Exam : 642-551

Title : Securing Cisco Network Devices

Ver : 02.28.07

QUESTION 1:

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: Attackers and hackers can employ social engineering techniques to pose as legitimate people seeking out information. A few well structured telephone calls to unsuspecting employees can provide a significant amount of information
Incorrect:
A - Is called 'Access attacks'
C - Is called 'Worms, Viruses and Trojan Horses'
D - Is called 'Denial of Service (DOS) attacks'
E - This is an example of social engineering

QUESTION 2:

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 3:

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 4:

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 5:

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 6:

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 7:

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
Incorrect:
A - This is called 'Isolated'
B - This is called 'Community'
D - No such PVLAN

QUESTION 8:

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:
The Allowed Hosts option enables you to define which IP addresses are allowed to access the sensor via its management interface.

QUESTION 9:

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:
Version 3 or above is required to support Cryptographic authentication mechanism between peers.

QUESTION 10:

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

QUESTION 11:

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:
These attacks are 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.
Incorrect:
A - Is called 'Access attacks'
B - Is called 'Reconnaissance attacks'
C - Is called 'Worms, Viruses and Trojan Horses'

QUESTION 12:

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 centralsite VPN aggregation. SOHO solutions include platforms for fast-emerging cable and DSLaccess 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 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:

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 15:

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
Reference: http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/

QUESTION 16:

Which protocol does the Cisco Web VPN solution use?

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

Answer: C
Reference:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns347/networking_solutions_sub_solution_home.html

---

QUESTION 17:

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 18:

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 19:

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

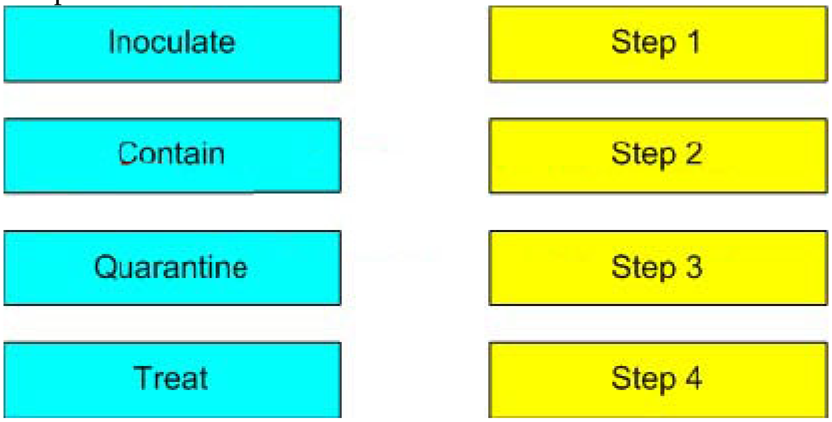
A. SNMP
B. Telnet

C. Poor passwords
D. Poor encryption

Answer: C
Explantion:
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 forpotential 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.

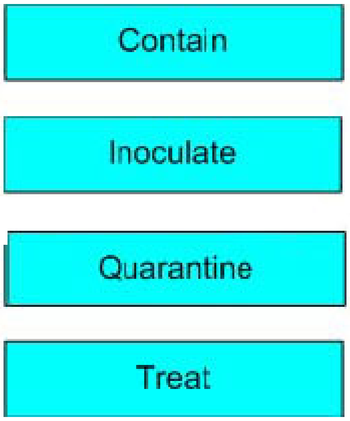
QUESTION 20:

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



Answer:

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 21:

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 22:

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 23:

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 24:

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:
Lightweight EAP (LEAP): Cisco Systems has been shipping a security scheme known as LEAP since November 2000.

QUESTION 25:

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 serviceor 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 26:

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 27:

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.

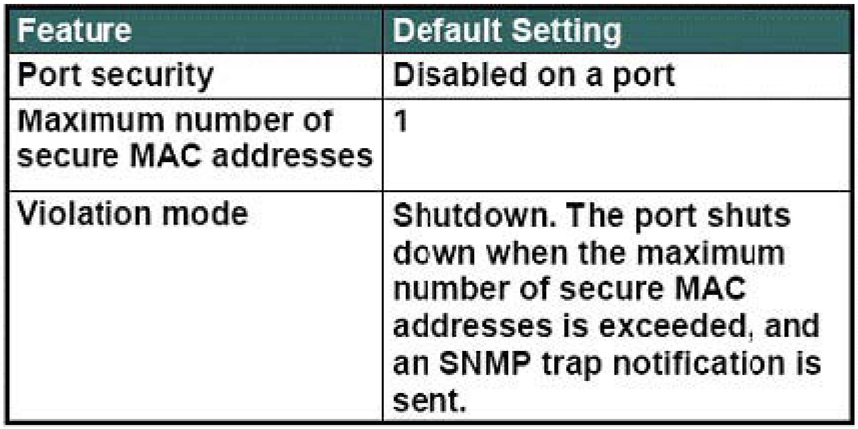
QUESTION 28:

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 29:

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 30:

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

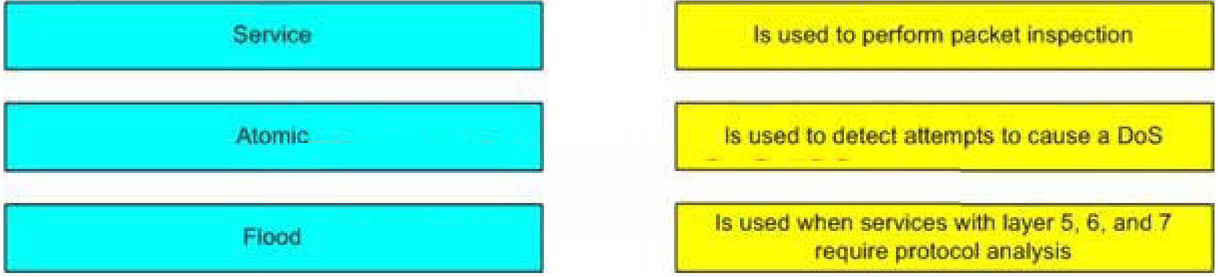
A. show nat
B. show xlate
C. show global
D. show conn

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 31:

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

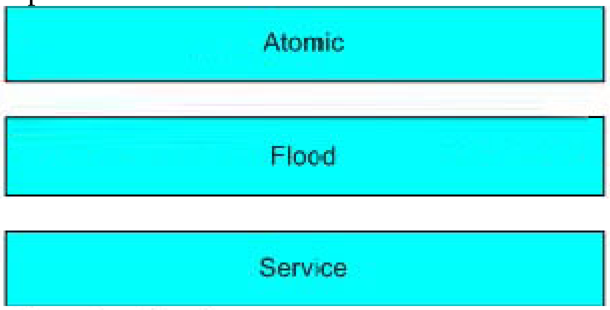


Service
Atomic
Flood

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

Answer:

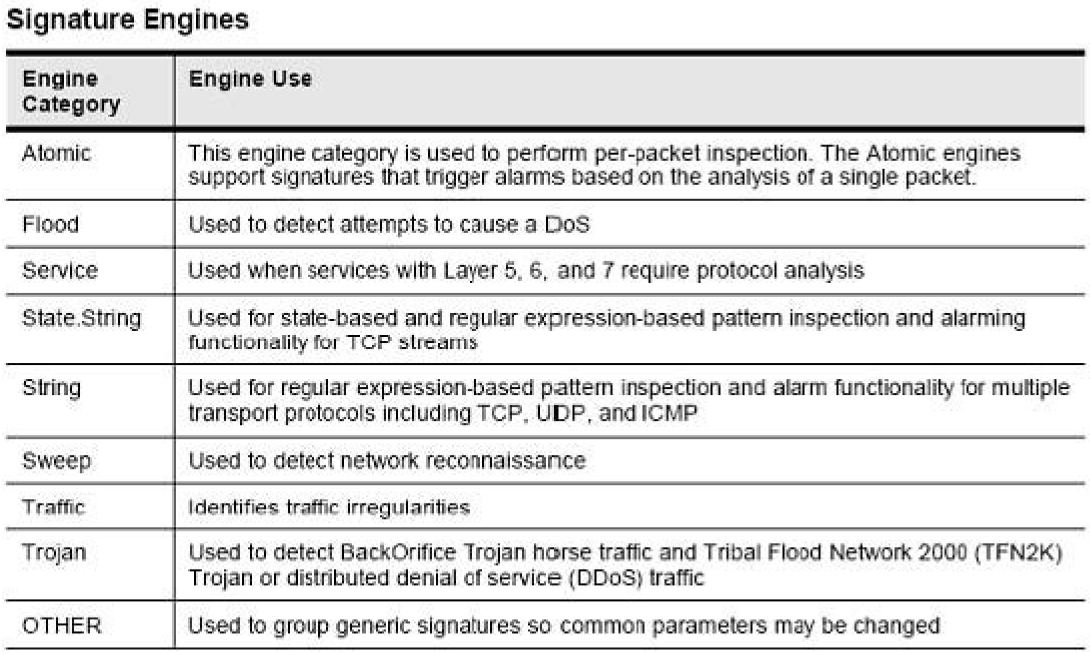
Explanation:



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 32:

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, processesaccess 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 ACLswithout 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 33:

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 34:

What would the following command indocate if it were used on the Cisco PIX Security Appliance?
nameifethernet2 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:
nameifhardware_id if_name security_level

QUESTION 35:

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 36:

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 37:

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 routerbased 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.

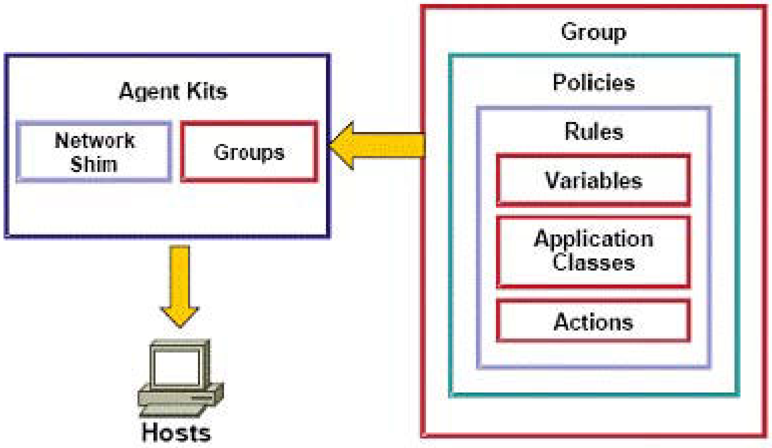
QUESTION 38:

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 39:

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

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

Answer: B

Explanation:
Use the logging command in global configuration mode to set the destination (log) hosts.
The syntax for the logging command is as follows:
logging [host-name | ip-address]

QUESTION 40:

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 41:

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:
SSH version 1 is supported in Cisco IOS Software Releases 12.1(1)T and later. SSH version 2 is supported in Cisco IOS Software Releases 12.3(4)T and later.
Cisco routers configured for SSH act as SSH servers.

QUESTION 42:

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

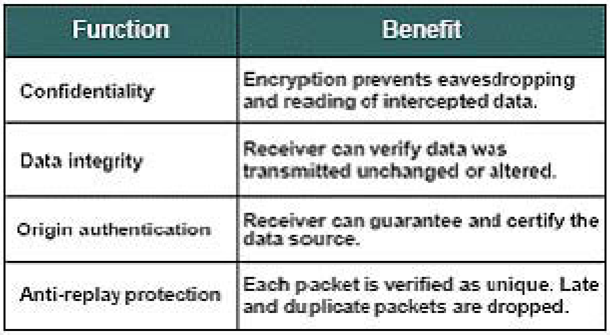
QUESTION 43:

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

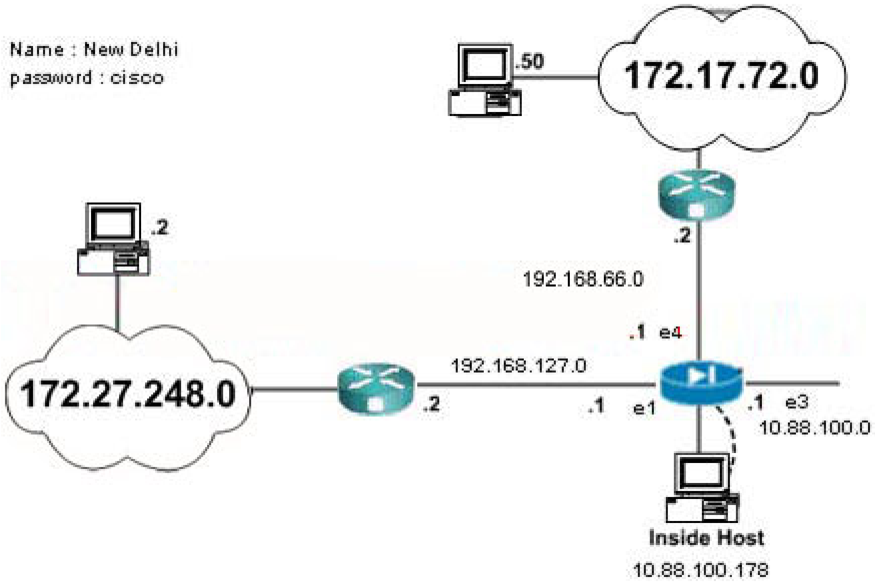
Explanation:



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 44:

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 (conifg)# interface e1
New Delhi (conifg-if)# nameif aikman
New Delhi (conifg-if)#ip address 192.168.127.1 255.255.255.0
New Delhi (conifg-if)#speed 100
New Delhi (conifg-if)#duplex full
New Delhi (conifg-if)#security 60
New Delhi (conifg-if)#no shut
New Delhi (conifg-if)#exit
New Delhi (config)#show interface
New Delhi (config)#show ip address
New Delhi (config)#write memory
```

QUESTION 45:

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 46:

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.

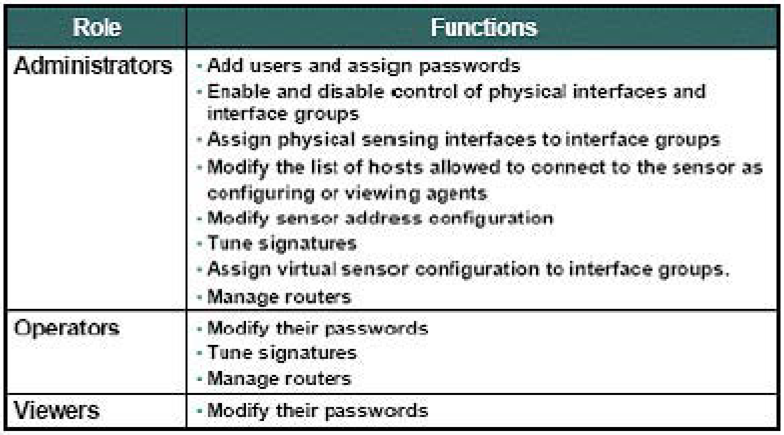
QUESTION 47:

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	· 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	· Modify their passwords · Tune signatures · Manage routers
Viewers	· Modify their passwords

QUESTION 48:

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.

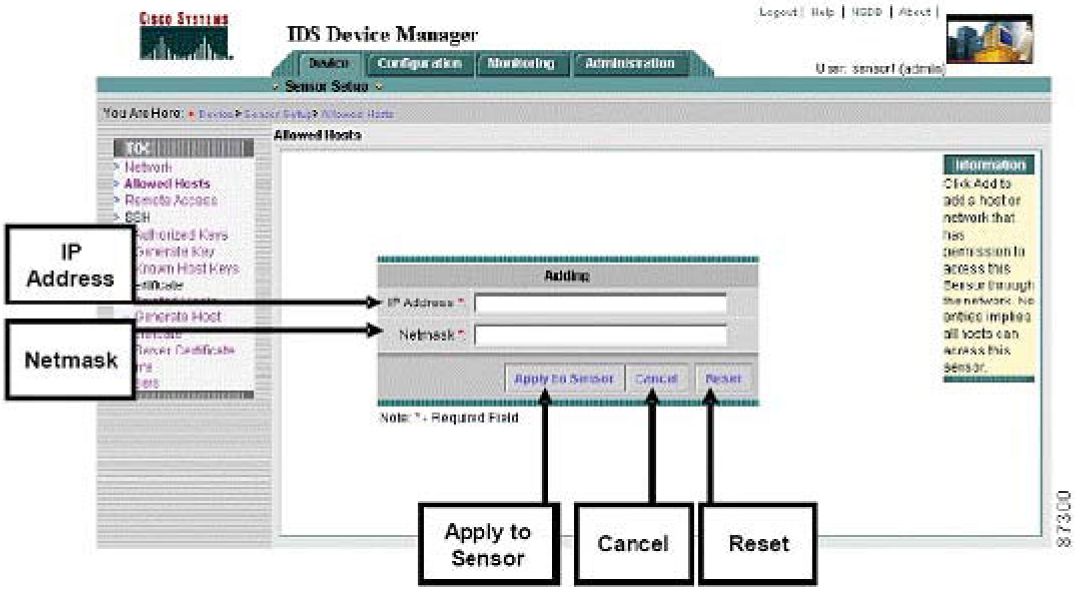
QUESTION 49:

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:



Click Add to add a host or network that has permission to access this Sensor through the network. No entries implies all hosts can access this sensor.

Note: * - Required Field

QUESTION 50:

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 betweenpeers. 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 exchangedbetween endpoints. The final result of IKE phase 1 and phase 2 is a securecommunications channel between peers.

