



Exam : 642-552

Title : Securing Cisco Network Devices

Ver : 01-21-09

QUESTION 1:

A malicious program is disguised as another useful program; consequently, when the user executes the program, files get erased and then the malicious program spreads itself using emails as the delivery mechanism. Which type of attack best describes how this scenario got started?

- A. DoS
- B. worm
- C. virus
- D. trojan horse
- E. DDoS

Answer: D

Explanation:

Denial of Service (DoS) is an attack designed to render a computer or network incapable of providing normal services. The most common DoS attacks will target the computer's network bandwidth or connectivity. Bandwidth attacks flood the network with such a high volume of traffic, that all available network resources are consumed and legitimate user requests cannot get through. Connectivity attacks flood a computer with such a high volume of connection requests, that all available operating system resources are consumed and the computer can no longer process legitimate user requests.

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include

- * attempts to "flood" a network, thereby preventing legitimate network traffic
- * attempts to disrupt connections between two machines, thereby preventing access to a service
- * attempts to prevent a particular individual from accessing a service
- * attempts to disrupt service to a specific system or person

Distributed Denial of Service

- * An attacker launches the attack using several machines. In this case, an attacker breaks into several machines, or coordinates with several zombies to launch an attack against a target or network at the same time.
- * This makes it difficult to detect because attacks originate from several IP addresses.
- * If a single IP address is attacking a company, it can block that address at its firewall. If it is 300 00 this is extremely difficult.

QUESTION 2:

What is the key function of a comprehensive security policy?

- A. informing staff of their obligatory requirements for protecting technology and information assets
- B. detailing the way security needs will be met at corporate and department levels

- C. recommending that Cisco IPS sensors be implemented at the network edge
- D. detailing how to block malicious network attacks

Answer: A

Explanation:

Developing a strong security policy helps to protect your resources only if all staff members are properly instructed on all facets and processes of the policy. Most companies have a system in place whereby all employees need to sign a statement confirming that they have read and understood the security policy. The policy should cover all issues the employees encounter in their day-to-day work, such as laptop security, password policy, handling of sensitive information, access levels, tailgating, countermeasures, photo IDs, PIN codes, and security information delivered via newsletters and posters. A top-down approach is required if the policy is to be taken seriously. This means that the security policy should be issued and supported from an executive level downward.

QUESTION 3:

Which building blocks make up the Adaptive Threat Defense phase of Cisco SDN strategy?

- A. VoIP services, NAC services, Cisco IBNS
- B. network foundation protection, NIDS services, adaptive threat mitigation services
- C. firewall services, intrusion prevention, secure connectivity
- D. firewall services, IPS and network antivirus services, network intelligence
- E. Anti-X defense, NAC services, network foundation protection

Answer: D

Explanation:

Computer connected to the Internet without a firewall can be hijacked and added to an Internet outlaw's botnet in just a few minutes. A firewall can block malware that could otherwise scan your computer for vulnerabilities and then try to break in at a weak point. The real issue is how to make one 99.9% secure when it is connected to in Internet. At a minimum computers need to have firewall, antivirus and anti-spyware software installed and kept up-to-date. A home network that uses a wired or wireless router with firewall features provides additional protection.

A computer virus can be best described as a small program or piece of code that penetrates into the operating system, causing unexpected and negative events to occur. A well-known example is a virus, SoBig. Computer viruses reside in the active memory of the host and try to duplicate themselves by different means. This duplication mechanism can vary from copying files and broadcasting data on local-area network (LAN) segments to sending copies via e-mail or an Internet relay chat (IRC). Antivirus software applications are developed to scan the memory and hard disks of hosts for known viruses.

If the application finds a virus (using a reference database with virus definitions), it informs the user.

QUESTION 4:

DRAG DROP

You work as a network administrator at Certkiller .com. Your boss Mrs. Certkiller asks you to match the malicious network attack types with the correct definition.

Options,select from these.Use each option once and only once

Brute Force

Dos

Reconnaissance

Definitions

An attacker is trying to log in to a server in a DMZ that has a trust relationship with a system on the inside of a firewall

An intruder attacks networks or systems to retrieve data, gain access, or escalate access privileges.

A program that computes a hash for every possible password is run accross a networkto attempt to log in to a server

An intruder attempts to discover and map system services, and vulnerabilites

An intruder attacks your network in a way that damages or corrupts your computer system, or denies you and others access to a network

Malicious software is inserted onto a host in order to damage a system, corrupt a system, replicate itself, or deny services

Options,place here

Place here

Place here

Place here

Place here

Place here

Place here

Answer:

Definitions

An attacker is trying to log in to a server in a DMZ that has a trust relationship with a system on the inside of a firewall

An intruder attacks networks or systems to retrieve data, gain access, or escalate access privileges.

A program that computes a hash for every possible password is run across a network to attempt to log in to a server

An intruder attempts to discover and map system services, and vulnerabilities

An intruder attacks your network in a way that damages or corrupts your computer system, or denies you and others access to a network

Malicious software is inserted onto a host in order to damage a system, corrupt a system, replicate itself, or deny services

Options, place here

Place here

Place here

Brute Force

Reconnaissance

DoS

Place here

Explanation:

1. Reconnaissance:

Reconnaissance refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of attack prior to launching an attack. This phase is also where the attacker draws on competitive intelligence to learn more about the target. The phase may also involve network scanning either external or internal without authorization.

This is a phase that allows the potential attacker to strategize his attack. This may spread over time, as the attacker waits to unearth crucial information. One aspect that gains prominence here is social engineering. A social engineer is a person who usually smooths talk's people into revealing information such as unlisted phone numbers, passwords or even sensitive information. Other reconnaissance techniques include dumpster diving. Dumpster diving is the process of looking through an organization's trash for discarded sensitive information. Building user awareness of the precautions they must take in order to protect their information assets is a critical factor in this context.

2. DOS (Denial Of Service)

Denial of Service (DoS) is an attack designed to render a computer or network incapable of providing normal services. The most common DoS attacks will target the computer's network bandwidth or connectivity. Bandwidth attacks flood the network with such a high volume of traffic, that all available network resources are consumed and legitimate user requests cannot get through. Connectivity attacks flood a computer with such a high volume of connection requests, that all available operating system resources are consumed and the computer can no longer process legitimate user requests.

3. Brute force

The brute force method is the most inclusive - though slow. Usually, it tries every possible letter and number combination in its automated exploration.

QUESTION 5:

DRAG DROP

You work as a network administrator at Certkiller .com. Your boss Mrs. Certkiller asks you to match signature type with the correct definition.

Options, Select from these

Exploit	DOS
String	Connection

Definitions

Are attack signatures based on the TCP or UDP and port number of the packets being monitored
Indicates attempts by attack tools to consume bandwidth or computing resources to disrupt normal operations
Seeks to identify network activity or upper-level protocol transactions that are unique to a specific exploit or attack tool
Looks for a fixed sequence of bytes in a single packet

options , place here

Place here
Place here
Place here
Place here

Answer:

Definitions

Are attack signatures based on the TCP or UDP and port number of the packets being monitored
Indicates attempts by attack tools to consume bandwidth or computing resources to disrupt normal operations
Seeks to identify network activity or upper-level protocol transactions that are unique to a specific exploit or attack tool
Looks for a fixed sequence of bytes in a single packet

Options place here

Connection
DoS
Exploit
String

Explanation:

1. DOS (Denial Of Service)

Denial of Service (DoS) is an attack designed to render a computer or network incapable of providing normal services. The most common DoS attacks will target the computer's network bandwidth or connectivity. Bandwidth attacks flood the network with such a

high volume of traffic, which all available network resources are consumed and legitimate user requests cannot get through. Connectivity attacks flood a computer with such a high volume of connection requests, that all available operating system resources are consumed and the computer can no longer process legitimate user requests.

2. Exploit

A defined way to breach the security of an IT system through vulnerability.

QUESTION 6:

Which of these two ways does Cisco recommend that you use to mitigate maintenance-related threats? (Choose two.)

- A. Maintain a stock of critical spares for emergency use.
- B. Ensure that all cabling is Category 6.
- C. Always follow electrostatic discharge procedures when replacing or working with internal router and switch device components.
- D. Always wear an electrostatic wrist band when handling cabling, including fiber-optic cabling.
- E. Always employ certified maintenance technicians to maintain mission-critical equipment and cabling.

Answer: A,C

QUESTION 7:

What are two security risks on 802.11 WLANs that implement WEP using a static 40-bit key with open authentication? (Choose two.)

- A. The IV is transmitted as plaintext, and an attacker can sniff the WLAN to see the IV.
- B. The challenge packet sent by the wireless AP is sent unencrypted.
- C. The response packet sent by the wireless client is sent unencrypted.
- D. WEP uses a weak-block cipher such as the Data Encryption Algorithm.
- E. One-way authentication only where the wireless client does not authenticate the wireless-access point.

Answer: A,E

Explanation:

The wireless nature and the use of radio frequency for networking makes securing WLANs more challenging than securing a wired LAN. Originally, the Wired Equivalent Privacy (WEP) protocol was developed to address this issue. It was designed to provide the same privacy that a user would have on a wired network. WEP is based on the RC4 symmetric encryption standard and uses either 64-bit or 128-bit key. However, the keys are not really this many bits because a 24-bit Initialization Vector (IV) is used to provide randomness. So the "real key" is actually 40 or 104 bits long. There are two ways to implement the key. First, the default key method shares a set of up to four default keys

with all the wireless access points (WAPs). Second is the key mapping method, which sets up a key-mapping relationship for each wireless station with another individual station. Although slightly more secure, this method is more work. Consequently, most WLANs use a single shared key on all stations, which makes it easier for a hacker to recover the key. Now, let's take a closer look at WEP and discuss the way it operates. To better understand the WEP process, you need to understand the basics of Boolean logic. Specifically, you need to understand how XORing works. XORing is just a simple binary comparison between two bytes that produce another byte as a result of the XORing process. When the two bits are compared, XORing looks to see if they are different. If they are different, the resulting output is 1. If the two bits are the same, the result is 0. If you want to learn more about Boolean logic, a good place to start is here: http://en.wikipedia.org/wiki/Boolean_algebra. All this talk about WEP might leave you wondering how exactly RC4 and XORing are used to encrypt wireless communication. To better explain those concepts, let's look at the seven steps of encrypting a message:

1.	The transmitting and receiving stations are initialized with the secret key. This secret key must be distributed using an out-of-band mechanism such as email, posting it on a website, or giving it to you on a piece of paper the way many hotels do.
2.	The transmitting station produces a seed, which is obtained by appending the 40-bit secret key to the 24-bit Initialization Vector (IV), for input into a Pseudo Random Number Generator (PRNG).
3.	The transmitting station inputs the seed to the WEP PRNG to generate a key stream of random bytes.
4.	The key stream is XORd with plaintext to obtain the cipher text.
5.	The transmitting station appends the cipher text to the IV and sets a bit indicates that it is a WEP-encrypted packet. This completes WEP encapsulation, and the results are transmitted as a frame of data. WEP only encrypts the data. The header and trailer are sent in clear text.
6.	The receiving station checks to see if the encrypted bit of the frame it received is set. If so, the receiving station extracts the IV from the frame and appends the IV with the secret key.

- | | |
|----|--|
| 7. | The receiver generates a key stream that must match the transmitting station's key. This key stream is XORd with the cipher text to obtain the sent plaintext. |
|----|--|

QUESTION 8:**DRAG DROP**

You work as a network administrator at Certkiller .com. Your boss Mrs. Certkiller asks order the steps to mitigate a worm attack.

Steps, Select from these	Steps,place here
Contain	Place first step here
Inoculate	Place second step, if any, here
Treat	Place third step, if any, here
Quaranting	Place fourth step, if any, here

Answer:

Steps, Select from these	Steps Place, here
	Contain
	Inoculate
	Quarantine
	Treat

Explanation:

Viruses and worms are part of a larger category of malicious code or malware. Viruses and worms are programs that can cause a wide range of damage from displaying messages to making programs work erratically or even destroying data or hard drives. Viruses accomplish their designed task by placing self-replicating code in other programs. When these programs execute, they replicate again and infect even more programs. Closely related to viruses and worms is spyware. Spyware is considered another type of malicious software. In many ways, spyware is similar to a Trojan, as most

users don't know that the program has been installed and it hides itself in an obscure location. Spyware steals information from the user and also eats up bandwidth. If that's not enough, it can also redirect your web traffic and flood you with annoying pop-ups. Many users view spyware as another type of virus.

The following are the recommended steps for worm attack mitigation:

1. Containment: Contain the spread of the worm inside your network and within your network. Compartmentalize parts of your network that have not been infected.
2. Inoculation: Start patching all systems and, if possible, scanning for vulnerable systems.
3. Quarantine
: Track down each infected machine inside your network. Disconnect, remove, or block infected machines from the network.
4. Treatment: Clean and patch each infected system. Some worms may require complete core system reinstallations to clean the system.

QUESTION 9:

Which method of mitigating packet-sniffer attacks is the most effective?

- A. implement two-factor authentication
- B. deploy a switched Ethernet network infrastructure
- C. use software and hardware to detect the use of sniffers
- D. deploy network-level cryptography using IPsec, secure services, and secure protocols

Answer: D

Explanation:

You cannot talk about VPNs without saying something about IP Security (IPSec). IPSec is a framework of open standards. It is not bound to any specific encryption or authentication algorithm keying technology. IPSec acts on the network layer, where it protects and authenticates IP packets between participating peers such as firewalls, routers, or concentrators. IPSec security provides four major functions:

- * Confidentiality The sender can encrypt the packets before transmitting them across the network. If such a communication is intercepted, it cannot be read by anybody.
- * Data integrity The receiver can verify whether the data was changed while traveling the Internet.
- * Origin authentication The receiver can authenticate the source of the packet.
- * Antireplay protection The receiver can verify that each packet is unique and is not duplicated.

QUESTION 10:

What is a reconnaissance attack?

- A. when an intruder attacks networks or systems to retrieve data, gain access, or escalate access privileges.

- B. when an intruder attempts to discover and map systems, services, and vulnerabilities
- C. when malicious software is inserted onto a host in order to damage a system, corrupt a system, replicate itself, or deny service or access to networks, systems, or services
- D. when an intruder attacks your network in a way that damages or corrupts your computer system, or denies you and other access to your networks, systems, or services
- E. when an intruder attempts to learn user IDs and passwords that can later be used in identity theft

Answer: B

Explanation:

Reconnaissance refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of attack prior to launching an attack. This phase is also where the attacker draws on competitive intelligence to learn more about the target. The phase may also involve network scanning either external or internal without authorization.

This is a phase that allows the potential attacker to strategize his attack. This may spread over time, as the attacker waits to unearth crucial information. One aspect that gains prominence here is social engineering. A social engineer is a person who usually smooths talk's people into revealing information such as unlisted phone numbers, passwords or even sensitive information. Other reconnaissance techniques include dumpster diving. Dumpster diving is the process of looking through an organization's trash for discarded sensitive information. Building user awareness of the precautions they must take in order to protect their information assets is a critical factor in this context.

QUESTION 11:

What should be the first step in migrating a network to a secure infrastructure?

- A. developing a security policy
- B. securing the perimeter
- C. implementing antivirus protection
- D. securing the DMZ

Answer: A

Explanation: The development of a security policy is the first step to a secure infrastructure, without this availability of your network will be compromised.

QUESTION 12:

What is a DoS attack?

- A. when an intruder attacks networks or systems to retrieve data, gain access, or escalate access privileges
- B. when an intruder attempts to discover and map systems, services, and vulnerabilities

- C. when malicious software is inserted onto a host in order to damage a system, corrupt a system, replicate itself, or deny services or access to networks, systems, or services
- D. When an intruder attacks your network in a way that damages or corrupts your computer system, or denies you and others access to your networks, systems, or services

Answer: D

Explanation:

Denial of Service (DoS) is an attack designed to render a computer or network incapable of providing normal services. The most common DoS attacks will target the computer's network bandwidth or connectivity. Bandwidth attacks flood the network with such a high volume of traffic, that all available network resources are consumed and legitimate user requests cannot get through. Connectivity attacks flood a computer with such a high volume of connection requests, that all available operating system resources are consumed and the computer can no longer process legitimate user requests.

