



Exam : 350-018

Title : CCIE Pre-Qualification Test for Security

Ver : 09-04-08

QUESTION 1:**DRAG DROP**

You work as a network engineer at Certkiller .com. Your boss, Miss Certkiller, is interested in Risk Analysis methods. Match the attributes with the appropriate methods.

Options, select from these

Is easier to automate and evaluate

Involves high degree of guess work

Requires complex calculations

Uses verifiable and objective metrics

Uses the opinions of individuals who know the process

Quantitative Risk Analysis

Place here

Place here

Place here

Qualitative Risk Analysis

Place here

Place here

Place here

Answer:

Quantitative Risk Analysis

Is easier to automate and evaluate

Requires complex calculations

Uses verifiable and objective metrics

Qualitative Risk Analysis

Involves high degree of guess work

Uses the opinions of individuals who know the process

Place here

Explanation:

Qualitative Risk Analysis

Involves a high degree of guess work

Uses the opinions of individuals who know the process

Quantitative Risk Analysis

Requires complex calculations

Uses verifiable and objective metrics

Is easier to automate and evaluate

Qualitative Risk Analysis

Qualitative Risk Analysis assesses the impact and likelihood of the identified risks in a rapid and cost-effective manner. By evaluating the priority of risks with consideration to impact on the project's cost, schedule, scope and quality objectives, Qualitative Risk Analysis provides a foundation for a focused quantitative analysis or Risk Response Plan.

Quantitative Risk Analysis

Quantitative risk analysis is the practice of creating a mathematical model of a project or process that explicitly includes uncertain parameters that we cannot control, and also decision variables or parameters that we can control. A quantitative risk model calculates the impact of the uncertain parameters and the decisions we make on outcomes that we care about -- such as profit and loss, investment returns, environmental consequences, and the like. Such a model can help business decision makers and public policy makers understand the impact of uncertainty and the consequences of different decisions.

QUESTION 2:

DRAG DROP

You work as a network engineer at Certkiller .com. Your boss, Miss Certkiller, is interested protocol port numbers. Match the port numbers with the appropriate protocols.

Use only ports that apply.

Options, select from these

TCP port 443	UDP port 500
UDP port 4500	IP protocol 47
IP protocol 51	IP protocol 50

Protocol

AH
ESP
IKE
NAT-T

Options,place here

Place here
Place here
Place here
Place here

Answer:

Options, select from these

TCP port 443

IP protocol 47

Protocol

Options, place here

AH

IP protocol 51

ESP

IP protocol 50

IKE

UDP port 500

NAT-T

UDP port 4500

Explanation:

Application Protocol Protocol Port

GRE TCP 47

IPsec ESP TCP 50

IPsec AH TCP 51

HTTPS TCP 443

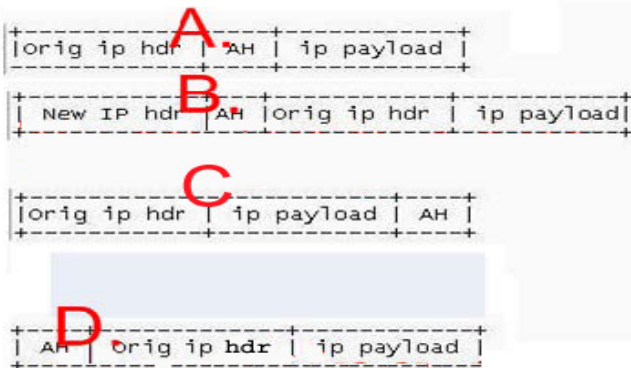
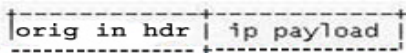
IPsec ISAKMP UDP 500

NAT-T UDP 4500

<http://support.microsoft.com/kb/832017>**QUESTION 3:**

Exhibit:

Original data Packet



You work as a network administrator at Certkiller .com. Please study the exhibit carefully.

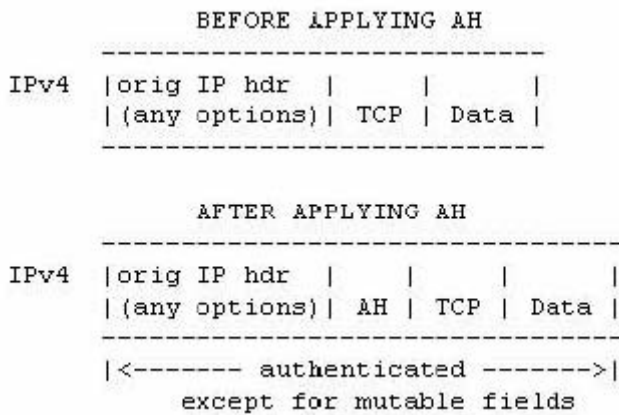
Assuming the shown data packet is to be protected by AH (Authentication Header) in transport mode, which of the following correctly describes the packet structure after AH is applied?

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

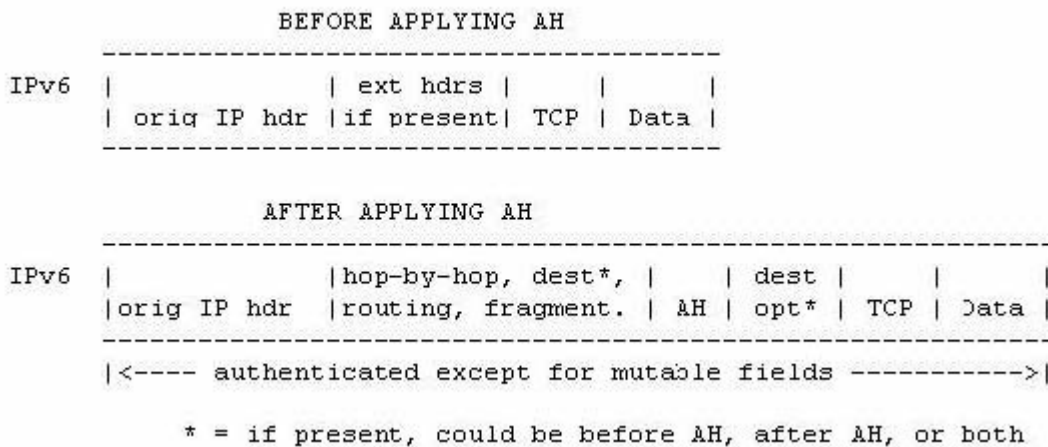
Answer: B

Explanation.

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



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



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

```

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

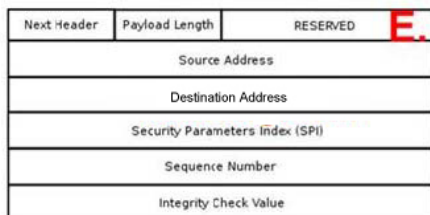
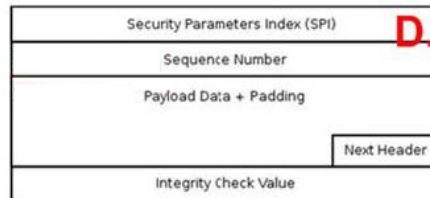
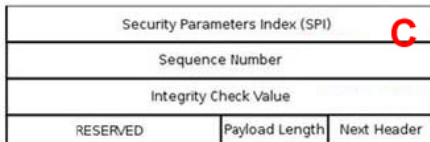
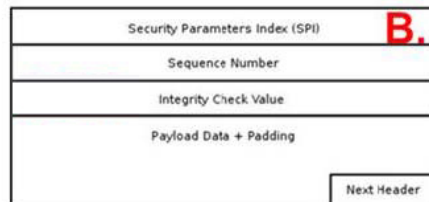
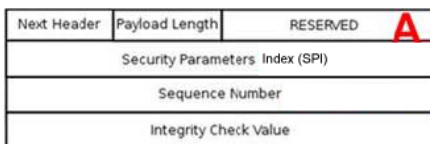
IPv6 |   | ext hdrs* |   |   | ext hdrs* |   |   |
    | new IP hdr* | if present | AH | orig IP hdr* | if present | TCP | Data |
    -----
    | <-- authenticated except for mutable fields in new IP hdr --> |
    -----

```

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

QUESTION 4:

Exhibit:



You work as a network administrator at Certkiller .com. Please study the exhibit carefully.

Which of the following is the correct diagram for an IPSec Authentication Header?

- A. A
- B. B
- C. C

- D. D
- E. E

Answer: A

Explanation:

Authentication header (AH)

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

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

Field meanings:

Next header

Identifies the protocol of the transferred data.

Payload length

Size of AH packet.

RESERVED

Reserved for future use (all zero until then).

Security parameters index (SPI)

Identifies the security parameters, which, in combination with the IP address, then identify the security association implemented with this packet.

Sequence number

A monotonically increasing number, used to prevent replay attacks.

Authentication data

Contains the integrity check value (ICV) necessary to authenticate the packet; it may contain padding.

QUESTION 5:

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

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

Answer: B

Explanation:

Passive FTP

In order to resolve the issue of the server initiating the connection to the client a different method for FTP connections was developed. This was known as passive mode, or PASV, after the command used by the client to tell the server it is in passive mode.

In passive mode FTP the client initiates both connections to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server. When opening an FTP connection, the client opens two random unprivileged ports locally ($N > 1023$ and $N+1$). The first port contacts the server on port 21, but instead of then issuing a PORT command and allowing the server to connect back to its data port, the client will issue the PASV command. The result of this is that the server then opens a random unprivileged port ($P > 1023$) and sends the PORT P command back to the client. The client then initiates the connection from port $N+1$ to port P on the server to transfer data.

From the server-side firewall's standpoint, to support passive mode FTP the following communication channels need to be opened:

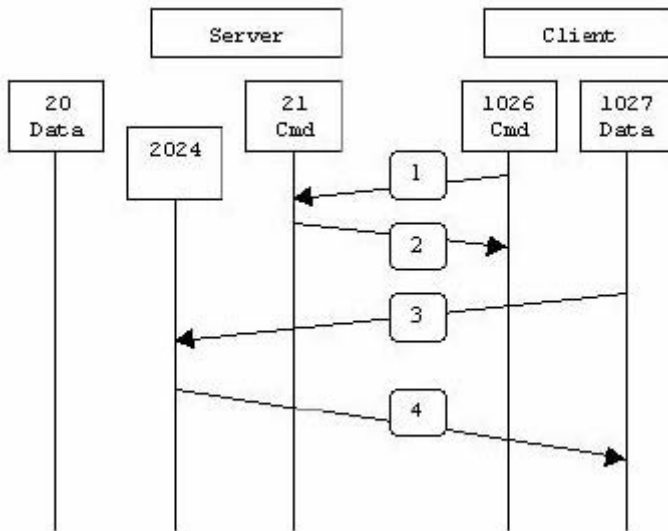
FTP server's port 21 from anywhere (Client initiates connection)

FTP server's port 21 to ports > 1023 (Server responds to client's control port)

FTP server's ports > 1023 from anywhere (Client initiates data connection to random port specified by server)

FTP server's ports > 1023 to remote ports > 1023 (Server sends ACKs (and data) to client's data port)

When drawn, a passive mode FTP connection looks like this:



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

QUESTION 6:

What does the common criteria standard define?

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

Answer: D

Explanation:

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

assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.

QUESTION 7:

What is the size of a Point-to-Point GRE header and Protocol Number of IP Layer?

- A. 8 bytes and 74
- B. 4 bytes and 47
- C. 2 bytes and 71
- D. 24 bytes and 1

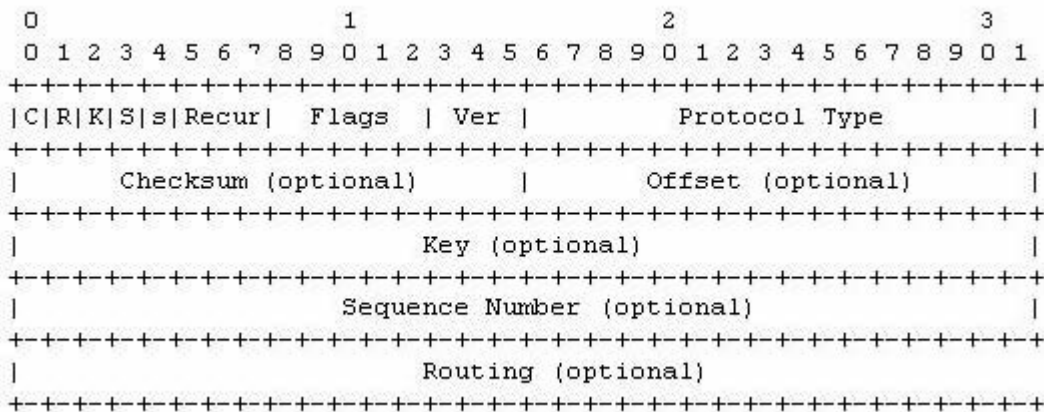
Answer: B

Explanation

Protocol suite: TCP/IP. Type: Transport layer encapsulation protocol. IP Protocol: 47.

Generic Routing Encapsulation (GRE)

Packet header The GRE packet header has the form:



Flags and version (2 octets)

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

RFC 1701 Generic Routing Encapsulation (GRE) October 1994

Checksum Present (bit 0)

If the Checksum Present bit is set to 1, then the Checksum field is present and contains valid information. If either the Checksum Present bit or the Routing Present bit are set, BOTH the Checksum and Offset fields are present in the GRE packet.

Routing Present (bit 1) If the Routing Present bit is set to 1, then it indicates that the Offset and Routing fields are present and contain valid information. If either the Checksum Present bit or the Routing Present bit are set, BOTH the Checksum and Offset fields are present in the GRE packet.

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

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

Strict Source Route (bit 4) The meaning of the Strict Source route bit is defined in other documents. It is recommended that this bit only be set to 1 if all of the the Routing Information consists of Strict Source Routes.

Recursion Control (bits 5-7) Recursion control contains a three bit unsigned integer which contains the number of additional encapsulations which are permissible. This SHOULD default to zero.

RFC 1701 & 2890

QUESTION 8:

Exhibit:

```
Interface Fa0/1
Switchport access Vlan 100
Switchport mode access
Dot1x port control auto
Dot1x guest-vlan 10
```

You work as a network administrator at Certkiller .com. Please study the exhibit carefully.

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

- A. VLAN 10, the guest vlan is also known as the restricted vlan
- B. Client without an 802.1x supplicant connecting to port fa0/1 will be assigned to the vlan 10
- C. Client connecting to port fa0/1 with an 802.1x supplicant but fails authentication will be assigned to the vlan 10
- D. Client Connecting to port fa0/1 with an 802.1x supplicant but fails authentication will be assigned to the vlan 100

Answer: B

Explanation

switchport access

Use the switchport access interface configuration command to configure a port as a static-access port. The port operates as a member of the configured VLAN.

Use the no form of this command to reset the access mode to the default VLAN for the switch.

Syntax

switchport access vlan vlan-id

no switchport access vlan vlan-id

Syntax Description

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

dot1x port-control

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

Syntax Description

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

QUESTION 9:

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

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

Answer: A

Explanation

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

QUESTION 10:

Which of the following describes the DHCP "Starvation" attack?

- A. Exhaust the address space available on the DHCP servers so an attacker can inject their own DHCP server or serve addresses for malicious reasons
- B. Saturate the network with DHCP requests preventing other network services working
- C. Inject a DHCP server on the network for the purpose of overflowing DNS servers with bogus learned host names
- D. DHCP starvation is the act of sending DHCP response packets for the purpose of overloading layer two CAM tables

Answer: A

Explanation

DHCP Starvation

A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. This is easily achieved with attack tools such as gobble. If enough requests are sent, the network attacker can exhaust the address space available to the DHCP servers for a period of

time. This is a simple resource starvation attack just like a SYN flood is a starvation attack. The network attacker can then set up a rogue DHCP server on his or her system and respond to new DHCP requests from clients on the network. Exhausting all of the DHCP addresses is not required to introduce a rogue DHCP server, though.

QUESTION 11:

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

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

Answer: A,B,D,E

Explanation

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

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

NetFlow packet details

NetFlow Analyzer accounts for the following details from the NetFlow Packets :

Source and destination IP address

Input and output interface number

Source and destination port number

Layer 4 Protocol

Number of packets in the flow

Total Bytes in the flow

Time stamp in the flow

Source and destination AS

TCP_Flag & TOS

Security Monitoring for Threat Control

Cisco Security Monitoring, Analysis and Response System (MARS) provides security monitoring for network security devices and host applications made by Cisco and other providers. Security monitoring greatly reduces false positives by providing an end-to-end view of the network, and can increase effective mitigation responses. Other features and benefits of Cisco MARS:

- * "Understands" the configuration and topology of your environment
 - * Promotes awareness of environmental anomalies with Network Behavior Analysis using NetFlow
 - * Provides quick and easy access to audit compliance reports with more than 150 ready-to-use customizable reports
 - * Makes precise recommendations for threat removal, including the ability to visualize the attack path and identify the source of the threat with detailed topological graphs that simplify security response at Layer 2, and above
- Security monitoring with Cisco Security MARS and Cisco Security Manager are part of the Cisco Security Management Suite, which delivers policy administration and enforcement for the Cisco Self-Defending Network.

QUESTION 12:

Which ones are the two types of ciphers?

- A. Blocking cipher and non-blocking cipher
- B. CBC cipher and ECB cipher
- C. Block cipher and Stream cipher
- D. Blocker cipher and Streamer cipher
- E. 3DES cipher and AES cipher

Answer: C

Explanation

In cryptography, a block cipher is a symmetric key cipher which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation. When encrypting, a block cipher might take a (for example) 128-bit block of plaintext as input, and output a corresponding 128-bit block of ciphertext. The exact transformation is controlled using a second input - the secret key.

Decryption is similar: the decryption algorithm takes, in this example, a 128-bit block of ciphertext together with the secret key, and yields the original 128-bit block of plaintext.

To encrypt messages longer than the block size (128 bits in the above example), a mode of operation is used.

Block ciphers can be contrasted with stream ciphers; a stream cipher operates on individual digits one at a time, and the transformation varies during the encryption. The distinction between the two types is not always clear-cut: a block cipher, when used in certain modes of operation, acts effectively as a stream cipher.

An early and highly influential block cipher design was the Data Encryption Standard (DES), developed at IBM and published as a standard in 1977. A successor to DES, the Advanced Encryption Standard (AES), was adopted in 2001.

QUESTION 13:

What Cisco technology protects against Spanning-Tree Protocol manipulation?

- A. Spanning Tree protect
- B. Root Guard and BPDU Guard
- C. Unicast Reverse Path Forwarding
- D. MAC Spoof Guard
- E. Port Security

Answer: B

Explanation

Network Security at the Data Link Layer (Layer 2) of LAN

Every layer of communication has its own unique security challenges. The data link layer (layer 2) communication is a weak link in terms of security. Network security should be addressed at multiple layers to for different vulnerabilities. In this article, we focus on the security issues related to wired local area networks. Wireless LAN and the securities issues for wide area networks (WAN) are discussed in separate articles. Switches are key components at the layer 2 communications and they are also used for layer 3 communications. They are susceptible to many of the same Layer 3 attacks as routers, as well as many unique network attacks, which include:

* Content-Addressable Memory (CAM) table overflow: The CAM table in a switch contains information such as the MAC addresses available on a given physical port of a switch, as well as the associated VLAN parameters. CAM tables are limited in size. Typically a network intruder will flood the switch with a large number of invalid-source MAC addresses until the CAM table fills up. When that occurs the switch will flood all ports with incoming traffic because it cannot find the port number for a particular MAC address in the CAM table. CAM table overflow only floods traffic within the local VLAN so the intruder will see only traffic within the local VLAN to which he or she is connected.

* VLAN hopping: VLAN hopping is a network attack whereby an end system sends out packets destined for a system on a different VLAN that cannot normally be reached by the end system. This traffic is tagged with a different VLAN ID to which the end system belongs. Or, the attacking system may be trying to behave like a switch and negotiate trunking so that the attacker can send and receive traffic between other VLANs.

* Spanning-Tree Protocol manipulation: Spanning-Tree Protocol is used in switched networks to prevent the creation of bridging loops in an Ethernet network topology. By attacking the Spanning-Tree Protocol, the network attacker hopes to spoof his or her system as the root bridge in the topology. To do this the network attacker broadcasts out Spanning-Tree Protocol Configuration/Topology Change Bridge Protocol Data Units (BPDUs) in an attempt to force spanning-tree recalculations. The BPDUs sent out by the network attacker's system announce that the attacking system has a lower bridge priority. If successful, the network attacker can see a variety of frames.

*

Media Access Control (MAC) Address spoofing: MAC spoofing attacks involve the use of a known MAC address of another host to attempt to make the target switch forward frames destined for the remote host to the network attacker. By sending a single frame with the other host's source Ethernet address, the network attacker overwrites the CAM table entry so that the switch forwards packets destined for the host to the network attacker. Until the host sends traffic it will not receive any traffic. When the host sends out traffic, the CAM table entry is rewritten once more so that it moves back to the original port.

* Address Resolution Protocol (ARP) attack: ARP is used to map IP addressing to MAC addresses in a local area network segment where hosts of the same subnet reside. ARP attack happens when someone is trying to change the ARP table of MAC and IP addresses information without authorization. By doing so, hackers can spoof his/her MAC or IP address to launch the following two types of attacks: Denial of Service and Man-In-The-Middle attacks.

* Private VLAN: Private VLANs work by limiting the ports within a VLAN that can communicate with other ports in the same VLAN. Isolated ports within a VLAN can communicate only with promiscuous ports. Community ports can communicate only with other members of the same community and promiscuous ports. Promiscuous ports can communicate with any port. One network attack capable of bypassing the network security of private VLANs involves the use of a proxy to bypass access restrictions to a private VLAN.

* DHCP starvation: A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. This is easily achieved with attack tools such as gobble. If enough requests are sent, the network attacker can exhaust the address space available to the DHCP servers for a period of time. This is a simple resource starvation attack just like a SYN flood. The network attacker can then set up a rogue DHCP server on his or her system and respond to new DHCP requests from clients on the network.

Mitigations of LAN Security Risks

The CAM table-overflow attack can be mitigated by configuring port security on the switch. This option provides for either the specification of the MAC addresses on a particular switch port or the specification of the number of MAC addresses that can be learned by a switch port. When an invalid MAC address is detected on the port, the switch can either block the offending MAC address or shut down the port.

Mitigating VLAN hopping attacks requires several modifications to the VLAN configuration. One of the more important elements is to use dedicated VLAN IDs for all trunk ports. Also, disable all unused switch ports and place them in an unused VLAN. Set all user ports to nontrunking mode by explicitly turning off DTP on those ports.

To mitigate Spanning-Tree Protocol manipulation use the root guard and the BPDU guard enhancement commands to enforce the placement of the root bridge in the network as well as enforce the Spanning-Tree Protocol domain borders. The root guard feature is designed to provide a way to enforce the root-bridge placement in the network.

The Spanning-Tree Protocol BPDU guard is designed to allow network designers to keep the active network topology predictable. While BPDU guard may seem unnecessary given that the administrator can set the bridge priority to zero, there is still no guarantee that it will be elected as the root bridge because there might be a bridge with priority zero and a lower bridge ID. BPDU guard is best deployed towards user-facing ports to prevent rogue switch network extensions by an attacker.

Use the port security commands to mitigate MAC-spoofing attacks. The port security command provides the capability to specify the MAC address of the system connected to a particular port. The command also provides the ability to specify an action to take if a port-security violation occurs. However, as with the CAM table-overflow attack mitigation, specifying a MAC address on every port is an unmanageable solution. Hold-down timers in the interface configuration menu can be used to mitigate ARP spoofing attacks by setting the length of time an entry will stay in the ARP cache.

Configure access control lists (ACLs) on the router port to mitigate private VLAN attacks. Virtual ACLs can also be used to help mitigate the effects of private VLAN attacks.

The techniques that mitigate CAM table flooding also mitigate DHCP starvation by limiting the number of MAC addresses on a switch port. As implementation of RFC 3118, Authentication for DHCP Messages, DHCP starvation attacks will become more difficult.

In addition, IEEE 802.1X, a standard for passing the Extensible Authentication Protocol (EAP) framework over a wired or wireless network, acts as a gatekeeper for basic network access at the data link layer. By denying access to the network before authentication is successful, 802.1X can prevent many attacks against network infrastructure that depend on having basic IP connectivity. Originally written to be used within the Point-to-Point Protocol (PPP) of dial-up and remote access networks, 802.1x allows for EAP to be used within the context of LANs, including wireless LAN.

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

QUESTION 14:

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

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

Answer: B

Explanation

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

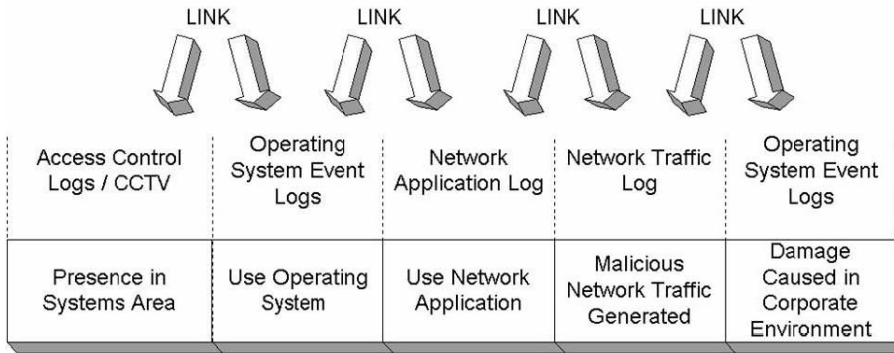


Fig. 1: Chain of Evidence Linking User to Crime

Chain-of-Evidence Model

The Chain-of-Evidence Model illustrates the discrete sets of actions carried out by an insider attempting to inflict malicious damage in an intranet environment. One group of actions is separated from another, based on the level of authority required to execute them. Each group of actions has a different corresponding source of evidence that must be responsible for documenting activity for forensic purposes. However each such source of evidence must be linked to the logs next to it (see above figure) in order to form a complete chain of evidence. The figure above starts with physical access to computer systems that must precede any malicious activity. It is in this stage that the crucial link between physical recognition and computer recognition take place. Following log-on procedures the user proceeds to invoke the services of a network application that must be used as a vehicle to inflict damage on a remote system. The network application issues the malicious network traffic that reaches a remote computer and executes the intended behavior.

QUESTION 15:

Exhibit:

Certkiller1# debug ip ospf adj

```

23:48:06:OSPF:interface OSPF_VL1 going Up
23:48:06: OSPF: Send with youngest Key 0
23:48:07: OSPF: Build router LSA for area 0, router ID 3.3.3.3, seq 0x80000001
23:48:07: OSPF: Build router LSA for area 2, router ID 3.3.3.3, seq 0x80000033
23:48:07: OSPF: Build router LSA for area 1, router ID 3.3.3.3, seq 0x80000030
23:48:14: OSPF: 2 Way Communication to 1.1.1.1 on OSPF_VL1, state 2WAY
23:48:14: OSPF: Send DBD to 1.1.1.1 on OSPF_VL1 seq 0x1EA opt 0x62 flag 0x7 len 32
23:48:14: OSPF: Send with youngest Key 1
23:48:14: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x3FB opt 0x62 flag 0x7 len 32 mtu 0 state EXSTART
23:48:14: OSPF: First DBD and we are not SLAVE 23:48:16: OSPF: Send with youngest Key 1
23:48:19: OSPF: Send DBD to 1.1.1.1 on OSPF_VL1 seq 0x1EA opt 0x62 flag 0x7 len 32
23:48:19: OSPF: Send with youngest Key 1 23:48:19: OSPF: Retransmitting DBD to 1.1.1.1 on OSPF_VL1 [1]
23:48:19: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x3FB opt 0x62 flag 0x7 len 32 mtu 0 state EXSTART 2
3:48:19: OSPF: First DBD and we are not SLAVE
23:48:19: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x1EA opt 0x62 flag 0x2 len 172 mtu 0 state EXSTART
23:48:19: OSPF: NBR Negotiation Done. We are the MASTER
23:48:19: OSPF: Send DBD to 1.1.1.1 on OSPF_VL1 seq 0x1EA opt 0x62 flag 0x2 len 112
23:48:19: OSPF: Send with youngest Key 1
23:48:19: OSPF: Send with youngest Key 1
23:48:19: OSPF: Database request to 1.1.1.1
23:48:19: OSPF: sent LS REQ packet to 5.0.0.1, length 48
23:48:19: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x1EB opt 0x62 flag 0x0 len 32 mtu 0 state EXCHANGE
23:48:19: OSPF: Send DBD to 1.1.1.1 on OSPF_VL1 seq 0x1EC opt 0x62 flag 0x1 len 32
23:48:19: OSPF: Send with youngest Key 1
23:48:19: OSPF: Build router LSA for area 0, router ID 3.3.3.3, seq 0x80000030
23:48:19: OSPF: Rcv DBD from 1.1.1.1 on OSPF_VL1 seq 0x1EC opt 0x62 flag 0x0 len 32 mtu 0 state EXCHANGE
23:48:19: OSPF: Exchange Done with 1.1.1.1 on OSPF_VL1
23:48:19: OSPF: Synchronized with 1.1.1.1 on OSPF_VL1, state FULL
23:48:19: %OSPF-6-ADJCHG: Process 2, Nbr 1.1.1.1 on OSPF_VL1 from LOADING to FULL, Loading Done

```

You work as a network administrator at Certkiller .com. Please study the exhibit carefully.

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

+

- A. The Certkiller 1 (local) router is the DR
- B. Both Certkiller 1 (local) and the remote OSPF neighbor are not directly connected to Area 0
- C. The Remote OSPF neighbor has an OSPF Router ID of 3.3.3.3
- D. The OSPF neighbors are establishing a virtual link
- E. The OSPF neighbors are using MD5 Authentication

Answer: D,E

Explanation

debug ospf flood

To display information about flood events such as acknowledgments and updates received, use the debug ospf flood command in EXEC mode. To disable debugging output, use the no form of this command.

debug ospf instance-name flood [access-list-name]

no debug ospf instance-name flood [access-list-name]

Syntax Description

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

Defaults

Debugging is disabled.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.

Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the Configuring AAA Services on Cisco IOS XR Software module of the Cisco IOS XR System Security Configuration Guide.

Debugging output is assigned high priority in the CPU process and, therefore, can affect system performance. For more information about the impact on system performance when using debug commands, refer to Using Debug Commands on Cisco IOS XR Software.

Use the debug ospf flood command to display messages containing information related to flood events.

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

Task ID

Task ID	Operations
ospf	read, write

Examples

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

```
RP/0/RP0/CPU0:router# debug ospf 1 flood
RP/0/RP0/CPU0:33:19: ospf[239]: Rcv Update Type 2, LSID 192.168.20.207, Adv rtr
192.168.20.207, age 764, seq 0x80000001
RP/0/RP0/CPU0:33:19: ospf[239]: Mask 255.255.255.0
RP/0/RP0/CPU0:33:19: ospf[239]: %ROUTING-OSPF-5-ADJCHG : Process 1, Nbr
192.168.20.207 on
GigabitEthernet0/2/0/0 from LOADING to FULL, Loading Done
RP/0/RP0/CPU0:33:19: ospf[239]: Sending update on GigabitEthernet0/2/0/0 to 192.168.20.207
Area 0
RP/0/RP0/CPU0:33:19: ospf[239]: Send Type 1, LSID 1.1.1.1, Adv rtr 1.1.1.1, age 40, seq
0x80000001 (0)
RP/0/RP0/CPU0:33:19: ospf[239]: Inc retrans unit nbr count index 1 (0/1) to 1/1
RP/0/RP0/CPU0:33:19: ospf[239]: Set Nbr 192.168.20.207 1 first flood info from 0 (0) to
0x81e1994 (18)
RP/0/RP0/CPU0:33:19: ospf[239]: Init Nbr 192.168.20.207 1 next flood info to 0x81e1994
RP/0/RP0/CPU0:33:19: ospf[239]: Add Type 1 LSA ID 1.1.1.1 Adv rtr 1.1.1.1 Seq 80000002 to
GigabitEthernet0/2/0/0 192.168.20.207 retransmission list
```


RP/0/RP0/CPU0:33:19: ospf[239]: Start GigabitEthernet0/2/0/0 192.168.20.207 retrans timer
RP/0/RP0/CPU0:33:19: ospf[239]: Set idb next flood info from 0 (0) to 0x81e1994 (18)
RP/0/RP0/CPU0:33:19: ospf[239]: Add Type 1 LSA ID 1.1.1.1 Adv rtr 1.1.1.1 Seq 80000002 to GigabitEthernet0/2/0/0 flood list
RP/0/RP0/CPU0:33:19: ospf[239]: Start GigabitEthernet0/2/0/0 pacing timer for 0.000001 msec
RP/0/RP0/CPU0:33:19: ospf[239]: Flooding update on GigabitEthernet0/2/0/0 to 224.0.0.5 Area 0
RP/0/RP0/CPU0:33:19: ospf[239]: Send Type 1, LSID 1.1.1.1, Adv rtr 1.1.1.1, age 1, seq 0x80000002 (0)
RP/0/RP0/CPU0:33:19: ospf[239]: Create retrans unit 0x81e0178/0x81df818 1 (0/1) 1
RP/0/RP0/CPU0:33:19: ospf[239]: Set nbr 1 (0/1) retrans to 4976 count to 1
RP/0/RP0/CPU0:33:19: ospf[239]: Set idb next flood info from 0x81e1994 (18) to 0 (0)
RP/0/RP0/CPU0:33:19: ospf[239]: Remove Type 1 LSA ID 1.1.1.1 Adv rtr 1.1.1.1 Seq 80000002 from GigabitEthernet0/2/0/0 flood list
RP/0/RP0/CPU0:33:19: ospf[239]: Stop GigabitEthernet0/2/0/0 flood timer
RP/0/RP0/CPU0:33:21: ospf[239]: Sending delayed ACK on GigabitEthernet0/2/0/0
RP/0/RP0/CPU0:33:21: ospf[239]: Ack Type 1, LSID 192.168.20.207, Adv rtr 192.168.20.207, age 764, seq 0x80000003
RP/0/RP0/CPU0:33:21: ospf[239]: Ack Type 2, LSID 192.168.20.207, Adv rtr 192.168.20.207, age 764, seq 0x80000001
RP/0/RP0/CPU0:33:21: ospf[239]: Received ACK from 192.168.20.207 on GigabitEthernet0/2/0/0
RP/0/RP0/CPU0:33:21: ospf[239]: Rcv Ack Type 1, LSID 1.1.1.1, Adv rtr 1.1.1.1, age 40, seq 0x80000001
RP/0/RP0/CPU0:33:24: ospf[239]: Retransmitting update on GigabitEthernet0/2/0/0 to 192.168.20.207 Area 0

QUESTION 16:

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

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

Answer: B,D

Explanation

VTP has 3 protocol versions Version 1, 2, & 3. VTP Version 3 incorporates many changes from VTP V1 and V2.

VTP Messages in Detail

VTP packets are sent in either Inter-Switch Link (ISL) frames or in IEEE 802.1Q (dot1q) frames. These packets are sent to the destination MAC address 01-00-0C-CC-CC-CC with a logical link control (LLC) code of Subnetwork Access Protocol (SNAP) (AAAA) and a type of 2003 (in the SNAP header). This is the format of a VTP packet that is encapsulated in ISL frames:

ISL Header	Ethernet Header DA: 01-00-0C-00-00-00	LLC Header SSAP: AA DSAP: AA	SNAP Header OUI: cisco Type 2003	VTP Header	VTP Message	CRC
26 bytes	14 bytes	3 bytes	3 bytes	VARIABLE LENGTH (SEE AFTER)		

Of course, you can have a VTP packet inside 802.1Q frames. In that case, the ISL header and cyclic redundancy check (CRC) is replaced by dot1q tagging.

Summary Advertisements

By default, Catalyst switches issue summary advertisements in five-minute increments. Summary advertisements inform adjacent Catalysts of the current VTP domain name and the configuration revision number.

When the switch receives a summary advertisement packet, the switch compares the VTP domain name to its own VTP domain name. If the name is different, the switch simply ignores the packet. If the name is the same, the switch then compares the configuration revision to its own revision. If its own configuration revision is higher or equal, the packet is ignored. If it is lower, an advertisement request is sent.

Summary Advert Packet Format:

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

This list clarifies what the fields means in the summary advertisement packet:

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

Subset Advertisements

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

Subset Advert Packet Format:

0	1	2	3
0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9 0 1
Version	Code	Sequence Number	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revision			
VLAN-info field 1			
.....			
VLAN-info field N			

VTP Pruning

VTP ensures that all switches in the VTP domain are aware of all VLANs. However, there are occasions when VTP can create unnecessary traffic. All unknown unicasts and broadcasts in a VLAN are flooded over the entire VLAN. All switches in the network receive all broadcasts, even in situations in which few users are connected in that VLAN. VTP pruning is a feature that you use in order to eliminate or prune this unnecessary traffic.

http://www.cisco.com/warp/public/473/21.html#vtp_pruning

VLAN Pruning

VTP can prune unneeded VLANs from trunk links. VTP maintains a map of VLANs and switches, enabling traffic to be directed only to those switches known to have ports on the intended VLAN. This enables more efficient use of trunk bandwidth.

Each switch will advertise which VLAN's it has active to neighboring switches. The neighboring switches will then "prune" VLAN's that are not active across that trunk, thus saving bandwidth. If a VLAN is then added to one of the switches, the switch will then re-advertise it's active VLAN's so that pruning can be updated by its neighbors. For this to work, VLAN pruning must be enabled on both ends of the trunk. It is easiest to enable VLAN pruning for an entire VTP management domain by simply enabling it on one of the VTP servers for that domain. To enable VLAN pruning for a VTP domain, enter the following command on a VTP server for that domain...

VTP_Server_Sw1(config)# vtp pruning

This will then propagate to all switches in the vtp domain.

Configure VLAN Pruning

	Task	Command
Step 1	Enable VTP pruning in the	set vtp pruning enable
	management domain.	
Step 2	(Optional) Make specific	clear vtp pruneeligible
	VLANs pruning-ineligible on the device.	vlan_range
	(By default, VLANs 2-1000 are pruning-eligible.)	
Step 3	(Optional) Make specific	set vtp pruneeligible
	VLANs pruning-eligible on the	vlan_range
	device.	
Step 4	Verify the VTP pruning	show vtp domain
	configuration.	
Step 5	Verify that the appropriate	show trunk
	VLANs are being pruned on	
	trunk ports.	

QUESTION 17:

Which of the following statements are true regarding hashing?

- A. MD5 produces a 160-bit result
- B. SHA-256 is an extension to SHA-1 with a longer output

- C. MD5 takes more CPU cycles to compute than SHA-1
- D. Changing 1 bit of the input to SHA-1 changes 1 bit of the output
- E. SHA-1 is stronger than MD5 because it can be used with a key to prevent modification

Answer: B,D

Explanation

Answer A is incorrect because, in cryptography, MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321).

It is easy to generate MD5 collisions, it is possible for the person who created the file to create a second file with the same checksum, so this technique cannot protect against some forms of malicious tampering

The SHA hash functions are five cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S.

Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length. They are called "secure" when (in the words of the standard), "it is computationally infeasible to:

find a message that corresponds to a given message digest, or

find two different messages that produce the same message digest.

Any change to a message will, with a very high probability, result in a different message digest."

B is correct and C is incorrect because of the following

The five algorithms are denoted SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.

The latter four variants are sometimes collectively referred to as SHA-2. SHA-1 produces a message digest that is 160 bits long; the number in the other four algorithms' names denote the bit length of the digest they produce.

SHA-1 is employed in several widely used security applications and protocols, including TLS and SSL, PGP, SSH, S/MIME, and IPsec. It was considered to be the successor to MD5, an earlier, widely-used hash function.

E is incorrect because of the following

The security of SHA-1 has been somewhat compromised by cryptography researchers[1].

Although no attacks have yet been reported on the SHA-2 variants, they are

algorithmically similar to SHA-1 and so efforts are underway to develop improved

alternative hashing algorithms.[2][HYPERLINK \l "_note-2"](#)[3] An open competition for

a new SHA-3 function was formally announced in the Federal Register on November 2,

2007. [4] "NIST is initiating an effort to develop one or more additional hash algorithms

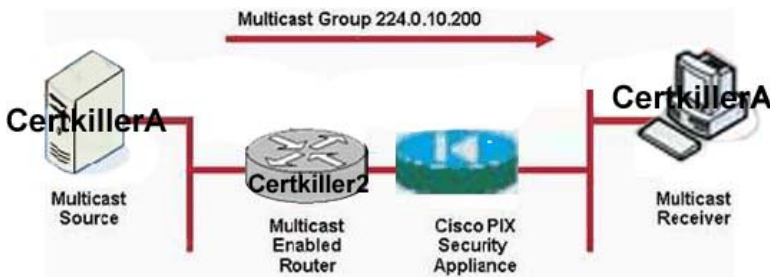
through a public competition, similar to the development process for the Advanced

Encryption Standard (AES)."[5] Submissions are due October 31, 2008 and the

proclamation of a winner and publication of the new standard are scheduled to take place in 2012.

QUESTION 18:

Network Topology Exhibit:



You work as a network administrator at Certkiller .com. Please study the exhibit carefully.

A cisco Security Appliance has been inserted between a multicast source and its receiver, preventing multicast traffic between them. What is the best solution to address this problem?

- A. Configure the security appliance as an IGMP multicast client
- B. Configure a GRE tunnel to allow the multicast traffic to bypass the security appliance
- C. Configure the security appliance as the rendezvous point of the multicast network so that (*,G) trees traverse it
- D. Create a static route on the multicast source and receiver pointing to the outside and inside interface of the security appliance respectively
- E. Configure SMR so the security appliance becomes an IGMP proxy agent, forwarding IGMP messages from hosts to the upstream multicast router

Answer: E

Explanation

A security appliance is nothing more than a Cisco PIX or an ASA.

A is wrong because

Multicast Support (IGMP v2 and Stub Multicast Routing)

This release enables you to statically configure multicast routes or use an IGMP helper address for forwarding IGMP reports and leave announcements.

The following summarizes multicast support in this release:

NAT and PAT can be performed on the multicast packet source addresses only.

IGMP packets for address groups within the 224.0.0.0-224.0.0.255 range are not forwarded because these addresses are reserved for protocol use.

NAT is not performed on IGMP packets. When IGMP forwarding is configured, the adaptive security appliance forwards the IGMP packets (report and leave) with the IP address of the helper interface as the source IP address.

Multicast Support

PIM sparse mode was added to allow direct participation in the creation of a multicast tree using PIM-SM. This capability extends existing multicast support for IGMP forwarding and for Class D access control policies and ACLs. PIM-SM provides an alternative to transparent mode operation in multicast environments.

The pim commands and the multicast-routing command added support to the new functionality in addition to the show mrib EXEC command in this feature. For more information, see the "Configuring Multicast Routing" section in the Cisco Security Appliance Command Line Configuration Guide.

For a complete description of the command syntax, see the Cisco Security Appliance Command

Reference.

http://www.cisco.com/en/US/docs/security/asa/asa70/release/notes/asa_rn.html#wp208194

B is incorrect because of the following:

As explained in the PIX documentation, the PIX Firewall does not pass multicast packets, even though many routing protocols use multicast packets to transmit their data. Cisco considers it inherently dangerous to send routing protocols across the PIX Firewall. If the routes on the unprotected interface are corrupted, the routes transmitted to the protected side of the firewall pollute routers there as well.

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

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

C is incorrect because of the following:

Configuring a Static Rendezvous Point Address

All routers within a common PIM sparse mode or bidir domain require knowledge of the PIM RP address. The address is statically configured using the `pim rp-address` command.

The security appliance does not support Auto-RP or PIM BSR; you must use the `pim rp-address` command to specify the RP address.

Answer D is incorrect because

Configuring a Static Multicast Route

When using PIM, the security appliance expects to receive packets on the same interface where it sends unicast packets back to the source. In some cases, such as bypassing a route that does not support multicast routing, you may want unicast packets to take one path and multicast packets to take another.

Static multicast routes are not advertised or redistributed.

To configure a static multicast route for PIM, enter the following command:

```
hostname(config)# mroute src_ip src_mask {input_if_name | rpf_addr} [distance]
```

To configure a static multicast route for a stub area, enter the following command:

```
hostname(config)# mroute src_ip src_mask input_if_name [dense output_if_name] [distance]
```

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

Answer E more information

For More Information about Multicast Routing

The following RFCs from the IETF provide technical details about the IGMP and multicast routing standards used for implementing the SMR feature:

RFC 2236 IGMPv2

RFC 2262 PIM-SM

RFC 2262 IP Multicast and Firewalls

RFC 2588 IP Router Alert Option

IETF draft-ietf-igmp-proxy-01.txt

QUESTION 19:

When implementing best practices for IP Source spoofing and defeating Denial of Service attacks with IP Source Address Spoofing, What RFC is commonly used ot

protect your network?

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

Answer: D

Explanation

RFC 1149 - Standard for the transmission of IP datagrams on avian carriers

<http://www.faqs.org/rfcs/rfc1149.html>

RFC 3704 - Ingress Filtering for Multihomed Networks

<http://www.ietf.org/rfc/rfc3704.txt>

RFC 1918 - Address Allocation for Private Internets

<http://www.faqs.org/rfcs/rfc1918.html>

RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

<http://www.ietf.org/rfc/rfc2827.txt>

QUESTION 20:

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

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

Answer: E

Explanation

The switch supports these types of secure MAC addresses:

Static secure MAC addresses-These are manually configure by using the switchport port-security mac-address mac-address interface configuration command, stored in the address table, and added to the switch running configuration.

Dynamic secure MAC addresses-These are dynamically configured, stored only in the address table, and removed when the switch restarts.

Sticky secure MAC addresses-These are dynamically configured, stored in the addresses table.

and added to the running configuration. If these addresses are saved in the configuration file, when the switch restarts, the interface does not need to dynamically reconfigure them.

QUESTION 21:

Exhibit:

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

You work as a network administrator at Certkiller .com. Please study the exhibit carefully.

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

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

Answer: A,C,D

Explanation

This is an extended access-list because it falls in the range of 100 - 199. 1 - 99 are standard access lists. The interface that the access-list is applied to is a public IP address and the default gateway is listed as 192.168.20.3 which appears to be directly connected to interface ethernet 1. On a firewall interface 0 is generally considered to be the outside interface while interface 1 is considered to be the inside interface therefore answer A appears to be correct.

http://www.cisco.com/en/US/docs/ios/11_3/security/configuration/guide/scacsls.html

http://www.cisco.com/en/US/docs/ios/11_3/security/configuration/guide/secur_c.html

http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

Extended ACLs

Extended ACLs were introduced in Cisco IOS Software Release 8.3. Extended ACLs control traffic by the comparison of the source and destination addresses of the IP packets to the addresses configured in the ACL.

This is the command syntax format of extended ACLs. Lines are wrapped here for spacing considerations.

IP

access-list access-list-number [dynamic dynamic-name [timeout minutes]]

{deny | permit} protocol source source-wildcard

destination destination-wildcard [precedence precedence]

[tos tos] [log | log-input] [time-range time-range-name]

Answer B is incorrect because ICMP packet are checked when then are incomming not outgoing

ICMP Inspection Checking

Return packets are checked by the inspect code, not by ACLs. The inspect code tracks each destination address from outgoing packets and checks each return packet. For ECHO REPLY and TIMESTAMP REPLY packets, the return address is checked. For UNREACHABLE and TIME EXCEEDED packets, the intended destination address is extracted from the packet data and checked.

C is correct because

Context-Based Access Control

Life with CBAC: You're still using access lists, baby!

CBAC is not a type of access list, but rather it a stateful inspect engine that works in conjunction with ESACLs. ESACLs enforce the global access policy, and CBAC inspects the traffic and provides the following five key security enhancements to the IOS:

Dynamic filtering exceptions -- CBAC provides dynamic return-path filtering for ICMP, UDP, and TCP for single-session and multi-session conversations. This function is very similar in operation to reflexive access lists. CBAC creates dynamic entries based on the bi-directional session flows in the filtering of access lists when a conversation is first established. This allows session traffic to pass between only hosts involved with conversations. Since permit access entries are unique, this eliminates the need (in theory) to leave any statically open ports. The service ports that are opened dynamically are limited in lifespan (the duration of the conversation) and only to specific to hosts, thus limiting the opportunity for external attacks.

http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci914940,00.html

Context-based access control (CBAC) was introduced in Cisco IOS Software Release 12.0.5.T and requires the Cisco IOS Firewall feature set. CBAC inspects traffic that travels through the firewall in order to discover and manage state information for TCP and UDP sessions. This state information is used in order to create temporary openings in the access lists of the firewall.

Configure ip inspect lists in the direction of the flow of traffic initiation in order to allow return traffic and additional data connections for permissible session, sessions that originated from within the protected internal network, in order to do this.