Step 4
Data transfer: Data is transferred between IPSec peers based on the IPSec parametersand keys stored in the SA database.
Step 5
IPSec tunnel termination: IPSec SAs terminate through deletion or by timing out.

QUESTION 51:

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.
MC has a look and feel similar to the PDM; however, with Firewall MC, you can
CiscoWorks 2000 Management Center for Firewalls (Firewall MC) is a web-based interface for configuring and managing multiple Cisco PIX Security Appliances. Firewall 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 52:

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)

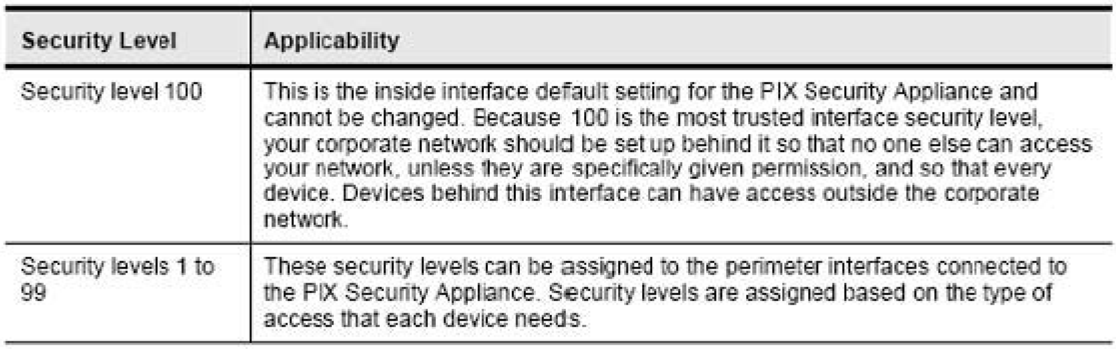
QUESTION 53:

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.

QUESTION 54:

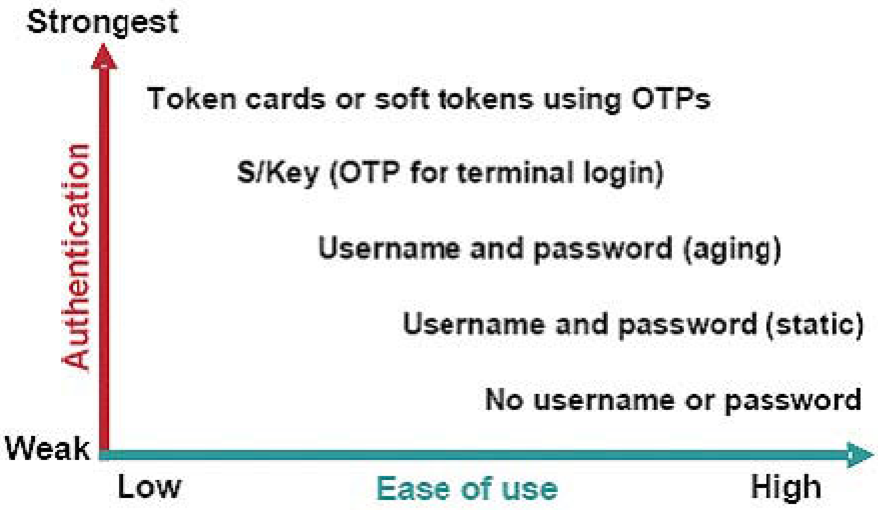
Which method of authentication is considered the strongest?

A. S/Key (OTP for terminal login)
B. Username and password (aging)
C. Token cards or SofTokens 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.


Strongest
Token cards or soft tokens using OTPs
S/Key (OTP for terminal login)
Username and password (aging)
Username and password (static)
No username or password
Authentication
Weak
Low
Ease of use
High

QUESTION 55:

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

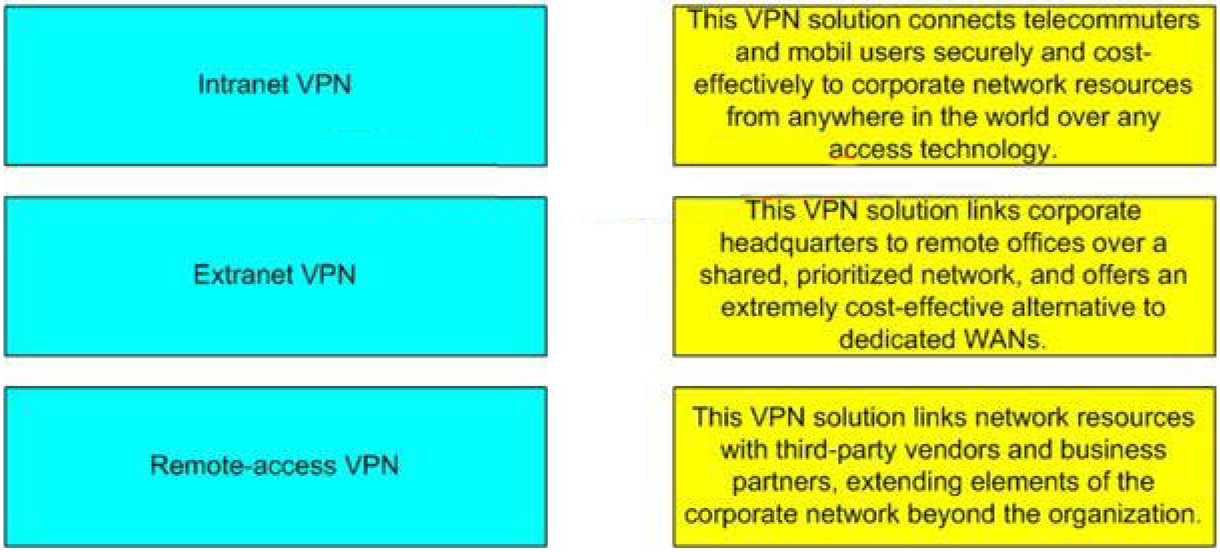
A. password min-length length
B. min-length security length
C. enable secret min-length
D. security passwords min-length length

Answer: D

Explanation:
securitypasswords 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 56:

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



Intranet VPN

Extranet VPN

Remote-access VPN

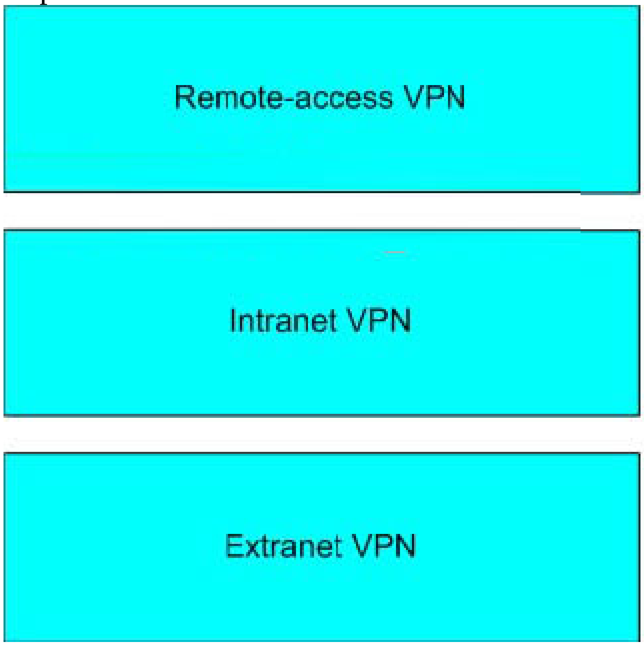
This VPN solution connects telecommuters and mobil users securely and cost-effectively to corporate network resources from anywhere in the world over any access technology.

This VPN solution links corporate headquarters to remote offices over a shared, prioritized network, and offers an extremely cost-effective alternative to dedicated WANs.

This VPN solution links network resources with third-party vendors and business partners, extending elements of the corporate network beyond the organization.

Answer:

Explanation:



Remote-access VPN

Intranet VPN

Extranet VPN

QUESTION 57:

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 58:

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 59:

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

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

Answer: C

Explanation:
Network Time Protocol (NTP) is used to synchronize the clocks of various devices across a network. Synchronization of the clocks within a network is critical for digital certificates and for correct interpretation of events within syslog data.

QUESTION 60:

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 61:

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 62:

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.