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include

- * attempts to "flood" a network, thereby preventing legitimate network traffic
- * attempts to disrupt connections between two machines, thereby preventing access to a service
- * attempts to prevent a particular individual from accessing a service
- * attempts to disrupt service to a specific system or person

QUESTION 13:

Which method of mitigation packet-sniffer attacks is most cost effective?

- A. authentication
- B. switched infrastructure
- C. antisniffer tools
- D. cryptography

Answer: D

Cryptography: Rendering packet sniffers irrelevant is the most effective method for countering packet sniffers. Cryptography is even more effective than preventing or detecting packet sniffers. If a communication channel is cryptographically secure, the only data a packet sniffer detects is cipher text (a seemingly random string of bits) and not the original message.

QUESTION 14:

During which phase of an attack does the attacker attempt to identify targets?

- A. penetrate
- B. propagate
- C. persist

- D. probe
- E. paralyze

Answer: D

Explanation:

Probe phase: The attacker identifies vulnerable targets in this phase. The goal of this phase is to find computers that can be subverted. Internet Control Message Protocol (ICMP) ping scans are used to map networks, and application port scans identify operating systems and vulnerable software. Passwords can be obtained through social engineering, a dictionary attack, a brute-force attack, or network sniffing.

Incorrect:

- A - Phase 2
- B - Phase 4
- C - Phase 3
- D - Phase 5

QUESTION 15:

What is considered the main administrative vulnerability of Cisco Catalyst switches?

- A. SNMP
- B. Telnet
- C. Poor passwords
- D. Poor encryption

Answer: C

Explanation:

By default, a Cisco switch shows the passwords in plaintext for the following settings in the configuration file: the .enable. password, the username password, the console line and the virtual terminal lines.

Using the same password for both the enable secret and other settings on a switch allows for potential compromise because the password for certain settings (for example, telnet) may be in plaintext and can be collected on a network using a network analyzer.

Also, setting the same password for the .enable secret. passwords on multiple switches provides a single point of failure because one compromised switch endangers other switches.

QUESTION 16:

DRAG DROP

Click and drag the four steps to mitigating worm attacks in order from step 1 to steep 4.

Inoculate	Step 1
Contain	Step 2
Quarantine	Step 3
Treat	Step 4

Answer:

Contain
Inoculate
Quarantine
Treat

Explanation:

Worm attack mitigation requires diligence on the part of system and network administration staff. Coordination between system administration, network engineering, and security operations personnel is critical in responding effectively to a worm incident.

The following are the recommended steps for worm attack mitigation:

1. Containment: Contain the spread of the worm inside your network and within your network. Compartmentalize parts of your network that have not been infected.
2. Inoculation: Start patching all systems and, if possible, scanning for vulnerable systems.
3. Quarantine: Track down each infected machine inside your network. Disconnect, remove, or block infected machines from the network.
4. Treatment: Clean and patch each infected system. Some worms may require complete core system reinstallations to clean the system.

QUESTION 17:

Certkiller .com network administrators have just configured SSH on their target router and have now discovered that an intruder has been using this router to perform a variety of malicious attacks. What have they most likely forgotten to do and which Cisco IOS commands do they need to use to fix this problem on their target router?

A. forgot to reset the encryption keys using the crypto key zeroize rsa Cisco IOS global

configuration command

B. forgot to close port 23 and they need to issue the no transport input telnet Cisco IOS global configuration command

C. forgot to disable vty inbound Telnet sessions and they need to issue the line vty 0 4 and the no transport input telnet Cisco IOS line configuration commands

D. forgot to restrict access to the Telnet service on port 23 using ACLs and they need to issue the access-list 90 deny any log Cisco IOS global configuration command, and the line vty 0 4 and access-class 90 in Cisco IOS line configuration commands

Answer: C

Explanation:

Telnet and rlogin commands are known as unsecure commands, they transports the data packets on plain text format. If anyone can tries to capture the packets they can easily read. So SSH (Secure Shell) is the most usable Remote Login tool. Which maintains the secure communication.

Router(Config)#line vty 0 4

Router(Config-router)transport input telnet | ssh | all

May be telnet is enabled so just disable the telnet using no.

QUESTION 18:

To verify role-based CLI configurations, which Cisco IOS CLI commands do you need use to verify a view?

A. parser view view-name, then use the ? to verify the available commands

B. enable view view-name, then use the ? to verify the available commands

C. enable view, then use the parser view view-name to verify the available commands

D. show view view-name to verify the available commands

Answer: B

Explanation:

The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to CiscoIOS EXEC and configuration (Config) mode commands. Views restrict user access to CiscoIOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices.

SUMMARY STEPS1.

enable view

2.

configure terminal

3.

parser view view-name

4.
secret 5 encrypted-password
5.
commands parser-mode {include | include-exclusive | exclude} [all] [interface
interface-name | command]
6.
exit
7.
exit
8.
enable [privilege-level] [view view-name]
9.
show parser view [all]

QUESTION 19:

What two tasks should be done before configuring SSH server operations on Cisco routers? (Choose two.)

- A. Upgrade routers to run a Cisco IOS Release 12.1(1)P image.
- B. Upgrade routers to run a Cisco IOS Release 12.1(3)T image or later with the IPsec feature set.
- C. Ensure routers are configured for external ODBC authentication.
- D. Ensure routers are configured for local authentication or AAA for username and password authentication.
- E. Upgrade routers to run a Cisco IOS Release 11.1(3)T image or later with the IPsec feature set.

Answer: B,D

Explanation:

Secure Shell (SSH) is a protocol which provides a secure remote access connection to network devices. Communication between the client and server is encrypted in both SSH version 1 and SSH version 2. Implement SSH version 2 when possible because it uses a more enhanced security encryption algorithm.

SSH was introduced into these IOS platforms and images:

1. SSH Version 1.0 (SSH v1) server was introduced in some IOS platforms and images starting in Cisco IOS Software Release 12.0.5.S.
2. SSH client was introduced in some IOS platforms and images starting in Cisco IOS Software Release 12.1.3.T.
3. SSH terminal-line access (also known as reverse-Telnet) was introduced in some IOS platforms and images starting in Cisco IOS Software Release 12.2.2.T.
4. SSH Version 2.0 (SSH v2) support was introduced in some IOS platforms and images starting in Cisco IOS Software Release 12.1(19)E.

Example of SSH Configuration on Cisco Router

aaanew-model

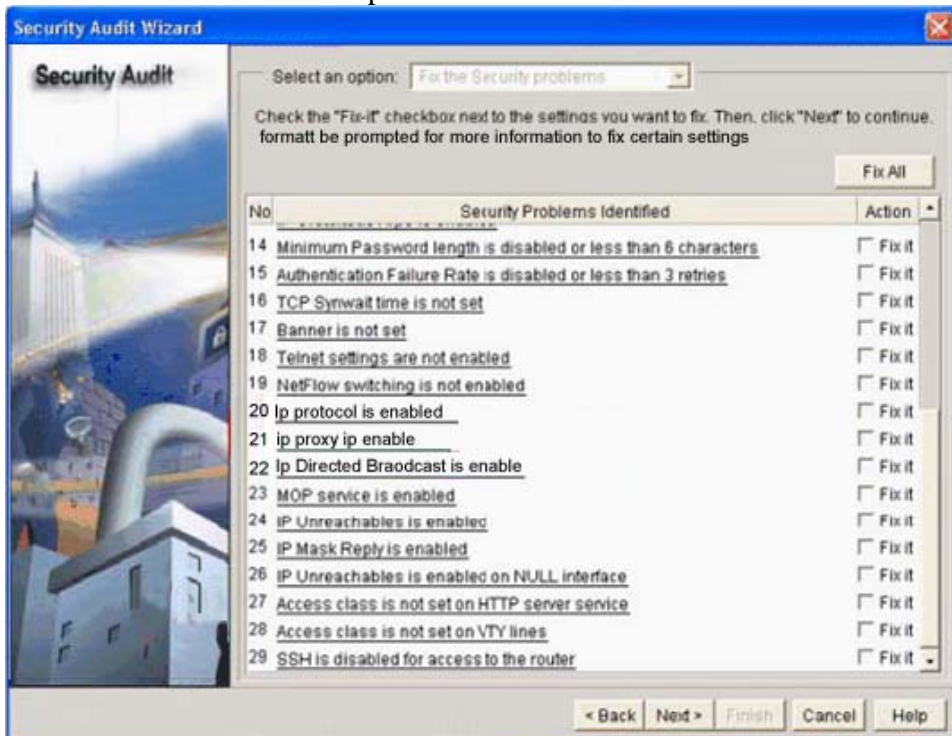
```

username cisco password 0 cisco
ip domain-name rtp.cisco.com
crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
transport input SSH

```

QUESTION 20:

In the Cisco SDM Security Audit Wizard screen shown in the figure, which Fix it action should be selected to prevent smurf denial of service attacks?



- A. IP Mask Reply is enabled
- B. IP Unreachables is enabled
- C. IP Directed Broadcast is enabled
- D. IP Redirects is enabled
- E. IP Proxy ARP is enabled
- F. Access class is not set on vty lines

Answer: C

Explanation:

Directed-Broadcast

An IP directed broadcast is a datagram sent to the broadcast address of a subnet that is not directly attached to the sending machine. The directed broadcast is routed through the

network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, which is connected directly to the target subnet, can conclusively identify a directed broadcast.

* IP directed broadcasts are used in the extremely common and popular smurf Denial of Service (DoS) attacks. In a smurf attack, the attacker sends ICMP echo requests from a falsified source address to a directed broadcast address, causing all the hosts on the target subnet to send replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger stream of replies, which can completely inundate the host whose address is being falsified.

* This service should be disabled on all interfaces when not needed to prevent smurf and DoS attacks.

* Cisco AutoSecure disables IP directed broadcasts using the no ip directed-broadcast command in interface configuration mode on each interface.

Reference:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_white_paper09186a00801dbf61.shtml

QUESTION 21:

Which two Cisco AutoSecure features are not supported in the One-Step Lockdown feature found in Cisco SDM Version 2.2a? (Choose two.)

- A. disable IP gratuitous ARPs
- B. disabling NTP
- C. set minimum password length to less than 6 characters
- D. configure antispoofing ACLs on outside interfaces
- E. disable CDP
- F. enable SSH for access to the router

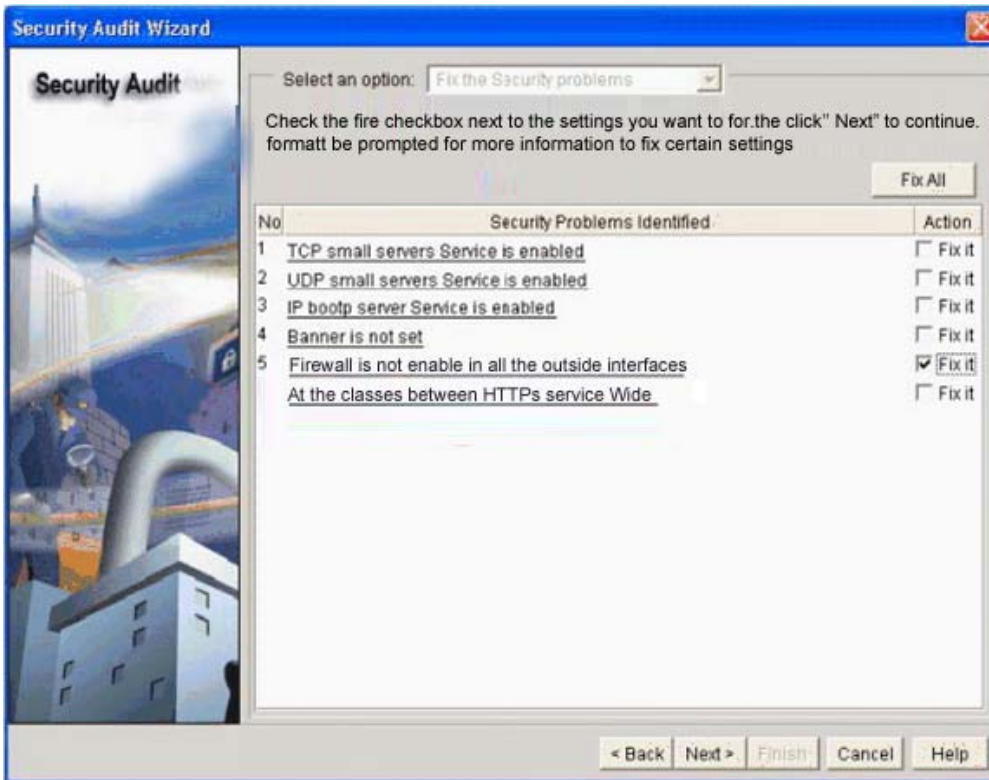
Answer: B,D

Explanation:

Cisco AutoSecure provides vital security requirements to Enterprise and Service Provider networks by incorporating a straightforward "one touch" device lockdown process. Cisco AutoSecure enables rapid implementation of security policies and procedures to simplify the security process, without having to understand all the Cisco Software IOS features and execute each of the many Command Line Interface (CLI) commands manually. This feature uses a single command that instantly configures the security posture of routers and disables non-essential system processes and services thereby eliminating potential security threats.

QUESTION 22:

Referring to the Cisco SDM Security Audit Wizard screen shown, what will happen if you check the Fix it box for Firewall is not enabled in all the outside interfaces then click the Next button?



- A. All outside access through the outside interfaces will immediately be blocked by an ACL.
- B. SDM will prompt you to configure an ACL to block access through the outside interfaces.
- C. SDM will take you to the Advanced Firewall Wizard.
- D. SDM will perform a one-step lockdown to lock down the outside interfaces.
- E. SDM will take you to the Edit Firewall Policy/ACL screen where you can configure an ACL to block access through the outside interfaces.

Answer: C

QUESTION 23:

On Cisco routers, which two methods can be used to secure privileged mode access?
(Choose two.)

- A. use the enable secret command to secure the enable password using MD5 encrypted hash
- B. use the service password-encryption command to secure the enable password using the SHA1
- C. use the privilege exec command to enable Role-Based CLI access
- D. use an external Cisco ACS server to authenticate privilege mode access
- E. use an external AAA server to encrypt and decrypt the enable password

Answer: A,D

Explanation:

Check the Fix it boxes next to any problems that you want Cisco Router and Security Device Manager (SDM) to fix. For a description of the problem and a list of the CiscoIOS commands that will be added to your configuration, click the problem description to display a help page about that problem

QUESTION 24:

Which SDM feature(s) can be used to audit and secure a Cisco router?

- A. AutoSecure and AAA Wizards
- B. AutoSecure or SDM Express Wizards
- C. Security Audit Wizard or One-Step Lockdown
- D. AAA or SDM Express Wizard
- E. IPS Wizard

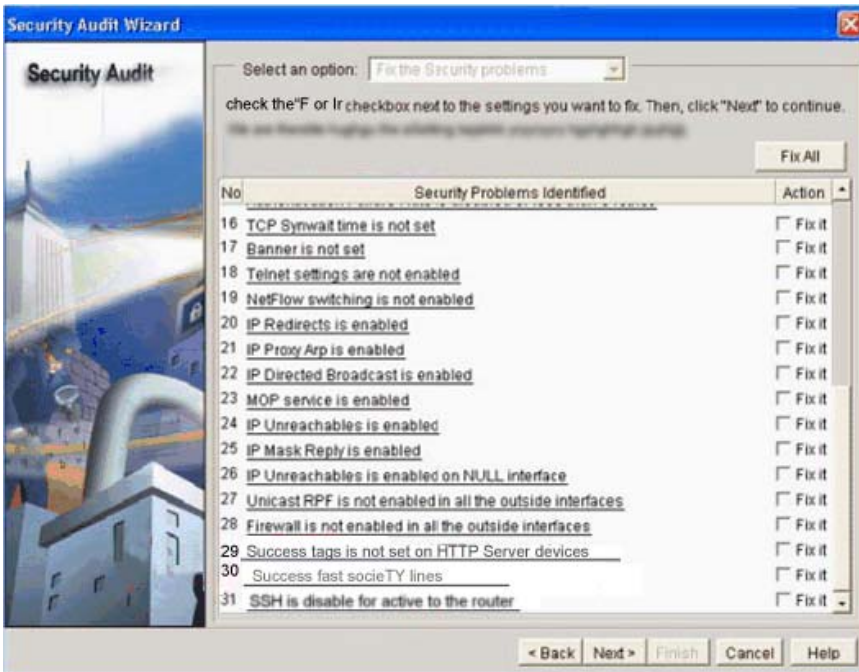
Answer: C

Explanation:

The CiscoSDMExpress windows guide you through basic configuration of the router. After you complete the basic configuration, the router is available on the LAN, has a WAN connection, and has a firewall.