This is the syntax for CBAC.

ip inspect name inspection-name protocol [timeoutseconds]

This is an example of the use of CBAC in order to inspect outbound traffic. Extended ACL 111 normally block the return traffic other than ICMP without CBAC opening holes for the return traffic.

ip inspect name myfw ftp timeout 3600

ip inspect name myfw http timeout 3600

ip inspect name myfw tcp timeout 3600

ip inspect name myfw udp timeout 3600

ip inspect name myfw tftp timeout 3600

interface Ethernet0/1

ip address 172.16.1.2 255.255.255.0

```
ip access-group 111 in
ip inspect myfw out
access-list 111 deny icmp any 10.1.1.0 0.0.0.255 echo
access-list 111 permit icmp any 10.1.1.0 0.0.0.255
```

D is correct

When access-lists are applied to a firewall or router all nodes that are not explicitly permitted are denied. Without a permit statement no traffic will be able to enter interface ethernet 1. Interface ethernet 0 has neither a permit or deny statement for incoming or outgoing. Because of this Interface ethernet 0 will need an inbound permit statement if one is not applied to interface ethernet 1 so that traffic can come into the router. Because interface ethernet 1 is on the same subnet as the default router interface ethernet 1 would require an inbound permit statement for this to work correctly.

QUESTION 22:

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

- A. No Virtual applications or operating system
- B. No Viruses or worms
- C. Appropriate security applications and patch levels
- D. Current IPS signatures
- E. Cisco Security Agent

Answer: C

Explanation:

Immunize Networks with Policy Enforcement

Cisco NAC Appliance (formerly Cisco Clean Access) is an easily deployed Network Admission Control (NAC) product that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With NAC Appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access. It identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network's security policies and repairs any vulnerabilities before permitting access to the network.

When deployed, Cisco NAC Appliance provides the following benefits:

- * Recognizes users, their devices, and their roles in the network. This first step occurs at the point of authentication, before malicious code can cause damage.
 - * Evaluates whether machines are compliant with security policies. Security policies can include specific antivirus or antispyware software, OS updates, or patches. Cisco NAC Appliance supports policies that vary by user type, device type, or operating system.
 - * Enforces security policies by blocking, isolating, and repairing noncompliant machines. Noncompliant machines are redirected into a quarantine area, where remediation occurs at the discretion of the administrator.
-

QUESTION 23:

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

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

Answer: A, B,D

Explanation:

With the authentication proxy feature, users can log into the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecure ACS, or other RADIUS, or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.

The authentication proxy is compatible with other Cisco IOS security features such as Network Address Translation (NAT), Context-based Access Control (CBAC), IP Security (IPSec) encryption, and VPN client software.

To configure the authentication proxy, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1.	<code>router(config)# ip auth-proxy auth- cache-time min</code>	Set the global authentication proxy idle timeout value in minutes. If the timeout expires, user authentication entries are removed, along with any associated dynamic access lists. The default value is 60 minutes.
2.	<code>router(config)# ip auth-proxy auth- proxy-banner</code>	(Optional) Display the name of the firewall router in the authentication proxy login page. The banner is disabled by default.
3.	<code>router(config)# ip auth-proxy name auth-proxy-name http [auth-cache-time min] [list std-access- list</code>	<p>Create authentication proxy rules. The rules define how you apply authentication proxy. This command associates connection initiating HTTP protocol traffic with an authentication proxy name. You can associate the named rule with an access control list, providing control over which hosts use the authentication proxy feature. If no standard access list is defined, the named authentication proxy rule intercepts HTTP traffic from all hosts whose connection initiating packets are received at the configured interface.</p> <p>(Optional) The auth-cache-time option overrides the global authentication proxy cache timer. This option provides more control over timeout values for a specific authentication proxy rule. If no value is specified, the proxy rule assumes the value set with the ip auth-proxy auth-cache-time command.</p> <p>(Optional) The list option allows you to apply a standard access list to a named authentication proxy rule. HTTP connections initiated from hosts in the access list are intercept by the authentication proxy.</p>
4.	<code>router(config)# interface type</code>	Enter interface configuration mode by specifying the interface type on which to apply the authentication proxy.
5.	<code>router(config-if)# ip auth-proxy auth- proxy-name</code>	In interface configuration mode, apply the named authentication proxy rule at the interface. This command enables the authentication proxy rule with that name.

debug ip auth-proxy

To display the authentication proxy configuration information on the router, use the show ip auth-proxy configuration command in privileged EXEC mode.

debug ip auth-proxy {ftp | function-trace | http | object-creation | object-deletion | tcp | telnet | timer}

Syntax Description

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

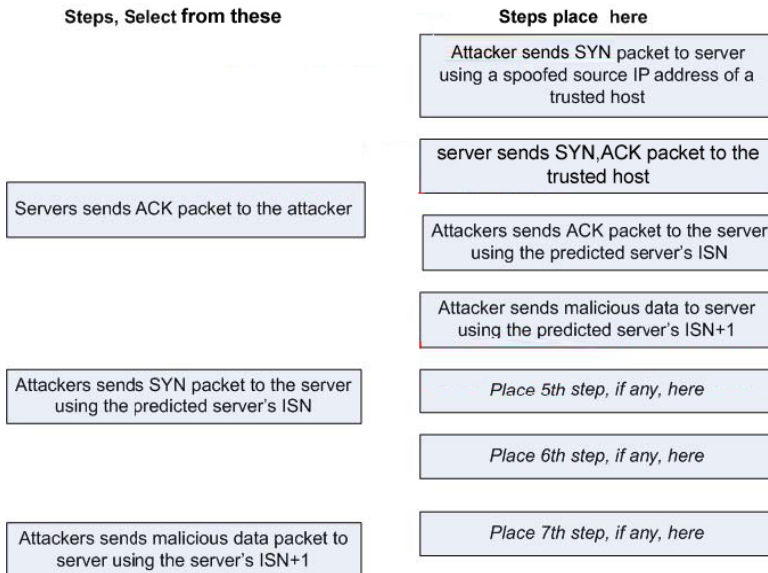
QUESTION 24:

DRAG DROP

You work as a network engineer at Certkiller .com. Your boss, Miss Certkiller, is interested in Server attack methods. In particular attacks performed by predicting the Server's TCP ISN (Initial Sequence Number). Place the appropriate steps in the correct order. Choose only steps that apply.

Steps, Select from these	Steps,place here
Server sends SYN, ACK packet to the trusted host.	Place first step here
Attacker sends malicious data to server using the predicted server's ISN+1	Place second step, if any, here
Servers sends ACK packet to the attacker	Place third step, if any, here
Attacker sends SYN packet to server using a spoofed source IP address of a trusted host	place fourth step,if ant,here
Attackers sends SYN packet to the server using the predicted server's ISN	Place 5th siep, if any, here
Attackers sends ACK packet to the server using the predicted server's ISN	Place 6th siep, if any, here
Attackers sends malicious data packet to server using the server's ISN+1	Place 7th siep, if any, here

Answer:



Explanation:

TCP Sequence Numbers:

A client machine sends a SYN signal to the host machine every time it wants to establish a new connection with it. The host machine then sends a SYN/ACK with a special identification number called the Initial Sequence Number (ISN). Both the client machine and the host machine exchange such sequence numbers (SQN) for error checking and reporting. RFC 793 specifies that the generation of a SQN be bound to a 32 bit clock which increments every 4 microseconds (i.e. 250,000 per second). Based on this timer the ISN will cycle once every 4.55 hours. Since the TTL for packets is much less than 4.55 hours it ensures that there are no more delayed segments on the network with the same SQN's.

Predicting TCP Sequence Numbers: Despite these guidelines, the majority of TCP implementations increment the SQN by a constant every second, and by another constant for each new connection. (The SQN is incremented by 128,000/sec and then 64,000 for each new connection.) Therefore, when you open a connection to a computer, you can determine with a high degree of confidence what next connection's sequence number will be.

Thus when an attacker A sends a SYNC to the victim server B requesting new connection it also send its ISN number. The latter then sends a SYN/ACK with its own ISN number which is 128,000 or higher than the previous connection.

Blind Spoofing: Using the previously mentioned technique for predicting TCP sequence numbers, it is possible to hijack a connection by:

DoS Server B through SYN flooding or other method

Spoof B's IP address and talk to host C

Since Server B has already been overloaded Host C will not know that it is talking to an attacker impersonating Server B.

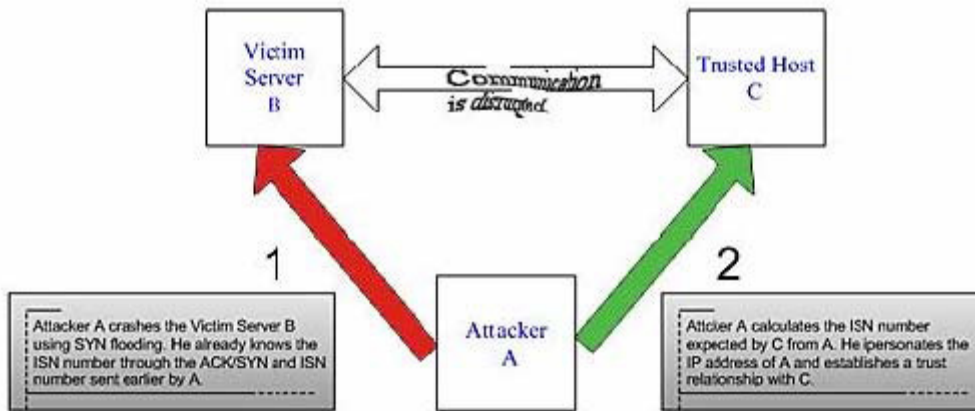
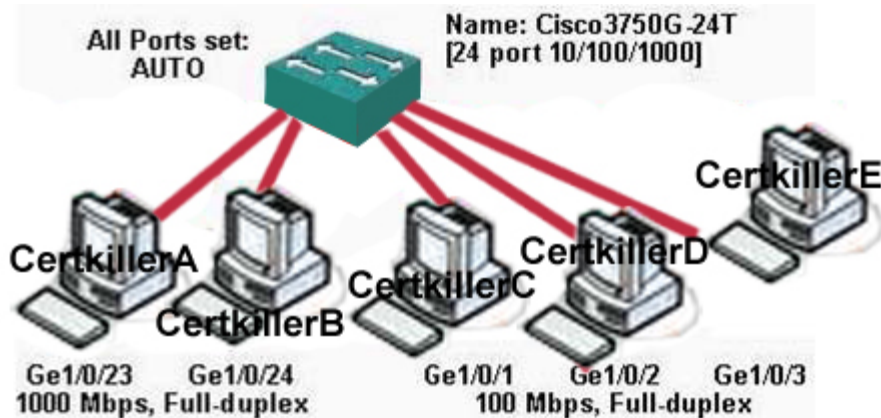


Fig 7: Blind Spoofing

The question remains, "Why don't computers realize that the IP address is spoofed?" The answer lies in the way and the type of information that is transferred by the TCP packets and IP packets. Since TCP is connection-oriented it carries only the Sequence Number and not the IP address. The IP packet on the other hand carries only the IP address and not the Sequence Number. Since the attacker already knows the IP address of the victim server, he predicts the SQN and spoofs the trusted host. Since the first victim (Server B) has been DoSed, it will not resume communications with Host C, and therefore the target (Host C) is blind to the fact that it is speaking with the wrong computer.

QUESTION 25:

Exhibit:



You work as a network administrator at Certkiller .com. Please study the exhibit carefully.

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

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

Answer: E

Explanation:

A is incorrect because very rarely will multiple NIC's fail on multiple PC's at the same time. The common denominator in this instance is the installation of the switch

B is incorrect because no sign of wrong configuration is shown

C is incorrect because it is also an extremely rare occurrence

D is incorrect because user workstation ports do not participate in Spanning tree

E is correct and can be a common occurrence this requires the port speed to be statically configured on the 100mbps switch ports

QUESTION 26:

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

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

Answer: E

Explanation:

Signatures

Cisco IPS prevents intrusion by comparing traffic against the signatures of known attacks. Cisco IOS images that support Cisco IPS have built-in signatures that Cisco IPS can use, and you can also have Cisco IPS import signatures for the router to use when examining traffic. Imported signatures are stored in a signature definition file (SDF).

This window lets you view the configured Cisco IPS signatures on the router. You can add customized signatures, or import signatures from SDFs downloaded from Cisco.com. You can also edit, delete, enable, and disable signatures.

Cisco IPS is shipped with an SDF that contains signatures that your router can accommodate. To learn more about the SDF shipped with Cisco IPS, and how to have Cisco IPS use it, click IPS-Supplied Signature Definition Files.

Adding a 5.x Custom Signature By Using the Signature Wizard

You can create custom signatures using the Signature Wizard. The Signature Wizard creates custom signatures at the device level, not at the group level.

To use the Signature Wizard, follow these steps:

Step 1 Select Configuration > Settings.

Step 2 In the TOC, click the Object Selector handle.

Step 3 In the Object Selector, select the 5.x sensor for which you want to create a custom signature.

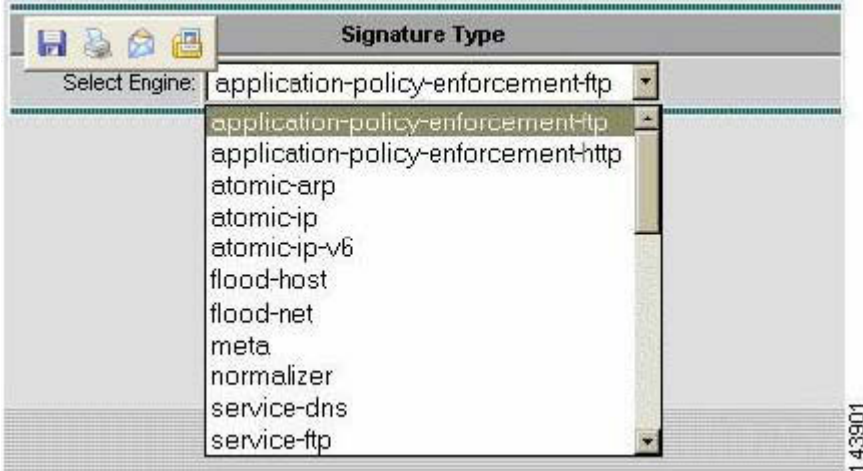
Step 4 In the TOC, select Signature Wizard > IPS 5.x.

The Signature Wizard welcome page appears.

Step 5 Click Start the Wizard.

a. Select either Engine Type or Protocol Type as the type of signature you want to create.

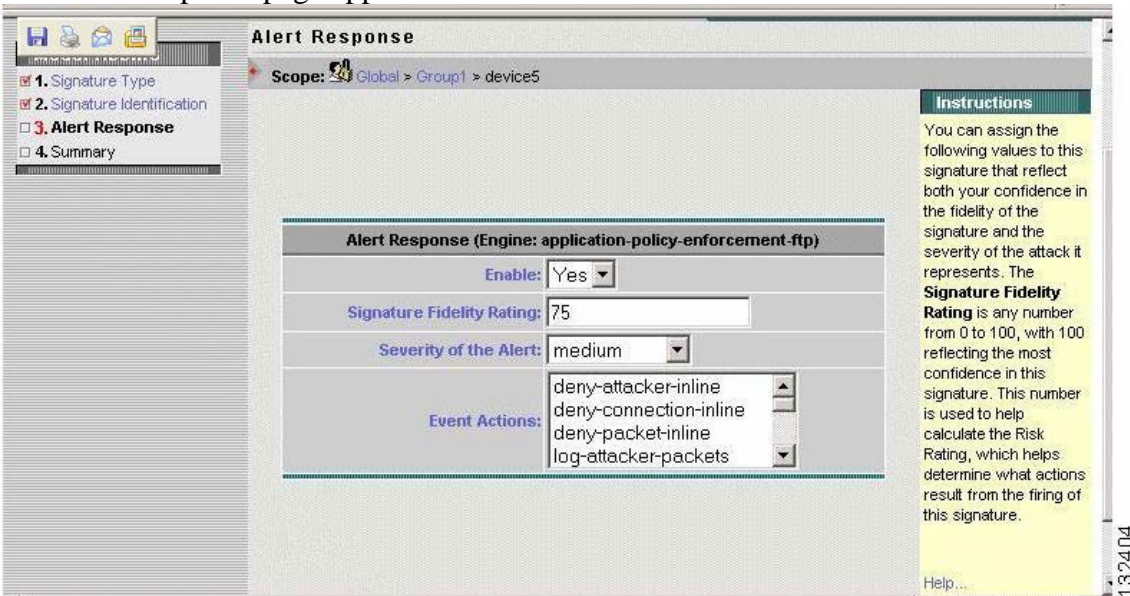
The Select Engine drop-down list appears.



b.

Enter the signature name in the Signature Name field and then click Next>.

The Alert Response page appears.



d.

Enter the signature fidelity rating in the Signature Fidelity Rating field.

f.

Select the action or actions that should be taken from the Event Action list. Then click Next>.

You can press and hold the Ctrl key while selecting, to select more than one Event Action from the list.

The Summary page appears.

h.

Click Finish>.

The system displays a message that notifies you that the signature has been successfully created.

j.

Verify that the new custom signature has been specified correctly:

a.

In the TOC, select Signatures.

c.

In the Select Group list box, select Custom.

e. Confirm the appearance of the new custom signature in the list, which signifies that it was added.

QUESTION 27:

What is NTP curcial for?

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

Answer: A,C,E

Explanation:

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

Answer A is correct

NTP synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows events to be correlated when system logs are created and other time-specific events occur.

http://www.cisco.com/en/US/tech/ CK6 48/ CK3 62/ CK4 61/tsd_technology_support_sub-protocol_home.html

C is correct

Proper validation of certificates typically requires checking to ensure the certificate has not yet expired. If devices have a real-time clock, they SHOULD verify the certificate validity dates.

If no real-time clock is available, the device SHOULD attempt to determine the current time using NTP prior to certificate validation. If neither is available, devices SHOULD verify that the start validity date of its peer's certificate is less than its

own certificate's expiration date, and its peer's expiration date is greater than its own start date. Note that failure to check a certificate's temporal validity can make a device vulnerable to man-in-the-middle attacks launched using compromised, expired certificates, and therefore devices should make every effort to perform this validation.

E is correct

Kerberos time sensitivity

Time is a critical service in Windows 2000 and Windows Server 2003. Timestamps are needed for directory replication conflict resolution, but also for Kerberos authentication. Kerberos uses timestamps to protect against replay attacks. Computer clocks that are out of sync between clients and servers can cause authentication to fail or extra authentication traffic to be added during the Kerberos authentication exchange.

QUESTION 28:

The following is an example of an IPSEC error message:

IPSEC(validate_proposal): invalid local address 192.1.1.1

ISAKMP (0:3): atts not acceptable

Next Payload is 0

ISAKMP (0:3): SA not acceptable!

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

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

Answer: D

Explanation:

This error message is attributed to one of these two common problems.

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

QUESTION 29:

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

- A. Anomaly Detection
- B. SYN Cookies
- C. Application Inspection
- D. Content Filtering

- E. Anti-x Protection
- F. Anti Virus

Answer: A

Explanation:

NetFlow is an embedded instrumentation within Cisco IOS Software to characterize network operation. Visibility into the network is an indispensable tool for IT professionals. In response to new requirements and pressures, network operators are finding it critical to understand how the network is behaving including:

- Application and network usage
- Network productivity and utilization of network resources
- The impact of changes to the network
- Network anomaly and security vulnerabilities
- Long term compliance issues

QUESTION 30:

With PGP, which of the following entity signs a users public key?

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

Answer: D

Explanation

Pretty Good Privacy is a computer program that provides cryptographic privacy and authentication. It was originally created by Philip Zimmermann in 1991.

PGP and other similar products follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data.

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

Web of trust

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

any tampering (or accidental garble) is readily detectable. But merely making a certificate effectively impossible to modify undetectably is also insufficient. It can prevent corruption only after the certificate has been created, not before. Users must also ensure by some means that the public key in a certificate actually does belong to the person/entity claiming it. From its first release, PGP products have included an internal certificate 'vetting scheme' to assist with this; a trust model which has been called a web of trust. A given public key (or more specifically, information binding a user name to a key) may be digitally signed by a third party user to attest to the association between someone (actually a user name) and the key. There are several levels of confidence which can be included in such signatures. Although many programs read and write this information, few (if any) include this level of certification when calculating whether to trust a key.

The web of trust protocol was first described by Zimmermann in the manual for PGP version 2.0:

As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys.

The web of trust mechanism has advantages over a centrally managed PKI scheme such as that used by S/MIME, but has not been universally used. Users have been willing to accept certificates and check their validity manually, or to simply accept them. The underlying problem has found no satisfactory solution.

QUESTION 31:

Which of the following are not steps in settingup a TLS session?

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

Answer: B

Explanation:

Transport Layer Security(TLS) IETF RFC 4507 / RFC4507

These goals are achieved by the handshake protocol, which can be summarized as follows: The client sends a client hello message to which the server must respond with a server hello message, or else a fatal error will occur and the connection will fail. The client hello and server hello are used to establish security enhancement capabilities between client and server. The client hello and server hello establish the following attributes: Protocol Version, Session ID, Cipher Suite, and Compression Method. Additionally, two random values are generated and exchanged: ClientHello.random and ServerHello.random.

The client indicates that it supports this mechanism by including a SessionTicket TLS extension in the ClientHello message. The extension will be empty if the client does not already possess a ticket for the server. The extension is described in Section 3.2. If the server wants to use this mechanism, it stores its session state (such as ciphersuite and master secret) to a ticket that is encrypted and integrity-protected by a key known only to the server. The ticket is distributed to the client using the NewSessionTicket TLS handshake message described in Section 3.3. This message is sent during the TLS handshake before the ChangeCipherSpec message, after the server has successfully verified the client's Finished message.

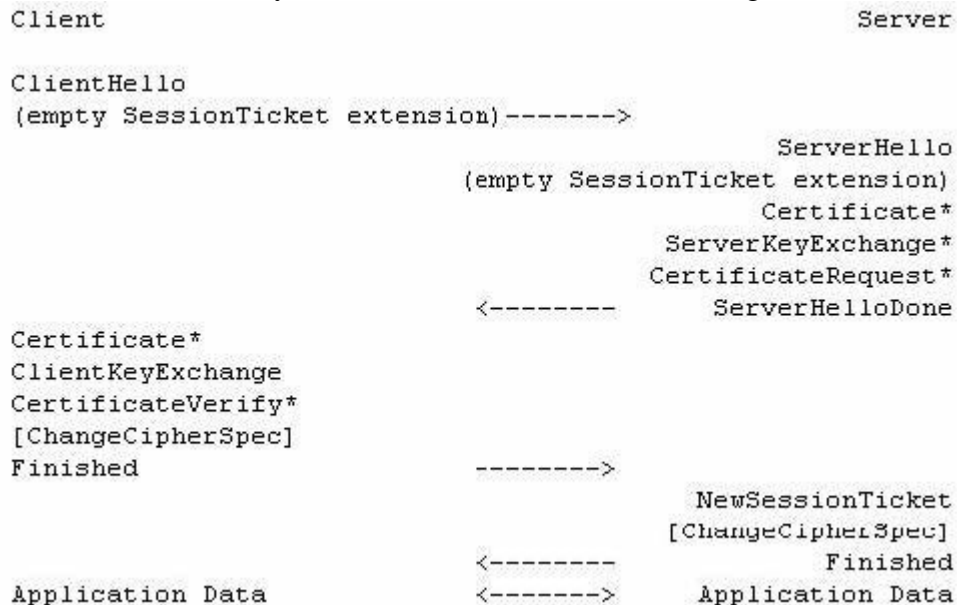


Figure 1: Message flow for full handshake issuing new session ticket The client caches this ticket along with the master secret and other parameters associated with the current session. When the client wishes to resume the session, it includes the ticket in the SessionTicket extension within the ClientHello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

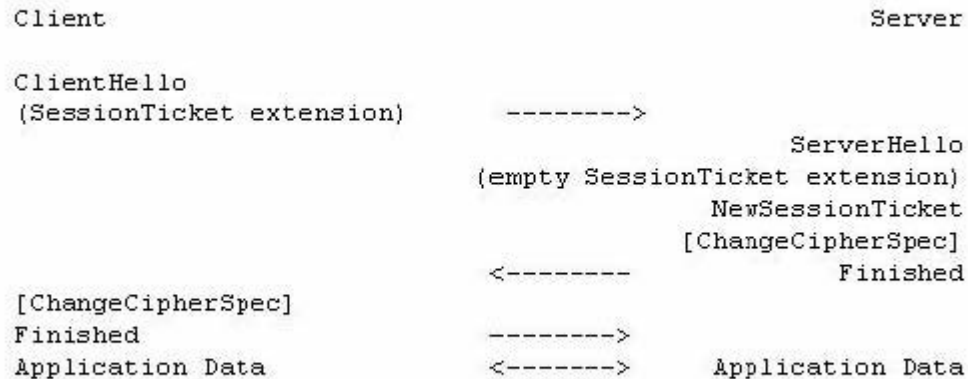


Figure 2: Message flow for abbreviated handshake using new session ticket

pre_master_secret This random value is generated by the client and is used to generate the master secret

When RSA is used for server authentication and key exchange, a 48- byte pre_master_secret is generated by the client, encrypted under the server's public key, and sent to the server. The server uses its private key to decrypt the pre_master_secret. Both parties then convert the pre_master_secret into the master_secret, as specified above.

If the client has a certificate containing fixed Diffie-Hellman parameters, its certificate contains the information required to complete the key exchange. Note that in this case the client and server will generate the same Diffie-Hellman result (i.e., pre_master_secret) every time they communicate.

QUESTION 32:

Exhibit:

1. 254 hrs
2. Only One IP Address by your ISP
3. Your IP Address is assigned dynamically
4. The CPE from the ISP is pre-provisioned and working
5. You are expected to make changes on your router.

Which RFCs are used to establish internet connectivity from a private office with the requirements displayed in the exhibit?

- A. IP Network Address Translator (NAT): Defined in RFC 1631
- B. IP Network Address Translator (NAT) Terminology and considerations: Defined in RFC 2663
- C. Network Address Translator (NAT) - Firendly/Application Design Guidelines:

Defined in RFC 3235

D. Address Allocation for Private Internets: Defined in RFC 1918

E. PPP and IPCP: Defined in RFC 1332

F. DHCP: Defined in RFC 2131

Answer: A,D,F

Explanation:

NAT will be required if the ISP has only provide 1 IP Address for all users to access the internet.

NAT is defined in both A & B. A explains CIDR and B explains NAT IP Address mappings.

Internally a private IP Address will be used these are defined in answer C RFC 1918.

The IP Addresses have to provided dynamically this is defined in F

QUESTION 33:

The following ip protocols and ports are commonly used in IPSec protocols

A. IP Protocol 50 and 51, UDP port 500 and 4500

B. UDP ports 50,51,500 and 4500

C. TCP ports 50,51,500 and 4500

D. IP protocols 50,51,500 and 4500

E. IP protocols 50 and 51, UDP port 500 and TCP port 4500

Answer: A

Explanation:

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

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

QUESTION 34:

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

A. The IPS device identified an incorrect value in Layer 7

B. There was no information in the IPS state table for the connection

C. The IPS device identified an incorrect value in layer 6

D. There was a valid SYN ACK in the state table but the subsequent packets were fragmented and did not constitute a valid flow

E. The IPS device identified an incorrect value in layer 5

Answer: B,D

Explanation:

The IPS Normalizer takes place on layers 3 and 4, therefore only B & D can be the correct answers.

The Normalizer engine deals with IP fragment reassembly and TCP stream reassembly. With the Normalizer engine you can set limits on system resource usage, for example, the maximum number of fragments the sensor tries to track at the same time.

Note

You cannot add custom signatures to the Normalizer engine. You can tune the existing ones. IP Fragmentation Normalization - Intentional or unintentional fragmentation of IP datagrams can hide exploits making them difficult or impossible to detect. Fragmentation can also be used to circumvent access control policies like those found on firewalls and routers. And different operating systems use different methods to queue and dispatch fragmented datagrams. If the sensor has to check for all possible ways that the end host can reassemble the datagrams, the sensor becomes vulnerable to DoS attacks. Reassembling all fragmented datagrams inline and only forwarding completed datagrams, refragmenting the datagram if necessary, prevents this. The IP Fragmentation Normalization unit performs this function.

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

The association of VLANs in pairs on a physical interface is known as inline VLAN pair mode. Packets received on one of the paired VLANs are analyzed and forwarded to the other VLAN in the pair. Inline VLAN pairs are supported on all sensors that are compatible with IPS 5.1, except NM?CIDS, AIP?SSM?10, and AIP?SSM?20.

QUESTION 35:

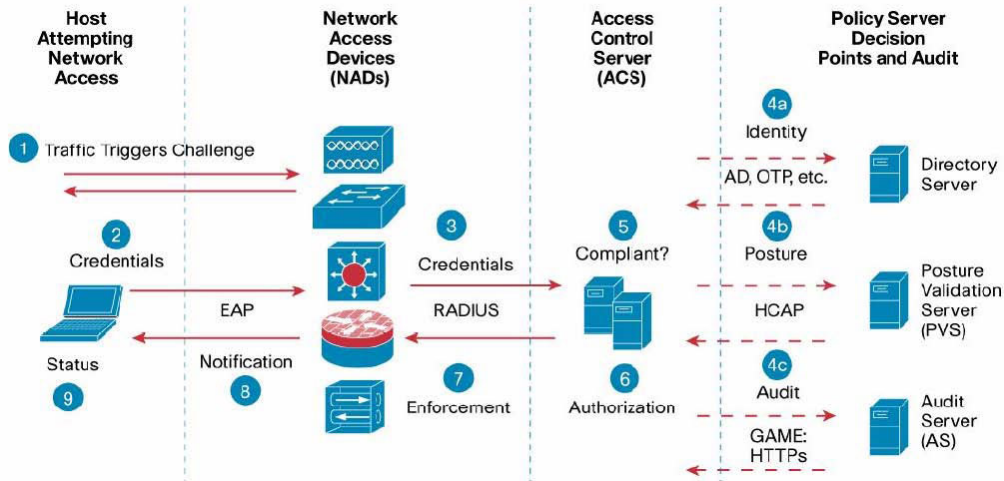
Which is the function of a Cisco router acting as a Network Access Device (NAD) in a NAC Framework solution?

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

Answer: D

Explanation:

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



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

Step 1. Posture validation occurs when a NAC-enabled network access device detects a host attempting to connect or use its network resources.

Step 2.

Upon detection of a new endpoint, the NAD sets up a communication path between the AAA server (ACS) and the posture agent. After the communication path has been established, the AAA server requests the endpoint for posture credentials from one or more posture plugins.

Step 3. The host responds to the request with its posture credentials from available posture plugins from NAC-compatible software components on the host.

Step 4. The AAA server either validates the posture information locally, or it can in turn delegate parts of the decision to external posture validation servers.

Step 5. The AAA server aggregates the individual posture results, or posture tokens, from all of the delegate servers to determine the overall compliance of the host, or system posture token.

Step 6. The identity authentication and system posture token are then mapped to a network authorization in the network access profile, which consists of RADIUS attributes for timers, VLAN assignments, or downloadable access control lists (ACLs).

Step 7. These RADIUS attributes are sent to the NAD for enforcement on the host.

Step 8. The CTA on the host is then sent its posture status for notifying the respective plugins of their individual application posture as well as the entire system posture.

Step 9. A message can be optionally sent to the end-user using the CTA's notification dialog so they know the host's current state on the network.

QUESTION 36:

Which SSL protocol takes an applications messages to be transmitted, framgements the data into mageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header and transmits the resulting unit in a TCP segment?

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

Answer: C

Explanation:

SSL Architecture

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

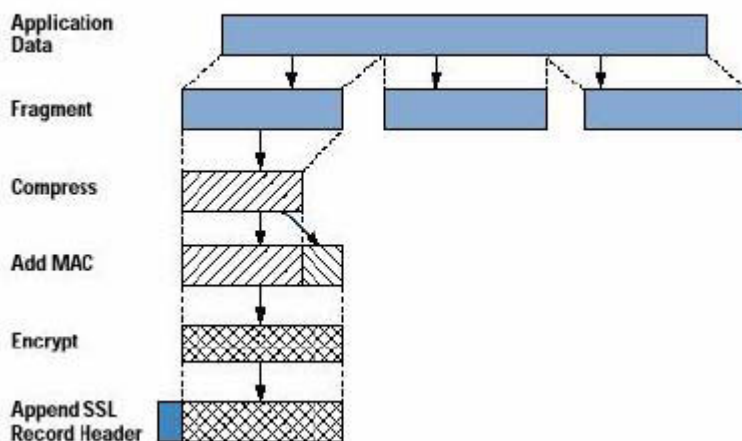
The SSL Record Protocol provides basic security services to various higher-layer protocols. In particular, the HTTP, which provides the transfer service for Web client/server interaction, can operate on top of SSL. Three higher-layer protocols are defined as part of SSL: the Handshake Protocol, the Change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

SSL Record Protocol

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

Figure 1 indicates the overall operation of the SSL Record Protocol. The Record Protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment. Received data is decrypted, verified, decompressed, and reassembled and then delivered to the calling application, such as the browser.

Figure 1: SSL Record Protocol Operation



The first step is fragmentation. Each upper-layer message is fragmented into blocks of 2¹⁴ bytes (16,384 bytes) or less. Next, compression is optionally applied. In SSLv3 (as well as the current version of TLS), no compression algorithm is specified, so the default compression algorithm is

null. However, specific implementations may include a compression algorithm.

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

Next, the compressed message plus the MAC are encrypted using symmetric encryption. A variety of encryption algorithms may be used, including the Data Encryption Standard (DES) and triple DES. The final step of SSL Record Protocol processing is to prepend a header, consisting of the following fields:

Content Type (8 bits): The higher-layer protocol used to process the enclosed fragment.

Major Version (8 bits): Indicates major version of SSL in use. For SSLv3, the value is 3.

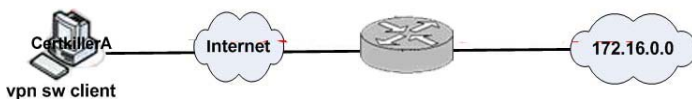
Minor Version (8 bits): Indicates minor version in use. For SSLv3, the value is 0.

Compressed Length (16 bits): The length in bytes of the plain-text fragment (or compressed fragment if compression is used).

The content types that have been defined are change_cipher_spec, alert, handshake, and application_data. The first three are the SSL-specific protocols, mentioned previously. The application-data type refers to the payload from any application that would normally use TCP but is now using SSL, which in turn uses TCP. In particular, the HTTP protocol that is used for Web transactions falls into the application-data category. A message from HTTP is passed down to SSL, which then wraps this message into an SSL record.

QUESTION 37:

Network Topology Exhibit:



Certkiller 2 configuration exhibit:


```
hostname Certkiller2
|
aaa new-model
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authorization exec default local
aaa authorization network sdm_vpn_group_ml_1 local
|
username test privilege 15 secret 5 $ 1$K 3v c$ vyvd
|
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
|
crypto isakmp client configuration group test
key cisco123
pool SDM_POOL_1
acl 100
|
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
|
crypto dynamic-map SDM_DYNMAP_1 1
set transform-set ESP-3DES-SHA
|
crypto map SDM_CMAP_1 client authentication list sdm_vpn_xauth_ml_1
crypto map SDM_CMAP_1 isakmp authorization list sdm_vpn_group_ml_1
crypto map SDM_CMAP_1 client configuration address respond
crypto map SDM_CMAP_1 65535 ipsec-isakmp dynamic SDM_DYNMAP_1
|

interface FastEthernet0/0
ip address 10.1.1.1 255.255.255.0
crypto map SDM_CMAP_1
|
interface FastEthernet0/1
ip address 172.16.1.1 255.255.255.0
|
ip local pool SDM_POOL_1 172.16.1.100 172.16.1.120
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
|
ip http server
ip http authentication local
ip http secure-server
ip http timeout-policy idle 600 life 86400 requests 10000
|
access-list 10 permit ip any 172.16.0.0 0.0.255.255
|
```

You work as a network administrator at Certkiller .com. Please study the exhibit carefully.

Referring to the network diagram and the Certkiller 2 Router Configurations shown in the exhibit, why remote users their Cisco VPN software client are not able to reach the 172.16.0.0 networks behind Certkiller 2 once they successfully VPN into Certkiller 2?

- A. The Cisco VPN software client does not support DH group 2
- B. Reverse Router Injection (RRI) is not enabled on Certkiller 2
- C. The Certkiller 2 Configuration is missing the crypto ACL
- D. The dynamic crypto map on Certkiller 2 is misconfigured
- E. The ACL 100 on Certkiller 2 is misconfigured

Answer: E

Explanation

A is incorrect because the Cisco VPN client does support DH Group 2

B is incorrect because

Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.

Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote Virtual Private Network (VPN) router as the next hop, the traffic is forced through the crypto process to be encrypted.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_14/gt_rrie.htm

C is incorrect because the crypto ACL is not missing

The Crypto Access Check on Clear-Text Packets feature removes the checking of clear-text packets that go through the IP Security (IPSec) tunnel just prior to encryption or just after decryption. The clear-text packets were checked against the outside physical interface access control lists (ACLs). This checking was often referred to as a double ACL check. This feature

enables easier configuration of ACLs and eliminates the security risks that are associated with a double check when using dynamic crypto maps.

crypto map map-name seq-number

Example:

Router(config)# crypto map vpn1 10

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_8/gt_crpk.htm

D is incorrect because the dynamic crypto map is not misconfigured

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvpnsng/icike.htm>

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

QUESTION 38:

What new features were added to the PIX in version 7.0? (Choose three.)

- A. WebVPN
- B. Rate-Limiting
- C. Support For Multiple Virtual Firewalls
- D. Transparent Firewall

Answer: B,C,D

Explanation

Release Highlights

ADVANCED FIREWALL SERVICES

Deep inspection firewall services for HTTP, FTP

ESMTP, and more

Instant messaging, peer-to-peer, and tunneling

application blocking

Cisco Modular Policy Framework with flow-based

security policies

Virtual firewall services

Layer 2 transparent firewall

3G Mobile Wireless security services

ROBUST IPSEC VPN SERVICES

VPN client security posture enforcement

Automatic VPN client software updating

OSPF dynamic routing overVPN tunnels

HIGH AVAILABILITY SERVICES

Active/Active failover with asymmetric routing support

Remote-access and site-to-site VPN stateful failover

Zero-downtime software upgrades

INTELLIGENT NETWORK SERVICES

PIM multicast routing

Quality of service (QoS)

IPv6 networking

FLEXIBLE MANAGEMENT SOLUTIONS

SSHv2 and SNMPv2c

Configuration rollback

Usability enhancements

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet0900aecd80225ae1.html

Rate-limiting is mention in version 7.0.4

<http://www.cisco.com/en/US/docs/security/pix/pix70/release/notes/pix704rn.html#wp217692>

The Web VPN client is not mention until version 7.2

<http://www.cisco.com/en/US/docs/security/pix/pix72/release/notes/pixrn72.html>

QUESTION 39:

What is the net effect of using ICMP type 4 messages to attact to RFC 1122 compliant hosts?

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

Answer: C

Explanation

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

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

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

1.1.1 Internet Hosts A host computer, or simply "host," is the ultimate consumer of communication services. A host generally executes application programs on behalf of user(s), employing network and/or Internet communication services in support of this function. An Internet host corresponds to the concept of an "End-System" used in the OSI protocol suite [INTRO:13]. An Internet communication system consists of interconnected packet networks supporting communication among host computers using the Internet protocols. The networks are interconnected using packet-switching computers called "gateways" or "IP routers" by the Internet community, and "Intermediate Systems" by the OSI world [INTRO:13]. The RFC "Requirements for Internet Gateways" [INTRO:2] contains the official specifications for Internet gateways. That RFC together with

<http://www.faqs.org/rfcs/rfc1122.html>

The Source Quench is an Internet Control Message Protocol message which requests the sender to decrease the traffic rate of messages to a router or host. This message may be generated if

the router or host does not have sufficient buffer space to process the request, or may occur if the router or host's buffer is approaching its limit.

QUESTION 40:

Exhibit:

The exhibit shows two screenshots from the Cisco ASDM configuration interface. The top screenshot displays the 'Interfaces' configuration table, and the bottom screenshot displays the 'Translation Example Rules' table.

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	Add	Edit	Delete
Ethernet1	inside	Yes	100	10.0.1.1	255.255.255.0	No			
Ethernet3	dmz2	Yes	50	172.16.11.1	255.255.255.0	Yes			
Ethernet2	dmz1	Yes	0	172.16.1.1	255.255.255.0	No			
Ethernet0	outside	Yes	0	192.168.1.2	255.255.255.0	No			

☐ Enable traffic between two or more interfaces which are configured with same levels

☐ Ethernet hahayyyjau nmanaget hahahahh haythdhynjdmdujj

Translation Example Rules

Show Rules for Interface:

Rule	Original		Translated	
Type	Interface	Source Network	Destination	Address
+	inside	in_host 10.0.1.1	any	outside 192.168.1.3
+	dmz1	dmz1_host 172.16.1.10	any	outside 192.168.1.4
+	dmz2	dmz2_host 172.16.11.12	any	outside 192.168.1.5
+	inside	10.0.1.0/24	any	dmz1 172.16.1.17-172.16.1.30
+	inside	10.0.1.0/24	any	outside 192.168.1.9-192.168.1.30

You work as a network administrator at Certkiller .com. Please study the exhibit carefully.

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

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

Answer: C

Explanation

Configuring Inter-Interface Communication

Allowing communication between same security interfaces provides the following benefits:

1

You want protection features to be applied equally for traffic between two interfaces; for example, you have two departments that are equally secure.

For different security level interfaces, many protection features apply only in one direction, for example, inspection engines, TCP intercept, and connection limits.

If you enable same security interface communication, you can still configure interfaces at different security levels as usual.

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

QUESTION 41:

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

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

Answer: B

Explanation

Answer A is wrong because

VACL is an acronym for VLAN Access Control Lists where VLAN stands for Virtual Local Area Network. Specifically created to filter and move VLAN traffic. May be used like a SPAN port or network tap it is a way to replicate computer network data that is coming and going from a computer or a network of computers. This is useful if you want to monitor that traffic to determine the health of the application(s) running on those computer(s) or health of the network itself.

VACL or VACL Ports can be much more discriminating of the traffic they forward than a standard SPAN port. They may be set to only forward specific types or specific VLANs to the monitoring port. However, they forward all traffic that matches the criteria as they do not have the functionality to select from ingress or egress traffic like SPAN ports.

Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations.

Election of the Root Switch

All switches in an extended LAN participating in Spanning-Tree Protocol gather information on other switches in the network through an exchange of data messages. These messages are bridge protocol data units (BPDUs). This exchange of messages results in the following:

- * The election of a unique root switch for the stable spanning-tree network topology.
- * The election of a designated switch for every switched LAN segment.
- * The removal of loops in the switched network by placing redundant switch ports in a backup state.

The Spanning-Tree Protocol root switch is the logical center of the spanning-tree topology in a switched

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

Table C-1: Root Switch Variables Affecting STP

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

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

B is correct because

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

C is wrong because

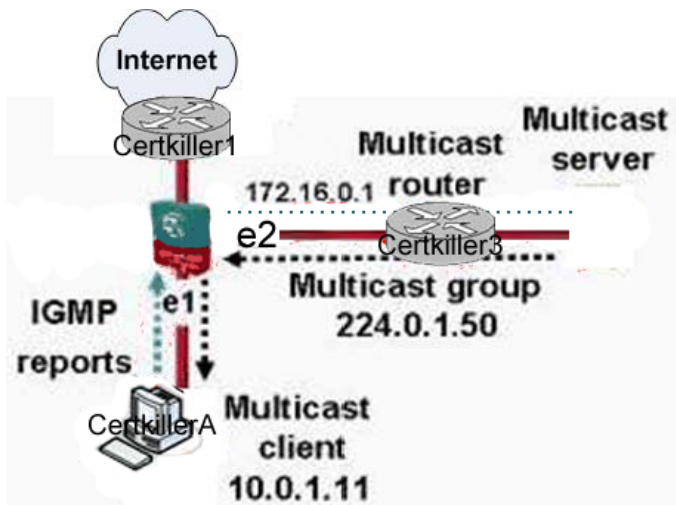
IP source guard is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. You can use IP source guard to prevent traffic attacks caused when a host tries to use the IP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

IP source guard is supported only on Layer 2 ports, including access and trunk ports. You can configure IP source guard with source IP address filtering or with source IP and MAC address filtering.

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

QUESTION 42:

Network Toplogy exhibit:



Certkiller 2 configuration exhibit:

```
Certkiller2(config)# access-list 120 permit udp any 10.0.1.0
255.255.255.0
Certkiller2(config)# interface ethernet2
Certkiller2(config-if)# igmp access-group 120
Certkiller2(config)# interface ethernet1
Certkiller2(config-if)# igmp forward interface dmz
```

You work as a network administrator at Certkiller .com. Please study the exhibit carefully.

Certkiller .com just completed the rollout of IP.TV. The first inside network MC Client to use the new feature claims they can't access the service after re-viewing the above ASA security appliance configuration and network diagram, the administrator was able to determine the following:

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

Answer: A

Explanation

TCP/IP Access Lists

You can have up to 99 Standard IP Access Lists ranging in number from 1 to 99, the Extended IP Access Lists number range is assigned from 100 to 199. The most common use of the Extended IP access list is to create a packet filtering firewall. This is where you specify the allowed destinations of each packet from an allowed source.

