local preference.
B. Route B, as it has a shorter AS path.
C. Neither route.
D. Both routes are best.
Answer: A
Explanation:

QUESTION .191 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
E. tacacs-server ; tacacs-server key

Answer: A
Explanation: To specify a TACACS+ host, use the tacacs-server host command in global configuration mode. To set the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon, use the tacacs-server key command in global configuration mode.

QUESTION .192 You want to set an enable password with the best encryption possible. What command do you use?
A. service password-encryption
B. enable password
C. enable secret
D. enable secret-encryption
Answer: C
Explanation: Enable secret is the command to use the encryption. service password encryption encrypts ALL password NOT JUST THE ENABLE

QUESTION .193 What is the skinny protocol?
A. SCCP
B. SSCP
C. SIP
D. H.323
E. RTSP
Answer: A
Explanation: SKINNY-Skinny Client Control Protocol.

QUESTION .194 Which of the following are valid ranges for IP or extended IP Cisco IOS access-lists? (Select all that apply)

B. 1300-1399
C. 100-199
D. 2000-2699
E. 200-299 F. 1000-1099
Answer: A, B, C, D
Explanation: ACL Number Type Supported 1-99 IP standard access list 100-199IP extended access list 200-299 Protocol type-code access list 300-399 DECnet access list 400-499 XNS standard access list 500-599 XNS extended access list 600-699 AppleTalk access list 700-799 48-bit MAC address access list 800-899 IPX standard access list 900-999 IPX extended access list 1000-1099IPX SAP access list 1100-1199 Extended 48-bit MAC address access list 1200-1299 IPX summary address access list 1300-1999 IP standard access list (expanded range) 2000-2699 IP extended access list(expanded range)

QUESTION .195 You want to make sure that you only receive routing updates about networks in the 10.x.x.xrange. What command would you use?
A. distribute-list
B. access-group
C. access-class
D. policy routing

Answer: A
Explanation: Distribute-list is the best option of the one that are viable

QUESTION .196 Which BGP attribute is set to tell an external AS which of your BGP paths is most preferred as the entry point to your AS?
A. MED
B. Local Pref
C. Weight
D. Origin
E. Entry
Answer: A

QUESTION .197 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.
E. All of the protocols are enabled.
Answer: A, B
Explanation:

QUESTION .198 What will filter packets based on upper layer session information?
A. reflexive access-lists
B. dynamic access-lists
C. standard access-lists
D. firewalls
E. lock-and-key
Answer: A
Explanation: Reflexive access lists are similar in many ways to other access lists. Reflexive access lists contain condition statements (entries) that define criteria for permitting IP packets. These entries are evaluated in order, and when a match occurs, no more entries are evaluated. However,
reflexive access lists have significant differences from other types of access lists. Reflexive access lists contain only temporary entries; these entries are automatically created when a new IP session begins (for example, with an outbound packet), and the entries are removed when the session ends. Reflexive access lists are not themselves applied directly to an interface, but are "nested" within an extended named IP access list that is applied to the interface. (For more information about this, see the section "Reflexive Access Lists Configuration Task List" later in this chapter

QUESTION .199 Exhibit:
ip http server ip http access-class 1access-list 1 deny any access-list 1 permit any Look at the attached exhibit. Who can access your router through the http interface?
A. Anyone
B. No one.

C. Only people on the 10.0.0.0 network.
D. The http server is not enabled.
E. Anyone with a username/password.
Answer: B
Explanation: ACCESS-LIST 1 is a DENY first

QUESTION .200 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
E. ip cef
Answer: A
Explanation: The Unicast RPF feature helps mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address.

QUESTION .201 Which of the following are distance-vector routing protocols? (Select all that apply)
A. RIP
B. IGRP
C. OSPF
D. BGP
E. IS-IS
Answer: A, B

QUESTION .202 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
E. /etc/shadow
Answer: A
Explanation: This file contains a history of su(1M) command usage. As a security measure, this file should not be readable by others. Truncate the /var/adm/sulog file periodically to keep the size of the file within a reasonable limit. The /usr/sbin/cron, the /sbin/rc0, or the /sbin/rc2 command can be
used to clean up the sulog file. You can add the appropriate commands to the /var/spool/cron/crontabs/root file or add shell commands to directories such as /etc/rc2.d, /etc/rc3.d, and so on. The following two line script truncates the log file and saves only its last 100 lines:

QUESTION .203 What is the BGP attribute that is most important on Cisco routers?
A. weight
B. local pref
C. MED
D. origin
E. as path

F. next hop
Answer: A

QUESTION .204 How could you deny telnet access to the aux port of your router?
A. access-list 52 deny 0.0.0.0 255.255.255.255line aux 0access-class 52 in
B. access-list 52 deny 0.0.0.0 255.255.255.255line aux 0access-group 52 in
C. There is no telnet access to the aux port.
D. You cannot do this.
E. access-class 52 permit 0.0.0.0 255.255.255.255line aux 0access-class 52 in
Answer: A

QUESTION .205 Which can control the per-user authorization of commands on a router?
A. RADIUS
B. TACACS+
C. IPSec
D. AAAA
E. NTLM
Answer: B