QUESTION 25:

In the Cisco SDM Security Audit Wizard screen shown in the figure, which Fix it action should be selected to prevent IP spoofing attack?



- A. IP Proxy ARP is enabled
- B. Unicast RPF is not enabled in all the outside interfaces
- C. IP Mask Reply is enabled
- D. IP Directed Broadcast is enabled
- E. IP Unreachables is enabled
- F. IP Redirects is enabled

Answer: B

Explanation:

Enable IP Unicast Reverse-Path Forwarding (RPF) on the outside interface-IP Unicast RPF is a feature that causes the router to check the source address of any packet against the interface through which the packet entered the router. If the input interface is not a feasible path to the source address according to the routing table, the packet will be dropped. This source address verification is used to defeat IP spoofing.

QUESTION 26:

The figure contains a sample configuration using Cisco IOS commands. Which Cisco IOS command or setting does the configuration need to get SSH to work?

```
Certkiller2# config t
Certkiller2 (Config) # ip domain -name cisco.com
Certkiller2(config) # crypto key zeroize rsa
Certkiller2(config) # ip ssh timeout 120
Certkiller2(config) # ip ssh authentication-retries 4
Certkiller2(config) # line vty 0 4
Certkiller2(config) # no transport input telnet
Certkiller2(config) # transport input ssh
Certkiller2(Config) # end
Certkiller2 #
```

- A. add the transport input telnet ssh Cisco IOS command after the line vty 0 4 Cisco IOS command
- B. add the transport output ssh Cisco IOS command after the line vty 0 4 Cisco IOS command
- C. set the SSH timeout value using the ip ssh timeout 60 Cisco IOS command
- D. add the crypto key generate rsa general-keys modulus 1024 Cisco IOS command
- E. set the SSH retries value using the ip ssh authentication-retries 3 Cisco IOS command

Answer: D

Explanation:

Secure Shell Daemon (SSHD) is a server program designed to log into another computer over a network, execute commands in a remote machine, and move files from one machine to another machine. It provides strong authentication and secure communications over non-secure channels. SSHD is intended as a replacement for rlogin, rsh, and rcp.

Router(config)# crypto key generate rsa : Enables the SSH server for local and remote authentication on the router. The recommended minimum modulus size is 1024 bits.

QUESTION 27:

What does the secure boot-config global configuration accomplish?

- A. enables Cisco IOS image resilience
- B. backs up the Cisco IOS image from flash to a TFTP server
- C. takes a snapshot of the router running configuration and securely archives it in persistent storage
- D. backs up the router running configuration to a TFTP server
- E. stores a secured copy of the Cisco IOS image in its persistent storage

Answer: C

Explanation:

secure boot-config : Stores a secure copy of the primary bootset in persistent storage.

QUESTION 28:

How can you recover a Cisco IOS image from a router whose password you have lost and on which the no service password-recovery Cisco IOS command has been configured?

- A. You cannot recover the router.
- B. Use the service password-recovery Cisco IOS command in ROMMON.
- C. Obtain a new Cisco IOS image on a FLASH SIMM or on a PCMCIA card.
- D. Use the service password Cisco IOS recovery command.
- E. Use the tftpdnld Cisco IOS command in ROMMON to use the TFTP facility to copy a new image to the router Flash memory.

Answer: C

Explanation:

The Cisco IOS software provides a password recovery procedure that relies upon gaining access to ROMMON mode using the Break key during system startup. In ROMMON mode, the router software can be reloaded at which time prompting a new system configuration that includes a new password.

The current password recovery procedure enables anyone with console access, the ability to access the router and its network. The No Service Password-Recovery feature prevents the completion of the Break key sequence and the entering of ROMMON mode during system startups and reloads.

The No Service Password-Recovery feature is a security enhancement that prevents anyone with console access from accessing the router configuration and clearing the password. It also prevents anyone from changing the configuration register values and accessing NVRAM.

QUESTION 29:

Referring to the partial router configuration shown, which can represent the highest security risk?

```
no aaa new-model
enable secret 5 $nk:fx$nTsR3eEzv5E9aBODvXFD80
username admin secret 5 $1$VQFJ$2gXN6FHeyXl216tFk5LWMd
line con 0
login local
line aux 0
login local
...
```

- A. AAA login authentication is not enabled for console access
- B. SSH is not enabled for console access
- C. using the default exec-timeout, which is too long

- D. using the local router database for console login authentication
- E. not using the Cisco proprietary cipher to protect the user password

Answer: C

Explanation:

You can also control access to the router by configuring activity timeouts. You can use the exec-timeout command to accomplish this task. Here is an example of the configuration:

Example:

```
line console 0
exec-timeout 5 0
end
```

QUESTION 30:

Which command is used to encrypt passwords in the router configuration file?

- A. service password-encryption
- B. password-encryption
- C. enable password encryption
- D. encrypt password

Answer: A

Explanation:

With the exception of the enable secret password, all Cisco router passwords are, by default, stored in clear text form within the router configuration. View these passwords with the show running-config command. Sniffers can also see these passwords if your Trivial File Transfer Protocol (TFTP) server configuration files traverse an unsecured intranet or Internet connection. If an intruder gains access to the TFTP server where the router configuration files are stored, the intruder will be able to obtain these passwords. A proprietary Cisco algorithm based on a Vigenere cipher (indicated by the number 7 when viewing the configuration) allows the service password-encryption command to encrypt all passwords (except the previously encrypted enable secret password) in the router configuration file. This method is not as safe as MD5, which is used with the enable secret command, but prevents casual discovery of the router line-level passwords.

QUESTION 31:

Which command sets the minimum length of all Cisco IOS passwords?

- A. password min-length length
- B. min-length security length
- C. enable secret min-length
- D. security passwords min-length length

Answer: D

Explanation:

security passwords min-length

IMPORTANT:

It has no effect on older passwords until you reboot the router.

(This is an important item for you to note when you configure your router passwords, and it is the reason why it is a good idea to set the minimum password length first.)

QUESTION 32:

With the security authentication failure rate 5 log command, which two of these happen if the number of failed login attempts reaches 5? (Choose two.)

- A. The router console exec-timeout will be set to 15 seconds.
- B. All further unsecured access to the router is disabled except for secured access like SSH.
- C. The TOOMANY_AUTHFAILS event message will be sent by the router to the configured syslog server.
- D. All further login to the router will be disabled until the router reloads.
- E. The router console exec-timeout will be set to 0 seconds (disabled).
- F. A 15-second delay timer starts.

Answer: C,F

Explanation:

The security authentication failure rate command provides enhanced security access to the router by generating syslog messages after the number of unsuccessful login attempts exceeds the configured threshold rate. This command ensures that there are not any continuous failures to access the router.

The following example shows how to configure your router to generate a syslog message after eight failed login attempts:

security authentication failure rate 8 log

QUESTION 33:

Why is TACACS+ the preferred AAA protocol to use with Cisco device authentication?

- A. TACACS+ encryption algorithm is more recent than other AAA protocols
- B. TACACS+ has a more robust programming interface than other AAA protocols
- C. TACACS+ was initially developed as open-source software
- D. TACACS+ provides true AAA functional separation and encrypts the entire body of the packet
- E. TACACS+ maintains authentication information in the local database of each Cisco IOS router

F. TACACS+ combines authentication and authorization to provide more robust functionalities

Answer: D

Explanation:

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your network access server are available.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service-authentication, authorization, and accounting-independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The goal of TACACS+ is to provide a methodology for managing multiple network access points from a single management service. The Cisco family of access servers and routers and the CiscoIOS user interface (for both routers and access servers) can be network access servers.

Network access points enable traditional "dumb" terminals, terminal emulators, workstations, personal computers (PCs), and routers in conjunction with suitable adapters (for example, modems or ISDN adapters) to communicate using protocols such as Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), Compressed SLIP (CSLIP), or AppleTalk Remote Access (ARA) protocol. In other words, a network access server provides connections to a single user, to a network or subnetwork, and to interconnected networks. The entities connected to the network through a network access server are called network access clients; for example, a PC running PPP over a voice-grade circuit is a network access client. TACACS+, administered through the AAA security services, can provide the following services:

Authentication-Provides complete control of authentication through login and password dialog, challenge and response, messaging support.

The authentication facility provides the ability to conduct an arbitrary dialog with the user (forexample, after a login and password are provided, to challenge a user with a number of questions, like home address, mother's maiden name, service type, and social security number). In addition, the TACACS+ authentication service supports sending messages to user screens. For example, a message could notify users that their passwords must be changed because of the company's password aging policy.

Authorization-Provides fine-grained control over user capabilities for the duration of the user's session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on what commands a user may execute with the TACACS+ authorization feature.

Accounting-Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track user activity for a security audit or to provide information for user billing. Accounting records include user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the network access server and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between a network access server and a TACACS+ daemon are encrypted.

You need a system running TACACS+ daemon software to use the TACACS+ functionality on your network access server.

Cisco makes the TACACS+ protocol specification available as a draft RFC for those customers interested in developing their own TACACS+ software.

QUESTION 34:

Using 802.1x authentication on a WLAN offers which advantage?

- A. enforces a set of the policy statements that regulate which resource to protect and which activities are forbidden
- B. allows inbound and outbound packet filter rules to be established at the interface level of a device
- C. limits access to network resources based on user login identity; especially suited for large mobile user populations
- D. enforces security policy compliance on all devices seeking to access network computing resources

Answer: C

Explanation:

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before it makes available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

QUESTION 35:

Which three ways can AAA services be implemented for Cisco routers? (Choose three.)

- A. self-contained AAA services in the router itself

- B. Cisco Secure ACS Network Module
- C. Cisco Secure ACS Solution Engine
- D. Cisco Security Manager AAA Service Module
- E. Cisco Secure ACS for Windows Servers
- F. Cisco Security Manager ACS Service Module

Answer: A,C,E

Explanation:

Authentication, authorization, and accounting (AAA) is a way to control who is allowed to access your network (authenticate), what they can do while they are there (authorize), and to audit what actions they performed while accessing the network (accounting).

AAA can be used in Internet Protocol Security (IPSec) to provide preshared keys during the Internet Security Association and Key Management Protocol (ISAKMP) process or to provide per-user authentication, known as XAUTH, during ISAKMP. AAA can be used to provide a mechanism for authorizing commands that administrators enter at the command line of a Cisco device. This is called command-line authorization. AAA is also seen in a Virtual Private Dial-Up Networking (VPDN) tunnel set up between two routers.

QUESTION 36:

Which authentication method is based on the 802.1x authentication framework, and mitigates several of the weaknesses by using dynamic WEP and sophisticated key management on a peer-packet basis?

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

Answer: C

Explanation:

Cisco LEAP is an 802.1X authentication type for wireless LANs (WLANs) that supports strong mutual authentication between the client and a RADIUS server using a logon password as the shared secret. It provides dynamic per-user, per-session encryption keys

QUESTION 37:

Which two protocols does Cisco Secure ACS use for AAA services? (Choose two.)

- A. TACACS+
- B. Telnet
- C. SSH
- D. RADIUS
- E. SSL

F. SMP

Answer: A, D

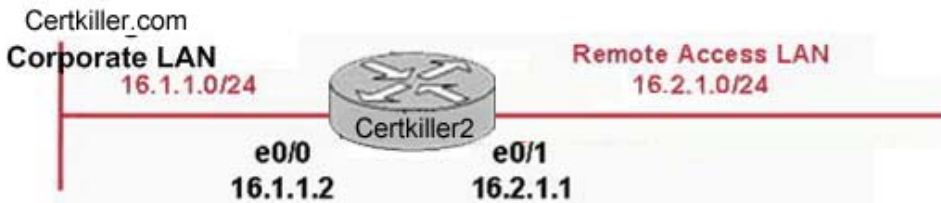
Explanation:

Cisco Secure ACS uses two distinct protocols for AAA services:

1. Remote Authentication Dial-In User Service (RADIUS) and
2. Terminal Access Controller Access Control System (TACACS+)

QUESTION 38:

Referring to the network diagram shown, Remote Access LAN users need access to the Corporate LAN. Which three Cisco IOS configuration commands will prevent users on the Remote LAN from spoofing their source IP address as Corporate LAN user? (Choose three.)



- A. access-list 1 deny 16.1.1.0 0.0.0.255
access-list 1 permit any
- B. access-list 2 deny 16.2.1.0 0.0.0.255
access-list 2 permit any
- C. int e0/0
- D. int e0/1
- E. ip access-group 1 in
- F. ip access-group 2 out

Answer: A,D,E

Explanation:

Explanation: We don't want to see any 16.1.1.0/24 traffic originating from (i.e. being spoofed from) the Remote Access LAN 16.2.1.0/24. Therefore, we would choose access-list 1 and apply it inbound on interface e0/1.

Not F: It is clear that option F could not be the answer because you would never enter "ip access-group 2 out" when you just completed creating "access-list 1 ...". You shouldn't be applying an ACL that doesn't exist (ACL 2) to any interface. In addition, standard access lists (numbered 1 to 99) can only define the SOURCE IP of the traffic. Therefore, it must be applied inbound on the e0/1 interface to have any affect on traffic sourced from 16.1.1.0/24 network (which is why we are trying to block).

QUESTION 39:

Which method does a Cisco router use for protocol type IP packet filtering?

- A. inspection rules
- B. standard ACLs
- C. security policies
- D. extended ACLs

Answer: D

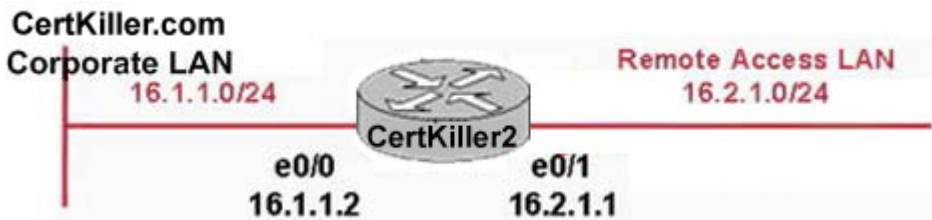
Explanation:

There are many reasons to configure access lists--for example, you can use access lists to restrict contents of routing updates, or to provide traffic flow control. But one of the most important reasons to configure access lists is to provide security for your network.

Standard ACL can filter the packets based on the Source Address only but Extended ACL can filter based on Source Address, Destination Address, Type of Protocol, Port Number etc. So Extended ACL is mostly used to ACL type to filter packets.

QUESTION 40:

Referring to the network diagram shown, which ACL entry will block any Telnet Client traffic from the Corporate LAN to any Telnet Servers on the Remote Access LAN?