UDP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp source source-wildcard [operator [port]]
destination destination-wildcard [operator [port]]
[precedence precedence] [tos tos] [log | log-input]
```

[time-range time-range-name]

In all software releases, the access-list-number can be 101 to 199. In Cisco IOS Software Release 12.0.1, extended ACLs begin to use additional numbers (2000 to 2699). These additional numbers are referred to as expanded IP ACLs. Cisco IOS Software Release 11.2 added the ability to use list name in extended ACLs. The value of 0.0.0.0/255.255.255.255 can be specified as any. After the ACL is defined, it must be applied to the interface (inbound or outbound). In early software releases, out was the default when a keyword out or in was not specified. The direction must be specified in later software releases.

interface

ip access-group {number|name} {in|out}

This extended ACL is used to permit traffic on the 10.1.1.x network (inside) and to receive ping responses from the outside while it prevents unsolicited pings from people outside, permitting all other traffic.

interface Ethernet0/1

ip address 172.16.1.2 255.255.255.0

ip access-group 101 in

access-list 101 deny icmp any 10.1.1.0 0.0.0.255 echo

access-list 101 permit ip any 10.1.1.0 0.0.0.255

igmp access-group

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

igmp access-group acl

no igmp access-group acl

QUESTION 43:

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

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

Answer: D

QUESTION 44:

What security reporting system is analogous to CS-MARS?

- A. Security information management system
- B. Security Reporting and Response System
- C. Security incident Response System
- D. Security Threat Mitigation System

Answer: D

Explanation

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

Security Monitoring for Threat Control

Cisco Security Monitoring, Analysis and Response System (MARS) provides security monitoring for network security devices and host applications made by Cisco and other providers. Security monitoring greatly reduces false positives by providing an end-to-end view of the network, and can increase effective mitigation responses. Other features and benefits of Cisco MARS:

- * "Understands" the configuration and topology of your environment
- * Promotes awareness of environmental anomalies with Network Behavior Analysis using NetFlow
- * Provides quick and easy access to audit compliance reports with more than 150 ready-to-use customizable reports
- * Makes precise recommendations for threat removal, including the ability to visualize the attack path and identify the source of the threat with detailed topological graphs that simplify security response at Layer 2, and above

QUESTION 45:

PEAP provides authentication for the EAP exchange using?

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

Answer: B

Explanation

Protected Extensible Authentication Protocol, Protected EAP, or simply PEAP (pronounced "peep"), is a method to securely transmit authentication information, including passwords, over wired or wireless networks. It was jointly developed by Cisco Systems, Microsoft, and RSA Security. Note that PEAP is not an encryption protocol; as with other EAP types it only authenticates a client into a network.

PEAP uses only server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server. The ensuing exchange of authentication information is then encrypted and user credentials are safe from eavesdropping.

PEAP is a joint proposal by Cisco Systems, Microsoft and RSA Security as an open standard. It is already widely available in products, and provides very good security. It is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication.

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

PEAPv0/EAP-MSCHAPv2

PEAPv1/EAP-GTC

QUESTION 46:

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

- A. The encryption key changes for each packet, resulting in a unique packet for each transmission
- B. The same key is used, but an index vector is used by IPSec to offset the key, resulting in a unique packet for each transmission
- C. The packets will likely be the same except for TTL and the sequence number
- D. A characteristics of 3-DES ensures that no two packets are alike
- E. The only way to ensure that packets are unique to use AH as a header protocol

Answer: B

QUESTION 47:

CSA network shield does which of the following?

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

Answer: E

QUESTION 48:

ASDM on the ASA platform is executed as:

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

Answer: E

QUESTION 49:

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

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

Answer: B,D

QUESTION 50:

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

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

Answer: E

QUESTION 51:

Exhibit:

```
ip inspect name test icmp alert on audit-trail on timeout 30
!
interface Ethernet0
ip address 192.168.10.2 255.255.255.0
ip inspect test in
!
interface Ethernet1
ip address 192.168.20.2 255.255.255.0
ip access-group 101 in
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.20.3
!
access-list 101 deny ip any any
```

You work as a network administrator at Certkiller .com. Please study the exhibit

carefully.

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

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

Answer: A,B,C

QUESTION 52:

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

- A. WebVPN
- B. Rate-Limiting
- C. Support for multiple Virtual firewalls
- D. Transparent Firewall

Answer: B,C,D

QUESTION 53:

What statement is true concerning PAT?

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

Answer: C

QUESTION 54:

In an L2TP voluntary tunneling scenario, the VPDN tunnel is terminated between:

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

Answer: D

QUESTION 55:

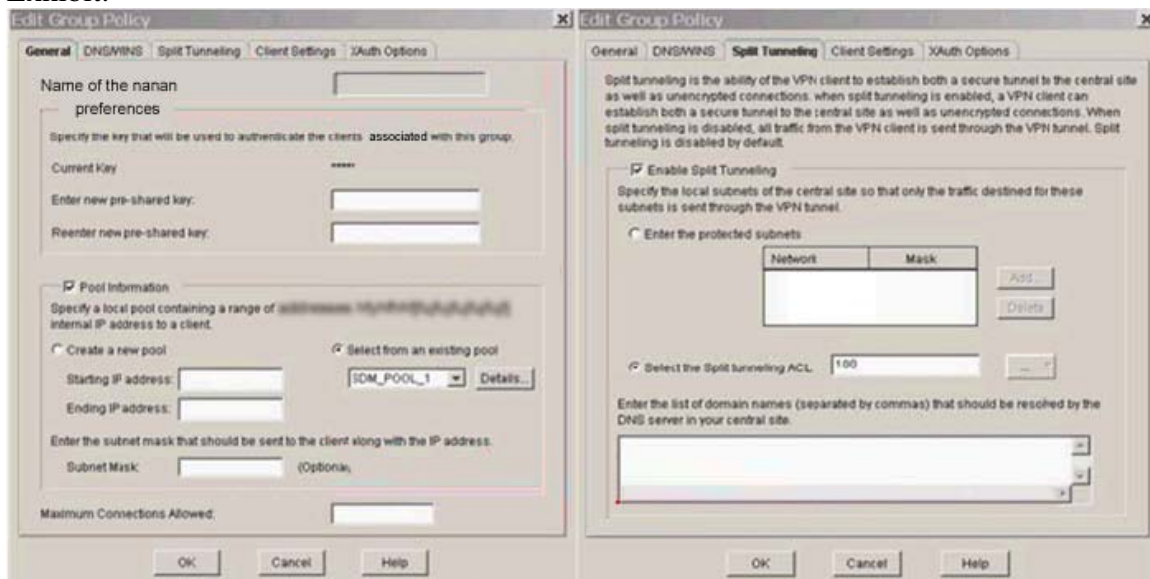
Which access control model provides access to system resources based on the job function of the user or the tasks that the user has been assigned?

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

Answer: C

QUESTION 56:

Exhibit:



You work as a network administrator at Certkiller .com. Please study the exhibit carefully.

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

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

IP Address pool

F. Pre-shared key (PSK) authentication will be used during the X-auth phase

Answer: D,E

QUESTION 57:

How is the ACS server used in the NAC framework?

- A. To autneticate devices based on quarantine information
- B. To authorize devices based on quarantine information
- C. To verify that the device certificates are correct
- D. To verify the virus patch levels

Answer: A

QUESTION 58:

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

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

Answer: B,C,E

QUESTION 59:

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

- A. 224.21.206.44
- B. 224.25.106.44
- C. 223.149.106.44
- D. 236.25.106.44
- E. 239.153.106.44

Answer: A,C

QUESTION 60:

TFTP security May be controlled by: (multiple answer)

- A. A username/password
- B. A default TFTP directory
- C. A TFTP directory
- D. A TFTP file
- E. A pre-existing file on the server before it will accept a put
- F. File privileges

Answer: E, F

QUESTION 61:

Which of the following controls TFTP security? (Choose all that apply.)

- A. A default TFTP directory.
- B. A username/password.
- C. A TFTP file.
- D. A pre-existing file on the server before it will accept a put.
- E. File privileges.

Answer: A, 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 solarwinds will download the running config via tftp and make the file

QUESTION 62:

Which of the following is a well known port commonly used for TFTP?

- A. TCP 23
- B. UDP 69
- C. UDP 23
- D. UDP 161

Answer: B

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 63:

Why would you advise the new Certkiller trainee technician NOT to use TFTP with authentication?

- A. TFTP makes use of UDP as transport method.
- B. A server initiates TFTP.
- C. TFTP protocol has no hook for a username/password.
- D. TFTP is already secure.
- E. All of the above.

Answer: C

Explanation: FTP requires a username and password. TFTP does not.

QUESTION 64:

What does the TFTP protocol do?

- A. TFTP protocol makes use of the UDP transport layer and requires user authentication.
- B. TFTP protocol makes use of the TCP transport layer and does not require user authentication.
- C. TFTP protocol makes use of the UDP transport layer and does not require user authentication.
- D. TFTP protocol makes use of TCP port 69.
- E. TFTP protocol makes 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 65:

Which statements about FTP are true? Select two.

- A. FTP always uses two separate TCP sessions - one for control and one for data.
- B. With passive mode FTP, both the control and data TCP session are initialed from the client.

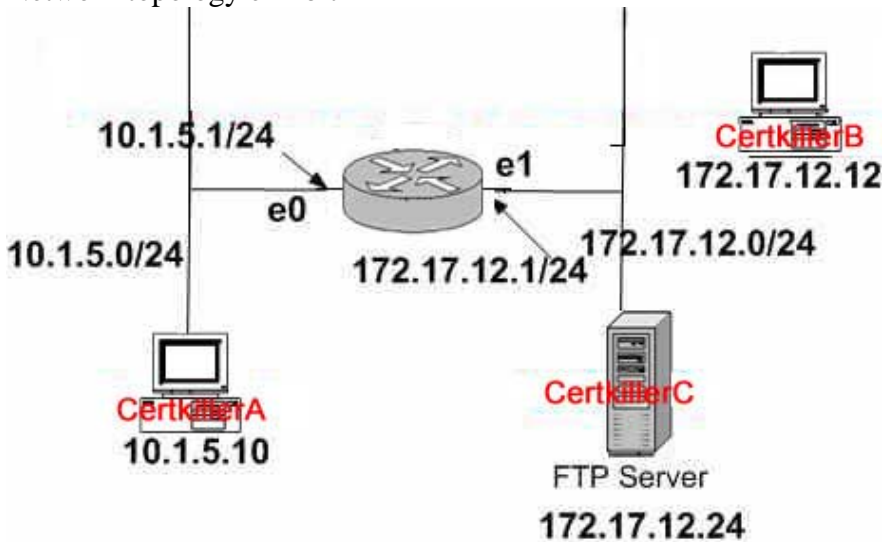
- C. With active mode FTP, the server the "PORT" command to tell the client on which port it wishes to send and data.
- D. For both active and passive mode FTP, the control session on the server always TCP port 21, and the data session

Answer: A, B

Not C: It is not the server who send 'PORT' command to client, but the reverse.

QUESTION 66:

Network topology exhibit



Symptoms:

1. Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
 2. Console login: level warnings, 0 messages logged
 3. Monitor logging: level informational, 0 messages logged
 4. Buffer logging: level informational, 0 messages logged
 5. Trap login: level informational, 0 message lines logged
- Note: Router Certkiller 1's CPU is normally about 25 busy switching packets

Scenario:

Host Certkiller A cannot reach the Certkiller C FTP Server, but can reach Host Certkiller B. The network administrator suspects that packets are traveling from network 10.1.5.0 to the Certkiller C FTP Server, but packets are not returning. The administrator logs in to console part of Router Certkiller 1. When Host Certkiller A sends a ping to the Certkiller C FTP Server, the administrator executes a "debug ip packet" command on the router.

The administrator does not see any output, what additional commands could be used to see the packet flowing from Ethernet 0 to Ethernet 1?

- A. terminal monitor
- B. configure terminal
- logging console debug

interfaces ethernet 1
no ip route-cache
C. configuring terminal
logging console debug
D. configure terminal
no logging buffered
E. configure terminal
interface ethernet0
no ip route-cache

Answer: B

QUESTION 67:

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

There are two type of connections used with FTP, a control connection and a data connection. A single control connection is established when the client initiates an FTP session. The control connection is then maintained and used to send commands and receive response messages. When data needs to be transfered (such as when a file is uploaded or downloaded, or when a directory listing is requested) a data connection is opened, used for the transfer, and then closed. If the data connection is blocked, the directory listing will fail.

QUESTION 68:

When building a non-passive FTP data connection, the FTP client:

- A. Indicates the port number to be use 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 send data from
- C. Uses port 20 for establishing the command channel and port 21 for the data channel
- D. Initiates the connection form an ephemeral port to the RFC specified port of the server

Answer: A

In active (non-passive) mode FTP the client connects from a random unprivileged port (N

> 1024) to the FTP server's command port, port 21. Then, the client starts listening to port N+1 and sends the FTP command PORT N+1 to the FTP server. The server will then connect back to the client's specified data port from its local data port, which is port 20.

QUESTION 69:

The Certkiller network administrator is troubleshooting a problem with FTP services. What will the administrator encounter if a device blocks the data connection?

- A. The administrator will experience very slow connect times.
- B. Incomplete execution, when issuing commands like "pwd" or "cd".
- C. User login problems will occur.
- D. Failure when listing a directory.
- E. No problems at all.

Answer: D

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 70:

What role does the FTP client play when building a non-passive FTP data connection?

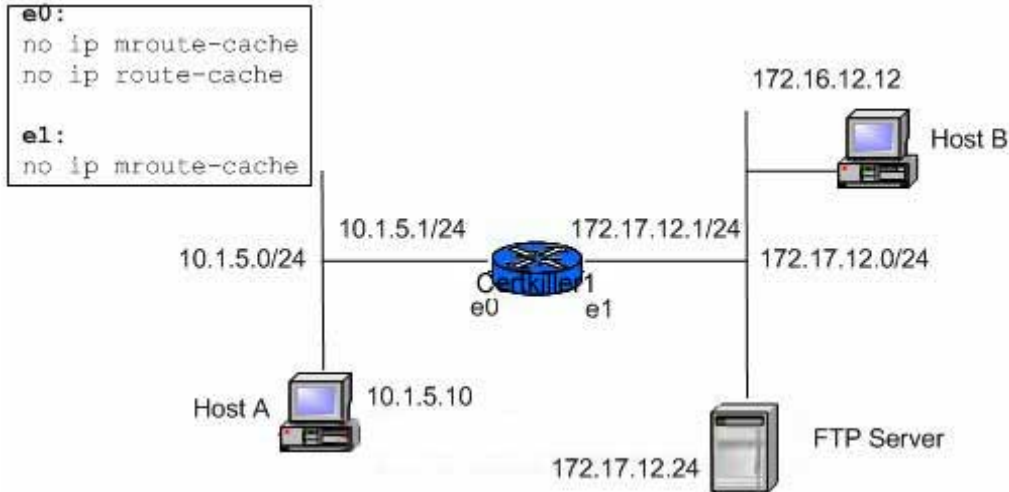
- A. The FTP client indicates the port number to be used for sending data over the command channel via the PORT command.
- B. The FTP client receives all data on port 20, the same port the FTP server daemon sends data from.
- C. The FTP client makes use of port 20 for establishing the command channel and port 21 for the data channel.
- D. The FTP client initiates the connection from an ephemeral port to the RFC specified port of the server.

Answer: A

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 21 on the server. This is referred to as the command channel. Cisco Secure PIX firewall Advanced 2.0 10-5

QUESTION 71:

Exhibit:



Symptoms:

- Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
- Console logging: level debugging, 0 messages logged
- Monitor logging: level informational, 0 messages logged
- Buffer logging: level informational, 0 messages logged
- Trapp Logging: level informational, 0 messages lines logged

Note: Router Certkiller 1's CPU is normally about 25% busy switching packets:

Scenario:

Host A is unable to reach the FTP Server, but can reach Host B. The Certkiller network administrator has a suspicion that packets are travelling from network 10.1.5.0 to the FTP Server, but not returning. The administrator logs into the console port of Router Certkiller 1. When Host A sends a ping to the FTP Server, the administrator executes a "debug ip packet" command on the router.

However during debugging, the administrator observes far too much output.

Which additional commands should the administrator use to limit the debug output in order to view ONLY host A's bi-directional ICMP ping packets? (Select 2 to 5 answers.)

A. configure terminal

access-list 101 permit icmp 10.1.5.10 0.0.0.0 172.17.12.24 0.0.0.0

access-list 101 permit icmp 172.17.12.24 0.0.0.0 10.1.5.10 0.0.0.0

B. no debug ip packet
debug ip icmp 101
C. debug ip packet 101
D. configure terminal
interface ethernet 1
no ip route-cache
E. configure terminal
access-list 101 permit ip 10.1.5.0 .0.0.0.255 172.17.12.0 0.0.0.255
access-list 101 permit ip 172.17.12.0 0.0.0.255 10.1.5.0 0.0.0.255

Answer: A, C

QUESTION 72:

Why is ICAP (Internet Content Adaption Protocol) significant from a security standpoint?

- A. ICAP removes harmful code from HTTP transaction.
- B. ICAP forwards HTTP content to an AV server for malicious code removal.
- C. ICAP is used to authenticate content based on a SSL certificate.
- D. ICAP processes running on cache devices act as application level IDS agents.

Answer: B

QUESTION 73:

Which describe a service that would be flagged as necessary and enabled by SDM?

- A. Password encryption service
- B. SNMP
- C. FTP
- D. SSH
- E. TELNET

Answer: A

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_chapter09186a00802d4895.htm

QUESTION 74:

Certkiller has just selected IPSec to protect its IP traffic traveling on the Internet. They also have decided to use certificates from a public CA vendor that supports

Simple Certificate Enrollment Protocol (SCEP).

What default port must be open in the firewall to allow the SCEP traffic?

- A. IP Protocol 50 and 51
- B. TCP 2002
- C. TCP 80
- D. UDP 500
- E. UDP 80

Answer: C

In the SCEP protocol, HTTP is used as the transport protocol for the PKI messages.

Reference:

http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm

Note: same answer would be true for CEP.

QUESTION 75:

Some packet filtering implementations block Java by finding the magic number 0xCAFEBABE at the beginning of documents returned via HTTP.

The newly appointed Certkiller trainee technician want to know how this Java filter be circumvented. What will your reply be?

- A. By using FTP to download using a web browser.
- B. By using Gopher.
- C. By using Java applets in zipped or tarred archives.
- 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 PORT AND 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 Internetwork Expert Security Exam v1.7 by John Kaberna pg 404

QUESTION 76:

The SSL protocol provides "channel security," but lacks what property?

- A. A private channel. Encryption is used for all messages after a simple handshake is used to define a secret key.
- B. An authenticated channel. The server endpoint of the conversation is always authenticated, while the client endpoint is optionally authenticated.
- C. A reliable channel. The message transport includes a message integrity check (using a MAC).
- D. An independent authentication where each transmission requires authentication by the server endpoint.

Answer: D

From the SSL 2.0 Protocol Specification:

The SSL protocol provides "channel security" which has three basic properties:

- * The channel is private. Encryption is used for all messages after a simple handshake is used to define a secret key.
- * The channel is authenticated. The server endpoint of the conversation is always authenticated, while the client endpoint is optionally authenticated.
- * The channel is reliable. The message transport includes a message integrity check (using a MAC).

QUESTION 77:

Besides Kerberos port traffic, what additional service does the router and the Kerberos server use in implementing Kerberos authentication on the router?

- A. TCP
- B. Telnet
- C. DNS
- D. FTP
- E. ICMP
- F. None of the above.

Answer: C

Explanation: They will need to use DNS unless the router is hard coded with the IP address of the server.

Note: Kerberos authentication requires that NTP is enabled. Additionally, we recommend that you enable DNS.

Not B:

The question is: What ADDITIONAL service does the router and the Kerberos server use. They do not USE the TELNET service during authentication.

QUESTION 78:

What is the default port(s) used for web-based SSL (Secure Socket Layer) Communication?

- A. TCP and UDP 1025.
- B. TCP and UDP 443.
- C. TCP 80.
- D. TCP and UDP 1353.

Answer: B

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 80 requests 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 79:

The Diffie-Hellman key exchange allows two parties to establish a shared secret key: (Select all that apply)

- A. Over an insecure medium
- B. After a secure session has been terminated
- C. Before a secure session has been initiated
- D. During a secure session over a secure medium

Answer: A, B, C

QUESTION 80:

Which of the following SMTP command has the ability to identify the SMTP client to the SMTP server?

- A. IDENT
- B. SEND
- C. HELLO
- D. HELO
- E. MAIL

Answer: D

QUESTION 81:

Which of the following protocols can be authenticated? (Choose all that apply.)

- A. TFTP
- B. Telnet
- C. HTTP
- D. FTP
- E. SMTP

Answer: B, C, D, E

Explanation:

C: HTTP can be authenticated, please refer to: -

RFC 2617 HTTP Authentication: Basic and Digest Access Authentication

QUESTION 82:

Which of the following commands can be issued to test to see if SMTP mail is operational on a remote host? Select all that apply.

- A. 'telnet remote_host 109' and issue the 'helo' command.
- B. 'telnet remote_host 110' and issue the 'helo' command.
- C. 'telnet remote_host 25' and issue the 'helo' command.
- D. 'telnet remote_host 25' and issue the 'esmtpl' command.

Answer: C

QUESTION 83:

An NTP server will NOT be synchronized by a peer in which modes? (Select two.)

- A. Server mode
- B. Peer mode
- C. Broadcast/Multicast mode
- D. Client mode

Answer: A, C

Server Mode--By operating in server mode, a host (usually a LAN time server) announces its willingness to synchronize, but not to be synchronized by a peer. This type of association is ordinarily created

upon arrival of a client request message and exists only in order to reply to that request, after which the association is dissolved. Server mode is a passive mode.

Client Mode--By operating in client mode, the host (usually a LAN workstation) announces its willingness to be synchronized by, but not to synchronize the peer. A host operating in client mode sends periodic messages regardless of the reachability or stratum of its peer. Client mode is an active mode.

Peer Mode--By operating in peer mode (also called "symmetric" mode), a host announces its willingness to synchronize and be synchronized by other peers. Peers can be configured as active (symmetric-active) or passive (symmetric-passive).

Broadcast/Multicast Mode--By operating in broadcast or multicast mode, the host (usually a LAN time server--operating on a high-speed broadcast medium) announces its willingness to synchronize all of the peers, but not to be synchronized by any of them. Broadcast mode requires a broadcast server on the same subnet, while multicast mode requires support for IP multicast on the client machine, as well as connectivity via the MBONE to a multicast server. Broadcast and multicast modes are active modes.

QUESTION 84:

- 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.
- What do you expect to happen when User_A tries to edit D:\data\word.doc given the above scenario on a Windows NT 4.0 network?

- A. User_A has full control and can edit the document successfully.
 - B. Insufficient information. Permissions for Microsoft Word are set within the application and are not subject to file and share level permissions.
 - C. Edit access would be denied.
- The "Read" permission is least permissive so it would apply in this situation.
- D. Access would be denied.
 - E. Global groups can not be placed into local groups.
- Only the owner of a file can edit a document.
- The situation could not exist.

Answer: A

QUESTION 85:

- 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 "No Access".
- 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.

What do you expect to happen when User_A tries to edit D:\data\word.doc given the above scenario on a Windows NT 4.0 network?

- A. User_A has full control and can edit the document successfully.
 - B. Insufficient information. Permissions for Microsoft Word are set within the application and are not subject to file and share level permissions.
 - C. Edit access would be denied.
- The "Read" permission is least permissive so it would apply in this situation.
- D. Access would be denied.
 - E. Global groups can not be placed into local groups.
- "No access" overrides all other permissions, unless the file is owned by the user.
- The situation could not exist.

Answer: D

QUESTION 86:

Exhibit:

```
FastEthernet0 is up, line protocol is up
Hardware is DEC21140, address is 00e0.1ea8.e299 (bia 00e0.1ea8.e299)
Description: Ethernet 100Mbps
Internet address is 1.1.1.1 /22
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 3/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
Half-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 1.1.1.1 /22 1500 bytes, BW 100000 Kbit
5 minute output 00:00:00, output 00:00:00, out 1.1.1.1 /22
47250970 packets input, 3285704002 bytes, 0 no buffer
Received 257038 broadcasts, 1056 runts, 0 giants, 0 throttles
1718 input errors, 662 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast
311 input packets with dribble condition detected
46168848 packets output, 3093573182 bytes, 0 underruns
0 output errors, 958 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
```

What statement is true regarding the following output of the show interface Fast Ethernet0 command?

- A. The interfaces is operating in 100mb Full duplex.
- B. There is a high rate of collisions recorded on the interface.
- C. There is a physical problem with the connection since there are recorded Runls and CRCs.
- D. Collisions, runts and CRC's are normal for a 100mb half-duplex connection.

Answer: D

QUESTION 87:

What effect do these configuration commands have?
Line vty 0 4
No login
Password cisco

- A. The VTY password is cisco
- B. The login password is login
- C. The VTY password is required but not set
- D. No password is required for VTY access

Answer: D

To enable password checking at login, use the login command in line configuration mode. To disable password checking and allow connections without a password, use the no form of this command.

QUESTION 88:

Of the following which can be identified as valid host IP addresses on the Internet?
(Choose all that apply.)

- 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 89:

What would be the consequence that all the other nodes would experience when a jam signal causes a collision on an Ethernet LAN?

- A. All other nodes will recognize the collision and all nodes should stop sending new data.
- B. All other nodes will compute part of a hash algorithm 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." WOULD SEEM 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 $\{0, \dots, 2^k - 1\}$ at random where k = number of collisions. This means k is initialized to 1 and 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 90:

Exhibit:

Router A:	Router B:
<pre>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 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 access-list 106 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255</pre>	<pre>crypto isakmp policy 4 authentication pre-share crypto isakmp key xxxxxx1234 address 100.232.202.210 crypto ipsec transform-set encrypt-des esp-des crypto map ipsecmap 7 ipsec-isakmp set peer 100.232.202.210 set transform-set encrypt-des match address 106 interface Serial0 ip address 100.228.202.154 255.255.255.252 crypto map ipsecmap interface FastEthernet0 ip address 192.168.2.1 255.255.255.0 ip classless ip route 0.0.0.0 0.0.0.0 100.228.202.153 ip route 192.168.1.0 255.255.255.0 100.228.202.153 access-list 106 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255</pre>

How will IP traffic from the clients typically behave between the two Ethernet subnets?

- A. Traffic between the Ethernet subnets on both routers will have to be decrypted.
- B. NAT will translate the traffic between the Ethernet subnets on both routers.
- C. Traffic will successfully access the Internet, though it will have to be decrypted between the router's Ethernet subnets.
- 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.
- F. Traffic bound for the Internet will eventually be dropped.

Answer: C

Explanation:

NOT ENOUGH OF THE EXHIBIT TO MAKE A REAL CHOICE. THE EXHIBIT IS ONE OF IPSEC TAKE YOUR BEST SHOT.

QUESTION 91:

What configuration command could be used to restrict SNMP access to a router?

- A. snmp-server public
- B. snmp-server password
- C. snmp-server community
- D. snmp-server host

Answer: C

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 92:

IEEE 802.1D describes a method to prevent the disconnection of a single end station from disrupting Spanning tree. What does the method describe?

- A. Re-setting the Topology Change flat to aero (0)
- B. Disabling the 801.1D Change Detection parameter
- C. Configuring the BridgeForwardDelay to 1/2 of the BridgeMaxage
- D. Using the BridgeForwardDelay timer to age out dynamic entries

Answer: D

QUESTION 93:

What does the term "slow start" mean in reference to TCP?

- A. This is a method of adjusting timers after detecting a network error.
- B. It is poor performance early in the TCP session, caused by setup overhead.
- C. It is a bug that caused poor Ethernet performance for short sessions in some early UNIX TCP/IP implementations.
- D. It is possible long latency between the time a connection request is made and the time a server is actually ready to respond to the request.
- E. The TCP window is set very low and increase slowly after the handshake.

Answer: E

QUESTION 94:

Exhibit:

10.1.1.0/24

10.1.3.0/24

10.1.14.64/26

10.1.5.192/30

Given the four networks listed, what valid summary address (below) contains the longest prefix?

A. 10.1.0.0/20

B. 10.1.0.0/16

C. 10.0.0.0/23

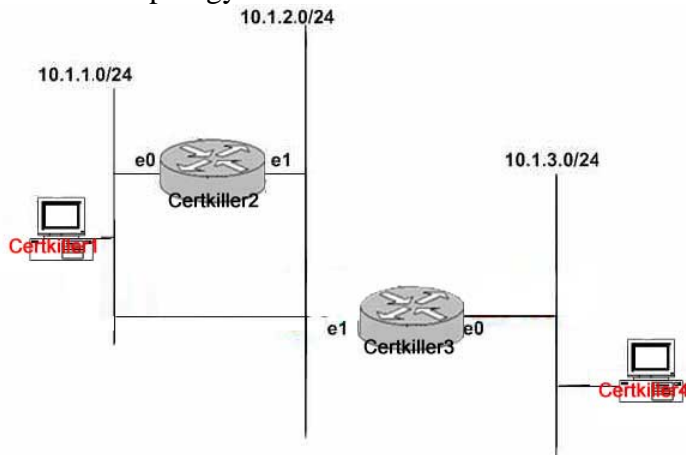
D. 10.1.16.0/19

E. These networks cannot be summarized.

Answer: A

QUESTION 95:

Network Topology Exhibit:



Host Certkiller 1 is attempting to send a packet through Router Certkiller 2 to Host Certkiller 4. there are no routing protocols configured nor are there any static routes for Router Certkiller 2 or Router Certkiller 2. However, Router Certkiller 2 does have a default-gateway configured to the IP address of Router Certkiller 3 using the configuration ip default-gateway 10.0.2. Will Host Certkiller 1's packet reach Host Certkiller 4?

A. This will work if the router are configured to bridge.

- B. This will work because Router Certkiller 2 will forward the packets destined to 10.1.3.0/24 to Router Certkiller 3 through its IP default-gateway configuration.
- C. The packets will reach Host Certkiller 4, but Host Certkiller 4 will not be able to communicate back to Host Certkiller 1, 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 Certkiller 1's packets will never reach Router Certkiller 3 or Host Certkiller 4.

Answer: E

By exclusion:

- A. This will not work if the routers are configured to bridge because the ip addresses are on a different subnet, and the Host Certkiller 4 will not respond to the arp request.
- B. IP default gateway will only send packets to that ip address for packets created locally on the router.
- C. The packets will not "reach" the network card unless bridging is enabled, but the host will ignore them because they are in a different subnet. See A.
- D. see potsmokers.com

QUESTION 96:

Exhibit:

Host Certkiller1	<table><tr><th>WINDOW</th><th>ACK</th><th>SEQUENCE</th><th>Bytes sent</th></tr><tr><td>512</td><td>38177</td><td>90708</td><td>1024</td></tr></table>	WINDOW	ACK	SEQUENCE	Bytes sent	512	38177	90708	1024
WINDOW	ACK	SEQUENCE	Bytes sent						
512	38177	90708	1024						
Host Certkiller1	<table><tr><th>WINDOW</th><th>ACK</th><th>SEQUENCE</th><th>Bytes sent</th></tr><tr><td>1024</td><td>90708</td><td>38177</td><td>512</td></tr></table>	WINDOW	ACK	SEQUENCE	Bytes sent	1024	90708	38177	512
WINDOW	ACK	SEQUENCE	Bytes sent						
1024	90708	38177	512						
Host Certkiller1	<table><tr><th>WINDOW</th><th>ACK</th><th>SEQUENCE</th><th>Bytes sent</th></tr><tr><td>2048</td><td>?</td><td>?</td><td>1024</td></tr></table>	WINDOW	ACK	SEQUENCE	Bytes sent	2048	?	?	1024
WINDOW	ACK	SEQUENCE	Bytes sent						
2048	?	?	1024						

Hosts Certkiller 1 and Certkiller 2 are communicating using TCP. A packet is sent from Certkiller 1 to Certkiller 2, Certkiller 2 replies back to Certkiller 1, and Certkiller 1 acknowledges Certkiller 2's reply. Selected information from this dialogue is shown. Based on the information, predict the correct values for the final acknowledgement from Certkiller 1:

- A. Ack=38689 Seq=91734
- B. Ack=38689 Seq=91732
- C. Ack=38700 Seq=71633
- D. Ack=38690 Seq=91733

Answer: D

QUESTION 97:

What response will a RADIUS server send to a client to indicate the client's user name or password is invalid?

- A. Authentication Denied
- B. Access-Reject
- C. Access-Deny
- D. Access-Fasil
- E. ERROR

Answer: B

The Access-Reject message is sent when any of the values offered by the NAS to AAA server are unacceptable to the AAA server

Reference:

Page 519, Network Security and Principle and Practices, Cisco press

QUESTION 98:

What does the established keyword in an extended access-list do?

- A. Applies to access-list to an interface.
- B. Matches established TCP connection packets.
- C. Requires a connection to be established before an access list can be applied.
- D. Matches if the TCP datagram has the acknowledgement (ACK) or reset (RST) bits set.

Answer: D

QUESTION 99:

Which best describes a common method used for VLAN hopping?

- A. Using VTP to configure a switchport to sniff all VLAN traffic
- B. Appending an additional tag to an 802.1Q frame such that the switch forwards to packet to the embedded VLAN ID
- C. Flooding the VLAN with traffic containing spoofed MAC addresses in an attempt to cause the CAM table to overflow
- D. Spoofing the IP address of the host to that of a host in the target VLAN

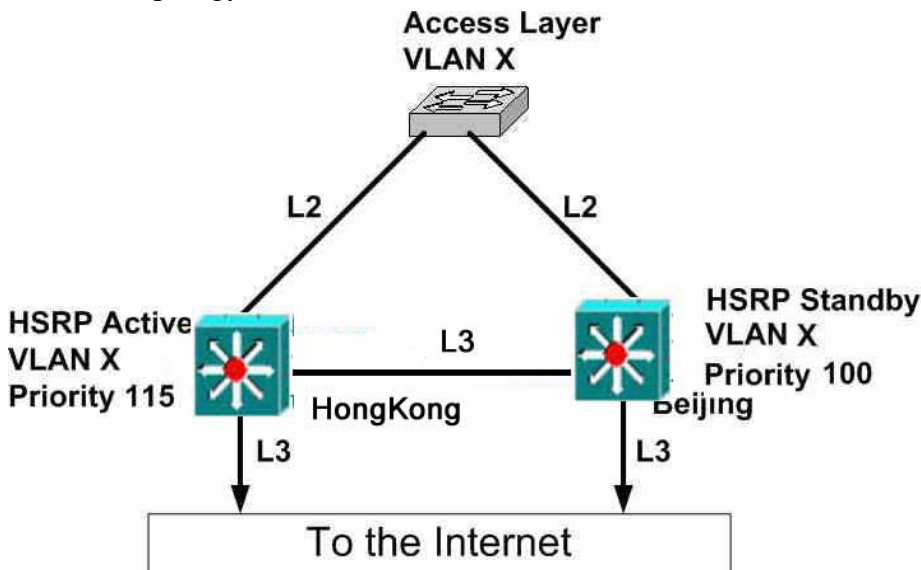
Answer: B

The double encapsulated VLAN hopping attack takes advantage of the way the

hardware on most switches operates. Most switches today perform only one level of IEEE 802.1Q decapsulation. This allows an attacker, in specific situations, to embed a hidden .1Q tag inside the frame, allowing the frame to go to a VLAN that the outer .1Q tag did not specify.

QUESTION 100:

Network topology exhibit:



When both L3 links in the HongKong switch fail, all users assigned to VLAN X in the Access Layer switch cannot reach the internet. What would be the best command to fix this problem?

- A. standby track
- B. standby timer
- C. standby authentication
- D. standby use-bia
- E. standby preempt

Answer: A

Standby track should be on Hong Kong, but standby preempt should be on Beijing

My guess would be A since the rest of the question is asked from the view of the Hong Kong switch.

The standby track command allows you to specify another interface on the router for the HSRP process to monitor in order to alter the HSRP priority for a given group. If the specified interface's line protocol goes down, the HSRP priority is reduced. This means that another HSRP router with higher priority can become the active router if it has standby preempt enabled.

QUESTION 101:

What statement is correct regarding Virtual LANs (VLANs)?

- A. It is permissible to bridge inside a VLAN, but not to route between VLANs.
- B. It is not permissible to bridge inside a VLAN, but it is valid to route between VLANs.
- C. It is permissible to bridge inside a VLAN, and to route between VLANs,
- D. It is not permissible to bridge inside or route between VLANs.

Answer: C

QUESTION 102:

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

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

Answer: B

QUESTION 103:

PGP can be used for:

- A. Authenticating an email origin.
- B. Routing when exchanging large numbers of routers.
- C. Installing new software onto a router.
- D. File transfer.
- E. Encrypting a Telnet session.

Answer: A

QUESTION 104:

What is the primary benefit of the "time-to-live" field in the IP header?

- A. To improve buffer utilization.

- B. To reduce the impact of routing loops.
- C. To allow calculation of round-trip delays.
- D. To remind us that all earthly jors are fleeting.
- E. To avoid delivery of packets that are no longer useful.

Answer: B

QUESTION 105:

A new Catalyst switch is in a lab. It is decided that a download of the latest supervisor image is needed, so the switch is connected to the corporate Catalyst switch in the lab through the supervisor gigabit ports that are both in VLAN 100 with a single fiber pair. VLAN 100 only existed on the two supervisor ports used and only one router existed on that VLAN. Shortly thereafter thousands of complaints are received that users cannot connect to anything on the network. What command should have been issued on the lab switch prior to connecting to the corporate switch to prevent this problem?

- A. clear cam dynamic
- B. set spantree uplinkfast enable 1/1
- C. set trunk 1/1 desirable isl
- D. set vtp mode transparent
- E. set port broadcast 1/1 25% unicast enable

Answer: D

QUESTION 106:

After adding a new switch to the network it is determined that it is not automatically learning the VLANs via VTP. What most likely the cause?

- A. The other switch is a VTP client.
- B. The VTP server has not sent out a peridoci VTP advertisement.
- C. There are not yet users on the new switch.
- D. The native VLAN on the trunk is VLAN 60.
- E. The VTP domain name is misconfigured.

Answer: E

QUESTION 107:

What functionality best defines the use of a 'stub' area within an OSPF

environment?

- A. A stub area appears only on remote areas to provide connectivity to the OSPF backbone.
- B. A stub area is used to inject the default route for OSPF.
- C. A stub area uses the no-summary keyword to explicitly block external routes, defines the non-transit area, and uses the default route to reach external networks.
- D. A stub area is used to reach networks external to the sub area.

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 108:

Which of the following statements regarding RIP v1 is valid? (Choose all that apply.)

- A. RIP v1 is a classful routing protocol.
- B. RIP v1 is incapable of carrying subnet information in its routing updates.
- C. RIP v1 is incapable of supporting Variable Length Subnet Masks (VLSM).
- D. RIP v1 can support discontinuous networks.

Answer: A, B, C

Explanation: RIP and IGRP are classful protocols

Why Doesn't RIP or IGRP Support Discontinuous Networks?

QUESTION 109:

Which of the following types of traffic is NOT subject to inspection in the IOS Firewall Feature Set?

- A. ICMP
- B. FTP

- C. TFTP
- D. SMTP

Answer: A

Explanation: CBAC-Supported applications (Deployable on a modular basis):
CBAC is available only for IP protocol traffic. Only TCP and UDP packets are inspected.
Other IP
traffic, such as ICMP, cannot be inspected with CBAC and should be filtered with basic
access
lists instead..

QUESTION 110:

Exhibit:

S* 0.0.0.0/0 [1/0] via 172.31.116.65

D 172.16.0.0/24 [90/48609] via 10.1.1.1

R 172.16.0.0/16 [120/4] via 192.168.1.4

What will you encounter when a router has the above routers listed in its routing
table and receives a packet destined for 172.16.0.45.?

- 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 172.31.116.65, since it has the lowest
administrative distance.
- D. The router will forward the packet through 10.1.1.1.
- E. The router will forward the packet through 192.168.1.4.

Answer: D

Explanation: C= 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 dont
match the other routes is to be forwarded to 172.31.116.65

QUESTION 111:

Why should a Route Reflector be used in a BGP environment?

- A. Route Reflector is used to overcome issues of split-horizon within BGP.
- B. Route Reflector is used to reduce the number of External BGP peers by allowing
updates to reflect without the need to be fully meshed.
- C. Route Reflector is used to allow the router to reflect updates from one Internal BGP
speaker to another without the need to be fully meshed.

- D. Route Reflector is used to divide Autonomous Systems into mini-Autonomous Systems, allowing the reduction in the number of peers.
- 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 112:

What reaction can be expected from the host when a router sends an ICMP packet, with the Type 3 (host unreachable) and Code 4 (DF bit set) flags set, back to the originating host?

- A. The host should reduce the size of future packets it may send to the router.
 - B. This scenario is not possible because the packet will be fragmented and sent to the original destination.
 - C. The sending station will stop sending packets, due to the router not expecting to see the DF bit in the incoming packet.
 - D. The sending station will clear the DF bit and resend the packet.
 - 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: A

Explanation: There must have been a reason the host set the DF flag to begin with. A router tries to forward an IP datagram, with the DF bit set, onto a link that has a lower MTU than the size of the packet, the router will drop the packet and return an Internet Control Message Protocol (ICMP) "Destination Unreachable" message to the source of this IP datagram, with the code indicating "fragmentation needed and DF set" (type 3, code 4). When the source station receives the ICMP message, it will lower the send MSS, and when TCP retransmits the segment, it will use the smaller segment size.

QUESTION 113:

Which of the following statements regarding Routing Information Protocol (RIP) is valid?

- A. RIP runs on TCP port 520.
- B. RIP runs directly on top of IP with the protocol ID 89.
- C. RIP runs on UDP port 520.
- D. RIP does not run on top of IP.

Answer: C

QUESTION 114:

A Certkiller security System Administrator is reviewing the network system log files. He notes the following:

- Network log files are at 5 MB at 12:00 noon.
- At 14:00 hours, the log files at 3 MB.

What should he assume has happened and what should he do about the situation?

- A. He should contact the attacker's ISP as soon as possible and have the connection disconnected.
- B. He should log the event as suspicious activity, continue to investigate, and take further steps according to site security policy.
- C. He should log the file size, and archive the information, because the router crashed.
- D. He should run a file system check, because the Syslog server has a self correcting file system problem.
- E. He should disconnect from the Internet discontinue any further unauthorized use, because an attack has taken place.

Answer: B

Explanation:

This question is 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 Internetwork Expert Security Exam V1.7/Vconsole update questions by John Kaberna See ccbootcamp.com

QUESTION 115:

Exhibit:

10.1.1.0/24 through OSPF
10.1.0.0/16 through EIGRP
10.1.0.0&16 static

Which one of the routers would forward a packet destined for 10.1.1.1 if a router had the three routers listed?

- A. 10.1.0.0/16 through 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: The answer is C because the longest match is always chosen, regardless of the AD of shorter match routes. This is true regardless of what routing protocols are running on the router. If EIGRP had a route definition of /24 here, it would be chosen because the longest match criteria would be the same as OSPF, and EIGRP has the lower (better) AD.

QUESTION 116:

You are the network administrator at Certkiller . The Certkiller network is using two remote LANs that are 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. How will you be able to ameliorate this situation?

- A. Change the hop count on an alternate path to be the same cost.
- B. Reduce or disable the holddown timer through the timersbasic command.
- C. Increase the bandwidth of the alternate serial connection.
- D. Configure a static route with an appropriate administrative cost, via the alternate route.

Answer: B

QUESTION 117:

What is the reason why file level permissions are not available with Windows 95 shares?

- A. Windows 95 is a 16-bit operating system and file level permissions require a 32-bit

operating system.

- B. Windows 95 machines use FAT partitions and they cannot be upgraded to VFAT which is the NT format.
- C. Windows 95 machines is incapable off being configured as network share points.
- D. NTFS is not supported in Windows 95 and File level permissions are only available on NTFS partitions.
- E. None of the above; File level permissions are configurable only by going to the file properties and selecting "Permissions" on the "Security" tab.

Answer: D

QUESTION 118:

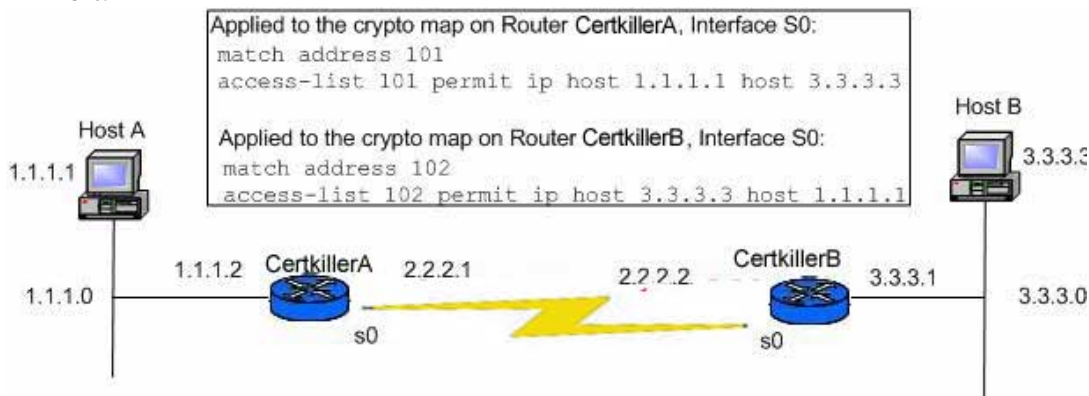
A router learns about an IP network via RIP and OSPF.
What mechanism is used for the selection of the preferred route?

- A. Default metrics
- B. Routing priority
- C. Type of service
- D. Lambic pentameter
- E. Administrative distance

Answer: E

QUESTION 119:

Exhibit:



Given the above IPSec scenario which of the following best describes the behavior of the network traffic?

- A. All traffic between networks 1.1.1.X and the 3.3.3.X will be blocked, except for traffic between hosts 1.1.1.1 and 3.3.3.3.
- B. Traffic between networks 1.1.1.X and 3.3.3.X will flow unencrypted, except for traffic between hosts 1.1.1.1 and 3.3.3.3.

These are the tunnel end points and all traffic between these devices will be encrypted.
C. Most traffic between networks 1.1.1.X and 3.3.3.X will flow unencrypted.
However, the traffic between hosts 1.1.1.1 and 3.3.3.3 will be encrypted on the segment between 2.2.2.1 and 2.2.2.2.
D. Traffic between 1.1.1.1 and 2.2.2.1 will be encrypted, as well as the traffic between 2.2.2.2 and 3.3.3.3.

Answer: C

C is the most appropriate answer.

Not B: Router Certkiller A and Router Certkiller B are the tunnel end points.

QUESTION 120:

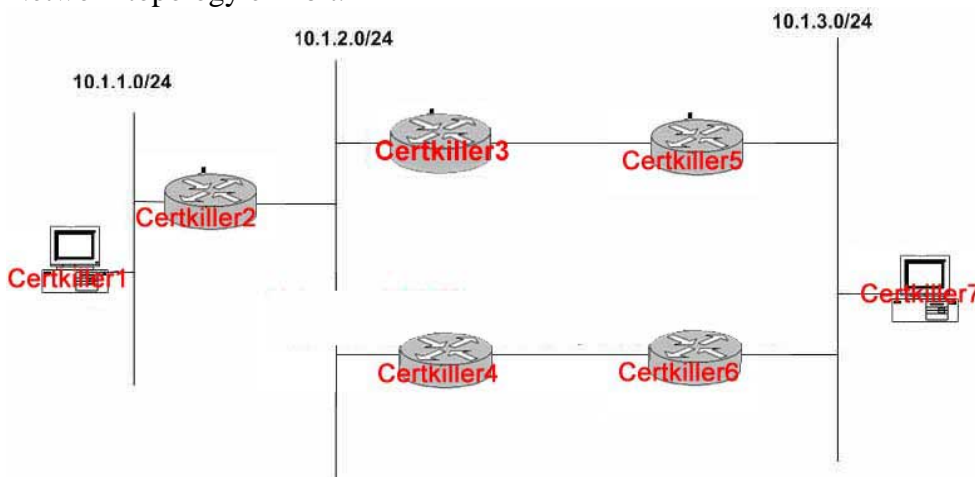
Which of the following represents the correct ways of releasing IBGP from the condition that all IBGP neighbors need to be fully meshed? (Choose all that apply.)

- A. Configure route reflectors
- B. Configure IBGP neighbors several hops away
- C. Configure confederations
- D. Configure local preference

Answer: A, C

QUESTION 121:

Network topology exhibit.



In this diagram, Host Certkiller 7 is attempting to send a packet to Host Certkiller 1 through Router Certkiller 5. All routers are running EIGRP. And Router Certkiller 5 has installed the following route in its routing table.

10.1.1.0/24 via router Certkiller 6

What will occur when Router Certkiller 5 receives packets from Host Certkiller 7 that are destined for Host Certkiller A?

- A. Certkiller 5 cannot have a route to 10.1.1.0/24 through Certkiller 6; so it will always choose the path through Certkiller 3.
- B. This is a routing loop; e will forward the traffic to Certkiller 6, and will send the traffic back to Certkiller 5.
- C. Router Certkiller 5 will forward the traffic to Router Certkiller 6.
- D. Router Certkiller 5 will forward the traffic to Router Certkiller 6 and send a 'host not reachable this direction' ICMP packet to Host Certkiller 7.
- E. Router Certkiller 5 will forward the traffic to Router Certkiller 6 and send an ICMP redirect to Host Certkiller 7.

Answer: E

ICMP redirect messages are used by routers to notify the hosts on the data link that a better route is available for a particular destination.

QUESTION 122:

Which of the following statements is NOT accurate regarding frame Relay?

- A. Frame Relay does not provide error recovery.
- B. Frame Relay provides error detection.
- C. Frame Relay is high-speed, shared bandwidth protocol.
- D. Frame Relay is based on a "packet-over-circuit" architecture.

Answer: C

QUESTION 123:

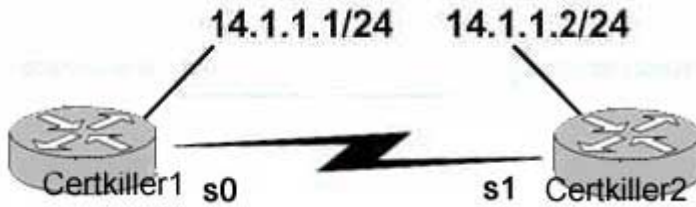
Within OSPF, what functionality best defines the use of a 'stub' area?

- 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

QUESTION 124:

Network topology exhibit:



Based on the information above, which OSPF configurations listed are valid? (Select two.)

- A. Router Certkiller 1
`router ospf 1`
`network 14.0.0.0 0.255.255.255 area 0`
 Router Certkiller 2
`router ospf 1`
`network 14.0.0.0 0.255.255.255 area 0`
- B. Router Certkiller 1
`router ospf 1`
`network 14.1.1.0 0.0.0.255 area 0`
 Router Certkiller 2
`router ospf 2`
`network 14.1.1.0 0.0.0.255 area 0`
- C. Router Certkiller 1
`router ospf 1`
`network 14.0.0.0 0.0.255.255 area 0`
 Router Certkiller 2
`router ospf 1`
`network 14.1.0.0 0.0.0.255 area 0`
- D. Router Certkiller 1
`router ospf 1`
`network 14.1.1.0 0.0.0.255 area 1`
 Router Certkiller 2
`router ospf 1`
`network 14.1.0.0 0.0.255.255 area 0`

Answer: A, B

QUESTION 125:

When using MD5 hash authentication with BGP, what part of the BGP packet is used to build the hash?

- A. TCP pseudo-header (in the order: source IP address, destination IP address, zero-padded protocol number, and segment length)0
- B. The TCP header, excluding options, and assuming a checksum of zero
- C. The TCP segment data (if any)
- D. An independently-specified key or password, known to both TCPs and presumably

connection-specific
E. All of the above

Answer: E

From RFC 2385:

Every segment sent on a TCP connection to be protected against spoofing will contain the 16-byte MD5 digest produced by applying the MD5 algorithm to these items in the following order:

1. The TCP pseudo-header (in the order: source IP address, destination IP address, zero-padded protocol number, and segment length)
2. The TCP header, excluding options, and assuming a checksum of zero
3. The TCP segment data (if any)
4. an independently-specified key or password, known to both TCPs and presumably connection-specific

QUESTION 126:

Is MTU part of the metric calculation of an EIGRP route?

- A. No. never
- B. Yes, always
- C. Only if the appropriate K-value is activated
- D. Only the smallest MTU of any links along the path is used with the metric calculation.

Answer: A

EIGRP uses these scaled values to determine the total metric to the network:

$\text{metric} = [K1 * \text{bandwidth} + (K2 * \text{bandwidth}) / (256 - \text{load}) + K3 * \text{delay}] * [K5 / (\text{reliability} + K4)]$

For default behavior, you can simplify the formula as:

$\text{Metric} = \text{bandwidth} + \text{delay}$

QUESTION 127:

What process will normally occur if an active Main Mode generated Phase One security association times out?

- A. Only Quick mode security associations will be generated.
- B. Main mode and Quick mode security associations must be generated.
- C. Aggressive mode will regenerate new security associations.
- D. Only Phase One security associations must be regenerated.
- E. No security associations will be regenerated.

Answer: B

QUESTION 128:

When using MD5 authentication in BGP where is the hash passed in the IP packet?

- A. The payload packet of a BGP request and response.
- B. In a TCP header flagged with an option 19.
- C. A specially defined BGP authentication packet.
- D. In a UDP header flagged with an option 16.
- E. In an IP packet flagged with an option 17.

Answer: B

Reference: RFC 2385

3.0 Syntax The proposed option has the following format:

```
+-----+-----+-----+ | Kind=19 |Length=18| MD5 digest... |
+-----+-----+-----+ || +-----+-----+ |
+-----+-----+-----+ || +-----+-----+ |
+-----+
```

QUESTION 129:

Which routing protocols are protected by an authentication mechanism?

- A. OSPF
- B. RIPv1
- C. RIPv2
- D. EIGRP
- E. BGP

Answer: A, C, D, E

QUESTION 130:

Routers CK1 and CK2 are running BGP in the same Autonomous System. Routes from Router CK2 show up in the BGP table of Router CK1 , but not in the routing table of Router CK1 as BGP routes.

What might cause this?

- A. Synchronization is on but Router CK1 is not receiving the same routes via an internal protocol.
- B. Synchronization is off but Router CK1 is not receiving the same routes via an internal protocol.
- C. Synchronization is off but the BGP peers are down.
- D. Next-hop-self is disabled on Router CK1 .

Answer: A

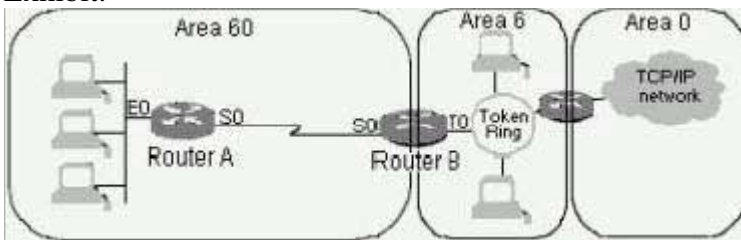
If your autonomous system is passing traffic from another AS to a third AS, BGP should not advertise a route before all routers in your AS have learned about the route via IGP. BGP will wait until IGP has propagated the route within the AS and then will advertise it to external peers. This is called synchronization.

Reference:

http://www.cisco.com/en/US/tech/CK365/technologies_tech_note09186a00800c95bb.shtml#synch

QUESTION 131:

Exhibit:



In a reorganization, OSPF areas are realigned. What changes will you advise the Certkiller trainee technician to make to the network and/or router configurations to render this a valid network design? (Select two.)

- A. The trainee should configure Router B as an Area Border Router between Area 60 and area 6.
- B. The trainee should configure a virtual link between Area 60 and Area 0.
- C. The trainee should install a serial line or other physical connection between devices in Area 60 and Area 0.
- D. This design is not a valid, and no changes can make it work.

Answer: A, B

Explanation:

To enable access from area 60 to area 0 the steps should be

(http://www.cisco.com/en/US/tech/CK365/technologies_configuration_example09186a00801ec9ee.shtml#how)

65/technologies_configuration_example09186a00801ec9ee.shtml#how)

:

How the Virtual Link Operates

Initially, the virtual link is down because Router1.1.1.1 does not know how to reach Router3.3.3.3 (the other end of the virtual link). All of the link-state advertisements (LSAs) in Area 1 need to be flooded, and the shortest path first (SPF) algorithm must be run within Area 1 by all three routers, for Router1.1.1.1 to know how to reach Router3.3.3.3 through Area 1.

After the routers know how to reach each other through the transit area, they try to form adjacency across the virtual link. The OSPF packets between the two ends of the virtual link are not multicast packets. They are tunneled packets, because they are tunneled to

the other end of the virtual link.

Once the routers become adjacent on the virtual link, Router3.3.3.3 considers itself an area border router (ABR), because it now has a link in Area 0. As a result, Router3.3.3.3 creates a summary LSA for 12.0.0.0/8 in Area 0 and in Area 1.

If the virtual link is misconfigured for some reason, then Router3.3.3.3 does not consider itself an ABR, because it does not have any interfaces in Area 0. If this is the case, it does not create summary LSAs or advertise 12.0.0.0/8 into Area 1.

QUESTION 132:

You are the Certkiller network administrator. Two remote LANs connected via a serial connection are exchanging routing updates via RIP. An alternate path exists with a higher hop count. When the serial link fails, you receive complaints of users regarding the time it takes to transfer to the alternate path.

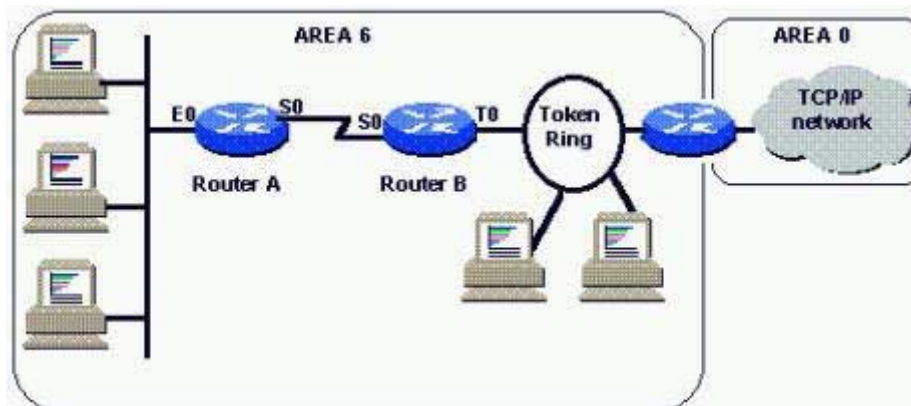
How will you ameliorate this situation?

- A. You could change the hop count on an alternate path to be the same cost.
- B. You could reduce or disable the holdown timer by making use of the timers basic command.
- C. You could increase the bandwidth of the alternate serial connection.
- D. You could configure a static route with the appropriate administrative cost via the alternate route.

Answer: B

QUESTION 133:

Exhibit:



In a move to support standards-based routing, the decision is made to use the OSPF routing protocol throughout the entire Certkiller 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 would you advice the new Certkiller trainee technician to configure OSPF on Router B?

- A. 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
- B. router ospf
network 108.3.0.0
- 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 6
- D. 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
- 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: C

Explanation: Networks 108.3.100.0 and 108.3.2.0 using a /24 need to be put into the ospf statement. both are 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.

Not A: The sub net mask in answer A is wrong. It is the correct way in answer C.

QUESTION 134:

When a user initiales a dailup PPP logon to a Cisco router running RADIUS, what attributes are sent to the RADIUS server for authentication? (assume a PAP password)

- A. Username (1), user service (7), PAP Password (8)
- B. Username (1), user service (7), Filter ID (11), Login port(16), reply message (18), Vendor Specific Attribute (26)
- C. Username (1), CHAP password (3)
- D. Username (1), PAP Password (2), NAS-ip (4), NAS-port (5), NAS port type (61), user service (7), framed protocol (6)

Answer: D

QUESTION 135:

The newly appointed Certkiller trainee technician want to know what is the best explanation for the command `aaaauthentication ppp default if-needed tacacs+`. What will your reply be?

- A. Use TACACS+ to perform authentication if authentication has been enabled on an interface.
- B. Use TACACS+ to perform authentication if the user requests authentication.
- C. Do not run PPP authentication if the user has already been authenticated by some other method.
- D. Do not run PPP authentication if the user is not configured to run PPP authentication.
- E. Do not run PPP authentication if the user knows the enable password.

Answer: C

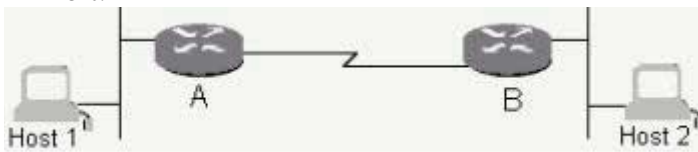
Explanation: `if-needed` (Optional) Used with TACACS and extended TACACS.

Does not perform

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

QUESTION 136:

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 IP traffic. Host 1 sends a packet to Host 2. A line hit on the serial line causes an error in the packet. How is a retransmission sent when this spesific error is detected?

- A. Host 1
- B. Host 2
- C. Router A
- D. Router B
- E. Protocol analyzer

Answer: C

QUESTION 137:

Under which circumstances will the Diffie-Hellman key exchange allows two parties to establish a shared secret key? (Choose all that apply.)

- A. Over an insecure medium.
- B. After the termination of a secure session.
- C. Prior to the initiation of a secure session.
- D. After a session has been fully secured.
- E. During a secure session over a secure medium.

Answer: A, B, C

Explanation: DH is used over an insecure medium

QUESTION 138:

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
```

What will happen when user ABC Telnetts to the router and tries to debug ICMP if a router has been configured as shown above? (Choose all that apply.)

- A. The user will be locked out due to the aaa new-model command being enabled and no TACACS server defined.
- B. The user can gain entry with a local username/password at Level 5 and run the debug ip icmp command unchallenged.
- C. The user can gain entry with the local username/password, but no debug commands will be carried out because command authorization will fail.
- D. 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.

Answer: B

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 139:

Which of the following commands must be present on the router (exact syntax would depend on the version) for the user with privilege level 15 (as defined in their TACACS+ profile) to be dropped into enabled mode immediately when that user telnets into a Cisco router?

- A. The global command: aaa authorization exec [default] [group] tacacs+
- B. The line command: logon authorization tacacs+
- C. The global command: privilege 15 enable
- D. The global command: aaa authentication enable default tacacs+

Answer: D

QUESTION 140:

Which of the following commands will result in the NAS to use the IP assignment sent from the RADIUS server for a remote PPP peer?

- A. aaa authorization default address radius
- B. aaa authorization default network radius
- C. aaa authentication ppp default radius
- D. aaa authorization default ipcp radius
- E. none of the above

Answer: C

QUESTION 141:

Which of the following statements would be valid when an UDP packet has to be fragmented?

- A. All fragments hold the UDP header, so that access-lists that look at ports would be usable.
- B. The first fragment holds only the UDP header, not the UDP data. The UDP data is transmitted in the subsequent fragments.
- C. Only the first fragment has the UDP header.
- D. None of the above.

Answer: D

QUESTION 142:

Which of the following controls Multilink PPP authorization in Cisco Secure?

- A. The <lcp multilink> command
- B. Bandwidth Allocation Protocol
- C. The <password multilink> command
- D. Token caching

Answer: C

QUESTION 143:

You are the network administrator at Certkiller . Your newly appointed Certkiller trainee wants to know what the first step in establishing PPP communications over a link is.

What will your reply be?

- A. The switch sends NCP frames to negotiate parameters such as data compression and address assignment.
- B. The originating node sends configuration request packets to negotiate the LCP layer.
- C. One or more Layer 3 protocols are configured.
- D. The originating node sends Layer 3 data packet to inform the receiving node's Layer 3 process.
- E. The receiving node performs PPP authentication on the node dialing in.

Answer: B

QUESTION 144:

In IP multicast networks, the Reverse Path Forward (RPF) check is primarily used to:

- A. Determine which interfaces should be included in the outgoing interface list.
- B. Prevent multicast traffic from looping through the network.
- C. Prevent multicast traffic from being sent by unauthorized sources.
- D. Establish the reverse flow path of multicast traffic from the receiver to the source.

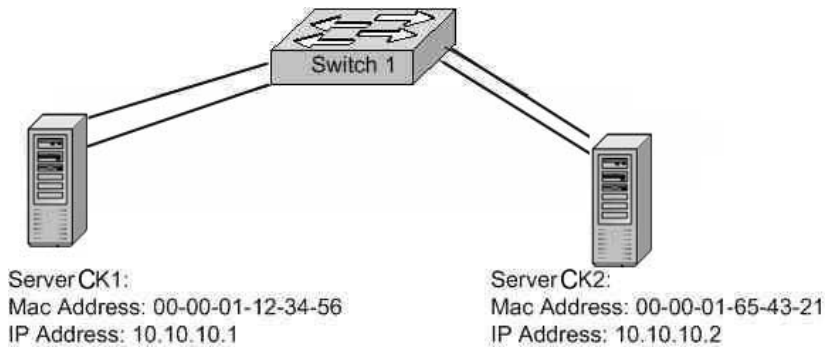
Answer: B

This RPF check helps to guarantee that the distribution tree will be loop free.

Reference:

http://www.cisco.com/en/US/tech/ CK8 28/tech_brief09186a00800a4415.html

QUESTION 145:



What is correct about the configuration of the Switch with regards to the channeling?

- A. Both channels should be given the same channel-ID.
- B. Load balancing traffic over the channel for traffic between two servers will not work.
- C. Spanning Tree needs to be disabled on the VLAN for the channel to come up.
- D. Channeling to a server is not supported.

Answer: B

Explanation: By exclusion.

Answer D is no good. Host can be a Server.

Fast EtherChannel provides parallel bandwidth of up to 800 Mbps (400-Mbps full duplex) between a switch and a router, host, or another switch

Answer A is no good. You do not give a channel a channel-ID.

This example shows how to create a two-port Fast EtherChannel bundle and verify the configuration:

Console> (enable) set port channel 1/1-2 on

Port(s) 1/1-2 channel mode set to on.

Answer C is no good. You would never turn off the Spanning tree on an entire VLAN.

Leaves us with Answer B.

Reading up on how the channel works we understand that it balances by source IP address or MAC

address. So between 2 servers the source would never change.... so no load balancing would take place.

QUESTION 146:

Multicast addresses in the range of 224.0.0.0 through 224.0.0.244 are reserved for:

- A. Administratively Scoped multicast traffic that is intended to remain inside of a private network and is never intended to be transmitted into the Internet.
- B. Global Internet multicast traffic intended to travel throughout the Internet.
- C. Link-local multicast traffic consisting of network control messages that never leave the

local subnet.

D. Any valid multicast data stream.

Answer: C

The IANA has reserved addresses in the 224.0.0.0 through 224.0.0.255 to be used by network protocols on a local network segment

Reference:

http://www.cisco.com/en/US/tech/CK8_28/tech_brief09186a00800a4415.html

QUESTION 147:

Which of the following is a primary difference between ISDN and iDSL?

- A. ISDN is a circuit switched service and iDSL is a dedicated service that uses the physical layer of ISDN.
- B. ISDN can be used on the same pair of wires as an analog POTS circuit, but iDSL cannot.
- C. An iDSL circuit can call a switched 56k circuit, but ISDN cannot.
- D. iDSL has two D channels and ISDN has one D channel.

Answer: A

QUESTION 148:

The Certkiller network administrator was requested to make a script with the following criteria:

- Must be owned by the root and executable by a group of users other than the root.
- Must not give other users root privileges other than execution of the script.
- Must not allow the users to modify the script.

Which of the following would be the best way to accomplish this task?

- A. Having the root use 'chmod 4755 <name_of_script>' to make it readable and executable by non-root users or the use 'chmod u-s <name_of_script>'.
- B. By having the users logged in under their own ID's, typing 'su' and inputting the root password after they have been given the root password, then executing the script.
- C. Changing permissions to read-write and changing ownership of the script to the group.
- D. By having root use 'chmod u-s <name_of_script>'.

Answer: A

QUESTION 149:

What is the purpose of BRI ISDN D channels?

- A. Data transfer
- B. Loopbacks
- C. Control signals
- D. None of the above

Answer: C

QUESTION 150:

The newly appointed Certkiller trainee technician wants to know when it would be wise to decrease the security association lifetime on a router. What will your reply be?

- A. To ease the workload on the router CPU and RAM.
- B. To give a potential hacker less time to decipher the keying.
- C. To improve Perfect Forward Secrecy (PFS).
- D. If the lifetime of the peer router on the other end of the tunnel is shorter, the lifetime on the local router must be decreased so that the SA lifetime of both routers is the same.
- E. None of the above.

Answer: D

QUESTION 151:

You are performing device management with a Cisco router. Which of the following is true?

- A. The Cisco Secure Intrusion Detection System sensor can apply access-list definition 198 and 199 (default) to the router in response to an attack signature.
- B. The Cisco Secure Intrusion Detection System sensor can shut down the router interface in response to an attack signature.
- C. The Cisco Secure Intrusion Detection System sensor can emit an audible alarm when the Cisco router is attached.
- D. The Cisco Secure Intrusion Detection System sensor can modify the routing table to divert the attacking traffic.

Answer: A

QUESTION 152:

In the context of Network Security, which of the following best describes the term 'contermeasure'?

- A. A policy, procedure or technology that protects a computer or network against a given vulnerability or exploit.
- B. Technology that legally permits you to launch a counter attack against someone who is attacking your network.
- C. A plan to identify intruders on your system.
- D. A plan to close all possible vulnerabilities on your network.

Answer: A

QUESTION 153:

What is NOT a TACACS+ password authentication type?

- A. PAP
- B. CHAP
- C. ARAP
- D. LCP

Answer: D

Link control protocol (LCP) is not used for authentication

QUESTION 154:

Which three methods best describe a secure wireless LAN implementation?

- A. Deploy WEP using a static 128 bit key.
- B. Deploy dynamic key management.
- C. Deploy mutual authentication between access point and client.
- D. Deploy mutual authentication between authentication server and client.
- E. Disable ad hoc mode.
- F. Enable MAC authentication.

Answer: B, C, D

Answer A is not a correct answer.

Key Management

Another type of key that is often used-but is not considered secure-is a "static" WEP key.

A

static WEP key is a key composed of either 40 or 128 bits

Answer B is good.

802.1X/EAP

An alternative WLAN security approach focuses on developing a framework for providing centralized authentication and dynamic key distribution.

Answer C is good.

Key EAP Devices

* Wireless client adapter and software-A software solution that provides the hardware and software

necessary for wireless communications to the access point; it provides mutual authentication to

the access point via an EAP mutual authentication type;

Answer D is good.

802.1X/EAP

Mutual authentication between client and authentication (Remote Access Dial-In User Service

[RADIUS]) server

QUESTION 155:

When defining a crypto ISAKMP policy, what are "Group 1" and "Group 2"?

A. Group 1 is 768-bit Diffie-Hellman exchange, Group 2 is 1024-bit Diffie-Hellman exchange.

B. Group 1 does not have Perfect Forwarded Secrecy (PFS), Group 2 includes PFS.

C. Group 1 is 1024-bit Diffie-Hellman exchange, Group 2 is 2048-bit Diffie-Hellman exchange.

D. The numbers in the 'Group #' refer to the standard access-list which must also be defined.

Answer: A

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a0080080161.html#xtor

QUESTION 156:

When using a sniffer directly connected to an access switch, the sniffer sees an excessive amount of BPDUs with the TCA bit set. Which are the most likely explanations?

A. There are no problems in the network.

B. Ports connecting to workstations do not have spanning tree portfast configured.

C. Bad cabling is being used in the network.

D. The CPU utilization on the root switch is getting up to 99% and thus not sending out any BPDUs.

Answer: B

When a switchport is configured for portfast, the switch never generates a TCN (topology

change notification) when a port configured for portfast is going up or down. A TCN causes the root bridge to send out a TCA (topology change acknowledgement).

QUESTION 157:

What is the purpose of ICMP messages?

- A. To check ARP and routing tables
- B. To report error and control messages
- C. To check reliability, delay, and forwarding rate of LAN traffic
- D. To generate management messages to gather statistics
- E. To carry link-state announcement information for OSPF

Answer: B

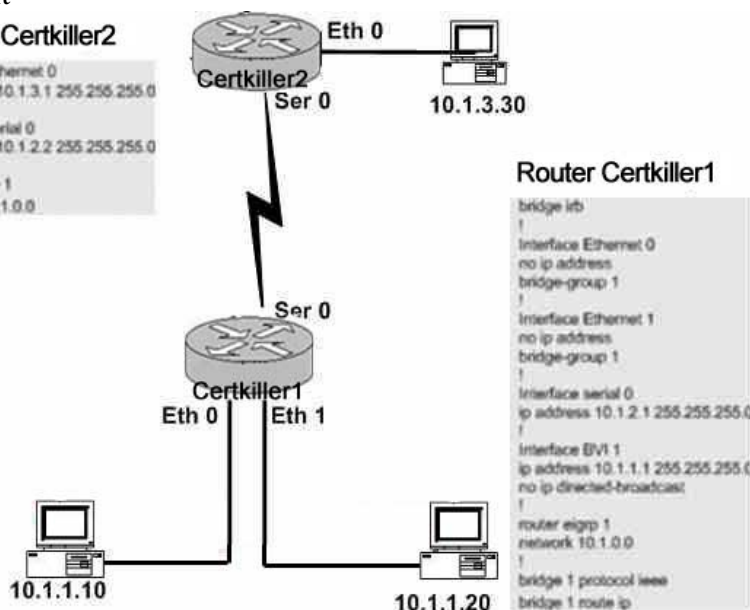
From RFC 792: The purpose of ICMP control messages is to provide feedback about problems in the communication environment. The ICMP messages typically report errors in the processing of datagrams.

QUESTION 158:

Exhibit

Router Certkiller2

```
Interface Ethernet 0
ip address 10.1.3.1 255.255.255.0
!
Interface serial 0
ip address 10.1.2.2 255.255.255.0
!
router eigrp 1
network 10.1.0.0
```



Router Certkiller1

```
bridge lab
!
Interface Ethernet 0
no ip address
bridge-group 1
!
Interface Ethernet 1
no ip address
bridge-group 1
!
Interface serial 0
ip address 10.1.2.1 255.255.255.0
!
Interface EVI 1
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast
!
router eigrp 1
network 10.1.0.0
!
bridge 1 protocol ieee
bridge 1 route ip
```

Assume this network has just been brought up. If a user on device 10.1.1.10 pinged device 10.1.3.30 how would Router A forward the ICMP's?

- A. Router A would forward the ICMP's out both serial 0 and Ethernet 1.
- B. Router A would only forward the ICMP's out Ethernet 1.
- C. Router A would only forward the ICMP's out Serial 0.
- D. Router A would not forward the ICMP out any interface.

Answer: C

QUESTION 159:

Which methods can be used to encrypt all communication between a client and a Cisco router (Select two.)

- A. RADIUS
- B. Secure-shell
- C. Kerberized telnet
- D. TACACS
- E. XTACACS

Answer: B, C

QUESTION 160:

What is the main difficulty facing exploit software when trying to hijack a TCP session?

- A. Spoofing a source address.
- B. Hopping a VLAN to get in-line with the connection.
- C. Calculating the sequence number.
- D. Injecting their IP address as a default gateway.
- E. Converting the TCP packet to UDP for easier injection.

Answer: C

QUESTION 161:

Which of the following is a description of the principle on which a Denial of Service (DoS) attack works?

- A. MS-DOS and PC-DOS operating systems using a weak security protocol.
- B. Overloaded buffer systems can easily address error conditions and respond appropriately.
- C. Host systems are incapable of responding to real traffic, if they have an overwhelming number of incomplete connections (SYN/RCVD State).
- D. All CLIENT systems have TCP/IP stack compromisable implementation weaknesses and permit them to launch an attack easily.
- E. A server ceases accepting connections from certain networks as soon as they become flooded.

Answer: C

Explanation: Denial-of-service (DOS) attacks might attempt to starve a host of resources needed to function correctly.

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

QUESTION 162:

The newly appointed Certkiller trainee technician wants to know Global deployment of RFC 2827 (ingress and egress filtering) would help mitigate what classification of attack. What will your reply be?

- A. Sniffing attack
- B. Denial of service attack
- C. Spoofing attack
- D. Reconnaissance attack
- E. Port Scan attack
- F. All of the above.

Answer: C

Explanation: Network Ingress Filtering- Defeating Denial of Service Attacks which employ IP Source Address Spoofing

QUESTION 163:

The CEO of Certkiller want to know which security programs can effectively protect your network against password sniffer programs? (Choose three.)

- A. IPSec, due to it encrypting data.
- B. RLOGIN, because it does not send passwords.
- C. Kerberos, due to encrypt password abilities.
- D. One time passwords, because the passwords always change.
- E. Use of POP e-mail, because it is better than using SMTP.

Answer: A, C, D

QUESTION 164:

Which describe the default rules of a host version of the Cisco Security Agent? Select three.

- A. It prevents writing to the system directory.
- B. It provides deep packet inspection to prevent internet worms.
- C. It prevents updates to the system registry.
- D. It stops unauthorized systems from initiating network connections to the CSA protected host.
- E. It provides stateful inspection to prevent mail and web viruses.
- F. It communicates with Network Intrusion Detection to stop network based attacks.

Answer: B, D, E

Answer B is good.

Q. Is the standalone agent effective against Internet worms like MS Blaster?

- A. Yes. Cisco Security Agent prevents the MS Blaster worm and others like it from rooting and propagating. It also stops the denial of service attacks these worms tend to launch.

Answer D is good.

Basic Network Security Features

Inbound and outbound port blocking

The distributed firewall policies in the Cisco Security Agent control all aspects of network traffic, including all inbound and outbound connections.

The Cisco Security Agent also controls traffic based on protocol, port, and communicating host address.

Answer E is good.

Active content sandbox protects Web browsers from subversion using mobile code like Java,

JavaScript, and ActiveX

E-mail worm protection blocks e-mail worm attacks like NIMDA or GONER

QUESTION 165:

MPPE (Microsoft Point to Point Encryption):

- A. Is the Microsoft implementation of RFC's 2409 and 2402
- B. Has an encryption keying mechanism that is independent of the user's password
- C. Uses the RC4 encryption algorithm
- D. Uses 768 or 1024-bit encryption keys

Answer: C

MPPE uses the RSA RC4 algorithm to provide data confidentiality.

QUESTION 166:

Global deployment of RFC 2827 would help mitigate what classification of attack?

- A. Sniffing attack
- B. Denial of service attack
- C. Spoofing attack
- D. Reconnaissance attack
- E. Prot Scan attack

Answer: C

RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

QUESTION 167:

The primary benefit of RSA encrypted nonces over RSA signatures is:

- A. They do not require a certificate authority.
- B. They offer repudiation.
- C. They are not subject to export control
- D. There is better scalability for multiple peers.

Answer: B

Explanation:

The main reason for choosing either RSA signatures or RSA nonces is if the party wants repudiation or non-repudiation.

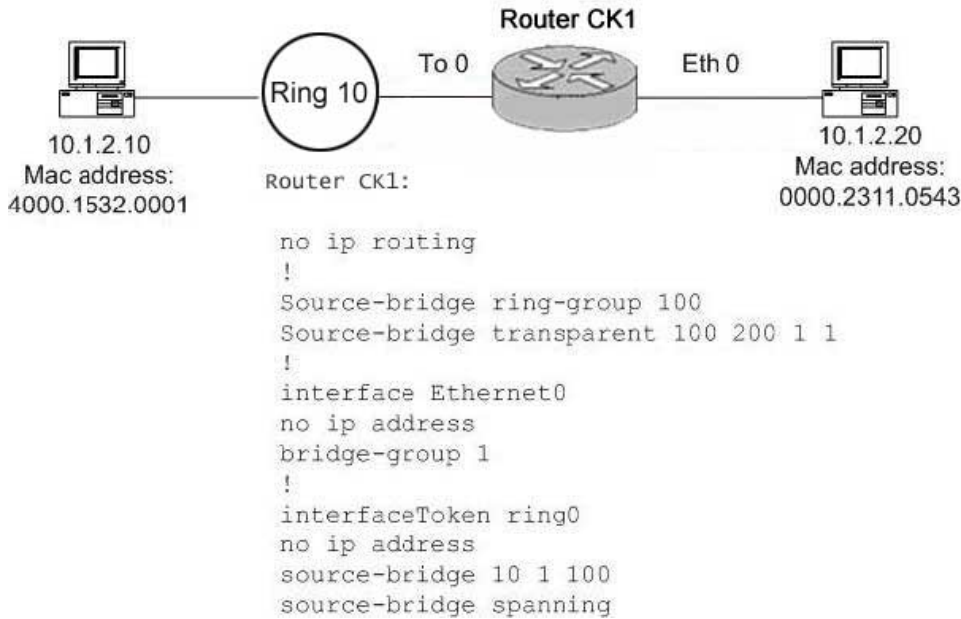
QUESTION 168:

When a TCP segment is lost, the TCP sender reacts by: (Multiple answer)

- A. Resending the segment.
- B. Increasing the window size.
- C. Resetting the session.
- D. Increasing the amount of time it will wait, when timing out the next segment that is sent.

Answer: A, D

QUESTION 169:



If a non source route ARP Requests is sourced by 10.1.2.10 destined to 10.1.2.20, based on the configuration of Router CK1 , what would it do with the frame?

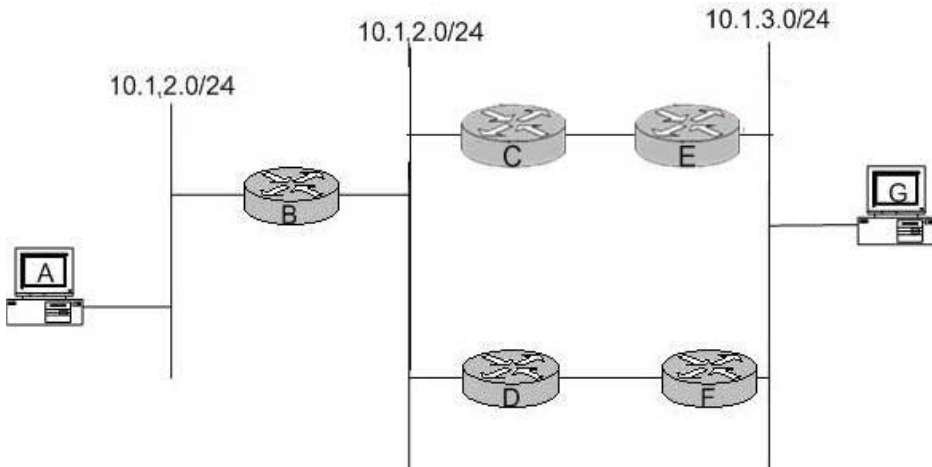
- A. Router CK1 would foreward the ARP request to the Ethernet interface without changing anything within the frame.
- B. Router CK1 would bitswap the MAC addresses then forward the frame out of the Ethernet.
- C. Router CK1 would not forward the frame since it is not source routable.
- D. Router CK1 would cache the Routing Information Field (RIF), bitswap the MAC addresses then forward the frame out the Ethernet.

Answer: D

The RIF is cached on the router and a bitswap on MAC address has to take place.

- 1.The cisco1 router receives a packet from the Ethernet. This is from pc_1 to host_1.
- 2.cisco1 needs a RIF to reach host_1, so it creates an explorer to determine the path to reach host_1.
- 3.After cisco1 receives the response, it sends the response (without a RIF) to the Ethernet station.
- 4.pc_1 sends an exchange identification (XID) to the host MAC address.
- 5.cisco1 gets the Ethernet packet, attaches the RIF to the host, and sends the packet on its way.

QUESTION 170:



Routers E and F are configured for HSRP (Hot Standby Routing Protocol). E has a priority of 100, while F has a priority of 50. At one point, when E is the active router. It fails, and F takes over as the active router. A few minutes later, E returns to service.

What will happen?

- A. F will remain the active router, there is no way for E to become the active router again unless F fails.
- B. E and F will negotiate which router should be active based on their IP addresses.
- C. E will always take over the active role, there is no way for F to remain active once another router with a higher priority is on the network.
- D. E will become the active router, if it is configured to preempt.
- E. F will remain the active router because having a lower priority is better.

Answer: D

QUESTION 171:

A router is connected to a serial link with a protocol MTU of 512 bytes.
If the router receives an IP packet containing 1024 bytes, it will: (Select two)

- A. Always drop the packet.
- B. Fragment the packet, also, the router at the other side of the serial link will reassemble the packet.
- C. Drop the packet if the DF bit is set.
- D. Fragment the packet and send it, also, the destination will reassemble the packet when it arrives.

Answer: C, D

Sometimes a router will have a link with a large (1500 byte) MTU, but the router is unable to deliver a datagram of that size over that link. That router will not return a "Fragmentation needed but DF set" ICMP error to the sender, because the link does not actually have a small MTU. However, large datagrams will be unable to pass through the

link. Therefore, PMTUD will not help, and all large-packet transmission attempts through this link will fail.

QUESTION 172:

What statement is true concerning Multilayer Switching?

- A. The first packet in every flow will be forwarded by the MLS Switching Engine.
- B. The first packet in every flow will be forwarded by the MLS Route Processor.
- C. Every 10th packet in every flow will be redirected to the MSL Route Processor.
- D. Every 10th packet in every flow will be forwarded by the MLS Route Processor.
- E. All traffic will be forwarded by the MLS Swicthing Engine.

Answer: B

QUESTION 173:

Traceroute does not work on Host A (a Unix workstation) to the Internet. Currently, there is an inbound access-list applied to the serial interface on Router 1 that says "access-list 101 permit tcp any any".

What access-list entry may need to be added in order to get traceroute to work?

- A. access-list 101 permit udp any any
- B. access-list 101 permit icmp any any time-exceeded
- access-list 101 permit icmp any any port-unreachable
- C. access-list 101 permit icmp any any time-exceeded
- access-list 101 permit icmp any any net-unreachable
- D. access-list 101 permit icmp any any echo
- access-list 101 permit icmp any any net-unreachable
- E. access-list 101 permit udp any any
- access-list 101 permit icmp any any protocol-unreachable

Answer: B

Traceroute sends UDP datagrams to the destination host, but it chooses the destination UDP port number to be an unlikely value (larger than 30,000), making it improbable that an application at the destination is using that port. This causes the destination host's UDP module to generate an ICMP "port unreachable" error (Section 6.5) when the datagram arrives. All Traceroute needs to do is differentiate between the received ICMP messages-time exceeded versus port unreachable-to know when it's done.

Reference:

http://www.starlet.spb.ru/tcp_stivens_book/tracerou.htm#8_0

QUESTION 174:

Below are four 'out' access-lists, configured on an interface.

What list will block an IP packet with source address 144.23.67.94, destination address 197.55.34.254, destination TCP port 23 from leaving the router?

- A. access-list 100 deny ip tcp 144.23.67.0 0.0.0.7 eq telnet 197.55.34.240 0.0.0.15 eq telnet
access-list 100 permit ip any any
- B. access-list 100 deny tcp 144.23.67.94 0.0.0.7 any eq telnet
access-list 100 permit ip 197.55.34.240 0.0.0.15 eq telnet any
- C. access-list 100 deny tcp 144.23.67.96 0.0.0.7 eq telnet 197.55.34.240 0.0.0.15
access-list 100 permit ip any any
- D. access-list 100 deny ip 144.23.67.94 0.0.0.7 host 144.23.67.94
access-list 100 permit ip any any

Answer: B

QUESTION 175:

How would you say PIX is acting like when the PIX firewall is not configured with a static/conduit to permit explicit access from the outside to the inside and data sent to inside addresses result in the firewall dropping the packets sent to it?

- A. A black hole router
- B. A brouter
- C. A bridge
- D. A router
- E. None of the above

Answer: A

The PIX will not send any reply to the source of traffic and just drop the packets.

Black Holes

A black hole occurs on a network when a router discards packets without any notification of the problem

There are many types of black hole routers...

QUESTION 176:

The addresses on the inside of a packet-filtering router are configured from the network 10.0.0.0/8.

Which of the following access-list entries on the outside gateway router would prevent spoof attacks to this network?

- A. access-list 101 deny ip 10.0.0.0 0.0.0.255 0.0.0.0 255.255.255.255
- B. access-list 101 deny ip 10.0.0.0 255.0.0.0 0.0.0.0 0.0.0.0
- C. access-list 101 deny ip any 10.0.0.0 255.255.255
- D. access-list 1 deny 10.0.0.0
- E. access-list 101 deny ip 10.0.0.0 0.255.255.255 any

Answer: E

QUESTION 177:

Exhibit:

WINDOW 512	ACK 38177	SEQUENCE 90708	Bytes sent 1024	HOST A
WINDOW 1024	ACK 91732	SEQUENCE 38177	Bytes sent 512	HOST B
WINDOW 2048	ACK ?	SEQUENCE ?	Bytes sent 1024	HOST A

Host A and B are communicating by using TCP. A packet is sent from A to B, B replies back to A, and A acknowledges B's reply. Selected information from this dialogue is shown.

Based on the information provided what will be the correct values for the final acknowledgment from A:

- A. Ack=38689 Seq=91734
- B. Ack=38689 Seq=91732
- C. Ack=38700 Seq=91633
- D. Ack=38690 Seq=91733

Answer: D

QUESTION 178:

The newly appointed Certkiller trainee technician wants to know how a route running Certificate Enrollment Protocol (CEP) obtains a certificate. What will your reply be?

- A. The router administrator should send an e-mail message to 'sysadmin@icsa.net'.

This message should request a certificate and include the FQDN of the device.

B. If using Cisco IOS version 11.3 or 12.0, the router administrator should enter the following configuration:

```
crypto ca identity <registered_ca_name> enrollment ftp://  
<certificate_authority>
```

C. The router administrator has to copy the certificate from the peer router at the other end of the tunnel and then paste it onto the local router.

D. If using Cisco IOS version 11.3 or 12.0, the router administrator should enter the following configuration:

```
crypto ca identity <registered_ca_name> enrollment http:// <certificate authority>
```

E. If using Cisco IOS version 11.3 or 12.0, the router administrator should enter the following configuration:

```
crypto ca identify <registered_ca_name> enrollment http://  
<certificate authority>
```

Answer: D

Explanation:

The correct answer should read `crypto ca identity <registered_ca_name> enrollment http:// <certificate authority>`

QUESTION 179:

What is the primary benefit of RSA encrypted nonces over RSA signatures?

- A. RSA encrypted nonces offer repudiation.
- B. RSA encrypted nonces are not subjected to export control.
- C. There is better scalability to multiple peers.
- D. RSA encrypted nonces does not require a certificate authority.

Answer: D

QUESTION 180:

What are the two options for OSPF authentication methods in PIX OS?

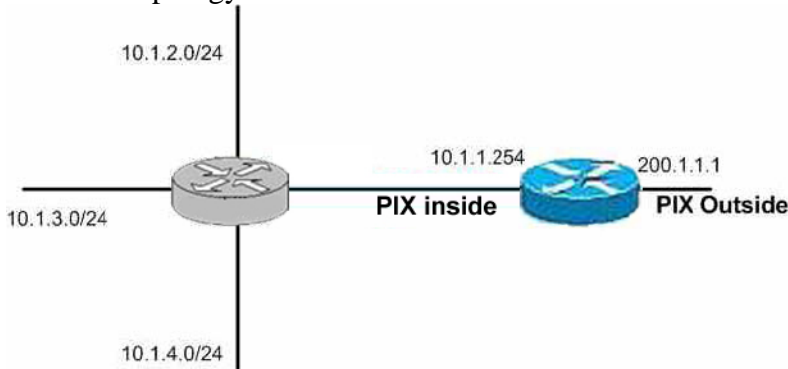
- A. Kerberos
- B. Area
- C. Password
- D. Tacacs+
- E. MD5
- F. Radius

Answer: C, E

Q. Are OSPF routing protocol exchanges authenticated? Yes, OSPF can authenticate all packets exchanged between neighbors. Authentication may be through simple passwords or through MD5 cryptographic checksums.

QUESTION 181:

Network topology Exhibit:



After viewing the PIX syslog output below, what answer best describe what MAY be going on in the network? (Assume three network on the inside of the PIX all with private addresses and the outside is connected to the internet).

14:25:02 10.1.1.1.254 : %PIX-7-710005: TCP request discarded from 88.3.62.

119/57088 to inside : 10.1.1.254/www

14:25:02 10.1.1.1.254 : %PIX-7-710005: TCP request discarded from 169.236.78.115/56832 to inside: 10.1.1.254/www

14:25:02 10.1.1.1.254 : %PIX-7-710005: TCP request discarded from 7.237.99.75/56576 to inside: 10.1.1.254/www

14:25:02 10.1.1.1.254 : %PIX-7-710005: TCP request discarded from 211.39.49.98/56320 to inside 10.1.1.254/www

14:25:02 10.1.1.1.254 : %PIX-7-710005: TCP request discarded from 96.126.207.4/56064 to inside: 10.1.1.254/www

14:25:02 10.1.1.1.254 : %PIX-7-710005: TCP request discarded from 70.175.181.20/55808 to inside: 10.1.1.254/www

14:25:02 10.1.1.1.254 : %PIX-7-710005: TCP request discarded from 200.230.90.97/55552 to inside: 10.1.1.254/www

14:25:02 10.1.1.1.254 : %PIX-7-710005: TCP request discarded from 208.240.228.30/55296 to inside: 10.1.1.254/www

- A. A port scan is being launched from the inside network.
- B. Several IP addresses on the inside have all launched an attack against the PIX web server.
- C. A host on the inside has launched a denial of service attack generating random source addresses and aimed at the PIX inside interface.
- D. A host on the inside has been compromised and is attempting to log onto the PIX http server.
- E. Several zombies hosts have been activated on the outside of the PIX and are trying to

crash the PIX HTTP server.

Answer: C

Explanation:

Answer A is no good. No port scan going on, all traffic to port 80.

Answer B is not a likely answer. We do not see A private network having that many different Subnets and legal IP address ranges.

Answer C is the best answer. All 8 connections are happening during the same second 14:25:02 so this seems like a Denial of service attack with spoofed IP address.

Answer D can be correct but not best answer.

Answer E Is talking about outside traffic, so this is a wrong answer.

QUESTION 182:

Which command allow a PIX Firewall to be configured for a dual NAT environment?

Select two,.

- A. alias
- B. nat [(ifname0} 0 access-list
- C. sysopt permit dnat
- D. NAT (outside)
- E. Pat [(ifname)] 0 access-list

Answer: A, C

The alias command is used on the PIX to administer overlapping addresses with dual NAT.

'sysopt permit dnat' command is deprecated starting in PIX Firewall version 6.2.

QUESTION 183:

PIX is capable of running which routing protocols? (Choose three)

- A. OSPF
- B. IPv1
- C. IPv2
- D. EIGRP
- E. BGP

Answer: A, B, C

QUESTION 184:

The Certkiller network manager ascertained that security has been breached on a router or PC client and thus wants to revoke the CA certificate. What should he/she do to accomplish this?

- A. type: configure terminal crypto ca revoke <name> if there is a router involved.
- B. Contact the CA administrator and be prepared to provide the challenge password chosen upon installation.
- 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 by default).
- D. Send e-mail to 'sysadmin@icsa.net' with the hostname and IP of the compromised device requesting certificate revocation.

Answer: B

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 185:

The newly appointed Certkiller trainee technician wants to know what an Inter Switch Link (ISL) is. What will your reply be?

- A. An ISL is a protocol to interconnect switches across ATM only.
- B. An ISL is a Cisco proprietary protocol for interconnecting multiple switches.
- C. An ISL is a protocol to interconnect switches across FDDI only.
- D. An ISL is an IEEE protocol to interconnect multiple switches.
- E. An ISL is an IEEE protocol to interconnect multiple switches across Fast Ethernet.

Answer: B

QUESTION 186:

Which of the following commands will permit a PIX Firewall to be configured for a dual NAT environment? Select two.

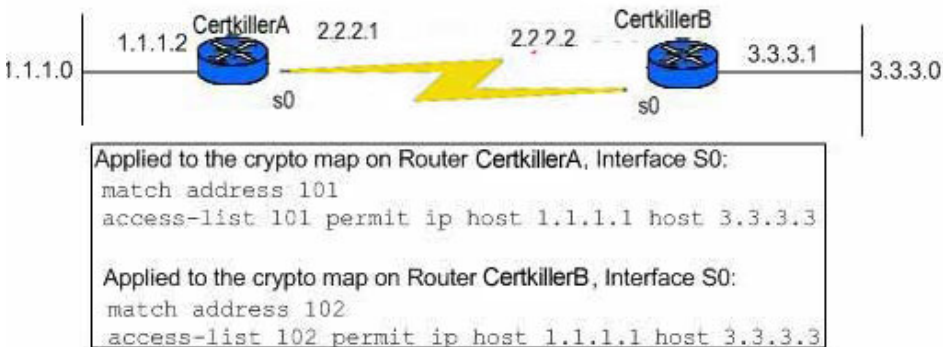
- A. nat [(ifname)] 0 access-list
- B. sysopt permit dnat
- C. alias
- D. bidirectional nat
- E. pat [(ifname)] 0 access-list

Answer: B, C

'sysopt permit dnat' command is deprecated starting in PIX Firewall version 6.2.
The alias command is used on the PIX to administer overlapping addresses with dual NAT.

QUESTION 187:

Exhibit:



What will happen when a user attempts to telnet from network 1.1.1.X to network 3.3.3.X when taking the IPsec example and IPsec with IKE as shown, into account?

- A. The telnet will succeed with decrypted traffic only.
- B. The telnet will succeed and the traffic will be directionally encrypted.
- C. The telnet will fail due to asymmetric access lists.
- D. The telnet will fail because access-list 101 should have been applied to router A's interface 1.1.1.2.

Answer: C

QUESTION 188:

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 address 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

QUESTION 189:

What is the benefit of using Secure Shell instead of Telnet?

- A. It offers native accounting.
- B. It requires IPSec.
- C. It qualifies for C1 security under TCSEC guidelines.
- D. It provides encrypted sessions
- E. It offers increased key length of encryption.

Answer: D

QUESTION 190:

When configuring IOS NAT (Network Address Translation,) what keyword is used to specify Port Address Translation?

- A. pat
- B. port
- C. extended
- D. overload
- E. netmask 255.255.255.255

Answer: D

QUESTION 191:

There are certain IP unicast address ranges (10.0.0.0/8, 192.168.0.0/16, etc. [RFC 1918]) that are reserved for private use, and should not be used on the internet, similarly, there is group of multicast group addresses that are served for private use and should not be used on the internet (RFC 1700). What is that group of addresses?

- A. 224.0.0.0-224.255.255.255
- B. 255.0.0.0-255.255.255.255
- C. 232.0.0.0-232.255.255.255
- D. 239.0.0.0-239.255.255.255
- E. All of the above

Answer: D

QUESTION 192:

Exhibit:

Router Certkiller1

```
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 168.1.1 255.255.255.1 255.255.255.0
 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
 match ip address 150
```

Router Certkiller2

```

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 106.192.168.2 0.154.255.255.0
 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
 match ip address 150

```

Give the configuration shown, what is the expected behavior of IP traffic traveling from the attached client to the two Ethernet subnets? (Select two)

- A. Traffic will not successfully access the internet or the subnets of the remote router's Ethernet interface.
- B. Traffic between the Ethernet subnets on both routers will be encrypted.
- C. Traffic bound for the internet will be translated by NAT and will not be encrypted.
- D. Traffic will be translated by NAT between the Ethernet subnets on both routers.
- E. Traffic bound for the internet will not be routed because the source IP addresses are private.

Answer: B, C

QUESTION 193:

What is the primary reason for using NAT translation on a firewall?

- A. To translate RFC 1918 addresses for access to the Internet.
- B. To increase the number of registered IP addresses used.
- C. To increase firewall performance.

D. To improve security.

Answer: A

QUESTION 194:

Generally speaking which of the following could be done to mitigate a Day Zero host or server attack?

- A. Install software that prevents actions such as buffer overflows and writes to the system directory.
- B. Deploy Intrusion Detection on all switches that directly connect to hosts or servers.
- C. Install Virus scanning software.
- D. Ensure that your hosts and servers all have the latest security patches.
- E. Generally speaking Day Zero attacks cannot be stopped.

Answer: A

In a zero-day attack, a worm or virus generally overflows a buffer, writes to the registry, or writes to the system directory.

Reference:

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009

QUESTION 195:

The Cisco Secure Intrusion Detection System sensor does not have the following type of interface available:

- 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 196:

Exhibit:

Router A:	Router B:
<pre>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</pre>	<pre>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 7 ipsec-isakmp set peer 100.232.202.210 set transform-set encrypt-des match address 106 interface Serial0 ip address 100.228.202.154 255.255.255.252 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 interface Serial0 overload ip classless ip route 0.0.0.0 0.0.0.0 100.228.202.153 ip route 192.168.1.0 255.255.255.0 100.228.202.153 access-list 106 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 access-list 150 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 access-list 150 permit ip 192.168.2.0 0.0.0.255 any route-map ipsecnat permit 10</pre>

Taking the exhibit above into consideration how would you expect IP traffic from the clients attached to the two Ethernet subnets to behave? (Choose all that apply.)