- A. access-list 190 deny tcp any eq 23 16.2.1.0 0.0.0.255
- B. access-list 190 deny tcp 16.1.1.0 0.0.0.255 eq 23 16.2.1.0 0.0.0.255 eq 23
- C. access-list 190 deny tcp any 16.1.1.0 0.0.0.255 eq 23
- D. access-list 190 deny tcp any 16.2.1.0 0.0.0.255 eq 23
- E. access-list 190 deny tcp 16.2.1.0 0.0.0.255 eq 23 16.1.1.0 0.0.0.255 eq 23

Answer: D

Explanation:

There are many reasons to configure access lists--for example, you can use access lists to restrict contents of routing updates, or to provide traffic flow control. But one of the most important reasons to configure access lists is to provide security for your network.

Standard ACL can filter the packets based on the Source Address only but Extended ACL can filter based on Source Address, Destination Address, Type of Protocol, Port Number etc. So Extended ACL is mostly used to ACL type to filter packets.

Syntax of Extended ACL is:

Access-list <ACL Number> permit or deny <protocol> <Source Address> <Destination

Address> eq port number

According to questions, block the telnet connection from any source so used the any wildcard. Telnet is TCP based service and is used 23 port number.

QUESTION 41:

At which location in an access control list is it recommended that you place the more specific entries?

- A. in the middle of the access control list?
- B. higher in the access control list
- C. lower in the access control list
- D. at the bottom of the access control list

Answer: B

Explanation:

Place more specific access list statements higher in the access list. Ensure statements at the top of the access list do not negate any statements found lower in the list.

For example; blocking all UDP traffic at the top of the list negates the blocking of SNMP packets lower in the list.

Care must be taken that statements at the top of the access list do not negate any statements found lower in the list.

QUESTION 42:

To which router platform can Turbo ACLs be applied?

- A. Cisco 800 Router
- B. Cisco 2600 series router
- C. Cisco 3500
- D. Cisco 7200 Router

Answer: D

Explanation:

The Turbo ACL feature, supported by Cisco 7200 Series, 7500 Series and 12000 Series routers, processes access lists into lookup tables. Packet headers are used to access these tables in a small, fixed number of lookups, independent of the existing number of ACL entries.

The benefits of the Turbo ACL feature are:

1. For ACLs larger than 3 entries, the CPU load required to match the packet to the predetermined packet-matching rule is lessened.

The CPU load is fixed, regardless of the size of the ACL, which allows for larger ACLs without incurring additional CPU overhead penalties.

The larger the ACL, the greater the benefit.

1. The time taken to match the packet is fixed, so that latency of the packets are smaller

(significantly in the case of large ACLs) and more importantly, the time taken to match is consistent, which allows better network stability and more accurate transit times.

QUESTION 43:

Which Cisco IOS command enables the AAA access-control commands and functions on the router, and overrides the older TACACS and extended TACACS commands?

- A. no aaa authentication login default enable
- B. aaa authentication login default local
- C. aaa new-model
- D. login authentication default
- E. no login authentication default

Answer: C

Explanation:

The aaa new-model command forces the router to override every other authentication method previously configured for the router lines.

Warning!

If an administrative Telnet or console session is lost while enabling AAA on a Cisco router, and no local AAA user authentication account and method exists, the administrator will be locked out of the router.

QUESTION 44:

Which type of access control list can secure multichannel operations that are based on upper-layer information?

- A. dynamic
- B. CBAC
- C. Reflexive
- D. Time-based

Answer: B

Explanation:

CBAC can secure multichannel operations based on upper-layer information.

CBAC examines packets as they enter or leave router interfaces, and determines which application protocols to allow. CBAC access lists are available starting in Cisco IOS Software Release 12.0T as part of the firewall feature set.

Incorrect:

Dynamic

Dynamic access lists (also known as lock and key), create specific, temporary openings in response to user authentication.

Reflexive

These access lists create dynamic entries for IP traffic on one interface of the router based upon sessions originating from a different interface of the router.

Time-based

These access lists are simply numbered or named access lists that are implemented based upon the time of day or the day of the week.

QUESTION 45:

Which three new features does SNMPv3 provide? (Choose three.)

- A. HMAC with MD5
- B. AES encryption
- C. 3DES encryption
- D. HMAC with SHA
- E. DES-56 encryption
- F. IDEA encryption

Answer: A,D,E

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.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet. Three security models are available: SNMPv1, SNMPv2c, and SNMPv3.

QUESTION 46:

What is a secure way of providing clock synchronization between network routers?

- A. sync each router acting as an NTPv2 client to the UTC via the Internet
- B. implement an NTPv3 server synchronized to the UTC via an external clock source like a radio or atomic clock, then configure the other routers as NTPv3 clients
- C. use CDPv2 and NTPv3 to pass and sync the clocking information between the adjacent routers in the network
- D. implement in-band management to sync the clock between the routers using a

peer-to-peer architecture using NTPv4 or higher

Answer: B

Explanation:

The Network Time Protocol (NTP) was first described in RFC 958 and has developed into the standard Internet time synchronization protocol. It is extremely efficient and needs no more than about one packet a minute to synchronize systems on a LAN to within 1 millisecond, and systems across WANs to within about 10 milliseconds.

Without proper time synchronization between your routers, you may not only have trouble with correlating log files, but inaccurate time may also affect your ability to perform accounting, fault analysis, network management, and even time-based AAA authentication and authorization. So good time management is a necessary part of keeping your network healthy and secure.

NTP modes differ based on how NTP allows communication between systems. NTP communication consists of time requests and control queries. Time requests provide the standard client/server relationship in which a client requests time synchronization from an NTP server. Control queries provide ways for remote systems to get configuration information and reconfigure NTP servers. Here is a short explanation of the NTP modes:

Client

An NTP client is configured to let its clock be set and synchronized by an external NTP timeserver. NTP clients can be configured to use multiple servers to set their local time and are able to give preference to the most accurate time sources. They will not, however, provide synchronization services to any other devices.

Server

An NTP server is configured to synchronize NTP clients. Servers can be configured to synchronize any client or only specific clients. NTP servers, however, will accept no synchronization information from their clients and therefore will not let clients update or affect the server's time settings.

Peer

With NTP peers, one NTP-enabled device does not have authority over the other. With the peering model, each device shares its time information with the other, and each device can also provide time synchronization to the other.

Broadcast/multicast

Broadcast/multicast mode is a special server mode with which the NTP server broadcasts its synchronization information to all clients. Broadcast mode requires that clients be on the same subnet as the server, and multicast mode requires that clients and servers have multicast access available and configured.

QUESTION 47:

Which security log messaging method is the most common message logging facility and why?

A. SNMP traps, because the router can act as an SNMP agent and forward SNMP traps to an external SNMP server

- B. buffered logging, because log messages are stored in router memory and events are cleared whenever the router is rebooted
- C. console logging, because security messages are not stored and do not take up valuable storage space on network servers
- D. syslog, because this method is capable of providing long-term log storage capabilities and supporting a central location for all router messages
- E. logging all events to the Cisco Incident Control System to correlate events and provide recommended mitigation actions

Answer: D

Explanation:

By default Cisco routers send syslog messages to their logging server with a default facility of local7. Don't set the facility in this case, but do tell the router to timestamp the messages and make the messages have the source IP address of the loopback interface.

Example:

```
service timestamps log datetime localtime
no logging console
no logging monitor
logging 192.168.1.100
```

QUESTION 48:

What is a syslog configuration oversight that makes system event logs hard to interpret and what can be done to fix this oversight?

- A. The system time does not get set on the router, making it difficult to know when events occurred. Recommend that an NTP facility be used to ensure that all the routers operate at the correct time.
- B. Third-party flash memory gets installed and doesn't provide easily understandable error or failure codes. Only Cisco-authorized memory modules should be installed in Cisco devices.
- C. The syslog message stream does not get encrypted and invalid syslog messages get sent to the syslog server. Encrypt the syslog messages.
- D. The syslog messages filter rules did not get configured on the router, resulting in too many unimportant messages. Configure syslog messages filter rules so that low-severity messages are blocked from being sent to the syslog server and are logged locally on the router.

Answer: A

Explanation:

By default Cisco routers send syslog messages to their logging server with a default facility of local7. Don't set the facility in this case, but do tell the router to timestamp the messages and make the messages have the source IP address of the loopback interface.

Log messages stores based on time and date. If there is time mismatch between syslog server and client very hard to interpret the log.

QUESTION 49:

What is the first step you need to perform on a router when configuring role-based CLI?

- A. place the router in global configuration mode
- B. create a parser view called root view
- C. enable role-based CLI globally on the router using the privilege exec level Cisco IOS command.
- D. enable the root view on the router
- E. log in to the router as the "root" user

Answer: D

Explanation:

he Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to CiscoIOS EXEC and configuration (Config) mode commands. Views restrict user access to CiscoIOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices.

When a system is in "root view," it has all of the access privileges as a user who has level 15 privileges. If the administrator wishes to configure any view to the system (such as a CLI view, a superview, or a lawful intercept view), the system must be in root view.

The difference between a user who has level 15 privileges and a root view user is that a root view user can configure a new view and add or remove commands from the view. Also, when you are in a CLI view, you have access only to the commands that have been added to that view by the root view user.

QUESTION 50:

In which version did NTP begin to support cryptographic authentication?

- A. version 5
- B. version 4
- C. version 3
- D. version 2

Answer: C

Explanation:

The Network Time Protocol (NTP) was first described in RFC 958 and has developed

into the standard Internet time synchronization protocol. It is extremely efficient and needs no more than about one packet a minute to synchronize systems on a LAN to within 1 millisecond, and systems across WANs to within about 10 milliseconds. Without proper time synchronization between your routers, you may not only have trouble with correlating log files, but inaccurate time may also affect your ability to perform accounting, fault analysis, network management, and even time-based AAA authentication and authorization. So good time management is a necessary part of keeping your network healthy and secure.

NTP modes differ based on how NTP allows communication between systems. NTP communication consists of time requests and control queries. Time requests provide the standard client/server relationship in which a client requests time synchronization from an NTP server. Control queries provide ways for remote systems to get configuration information and reconfigure NTP servers. Here is a short explanation of the NTP modes:

Client

An NTP client is configured to let its clock be set and synchronized by an external NTP timeserver. NTP clients can be configured to use multiple servers to set their local time and are able to give preference to the most accurate time sources. They will not, however, provide synchronization services to any other devices.

Server

An NTP server is configured to synchronize NTP clients. Servers can be configured to synchronize any client or only specific clients. NTP servers, however, will accept no synchronization information from their clients and therefore will not let clients update or affect the server's time settings.

Peer

With NTP peers, one NTP-enabled device does not have authority over the other. With the peering model, each device shares its time information with the other, and each device can also provide time synchronization to the other.

Broadcast/multicast

Broadcast/multicast mode is a special server mode with which the NTP server broadcasts its synchronization information to all clients. Broadcast mode requires that clients be on the same subnet as the server, and multicast mode requires that clients and servers have multicast access available and configured.

NTP Version 3 Supports cryptographic authentication.

Example:

AuthenticationFor additional security, you can configure your NTP servers and clients to use authentication. Cisco routers support only MD5 authentication for NTP. To enable a router to do NTP authentication:

1. Enable NTP authentication with the `ntp authenticate` command.
2. Define an NTP authentication key with the `ntp authentication-key` command. A unique number identifies each NTP key. This number is the first argument to the `ntp authentication-key` command.
3. Use the `ntp trusted-key` command to tell the router which keys are valid for authentication. The `ntp trusted-key` command's only argument is the number of the key defined in the previous step.

To enable authentication on RouterOne and define key number 10 as MySecretKey, type:
RouterOne#configterminalEnter configuration commands, one per line. End with

```
CNTL/Z.RouterOne(config)#ntppauthenticateRouterOne(config)#  
ntppauthentication-key 10 md5 MySecretKeyRouterOne(config)#  
ntpptrusted-key 10RouterOne(config)#^Z
```

QUESTION 51:

Which command is used to configure syslog on a Cisco router?

- A. syslog
- B. logging
- C. logging-host
- D. syslog-host

Answer: B

Explanation:

By default Cisco routers send syslog messages to their logging server with a default facility of local7. Don't set the facility in this case, but do tell the router to timestamp the messages and make the messages have the source IP address of the loopback interface.

Example:

```
service timestamps log datetime localtime  
no logging console  
no logging monitor  
logging 192.168.1.100
```

QUESTION 52:

When Cisco routers are configured for SSH, how do they act?

- A. as SSH servers
- B. as SSH clients
- C. as SSH and SSL servers
- D. as SSH and SSL clients
- E. as SSH accelerators
- F. as SsH proxies

Answer: A

Explanation:

Secure Shell (SSH) is an application and a protocol that provide a secure replacement to the Berkeley r-tools. The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools. There are currently two versions of SSH available: SSHVersion 1 and SSHVersion 2. Only SSHVersion 1 is implemented in the CiscoIOS software. The SSH Server feature enables a SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality that is similar to that of an inbound

Telnet connection. Before SSH, security was limited to Telnet security. SSH allows a strong encryption to be used with the CiscoIOS software authentication. The SSH server in Cisco IOS software will work with publicly and commercially available SSH clients

QUESTION 53:

Which management protocol is used to synchronize the clocks across a network?

- A. SNMP
- B. Syslog
- C. NTP
- D. TFTP

Answer: C

Explanation:

The Network Time Protocol (NTP) was first described in RFC 958 and has developed into the standard Internet time synchronization protocol. It is extremely efficient and needs no more than about one packet a minute to synchronize systems on a LAN to within 1 millisecond, and systems across WANs to within about 10 milliseconds. Without proper time synchronization between your routers, you may not only have trouble with correlating log files, but inaccurate time may also affect your ability to perform accounting, fault analysis, network management, and even time-based AAA authentication and authorization. So good time management is a necessary part of keeping your network healthy and secure.

QUESTION 54:

What are two ways of preventing VLAN hopping attacks? (Choose two.)

- A. Disable DTP on all the trunk ports.
- B. Enable VTP pruning on all trunk ports to limit the VLAN broadcast.
- C. Set the native VLAN on all the trunk ports to an unused VLAN.
- D. Using port security, set the maximum number of secure MAC addresses to 1 on all trunk and access ports.
- E. Disable portfast on all access ports.

Answer: A,C

Explanation:

Dynamic Trunking Protocol (DTP). If a port can become a trunk, it may also have the ability to trunk automatically, and in some cases even negotiate what type of trunking to use on the port. DTP provides this ability to negotiate the trunking method with the other device.

On an IEEE 802.1Q trunk port, all transmitted and received frames are tagged except for

those on the VLAN configured as the native VLAN for the port. Frames on the native VLAN are always transmitted untagged and are normally received untagged.

QUESTION 55:

You work as a network administrator at Certkiller .com. A mission critical server application embeds a private IP address and port number in the payload of packets that is used by the client to reply to the server. Why is implementing NAT over the Internet supporting this type of application an issue?

- A. Embedded IP addresses causes NAT to do extensive packet manipulation. This process is very time intensive and the added delay causes the connection in these types of applications to time out and fail.
- B. When the client attempts to reply to the server using the embedded private IP address instead of the public IP address mapped by NAT, the embedded private IP address will not be routable over the Internet.
- C. NAT traversal can't be used for embedded IP addresses. Mission critical applications typically use NAT transversal to ensure stable timely connections, but not when embedded IP addresses and ports are used.
- D. Using NAT makes troubleshooting difficult. You must know the IP address assigned to a device on its NIC and its translated address; it takes too long to determine the source and destination of an embedded IP address, and this delay is not appropriate for mission critical applications.

Answer: B

Explanation:

Network Address Translation (NAT) simplifies and conserves IP address usage. NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) address in the internal network into legal addresses before packets are forwarded onto another network. NAT can be configured to advertise only one address for the entire network to the outside world. This ability provides additional security, effectively hiding the entire internal network behind that one address.

QUESTION 56:

How does an application-layer firewall work?

- A. examines the data in all network packets at the application layer and maintains complete connection state and sequencing information
- B. operates at Layers 3, 4 and 5, and keeps track of the actual application communication process by using an application table
- C. determines whether the connection between two applications is valid according to configurable rules

D. allows an application on your private network that does not have a valid registered IP address to communicate with other applications through the Internet

Answer: A

Explanation:

An application layer firewall is a third-generation firewall technology that evaluates network packets for valid data at the application layer before allowing a connection. It examines the data in all network packets at the application layer and maintains complete connection state and sequencing information. In addition, an application layer firewall can validate other security items that only appear within the application layer data, such as user passwords and service requests.

Most application layer firewalls include specialized application software and proxy services. Proxy services are special-purpose programs that manage traffic through a firewall for a specific service, such as HTTP or FTP. Proxy services are specific to the protocol that they are designed to forward, and they can provide increased access control, careful detailed checks for valid data, and generate audit records about the traffic that they transfer.

QUESTION 57:

Why does PAT fail with ESP packets?

- A. because ESP is a portless protocol riding directly over IP, ESP prevents the PAT from creating IP address and port mappings
- B. because using tunnel mode, ESP includes the outer IP header in computing the ICV, thus if PAT modifies the outer IP header, the ICV will fail
- C. because ESP does not support tunnel mode
- D. because the ESP header is encrypted
- E. because ESP uses dynamic port number

Answer: A

Explanation:

PAT does not work with Encapsulating Security Payload (ESP) packets due to the lack of L4(TCP/UDP) port information in them. UDP encapsulation must be used instead to hide the ESP packet behind the UDP header so that PAT treats the ESP packet as a UDP packet and processes the ESP packet as a normal UDP packet.

QUESTION 58:

Using a stateful firewall, which information is stored in the stateful session flow table?

- A. the outbound and inbound access rules (ACL entries)
- B. the source and destination IP addresses, port numbers, TCP sequencing information,

- and additional flags for each TCP or UDP connection associated with a particular session
- C. all TCP and UDP header information only
 - D. all TCP SYN packets and the associated return ACK packets only
 - E. the inside private IP address and the translated global IP address

Answer: B

Explanation:

A stateful firewall is able to hold in memory significant attributes of each connection, from start to finish. These attributes, which are collectively known as the state of the connection, may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection. The most CPU intensive checking is performed at the time of setup of the connection. All packets after that (for that session) are processed rapidly because it is simple and fast to determine whether it belongs to an existing, pre-screened session. Once the session has ended, its entry in the state-table is discarded.

The stateful firewall depends on the famous three-way handshake of the TCP protocol. When a client initiates a new connection, it sends a packet with the SYN bit set in the packet header. All packets with the SYN bit set are considered by the firewall as NEW connections. If the service which the client has requested is available on the server, the service will reply to the SYN packet with a packet in which both the SYN and the ACK bit are set. The client will then respond with a packet in which only the ACK bit is set, and the connection will enter the ESTABLISHED state. Such a firewall will pass all outgoing packets through but will only allow incoming packets if they are part of an ESTABLISHED connection, ensuring that hackers cannot start unsolicited connections with the protected machine.

QUESTION 59:

What is a potential security weakness of traditional stateful firewall?

- A. cannot support non-TCP flows
- B. retains the state of user data packet and dynamically assigned ports in the state table
- C. cannot track the state of each connection setup to ensure that each connection follows a legitimate TCP three-way handshake
- D. cannot detect application-layer attacks

Answer: D

Explanation:

A stateful firewall is able to hold in memory significant attributes of each connection, from start to finish. These attributes, which are collectively known as the state of the connection, may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection. The most CPU intensive checking is performed at the time of setup of the connection. All packets after that (for that session) are processed rapidly because it is simple and fast to

determine whether it belongs to an existing, pre-screened session. Once the session has ended, its entry in the state-table is discarded.

The stateful firewall depends on the famous three-way handshake of the TCP protocol. When a client initiates a new connection, it sends a packet with the SYN bit set in the packet header. All packets with the SYN bit set are considered by the firewall as NEW connections. If the service which the client has requested is available on the server, the service will reply to the SYN packet with a packet in which both the SYN and the ACK bit are set. The client will then respond with a packet in which only the ACK bit is set, and the connection will enter the ESTABLISHED state. Such a firewall will pass all outgoing packets through but will only allow incoming packets if they are part of an ESTABLISHED connection, ensuring that hackers cannot start unsolicited connections with the protected machine.

The problem of traditional stateful firewall is unable to detect application-layer attacks.

QUESTION 60:

A client wants their web server on the DMZ to use a private IP address and to be reachable over the Internet with a fixed outside public IP address. Which type of technology will be effective in this scenario?

- A. PAT
- B. Dynamic NAT
- C. Cut-Through Proxy
- D. Application inspection
- E. Static NAT

Answer: E

Explanation:

Static NAT is used to map a single inside global IP address to a single inside local IP address. Usually the inside IP address is one from the RFC 1918 address space and the outside IP address is an Internet routable address. IP addresses must be assigned to interfaces on the router that will be participating in NAT. You must be in global configuration mode in order to configure NAT. The command to use is `ip nat inside source static local-ip global-ip`.

The local-ip is the IP address of the host on the inside of the network to translate, and the global-ip is the IP address this inside host will be known as to the outside world. In this example a host on the inside network needs to access the Internet. Its IP address is 10.1.2.25 and is not routable on the Internet. When the NAT border router receives a packet from 10.1.2.25 destined for the Internet, the router must be configured to translate that IP address to one that is globally routable. In this case it is 200.1.1.25 and the following command is used:

```
Router(config)#ip nat inside source static 10.1.2.25 200.1.1.25
```

QUESTION 61:

Which feature is available only in the Cisco SDM Advanced Firewall Wizard?

- A. configure a router interface connected to a WLAN
- B. create a firewall policy to block SDM access to the router from the outside interface
- C. specify the router outside interface to use for remote management access
- D. choose physical and logical interfaces connected to a WLAN
- E. configure DMZ interfaces with access and inspection rules

Answer: E

Explanation:

Cisco SDM Advanced Firewall wizard allows security administrators to easily and quickly manage ACLs and packet-inspection rules through a graphical and intuitive policy table

QUESTION 62:

Which command on the Cisco PIX Security Appliance is used to write the current running config to the Flash memory startup config?

- A. write terminal
- B. write config
- C. write memory
- D. write startup config

Answer: C

Incorrect:

- A - Shows running configuration on screen, like show running-configuration
- B - No such command
- D - No such command

QUESTION 63:

In which Cisco Catalyst Series switches can the Firewall Service Modules be installed?

- A. Catalyst 2900 and 3500 XL Series
- B. Catalyst 1900 and 2000 Series
- C. Catalyst 4200 and 4500 Series
- D. Catalyst 6500 and 7600 Series

Answer: D

Explanation:

Cisco Firewall Services Module (FWSM)-a high-speed, integrated firewall module for Cisco Catalyst 6500 switches and Cisco 7600 Series routers-provides the fastest firewall

data rates in the industry: 5-Gbps throughput, 100,000 CPS, and 1M concurrent connections. Up to four FWSMs can be installed in a single chassis, providing scalability to 20 Gbps per chassis. Based on Cisco PIX Firewall technology, the Cisco FWSM offers large enterprises and service providers unmatched security, reliability, and performance.

Reference:

<http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html>

QUESTION 64:

Which method does a Cisco firewall use for packet filtering?

- A. inspection rules
- B. ACLs
- C. Security policies
- D. VACLs

Answer: B

Explanation:

The access list is a group of statements. Each statement defines a pattern that would be found in an IP packet. As each packet comes through an interface with an associated access list, the list is scanned from top to bottom and in the exact order in which it was entered, for a pattern that matches the incoming packet. A permit or deny rule associated with the pattern determines the fate of that packet.

Cisco uses access lists as packet filters to decide which packets can access a router service or which packets can be allowed across an interface. Packets that are allowed across an interface are called permitted packets. Packets that are not allowed across an interface are called denied packets. Access lists contain one or more rules or statements that determine what data is to be permitted or denied, or both permitted or denied, across an interface.

QUESTION 65:

Which command is used to reboot the Cisco PIX Security Appliance?

- A. reboot
- B. restart
- C. boot
- D. reload

Answer: D

Explanation:

The reload command reboots the PIX Security Appliance and reloads the configuration from Flash memory. You are prompted with .Proceed with reload?. for confirmation before the reload process begins. Any response other than no causes the reboot to occur.

The noconfirm command option permits the PIX Security Appliance to reload without user confirmation. The PIX Security Appliance does not accept abbreviations to the keyword noconfirm.

QUESTION 66:

Which connections does stateful packet filtering handle?

- A. TCP and UDP
- B. Packet
- C. TCP only
- D. ICMP

Answer: A

Explanation:

Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid.

A stateful firewall may examine not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination.

QUESTION 67:

Which browser-based configuration device can be used to monitor and manage multiple Cisco PIX Security Appliance?

- A. Cisco PIX Device Manager
- B. Cisco ASA Device Manager
- C. Firewall Management Center
- D. PIX Management Center

Answer: C

Explanation:

The PDM monitors and configures a single PIX Security Appliance.

You can use the PDM to create a new configuration and to monitor and maintain current PIX Security Appliances. You can point your browser to more than one PIX Security Appliance and administer several PIX Security Appliances from a single workstation.

CiscoWorks 2000 Management Center for Firewalls (Firewall MC) is a web-based interface for configuring and managing multiple Cisco PIX Security Appliances. Firewall MC has a look and feel similar to the PDM; however, with Firewall MC, you can configure multiple firewalls instead of configuring only one at a time. Firewall MC centralizes and accelerates the deployment and management of multiple PIX Security Appliances.

QUESTION 68:

What is the default security-level definition setting for the outside interface for the Cisco PIX Security Appliance?

- A. 0
- B. 100
- C. 50
- D. 25

Answer: A

Explanation:

Security Level	Applicability
Security level 100	This is the inside interface default setting for the PIX Security Appliance and cannot be changed. Because 100 is the most trusted interface security level, your corporate network should be set up behind it so that no one else can access your network, unless they are specifically given permission, and so that every device. Devices behind this interface can have access outside the corporate network.
Security levels 1 to 99	These security levels can be assigned to the perimeter interfaces connected to the PIX Security Appliance. Security levels are assigned based on the type of access that each device needs.
Security level 0	This is the outside interface default setting for the PIX Security Appliance and cannot be changed. Because 0 is the least-trusted interface security level, you should set your most untrusted network behind this interface so that it does not have access to other interfaces unless it is specifically given permission. This interface is usually used for Internet connections.

QUESTION 69:

Which administrative access mode for the Cisco PIX Security Appliance allows you to change the current settings?

- A. unprivileged mode
- B. privileged mode
- C. configuration mode
- D. monitor mode

Answer: B

Explanation:

The PIX Security Appliance contains a command set based on Cisco IOS software, and provides these four administrative access modes:

Unprivileged mode:

This mode is available when you first access the PIX Security Appliance.

The > prompt is displayed.

This mode provides a restricted and limited view of PIX Security Appliance settings.

Privileged mode:

This mode displays the # prompt and enables you to change the current settings.

Any unprivileged command also works in privileged mode.

Configuration mode:

This mode displays the (config)# prompt and enables you to change system configurations.

All privileged, unprivileged, and configuration commands work in this mode.

Monitor mode:

This is a special mode that enables you to update the image over the network or to perform password recovery. While in the monitor mode, you can enter commands specifying the location of the TFTP server and the PIX Security Appliance software image or password recovery binary file to download.

QUESTION 70:

Which administrative access mode for the Cisco PIX Security Appliance allows you to view a restricted and limited view of current settings?

- A. unprivileged mode
- B. privileged mode
- C. configuration mode
- D. monitor mode

Answer: A

Explanation:

Unprivileged mode:

This mode is available when you first access the PIX Security Appliance.

The > prompt is displayed.

This mode provides a restricted and limited view of PIX Security Appliance settings.

Privileged mode:

This mode displays the # prompt and enables you to change the current settings.

Any unprivileged command also works in privileged mode.

Configuration mode:

This mode displays the (config)# prompt and enables you to change system configurations.

All privileged, unprivileged, and configuration commands work in this mode.

Monitor mode:

This is a special mode that enables you to update the image over the network or to perform password recovery. While in the monitor mode, you can enter commands specifying the location of the TFTP server and the PIX Security Appliance software image or password recovery binary file to download.

QUESTION 71:**DRAG DROP**

You work as a network administrator at Certkiller .com. Your boss Mrs. Certkiller asks you to match IPS alarm type with the correct definition.

Options, select from these

False negative

False positive

True negative

True positive

Definitions

When a signature is not fired when offending traffic is detected

When a signature is not fired when non-offending traffic is captured and analyzed

When a signature is correctly fired when offending traffic is detected and an alarm is generated

When an alarm fires for normal traffic or a benign action

Options, place here

Place here

Place here

Place here

Place here

Answer:

Definitions

When a signature is not fired when offending traffic is detected

When a signature is not fired when non-offending traffic is captured and analyzed

When a signature is correctly fired when offending traffic is detected and an alarm is generated

When an alarm fires for normal traffic or a benign action

Options, place here

False negative

True negative

True positive

False Positive

Explanation:

Cisco Secure IDS (formerly NetRanger) triggers an alarm when a given packet or sequence of packets matches the characteristics of known attack profiles defined in the Cisco Secure IDS signatures. A critical IDS signature design criterion is to minimize the occurrence of false positive and false negative alarms.

False positives (benign triggers) occur when the IDS reports certain benign activity as malicious. This requires human intervention to diagnose the event. A large number of false positives can significantly drain resources, and the specialized skills required to analyze them are costly and difficult to find.

False negatives occur when the IDS does not detect and report actual malicious activity. The consequence of this can be catastrophic and signatures must be continuously updated as new exploits and hacking techniques are discovered. Minimizing false negatives is given a very high priority, sometimes at the expense of higher occurrences of false positives.

Due to the nature of the signatures that IDSs use to detect malicious activity, it is almost impossible to completely eliminate false positives and negatives without severely degrading the effectiveness of the IDS or severely disrupting the computing infrastructure of an organization (such as hosts and networks). Customized tuning when an IDS is deployed minimizes false positives. Periodic re-tuning is required when the computing environment changes (for example, when new systems and applications are deployed). Cisco Secure IDS provides a flexible tuning capability that can minimize false positives during steady-state operations.

QUESTION 72:

By default, what will a router do with incoming network traffic when the Cisco IOS IPS software fails to build a SME?

- A. scan traffic using the most recently installed SME
- B. drop all packets destined for that SME
- C. print a syslog message indicating that failure of the SME build
- D. pass traffic packets destined for that SME without scanning them

Answer: D

Explanation:

Cisco IOS IPS uses signature microengines (SMEs) to load the SDF and scan signatures. Signatures contained within the SDF are handled by a variety of SMEs. The SDF typically contains signature definitions for multiple engines. The SME typically corresponds to the protocol in which the signature occurs and looks for malicious activity in that protocol.

A packet is processed by several SMEs. Each SME scans for various conditions that can lead to a signature pattern match. When an SME scans the packets, it extracts certain values, searching for patterns within the packet via the regular expression engine.

Example of Alarm Message: %IPS-5-PACKET_UNSCANNED:SERVICE.DNS
-packets passed unscanned while engine is building

It means Packets are passing through the network but are not being scanned because the specified IPS module is not functioning and the ipips fail closed command is not configured.

The message is rate limited to 1 message per 60seconds

QUESTION 73:

What is the difference between the attack-drop.sdf file and the 128MB.sdf and the 256MB.sdf files?

- A. attack-drop.sdf has fewer signatures
- B. attack-drop.sdf takes up more router memory space
- C. attack-drop.sdf signatures cannot be tuned
- D. attack-drop.sdf only contains the Atomic signatures
- E. attack-drop.sdf only contains the String signatures

Answer: A

Explanation:

Attack-drop.sdf contains about 80 signatures for routers with less than 128 MB of DRAM. 128MB.sdf and 256MB.sdf contain about 300 and 500 signatures respectively, and are used for routers with DRAM of 128 MB and 256 MB or less

QUESTION 74:

What is the primary type of intrusion prevention technology used by Cisco IPS security appliances?