- A. Traffic bound for the Internet will be translated by NAT and will be decrypted.
- B. Traffic bound for the Internet will be unrouted due to private source IP addresses.
- C. Traffic will not successfully access the Internet or the subnets of the remote router's Ethernet interface.
- D. Traffic between the Ethernet subnets on both routers will be encrypted.
- E. Traffic will be translated by NAT between the Ethernet subnets on both routers.

Answer: D

QUESTION 197:

Under which of the following circumstances will Network Address Translation (NAT) not work well?

- A. With outbound HTTP when AAA authentication is involved.
- B. With traffic that carries source and/or destination IP addresses in the application data stream.
- C. With ESP Tunnel mode IPsec traffic.
- D. When PAT (Port Address Translation) is used on the same firewall.
- E. When used in conjunction with static IP addresses assignment to some devices.

Answer: B

Explanation:

AH does not work with NAT

QUESTION 198:

Inside addresses = 131.108.0.0

Outside global addresses = 198.108.10.0

Serial 0 is connected to the outside world

Which of the following Network Address Translation (NAT) configuration is correct when you consider the above information?

A. ip nat pool CCIE-198 198.108.10.0 198.108.10.255
prefix-length 24.

ip nat inside source list 1 pool CCIE-198

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 24

ip nat inside source list 1 pool CCIE-198

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 CCIE-198

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 CCIE-131

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 199:

The newly appointed Certkiller trainee technician wants to know how many inside sessions can be translated when using NAT overload on a Cisco IOS or PIX-based firewall. What will your reply be?

- A. 1 to 65,535
- B. 1024 to 65,535
- C. 1024 to 32,768
- D. 1 to 64,000
- E. 1024 to 64,000

Answer: A

QUESTION 200:

At which layers of the OIS model do firewalls typically operate? (Select three)

- A. Application
- B. Network
- C. Transport
- D. Session
- E. Physical

Answer: A, B, C

QUESTION 201:

In the IOS Firewall Feature Set, which network layers are examined by CBAC to make filtering decisions? Select three.

- A. Transport
- B. Application
- C. Network
- D. Presentation
- E. Data Link

Answer: A, B, C

Context-based Access Control (CBAC) examines not only networklayer and transportlayer information, but also examines the application-layer protocol information (such as FTP information) to learn about the state of TCP and UDP connections.

QUESTION 202:

A bastion host is:

- A. An impenetrable decoy firewall
- B. A host that is not protected by a firewall and all security is handled by the applications
- C. A host that is to be sacrificed to all hacking attempts in order to log and monitor the hacking activity.
- D. A network's first line of defense against attack, typically located on the outside of a firewall
- E. A network last line of defense against attack, typically located on the inside of a firewall.

Answer: D

QUESTION 203:

What command in the IOS Firewall Feature Set is used to turn off CBAC?

- A. no ip inspect cbac
- B. no enable ip inspect
- C. no enable cbac
- D. no ip inspect
- E. no ip inspect all

Answer: D

To turn off Context-based Access Control (CBAC) completely at a firewall, use the no ip inspect command in global configuration mode.

QUESTION 204:

On what is proper firewall implementaion always dependent?

- A. The selection of the most expensive equipment.
- B. The use of IPSec, IKE and PKI.
- C. Identifying network assets to discard.
- D. Increasing the number of passwords each user must maintain.
- E. Pervasive security

Answer: E

QUESTION 205:

What sets the FECN bit in Frame Relay?

- A. The Frame Relay network, to inform the DTE receiving the frame that congestion was experienced in the path from source to destination.
- B. The Frame Relay network, in frames traveling in the opposite direction from those frames that encountered congestion.
- C. The receiving DTE, to inform the Frame Relay network that it is overloaded and that the switch should throttle back.
- D. The sending DTE, to inform the Frame Relay network that it is overloaded and that the switch should throttle back.
- E. Any device that uses an extended DLCI address.

Answer: A

QUESTION 206:

What are the available AAA protocols with the IOS Firewall Feature Set? (Choose all that apply.)

- A. PAP
- B. Kerberos
- C. XTACACS
- D. TACACS+

Answer: B, D

QUESTION 207:

Which of the following represents the correct description of the authentication sequence for the IOS Firewall Authentication Proxy?

- A. The user authenticates by FTP, and route maps are downloaded from the proxy server.

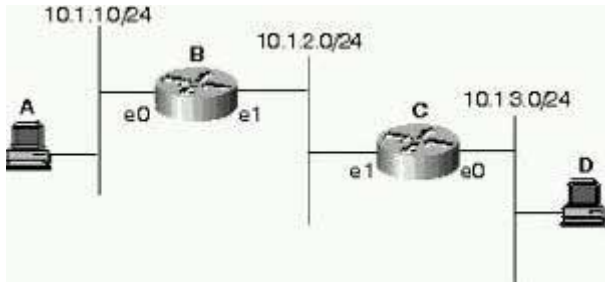
- B. The user authenticates locally to the router.
- C. The user authenticates by HTTP, and access lists are downloaded from the AAA server.
- D. The user authenticates by Telnet, and access lists are downloaded from the AAA server.
- E. The user authenticates by HTTP, or Telnet, and access lists are downloaded from the AAA server.

Answer: C

Explanation: When a user initiates an HTTP session through the firewall, the authentication proxy is triggered

QUESTION 208:

Exhibit:



Host A is attempting to send a packet through Router B to Host D as illustrated above. There are neither 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. Yes, the packets will reach Host D if the routers are configured to bridge.
- B. Yes, the packets will reach Host D because Router B will forward the packets destined to 10.1.3.0/24 to Router C through its IP default-gateway configuration.
- C. Yes, 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: E

Explanation: By disabling routing in router, router no longer forwards packets that it received.

By configuring IP default gateway, router only send packets it creates itself.

QUESTION 209:

What is the purpose of Administrative Distance, as used by Cisco routers?

- A. It is a means of choice between routes from different routing protocols when receiving updates for the same network.
- B. It is used to identify which routing protocol forwarded the update.
- C. It defines the distance to the destination used in deciding the best path.
- D. It is meant 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 210:

When using PKI what is true about CRL?

- A. 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.
- B. 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.
- C. The router's CRL includes a list of client that have presented invalid certificates to the router in the past.
- D. The CRL is used to check presented certificates to determine if they are revoked.

Answer: D

QUESTION 211:

What is the rationale behind a Network Administrator wanting to use Certificate Revocation Lists (CRLs) in their IPSec implementations?

- A. CRLs allow network administrators the ability to do "on the fly" authentication of revoked certificates.
- B. They help to keep a record of valid certificates that have been issued in their network.
- C. CRLs allow network administrators to deny devices with certain certificates from being authenticated to their network.
- D. Wildcard keys are much more efficient and secure.

CRLs should only be used as a last resort.

Answer: C

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 212:

What happens during a SYN flood attack?

- A. TCP connection requests floods a target machine is flooded with randomized source address & ports for the TCP ports.
- B. A TCP SYN packet, which is a connection initiation, is sent to a target machine, 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 SYN-ACK 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 213:

Which of the following statements regarding Certificate Revocation List (CRL) is valid when using PKI?

- A. The CRL resides on the CA server and is built by querying the router or PIX to determine which clients' certificate status in the past.
- B. The CRL is used to check presented certificates to determine if they are revoked.
- C. A router or PIX will not require that the other end of the IPSec tunnel have a certificate if the `crl` optional command is in place.
- D. The router's CRL includes a list of clients that have presented invalid certificates to the router in the past.

Answer: B

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 REASONABLE ANSWER BUT HERE IS WHY I 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 `crloptional` 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 214:

Which of the following responses will an experienced Security Manager disprove of when a remote user tries to login to a secure network using Telnet, but accidentally types in an invalid username or password? (Choose two.)

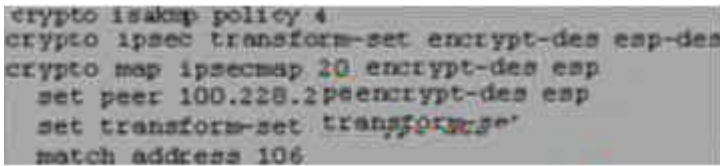
- A. Authentication Failure
- B. Logon Attempt Failed
- C. Invalid Username
- D. Invalid Password

E. Access Denied

Answer: C, D

QUESTION 215:

Exhibit:



```
crypto isakmp policy 4
crypto ipsec transform-set encrypt-des esp-des
crypto map ipsecmap 10 encrypt-des esp
 set peer 100.228.228.228 encrypt-des esp
 set transform-set transform-set
 match address 106
```

Click the Exhibit button to view the configuration.

Assuming the configuration given, what will be the attributes of the Phase One negotiation?

- A. Authentication: Pre-share
Hash Algorithm: SHA-1
Encryption: 56-bit DES-CBC
- B. Authentication: RSA-SIG
Hash Algorithm: SHA-HMAC
Encryption: 56-bit DES-CBC
- C. Authentication: RSA-SIG
Hash Algorithm: SHA-1
Encryption: 56-bit DES-CBC
- D. Authentication: RSA-SIG
Hash Algorithm: SHA-1
Encryption: 3 DES-CBC
- E. Authentication: Pre-share
Hash Algorithm: SHA-HMAC
Encryption: 56-bit DES-CBC

Answer: C

Default authentication method is RSA-SIG.

QUESTION 216:

802.1x protocol is used primarily for what purpose?

- A. Layer two authentication
- B. Layer three authentication
- C. Application layer authentication
- D. MS-CHAP Authentication
- E. VLAN allocation

Answer: A

802.1x is used for layer 2 authentication.

QUESTION 217:

The newly appointed Certkiller trainee technician wants to know where Kerberos is mainly used. What will your reply be?

- A. Session-layer protocols, for data integrity and checksum verification.
- B. Application-layer protocols, like Telnet and FTP.
- C. Presentation-layer protocols, as the implicit authentication system for data stream or RPC.
- D. Transport and Network-layer protocols, for host to host security in IP, UDP, or TCP.
- E. Datalink-layer protocols, for cryptography between bridges and routers.

Answer: B

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

QUESTION 218:

Why would you advice the new Certkiller trainee technician NOT to use NFS protocol for use across a firewall or a security domain?

- A. The security of the protocol is not stringent because File permissions can easily be modified in the requests.
- B. Industry technicians do not understand NFS well, but is actually appropriate to run across various security domains.
- C. NFS is not secure because it does not have the concept of users and permissions.
- D. It is UDP based which makes its state difficult to track.
- E. This protocol uses a range of ports, and firewalls have difficulty opening the proper entry points to allow traffic.

Answer: D

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 219:

MPPE (Microsoft Point to Point Encryption) is valid with which of the following forms of authentication?

- A. MS-CHAP or EAP
- B. CHAP (RFC 1994)
- C. PAP
- D. SPAP (Shiva PAP)
- E. A and B

Answer: A

QUESTION 220:

Which of the following represents a definition of Cipher text?

- A. Cipher text can be defined as the key to encrypt a message.
- B. Cipher text can be defined as the public key that has been changed with a peer to determine the original message.
- C. Cipher text can be defined as the result of an already decrypted message on the receiving end.
- D. Cipher text can be defined as the post-encrypted message that travels on the wire.
- E. Cipher text can be defined as the key used for a one way hash in an IPSec Phase Two exchange.

Answer: D

QUESTION 221:

What is the advantage of using Secure Shell instead of Telnet?

- A. Secure Shell offers native accounting.
- B. Secure Shell requires IPSec.
- C. Secure Shell qualifies for C1 security under TCSEC guidelines.
- D. Secure Shell provides an encrypted tunnel.
- E. Secure Shell offers increased key length for encryption.

Answer: D

QUESTION 222:

Which of the following statements regarding MPPE (Microsoft Point to Point Encryption) is valid?

- A. MPPE is the Microsoft implementation of RFC's 2409 and 2402.
- B. MPPE has an encryption mechanism that is independent of the user's password.
- C. MPPE uses the RC4 encryption algorithm.
- D. MPPE uses 768 or 1024-bit encryption keys.

Answer: C

FC 2409 and 2402 refers to ISAKMP and IPSec.

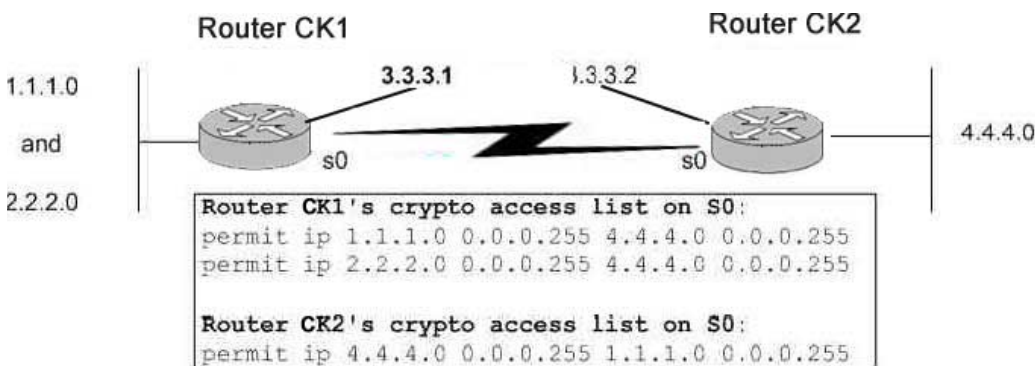
QUESTION 223:

Which of the following commands is NOT a Kerberos executable on a Kerberos Version 5 Unix system?

- A. kadmin
- B. keytab
- C. kdb5_util
- D. krb5kdc

Answer: B

QUESTION 224:



What will happen to the traffic flow between two routers with asymmetric crypto access-lists when configured as shown?

- A. The flow source 2.2.2.X through CK1 to destination 4.4.4.X on the other side of CK2 will be encrypted.
The flow from source 4.4.4.X through CK2 to destination 2.2.2.X on the other side of CK1 will not be encrypted.
- B. All traffic between 2.2.2.X and 4.4.4.X will be encrypted.
- C. All traffic between 2.2.2.X and 4.4.4.X will be unencrypted.
- D. No traffic will flow between 2.2.2.X and 4.4.4.X, because CK1 is expecting traffic with a source of 4.4.4.X and destination of 2.2.2.X to be encrypted. However, CK2 is not encrypting this traffic.

Answer: D

The crypto access-list not only defines what outbound traffic is protected, but also what inbound traffic protected. If traffic arrives that matches the crypto access list, but is not protected in the manner defined by the transform set, the traffic is dropped.

Reference:

Page 673, Troubleshooting Virtual Private Networks, Cisco press

QUESTION 225:

What would be the biggest challenge to a hacker writing a man-in-the-middle attack aimed at VPN tunnels using digital certificates for authentication?

- A. Programmatically determining the private key so they can proxy the connection between the two VPN endpoints.
- B. Determining the ISAKMP credentials when passed to establish the key exchange.
- C. Determining the phase two credentials used to establish the tunnel attributes.
- D. Decrypting and encrypting 3DES once keys are known.
- E. Decrypting and encrypting AES once keys are known.

Answer: A

QUESTION 226:

Which are valid modes in the Cisco IDS signature engine parameter Alarm Throttle?

- A. NoSummarize
- B. Summarize
- C. GlobalSummarize
- D. FireOnce
- E. FireEvery
- F. Null
- G. FireAll

Answer: B, C, D, G

Alarm Throttle parameters are: AlarmThrottleFireOnce, AlarmThrottleFireAll, AlarmThrottle Summarize, AlarmThrottle GlobalSummarize

QUESTION 227:

Which are possible pattern matching techniques that are used in Cisco's network IDS? Select three.

- A. Stateful
- B. Statistical moments
- C. Heuristic analysis
- D. Threshold matching
- E. Protocol anomaly - based

Answer: A, C, E

QUESTION 228:

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 message at particular alarm levels via event.
- C. It send a TCP reset to the intruder when operating in packet sniffing mode.
- D. It performs a traceroute to the intruding system.

Answer: D

The IDS does not perform a traceroute to the intruding system.

You can configure the IDS appliance to respond to recognized signatures as it captures and analyzes network traffic. These responses include logging the event, forwarding the event to the IDS manager, performing a TCP reset, generating an IP log, and/or reconfiguring a router.

QUESTION 229:

Exhibit:

	Evasion Traversal		Code Example
1	Method Replicating Directory	D	//cgi-bin/example/example.cgi
2	Double Slashes	B	GET /%63/%67/%69/%2D/%62/%69/%6E/example.cgi
3	Parameter Hiding	C	/cgi-bin/./././example.cgi
4	DOS/Windows Directory Syntax	D	GET /cgi-bin/example.cgi -> HEAD /cgi-bin/example.cgi
5	Reverse Traversal	E	//cgi-bin/example.cgi
6	Session Splicing	F	GET /index.html%3Fparam=../cgi-bin/example.cgi
7	URL Encoding	G	http://server/cgi-bin/example.cgi
8	Self-referencing directories	H	The URL is sent in small packets: "GE", "T", " /", "ex", "a", "m", "pl", "e", "c", "gi"

Match the shown IDS evasion methods with the proper example given.

- A. 1 -C, 2 - E, 3 - F, 4 - G, 5 - A, 6 - H, 7 - B, 8 - D
- B. 1 -D, 2 - E, 3 - F, 4 - G, 5 - C, 6 - H, 7 - B, 8 - A
- C. 1 -C, 2 - F, 3 - E, 4 - G, 5 - A, 6 - H, 7 - B, 8 - C
- D. 1 -D, 2 - E, 3 - F, 4 - G, 5 - A, 6 - H, 7 - B, 8 - C

Answer: D

QUESTION 230:

How does Anomaly-based Intrusion detection recognize that a network attack is in progress?

- A. The IDS matches packets with a signature and then logs the unusual activity.
 - B. The IDS normalizes network traffic and alarms when sampled traffic falls out of that norm.
 - C. Protocol adherence rules are established by the administrator and any deviation from that is flagged as a potential attack.
 - D. The IDS normalizes network traffic The System manager then creates signatures based on the normalization.
- If it detects different patterns it will report those patterns as potential attacks.

Answer: B

QUESTION 231:

What is the main difficulty facing exploit software when trying to hijack a TCP session?

- A. Spoofing a source address.
- B. Hopping a VLAN to get in-line with the connection.
- C. Calculating the sequence number.
- D. Injecting their IP address as a default gateway.
- E. Converting the TCP packet to UDP for easier injection.

Answer: C

Reference:

<http://www.ietf.org/rfc/rfc1948.txt?number=1948>

QUESTION 232:

What are the potential dangers of running the Finger service on hosts?

- A. Finger opens a port that data can be transferred to, thus enabling an intruder to access password files.
- B. If Finger has a trust relationship to another server, the associated port can be exploited for unauthorized logon.
- C. Finger allows users to logon physically to a system of the service aborts.

D. Some Finger services have forwarding capabilities that allow intruders to mask their identities when gaining access to the service.

Answer: D

QUESTION 233:

Mail Server A is trying to contact Mail Server B behind a firewall. Mail Server A makes the initial connection, but there is a consistent long delay (1 minute) before the queued mail is actually sent.

A reason for this might be:

- A. Mail Server A does not have a default route.
- B. Mail Server B does not have a default route.
- C. The firewall is blocking TCP port 113.
- D. A third Mail Server is delaying the traffic.
- E. Mail Server A does not have the IDENT server running.

Answer: A

QUESTION 234:

What happens when one experiences a ping of death?

- A. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP) and the "type" field in the ICMP header is set to 18 (Address Mask Reply).
- B. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP), the Last Fragment bit is set, and $(\text{IP offset} \times 8) + (\text{IP data length}) > 65535$. In other words, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8-byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
- C. This is when an IP datagram is received with the "protocol" field in the IP header set to 1 (ICMP) and the source equal to destination address.
- D. This is when 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 $(\text{IP offset} \times 8) + (\text{IP data length}) > 65535$. 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 235:

CiscoWorks VMS consists of several management consoles or MCs. The IDS is used to control the configuration of the IDS sensors and IDSM blades deployed in an enterprise. Which parameters must be unique when in a given PostOffice domain?

- A. IP address and PostOffice ID
- B. Host ID and PostOffice domain name
- C. Host ID and IP address
- D. Organization ID and Host ID
- E. Organization name and Organization ID
- F. Organization ID and PostOffice ID

Answer: D

Within a postoffice domain, no sensor or sensor group can have the same Org ID/Host ID pair as another sensor or sensor group."

QUESTION 236:

Which of the following is a primary difference between UNIX implementation of traceroute and tracert.exe version found on Windows NT?

- A. Unix traceroutes use ICMP echo requests with varying TTLs, while NT sends UDP probes on a pseudo random port with varying TTLs and watches for returning ICMP messages.
- B. It is a similar implementation strategy regardless of the operation system.
- C. Unix traceroutes send UDP probes on a pseudo random port with varying Time to Live (TTL) settings and watch for returning ICMP messages, whereas NT makes use of ICMP echo requests with varying TTLs.
- D. NT makes use of UDP probes on port 33000 and Unix makes use of UDP probes on port 335000.
- E. None of the above.

Answer: E

QUESTION 237:

What can be used to solve a problem situation where a user's PC is unable to ping a server located on a different LAN connected to the same router?

- A. Ensure routing is enabled.
- B. A default gateway from the router to the server must be defined.
- C. Check to see if both the PC and the server have properly defined default gateways.
- D. Both the server and the PC must have defined static ARP entries.

Answer: C

QUESTION 238:

If the PIX firewall is not configured with a static/conduit to allow explicit access from the outside to the inside, data sent to inside addresses result in the firewall dropping the packets sent to it. In this regard, the PIX is acting like

- A. A black hole router
- B. A bridge
- C. A router
- D. A brouter
- E. None of the above

Answer: A

QUESTION 239:

The PIX firewall allows users to block Java when using what combination of keywords and implementation?

- A. "no cafebabe" in a static
- B. "no java" in a static
- C. "no cafebabe" in an outbound list
- D. "filter java" in an outbound list

Answer: D

The filter java command filters out Java applets that return to the PIX Firewall from an outbound connection.

Reference:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/config/mngacl.htm#wp1016381

QUESTION 240:

Which network layers are examined by CBAC to make filtering decisions in the IOS Firewall Feature Set environment? (Choose all that apply.)

- A. Transport
- B. Presentation
- C. Data Link
- D. Application
- E. Network

Answer: A, D, E

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 241:

Why do scanning tools may report a root Trojan Horse compromise when it is run against an IOS component?

- A. IOS is based on BSD UNIX and is thus subject to a Root Trojan Horse compromise.
- B. The scanning software is detecting the hard-coded backdoor password in IOS.
- C. Some IOS versions are crashable with the telnet option vulnerability.
- D. The port scanning package mis-parses the IOS error messages.
- E. IOS will not respond to vulnerability scans.

Answer: D

QUESTION 242:

What does a "yellow" sensor icon signify in the Cisco Secure Intrusion Detection System/HP OpenView interface?

- A. A "yellow" sensor icon means that a sensor daemon had logged a level 4 or 5 alarm.
- B. A "yellow" sensor icon means that the director that the sensor reports to is operating in

degraded mode.

C. A "yellow" sensor icon means that a sensor daemon had logged a level 3 alarm.

D. A "yellow" sensor icon means that the device that the sensor detected being attacked is inoperative due to the attack.

Answer: C

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 243:

Symptoms:

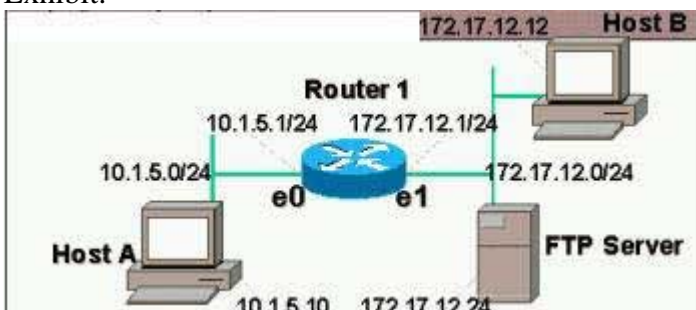
- Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
- Console logging: level warning, 0 messages logged
- Monitor logging: level informational, 0 messages logged
- Buffer logging: level informational, 0 message lines logged

Note: Router 1's CPU is usually above 25% busy switching packets

Scenario:

Host A cannot reach the FTP Server, but can reach Host B. The Certkiller network administrator suspects that packets are travelling from network 10.1.5.0 to the FTP Server, but 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 Certkiller administrator does not see any output. What are the additional commands that he could use to see the packets flowing from Ethernet 0 to Ethernet 1?

- A. terminal monitor
- B. configure terminal
logging console debug
- C. configure terminal

```
no logging buffered
D. configure terminal
logging console debug
interface ethernet1
no ip route-cache
E. configure terminal
interface ethernet0
no ip route-cache
```

Answer: D

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 in debugging 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 244:

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 included 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.
- What would you expect to happen when User _A attempts to edit D:\\word.doc given this scenario on a Windows NT 4.0 network?

A. Insufficient information.

Permissions on Microsoft Word are set within the application and are not subject to file and share level permissions.

B. Local groups cannot be placed into global groups.

The situation could not exist.

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: B

QUESTION 245:

Which of the following is an invalid Cisco Secure Intrusion Detection System function?

A. Cisco Secure Intrusion Detection System sets off an alarm when certain user-configurable strings are matched.

B. Cisco Secure Intrusion Detection System sends e-mail messages at particular alarm levels via eventd.

C. Cisco Secure Intrusion Detection System performs a traceroute to the intruding system.

D. Cisco Secure Intrusion Detection System sends a TCP reset to the intruder when operating in packet sniffing mode.

Answer: C

Explanation: Traceroute is not done.

QUESTION 246:

How does Cisco Secure Intrusion Detection System sensor behave when it detects unauthorized activity?

A. Cisco Secure Intrusion System sensor will send an e-mail to the network administrator.

B. Cisco Secure Intrusion System sensor will send an alarm to Cisco Secure Intrusion Detection System Director.

C. Cisco Secure Intrusion System sensor will shut down the interface where the traffic arrived, if device management is configured.

D. Cisco Secure Intrusion System sensor will perform 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 247:

The newly appointed Certkiller trainee technician wants to know if one can change the situation where every time a typing mistake is made at the exec prompt of a router, the message from the router indicates a lookup is being performed. Also, there is a waiting period of several seconds before the next command can be typed. What will your reply be?

- A. No, this is a default feature of Cisco IOS software.
- B. Yes, by using the no ip domain-lookup command.
- C. Yes, by using the no ip helper-address command.
- D. Yes, by using the no ip multicast helper-map command.
- E. Yes, by using 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 248:

Which network management software installation is a prerequisite for the Cisco Secure Intrusion Detection System Director software?

- A. CiscoWorks 2000 on Unix.
- B. SunNetManager on Solaris.
- C. Microsoft Internet Information Server on Windows NT.
- D. NetSonar on Linux.
- E. HP OpenView on HP-UX or Solaris.

Answer: E

Explanation: The following software must be installed on your workstation:

HP-UX

HP-UX 10.20

HP OpenView 4.1, 5.01, or 6.0

Web browser (for NSDB and help file)

Sun Solaris

Solaris 2.5.1 or 2.6

HP OpenView 4.1, 5.01, or 6.0
Web browser (for NSDB and help file)

QUESTION 249:

What does "counting to infinity" mean in a Distance Vector protocol environment?

- A. "counting to infinity" means calculating the time taken for a protocol to converge.
- B. "counting to infinity" means checking that the number of route entries do not exceed a set upper limit.
- C. "counting to infinity" can occur when Split Horizon is not enabled.
- D. "counting to infinity" means setting an upper limit for hop count, to break down routing loops if this limit is reached.
- E. "counting to infinity" means causing the router to enter an infinite loop and requires the router to be restarted.

Answer: D

QUESTION 250:

On which principle is the "Birthday Attack" based on?

- A. Statistics prove that holidays are focused on "birthdays", and systems are not monitored as carefully during these days.
- B. People using birthdays as passwords.
- C. Two subtly different messages may produce the same hash.
- D. Many systems seed random numbers from a DAY/TIME value.
- E. Statistics show that more than one person must know a birthdate for it to have importance.

Answer: C

A birthday attack is a name used to refer to a class of brute-force attacks. It gets its name from the surprising result that the probability that two or more people in a group of 23 share the same birthday is greater than 1/2; such a result is called a birthday paradox. If some function, when supplied with a random input, returns one of k equally-likely values, then by repeatedly evaluating the function for different inputs, we expect to obtain the same output after about $1.2k^{1/2}$. For the above birthday paradox, replace k with 365.

QUESTION 251:

The Certkiller network is using Cisco Secure Intrusion Detection System and the network traffic pattern appears ordinary. However, numerous false positives for a

particular alarm are received.

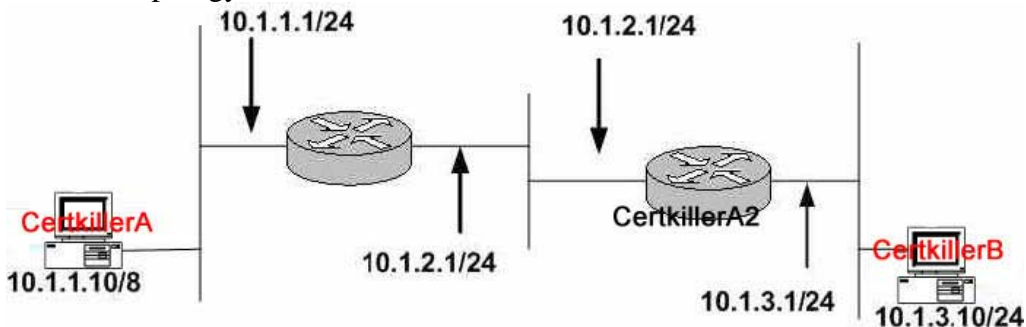
What can you do to avoid the quantity of "noise" in the future?

- A. Click the unmanage for the alarm in question in the HP OpenView/NR GUI interface.
- B. Click the acknowledge for the alarm in question in the HPOV/NR GUI interface.
- C. You can use ventd to decrease the alarm level severity.
- D. You could configure a decreases alarm level severity through nrconfigure.

Answer: D

QUESTION 252:

Network topology exhibit:



Host Certkiller A is the only device that has an 8 bit network mask. When Host Certkiller A needs to send a packet to Host Certkiller B, which are required in order for this to work?

Note: assume both Router Certkiller 1 and Router Certkiller 2 have routing entries for all networks involved.

- A. Host Certkiller A needs to have its default gateway pointing to Router Certkiller 1.
- B. Host Certkiller B needs to have its default gateway pointing to Router Certkiller 2.
- C. Proxy ARP needs to be enabled on Router Certkiller 1.
- D. 'Proxy ARP needs to be enabled on Router Certkiller 2'

Answer: B, C

QUESTION 253:

If an attacker is able to gain shell access with root or administrator privileges, what would be a logical next step to ensure that they could log on again in the future?

- A. Install a program, such as netcat, to initialize on system startup and provide remote access through a network accessible port.
- B. Install a program that can sniff usernames and passwords to the compromised systems.
- C. Install a program that will map the internal network so the attacker can find another

entry point and compromise other systems.

D. Install a DDos and schedule to launch once a week that will bring down the firewall so that attacker can gain network access.

Answer: B

QUESTION 254:

Using Ciscos' Security Device manager on an IOS router, what functions could you expect the security audit option to do for you?

A. Scan for and report open ports.

B. Report IOS vulnerabilities.

C. List identifiable configuration problems and suggest recommendations for fixing them.

D. Configure LAN and WAN interfaces with IP addresses and security related commands.

E. Generate and apply commands to close all unnecessary ports.

Answer: C

SDM also offers a 1-click router lockdown and an innovative Security Auditing capability to check and recommend changes to router configuration based on ICSA Labs, and Cisco TAC recommendations.

Reference:

<http://www.cisco.com/en/US/products/sw/secursw/ps5318/index.html>

QUESTION 255:

The newly appointed Certkiller trainee technician wants to know what PFS (Perfect Forward Security) requires. What will your reply be?

A. AH

B. ESP

C. Another Diffie-Hellman exchange when an SA has expired

D. Triple DES

E. A discrete client

F. All of the above

Answer: C

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

a new security association is negotiated using the Diffie-Hellman exchange.

QUESTION 256:

Which of the following services would you advice the new Certkiller trainee technician to enable on ISO firewall devices?

- A. SNMP with community string public.
- B. TCP small services.
- C. UDP small services.
- D. Password-encryption.
- E. CDP
- F. All of the above.

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 257:

Which file on the Unix system has to be modified to allow copying to occur when a network manager issues an RCP (Remote Copy) when copying a configuration from a router to a Unix system?

- 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 258:

The newly appointed Certkiller trainee technician wants to know what the definition of exploit signatures is in the context of Intrusion detection. What will your reply be?

- A. Exploit Signatures are policies that prevent hackers from your network.
- B. Exploit Signatures are security weak points in your network that are open to exploitation by intruders.
- C. Exploit Signatures are identifiable patterns of attacks detected on your network.
- D. Exploit Signatures are digital graffiti from malicious users.
- E. Exploit Signatures are certificates that authenticate authorized users.

Answer: C

QUESTION 259:

The Certkiller network administrator has forgotten the enable password of the router. There are no users logged into the router, but all passwords on the router are encrypted.

What can the administrator do to recover the enable secret password?

- A. The administrator can reboot the router, press the BREAK key during boot up, and boot the router into ROM Monitor mode to erase the configuration, and re-install the entire configuration as it was saved on a TFTP server.
- B. The administrator can call the Cisco Technical Assistance Center (TAC) for a specific code that will erase the existing password.
- C. The administrator can reboot the router, press the BREAK key during boot up, boot the router into ROM Monitor mode to either erase or replace the existing password, and reboot the router as usual.
- D. The administrator should erase the configuration, boot the router into ROM Monitor mode, press the BREAK key, and overwrite the previous enable password with a new one.

Answer: A

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 260:

Which well-known ports are used for DNS when taking the RCF 1700 into account?

- 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 261:

The newly appointed Certkiller trainee technician wants to know what the purpose of Lock & Key is. What will your reply be?

A.

Lock & Key secures the console port of the router so that even users with physical access to the router cannot gain access without entering the proper sequence.

B. Lock & Key permits Telnet to the router and have temporary access lists applied after issuance of the access-enable command.

C. Lock & Key require additional authentication for traffic travelling through the PIX for TTAP compliance.

D. Lock & Key is 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 262:

IDS tuning requires a step-by-step methodology in order to successfully tune IDS signatures effectively. Put the following tuning steps for a new sensor into their proper order.

A. Identify critical assets that require monitoring and protection.

B. Update sensors with new signatures.

C. Let sensors operate for a period of time generating alarms using the default configuration.

D. Apply initial configuration.

- E. Selectively implement response actions.
- F. Connect sensors to network.
- G. Analyze alarms and tune out false positives.

- A. A, F, D, C, G, E, B
- B. A, C, F, D, G, E, B
- C. A, B, C, D, E, G, F
- D. F, E, G, A, B, C, D

Answer: A

QUESTION 263:

CHAP password encryption uses a secret key on an Access service and an ACS Server to:

- A. Encrypt the passwords
- B. Encrypt the payload
- C. Issue a challenge
- D. Create a hash

Answer: D

QUESTION 264:

Current configuration:

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname Simon  
enable secret 5 $1SXV53$hqb0Ra7gwpky0cmL4u3EW0  
enable password cisco
```

Given the configuration shown above, what should you type to gain enable access on router Simon?

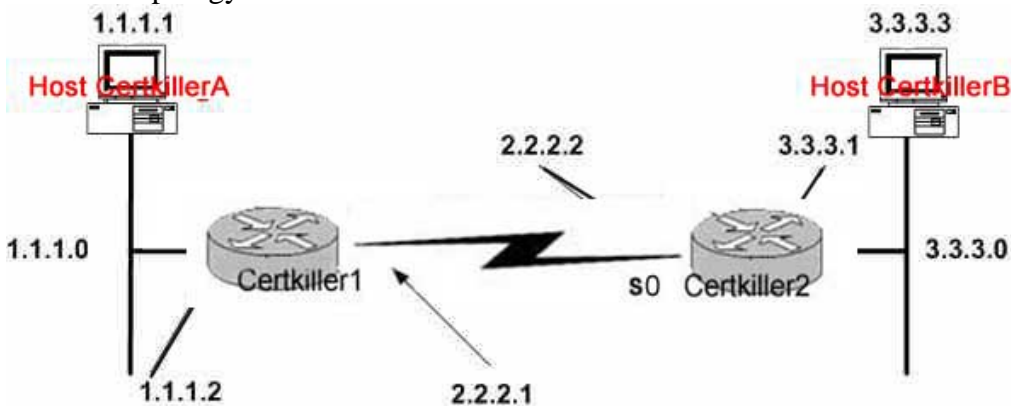
- A. cisco
- B. Simon
- C. 4u3EW0
- D. \$1sXV53\$hqb0Ra7gwpky0cmL4u3EWO
- E. Cannot tell

Answer: E

When an enable secret is specified, it takes precedence over the enable password. The secret password is encrypted and not readable in the config.

QUESTION 265:

Network topology exhibit:



```
Applied to the crypto map on Router Certkiller1's S0 Interface:
match address 101
access-list 101 permit ip host 1.1.1.1 host 3.3.3.3

Applied to the crypto map on Router Certkiller2's S0 Interface:
match address 102
access-list 102 permit ip host 3.3.3.3 host 3.3.3.1
```

Given the shown IPSec scenario:

- A. All traffic between networks 1.1.1.X and 3.3.3.X will be block, except for traffic between hosts 1.1.1.1 and 3.3.3.3.
- B. Traffic between network 1.1.1.X and 3.3.3.X will flow unencrypted. However, for traffic between hosts 1.1.1.1 and 3.3.3.3. These are the tunnel end points and all traffic between these devices will be encrypted.
- C. Most traffic between networks 1.1.1.X and 3.3.3.X will flow unencrypted. However, the traffic between hosts 1.1.1.1 and 3.3.3.3 will be encrypted on the segment between 2.2.2.1 and 2.2.2.2.
- D. Traffic between 1.1.1.1 and 2.2.2.1. will be encrypted, as well s traffic between 2.2.2.2. and 3.3.3.3.

Answer: C

The access-list in the exhibit on router CK2 is incorrect. It should read: "access-list 102 permit ip host 3.3.3.3 host 1.1.1.1". In this corrected scenario, traffic between the two

host addresses 1.1.1.1 and 3.3.3.3 will be encrypted on the serial link between CK1 and CK2 . All other traffic between these subnets will be unencrypted.

QUESTION 266:

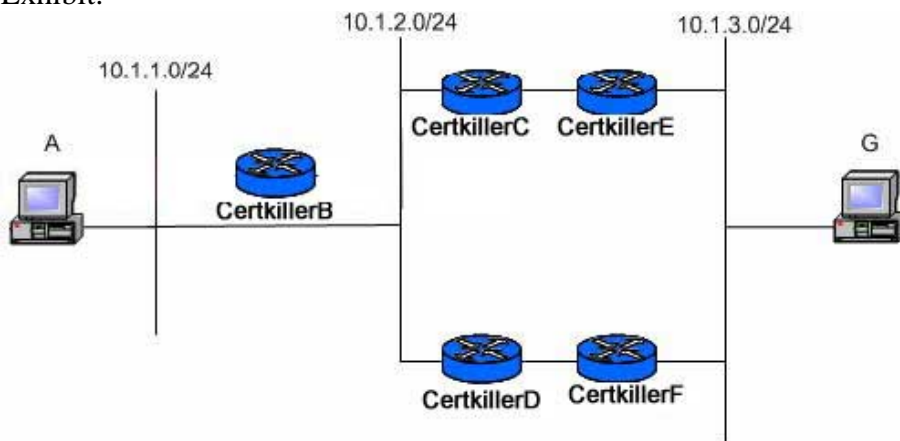
What statement about Diffie-Hellman key exchange is FALSE?

- 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 combines 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

QUESTION 267:

Exhibit:



The network administrator wants only Telnet traffic to travel over the link between Routers Certkiller C and Certkiller E, while all other traffic travels over the link between Routers Certkiller D and Certkiller F.

Is this possible?

- A. No, this strategy is impossible because routers can only route based on a destination address.
- B. The Telnet port traffic can travel the specified link using policy routing. However, there will be no control over the traffic coming from the Telnet port, since access-list can only be configured to look at the destination port number.
- C. Yes, it can be configured to work using extended access-list applied to the links between Routers Certkiller C, and Certkiller E, Certkiller D, and Certkiller F.

- D. Yes, it can be configured to work by making use of policy routing.
The match statements must use extended access-list which will match the traffic sourced from and destined to the telnet ports.
Also, policy routing could be applied to the Ethernet ports on Routers Certkiller B, Certkiller D, and Certkiller F, if routing is configured properly.
E. Yes, this can be enabled by making use of EIGRP with route tags.

Answer: D

QUESTION 268:

The no ip directed-broadcast command is useful in preventing SMURF style attacks for the following reason:

- A. It prevents your network device from being a target.
- B. It prevents your network device from launching an attack.
- C. It prevents your network device from being a reflector in an attack.
- D. It prevents your network device from being traced as the source of an attack.
- E. None of the above.

Answer: D

Reference:

http://www.pentics.net/denial-of-service/presentations/19971027_smurf_files/frame.htm

QUESTION 269:

NTP (Network Time Protocol) or the clock set command must be set up when which features or services are employed on a router? (Select two)

- A. L2TP
- B. Intrusion Detection
- C. Kerberos
- D. PKI

Answer: C, D

QUESTION 270:

What range can Cisco Secure Intrusion Detection System user-definable string-matches have?

- A. Signatures 1000
- B. Signatures 3000

- C. Signatures 8000
- D. Any signature range

Answer: C

8000 series of signature category is string match signatures for the signature types of custom string matches and TCP applications.

Reference:

Page 445, Network Security and Principle and Practices, Cisco press

QUESTION 271:

What is a Trojan Horse?

- A. A malicious program that captures your username and password
- B. Malicious code masquerading as or replacing legitimate code
- C. An unauthorized user who gains access to your user database and adds themselves as a user
- D. A server that is to be sacrificed to all hacking attempts in order to log and monitor the hacking activity

Answer: B

QUESTION 272:

What attack may be successful even though one time passwords are being used for authentication?

- A. Password sniffing
- B. Brute force password attacks
- C. Session hijacking
- D. Key manipulation
- E. Trojan Horse

Answer: B

Several attacks are possible on a one-time password solution:

Brute force attacks

Dictionary attacks

Modified sniffing attacks

Note: Can argue Trojan Horse password attacks as well.

There are several ways in which a password may be snooped directly on the client machine. For instance, someone with root access may maliciously have installed a trojan horse version of an application program or a "wiretap" device driver in the kernel. We can employ OTPs for authentication purposes. Since each password is valid for only one time, the password, if snooped, is not useful for later authentications.

QUESTION 273:

A denial of Service (DoS) attack works on the following principle:

- A. MS-DOS and PC-DOS operating system utilize a weaknesses that can be compromised and permit them to launch an attack easily.
- B. All CLIENT systems have TCP/IP stack implementation weakness that can be compromised and permit them to lunch 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 one those network become flooded.

Answer: D

QUESTION 274:

What would be a reason to decrease the security association lifetime on a router?

- A. To ease the workload on the router CPU and RAM
- B. To give a potential hacker less time to decipher the keying
- C. To improve Perfect Forward Secrecy (PFS)
- D. If the lifetime of the peer router on the other end of the tunnel is shorter, the lifetime on the local router must be decreased so that the SA lifetime of both routers is the same.

Answer: B

QUESTION 275:

If the result of an attack left an ARP table in the state below, what address would you suspect of launching the attack?

Internet 171.16.1.100 - 000c.5a35.3c77 ARPA FastEthernet0/0
Internet 171.16.1.111 0 00bc.d1f5.f769 ARPA FastEthernet0/0
Internet 171.16.1.112 0 00bc.d1f5.f769 ARPA FastEthernet0/0
Internet 171.16.1.113 3 00bc.d1f5.f769 ARPA FastEthernet0/0
Internet 171.16.1.114 0 00bc.d1f5.f769 ARPA FastEthernet0/0

- A. 171.16.1.100
- B. 171.16.1.111
- C. 171.16.1.112

- D. 171.16.1.113
- E. 171.16.1.114

Answer: D

The second column represents the age in minutes of the arp entry. 113 has the oldest age in the arp table and is mapped to the mac address that has flooded the arp table with different IP addresses.

QUESTION 276:

What is the term used to describe an attack that falsifies a broadcast ICMP echo request and includes a primary and secondary victim?

- A. Fraggle Attack
- B. Man in the Middle Attack
- C. Trojan Horse Attack
- D. Smurf Attack
- E. Back Orifice Attack

Answer: D

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 Northcutt 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 277:

A switch has been configured to support MultiLayer Switching (MLS). In addition, Access Control Lists on the MLS-Route Processor have been configured to block all FTP traffic destined to the Internet.

What flow mask will be used to create each shortcut?

- A. Application flow mask
- B. Full flow mask
- C. Destination-Source flow mask
- D. Destination flow mask

Answer: B

There are three types of IP MLS flow-mask modes: destination-ip, source-destination-ip,

and full-flow-ip. This section describes how these three flow-mask modes work.

1. destination-ip-The least-specific flow mask. The PFC maintains one MLS entry for each destination IP address. All flows to a given destination IP address use this MLS entry. In destination-ip mode, the destination IP address of the switched flows are displayed, along with the packet rewrite information: rewritten destination MAC, rewritten VLAN, and egress interface.
2. source-destination-ip-The PFC maintains one MLS entry for each source and destination IP address pair. All flows between a given source and destination use this MLS entry regardless of the protocol-specific Layer 4 port information.
3. full-flow-ip-The most-specific flow mask. The PFC creates and maintains a separate MLS cache entry for each IP flow. A full-flow-ip entry includes the source IP address, destination IP address, protocol, and protocol-specific Layer 4 port information.

Reference:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007e

QUESTION 278:

What statement about AH and ESP is FALSE?

- A. ESP encapsulates the IP header, while AH does not.
- B. ESP uses protocol 50.
- C. AH uses protocol 51.
- D. AH does not lent itself to a NAT environment becayse of IP header encapsulation.

Answer: A

AH-Authentication Header. A security protocol which provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).

ESP-Encapsulating Security Payload. A security protocol which provides data privacy services and optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.

QUESTION 279:

Cisco Security Device Manager uses what protocol to provide a secure connection to the IOS device?

- A. Secure Telnet
- B. SSH
- C. SSL
- D. HTTP
- E. ESP-3DES
- F. AES

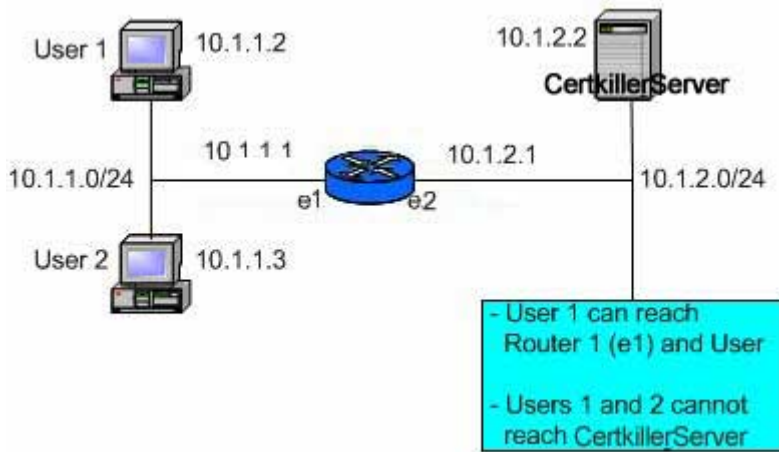
Answer: C

Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_data_sheet0900aecd800fd118.html

QUESTION 280:

Exhibit:



The Network Administrator at Certkiller decides to take a detailed look at the traffic going through the router.

Which of the following represents the proper steps that should be taken to ensure that debugging does not overwhelm the router, while still allowing the administrator to see if the user's traffic reached the router?

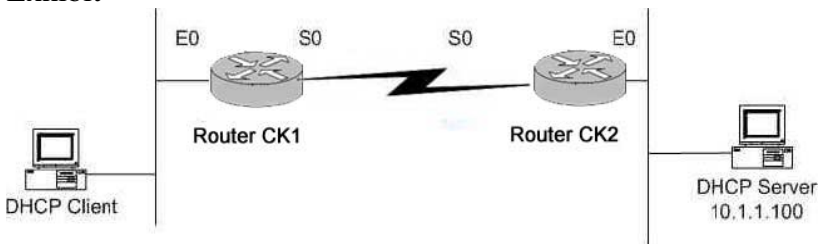
- A. `config t`
`int ethernet0`
`no ip route-cache`
`access-list 1 permit ip 10.1.1.0 255.255.255.0`
`end`
`debug ip packet detail 1`
- B. `config t`
`int ethernet0`
`no ip route-cache`
`access-list 1 permit 10.1.1.0 0.0.0.255`
`end`
`debug ip packet detail 1`
- C. `config t`
`int ethernet1`
`no ip route-cache`
`end`
`debug ip packet detail 10.1.1.0 0.0.0.0.255 any`
- D. `config t`
`int ethernet1`

```
no ip route-cache
access-list 1 permit 10.1.1.0 255.255.255.0
end
debug ip packet detail 1
E. config t
int ethernet1
no ip route-cache
access-list 1 permit 10.1.1.0 255.255.255.0
end debug ip packet detail 1
```

Answer: B

QUESTION 281:

Exhibit



In order for the DHCP client to be able to get a DHCP address upon boot, which is the minimal configuration required?

- A. Enable the command "ip helper-address 10.1.1.100" under the S0 interfaces on both Router CK1 and Router CK2 .
- B. Enable the command "ip helper-address 10.1.1.100" under the E0 interface on Router CK1 .
- C. Enable the command "ip helper-address 255.255.255.255" under the E0 interface on Router CK1 .
- D. Enable the command "ip directed-broadcast" on all interfaces on Router CK1 and Router CK2 .

Answer: B

QUESTION 282:

Using Cisco's Security Device manager on an IOS router, what functions could you expect the security audit option to do for you?

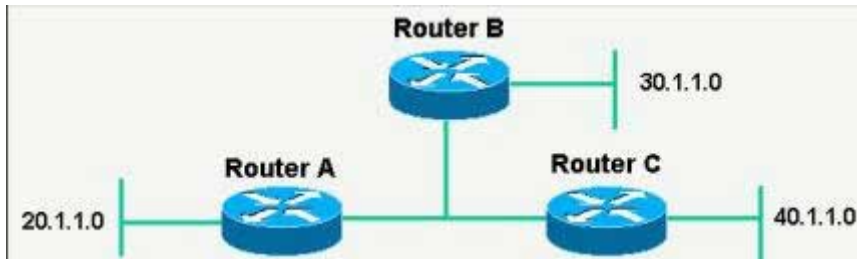
- A. Scan for and report open ports.
- B. Report IOS vulnerabilities.
- C. List identifiable configuration problems and suggest recommendations for fixing them.

- D. Configure LAN and WAN interfaces with IP addresses and security related commands.
- E. Generated and apply commands to close all unnecessary ports.

Answer: C

QUESTION 283:

Exhibit:



Which of the following crypto maps and access list commands should be used to permit the IPsec to handle multiple peers from Router A?

- A. crypto map foo 10 ipsec-isakmp
set peer B
set peer C
match address 101
set trans bar
access-list 101 permit ip 20.1.1.0 0.0.0.255 30.1.1.0
0.0.0.255
access-list 101 permit ip 20.1.1.0 0.0.0.255 40.1.1.0
0.0.0.255
- B. crypto map foo 10 ipsec-isakmp
set peer B
match address 101
set trans bar
crypto map foo 20 ipsect-isakmp
set 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
0.0.0.255
access-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-isakmp
set peer B
match address 101
set trans bar
crypto map foo 20 ipsec-isakmp
set peer C
match address 102

```
set trans bar
access-list 101 permit ip 20.1.1.0 0.0.255 30.1.1.0
0.0.0.255
access-list 102 permit ip 20.1.1.0 0.0.255 40.1.1.0
0.0.0.255
D. crypto map foo 10 ipsec-isakmp
set peer B
match address 101
set trans bar
crypto trans bar
crypto map foo 20 ipsec-isakmp
set 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-isakmp
set peer B
match address 101
set trans bar
crypto map foo 10 ipsec-isakmp
set 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: C

QUESTION 284:

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

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

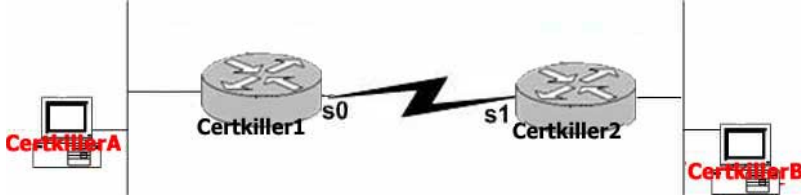
Answer: D

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 285:

Network topology exhibit:



Host Certkiller A and Host Certkiller B are on Ethernet LANs in different buildings. A serial line is installed between two Cisco routers using Cisco HDLC serial line encapsulation. Routers Certkiller 1 and Certkiller 2 are configured to route IP traffic. Host Certkiller A sends a packet to Host Certkiller B. A line hit on the serial line cause an error in the packet. When this is detected, the retransmission is sent by:

- A. Host Certkiller A
- B. Host Certkiller B
- C. Router Certkiller 1
- D. Router Certkiller 2
- E. Protocol analyzer

Answer: A

QUESTION 286:

The BGP backdoor command:

- A. Changes the distance of an iBGP route to 20
- B. Changes the distance of an eBGP route to 200
- C. Changes the distance of an IGP route to 200
- D. Changes the distance of an IGP route to 20
- E. Does not change the distance of the route

Answer: B

BGP Backdoor changes the administrative distance of the configured route learnt via eBGP from 20 (default eBGP Admin Distance) to 200 (which happens to be the same as the default iBGP admin. distance). This will cause IGP protocols (assuming default administrative distances) to take precedence over the BGP backdoor route.