- A. profile-based
- B. rule-based
- C. signature-based
- D. protocol analysis-based

Answer: C

Explanation:

Cisco IOS IPS uses signature microengines (SMEs) to load the SDF and scan signatures. Signatures contained within the SDF are handled by a variety of SMEs. The SDF typically contains signature definitions for multiple engines. The SME typically corresponds to the protocol in which the signature occurs and looks for malicious activity in that protocol.

A packet is processed by several SMEs. Each SME scans for various conditions that can lead to a signature pattern match. When an SME scans the packets, it extracts certain values, searching for patterns within the packet via the regular expression engine.

QUESTION 75:

What is a description of a promiscuous PVLAN port?

- A. It has a complete Layer 2 separation from the other ports within the same PVLAN.
- B. It can only communicate with other promiscuous ports.
- C. It can communicate with all interfaces within a PVLAN.
- D. It cannot communicate with other ports.

Answer: C

Explanation:

Private VLANs provide isolation for ports that are configured within the private VLAN structure. You can use private VLANs when hosts on the same segment do not need to communicate with each other but do need to communicate with the same router or firewall. Private VLANs provide isolation at Layer 2 of the OSI model.

Private VLANs consist of the following VLANs:

1. Primary VLAN-Receives frames from the promiscuous port and forwards it to ports in the primary, isolated, and community VLANs.
2. Isolated VLAN-All ports in this VLAN can communicate only with the promiscuous port. Isolated ports cannot communicate with other isolated ports. Isolated VLANs are secondary VLANs.
3. Community VLAN-All ports in this VLAN can communicate with each other and with the promiscuous port. Community VLANs are secondary VLANs.

QUESTION 76:

How do you enable a host or a network to remotely access the Cisco IPS/IDS sensor?

- A. Configure static routes.
- B. Configure dynamic routing.
- C. Configure allowed hosts.
- D. Configure DHCP.

Answer: C

Explanation:

Cisco IPS maintains a list of all the trusted hosts it communicates with, including blocking devices, TLS/SSL servers, and external products such as Cisco Security Agent MC. This list contains the digital certificates of the trusted systems used by IPS to establish secure connections.

As part of the Cisco Security Agent/IPS interface configuration the system running Cisco Security Agent MC needs to be added as a trusted host. In the process of adding the system the IPS retrieves the digital certificate of the Cisco Security Agent MC and displays its fingerprint, which is then presented to the administrator for approval. After the administrator approves the associated fingerprint the Cisco Security Agent MC system is added as a trusted host.

QUESTION 77:

What must be configured on a network-based Cisco IDS/IPS to allow to monitor traffic?

- A. Enable rules.
- B. Enable signatures.

- C. Disable rules.
- D. Disable signatures.

Answer: B

Explanation:

Effectively monitoring the alerts generated by your Cisco IPS devices is crucial to protecting your network from attack. The Cisco Security Monitor is the graphical tool you can use to monitor the events being generated by your various Cisco IPS devices. To allow the monitoring traffic of Cisco IDS/IPS you need to enable signatures.

QUESTION 78:

DRAG DROP

Click and drag the Cisco IDS/IPS engine categories on the left to their function on the right.

Service	Is used to perform packet inspection
Atomic	Is used to detect attempts to cause a DoS
Flood	Is used when services with layer 5, 6, and 7 require protocol analysis

Answer:

Atomic
Flood
Service

Signature Engines

Engine Category	Engine Use
Atomic	This engine category is used to perform per-packet inspection. The Atomic engines support signatures that trigger alarms based on the analysis of a single packet.
Flood	Used to detect attempts to cause a DoS
Service	Used when services with Layer 5, 6, and 7 require protocol analysis
State.String	Used for state-based and regular expression-based pattern inspection and alarming functionality for TCP streams
String	Used for regular expression-based pattern inspection and alarm functionality for multiple transport protocols including TCP, UDP, and ICMP
Sweep	Used to detect network reconnaissance
Traffic	Identifies traffic irregularities
Trojan	Used to detect BackOrifice Trojan horse traffic and Tribal Flood Network 2000 (TFN2K) Trojan or distributed denial of service (DDoS) traffic
OTHER	Used to group generic signatures so common parameters may be changed

QUESTION 79:

Which Cisco IDS/IPS feature enables the appliance to aggregate alarms?

- A. FireOnce
- B. Response actions
- C. Alarm summarization
- D. Threshold configuration

Answer: C

Explanation:

Alarm summarization

This feature enables the sensor to aggregate alarms to limit the number of times an alarm is sent when the signature is triggered.

Incorrect:

FireOnce

Sends the first alarm and then deletes the inspector.

This technique is used to limit alarm firings.

Response actions

This capability enables the sensor to take an action when the signature is triggered.

Threshold configuration

This capability enables a signature to be tuned to perform optimally in a network.

QUESTION 80:

What are three common types of user accounts on the Cisco IDS/IPS? (Choose three.)

- A. administrator
- B. guest
- C. operator
- D. viewer
- E. privileged
- F. executive

Answer: A, C, D

Explanation:

Role	Functions
Administrators	<ul style="list-style-type: none">• Add users and assign passwords• Enable and disable control of physical interfaces and interface groups• Assign physical sensing interfaces to interface groups• Modify the list of hosts allowed to connect to the sensor as configuring or viewing agents• Modify sensor address configuration• Tune signatures• Assign virtual sensor configuration to interface groups.• Manage routers
Operators	<ul style="list-style-type: none">• Modify their passwords• Tune signatures• Manage routers
Viewers	<ul style="list-style-type: none">• Modify their passwords

QUESTION 81:

What is a set of conditions that, when met, indicates that an intrusion is occurring or has occurred?

- A. rules
- B. state tables
- C. signatures
- D. master parameters

Answer: C

Explanation:

Cisco IDS and IPS use over a hundred signatures to detect patterns of misuse in network traffic to identify of the most common attacks. Simple signatures check the value of a header field.

More complex signatures may track the state of a connection or perform extensive protocol analysis on the traffic.

QUESTION 82:

Which of these is true regarding IKE Phase 2?

- A. The SAs used by IPsec are unidirectional, so a separate key exchange is required for each data flow.
- B. Either main or aggressive mode can be used to establish the SAs.
- C. Quick mode is used to establish the unidirectional IKE SA and the bidirectional IPsec SAs.
- D. XAUTH can be optionally used to reauthenticate the IPsec peers.
- E. The Diffie-Hellman protocol is used to exchange the public and private keys between the two IPsec peers.

Answer: A

Explanation:

The purpose of IKE phase 2 is to negotiate IPsec SAs to set up the IPsec tunnel. IKE phase 2 performs the following functions:

1. Negotiates IPsec SA parameters protected by an existing IKE SA
2. Establishes IPsec security associations
3. Periodically renegotiates IPsec SAs to ensure security
4. Optionally performs an additional Diffie-Hellman exchange

IKE phase 2 has one mode, called quick mode. Quick mode occurs after IKE has established the secure tunnel in phase 1. It negotiates a shared IPsec policy, derives shared secret keying material used for the IPsec security algorithms, and establishes IPsec SAs. Quick mode exchanges nonces that provide replay protection. The nonces are used to generate new shared secret key material and prevent replay attacks from generating bogus SAs.

QUESTION 83:

Why was the Diffie-Hellman key agreement protocol created?

- A. to eliminate the possibility of man-in-the-middle attacks, replacing the RSA method, which is susceptible to this type of attack
- B. a practical method for establishing a shared secret over an unprotected communications channel was needed
- C. an iterated HMAC function to generate pseudorandom data streams was needed
- D. to provide a scalable and secure mechanism for distributing, managing, and revoking encryption and identity information

Answer: B

Explanation:

The Diffie-Hellman (D-H) key agreement is a public key encryption method that provides a way for two IPsec peers to establish a shared secret key that only they know, although they are communicating over an insecure channel.

With D-H, each peer generates a public and private key pair. The private key generated

by each peer is kept secret and never shared. The public key is calculated from the private key by each peer and is exchanged over the insecure channel. Each peer combines the other's public key with its own private key and computes the same shared secret number. The shared secret number is then converted into a shared secret key. The shared secret key is never exchanged over the insecure channel.

QUESTION 84:

Which IPsec protocol is the most popular and why?

- A. AH, because it provides encryption and authentication
- B. AH, because it supports tunnel mode
- C. AH, because it works with PAT
- D. ESP, because it provides encryption and authentication
- E. ESP, because it supports tunnel mode
- F. ESP, because it works with PAT

Answer: D

Explanation:

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF).

IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices ("peers"), such as Cisco routers.

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:

1. Data Confidentiality-The IPSec sender can encrypt packets before transmitting them across a network.
2. Data Integrity-The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
3. Data Origin Authentication-The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
4. Anti-Replay-The IPSec receiver can detect and reject replayed packets.

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 85:

Which of these two functions are required for IPsec operation? (Choose two.)

- A. using SHA for encryption
- B. using PKI for shared-key authentication
- C. using IKE to negotiate the SA

- D. using AH protocols for encryption and authentication
- E. using Diffie-Hellman to establish a shared-secret key

Answer: C,E

Explanation:

Internet Key Exchange (IKE)-A hybrid protocol which implements Oakley and SKEME key exchanges inside the ISAKMP framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec security associations, and establishes IPSec keys.

- AH-AH, is the appropriate protocol when confidentiality is not required or permitted. It provides data authentication and integrity for IP packets passed between two systems. It is a means of verifying that any message passed from Router A to Router B was not modified during transit. It verifies that the data's origin was either Router A or Router B. AH does not provide data confidentiality (encryption) of packets. It does the following:

1. Ensures data integrity
2. Provides origin authentication (ensures that packets definitely came from the peer router)
3. Uses a keyed-hash mechanism
4. Does not provide confidentiality (no encryption)
5. Provides anti-replay protection

QUESTION 86:

Which IKE function is optional?

- A. authentication during SA negotiation
- B. XAUTH protocol for user authentication
- C. Quick Mode for IKE Phase 2
- D. IKE SA establishment

Answer: B

Explanation:

Authentication schemes such as Remote Authentication Dial-In User Service (RADIUS) and SecureID are commonly used for providing secure remote access. It is highly desirable to leverage these authentication mechanisms for IPSec remote access. But Internet Key Exchange (IKE) protocol does not provide a method to leverage these unidirectional authentication schemes. Extended Authentication, commonly referred to as XAUTH, was developed to leverage these legacy authentication schemes with IKE. XAUTH provides an additional level of authentication by allowing the IPSec gateway to request extended authentication from remote users, thus forcing remote users to respond with their credentials before being allowed access to the VPN. It should be noted that

XAUTH functions by first forming an IKE phase 1 SA using conventional IKE, and then by extending the IKE exchange to include additional user authentication exchanges.

QUESTION 87:

Remote users are having a problem using their Cisco VPN Client software to connect to a Cisco Easy VPN Server. Which of the following could be causing the problem?

- A. The Cisco Easy VPN Server is configured with more than one ISAKMP policy.
- B. The Cisco Easy VPN Server is configured with only one ISAKMP policy specifying Diffie-Hellman Group 5.
- C. The Cisco Easy VPN Server transform set configuration includes both encryption and authentication.
- D. The Cisco Easy VPN Server is configured with more than one transform set using ESP.
- E. The Cisco VPN Client software does not support ESP, so the Cisco VPN Server transform set needs to use AH instead.

Answer: B

Explanation:

The Unity Protocol supports only Internet Security Association Key Management Protocol (ISAKMP) policies that use group 2 (1024-bit Diffie-Hellman) Internet Key Exchange (IKE) negotiation, so the Easy VPN server being used with the Cisco Easy VPN Remote feature must be configured for a group2 ISAKMP policy. The Easy VPN server cannot be configured for ISAKMP group 1 or group 5 when being used with a CiscoEasy VPN client.

QUESTION 88:

Which three components are used in the PKI environment? (Choose three.)

- A. a CA to grant and maintain private shared keys
- B. a CA to grant and maintain digital certificates
- C. an RA to offload the CA by processing enrollment requests
- D. a distribution mechanism for public key revocation lists
- E. a distribution mechanism for certification revocation lists
- F. an eToken key on the router to store the CA private key

Answer: B,C,E

Explanation:

Certificate authority. An entity in a network that issues and manages security credentials and public keys (in the form of X509v3 certificates) for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify

information provided by the requestor of a digital certificate. If the RA verifies the information of the requestor, the CA can then issue a certificate. Certificates generally include the public key of the owner, the expiration date of the certificate, the name of the owner, and other information about the public key owner.

QUESTION 89:

Which two encryption algorithms are commonly used to encrypt the contents of a message? (Choose two.)

- A. DH
- B. AES
- C. SHA1
- D. 3DES
- E. PKI

Answer: B,D

Explanation:

Some of the standard algorithms are as follows:

1. Data Encryption Standard (DES) algorithm-Used to encrypt and decrypt packet data.
 2. 3DES algorithm-Effectively doubles encryption strength over 56-bit DES.
 3. Advanced Encryption Standard (AES)-A newer cipher algorithm designed to replace DES. Has a variable key length between 128 and 256 bits. Cisco is the first industry vendor to implement AES on all its VPN-capable platforms.
 4. Message Digest 5 (MD5) algorithm-Used to authenticate packet data.
 5. Secure Hash Algorithm 1 (SHA-1)-Used to authenticate packet data.
 6. Diffie-Hellman(DH)-A public-key cryptography protocol that allows two parties to establish a shared secret key used by encryption and hash algorithms (for example, DES and MD5) over an insecure communications channel.
-

QUESTION 90:

Which of these can be used to authenticate the IPsec peers during IKE Phase 1?

- A. Diffie-Hellman Nounce
- B. Pre-Shared Key
- C. XAUTH
- D. ICV
- E. ACS
- F. AH

Answer: B

Explanation:

With preshared keys, the same preshared key is configured on each IPSec peer. At each end, the preshared key is combined with other information to form the authentication key. Starting at the local end, the authentication key and the identity information (device-specific information) are sent through a hash algorithm to form hash_I. The local Internet Key Exchange (IKE) peer provides one-way authentication by sending hash_I to the remote peer. If the remote peer can independently create the same hash, the local peer is authenticated.

The authentication process continues in the opposite direction. The remote peer combines its identity information with the preshared-based authentication key and sends them through a hash algorithm to form hash_R. hash_R is sent to the local peer. If the local peer can independently create the same hash from its stored information and preshared-based authentication key, the remote peer is authenticated. Each peer must authenticate its opposite peer before the tunnel is considered secure. Preshared keys are easy to configure manually but do not scale well. Each IPSec peer must be configured with the preshared key of every other peer with which it communicates.

QUESTION 91:

What does the MD5 algorithm do?

- A. takes a message less than 2^{64} bits as input and produces a 160-bit message digest
- B. creates a variable-length message and produces a 168-bit message digest
- C. takes a variable-length message and produces a 128-bit message digest
- D. takes a fixed-length message and produces a 128-bit message digest

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" digest of the input.
- * 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.

QUESTION 92:

Router A can not establish a standard IPsec VPN tunnel with router B. An analysis reveals one or more NAT points in the delivery path of each IPsec packet being sent to router B. What is the problem and what is the solution?

- A. IPsec encrypts Layer 4 port information and IKE NAT transversal needs to be configured on this network.
- B. The port number information in the ESP header is encrypted. Use ESP tunnel mode instead of transport mode.
- C. Router A needs to decrypt the Layer 4 port information. Configure ESP protocol on router A.

D. NAT changes the source IP address of the packets so IPSEC ESP integrity check will fail. Use PAT instead of NAT.

Answer: A

QUESTION 93:

Which of these is the strongest symmetrical encryption algorithm?

- A. DES
- B. 3DES
- C. AES
- D. RSA
- E. SHA
- F. Diffie-Hellman

Answer: C

Explanation:

Advanced Encryption Standard (AES)

-A newer cipher algorithm designed to replace DES. Has a variable key length between 128 and 256 bits. Cisco is the first industry vendor to implement AES on all its VPN-capable platforms.