The backdoor command does not change admin distance of the iBGP route to 20, does not change the the IGP AD to 20, and it does change the AD of the (eBGP) route.

QUESTION 287:

A POP3 client contacts the POP3 server:

- A. To send mail
- B. To receive mail
- C. to send and receive mail
- D. to get the address to send mail to
- E. initiate a UDP SMTP connection to read mail

Answer: B

POP is used to receive e-mail.

SMTP is used to send e-mail.

QUESTION 288:

What are the main drawbacks for anti-virus software?

- A. AV software is difficult to keep up to the current revisions.
- B. AV software can detect viruses but can take no action.
- C. AV software is signature driven so new wxploits are not detected.
- D. It's relatively easy for an attacker to change the anatomy of an attack to bypass AV systems
- E. AV software isn't available on all major operating systems platforms.
- F. AV software is very machine (hardware) dependent.

Answer: C

QUESTION 289:

TACACS + and RADIUS authentication can be used on the same router if:

- A. The tacacs extended command is used.
- B. Multilink PPP is setup cottoctly.
- C. Different list names are used and applied to different interfaces.
- D. The login tacacs command is used on some interfaces and the login radius command is used on the remaining interfaces.
- E. The radius mulitsecurity command is used.

Answer: C

QUESTION 290:

In network architecture, which components should be considered security devices?

- A. Routers
- B. Switches
- C. Firewalls
- D. Intrusion detection Appliances
- E. VPN Concentrators
- F. All of the above

Answer: F

QUESTION 291:

What RADIUS AV pair is NOT vendor specific?

- A. Icp:callback-dialstring=3179721407
- B. Ip:callback-rotary=1
- C. Icp:nocallback-verify=1
- D. Farmed-Compression913)=(integer)

Answer: D

Vendor-Specific allows vendors to support their own extended attributes unsuitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification.

Cisco's vendor-ID is 9, and the supported option has vendor-type 1, cisco-avpair. The value is a string of the format:

protocol:attribute sep value

Answer D does not match the format for a vendor specific AV pair

QUESTION 292:

The purpose of RADIUS "check items" is:

- A. To define the attributes to be sent to the NAS
- B. To define the attributes required for authentication
- C. To provide an optional list of attributes that the NAS may choose to enforce or ignore
- D. To define CRC values to aid in packet integrity checks
- E. To flag interesting items for accounting purposes

Answer: B

Radius check items are attributes required for authentication, such as user ID and password.

QUESTION 293:

What statement about RADIUS is true?

- A. User can only be authorized if they have been authenticated first.
- B. Users can only be authenticated if they have been authorized first.
- C. Users can only be authenticated if they have been authorized first.
- D. Accounting can only be run on users that have been authenticated./
- E. Accounting can only be run on users that have been athesized.

Answer: A

QUESTION 294:

In order to send vendor-specific information about callback from a RADIUS server to a Cisco router, a network administrator would use:

- A. Check item 26, vendor code 9, lcp:callback-dialstring=3175551407
- B. Check item 9, vendor code 26, lcp:callback-dialstring=3175551407
- C. Check item 9, reply attribute 26, lcp:callback-dialstring=3175551407
- D. Reply attribute 9, vendor code 26 lcp:callback-dialstring=3175551407
- E. Reply attribute 26, vendor code 9, lcp:callback-dialstring=3175551407

Answer: E

Attribute 26 is used to specify a vendor-specific attribute. Cisco's vendor-ID is 9.

QUESTION 295:

Which of the following statements regarding the RADIUS authentication protocol is valid? (Choose all that apply.)

- 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 "datametrics" service. The officially assigned port number for RADIUS is 1812.

QUESTION 296:

What is the function of the RADIUS attribute represented by the value 26?

- A. It specifies accounting data specific to a particular vendor service.
- B. It specifies the vendor name of the NAS.
- C. It allows vendors to define out-of-band RADIUS timeouts.
- D. It transmits 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 297:

Which of the following statements regarding the DLCI field in the Frame Relay header is valid?

- A. It consists of two portions, namely source and destination, which map data to a logical channel.
- B. It usually only has significance between the local switch and the DTE device.
- C. It is an optional field in the ITU-T specification.
- D. It is only present in data frames that are sent through the network.

Answer: B

Explanation: DLCI is only locally significant

QUESTION 298:

What information will be received from the ISP authentication server when a user dials into the ISP router of a VPDN network as 'dBill@abc.xzy' and the router is using TACACS+ or RADIUS authentication and authorization?

- A. The tunnel-id and IP address of the Home Gateway (HGW) router based on domain abc.xzy.
- B. An access-accept or access-reject (if RADIUS) or a PASS or FAIL (if TACACS) for userid dBill@abc.xzy.
- C. The tunnel-id, IP address of the HGW router, and the IP address of outgoing ISP router interface based on domain abc.xzy.
- D. The IP address of the HGW router and IP address of the outgoing ISP router interface based on domain abc.xzy.

Answer: B

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

QUESTION 299:

The newly appointed Certkiller trainee technician wants to know what are the only two part found in a RADIUS user profile. What will your reply be?

- A. Reply attributes, check attributes
- B. Check items, reply attributes
- C. Check attributes, reply items
- D. Reply items, check items

Answer: B

Explanation:

http://www.cisco.com/en/US/products/sw/secursw/ps4911/products_user_guide_chapter09186a008015c5bc.htm

Step 7 Specify RADIUS-Cisco Check Item and Reply attributes:

- a. Click the RADIUS-Cisco attribute icon in the Profile pane. This displays the RADIUS-Cisco Options menu in the Attributes pane.
- b. Select Reply Attributes and Check Items in the Options menu and click Apply.

QUESTION 300:

Which of the following is never included in a RADIUS Access-Accept response?

- A. The type of service
- B. An Access-Challenge
- C. An IP Address
- D. The MTU
- E. The user's encrypted password, using the shared secret key as an MD5 hash key.

Answer: E

QUESTION 301:

The Certkiller network administrator was requested to design a dial-in solution that will allow both scripted login for dial-in clients and pure PPP login for packet mode connections. The network administrator must configure the NAS to authenticate both types of users with RADIUS.

Assuming the lines and interfaces are configured correctly, which of the following represents the correct AAA authentication configuration?

- A. aaa new-model
aaa authentication login default radius
aaa authentication ppp default-if-needed radius
- B. aaa new-model
aaa authentication default radius
- C. aaa new-model
aaa authentication slip default radius
aaa authentication ppp default radius
- D. aaa new-model
aaa authentication radius default
- E. aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius

Answer: A

QUESTION 302:

What are the reasons for the differences in convergence for Link State protocols and Distance Vector protocols in general? (Choose all that apply.)

- A. Poison reverse updates are sent by link state protocols.
- B. The Designated Router handles route calculation centrally and updates all routers.
- C. Link state updates are sent to all routers through "flooding".
- D. Periodical partial updates from all routers can be processed more quickly than regular full updates from neighbors.

Answer: B, D

QUESTION 303:

With regard to the CERT/CC, which of the following is true.

- A. It is a clearinghouse for security and vulnerability information.
- B. It maintains Secure Computing standards.
- C. It provides Certificates of Authority services for the public.
- D. It coordinates orchestrated attacks on political network targets.
- E. It is in charge of issuing new TLAs for new technologies.

Answer: A

QUESTION 304:

You are the network administrator at Certkiller. Certkiller has a CiscoSecure UNIX. Your newly appointed Certkiller trainee technician wants to know how RADIUS debugging is turned on for the CiscoSecure UNIX. What will your reply be?

- A. Set the server value to debug in the advanced GUI, and modify the syslog.conf and CSU.cfg files.
- B. Modify the syslogd.conf and CSU.cfg files.
- C. Modify the CSU.cfg file.
- D. Issue the debug radius command.
- E. Issue the debug UNIX command.

Answer: A

QUESTION 305:

Cisco's RADIUS implementation supports one vendor-specific option using which of the following formats?

- A. Vendor-ID 26, and the supported option has vendor-type 1, which is named "cisco-avpair".
- B. Vendor-ID 9, and the supported option has vendor-type 26, which is named "cisco-avpair".
- C. Vendor-ID 9, and the supported option has vendor-type 1, which is named "cisco-avpair".
- D. Vendor-ID 1, and the supported option has vendor-type 9, which is named "cisco-avpair".
- E. Vendor-ID 1, and the supported option has vendor-type 9, which is named extended "cisco-avpair".
- F. All of the above.

Answer: C

QUESTION 306:

Why would you advise the new Certkiller trainee technician to configure a "clients" file on a RADIUS server?

- A. To define a list of remote node devices that users may use for connectivity to the network.
- B. To define a list of IP hosts that are granted permissions to administer the RADIUS database.
- C. To define a list of users and their access profiles.
- D. To define a list of NASs the RADIUS server for communication purposes.
- E. All of the above.

Answer: D

QUESTION 307:

Exhibit:

CA Certificate

Status: Available

Certificate Serial Number: 68690A1A21B65B343679274B37E7BB

Key Usage: Signature

CN = Version CertServer

OU = user

O = user

L = User City

ST = CA

C = US

EA =<16> user@anyone.com

Validity Date:

start date: 14:32:48 PST Mar 17 2000

end date: 14:41:28 PST Mar 17 2002

You are the network administrator at Certkiller . You are experiencing problems getting two IPSec routers to authenticate using RSA-sig as an authentication method. The output of the IOS command show crypto ca cert yields the above output.

What is the most probable reason for this authentication failure?

- A. The certificate has a leading one in the serial number field which violated the x.509 certificate standard.
- B. The router has not yet obtained an identity certificate from the root CA.
- C. The current date of the router is out of the range of the certificate's validity date.
- D. The root CA has rejected the other routers attempt to authenticate.

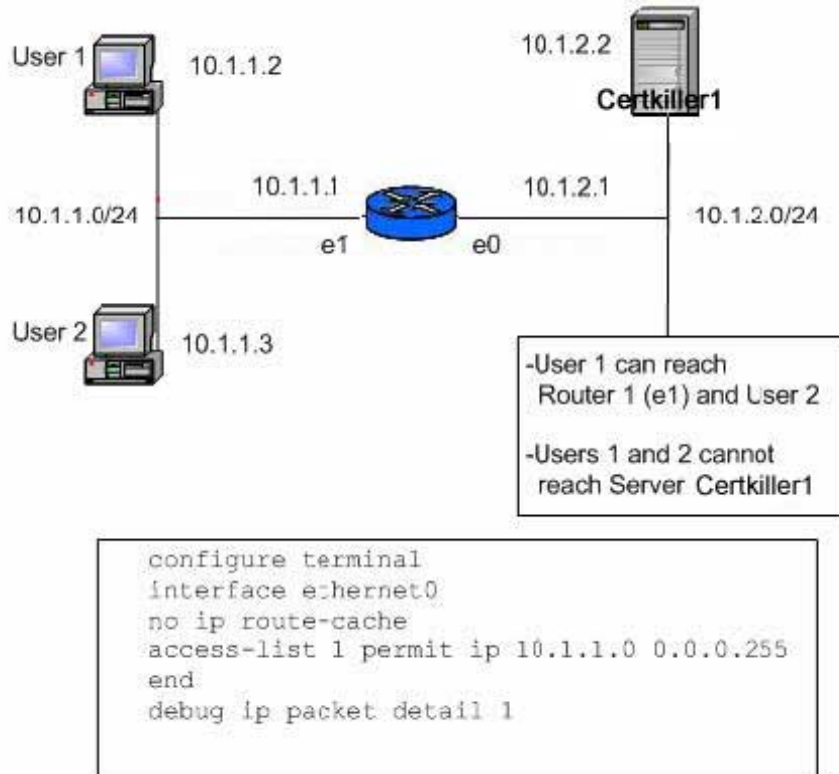
E. None of the above.

Answer: C

As the current date are out of the range of the validity date , the IPSec peers could not authenticate each other..

QUESTION 308:

Exhibit:



The Certkiller Network Administrator can view user traffic reaching the router. However, the administrator also wants to see the return traffic from the server as well.

What other commands is necessary to be configured to enable viewing both the outgoing and return traffic, without overwhelming the router?

A. config t

int ethernet1

no ip route-cache

end

B. config t

int ethernet0

no ip route-cache

end

debug ip packet detail any 10.1.1.0 0.0.0.255

```
C. config t
int ethernet0
no ip route-cache
access-list 1 permit 10.1.1.0 255.255.255.0
end
debug ip packet detail 1
D. config t
int ethernet1
no ip route-cache
no access-list 1
access-list 101 permit ip 10.1.1.0 0.0.0.255 any
access-list 101 permit ip any 10.1.1.0 0.0.0.255
end
debug ip packet detail 101
E. config t
int ethernet1
no ip route-cache
access-list 101 permit ip 10.1.1.0 0.0.0.255 any
access-list 101 permit ip any 10.1.1.0 0.0.0.255
end
debug ip packet detail 101
```

Answer: E

QUESTION 309:

What would the Certkiller network administrator use in order to send vendor-specific information about callback from a RADIUS server to a Cisco router?

- A. Check item 26, vendor code 9, lcp:callback-dialstring=3175551407
- B. Check item 9, reply attribute 26, lcp:callback-dialstring=3175551407
- C. Reply attribute 9, vendor code 26, lcp:callback-dialstring=3175551407
- D. Check item 9, vendor code 26, lcp:callback-dialstring=3175551407
- E. Reply attribute 26, vendor code 9, lcp:callback-dialstring=3175551407

Answer: E

Attribute 26 is used to specify a vendor-specific attribute. Cisco's vendor-ID is 9.

QUESTION 310:

Exhibit:

```
aaa authentication login default local tacacs
aaa authorization exec default tacacs
aaa authentication login vty tacacs local
aaa authentication exec vty tacacs login:authenticated
user authentication login
line vty 0 4
exec-timeout 0 0
```

If a router running IOS is configured as shown and the TACACS server is down, what will happen when someone telnetts into the router?

- A. Using the local username, the user will pass authentication but fail authorization.
- B. The user will be able 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: A

Not B: list "vty" is not applied on the vty lines.

QUESTION 311:

What answer describes a network service that would be flagged as high risk and disabled by SDM?

- A. SNMP
- B. FTP
- C. SSH
- D. TELNET

Answer: A

QUESTION 312:

Which statements about TACACS+ are true? (Select three)

- A. If more than one 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

QUESTION 313:

What is the best explanation for the command `aaa authentication ppp default if-needed tacacs+`?

- 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

The if-needed option tells the router to perform the specified authentication only if the user has not been authenticated by another method.

QUESTION 314:

Which of the following statements regarding TACACS+ is valid? (Choose all that apply.)

- A. Whenever more than one 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. If a key is used at both ends, the TACACS+ server's connection to the NAS encrypts the entire packet.
- C. UDP must be used by the TACACS+ server for its connection to the NAS.
- D. TCP or UDP for the NAS connection must be configured on the TACACS+ server.
- E. TCP must be used by the TACACS+ server for its connection to the NAS.

Answer: A, B, E

Explanation: PIXFirewall 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 315:

In which way 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 316:

What is the function of gratuitous ARP? (Choose all that apply.)

- A. ARP refreshes other devices' ARP caches after reboot.
- B. ARP will look for duplicate IP addresses.
- C. ARP refreshes the originating server's cache every 20 minutes.
- D. ARP will identify stations without MAC addresses.
- E. ARP will 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 2

Gratuitous 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 initialising 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 initialisation.

QUESTION 317:

To what does "message repudiation" refer to what concept in the realm of email security?

- A. Message repudiation means a user can validate which mail server or servers a message was passed through.
- B. Message repudiation means a user can claim damages for a mail message that damaged their reputation.
- C. Message repudiation means a recipient can be sure that a message was sent from a particular person.
- D. Message repudiation means a recipient can be sure that a message was sent from a certain host.
- E. Message repudiation means 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 318:

What is the function of a RARP?

- A. A RARP is sent to map a hostname to an IP address.
- B. A RARP is sent to map an IP address to a hostname.
- C. A RARP is sent to map a MAC address to an IP address.
- D. A RARP is sent to map a MAC address to a hostname.
- E. A RARP is sent to map an IP address to a MAC address.

Answer: C

Explanation:

RARP is used to translate hardware interface addresses to protocol addresses

QUESTION 319:

What is the sequence number in the TACACS+ protocol? (Select two.)

- A. It is an identical number contained in every packet.
- B. The sequence number is a number that must start with 1 (for the first packet in the session) and increment each time a request or response is sent.
- C. The sequence number is always an odd number when sent by the client.
- D. The sequence number is 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 in 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 $2^{32}-1$ 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 320:

In the IPSec protocol suit, 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: A, D

The AH provides connectionless data integrity and data origin authentication of IP packets, but does not provide confidentiality through encryption. ESP does allow encryption but does not protect the new IP header, so for strong authentication plus confidentiality, AH and ESP can be deployed in tandem in either transport mode or tunnel mode.

QUESTION 321:

Which methods can be used to encrypt all communication between a client and a Cisco router (Multiple answer):

- A. RADIUS
- B. Secure-shell
- C. Kerberized telnet
- D. TACACS+
- E. XTACACS

Answer: B, C

Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over unsecure channels.

Kerberos is a secret-key network authentication protocol, developed at the Massachusetts Institute of Technology (MIT), that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Telnet is one of the network services supported by Kerberos.

QUESTION 322:

In which of the following ways does a Hash (such as MD5) differs from an Encryption (such as DES)?

- A. A hash is easier to break.
- B. Encryption cannot be broken.
- C. A hash, such as MD5, has a final fixed length.
- D. A hash is reversible.
- E. Encryption has a final fixed length.
- F. None of the above.

Answer: C

Explanation: The MD5 algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally 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 cleartext 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"

Managing Cisco Network Security by Michael Wenstrom pg 464

QUESTION 323:

What is the maximum number of combinations of a key is possible with a 56-bit key?

- A. 1056
- B. 228
- C. 256
- D. 56
- E. 56000

Answer: C

QUESTION 324:

Which of the following ports are commonly used for Kerberos communication:

- A. TCP Port 534
- B. TCP/UDP Port 634
- C. TCP/UDP Port 88
- D. UDP Port 527
- E. None of the above.

Answer: C

QUESTION 325:

Which three protocols are typically required to tunnel IPSec Traffic, including Multicast?
(Select three)

- A. ESP
- B. NTP
- C. SCEP
- D. ISAKMP
- E. ICMP
- F. GRE
- G. CEP

Answer: A, D, F

QUESTION 326:

What type of ICMP unreachable packet is using in conjunction with IPSec to allow normal operations of PMTU discovery?

- A. ICMP type 3 code 4
- B. ICMP type 3 code 3
- C. ICMP type 3 code 2
- D. ICMP type 3 code 1

Answer: A

Path MTU (PMTU) is used to discover the maximum packet size that can be sent without fragmentation.

ICMP type 3 codes:

- 1 Host Unreachable
- 2 Protocol Unreachable
- 3 Port Unreachable
- 4 Fragmentation Needed and Don't Fragment was Set

QUESTION 327:

In the IPSec suite of protocols, which are two of the main fields of the Security Association? (Multiple answer)

- A. SPI
- B. Connection ID
- C. Proxy IP addresses
- D. BIA (Burned in Address)
- E. MAC address

Answer: A, B

QUESTION 328:

What is NOT an example of supported ISAKMP credentials?

- A. Pre-shared
- B. RSA
- C. Certificate authority
- D. Perfect Forward Secrecy

Answer: D

QUESTION 329:

What strategy best describes how to pass EIGRP update through an IPSec tunnel?

- A. Define the IPSec tunnel as an interface on the router and specify that interface in the EIGRP configuration
- B. Define the IPSec proxy to allow and accept broadcast traffic
- C. Define the IPSec proxy to allow only EIGRP traffic through the tunnel
- D. Define a GRE tunnel, send the EIGRP updates through the GRE and encrypt all GRE traffic

Answer: D

QUESTION 330:

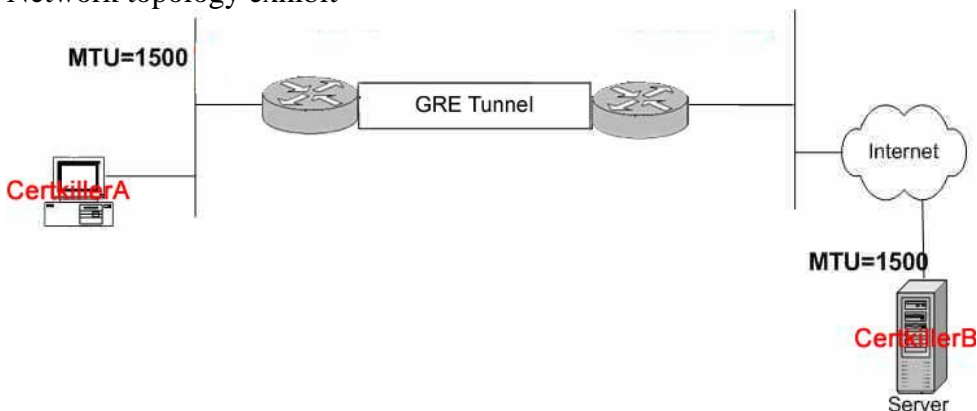
Cipher text can be defined as:

- A. The key used to encrypt a message
- B. The public key that has been exchanged with a peer and is used to determine the original message
- C. The post-encrypted message that travels on the wire
- D. The key used for a one way hash in an IPSec Phase Two exchange
- E. The result of a message after it has been decrypted on the receiving end

Answer: C

QUESTION 331:

Network topology exhibit



The client Certkiller A can ping through the GRE tunnel to the Certkiller B server and receive small files just fine, but large web page download and file transfer will

fail. "debug ip icmp" on router 2 shows "frag. Needed and DF set unreachable" messages sent to the server. Which are possible solutions to this problem?

- A. If the physical link between Router Certkiller 1 and Router Certkiller 2 can support a MTU size greater than 1524 bytes, then increase the interfaces MTU between the tunnel and points to greater than 1524 bytes, then
- B. Decrease the physical interface MTU between the tunnel and points to less than 1476 bytes.
- C. Increase the IP MTU on the tunnel interfaces to 1500
- D. Enable "ip unreachable" on all interfaces on Router Certkiller 2
- E. Check to see if there is a filtering device between Router Certkiller 2 and the server that's blocking ICMP messages. If so, change the filter rule to allow ICMP

Answer: A

QUESTION 332:

What would the recommended way to secure a credit card number on a public server?

- A. Encrypt the credit card number with a key known only by the admin or root account
- B. Encrypt the credit card number with a key derived by a combination of identity and password information entered by the user when they log onto the server
- C. Encrypt the credit card number with a randomly generated key hash under control of the admin or root account
- D. Encrypt the credit card number with a fixed key but regenerate the key on a frequent basis

Answer: B

QUESTION 333:

What IPSec component is used to ensure the integrity of the in an IP packet?

- A. ESP-DES
- B. AH
- C. IPSH
- D. TTL

Answer: B

QUESTION 334:

What built-in feature of the IPSec header is used to protect against replay attacks?

- A. Initialization vector
- B. Redundancy tag
- C. Resend cookie
- D. Header CRC
- E. Sequence number

Answer: E

A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence. The Sequence Number field is designed to thwart such attacks.

QUESTION 335:

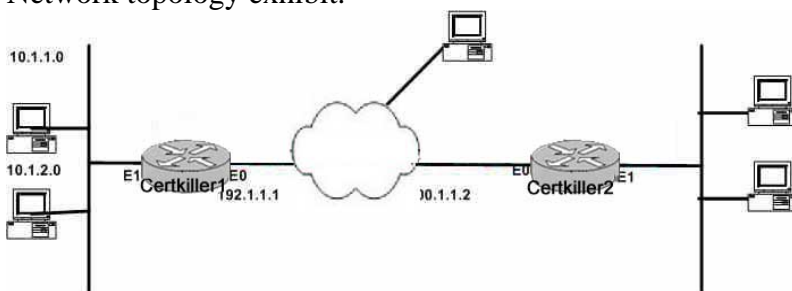
Assuring two systems that are using IPSec to protect traffic over the internet, what type of general attack could compromise the data? (Select one)

- A. Spoof Attack
- B. Smurf Attack
- C. Man in the Middle Attack
- D. Trojan Horse Attack
- E. Back Orifice Attack

Answer: C

QUESTION 336:

Network topology exhibit.



In the shown debugs from the router 192.1.1.1, why are outbound IPSec packets in the debugs not seen?

IP: s=200.1.1.2(Ethernet0), d=192.1.1.1(Ethernet0), len 136, rcvd3, proto=50

IP: s=10.1.2.2 (Ethernet0), d=10.1.1.10 (Ethernet1), g=10.1.1.10, len 84, forward
ICMP type=8, code=0

IP: s=10.1.1.10 (Ethernet1), d=10.1.2.2 (Loopback0), g=10.0.0.2, len 84, forward
ICMP type=0, code=0

- A. Router debugging works by displaying the packet in the outbound direction before IPSec is applied to the outbound packet.
- B. IPSec proxies do not match at either end.
- C. There would be no debugs because the return pings would not go through the IPSec tunnel.
- D. The crypto map is not correctly applied to the outbound interface 192.1.1.1.

Answer: A

QUESTION 337:

What statement is FALSE about Simple Certificate Enrollment Protocol (SCEP)?

- A. SCEP is used to obtain the CA's certificate.
- B. SCEP uses HTTP as a transport mechanism.
- C. SCEP is used to obtain CRLs.
- D. SCEP is used for router to router communication to check the peer's enrollment certificate.

Answer: D

QUESTION 338:

A remote user tries to login to a secure network using Telnet, but accidentally types in an invalid user name or password. Which responses would NOT be preferred by an experienced Security Manager? (multiple answer)

- A. Invalid Username
- B. Invalid Password
- C. Authentication Failure
- D. Login Attempt Failed
- E. Access Denied

Answer: A, B

As little information as possible should be given about a failed login attempt. Invalid username or password is not desirable.

QUESTION 339:

Which are the correct port numbers use for IPSec communication?

- A. IP Protocol 51 for ESP, IP Protocol 50 for AH
- B. IP Protocol 50 for ESP, IP Protocol 51 for AH
- C. IP Protocol 51 for ESP, IP Protocol 500 for AH
- D. TCP 51 for ESP, TCP 50 for AH
- E. TCP 50 for ESP, TCP 51 for AH

Answer: B

ESP uses IP protocol 50, AH uses IP protocol 51.

QUESTION 340:

Exhibit:



```
CA Certificate
Status: Available
Certificate: 76B74FB37E76B7E76B76B74FB37E76B76B74FB37E76B
Key Usage: Signature
CN = Versign CertServer
OU = user
O = user
L = User City
ST = CA
C = US
EA = <16> user@anyone.com
Validity Date
start date: 14:32:48 PST Mar 17 2000
end date: 14:41:28 PST Mar 17 2002
```

A network Admin is having problems getting two IPSec routers to authenticate using RSA-sig as an authentication method. The output of the IOS command show crypto ca cert yields the following output. What is the likely reason for the authentication failure?

- A. The current date of the router is out of the range of the certificate's validity date.
- B. The certificate has a leading one in the serial number field which violated the x.509 certificate standard.
- C. The router has not yet obtained an identity certificate from the root. CA.
- D. The root CA has rejected the other routers attempt to authenticate.

Answer: A

QUESTION 341:

Exhibit:

Router Certkiller1

```
access-list 101 permit ip 10 1.1.0 0.0.0.255 20.1.1.0 0.0.0.255
```

Router Certkiller2

```
access-list 101 permit ip host 20.1.1.0 10.1.1.0 0.0.0.255
```

The security Manager has configured two router with the IPSec access lists shown. What behavior is expected if a telnet is launched from 20.1.1.20, destined for 10.1.1.10?

- A. Traffic from 10.1.1.0/24 from Router Certkiller 1 will be encrypted when going to addresses 20.1.1.0/24 on Router.
- B. Telnet traffic to and from 20.1.1.10 will be encrypted.
- C. Phase Two negotiation will fail with invalid proxies and traffic will not flow.
- D. Phase Two will pass, but traffic will to be encrypted.

Answer: C

QUESTION 342:

The Certkiller 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, the administrator received a report that encrypted traffic is never successfully sent between the two endpoints. What is a possible cause?

- A. NAT could be running between the two IPSec endpoints.
- B. A mismatched transform set between the two IPSec endpoints.
- C. There is a NAT overload running between the two IPSec endpoints.
- D. Mismatched IPSec proxy between the two IPSec endpoints.

Answer: C

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 343:

The newly appointed Certkiller trainee technician want to know which of the following represents the principles of a one way hash function. What will your reply

be? (Choose two.)

- A. A fixed length output is created from a variable length input by a hash function.
- B. A hash function cannot be random and the receiver cannot decode the hash.
- C. A hash function is usually operated in an IPSec environment to provide a fingerprint for a packet.
- D. A hash function must be easily decipherable by anyone who is listening to the exchange.

Answer: A, C

Explanation: Developers use a hash function on their code to compute a digest, 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 344:

What is the consequence that one can expect when an IPSec authentication header (AH) is used in conjunction with NAT on the same IPSec endpoint?

- A. NAT has no impact on the authentication header.
- B. IPSec communication will fail due to AH creating a hash on the entire IP packet before NAT.
- C. Only IKE will fail due to AH using only IKE negotiation.
- 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 345:

Which of the following statements regarding SNMP v1 community strings is valid?

- A. SNMP v1 community strings are encrypted across the wire.
- B. SNMP v1 community strings can be used to gain unauthorized access into a device if the read-write string is known.

- C. SNMP v1 community strings are always the same for reading & writing data.
- D. SNMP v1 community strings 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 346:

How many IPSec security associations should be active on the system under normal circumstances, after a single IPSec tunnel has been established?

- 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 347:

Which of the following does NOT qualify to be an example of a supported ISAKMP keying mechanism?

- A. Pre-shared
- B. Perfect Forward Secrecy
- C. RSA
- D. Certificate authority

Answer: B

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 348:

What does the transport mode & tunnel mode in the IPSec protocol suite describe?

- A. It describes AH header and datagram layouts.
- B. It describes Diffie-Hellman keying.
- C. It describes SHA security algorithm.
- D. It describes ESP header and datagram layouts.

Answer: D

Explanation: OK I dont get this question ESP or AH can be used in tunnel or transport mode. - CCIE PROfessional Development Network Security Pratices and Principles by Saadit Malik pg 313-316 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 349:

Exhibit:

/etc/hosts.equiv:

2.2.2.2

/etc/passwd:

user_B:x:1003:1:User B:/export/home/user_B:/bin/ksh

user_C:x:1004:1:User C:/export/home/user_C:/bin/ksh

with host_B having the ip 2.2.2.2 & host C having the ip

3.3.3.3

Given the files shown in the exhibit, which policy would be enforced?

- A. Allow user_B on Host_B to access host_A via rlogin, rsh, rcp, & rcmd without a password.
- B. Allow users to telnet from host_B to host_A but prevent users from telnetting from unlisted hosts including host_C
- C. Allow users on host_A to telnet to host_B but not to unlisted hosts including host_C
- D. 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

Answer: A

QUESTION 350:

Given the situation where two routers have their SA lifetime configured for 86399 seconds and 2 million kilobytes. What will happen after 24 hours have passed and 500 KB of traffic have been tunneled?

- 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. Unencrypted traffic will be sent.

Answer: B

Explanation: more or less 86399 seconds is 23.9 hours however 86400 is 24 hours so the SA need to be renegotiated

QUESTION 351:

The Certkiller Security Manager needs to configure an IPSec connection using ISAKMP with routers from mixed vendors. Which information would be superfluous when configuring the local security device to communicate with the remote machine?

- A. Remote peer address.
- B. Main mode attributes.
- C. Peer gateway subnet.
- D. Quick mode attributes.
- E. Addresses that need to be encrypted.
- F. Encryption authentication method.

Answer: C

Explanation: The peers gateway subnet is not needed. The address is needed.

QUESTION 352:

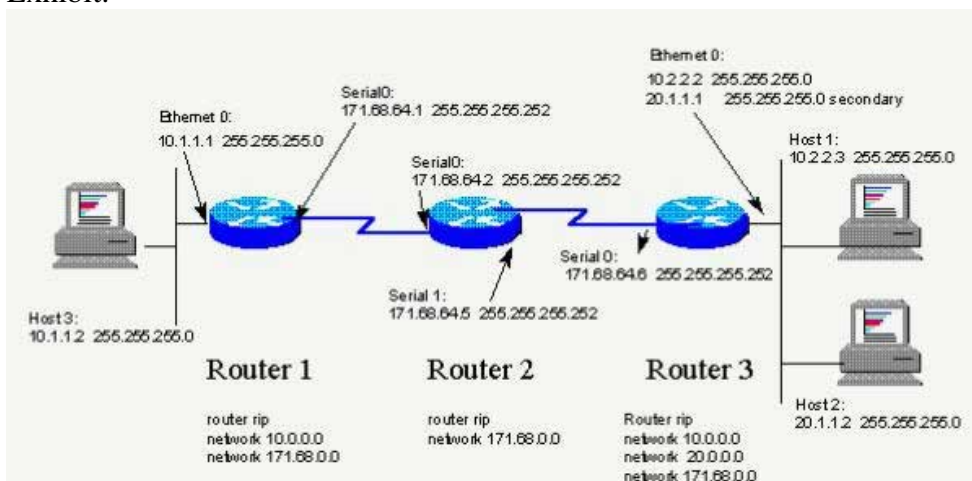
Why is an ISAKMP NOTIFY message used between IPSec endpoints?

- A. ISAKMP NOTIFY message informs the other side of failures that occurred.
- B. ISAKMP NOTIFY message informs the other side of the status of an attempted IPSec transaction.
- C. ISAKMP NOTIFY message informs the other side when a physical link with an applied SA has been torn down.
- D. ISAKMP NOTIFY message informs the other side when an SA has been brought up on an unstable physical connection; potential circuit flapping can cause problems for SPI continuity.

Answer: B

QUESTION 353:

Exhibit:



What could be the most likely reason why Host 1 cannot ping Host 2 and Host 2 cannot ping Host 1?

- A. Split horizon issue.
- B. Default gateway on hosts.
- C. Routing problem with RIP.
- D. All of the above.

Answer: B

As in the Exhibit, Host 1 and Host 2 are physically in same segment but logically different subnet, only the possible cause is default gateway setting in each host. If the question says Host 1 cannot PING Host 3 and Host 3 cannot PING host1, then D is the correct answer.

QUESTION 354:

Which of the following statements regarding the Diffie-Hellman key exchange is invalid?

- A. The local secret key is combined with known prime numbers n and g in each router for the purposes of generating a Public key.
- B. Each router uses the received random integer to generate a local secret (private) crypto key.
- C. Each router combines the private key received from the opposite router with its own public key in the creation of a shared secret key.
- D. The two routers involved in the key swap generate large random integers (i), which are exchanged covertly.

Answer: A

Diffie-Hellman refers to a type of public key cryptography using asymmetric encryption based on

large prime numbers to establish both Phase 1 and Phase 2 SAs.

Key words here are PRIME NUMBERS. So answers B and D are out.

next:

<http://www.securitydocs.com/library/2978>

The process begins when each side of the communication generates a private key (depicted by the

number 1 in Figure 1). Each side then generates a public key (number 2), which is a derivative of

the private key. The two systems then exchange their public keys. Each side of the communication

now has their own private key and the other systems public key (number 3).

So this rules out answer C. Private keys are NEVER exchanged.

In the article you can find that answer A is correct but its long and complicated.

QUESTION 355:

Exhibit:

Configuration of Router A:

```
crypto map tag 1 ipsec-isakmp  
set security-association lifetime seconds 240  
set security-association lifetime kilobytes 10000
```

Configuration of Peer Host Router B:

```
crypto map tag 1 ipsec-isakmp  
set security-association lifetime seconds 120  
set security-association lifetime kilobytes 20000
```

Router A is configured as shown. What situation will you encounter after 110 seconds and 1500 kilobytes of traffic?

- A. There will be no communication between Router A and 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 of traffic have traversed the link, because the interval will be the greater of 2 parameters - time and kilobytes.
- C. Security association renegotiation will have started by default
- D. The present security associations will continue until almost 240 seconds have elapsed, assuming the same traffic pattern and rate.

Answer: C

QUESTION 356:

The newly appointed Certkiller trainee technician wants to know which encryption algorithm is used for Microsoft Point-to-Point Encryption. What will your reply be?

- 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 357:

What type of crypto maps and keying mechanism would advise the new Certkiller trainee technician to 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: C

QUESTION 358:

You are the Certkiller network administrator. The Certkiller network is using Certificate Authorizes (CA) for ISAKMP negotiation. You want to configure ISAKMP.

Which of the following will work? (Select one)

- A. crypto isakmp policy 4
authentication cert-rsa
- B. crypto isakmp policy 4
authentication ca
- C. cpto isakmp policy 4
authentication cert-sig
- D. crypto isakmp policy 4
authentication rsa-sig
- E. cryptp isakmp policy 4
authentication rsa-enc

Answer: D

QUESTION 359:

You are the network administrator at Certkiller . A workstation on the Certkiller network has been the victim of a program that invokes a land.c attack. The newly appointed Certkiller trainee technician wants to know what this program does. What will your reply be?

- A. It sends a stimulus stream of ICMP echo requests ("pings") to the broadcast address of the reflector subnet, the source addresses of these packets are falsified to be the address of the ultimate target.
- B. It sends a stimulus stream of UDP echo requests to the broadcast address of the reflector subnet, the source addresses of these packets are falsified to be the address of the ultimate target.
- C. It sends an IP datagram with the protocol field of 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.

D. It sends a TCP SYN packet (a connection initiation), giving the target host's address as both source and destination, and using the same port on the target host as both source and destination.

Answer: D

QUESTION 360:

You are the network administrator at Certkiller . You want to pass RIP updates through an IPSec tunnel. What should you do?

- A. Define the IPSec tunnel as an interface on the router and specify that interface in the RIP configuration.
- B. Define the IPSec proxy to allow and accept broadcast traffic.
- C. Define the IPSec proxy to allow only RIP traffic through the tunnel.
- D. Define a GRE tunnel, send the RIP updates through the GRE and encrypt all GRE traffic.

Answer: D

QUESTION 361:

Which off the following lists the correct port numbers required for IPSec communication?

- A. UDP 500 ISAKMP, IP Protocol 51 for ESP, IP Protocol 50 for AH
- B. UDP 500 ISAKMP, IP Protocol 50 for ESP, IP Protocol 51 for AH
- C. UDP 500 ISAKMP, IP Protocol 51 for ESP, IP Protocol 500 for AH
- D. UDP 500 ISAKMP, TCP 51 for ESP, TCP 50 for AH
- E. UDP 500 ISAKMP, TCP 50 for ESP, TCP 51 for AH

Answer: B

QUESTION 362:

How can a Denial of Service (DoS) attack to a Firewall device be carried out?

- A. By flooding the device through sending excessive mail messages to it..
- B. Sending excessive UDP packets to it.
- C. By sending more packets to the device that it can process.
- D. Sending ICMP pings with very large data lengths to it.

E. All of the above.

Answer: E

QUESTION 363:

Which of the following IPSec components can be used to ensure the integrity of the data in an IP packet?

- A. ESP
- B. IPSH
- C. AH
- D. TTL
- E. None of the above.

Answer: C

QUESTION 364:

How would you characterize the source and type in a denial of service attack on a router?

- A. By performing a show ip interface to see the type and source of the attack based upon the access-list matches.
- B. By performing a show interface to see the transmitted load (txload) and receive load (rxload); if the interface utilization is not maxed out, there is no attack underway.
- C. By setting up an access-list to permit all ICMP, TCP, & UDP traffic with the log or log-input commands, then use the show access-list and show log commands to determine the type and source of attack.
- D. By applying an access-list to all incoming & outgoing interfaces, turn off route-cache on all interfaces, then, when telnetted into the router perform a debug ip packet detail.

Answer: C

QUESTION 365:

The Certkiller Network Administrator makes use of manual keys in her IPSec implementation. However, when data is sent across the tunnel, an error is generated that indicates malformed packets.

What is the most probable reason for this error?

- A. Unmatching cipher keys on both sides.

- B. Incomplete Phase One negotiation.
- C. Corrupted packets due to invalid key exchanges.
- D. Mismatched ISAKMP pre-shared keys on both sides.

Answer: D

QUESTION 366:

IKE Phase 1 policy negotiation can include:

- A. Main Mode
- B. Neither Main Mode or Quick Mode
- C. Either Aggressive Mode or Main Mode
- D. Quick Mode only
- E. IPsec mode
- F. Aggressive mode

Answer: C

QUESTION 367:

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-lists

Answer: E

QUESTION 368:

IKE Phase 1 policy negotiation includes:

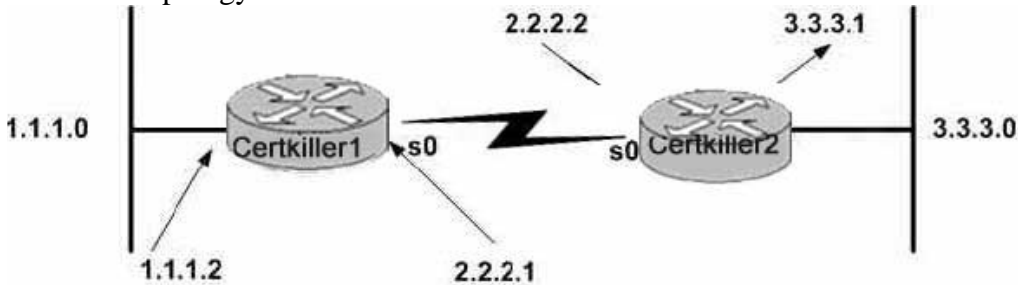
- A. Main mode
- B. Aggressive mode
- C. Either Main mode or Aggressive mode
- D. Neither Main mode nor Aggressive mode

Answer: C

IKE phase 1 negotiation can be completed using either main mode or aggressive mode.

QUESTION 369:

Network Topology Exhibit:



```

Applied to the crypto map on Router Certkiller1's S0 Interface:
match address 101
access-list 101 permit ip host 1.1.1.X host 3.3.3.X

Applied to the crypto map on Router Certkiller2's S0 Interface:
match address 102
access-list 102 permit ip host 1.1.1.x host 3.3.3.x
  
```

Given the shown Ipsec example and IPSec with IKE, when a user attempts to telnet from network 1.1.1.X to network 3.3.3.X:

- A. The telnet will succeed but the traffic will not be encrypted.
- B. The telnet will fail because the access lists are asymmetric
- C. The telnet will succeed and the traffic will be bidirectionally encrypted
- D. The telnet will fail because access-list 101 should have been applied to router A's interface 1.1.1.2

Answer: B

The access-lists on the two routers need to be symmetric for traffic to be encrypted in both directions. The access-list on router CK2 needs to be:

Access-list 102 permit ip host 3.3.3.x host 1.1.1.x

QUESTION 370:

RPF is an acronym for which of the following:

- A. Reverse Path Flooding
- B. Router Protocol Filter
- C. Routing Protocol File
- D. Reverse Path Forwarding
- E. None of the above.

Answer: D

Explanation: This chapter describes Unicast Reverse Path Forwarding (Unicast RPF) commands.

QUESTION 371:

Which negotiation is excluded from IKE Phase 1 policy?

- A. Encryption algorithm
- B. Authentication method.
- C. Crypto-map access-list
- D. Diffie-Hellman group.
- E. Lifetime
- F. All of the above.

Answer: C

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 PProfessional Development Network Security Pratices 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 PProfessional Development Network Security Pratices and Principles by Saadit Malik pg 280

QUESTION 372:

PPTP:

- A. Shares TPC and UDP ports 137, 128, & 139 with NetBIOS traffic.
- B. Is a modified version of GRE.
- C. Uses TCP ports 1030, 1031, & 1032.
- D. Used UDP ports 1030, 1031, & 1032.

Answer: B

PPTP can be used to tunnel a PPP session over an IP network. A tunnel is defined by a PNS-PAC pair. The tunnel protocol is defined by a modified version of GRE [1,2]. PPTP uses a TCP connection that uses TCP port 1723 and extension of GRE (IP protocol 47) to carry the actual data (PPP frame). The TCP connection is initial by client, followed by

the GRE connection that is initiated by server.

Reference:

<http://www.ietf.org/rfc/rfc2637.txt>

QUESTION 373:

You are the network technician at Certkiller . You are implementing a firewall on the Certkiller network. You need to ensure that PPTP can pass through the firewall. Which of the following should you permit?

- A. IP Protocol 47 and UDP 1723
- B. IP Protocol 47 and TCP 47.
- C. IP Protocol 47 and TCP 1723.
- D. IP Protocol 1723 and TCP 47.
- E. TCP and UDP 1723.

Answer: C

QUESTION 374:

802.1x is initiated by which actions?

- A. A machine that is plugged into a switch activates it's Ethernet port
- B. A switch or router sends an EOL start message
- C. A certificate being passed to an authentication server
- D. A radius authentication server request from a client

Answer: A

If you enable authentication on a port by using the dot1x port-control auto interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up.

QUESTION 375:

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 transmission are connection 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 x-auth.
- C. L2TP does not allow the use of wildcard pre-shred keys, which is not as secure as some other methods.

D. L2TP has less overhead than GRE.

Answer: B

L2TP uses UDP, so A is not correct. L2TP is an extension to the Point-to-Point Protocol (PPP), so B is the correct answer.

QUESTION 376:

A Security Manager needs to allow L2TP traffic through the firewall into the Internet network.

What ports generally need to be opened to allow this traffic to pass?

- A. TCP/UDP 1207
- B. TCP/UDP 500
- C. IP 50, IP 51
- D. TCP 49
- E. UDP 1701
- F. TCP 1072

Answer: E

UDP port 1701 is used as the carrier of all L2TP traffic, including the control traffic used to set up the tunnel between the LNS and the LAC.

Reference,

Page 243, Network Security and Principle and Practices, Cisco press

QUESTION 377:

What process will normally occur if an active Main Mode generated Phase One security association times out?

- A. Only Quick mode security associations will be regenerated.
- B. Main mode and Quick mode security associations must be regenerated.
- C. Aggressive mode will regenerate new security associations.
- D. Only Phase One security associations must be regenerated.
- E. No security associations will be regenerated.

Answer: B

QUESTION 378:

A Security Manager needs to allow L2TP traffic through the firewall into the Internet network.

What ports generally need to be opened to allow this traffic to pass?

- A. TCP/UDP 1207
- B. TCP/UDP 500
- C. IP 50, IP 51
- D. TCP 49
- E. UDP 1701
- F. TCP 1072

Answer: E

UDP port 1701 is used as the carrier of all L2TP traffic, including the control traffic used to set up the tunnel between the LNS and the LAC.

Reference,

Page 243, Network Security and Principle and Practices, Cisco press

QUESTION 379:

Identify the two types of access hardware involved in an L2TP connection:
(Multiple answer)

- A. L2TP Access Concentrator (LAC)
- B. Remote Access Concentrator (RAC)
- C. Layer 2 Forwarding Device (L2FD)
- D. L2TP Network Server (LNS)

Answer: A, D

Reference:

Page 243, Network Security and Principle and Practices, Cisco press

QUESTION 380:

When implementing network security at a specific site what would be your first step?

- 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. You must design a security policy.
- D. You have to purchase and install a firewall for network protection.
- E. You need to install access-control lists in your perimeter routers, to ensure that only known traffic is getting through your router.

Answer: C

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 381:

Why would you advise the new Certkiller trainee technician to select L2TP as a tunnel protocol for a VPN Client?

- A. L2TP makes use of TCP as a lower level protocol to result in connection oriented transmissions, resulting in more reliable delivery.
- B. L2TP makes use of PPP so address allocation and authentication is built into the protocol instead of IPSec extended function reliant, like mode config and a-auth.
- C. L2TP does not permit wildcard pre-shared keys usage, 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, or end-to-end application encryption. L2TP header: 16 bytes maximum (in case all options are used, RFC 2661) 24 (bit) for the GRE overhead

QUESTION 382:

What is the best description of poison reverse?

- A. It is a procedure used by OSPF to remove a network from the OSPF area.
- B. Once a connection disappears, the router advertising the bad network will send an update from this network indicating an infinite cost.
- C. The specific network is not sent out again on the interface it was received on.

D. The network is sent back out on the interfaces it was received on, but with a metric of one more than the metric in the received update.

Answer: B

QUESTION 383:

Exhibit

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco123 address 200.1.1.2
!
crypto ipsec transform-set vpntrans esp-des esp-md5-hmac
!
crypto map vpnmap 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set vpntrans
 match address 100
!
interface Ethernet0
 ip address 192.1.1.1 255.255.255.0
 ip nat outside
 crypto map ipsecmap
!
interface FastEthernet0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
!
ip nat pool p-name 192.1.1.20 192.1.1.24 netmask 255.255.255.0
ip nat inside source list 1 pool p-name
ip route 0.0.0.0 0.0.0.0 192.1.1.2
access-list 1 permit 10.1.1.0 0.0.0.0 255
```

A network administrator sees encrypted packets coming into the network from the 10.1.2.0 network. However, the return packets destined for the 10.1.2.0 network is being sent as clear text. According to the configurations, what should the administrator suspect the problem to be?

- A. The IPSec proxy is not defined correctly to encrypt outbound traffic.
- B. The VPNMAP is applied to the wrong interface.
- C. The default route is not allowing traffic to exit the correct interface to encrypt outbound traffic.
- D. NAT is not configured correctly, so outbound traffic is not matching the IPSec proxy.

Answer: D

QUESTION 384:

What is NOT a Windows NT 4.0 permission?

- A. Assign Ownership
- B. Take Ownership

- C. Read
- D. Execute
- E. Change Permission

Answer: A

QUESTION 385:

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

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

Answer: A

QUESTION 386:

What mechanism is used to authenticate PPTP control channel messages?

- A. AH
- B. ESP
- C. RSA Signatures
- D. PPTP has no authentication mechanism.

Answer: D

QUESTION 387:

NETBEUI is

- A. a routable protocol
- B. a non-routable protocol designed for small networks
- C. a routing protocol designed for large networks
- D. a data-link layer protocol

Answer: B

QUESTION 388:

A Windows client is using NetBIOS bound to TCP/IP can try to find another computer by:

- A. Sending a query to a WINS server.
- B. Looking in a local file named "HOST"
- C. Pinging the network
- D. Sending ICMP messages.

Answer: A

QUESTION 389:

What address range is correct for IP Multicast Group Addressing?

- A. 224.0.0.1 through 239.255.255.254
- B. 192.0.0.0 through 223.255.255.255
- C. 240.0.0.1 through 255.255.255.254
- D. None of the above

Answer: A

QUESTION 390:

What does the acronym CBAC stand for?

- A. Context Based Authentication Control
- B. Context Based Access Control
- C. Cisco IOS Based Authentication Control
- D. Cisco based Authentication Control

Answer: B

Context-based access control (CBAC) lets the router maintain a persistent state, based on information from inspected packets, and use that state information to decide which traffic should be forwarded. CBAC is the centerpiece of the firewall feature set, and the other features in the set build on CBAC. Connection information can be gathered from CBAC and logged to a syslog server.

QUESTION 391:

Whisker, nmap, and strobe are:

- A. Freeware programs used to determine & map device types through SNMP
- B. Port scanners
- C. Distributed denial of service (DDOS) programs
- D. Intrusion detection programs

Answer: B

nmap

nmap is a utility for port scanning large networks using various scanning techniques.

Whisker

Whisker is a CGI scanner with impressive features that makes it much better than most CGI

scanners.

strobe version 1.03

Strobe is a security/network tool that locates and describes all listening tcp ports on a (remote)

host

QUESTION 392:

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

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

Answer: B

A stateful firewall is a firewall that keeps track of the state of network connections (such as TCP streams) traveling across it. The firewall is programmed to know what legitimate packets are for different types of connections. Only packets which match a known connection state will be allowed by the firewall; others will be rejected.

QUESTION 393:

In Frame Relay, what devices resend packets that do not transmit correctly?

- A. Digital transmissions media cabled to monitor ports, as opposed to straight DCE signaling.
- B. Network end stations running intelligent protocols
- C. Network switches running SNMP management software

D. Special bridging devices within the backbone cloud

Answer: A

QUESTION 394:

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

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

Answer: A

QUESTION 395:

In order to avoid loops when sending routing updates, what is the correct technique to prevent a network from being forwarded on the same interface that it was learned?

- A. Poison Reverse
- B. The use of access-list used with distribute-list
- C. Split Horizon
- D. This is not a problem, since this cannot happen.

Answer: C

QUESTION 396:

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

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

```
radius-server key <key>
aaa authn login default radius
aaa new-model
D. radius-server host #.#.#.#
radius-server use-extended
login radius
```

Answer: A

QUESTION 397:

When the PIX Firewall is configured to authenticate connections to specific hosts, the PIX and the Client being authenticated use what password type?

- A. CHAP
- B. MS-CHAP
- C. Encrypted text
- D. PAP
- E. Clear text

Answer: E

QUESTION 398:

The RFC 1700 defined port used for NTP is:

- A. UDP 541
- B. TCP 551
- C. TCP and UDP 321
- D. TCP and UDP 123

Answer: D

QUESTION 399:

What return status will cause a AAA statement to look to next defined method for authentication?

- A. Fail
- B. Error
- C. Access-reject
- D. All of the above

Answer: B

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication succeed even if all methods return an error, specify none as the final method in the command line.

QUESTION 400:

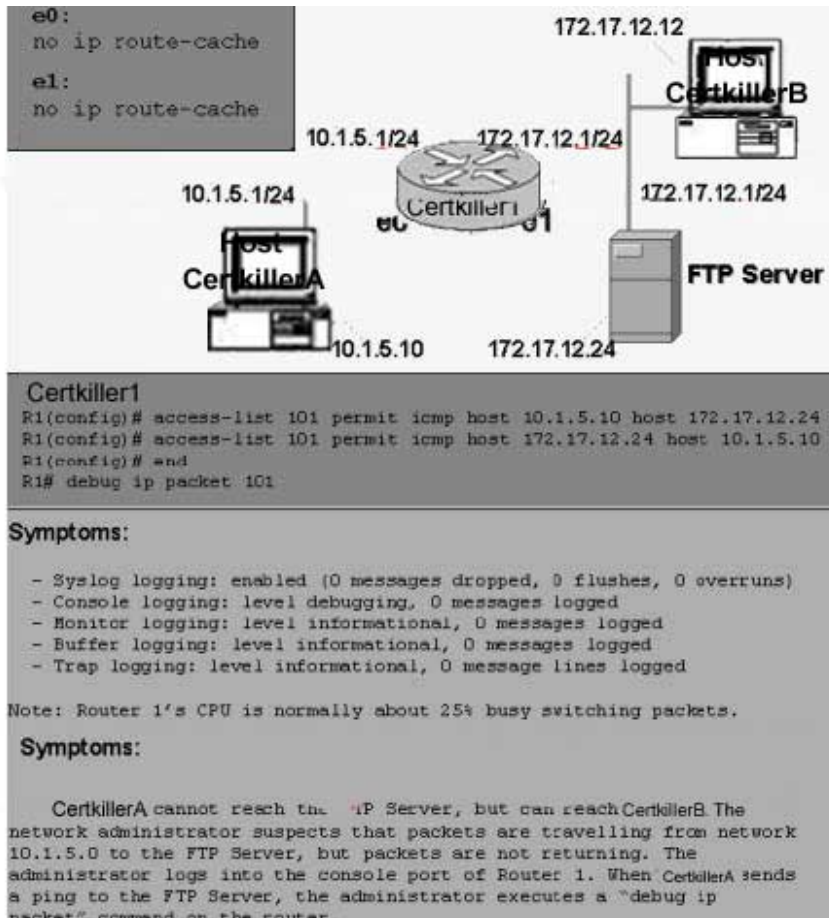
The ultimate target of a smurf attack should:

- A. Contact the reflectors, either to ask them to reconfigure their networks to shut down the attack, or to ask for their assistance in tracing the stimulus stream.
- B. Launch a retaliatory attack on the reflector network.
- C. Ask the reflector network administrator to quench the attack by allowing directed broadcasts.
- D. Use the access-list logging command on the inside interface of the router of the ultimate target network to determine the station inside the network launching the attack.

Answer: A

QUESTION 401:

Exhibit



A network technician at Certkiller .com found and fixed a problem. However, when the administrator was removing the router debug command, the router hung suddenly. Consequently, the administrator was forced to power cycle the router to recover.

What is the most likely reason this occurred?

- A. Several users on host 10.1.5.10 started FTP transfers with 172.17.12.24, while debugging was still running.
- B. When Fast-switching was re-enabled on Ethernet 0, but not on Ethernet 1, the router became unbalanced and hung.
- C. Access-list 101 was removed while debugging was still running.
- D. Fast switching was re-enabled while debugging was still running.
- E. Logging buffered was re-enabled while debugging was still running.

Answer: C

QUESTION 402:

Which record is not in DNS?

- A. MX

- B. PTR
- C. A
- D. FQDN
- E. NS

Answer: D

QUESTION 403:

When using Cisco Secure Intrusion Detection System, the network traffic pattern appears ordinary. However, too many false positives for a particular alarm are received. What can be done to avoid the quantity of "noise" in the future?

- A. Click on unmanage for the alarm in question in the HP OpenView/NR GUI interface
- B. Click on acknowledge for the alarm in question in the HPOV/NR GUI interface
- C. Use eventd to decrease the alarm level severity
- D. Configure a decreased alarm level severity through nrconfigure

Answer: C

Configuring Event Processing

Event processing is managed by the eventd daemon. eventd processes alarms sent to it and executes user-defined actions.

QUESTION 404:

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

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

Answer: B

QUESTION 405:

What statement is FALSE about Certificate Enrollment Protocol (CEP)?

- A. CEP is used to obtain the CA's certificate.
- B. CEP uses HTTP as a transport mechanism.
- C. CEP is used to obtain CRLs.
- D. CEP is used for router to router communication to check the peer's enrollment certificate.

Answer: D

QUESTION 406:

In Virtual Private Dial-up Networking (VPDN), a tunnel can be established from the ISP router to the Home Gateway router based on:

- A. Local authentication failure of the dial in client
- B. The domain name as specified by the dial-in user or DNIS
- C. The interface the inbound call is terminated on
- D. The IP address requested by the dial in client
- E. The negotiation of the Virtual Tunnel Control Protocol (VTCP)

Answer: B

QUESTION 407:

The Kerberos protocol can support what action?

- A. Encrypted LCP negotiation
- B. Encrypted accounting
- C. Encrypted login and session
- D. Clear-text password exchange

Answer: C

QUESTION 408:

When using a third party, one-time password generator, a user logs onto a NAS using DUN.

What must the user do to enable new PIN mode when logging on?

- A. Telnet
- B. Use the post dial window
- C. Check the encryption password in DUN

D. Any of the above

Answer: B

QUESTION 409:

In Frame Relay, the BECN bit is set by:

- A. The Frame Relay network, to inform the DTE receiving the frame that congestion was experienced in the path from source to destination.
- B. The Frame Relay network, in frames traveling in the opposite direction from those frames that encountered congestion
- C. The receiving DTE, to inform the Frame Relay network that it is overloaded and that the switch should throttle back
- D. The sending DTE, to inform the Frame Relay network that it is overloaded and that the switch should throttle back
- E. Any device that uses an extended DLCI address

Answer: B

QUESTION 410:

In the Cisco Secure Intrusion Detection System/HP OpenView 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 report 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

QUESTION 411:

A stateful firewall:

- A. Keeps a table of established sessions and evaluates session traffic based on this table.
- B. Evaluates incoming addresses and keeps track of what is passed through the device.
- C. Looks at the application layer of all protocols.
- D. Makes dynamic filter changes to TCP outgoing traffic.

Answer: A

QUESTION 412:

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 concepts of users and permissions, so it is not secure.

Answer: C

QUESTION 413:

When a Cisco Secure Intrusion Detection System Sensor communicates with a Cisco Secure Intrusion Detection System Director, what statement is FALSE?

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

Answer: D

QUESTION 414:

To determine if a Windows NT server has software listening on a particular port, for example udp/514, the command could be:

- A. netstat -s|find udp
- B. netstat -an|grep 514
- C. edit c:\WINNT\system32\drivers\etc\SERVICES
- D. netstat -an|findstr 514

Answer: D

QUESTION 415:

NAT overload does not work well when:

- A. Authentication is involved with outbound HTTP.
- B. One-to-one NAT is used on the same firewall.
- C. The number of inside hosts exceeds the number of addresses in the NAT pool
- D. Multimedia applications have an inbound data stream that is different from the outgoing control path.

Answer: D

QUESTION 416:

Which statement about transport layer protocols is true?

- A. TCP is connectionless.
- B. UDP is a datagram protocol,.
- C. TCP has a larger MTU.
- D. TCP is easier to implement.
- E. UDP is a stream protocol.

Answer: B

QUESTION 417:

In the IOS Firewall Feature Set, CBAC does not:

- A. Maintain state information for individual connections
- B. Use state information to allow or deny network traffic
- C. Inspect ICMP
- D. Dynamically create and delete openings in the firewall

Answer: C

QUESTION 418:

What technique could be used to resolve the problem of large routing table updates caused by the use of many Class C addresses?

- A. Variable-Length Subnet Masks
- B. Classless Inter-Domain Routing

- C. Propagate all the subnets to ensure reachability to all addresses.
- D. Use a Link State routing protocol.

Answer: B

QUESTION 419:

When a Catalyst 5000 authenticates PPP, the method it will use for password authentication is:

- A. PAP
- B. CHAP
- C. Clear
- D. None of the above, since the Catalyst does not authenticate PPP

Answer: D

QUESTION 420:

A Kerberos user defined in the Kerberos database is called a:

- A. Principal
- B. Kerberos user
- C. User
- D. Authenticator
- E. Accessor

Answer: A

QUESTION 421:

What is the best description of the isdn caller 551212 command?

- A. This is a global command that checks to see if the caller ID of an inbound call is 5551212.
- B. This is an interface command that permits ISDN calls to be placed to 5551212.
- C. This is a global command that permits ISDN calls to be placed to 5551212.
- D. This is an interface command that denies ISDN calls placed to 5551212.
- E. This is an interface command that permits ISDN calls from 5551212.

Answer: E

QUESTION 422:

In the Security Forums, Social Engineering refers to what concept?

- A. Creating security products that are easy to use, and based on typical social interactions for the User Interface schema.
- B. Bringing greater creativity to engineering groups through social interaction and stimulus.
- C. Breaking into systems by tricking people into providing the necessary information, such as codes, pass phrases, or even personal information.
- D. Breaking into systems using easily guessed passwords, or a list of passwords from a dictionary.
- E. Breaking into systems by learning the cryptography methods, and deciphering the secrets.

Answer: C

QUESTION 423:

From an outside Windows NT server, the network administrator can ping an internal NT Server behind an application firewall. The administrator wishes to browse the various shares on the inside NT Server, but receives an error message indicating the server cannot be found. In which ways can this desired functionality be achieved? Select all that apply.

- A. Use an LMHOSTS file with the name, IP address, and Domain of the internal NT Server
- B. Make sure the firewall has UDP 137, 138, and TCP 139 ports open to the outside server
- C. Use an inside host running an FTP server
- D. Use an outside host running NetBIOS Name Services (NBNS)

Answer: A, B, D

QUESTION 424:

What statement about AH and ESP is FALSE?

- A. ESP encapsulates the IP header, while AH does not.
- B. ESP uses protocol port 50.
- C. AH uses protocol port 51.
- D. AH does not lend itself to a NAT environment because of IP header encapsulation.

Answer: A

QUESTION 425:

If two routers connected to the same Ethernet are configured to run HSRP (Hot Standby Router Protocol) in the same group number, which router's MAC address will be associated with the virtual IP address?

- A. It depends on which router is active.
- B. Neither - a virtual MAC address will be assigned based on the group number, unless the routers are configured to use their burned in addresses (BIA).
- C. The routers will negotiate and decide automatically which MAC address to use based on the routers' ID.
- D. Both routers' MAC addresses will be associated with the virtual IP address.
- E. Neither - the hosts will broadcast all traffic which needs to travel off-segment.

Answer: B

QUESTION 426:

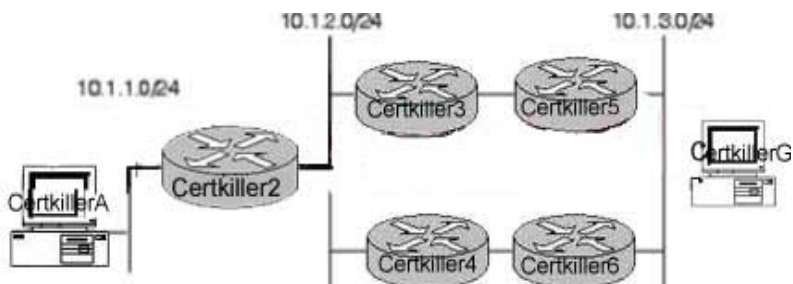
The master Kerberos server is also known as:

- A. The router configured for Kerberos
- B. The Key Distribution Center (KDC)
- C. The Realm Master (RM)
- D. The TGT server

Answer: B

QUESTION 427:

Exhibit:



Router Certkiller 3 and Certkiller 4 are both advertising 10.1.3.0/24 with equal metrics through one of the interior gateway protocols.

What is the result?

- A. Router Certkiller 2 will have two routes in its routing table for 10.1.3.0/24, and will alternate sending packets over both paths. However, the patch selected for sending packets will depend on the switching mode configured.
- B. Router Certkiller 2 will have only one path to 10.1.3.0/24 in the routing table.
- C. Router Certkiller will have two paths in its routing table, but will only use one path for forwarding traffic.
- D. Router Certkiller 2 will have two paths in the routing table. It will always copy each packet it receives destined for 10.1.3.0/24 and will send the copies down both paths simultaneously.
- E. The number of paths in Router Certkiller 2's routing table depends on the IGP routing protocol in use.

Answer: A

Explanation : By configuring ip route-cache command in Ethernet interface, it enables fast switching

The route cache allows outgoing packets to be load-balanced on a per-destination basis rather than on a per-packet basis.

Not E:

It is not IGP protocol issue at all. For any routing protocols such as RIP/IGRP/OSPF/EIGRP, they support equal path load balancing.

Refer to Routing TCP/IP Volume 1 by Jeff Doyle for equal cost load sharing (page 109--112).

QUESTION 428:

If the first line of output from show interface serial 0 command read "serial 0 up, line protocol down", what might this indicate?

- A. This should never happen.
- B. Keepalives are not being received from the remote router.
- C. The CSU/DSU is powered off.
- D. The remote CSU/DSU is powered off.
- E. The router serial cable is disconnected.

Answer: B

QUESTION 429:

Exhibit:

```
Certkiller1
crypto isakmp policy 4
 authentication pre-share
 lifetime 1000

Certkiller2
crypto isakmp policy 4
 authentication pre-share
 lifetime 2000
```

Assuming the configuration shown in the exhibit, what is the expected behavior of ISAKMP regarding security lifetimes (if Router Certkiller 2 is the initiator)?

- A. ISAKMP negotiation will fail because the routers' lifetimes do not match.
- B. ISAKMP negotiation will succeed. If the two peers' policy lifetimes are not the same, the initiating peer's lifetime must be longer and the responding peer's lifetime must be shorter. As a result, the shorter lifetime will be used.
- C. ISAKMP negotiation will fail. If the two peers' policy lifetimes are not the same, the initiating peer's lifetime must be shorter and the responding peer's lifetime must be longer. As a result, the longer lifetime will be used.
- D. ISAKMP negotiation will succeed. The initiating peer will re-key at 2000 seconds and the responding peer will re-key at 1000 seconds.
- E. ISAKMP negotiation will succeed. ISAKMP will compute the average of the two lifetimes and re-keying will happen every 1500 seconds.

Answer: B

QUESTION 430:

Select the protocols that use Link State routing: (multiple answer)

- A. AURP
- B. OSPF
- C. NetWare Link Services Protocol (NLSP)
- D. IS-IS
- E. EIGRP

Answer: B, C, D

QUESTION 431:

You work as a network administrator for Certkiller .com. You are viewing errors from an Ethernet interface on a Cisco router. The errors appear on the interface every 15 seconds and the up arrow in the terminal emulation program is not working.

What alias command would allow the administrator to see the errors, without having to type the extended show command?

- A. alias exec si show interface ethernet(0)
- B. alias exec si show ip interface ethernet(0)
- C. alias exec si show error ethernet(0)
- D. alias shell si show interface ethernet(0)
- E. alias shell si show ip interface ethernet(0)

Answer: A

QUESTION 432:

The name for an attack where network packets are intercepted by an attacker before they are transmitted to their final destination is:

- A. Hijacking
- B. Man in the middle
- C. Denial of service
- D. Trojan horse

Answer: B

QUESTION 433:

A Network Scanner can be used:

- A. To identify network exploit signatures.
- B. To identify network vulnerabilities
- C. To report network intrusion
- D. To identify network intruders
- E. To notify Security Managers when network perimeter has been compromised

Answer: B

QUESTION 434:

What is the proper way to use IPSec to encrypt IPX traffic?

- A. Define an IPX extended access list in the range 900-999 and add match address #, where 900-999 to the crypto map
- B. Define a GRE tunnel which will carry the IP and IPX traffic, then apply the crypto map to the tunnel interface. Finally, define a crypto access control list that matches the tunnel itself.
- C. Define a GRE tunnel which will carry the IP and IPX traffic, then apply the crypto

map to the physical interface associated with the tunnel. Finally, define a crypto access control list that matches the tunnel itself.

D. Define an IPX extended access list in the range 900-999 and add match address #, where # is the 900-999 to the transform set.

Answer: B

Explanation:

IPSEC only supports IP traffic, to

transport non IP traffic we always have to use another transportation mechanism usually GRE.

Below are reproduced the valid option for the setup of the interesting traffic regarding IPSEC :

router(config-crypto-map)#match address ?

<100-199> IP access-list number

<2000-2699> IP access-list number (expanded range)

WORD Access-list name

QUESTION 435:

For the spanning tree algorithm, a bridge builds part of its forwarding table based upon:

- A. Destination MAC addresses
- B. 802.2 headers
- C. Source MAC addresses
- D. The Ethernet type field
- E. The SNAP field

Answer: C

QUESTION 436:

Which statements are correct? Select two.

- A. IGRP supports discontinuous networks
- B. IGRP is a distance vector protocol.
- C. RIP v2 is a classful protocol.
- D. If there is only one area in an OSPF network, it can be assigned area 1.

Answer: B, D

QUESTION 437:

When a user logs in and out of a Unix system, where is the information stored?

- A. utmp and messages
- B. wtmp and lastlog
- C. /var/adm/acct
- D. /etc/login & /usr/bin/login

Answer: B

QUESTION 438:

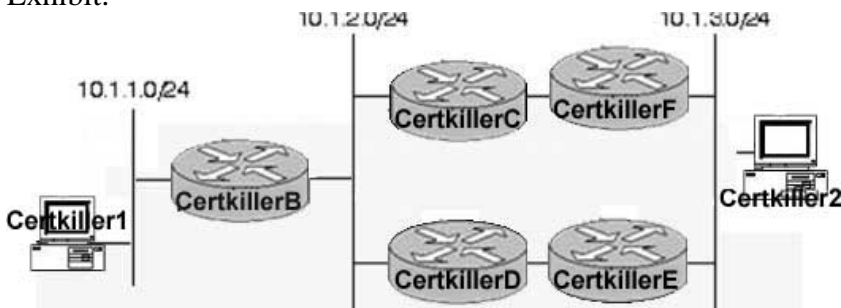
At what layer of the OSI model is data secured with IPSec tunnel mode?

- A. Application
- B. Data-Link
- C. Physical
- D. Network
- E. Transport

Answer: D

QUESTION 439:

Exhibit:



Routers Certkiller E and Certkiller F are running HSRP (Hot Standby Router Protocol). Router Certkiller E has a higher priority, and both routers have standby preempt configured. Since Router Certkiller E is normally the active reouter, what IP address should host Certkiller 2 use for its default gateway?

- A. 10.1.3.1
- B. Router Certkiller E's IP address, since it is normally active; Router Certkiller F will take over Router Certkiller E's address if it fails.
- C. Router Certkiller E's IP address; the active router will take over the standby router's IP address until it fails.
- D. The virtual address configured when enable HSRP

E. The virtual address assigned by HSRP; this address is dependant on the group number configured.

Answer: D

QUESTION 440:

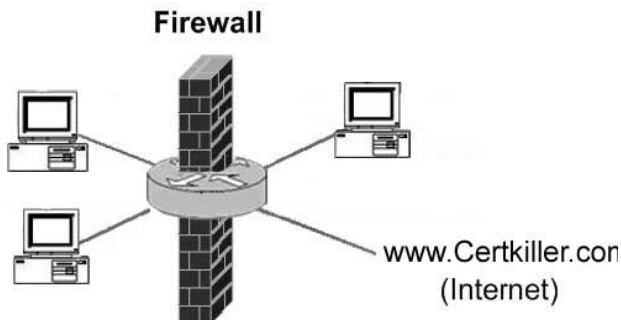
What security programs can effectively protect your network against password sniffer programs? Select three.

- 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, D

QUESTION 441:

Exhibit



A network engineer is troubleshooting a connectivity problem between hosts Certkiller A and Certkiller B. The following conditions exist:

1. Certkiller A can ping the firewall, but cannot ping Certkiller B
 2. Certkiller B can ping both the firewall and www.cisco.com
 3. The firewall can ping www. Certkiller .com
 4. Certkiller C can ping the firewall and www. Certkiller .com
 5. Certkiller A and Certkiller C have the same permissions on the firewall?
- What is the most likely problem?

- A. Routing protocols in the network are not set up properly, and not propagating across the firewall,.
- B. Certkiller A has an incorrect default gateway configured.
- C. Certkiller B has an incorrect default gateway configured.
- D. Certkiller C has an incorrect default gateway configured.
- E. The firewall has an incorrect default gateway configured.

Answer: B

QUESTION 442:

A router interface address is 180.60.45.96 with a mask of 255.255.255.224. What configuration statement will allow this interface to participate in OSPF Area 0?

- A. router ospf 1
network 180.60.45.96 255.255.255.32 area 0
- B. router ospf 1
network 180.60.45.96 0.255.255.224 area 0
- C. router ospf 1
network 180.60.45.96 0.0.0.31 area 0
- D. router ospf 1
network 180.60.45.96 0.0.0.224 area 0

Answer: C

QUESTION 443:

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 communications 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 not a factor when used in conjunction with NAT, unless Triple DES is included in the transform set.

Answer: B

QUESTION 444:

See the show run from 10.1.1.100 and the show arp below. version 12.3
service tcp-keepalives-in
service tcp-keepalives-out
service password-encryption
hostname Router!
logging buffered 51200
debugging logging console critical enable
secret 5 \$1\$QLym\$3KmYQ7OBI7XnT6eolVvt91
enable password 7 060506324F41!
ip subnet-zero
ip source-route
ip tcp synwait-time 10
ip dhcp excluded-address 10.1.1.1
10.1.1.110
ip dhcp excluded-address 10.1.1.116 10.1.1.254
ip dhcp pool sdm-pool1
network 10.1.1.0 255.255.255.0
default-router 10.1.1.100
lease infinite
interface FastEthernet0/0
description \$ETH-LAN\$\$FW_INSIDE\$
ip address


```
10.1.1.100 255.255.255.0no ip redirectsno ip unreachablesnop ip proxy-arpip route-cache
flow!interface FastEthernet0/1no ip addressno ip redirectsno ip unreachablesnop ip
proxy-arpip route-cache flowshutdown!ip http serverip http access-class 1ip http
authentication localip http secure-serverip classlessip route 0.0.0.0 0.0.0.0
10.1.1.254!!logging trap debugginglogging 10.1.1.10access-list 1 remark HTTP
Access-class listaccess-list 1 remark SDM_ACL Category=1access-list 1 permit 10.1.1.0
0.0.0.255access-list 1 deny anyaccess-list 100 remark VTY Access-class listaccess-list
100 remark SDM_ACL Category=1access-list 100 permit ip 10.1.1.0 0.0.0.255
anyaccess-list 100 deny ip any anyno cdp run!!line vty 0 4access-class 100 inprivilege
level 15login localtransport input telnet ssh!scheduler allocate 4000
1000!!endRouter#Internet 192.168.1.11 0 00b0.d0f3.f7f0 ARPA FastEthernet0/0Internet
192.168.1.1 0 00b0.d0f3.f7f0 ARPA FastEthernet0/0Internet 192.168.1.20 0
00b0.d0f3.f7f0 ARPA FastEthernet0/0Internet 192.168.1.100 - 000b.5f35.3c81 ARPA
FastEthernet0/0Internet 192.168.1.114 179 0009.5b20.f4a2 ARPA
FastEthernet0/0Internet 192.168.1.115 178 0009.5b20.f4a2 ARPA
FastEthernet0/0Internet 192.168.1.112 0 00b0.d0f3.f7f0 ARPA FastEthernet0/0Internet
192.168.1.113 3 00b0.d0f3.f7f0 ARPA FastEthernet0/0Internet 192.168.1.254 0
00b0.d0f3.f7f0 ARPA FastEthernet0/0Internet 192.168.1.255 0 00b0.d0f3.f7f0 ARPA
FastEthernet0/0
What type of an attack MAY have taken place that would cause the show arp
output of the router?
```

- A. The router is doing a proxy ARP for the DHCP pool so the MAC addresses are all the same.
- B. An ARP poisoning attack has been launched on the subnet, so that all packets will be sent to the attacking host.
- C. No attack has taken place, the arp table is corrupt.
- D. An attacker has spoofed the MAC address of the router and all packets will be forwarded to the attacker.

Answer: B

QUESTION 445:

A company has 2 border routers running BGP to 2 different ISP's. They want to control which path inbound traffic takes without the use of communities. What is the most important consideration?

- A. Metric
- B. MED
- C. AS-path prepending
- D. Weight
- E. Local preference

Answer: C

QUESTION 446:

A company has deployed a new e-commerce web farm. They are using teamed servers that use multicast to maintain a heartbeat between redundant pairs. All servers are in the 192.168.202.0/24 network. For increased security, they require each pair of servers be allowed to see multicast/broadcast traffic from their default gateway and from each other. No pair of servers should ever see any broadcast/multicast traffic from any other pair of servers. Which is the best mechanism for the server ports to accomplish this?

- A. Isolated Ports
- B. Promiscuous Ports
- C. Community Ports
- D. Teamed Ports
- E. Span Ports

Answer: C

QUESTION 447:

What of the following is a primary objective of a DHCP starvation attack?

- A. To cause a DoS against a DHCP server and insert a rogue DHCP server and gateway such that the attacker can see all network traffic
- B. To insert a rouge DHCP server, so the attacker can obtain a valid network address and more easily get network access for future attacks
- C. Overflow a buffer in the DHCP server and obtain a system level command shell from which the attacker can control the network
- D. Intercept DHCP broadcasts, identify the DHCP server address, which is usually the Domain server, then run brute force attacks against that server

Answer: A

QUESTION 448:

When deploying a VPN concentrator, which best practice, with regards to firewall placement, provide maximum security?

- A. Place the VPN concentrator on the outside of the firewall.
- B. Place the VPN concentrator in parallel with the FW.
- C. Place the VPN concentrator on the inside of the firewall and enable NAT for address hiding.

- D. Place the VPN concentrator on the inside of the firewall and enable DOS features.
- E. Place VPN concentrator inside interface on the FW DMZ.

Answer: E

QUESTION 449:

A router is receiving updates for a subnet from different routing protocols. The administrator wishes to take advantage of a path via a route with a less favorable Administrative Distance. What can be done to effect this without losing any of the updates?

- A. Configure a static route with an Administrative Distance of 120
- B. Use the Router Configuration mode command distance with an appropriate 'weight' for this subnet
- C. Create a distribute-list to block this subnet
- D. Modify the default-metric weight of the routing protocol offering the more favorable Administrative Distance

Answer: B

QUESTION 450:

How does QoS interact with VPN encapsulation?

- A. QoS cannot be used with VPN because the TOS bits in the IP header are not written to the outside IP header of an ESP packet therefore no increased performance is gained.
- B. QoS is commonly used to prioritize the process switching of all VPN packets at both endpoints except when NAT is applied at either endpoint.
- C. QoS IP header bits are copied between the original packet and the IP header encapsulating the VPN tunnel.
- D. QoS cannot be used with VPN because the TOS bits in the IP header are not written when traversing a Router.

Answer: C

QUESTION 451:

What answer best describes the Cisco Security Agent (CSA)?

- A. The primary function of CSA is to provide authentication services for Cisco devices.
- B. CSA uses a set of predefined rules to protect a host or server.
- C. CSA is a server that can recognize network attacks and take action to mitigate the

attacks.

D. CSA is a passive device that sits on the network and provides real time reporting to a CSA management host.

Answer: B

QUESTION 452:

Exhibit:

```
Switch-B> (enable)
%SPANTREE-2-CHNMISCFG: STP loop Channel 2/1-4 is disabled in vlan 1.
%PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4
%PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4
%PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4
%PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4
```

After configuring EtherChannel on Switch-B in ports 2/1-4 to Switch-A using set port channel 2/1-4 on, the message shown in the exhibit is received. There is no connectivity to Switch-A, even after disabling the EtherChannel on Switch-B. What command needs to be issued on Switch-B to most likely restore communication to Switch-A?

- A. set trunk 2/1-4 desirable dot1q
- B. set port channel all mode off
- C. set port enable 2/1-4
- D. set port channel 2/1-4 mode desirable

Answer: C

QUESTION 453:

Exhibit:

```

2511a#show line 6
Tty Typ Tx/Rx A Modem Roty AccO Accl Uses Noise Overruns
6 TTY 9600/9600 - - - - - 14 59898 0/0

Line 6, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600, no parity, 1 stopbits, 8 databits
Status: Ready
Capabilities: none
Modem state: Ready
Group codes: 0
Modem hardware state: CTS* noDSR* DTR RTS
Special Chars: Escape Hold Stop Start Disconnect Activation
BREAK none - - none
Timeouts: Idle EXEC Idle Session Modem Answer Session Dispatch
00:10:00 00:15:00 none not set
Idle Session Disconnect Warning
never
Modem type is unknown.
Session limit is not set.
Time since activation: 1d04h
Editing is enabled.
History is enabled, history size is 10.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed transports are lat pad telnet rlogin mop nasi. Preferred is lat.
No output characters are padded
No special data dispatching characters
2511a#

```

A router has been configured as a Terminal Server. Issues are encountered with line 6 due to spurious signals. After reviewing the exhibit, what command would most likely fix the issue?

- A. flowcontrol hardware
- B. transport input telnet
- C. no exec
- D. exec-timeout 0 0

Answer: C

QUESTION 454:

Which layers in the OSI reference model are missing from the TCP/IP reference model?(Choose Three)

- A. Network
- B. Presentation
- C. Transport
- D. Session
- E. Application

Answer: B,D,E

QUESTION 455:

What statement is FALSE concerning the use of SPAN on the Catalyst 6500?

- A. It is possible to configure SPAN to have a Gigabit port, such as source port, and a 10/100 port as the destination port.
- B. If the source port is configured as a trunk port, the traffic on the destination port will be tagged as well, regardless of the configuration on the destination port.
- C. When a SPAN session is active the destination port does not participate in Spanning Tree.
- D. With SPAN an entire VLAN can be configured to be the source.
- E. In one SPAN session it is possible to monitor multiple ports that do not belong to the same VLAN.

Answer: B

QUESTION 456:

What has to happen in order for a man-in-the-middle to successfully hijack an SSL session?

- A. The MITM needs to be on the same network segment as the client.
- B. The MITM needs to be on the same network segment as the server.
- C. The MITM needs to successfully exchange keys with the client and the server acting similar to a proxy.
- D. The MITM needs to know or glean the SSL certificate.
- E. The MITM needs to spoof the IP address of the client.

Answer: C

QUESTION 457:

What is not a cause of a port going to err-disable?

- A. Duplex mismatch
- B. Unidirectional Link
- C. Bidirectional Link running to different two switches
- D. Spanning Tree loop
- E. VLANs on the trunk were not matching on both sides

Answer: E

QUESTION 458:

What is the main type of attack that can enable an attacker to hop VLANs on a layer two device?

- A. CAM table overflow
- B. Double encapsulation
- C. Spanning-Tree Protocol manipulation
- D. Media Access Control (MAC) address spoofing
- E. Private VLAN redirection
- F. All of the above

Answer: F

QUESTION 459:

What feature of Security Device Manager can be used to apply access-lists for controlling Telnet and SSH access with a single click?

- A. SDM Wizard
- B. Auto secure feature
- C. Advanced mode access rules
- D. One step lockdown
- E. Single click lockdown

Answer: D

QUESTION 460:

What protocol is not disabled by the 'no service tcp-small-servers' command?

- A. Echo
- B. Finger
- C. Chargen
- D. Discard
- E. Daytime

Answer: B

QUESTION 461:

What statement best describes Cisco Threat Response?

- A. CTR reads IDS alarms and performs automated forensics on hosts or servers that may have been compromised.

- B. CTR is an add-on to Network IDS and logs onto network devices such as routers or switches to see if they have been compromised.
- C. CTR analyzes router logs and Netflow statistics to determine if a DoS attack is in progress.
- D. CTR is an inline device that does deep packet inspection looking for attacks on Cisco network devices such as routers and switches.

Answer: A

QUESTION 462:

The TCP PUSH flag indicates:

- A. The data in the TCP receive buffer should be sent to the application listening to this TCP connection without waiting for further data.
- B. Any data being buffered by routers between the source and destination for this connection should be sent immediately.
- C. The sender should make certain its send buffer is pushed onto the wire.
- D. This session is about to end.

Answer: A

QUESTION 463:

A PIX Firewall running IDS has these messages in its syslog:

Dec 10 18:25:38 router 97630: Dec 10 18:25:38.436: %IDS-4-TCP_SYN_FIN_SIG:
Sig:3041:TCP - SYN and FIN bits set - from 192.168.1.1 to test.net.199.0 Dec 10
18:25:39 router 97631: Dec 10 18:25:38.440: %SEC-6-IPACCESSLOGP: list 102 denied
tcp 192.168.1.1(53) -> test.net.199.0(53), 1 packet Dec 10 18:25:40 router 97632: Dec 10
18:25:39.450: %SEC-6-IPACCESSLOGP: list 102 denied tcp 192.168.1.1(53) ->
test.net.199.51(53), 1 packet Dec 10 18:25:40 router 97633: Dec 10 18:25:40.451:
%SEC-6-IPACCESSLOGP: list 102 denied tcp 192.168.1.1(53) -> test.net.199.101(53),
1 packet

What can be deduced from the information given above?

- A. A DNS zone transfer is in progress.
- B. DNS responses are being blocked by the firewall.
- C. Someone is scanning the DNS server probably looking for vulnerabilities.
- D. 192.168.1.1 is trying to initiate a DNS zone transfers.
- E. DNS zone transfers are being blocked by the firewall.

Answer: C

QUESTION 464:

Which are NOT valid protocols supported by the authentication proxy feature in the IOS Firewall or PIX Security Appliance? (multiple answer)(Choose Two)

- A. Telnet
- B. SSH
- C. HTTP
- D. HTTPs
- E. SMTP

Answer: B,E

QUESTION 465:

What feature is provided by IOS NAT (Network Address Translation)?

- A. Dynamic network address translation using a pool of IP addresses, or port address translation using a single IP address
- B. Destination based address translation using either route map or an extended access-list
- C. Dynamic translation for DNS "A" and "PTR" queries
- D. Inside and outside source static network translation that allows overlapping network address spaces on the inside and the outside
- E. All of the above

Answer: A

QUESTION 466:

Consider two hosts on different router interfaces, the router contains an access list that denies an ICMP echo request on either interface. The first host tries to ping the second host. What ICMP reply from the router will the originating host receive?

- A. Administratively-prohibited destination unreachable
- B. Access denied
- C. Destination unreachable
- D. No route to host
- E. None of the above

Answer: A

QUESTION 467:

When using Certificate Authorities (CA) for ISAKMP negotiation, what ISAKMP configuration will work?(Choose Two)

- A. crypto isakmp policy 4authentication cert-rsa
- B. crypto isakmp policy 4authentication ca
- C. crypto isakmp policy 4authentication cert-sig
- D. crypto isakmp policy 4authentication rsa-sig
- E. crypto isakmp policy 4authentication rsa-enc

Answer: D,E

QUESTION 468:

An IDS sensor on a DMZ segment records the traffic, in the shown output, in its database.15:59:34.898799

```
10.16.17.101.41738 > 10.16.17.206.80: F 0:0(0) win 409615:59:34.898863
10.16.17.101.41738 > 10.16.17.206.80: F 0:0(0) win 409615:59:34.898995
10.16.17.101.41738 > 10.16.17.206.25: F 0:0(0) win 409615:59:34.899009
10.16.17.101.41738 > 10.16.17.206.25: F 0:0(0) win 409615:59:34.899082
10.16.17.101.41738 > 10.16.17.206.443: F 0:0(0) win 409615:59:34.899096
10.16.17.101.41738 > 10.16.17.206.443: F 0:0(0) win 409615:59:34.899150
10.16.17.206.25 > 10.16.17.101.41738: R 0:0(0) ack 1 win 0 (DF)15:59:34.899199
10.16.17.101.41738 > 10.16.17.206.53: F 0:0(0) win 409615:59:34.899212
10.16.17.101.41738 > 10.16.17.206.53: F 0:0(0) win 409615:59:34.899282
10.16.17.101.41738 > 10.16.17.206.5901: F 0:0(0) win 409615:59:34.899295
10.16.17.101.41738 > 10.16.17.206.5901: F 0:0(0) win 409615:59:34.899343
10.16.17.206.53 > 10.16.17.101.41738: R 0:0(0) ack 1 win 0 (DF)15:59:34.899379
10.16.17.101.41738 > 10.16.17.206.5801: F 0:0(0) win 409615:59:34.899392
10.16.17.101.41738 > 10.16.17.206.5801: F 0:0(0) win 409615:59:35.201694
10.16.17.101.41739 > 10.16.17.206.80: F 0:0(0) win 409615:59:35.201758
10.16.17.101.41739 > 10.16.17.206.80: F 0:0(0) win 409615:59:35.201887
10.16.17.101.41739 > 10.16.17.206.443: F 0:0(0) win 409615:59:35.201901
10.16.17.101.41739 > 10.16.17.206.443: F 0:0(0) win 409615:59:35.201973
10.16.17.101.41739 > 10.16.17.206.5901: F 0:0(0) win 409615:59:35.201986
10.16.17.101.41739 > 10.16.17.206.5901: F 0:0(0) win 409615:59:35.202055
10.16.17.101.41739 > 10.16.17.206.5801: F 0:0(0) win 409615:59:35.202068
10.16.17.101.41739 > 10.16.17.206.5801: F 0:0(0) win 409615:59:35.803629
10.16.17.101.41738 > 10.16.17.206.5801: F 0:0(0) win 409615:59:35.803696
10.16.17.101.41738 > 10.16.17.206.5801: F 0:0(0) win 409615:59:35.803817
10.16.17.101.41738 > 10.16.17.206.5901: F 0:0(0) win 409615:59:35.803832
10.16.17.101.41738 > 10.16.17.206.5901: F 0:0(0) win 409615:59:35.803904
10.16.17.101.41738 > 10.16.17.206.443: F 0:0(0) win 409615:59:35.803918
10.16.17.101.41738 > 10.16.17.206.443: F 0:0(0) win 409615:59:35.803987
10.16.17.101.41738 > 10.16.17.206.80: F 0:0(0) win 409615:59:35.804000
```

10.16.17.101.41738 > 10.16.17.206.80: F 0:0(0) win 409615:59:36.405546
10.16.17.101.41739 > 10.16.17.206.5801: F 0:0(0) win 409615:59:36.405612
10.16.17.101.41739 > 10.16.17.206.5801: F 0:0(0) win 409615:59:36.405726
10.16.17.101.41739 > 10.16.17.206.5901: F 0:0(0) win 409615:59:36.405740
10.16.17.101.41739 > 10.16.17.206.5901: F 0:0(0) win 409615:59:36.405811
10.16.17.101.41739 > 10.16.17.206.443: F 0:0(0) win 409615:59:36.405825
10.16.17.101.41739 > 10.16.17.206.443: F 0:0(0) win 409615:59:36.405894
10.16.17.101.41739 > 10.16.17.206.80: F 0:0(0) win 409615:59:36.405907
10.16.17.101.41739 > 10.16.17.206.80: F 0:0(0) win 409615:59:37.010929
10.16.17.101.41745 > 10.16.17.206.80: SE 261179130:261179130(0) win 4096
15:59:37.010991 10.16.17.101.41745 > 10.16.17.206.80: SE 261179130:261179130(0)
win 409615:59:37.011124 10.16.17.101.41746 > 10.16.17.206.80: . win 4096
15:59:37.011138 10.16.17.101.41746 > 10.16.17.206.80: . win 4096 15:59:37.011191
10.16.17.206.80 > 10.16.17.101.41745: S 3168497056:3168497056(0) ack 261179131
win 5792 (DF)15:59:37.011221 10.16.17.101.41745 > 10.16.17.206.80: R
261179131:261179131(0) win 015:59:37.011260 10.16.17.101.41745 > 10.16.17.206.80:
R 261179131:261179131(0) win 015:59:37.011344 10.16.17.101.41747 >
10.16.17.206.80: SFP 261179130:261179130(0) win 4096 15:59:37.011357
10 16 17 101 41747 10 16 17 206 80 SFP 261179130 261179130(0) i 4096

- A. Nothing out of the ordinary. This is normal traffic.
- B. This is a buffer overflow attempt against an Microsoft IIS web server running on port 80.
- C. This is a TCP FIN scan against the host 10.16.17.206
- D. None of the above

Answer: C

QUESTION 469:

An administrator is attempting to prioritize any audio or video clips that are served by the Human Resources web server over the static content like text and graphics as part of its http flows. What mechanism best accomplishes this?

- A. LLC
- B. CBWFQ
- C. NBAR
- D. LFI
- E. FRF.8

Answer: C

QUESTION 470:

Which statements correctly describe the sliding window protocol?(Choose Two)

- A. It allows the sender to transmit multiple frames before waiting for an acknowledgement.
- B. The offered window is advertised by the sender.
- C. The size of the sliding window can only increase or stay the same.
- D. The sender does not have to transmit a full window's worth of data.
- E. The receiver has to wait for the window to fill before sending an ACK.

Answer: A,D

QUESTION 471:

What is the purpose of the clock source command used in IOS T1/E1 interface command mode, and what is the default setting?

- A. Routers are DTEs and NEVER supply clock to a T1/E1 line
- B. clock source identifies the stratum level associated with the router T1/E1 and the default is Stratum 1
- C. clock source chooses a source for the interface to clock outbound data. The default is clock source line -Specifies that the T1/E1 link uses the recovered clock from the line
- D. clock source chooses a source for the interface to clock buffered data. The default is clock source loop-timed -Specifies that the T1/E1 interface takes the clock from the Tx (line) and uses it for Rx

Answer: C

QUESTION 472:

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 datagrams.

QUESTION 473:

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 474:

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 475:

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 476:

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 477:

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 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 1
172 96
19 133

QUESTION 478:

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-SeeMe (only the White Pine version) FTP H 323 (such as NetMeeting, ProShare) Java UNIX R-commands (such as rlogin, rexec, and rsh) RealAudio RPC (Sun RPC, not DCE RPC or Microsoft RPC) SMTP SQL*Net StreamWorks TFTP VDOLive In the case of RTSP inspection, session output can vary based on the multimedia protocol and the transport mode.

QUESTION 479:

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 480:

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/half-open/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:0

The Following show commands are not real commands

show ip verify statistics

show ip ids statistics

show audit statistics

show ids statistics

QUESTION 481:

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 482:

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 483:

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 484:

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 485:

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 486:

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 487:

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 488:

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 489:

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 TCP MSS 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 endhosts now send TCP/IP packets no larger than this value.

QUESTION 490:

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 491:

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 492:

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 493:

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 494:

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 495:

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 496:

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 497:

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 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 498:

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 499:

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 500:

Routers operate on what layer?

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

Answer: A

Explanation: Network Layer

QUESTION 501:

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 502:

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 dont apply

QUESTION 503:

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 504:

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 505:

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 506:

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

QUESTION 507:

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 508:

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 509:

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 510:

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 1 and IGRP is a routing protocol (like rip)

QUESTION 511:

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 floodguard 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 512:

Exhibit:

```
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
```

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 513:

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 514:

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 515:

What are triggered updates?

- A. When a router waits until the holddown 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

QUESTION 516:

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 ipsec-isakmp crypto map entries.) In order for the peer's request to be accepted during negotiation, the peer must specify a data flow that is "permitted" by a crypto access list associated with an ipsec-isakmp crypto map command entry. 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 517:

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 518:

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 519:

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 520:

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 521:

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 522:

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 523:

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 524:

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 525:

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 non-IOS commands) will usually suffice

QUESTION 526:

What if the TACACS+ server is unavailable and you have the following command configured? (Select all that apply)
tacacs-serverlast-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 527:

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 528:

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 nameif commands for the inside and outside interfaces. Use the show nameif command to view these commands. They will appear as: nameif ethernet0 outside security0 nameif ethernet1 inside security100

QUESTION 529:

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 530:

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 531:

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 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 any
```

^

Invalid input detected at '^' marker.

```
R1(config)#access-list 2000 deny ip any any
```

I don't agree with the question/answer here as it is not a supported command. The question has IPX and you can't 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 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 a real test the answer could be B if the X is dropped to be just IP (not IPX)

QUESTION 532:

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 533:

ISDN routers in the United States provide which interface?