QUESTION 94:

Cisco routers, such as the ISRs, are best suited for deploying which type of IPsec VPN?

- A. remote-access VPN
- B. overlay VPN
- C. WAN-to-WAN VPN
- D. site-to-site VPN
- E. SSL VPN

Answer: D

Explanation:

Site-to-site VPNs can be deployed using a wide variety of Cisco VPN Routers. Cisco VPN routers provide scalability through optional encryption acceleration. The Cisco VPN router portfolio provides solutions for small office and home office (SOHO) access through central site VPN aggregation. SOHO solutions include platforms for fast-emerging cable and DSL access technologies.

Incorrect:

A - This VPN solution connects telecommuters and mobile users securely and

cost-effectively to corporate network resources from anywhere in the world over any access technology.

QUESTION 95:

Which encryption method uses a 56-bit to ensure high-performance encryption?

- A. 3DES
- B. AES
- C. RSA
- D. DES

Answer: D

Incorrect:

A - 3DES 3*56bits

B - Advanced Encryption Standard

C - It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography.

QUESTION 96:

Which protocol does the Cisco Web VPN solution use?

- A. SSH
- B. Telnet
- C. SSL
- D. IPSec
- E. XML

Answer: C

Explanation:

Secure Sockets Layer (SSL)-based VPN is an emerging technology that provides remote-access connectivity from almost any Internet-enabled location using a Web browser and its native SSL encryption. SSL VPN provides the flexibility to support secure access for all users, regardless of the endpoint host from which they are establishing the connection. If application access requirements are modest, SSL VPN does not require a VPN client to be preinstalled on the endpoint host.

QUESTION 97:

What are the four critical services of IPSec functions? (Choose four.)

- A. replay protection
- B. confidentiality
- C. data integrity

- D. data mining
- E. origin authentication
- F. anti-replay protection

Answer: B, C, E, F

Explanation:

Function	Benefit
Confidentiality	Encryption prevents eavesdropping and reading of intercepted data.
Data integrity	Receiver can verify data was transmitted unchanged or altered.
Origin authentication	Receiver can guarantee and certify the data source.
Anti-replay protection	Each packet is verified as unique. Late and duplicate packets are dropped.

QUESTION 98:

With IPSec operation, what happens when a basic set of security services are negotiated and agreed upon between peers?

- A. data transfer
- B. IKE Phase 1
- C. IPSec tunnel termination
- D. IKE Phase 2

Answer: B

Explanation:

IPSec operation can be broken down into five simple steps.

Step 1

Interesting traffic: Traffic is deemed interesting when the VPN device recognizes that the traffic you want to send needs to be protected.

Step 2

IKE phase 1: A basic set of security services are negotiated and agreed upon between peers. This basic set of security services protects all subsequent communications between the peers.

Step 3

IKE phase 2: IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers. These security parameters are used to protect data and messages exchanged between endpoints. The final result of IKE phase 1 and phase 2 is a secure communications channel between peers.

Step 4

Data transfer: Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.

Step 5

IPSec tunnel termination: IPSec SAs terminate through deletion or by timing out.

QUESTION 99:

DRAG DROP

Click and drag the VPN solution on the left to its definition on the right.

Intranet VPN	This VPN solution connects telecommuters and mobile users securely and cost-effectively to corporate network resources from anywhere in the world over any access technology.
Extranet VPN	This VPN solution links corporate headquarters to remote offices over a shared, prioritized network, and offers an extremely cost-effective alternative to dedicated WANs.
Remote-access VPN	This VPN solution links network resources with third-party vendors and business partners, extending elements of the corporate network beyond the organization.

Answer:

Remote-access VPN
Intranet VPN
Extranet VPN

QUESTION 100:

The DH exchange used to generate the shared secret keys occurs in which IKE and exchange phase?

- A. first exchange
- B. second exchange
- C. third exchange
- D. fourth exchange

Answer: B

Explanation:

Main mode has three two-way exchanges between the initiator and receiver:

First exchange:

The algorithms and hashes used to secure the IKE communications are negotiated.

Second exchange:

A DH exchange generates shared secret keys.

Third exchange:

This exchange verifies the identity of the other side to make sure they are communicating with the devices with which they think they are communicating.

QUESTION 101:

Which type of VPN is considered an extension of a classic WAN?

- A. remote-access VPN
- B. site-to-site VPN
- C. GRE VPN
- D. L2TP VPN

Answer: B

Explanation:

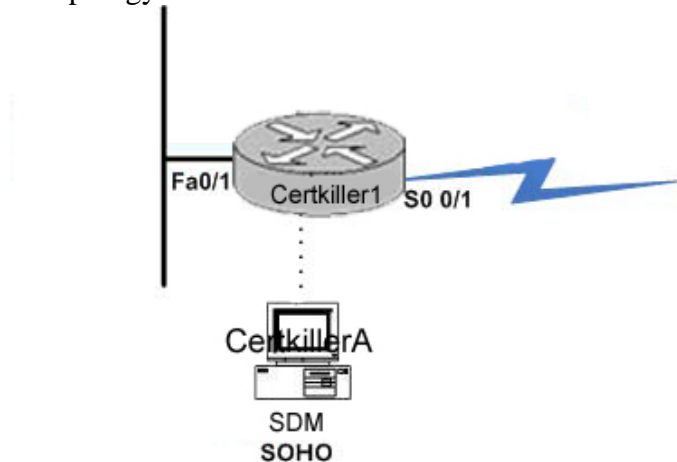
VPN site-to-site can be used to connect corporate sites. With Internet access, leased lines and frame relay lines can be replaced with site-to-site VPN for network connection.

VPN can support company intranets and business partner extranets.

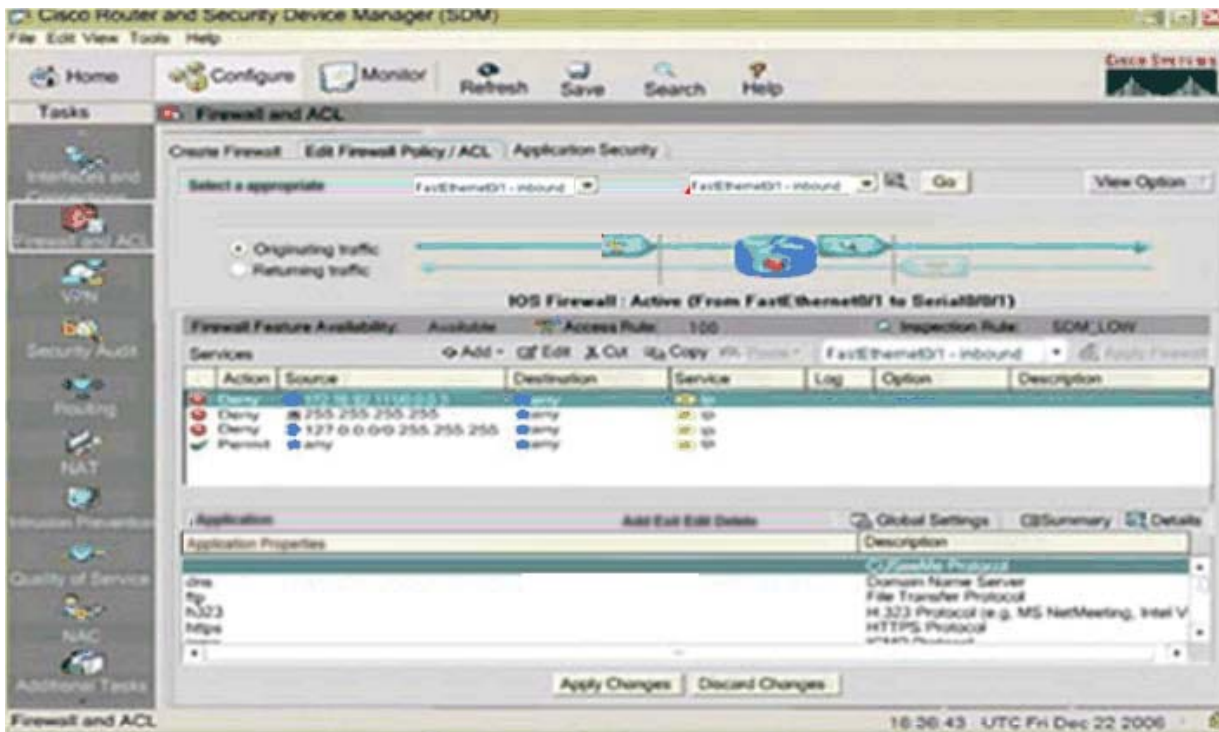
Site-to-site VPN is an extension of the classic WAN.

Certkiller .com, Scenario

Network topology exhibit:



Configuration exhibit



You work as a network technician at Certkiller .com. Certkiller .com is a large company with offices across North America. You work at the Certkiller .com Edmonton office. Your boss at Certkiller , Mrs. Certkiller, has asked you to document the current Cisco IOS Firewall configuration on the Certkiller 2 router which is being deployed at the Small Office Home Office at the local Boston office. You must the SDM output and the ACL Tasks configure Tab exhibits to answer the four questions belonging to this scenario.

Certkiller .com Questions (4 Questions)

QUESTION 102:

Which traffic will be permitted inbound to the untrusted interface?

- A. Any ICMP packets from any non-private IP address source destined to the 172.16.92.111/30 subnet
- B. Any IP packets sourced from the 10.31.17.0/24 subnet to the 172.16.92.111/30 subnet.
- C. Any IP packets sourced from the 10.31.17.0/24 subnet any destinations
- D. ICMP echo-requests from any source destined to 172.16.92.111.
- E. ICMP echo-reply from any source destined to 172.16.92.111.

Answer: E

QUESTION 103:

Which one of these will be dynamically altered by the IOS Firewall to allow the returning traffic through the firewall?

- A. Both ACL 100 and ACL 101
- B. ACL 100 only
- C. ACL 101 only
- D. SOM_LOW inspection Rule - Inbound
- E. SOM_LOW inspection Rule - Outbound

Answer: D

Explanation:

SOM_LOW inspection Rule - Inbound

QUESTION 104:

Which three of these statements correctly describe how the Cisco IOS Firewall is configured? Select three.

- A. ACL 101 is used for performing stateful inspection of the traffic originated from the trusted interface.
- B. Fa0/1 is the untrusted interface and S0 0/1 is the trusted interface.
- C. The untrusted subnet is 172.16.92.111/30
- D. The inspect Rule named SDM_LOW is used for performing stateful inspection of the traffic originated from the trusted interface
- E. The trusted subnet is 10.31.17.0/24
- F. The inspect Rule named SDM_LOW is applied to interface S0 0/1 in the inbound direction.

Answer: D, E, F

QUESTION 105:

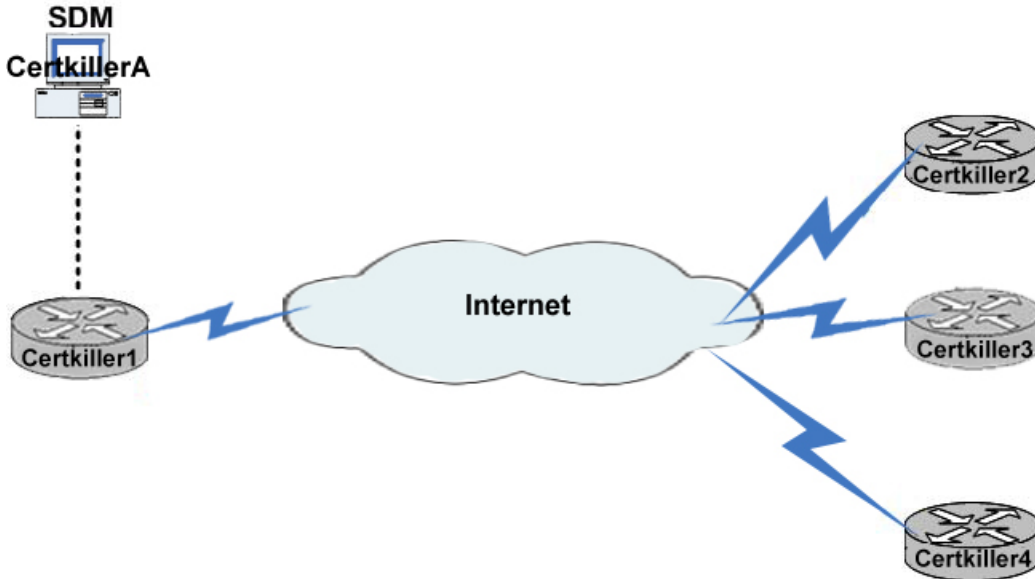
Which traffic will be permitted inbound on the trusted interface?

- A. Any IP Packets
- B. ICMP echo-reply from any sourced to 172.16.10.1
- C. Any IP packets sourced from the 127.0.0.0/8 network to any destinations.
- D. Any IP packets sourced from the 172.16.92.111/30 subnet to any destinations
- E. Any IP packets sourced from the 10.31.17.0/24 subnet to any destinations

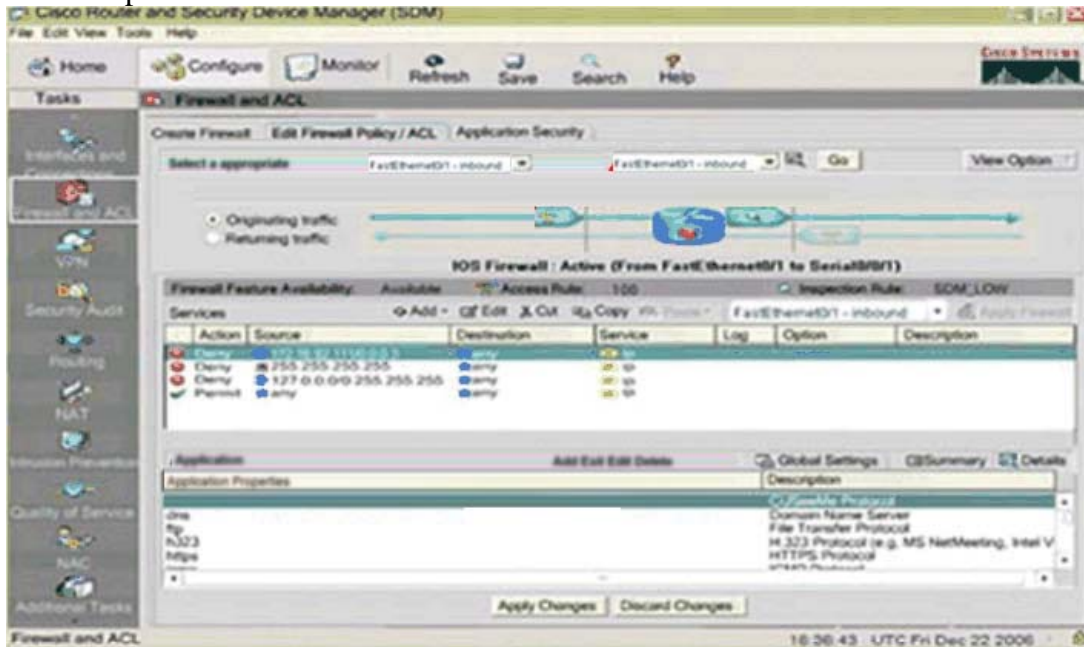
Answer: B

Certkiller .com Madrid, Scenario

Network topology exhibit:



SDM output exhibit



You work as a network technician at Certkiller .com. Certkiller .com is a large company with offices across Europe. You work at the Certkiller .com Spain branch. The Madrid office, with the Certkiller 1 router, is the main office. The Spanish branch of Certkiller .com also has three remote offices denoted Certkiller 2, Certkiller 3, and Certkiller 4 in the network topology exhibit. IPSec VPN is used for the connections between the remote branch offices and the Madrid main office.

Your boss at Certkiller , Mrs. Certkiller, has asked you to document the current IPSec VPN configurations from Madrid to the remote locations. Using the SDM utility you study the SDM Output from VPN Tasks under the Configure tab. Please refer to the SDM output exhibit.