- A. U
- B. R

- C. S
- D. T
- E. NT2

Answer: A

QUESTION 534:

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

Explanation: "Split horizon" is a scheme for avoiding problems caused by including routes in updates sent to 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.

QUESTION 535:

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 HTTP-over-SSL connection itself, and because this is on TCP port 443, it will not be intercepted by a Content Engine.

QUESTION 536:

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 537:

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 11 and 12 and Routers 21 and 22.

QUESTION 538:

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@REALM Use the ank command to add a privileged instance

of a user. ank
username/instance@REALM

QUESTION 539:

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 540:

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 541:

Exhibit:
r1#sh line
Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns
Int
* 0 CTY - - - - - 8 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 mode -or with no hardware support:

1-64

r1#

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 4

access-class 1 in

B. You cannot do this.

C. access-list 1 permit 1.1.1.1 0.0.0.0

line vty 66 70

access-class 1 in

D. access-list 1 permit 1.1.1.1 255.255.255.255

line vty 0 4

access-class 1 in

Answer: A

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

QUESTION 542:

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 543:

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 IGRP CISCO IOS RELEASE 12.2 T---The IS-IS HMAC-MD5 authentication feature adds an HMAC-MD5 digest 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 544:

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 545:

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 546:

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 mulitcast addresses that are needed OSPF passive interface with listend but not actively be a part of Difference area types can cause adjacencies not to form ICMP has nothing to do with it as well

QUESTION 547:

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 548:

What port number does RADIUS use? Select one.

- A. 1812
- B. 1645
- C. 1813
- D. 110
- E. 25
- F. 1821

Answer: B

Explanation:

This question is ambiguous! Cisco (and Juniper) defaults to port 1645 (the selected answer) and IANA assigned 1812.

1812 (authentication) / 1813 Accounting (IANA) and 1645 (Authentication Cisco default) / 1646 (Accounting - Cisco default).

QUESTION 549:

The Cisco Secure IDS provides protection for which of the following? (Select all that apply)

- A. Unauthorized network access
- B. Worms
- C. E-business application attacks
- D. Virus signatures
- E. Spam
- F. Bandwidth overutilization

Answer: A, B, C

QUESTION 550:

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 551:

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.

dtl-45a#show crypto key mypubkey rsa

% Key pair was generated at: 11:31:59 PDT Apr 9 1998

Key name: dtl-45a.cisco.com

Usage: Signature Key

Key Data:

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C11854

39A9C75C

4E34C987 B4D7F36C A058D697 13172767 192166E1 661483DD 0FDB907B

F9C10B7A

CB5A034F A41DF385 23BEB6A7 C14344BE E6915A12 1C86374F 83020301 0001

% Key pair was generated at: 11:32:02 PDT Apr 9 1998

Key name: dtl-45a.cisco.com

Usage: Encryption Key

Key Data:

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DCF5AC
360DD5A6
C69704CF 47B2362D 65123BD4 424B6FF6 AD10C33E 89983D08 16F1EA58
3700BCF9
1EF17E71 5931A9FC 18D60D9A E0852DDD 3F25369C F09DFB75 05020301 0001

QUESTION 552:

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 553:

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. wr t
- 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 554:

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 555:

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 556:

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 557:

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 558:

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 asks 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 559:

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 560:

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 561:

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 (sessionless) 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 562:

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 563:

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

QUESTION 564:

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 0 router
```

```
line con 0
```

```
login authentication default
```

Look at the attached configuration. If the RADIUS server is unavailable, what will happen when the rootuser tries to login?

- A. He will be authenticated locally.
- B. Login will succeed through RADIUS.
- C. Login will fail.
- D. Router will crash.

Answer: A

Explanation: If there is no response from RADIUS server, according to the command , the router will search for its local database, and because the command 'username root xxxx' is there, root user will be authenticated successfully. So, the answer is A.

QUESTION 565:

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 566:

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 567:

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 568:

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 dont make assumptions. Security policy cover a huge reange of topics from accpetible use to applications.

QUESTION 569:

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 synwait-time is 30 sec -- tcp finwait-time is 5 sec

tcp idle-time is 3600 sec -- udp idle-time is 30 sec

dns-timeout is 5 sec

Inspection Rule Configuration

Inspection name mysite

ftp timeout 3600

smtp timeout 3600

tcp timeout 3600

Look at the attached command output. What protocols is CBAC currently configured to inspect?

(Select all that apply)

- A. ftp
- B. vdlive
- 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 570:

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 571:

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

QUESTION 572:

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-cleartext

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 573:

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 574:

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 any eq echo
access-list 101 deny ip any any eq discard
int lo0
access-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 575:

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

QUESTION 576:

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 577:

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 dont 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 578:

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

QUESTION 579:

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 580:

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

QUESTION 581:

By default, what is a peer router's ISAKMP identity?

- A. hostname
- B. IP Address
- C. pubkey
- D. keystore
- 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` sets 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 582:

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 `autocommand` 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 583:

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 configurator.

Answer: A

Explanation: PIX device manager

QUESTION 584:

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 585:

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 586:

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

- A. aaa new-model
radius-server host 172.22.53.201 auth-port 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

QUESTION 587:

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 588:

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 589:

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 590:

In RFC 2138 (RADIUS), vendor specific attributes (VSA) are specified. Specifically, this is called

VSA 26 (attribute 26). These allow vendors to support their own extended options.

Cisco's vendor

ID is 9. Which of the following commands tell the Cisco IOS to use and understand VSA's ? (Select all that apply)

- A. radius-server vsa send
- B. radius-server vsa send authentication
- C. radius-server vsa send accounting
- D. ip radius-server vsa send
- 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 591:

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 592:

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. logg buff 4096
- B. access-list 101 deny any 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 593:

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 594:

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 595:

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
- D. IOS firewall.
- E. 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 Internetwork Expert Security Exam v1.7 by John J. Kaberna pg 415

QUESTION 596:

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 597:

RADIUS uses what as its transport protocol?

- A. UDP
- B. TCP
- C. ARP
- D. IPSec
- E. IPX
- F. SSH

Answer: A

QUESTION 598:

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 (router-config-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 599:

If you run the "show ip ospf neighbor" command, which of the following are a possible output?

- A. init
- B. exstart/exchange
- C. 2-way
- D. loading

- E. nothing at all
- F. all of the above

Answer: F

QUESTION 600:

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 601:

What is the STP cost for a 10Mb ethernet link?

- A. 1
- B. 10
- C. 100
- D. 1000
- E. 64
- F. 250

Answer: C

QUESTION 602:

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

- A. rte-fltr-out#0="router igmp 60"
- B. user = georgia {
login = cleartext lab
service = ppp protocol = ip {
addr-pool=bbb

```
}}  
C. cisco-avpair = "ip:addr-pool=bbb"  
D. route#1="3.0.0.0 255.0.0.0 1.2.3.4"
```

Answer: C

QUESTION 603:

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

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 604:

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 605:

What is the command to disable IKE?

Answer: no crypto isakmp enable

QUESTION 606:

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 607:

Which of the following commands would apply a CBAC rule to an interface?

- A. ip inspect {inspection name} in
- B. ip inspection name} in
- C. There is no such command
- D. ip {inspection name} inspect in

Answer: A

QUESTION 608:

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

QUESTION 609:

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 610:

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 611:

Exhibit:

```
interface Serial1/0:0.254 point-to-point
ip address 10.0.100.1 255.255.255.252
no ip proxy-arp
access-group 155 out
no cdp enable
frame-relay class 1544Kfrkeepalive
frame-relay interface-dlci 45
access-list 155 permit ip any 10.254.0.0 0.0.255.255 eq
telnet time-range timelist
time-range timelist
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 any 10.254.0.0 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 612:

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 613:

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 614:

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 615:

Which of these routing protocols support discontinuous 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 discontinuous networks

QUESTION 616:

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 617:

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 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 any reflect tcptraffic Define the reflexive access list tcptraffic. This entry permits all outbound TCP traffic and creates a new access list named tcptraffic. 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 tcptraffic. The "access-list 101 permit tcp 0.0.0.0 255.255.255.255 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 618:

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 619:

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 require 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 620:

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

QUESTION 621:

What does a PIX do with tcp sequence number to minimize the risk of tcp sequence

number attacks? (Select all that apply)

- A. Randomize them.
- B. Make sure they are within an acceptable range.
- C. Doesn't use them.
- D. Uses the same numbers over and over again.
- 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 622:

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 (ie: attempt on a specific host)
Compound signatures (twenty-seven): detect complex patterns (ie: attack on multiple hosts, over extended time periods with multiple packets)
Info signatures (forty): detect information-gathering activities (ie: port sweep)
Attack signatures (sixty-one): detect malicious activity (ie: illegal ftp commands)

QUESTION 623:

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 624:

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 625:

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 626:

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. wr m

Answer: C

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

QUESTION 627:

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 628:

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 629:

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.

--Recently an instructor in a class I was taking said something I found interesting. I hope I can do justice to his words.

---Network layer: IP IP IP

---Transport layer: TCP UDP

---Application layer: BGP RIP EIGRP, OSPF, IGRP

QUESTION 630:

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
- B. RADIUS.
- C. No, AAA is not required to use RADIUS, just use the "ip auth radius" commands.
- D. Yes, you must configure AAA to use TACACS+, Kerberos, or RADIUS.

Answer: C

QUESTION 631:

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 632:

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 633:

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 authNoPriv MD5 or SHA Provides authentication based on

the HMAC-MD5 or HMAC-SHA algorithms. Version 3 authPriv MD5 or SHA DES Provides authentication based on the HMAC-MD5 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 634:

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 635:

Exhibit:

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

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

- A. The one from your RADIUS server.

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

QUESTION 636:

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 reenable 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 637:

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

QUESTION 638:

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 1
172 96
19 133

QUESTION 639:

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 640:

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 641:

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 642:

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 643:

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 644:

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 645:

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

QUESTION 646:

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: A, C

QUESTION 647:

What command is this output from?

```
nameif ethernet0 outside security0  
nameif ethernet1 inside security100
```

- A. show nameif
- B. show name
- C. show interfaces
- D. show ip int brief
- E. show run

Answer: A

QUESTION 648:

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 649:

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 650:

What protocol does TACACS+ use to communicate?

- A. TCP
- B. UDP
- C. IPX
- D. TAC
- E. RADIUS
- F. IPSec

Answer: A

QUESTION 651:

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

Access-list 2000 permit ip host 10.1.1.1 host 10.2.2.2

Access-list 2000 deny ip any any

Access-list 2000 permit ip any any log

- A. All traffic is allowed through.
- B. All traffic from host 10.1.1.1 to host 10.2.2.2 is allowed through.
- C. All traffic from host 10.2.2.2 to host 10.1.1.1 is allowed through.
- D. No traffic is allowed through.
- E. This access-list is invalid as 2000 is the range for IPX access-lists.

Answer: B

Explanation: Access-list 2000 deny ip any any

Access-list 2000 permit ip any any log

THIS IS IN THE WRONG ORDER! YOU DENY BUT THEN YOU ARE PERMITTING ALL BUT

LOGGING IT source to destination

QUESTION 652:

What command will show the security levels, configured for interfaces, on a PIX firewall?

- A. show nameif
- B. show interfaces
- C. show ip interface brief
- D. show name interfaces
- E. show run

Answer: A

QUESTION 653:

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 654:

What is the easiest way to clear your router of RSA keys that have been generated?

- A. no crypto key zeroize 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 zeroize rsa global configuration command

QUESTION 655:

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 656:

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 657:

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 658:

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

- A. $100 \text{ Mbps} / 10 \text{ Mbps} = 10$
- B. $100 \text{ Mbps} / 10 \text{ Mbps} = 1$
- C. $1000 \text{ Mbps} / 10 \text{ Mbps} = 100$
- D. $100 \text{ Bbps} / 10 \text{ Mbps} / \text{Cost} = .10$
- E. 10

F. $100 \text{ Mbps} / 10 \text{ Mbps} * \text{delay} = 10$

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 25

Ethernet-Default cost is 10

16-Mbps Token Ring-Default cost is 6

FDDI-Default cost is 1

ATM- Default cost is 1

QUESTION 659:

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 660:

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 Ciscoworks.
- E. Supports only PIX.

Answer: A, B, D

QUESTION 661:

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

QUESTION 662:

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 663:

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 664:

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 665:

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

- A. 1-99
- 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
100-199 IP 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
1000-1099 IPX 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 666:

You want to make sure that you only receive routing updates about networks in the 10.x.x.x range.

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 667:

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 668:

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

QUESTION 669:

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 670:

Exhibit:

```
ip http server
```

```
ip http access-class 1
```


access-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 671:

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 672:

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 673:

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 674:

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 675:

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

- A. access-list 52 deny 0.0.0.0 255.255.255.255
line aux 0
access-class 52 in
- B. access-list 52 deny 0.0.0.0 255.255.255.255

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

Answer: A

QUESTION 676:

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

- A. RADIUS
- B. TACACS+
- C. IPSec
- D. AAAA
- E. NTLM

Answer: B

QUESTION 677:

What is a benefit of implementing RFC 2827?

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

Answer: C

Explanation

RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

Recent occurrences of various Denial of Service (DoS) attacks which have employed forged source addresses have proven to be a troublesome issue for Internet Service Providers and the Internet community overall. This paper discusses a simple, effective, and straightforward method for using ingress traffic filtering to prohibit DoS attacks which use forged IP addresses to be propagated from 'behind' an Internet Service Provider's (ISP) aggregation point.

While the filtering method discussed in this document does absolutely nothing to protect against flooding attacks which originate from valid prefixes (IP addresses), it will prohibit an attacker within the originating network from launching an attack of this nature using forged source addresses that do not conform to ingress filtering rules. All providers of Internet connectivity are urged to implement filtering described in this

document to prohibit attackers from using forged source addresses which do not reside within a range of legitimately advertised prefixes. In other words, if an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.

QUESTION 678:

```
Access-list 111 permit udp any any eq 1434
Class-map match-all bad_worm
Match access-group 111
Match packet length min 404 max 404
Policy-map drop-bad-worm
Class bad-worm
Police 1000000 22250 22250 confirm-action drop exceed-action drop violate-action drop
```

Taking into consideration the shown configuration, what kind of attack are we attempted to mitigate?

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

Answer: C

QUESTION 679:

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

- A. Enables an EOUPD identity profile for clientless hosts
- B. Statically authorize and maps devices to an access policy
- C. Maps the NAD to clientless host for posture authorization
- D. Statically maps an access-list to a NAC agentless host (NAH)

Answer: B

QUESTION 680:

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

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

Answer: D

QUESTION 681:

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

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

Answer: D

QUESTION 682:

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

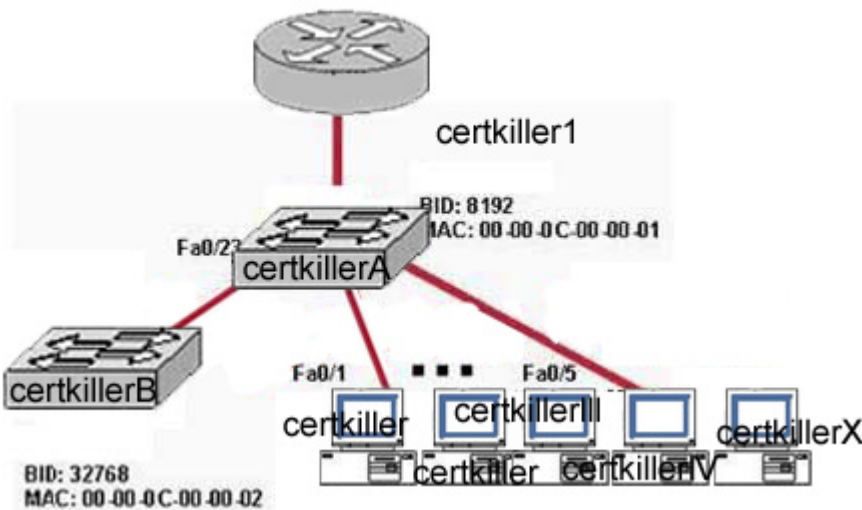
- A. ASA supports both stub multicast routing and PIM multicast routing. However, you can't configure both concurrently on a single security appliance
- B. When Configured for stub multicast routing, the ASA can act as the Rendezvous Point (RP)
- C. If the ASA detects IGMP version 1 routers, the ASA will automatically switch to IGMP version 1 operations
- D. The ASA supports both PIM-SM and bi-directional PIM
- E. Enabling multicast routing globally on the ASA automatically enables PIM and IGMP on all interfaces
- F. The ASA can be configured for IGMP snooping to constrain the flooding of multicast

traffic by dynamically configuring the multicast traffic to be forwarded only those interfaces associated with hosts requesting the multicast group

Answer: A,D,E

QUESTION 683:

Network topology exhibit:



You work as a network engineer at Certkiller .com. Please study the exhibit carefully. Switch Certkiller B has just been added to FastEthernet 0/23 on Certkiller

A. After a few seconds, interface FA0/23 on Certkiller A is placed in the error-disabled state. Certkiller B is removed from port 0/23 and inserted into Certkiller A port Fa0/22 with the same result. What is the most likely cause of this problem?

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

Answer: C

QUESTION 684:

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

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

Answer: A

QUESTION 685:

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

- A. VTP messages are sent out all switch-switch connections
- B. VTP L2 messages are communicated to neighbors using CDP
- C. VTP manages addition, deletion and renaming of VLANS 1 to 4094
- D. VTP pruning restricts flooded traffic, increasing available bandwidth
- E. VTP V2 can only be used in a domain consisting of V2 capable switches
- F. VTP v2 performs consistency checks on all sources of VLAN information

Answer: D,E

QUESTION 686:

Which of the following is true for RFC 4301 - Security Architecture for the Interface Protocol (obsoletes RFC 2401) (Select two.)

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

Answer: C,E

QUESTION 687:

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

- A. Policy based routing (PBR)
- B. Unicast Reverse Path Forwarding (uRPF)
- C. Local and Key ACL
- D. FRC 1918 filtering
- E. IP Source Routing

Answer: B

QUESTION 688:

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

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

Answer: A,B,D,E

QUESTION 689:

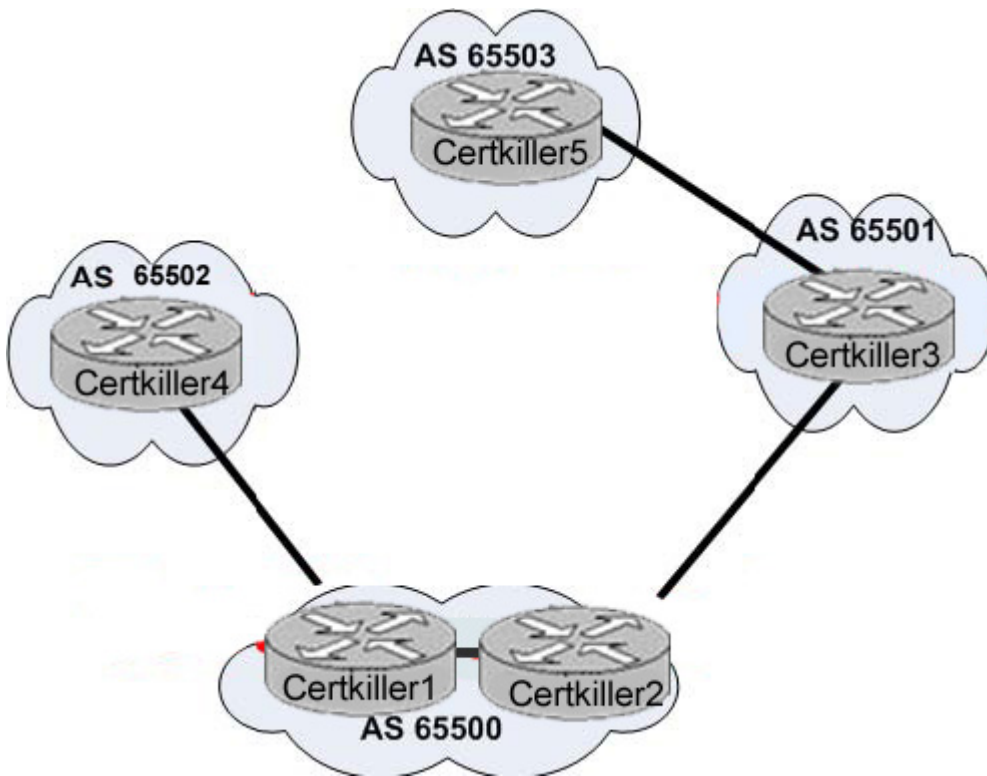
When configuring a multipoint GRE (mgre) tunnel interface, which one of the following is NOT a valid configuration option?

- A. Tunnel Source
- B. Tunnel Destination
- C. Tunnel key
- D. IP Address
- E. Tunnel vrf

Answer: B

QUESTION 690:

Network topology exhibit:



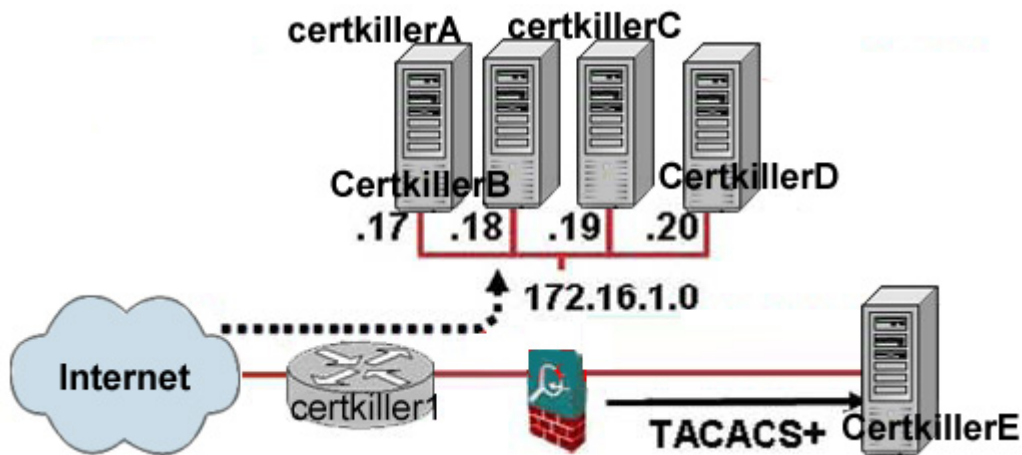
You work as a network engineer at Certkiller .com. Please study the exhibit carefully. What as-path access-list regular expression should be applied on Certkiller 2 to only allow updates originated from AS65501 or autonomous systems directly attached to AS65501?

- A. _65501_.*
- B. _65601_*\$
- C. ^65601_*\$
- D. _656501+[0-9]\$\
- E. ^65501_[0-9]*\$\
- F. \[0-9]*65501_+\[0-9]\$\

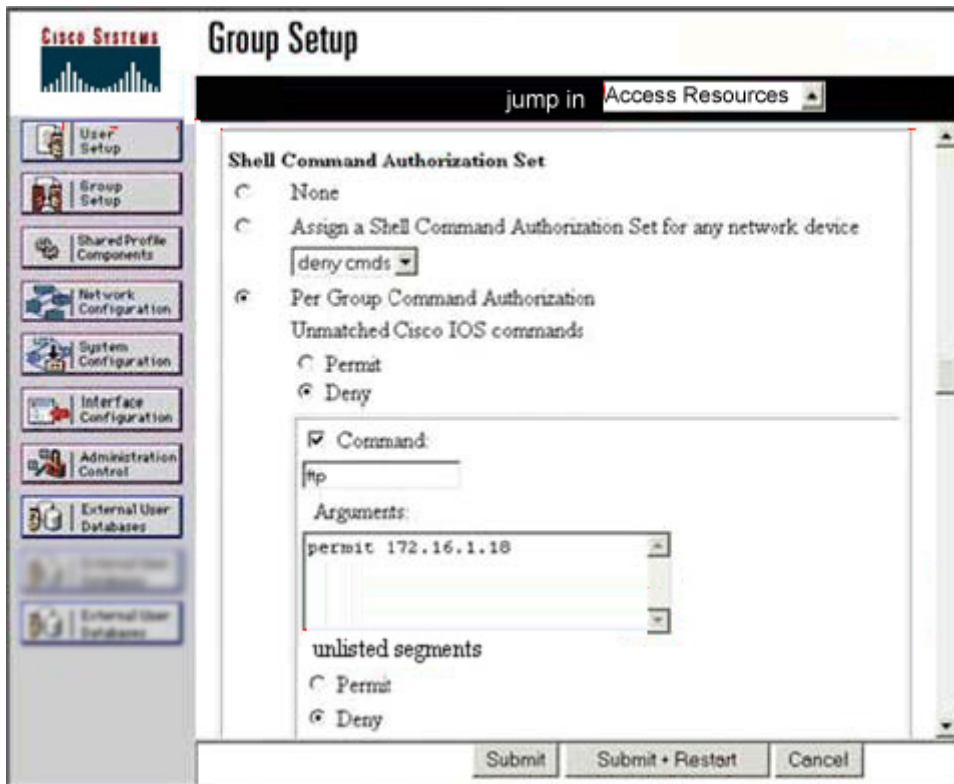
Answer: E

QUESTION 691:

Network topology exhibit:



Configuration exhibit:



You work as a network engineer at Certkiller .com. Please study the exhibits carefully.

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

A. Access any server on the DMZ

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

Answer: C,F

QUESTION 692:

Exhibit:

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

You work as a network engineer at Certkiller .com. Please study the exhibit carefully.
What is the most probable cause of the SSH debug messages?

- A. unsupported cipher
- B. Bad password
- C. Wrong user
- D. SSH client not supported

Answer: B

QUESTION 693:

Which algorithms did CKIP add to the 802.11 specification? (Choose 3)

- A. Key mixing

- B. AES-Based Encryption
- C. Anti-replay sequence counter
- D. Message integrity check
- E. Cyclic redundancy check

Answer: A,C,D

QUESTION 694:

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

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

Answer: A

QUESTION 695:

Which three steps are required to enable SSH server on an IOS router? (Choose three)

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

Answer: A,B,F

QUESTION 696:

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

- A. SDEE

- B. Telnet
- C. Console
- D. FTP
- E. HTTPS
- F. SSH

Answer: B,F

QUESTION 697:

Network topology exhibit:



You work as a network engineer at Certkiller .com. Please study the exhibit carefully.

```
certkiller1(config)# access-list 101 permit tcp any 10.2.1.0 0.0.0.255 established
certkiller1 (config)# access-list 101 deny ip any any log
certkiller1 (config)# interface e0/0
certkiller1 (config)if # ip access-group 101 in
certkiller1 (config) if # end
```

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

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

Answer: E

QUESTION 698:

Cisco IOS IPS sends IPS alerts messages using which two protocols? (Choose two.)

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

Answer: A,C

QUESTION 699:

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

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

Answer: B

QUESTION 700:

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

- A. Group 3
- B. Group 1
- C. Group 5
- D. Group 7

Answer: C

QUESTION 701:

Select the two correct statements from the list below that describes DES and 3DES.
(Choose two.)

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

operation

E. DES can only be used for encryption, whereas 3DES can also be used for authentication

Answer: C,D

QUESTION 702:

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

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

Answer: C,D

QUESTION 703:

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

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

Answer: B,D

QUESTION 704:

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

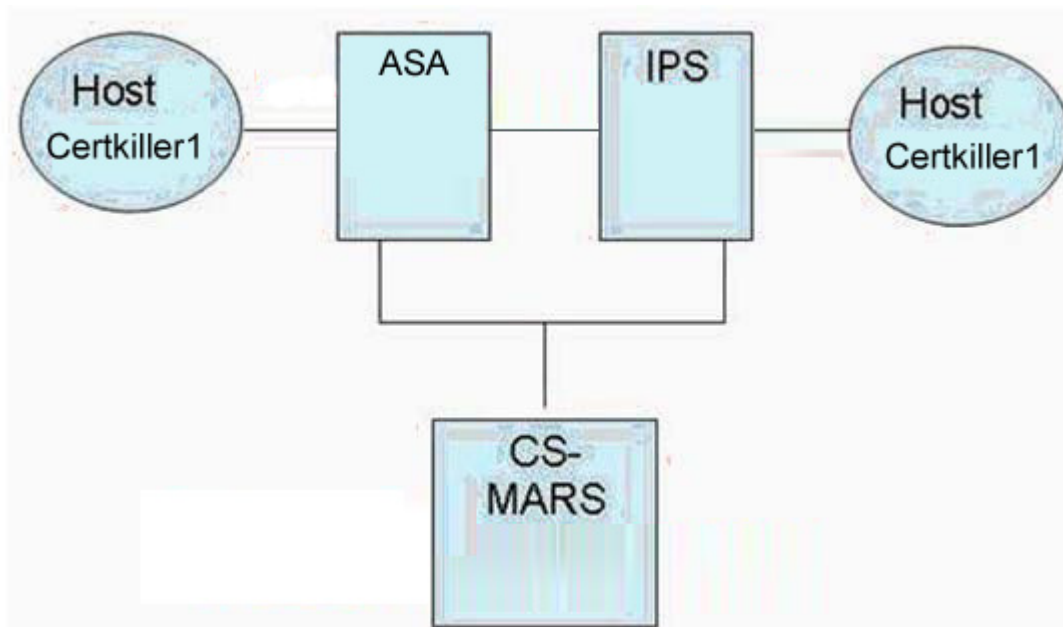
- A. At the untrusted interface in the inbound direction
- B. At the untrusted interface in the outbound direction
- C. At the trusted interface in the inbound direction

- D. At the trusted interface in the outbound direction
- E. At the trusted and untrusted interface in the inbound direction
- F. At the trusted and untrusted interfaces in the outbound direction

Answer: B,C

QUESTION 705:

Exhibit:



You work as a network engineer at Certkiller .com. Please study the exhibit carefully. In the example shown, Host A has attempted a D-COM attack using metasploit metasploit from Host A to Host B. Which answer best describes host event logs and IPS alerts can be used in conjunction with each other to determine if the attack was successful? (Choose 3)

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

Answer: A,B,E

QUESTION 706:

What technologies are included in Anti-X? (Choose three.)

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

Answer: A,B,D

QUESTION 707:

When configuring the FWSM for multiple security context in which context do you allocate interfaces?

- A. Context A
- B. System Context
- C. Admin Context
- D. Both B and C

Answer: B

QUESTION 708:

DRAG DROP

You work as a network engineer at Certkiller .com. Your boss, Miss Certkiller, is interested in protocol characteristics. Match the characteristics with the appropriate protocols.

Options, select from these

Combines the authentication and authorization functions

Only encrypts the password

Allows authorization of router commands on a per-user or pergroup hosts

Uses TCP port 49

Radius

Tacacs+

Place here

Place here

Place here

Place here

Answer:

Radius

Tacacs+

Combines the authentication and authorization functions

Allows authorization of router commands on a per-user or per-group basis

Only encrypts the password

Uses TCP port 49

QUESTION 709:

Choose the correct security statements about the HTTP protocol and its use (Choose Two.)

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

Answer: C,E

QUESTION 710:

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

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

Answer: C

QUESTION 711:

Which of the following is true about the Cisco IOS-IPS functionality? (Choose two.)

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

Answer: C,D

QUESTION 712:

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

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

Answer: D

QUESTION 713:

Asymmetric and symmetric ciphers differ in which of the following way(s)? (Choose two.)

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

Answer: B,D

QUESTION 714:

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

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

Answer: A

QUESTION 715:

Given the topology of a server (with IP 209.165.202.150) protected behind the inside interface of an ASA/PIX and the internet on the outside interface. Users on the Internet need to access the server at any time, but the firewall administrator does not want to NAT the address of the server ?? Since it is currently a public address. Which of the following commands can be used to accomplish this? (Choose three.)

- A. Nat(inside) 0 209.165.202.150 255.255.255.255
- B. Access-list no nat permit ip host 209.165.202.150 nat (inside) 0 access-list no-nat
- C. Static (inside, outside) 209.165.202.150 209.165.202.150 netmask 255.255.255.255
- D. No nat-control
- E. Nat (inside) 1 209.165.202.150 255.255.255.255

Answer: B,C,D

QUESTION 716:

Which of the following statements that describes the PPTP protocol is incorrect?

- A. The control session for PPTP runs over TCP port 1723
- B. A single PPTP tunnel can carry multiple end-to-end PPP sessions
- C. MPPE encryption to secure the tunnel is required for PPTP

D. The data session uses a modified version of GRE as transport

Answer: C

QUESTION 717:

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

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

Answer:

QUESTION 718:

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

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

Answer: C

QUESTION 719:

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

- A. Syn Flood
- B. Source IP Address spoofing
- C. Overlapping IP framgements
- D. Tiny IP Fragments
- E. Land.C
- F. Network Reconnaissance

Answer: B

QUESTION 720:

What is true about SYN cookies?

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

Answer: D

QUESTION 721:

What Cisco Switch feature best protects against CAM table overflow attacks?

- A. Strom control
- B. Port Security
- C. CAM table size definition
- D. IP Spoof prevention
- E. Network Based Application Recognition

Answer: B

QUESTION 722:

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

```
Crypto isakmp policy 7  
Encryption aes  
Hash sha 1  
Authentication rsa-sig  
Group 2  
Lifetime 86400
```

- A. Crypto isakmp policy 7
- B. Encryption aes
- C. Hash sha 1
- D. Authentication rsa-sig
- E. Group 2
- F. Lifetime 86400

Answer: C

QUESTION 723:

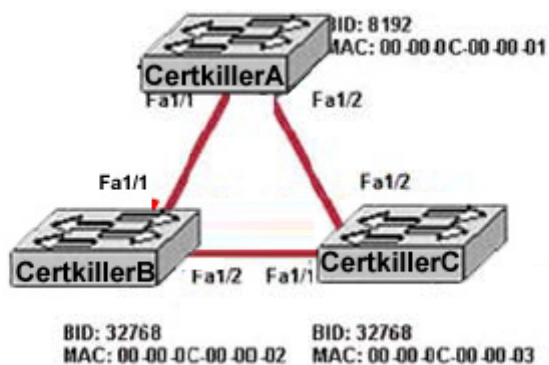
Which option describes the actions that can be taken when an IPS 5.x signature fires?

- A. Deny packet inline - Produce Alert
- B. Drop Connection - DROP Packet
- C. Procedure Alert - Produce Detailed Alert
- D. Block Connection - Generate SNMP Trap
- E. Drop Packet - Suppress Alert

Answer: A

QUESTION 724:

Network topology exhibit:



Configuration exhibit:

```

Certkiller1> (enable) show port 1

```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
1/1		connected	1	normal	a-full	a-100	10/100BaseTX
1/2		connected	1	normal	a-alf	a-100	10/100BaseTX

```

Certkiller2> show port counters 1

```

Port	Align-Err	FCS-Err	Xmit-Err	Rcv-Err	UnderSize
1/1	0	0	0	0	0
1/2	0	0	0	0	0

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

```

Certkiller3> (enable) show spanntree 1 active

```

VLAN 1

Spanning tree mode PVST+

Spanning tree type ieee

spanning tree enabled

Designated Root 00-00-0c-00-00-02

Designated Root Priority 32768

Designated Root Cost 19

Designated Root Port 1/1

Root Max Age 14 sec Hello Time 2 sec Forward Delay 10 sec

Bridge ID MAC ADDR 00-00-0c-00-00-03

Bridge ID Priority 32768

Bridge Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec

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

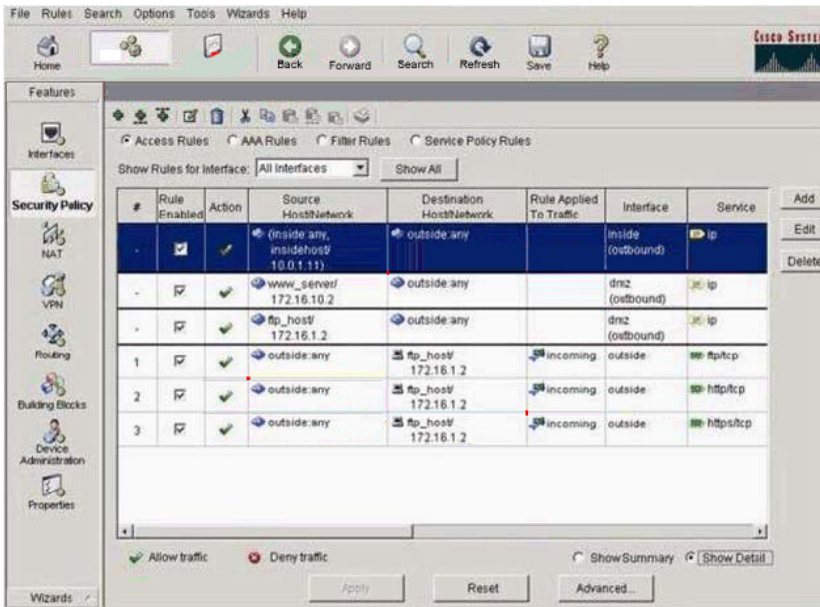
You work as a network engineer at Certkiller .com. Please study the exhibit carefully. Under normal conditions, Certkiller A is spanning tree root and the link between Certkiller B AND Certkiller C is in the blocking state. This network transports large amounts of traffic and is heavily loaded. After a software upgrade to these switches, users are complaining about slow performance. To troubleshoot the commands shown in the exhibit are entered. What tow are the most likely causes of this issue?

- A. Lack of BPDUs from high priority bridge Certkiller A causes Certkiller C to unblock Fa1/1
- B. Duplex mismatch on the link between Certkiller A and Certkiller C causing high rate of collisions
- C. The Max Age timers on Certkiller A and Certkiller B have been changed and no longer match the MAX age timer on Certkiller C
- D. UDLD has not been configured Certkiller A and Certkiller C on Certkiller C errantly sees its link to Certkiller A as up and operational

Answer: A,B

QUESTION 725:

Exhibit:



You work as a network engineer at Certkiller .com. Please study the exhibit carefully. Referring to the ASDM screen shot shown in the exhibit, which of the following traffic is permitted based on the current Access Rules?

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

Answer: E

QUESTION 726:

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

- A. Pre-Shared Key
- B. Secure hash
- C. SSL
- D. RSA signature

Answer: D

QUESTION 727:

Network topology exhibit:

```
crypto isakmp policy 1
encr 3des
authentication pre-state
group 2
!
crypto isakmp key cisco123 address 10.3.3.1
!
crypto ipsec transform-set mytrns esp-3des esp-sha-hmac
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
description Tunnel to 10.3.3.1
set peer 10.3.3.1
set transform-set mytrns
match address 103
!
interface FastEthernet0/0
description $FW_INSIDE$
ip address 172.16.4.2 255.255.255.0
ip access-group 100 in
ip inspect SDM_LOW in
ip nat inside
!
interface Serial0/0/0
description $FW_OUTSIDE$
ip address 10.4.1.255 255.255.255.252
ip access-group 102 in
ip verify unicast reverse-path
ip nat outside
crypto map SDM_CMAP_1
!
ip nat inside source route-map rmap interface Serial0/0/0 overload
!
route-map rmap permit 1
match ip address 104
!
access-list 100 deny ip 10.4.0.0 0.0.3 any
access-list 100 deny ip 172.16.14.0 0.0.255 any
access-list 100 deny ip host 255.255.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip any any
!
access-list 102 permit ip 172.16.3.0 0.0.255 172.16.4.0 0.0.255
access-list 102 permit udp host 10.3.3.1 host 10.4.4.1 eq non500-isakmp
access-list 102 permit udp host 10.3.3.1 host 10.4.4.1 eq isakmp
access-list 102 permit esp host 10.3.3.1 host 10.4.4.1
access-list 102 permit ah host 10.3.3.1 host 10.4.4.1
access-list 102 permit tcp any host 10.4.4.1 eq 1000
access-list 102 permit icmp host 10.3.3.1 host 10.4.4.1 echo
access-list 102 deny ip 172.16.4.0 0.0.255 any
access-list 102 deny ip 172.16.14.0 0.0.255 any
access-list 102 permit icmp any host 10.4.4.1 echo-reply
access-list 102 permit icmp any host 10.4.4.1 time-exceeded
access-list 102 permit icmp any host 10.4.4.1 unreachable
access-list 102 permit tcp any host 172.16.14.1 eq telnet
access-list 102 permit eigrp any any
access-list 102 deny ip 10.0.0.0 0.255.255.255 any
access-list 102 deny ip 172.16.0.0 0.15.255.255 any
access-list 102 deny ip 192.168.0.0 0.255.255.255 any
access-list 102 deny ip 127.0.0.0 0.255.255.255 any
access-list 102 deny ip host 255.255.255.255 any
access-list 102 deny ip host 0.0.0.0 any
access-list 102 deny ip any any log
!
access-list 103 permit ip 172.16.4.0 0.0.255 172.16.3.0 0.0.255
!
access-list 104 deny ip 172.16.4.0 0.0.255 172.16.3.0 0.0.255
access-list 104 permit ip 172.16.4.0 0.0.255 any
access-list 104 permit ip 172.16.14.0 0.0.255 any
```

You work as a network engineer at Certkiller .com. Please study the exhibit carefully. Referring to partial IOS router configuration shown in the exhibit, which statement is true?

- A. Traffic from subnet 172.16.4.0/24 to the 172.16.3.0/24 subnet will be protected by IPSec and will go through NAT
- B. Traffic from subnet 172.16.4.0/24 to any destinations will be protected by IPSec and will bypass NAT
- C. All IPSec protected traffic will bypass NAT
- D. All traffic from subnet 172.16.4.0/24 to the 172.16.3.0/24 subnet will go through NAT

Answer: D

QUESTION 728:

Referring to the debug output shown below, what is the causing the IKE Main Mode Failure?

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

- A. The IPSec transform set on the peers do not match
- B. The Crypto ACL is not a mirror image of the peer

- C. The IKE Phase 1 Policy does not match on both sides
- D. The pre-shared keys on the peers do not match

Answer: C

QUESTION 729:

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

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

Answer: B,E

QUESTION 730:

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

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

Answer: A

QUESTION 731:

CSA protects your host by:

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

Answer: A

QUESTION 732:

Network topology exhibit:

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

You work as a network engineer at Certkiller .com. Please study the exhibit carefully. In the sample configuration file what does the IP verify unicast reverse-path interface command accomplish?

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

Answer: C

QUESTION 733:

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

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

Answer: A,C

QUESTION 734:

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

- A. Day Zero attack
- B. Man-in-the Middle attacks
- C. Trojan Horse
- D. Buffer Overflow
- E. Land.c attack

Answer: A

QUESTION 735:

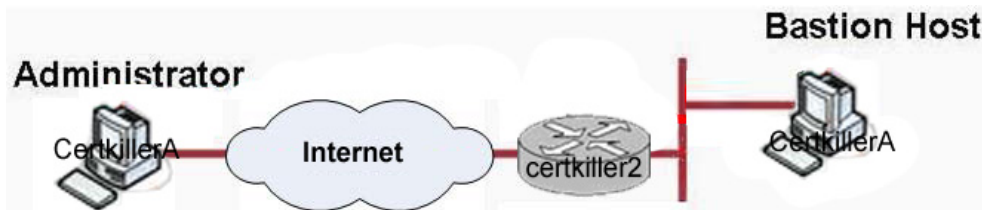
Select two statements that correctly describe the ESP protocol (Choose two.)

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

Answer: B,E

QUESTION 736:

Network topology exhibit:



You work as a network engineer at Certkiller .com. Please study the exhibit carefully. The Router in the exhibit only supports telnet access from the Bastion Host. The Bastion Host is running SSH. What option is SSH would allow the remote administrator to make a secure connection across the Internet to the route?

- A. Power Forwarding Option
- B. Telnet emulator option
- C. Secure telnet option
- D. There are no options to accomplish this

Answer: A

QUESTION 737:

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

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

Answer: E

QUESTION 738:

What of the following statements that describe Diffie Hellman Key Exchange are correct? (Choose Four)

- A. A DH key exchange is an algorithm that utilizes asymmetric cryptographic keys
- B. The DH key exchange is used to establish a shared secret over an insecure medium

during an IPSec phase 1 exchange

C. The DH exchange is susceptible to man-in-the-middle attacks

D. The DH exchange is used to authenticate the peer device during an IPSec phase 1 exchange

E. A DH exchange provides Perfect Forward Secrecy (PFS)

Answer: A,B,C,E

QUESTION 739:

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

A. Access-reject

B. Access-response

C. Access-challenge

D. Access-reply

E. Access-accept

Answer: B