Certkiller .com Spain (4 Questions)

QUESTION 106:

The IPSec tunnel to the Certkiller 4 branch office terminates at which IP address, and what is the protected subnet behind the Certkiller 4 branch office router? Select two.

- A. 10.5.64.0/24
- B. 192.168.8.4
- C. 192.168.2.17
- D. 10.2.55.0/24
- E. 192.168.5.12
- F. 10.8.74.0/24

Answer: B, F

Explanation: The highest IP address and the highest subnet.
192.168.8.4 is the VPN endpoint, 10.8.74.0/24 is the network

QUESTION 107:

Which one of the following statements in regards with the IPSec tunnel between Certkiller 1 and Certkiller 2 is correct?

- A. Tunnel mode is used; therefore a GRE tunnel interface will be configured.
- B. Only the ESP protocol is being used; AH is not being used.
- C. The Certkiller 4 branch office router is using dynamic IP address; therefore, the Certkiller 1 router is using a dynamic crypto map.
- D. Dead Peer Detection (DPD) is used to monitor the IPSec tunnel, so if there is no traffic traversing between the two sites, the IPSec tunnel will disconnect.

Answer: B

Explanation: All IPSec transform sets use ESP-3DES and ESP-SHA-HMAC, tunnel mode.

QUESTION 108:

Which of these is used to define which traffic will be protected by IPsec between the Madrid main office and the Certkiller 4 branch office?

- A. ESP-3DES-SHA1 transform set
- B. ACL 151
- C. ACL 168
- D. ACL 173
- E. ESP-3DES-SHA2 transform set

F. IKE Phase 1

Answer: D

Explanation: The ACL with the highest number.

QUESTION 109:

Which of the following statements is correct?

- A. IKE uses Digital Certificates
- B. IKE uses 3DES, DH group5 and tunnel mode
- C. IKE uses 3DES, DH group5 and transport mode
- D. IKE uses AES, DH group 2 and tunnel mode
- E. IKE uses pre-shared keys, DH group 2, 3DES

Answer: E

Practice Questions (19 Questions)

Study these questions as well to reinforce exam concepts.

QUESTION 110:

Which communication protocol is used by the administrator workstation to communicate with the CSA MC?

- A. SSH
- B. Telnet
- C. HTTPS
- D. SSL

Answer: D

Explanation: Management Center for Cisco Security Agent (CSA MC) uses a Secure Sockets Layer (SSL)-enabled web interface.

QUESTION 111:

Select two ways to secure hardware from threats. (Choose two.)

- A. The room must have steel walls and doors.
- B. The room must be static free.
- C. The room must be locked, with only authorized people allowed access.
- D. The room should not be accessible via a dropped ceiling, raised floor, window, ductwork, or point of entry other than the secured access point.

Answer: C, D

Explanation: -

Incorrect:

A - Not a required element.

B - Is called 'Environment Threat mitigation'

QUESTION 112:

At which layer of the OSI model does a proxy server work?

- A. data link
- B. physical
- C. application
- D. network
- E. transport

Answer: C

Explanation:

A proxy server is an application

QUESTION 113:

What are the three types of private VLAN ports? (Choose three.)

- A. typical
- B. isolated
- C. nonisolated
- D. promiscuous
- E. community
- F. bridging

Answer: B, D, E

Explanation:

There are three types of PVLAN ports:

Promiscuous: A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.

Isolated: An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. PVLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic from isolated port is forwarded only to promiscuous ports.

Community: Community ports communicate among themselves and with their promiscuous ports. These interfaces are separated at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN.

QUESTION 114:

How does HIPS inspect for attacks?

- A. by intercepting traffic that is incoming to the network interface card
- B. by inspecting syslog messages
- C. by inspecting traffic that is outgoing from the network interface card
- D. by intercepting calls to the OS kernel
- E. by inspecting API message between applications

Answer: D

Explanation:

HIPS operates by detecting attacks occurring on a host on which it is installed. HIPS works by intercepting operating system and application calls, securing the operating system and application configurations, validating incoming service requests, and analyzing local log files for after-the-fact suspicious activity.

QUESTION 115:

Which component within the Cisco Network Admission Control architecture acts as the policy server for evaluating the endpoint security information that is relayed from network devices, and for determining the appropriate access policy to apply?

- A. CiscoWorks
- B. CiscoWorks VMS
- C. Cisco Secure ACS
- D. Cisco Trust Agent
- E. Cisco Security Agent

Answer: C

QUESTION 116:

When port security is enabled on a Cisco Catalyst switch, what is the default action when the configured maximum of allowed MAC addresses value is exceeded?

- A. The port is shut down.
- B. The port is enabled and the maximum number automatically increases.
- C. The MAC address table is cleared and the new MAC address is entered into the table.
- D. The MAC address table is shut down.

Answer: A

Explanation:

Feature	Default Setting
Port security	Disabled on a port
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/port_sec.pdf

QUESTION 117:

Packet sniffers work by using a network interface card in which mode?

- A. inline
- B. cut-through
- C. promiscuous
- D. Ethernet
- E. passive

Answer: C

Explanation:

A packet sniffer is a software application that uses a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN.

Packet sniffers can only work in the same collision domain.

Promiscuous mode is a mode in which the network adapter card sends all packets received on the physical network wire to an application for processing.

QUESTION 118:

Which command would be used on the Cisco PIX Security Appliance to show the pool of addresses to be translated?

- A. show nat
- B. show xlate
- C. show global
- D. show conn

Answer: C

Explanation:

The show global command displays the global pool (or pools) of addresses configured in the PIX Security Appliance.

Incorrect:

Show NAT

Use the show nat command to display a single host or range of hosts to be translated.

Show Xlate

The show xlate command displays the contents of the translation slot.

Show Conn

Displays all active connections.

QUESTION 119:

What would the following command indicate if it were used on the Cisco PIX Security Appliance?

```
nameif ethernet2 dmz security50
```

- A. The administrator is naming an Ethernet interface only.
- B. The administrator is assigning a security level only.
- C. The administrator is removing a named interface.
- D. The administrator is naming an interface and assigning a security level to it.

Answer: D

Explanation:

The nameif command assigns a name to each interface on the PIX Security Appliance and specifies its security level (except for the inside and outside PIX Security Appliance interfaces, which are named by default).

The first two interfaces have the default names .inside. and .outside.. The inside interface has a default security level of 100; the outside interface has a default security level of 0.

Here, interface ethernet2 was assigned a name of DMZ with a security level of 50.

The syntax for the nameif command is as follows:

```
nameif hardware_id if_name security_level
```

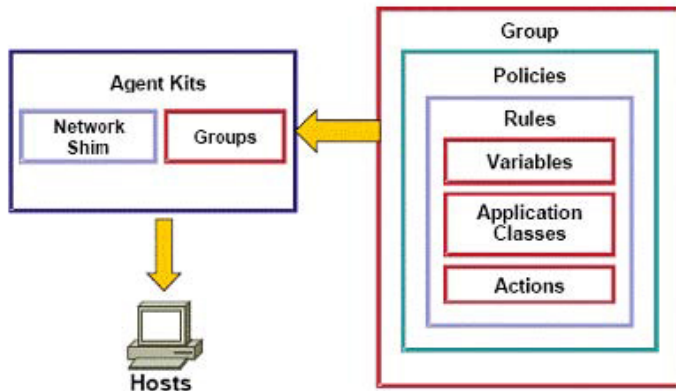
QUESTION 120:

Which CSA object contains associations with policies and can accept hosts as members?

- A. Groups
- B. Policies
- C. Variables
- D. Agent Kits

Answer: A

Explanation:



Groups

Groups contain associations with policies and can accept hosts as members.

Incorrect:

Policies

Policies contain rules and are applied to a group or multiple groups.

Variables, Application Classes, and Actions

These elements are combined to create rules.

Agent Kits

Agent kits contain groups and (optionally) the network shim.

Agent kits are deployed to hosts to install the CSA software and all of the policies and rules that have been built into them.

QUESTION 121:

Where is the Cisco Security Agent installed?

- A. on a router
- B. on a switch
- C. on a host
- D. on a hub

Answer: C

Explanation:

The CSA software that is installed in the host systems (for example, workstations, laptops, servers, and so on) across the network. This software continually monitors local system activity and analyzes the operations of that system. The CSA takes proactive action to block attempted malicious activity and polls the CSA MC at configurable intervals for policy updates.

QUESTION 122:

What is the purpose of the global command on the Cisco PIX Security Appliance?

- A. to set up the IP addresses on an interface
- B. to enable global configuration mode
- C. to create a pool of one or more IP addresses for use in NAT and PAT
- D. to enable global NAT

Answer: C

Explanation:

Creates a pool of one or more IP addresses for use in NAT and port address translation (PAT).

Incorrect:

To set up the IP addresses on an interface

ipaddress <int name> 192.168.0.254 255.255.255.0

To enable global configuration mode

Configure terminal

To enable global NAT

QUESTION 123:

SIMULATION

You are the network security administrator for Certkiller .com. Certkiller .com recently acquired Gamma Technologies. Your company wants you to add an interface to the Cisco PIX Security Appliance to support a dedicated network for the new employees. Your task is to enable the ethernet1 interface for 100-Mbps full-duplex communication and configure it with the following parameters:

The configuration will be as follows:

Name: aikman

Security level: 60

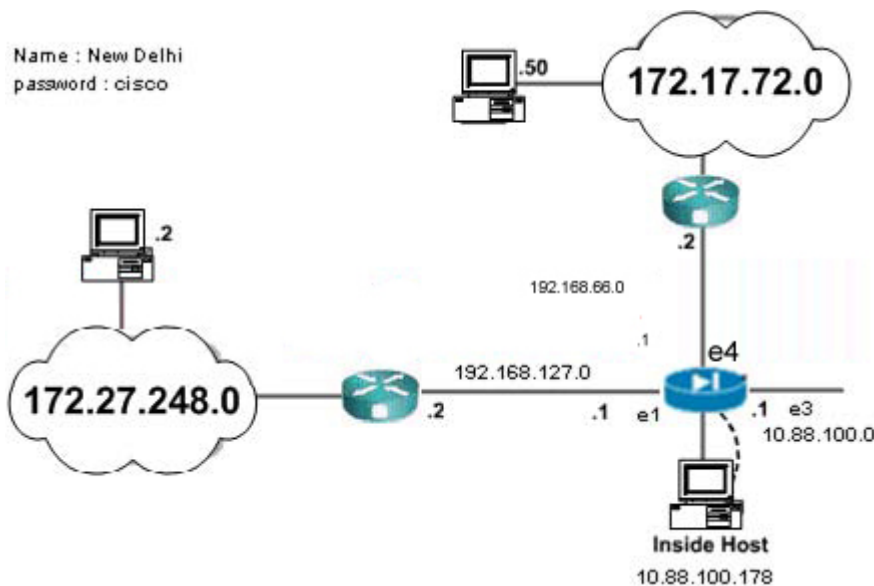
IP address: 192.168.127.1

Netmask 255.255.255.0

You will not be able to ping the inside PIX interface from an interface connected to an inside host.

The Firewall is named New Delhi

The enable password is cisco



Answer:

Explanation:

enable

password: cisco

conf t

(config) name if ethernet1 aikman security 60 (Name's Interface and set's security level)

(config) interface ethernet1 100full (Set's Interface to 100 Full)

(config) ip address aikman 192.168.127.1 255.255.255.0 (Give the named interface an IP and subnet)

(config) exit

write mem

1. NAMEIF ETHERNET1 AIKMAN SECURITY60 (Name's Interface and set's security level)

2. INTERFACE ETHERNET1 100FULL (Set's Interface to 100 Full)

3. IP ADDRESS AIKMAN 192.168.127.1 255.255.255.0 (Give the named interface an IP and subnet)

Alternative correct answer:

New Delhi >enable

Password:cisco

New Delhi #configure terminal

New Delhi (config)# interface e1

New Delhi (config-if)# nameif aikman

New Delhi (config-if)#ip address 192.168.127.1 255.255.255.0

New Delhi (config-if)#speed 100

New Delhi (config-if)#duplex full

New Delhi (config-if)#security 60

New Delhi (config-if)#no shut

New Delhi (config-if)#exit

New Delhi (config)#show interface

New Delhi (config)#show ip address
New Delhi (config)#write memory

QUESTION 124:

Which method does the Cisco IDM use to communicate with the sensor?

- A. Telnet
- B. HTTP
- C. SSH
- D. SSL

Answer: D

Explanation:

IDM is accessed securely via Secure Sockets Layer (SSL) and Transport Layer Security (TLS) using a Netscape or Internet Explorer web browser.

QUESTION 125:

Which command globally disables CDP?

- A. no dcp
- B. cdp disable
- C. no cdp enable
- D. no cdp run

Answer: D

Explanation:

Disable CDP globally on the router using the no cdp run command in global configuration mode as shown in the figure.

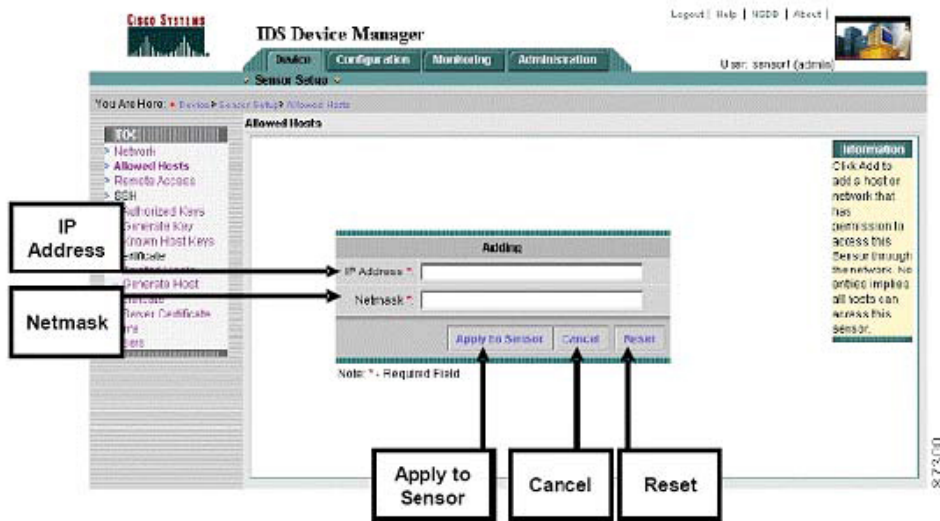
QUESTION 126:

If you choose Add from the Allowed Hosts panel in Cisco IDM, which two fields are available for the configuration? (Choose two.)

- A. Static Routes
- B. Dynamic Routes
- C. IP Address
- D. Default Route
- E. Netmask

Answer: C, E

Explanation:



QUESTION 127:

SIMULATION

You are the network security administrator for Certkiller .com. Certkiller .com has just added TACACS+ AAA authentication to the remote-access topology, requiring you to add two TACACS+ servers to the Austin router configuration. First, enable the AAA access-control model for the router, and then add the two TACACS+ servers and their respective keys. Use the following value as necessary:

Parameter Value

TACACS+ server A : IP address 10.0.71.2

TACACS+ server A : Key aaatest

TACACS+ server B : IP address 10.0.71.3

TACACS+ server B : Key aaahide

The enable secret keyword is cisco

Answer:

1. AAA NEW-MODEL (Enable's AAA on the Router)
2. TACACS-SERVER HOST 10.0.71.2 KEY AAATEST (Add Tacacs+ Server with key)
3. TACACS-SERVER HOST 10.0.71.3 KEY AAAHIDE (as above)

QUESTION 128:

Which method of authentication is considered the strongest?

- A. S/Key (OTP for terminal login)
- B. Username and password (aging)
- C. Token cards or SoftTokens using OTP
- D. Username and password (static)

Answer: C

Explanation:

A stronger method that provides the most secure username and password authentication. Most OTP systems are based on a .secret pass-phrase,. which is used to generate a list of passwords. They are only good for one login, and are therefore, not usefull to anyone who manages to eavesdrop and capture it.

