[Updated Constantly]

HERE

CCNA Security v2.0 Certification Practice Exam Answers

How to find: Press “Ctrl + F” in the browser and fill in whatever wording is in the question to find that question/answer.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. **During the AAA process, when will authorization be implemented?**

   immediately after an AAA client sends authentication information to a centralized server

   immediately after the determination of which resources a user can access

   immediately after successful authentication against an AAA data source*

   immediately after AAA accounting and auditing receives detailed reports

   AAA authorization is implemented immediately after the user is authenticated against a specific AAA data source.

2. **What is the primary function of the Diffie-Hellman algorithm?**

   to provide data integrity

   to prevent man-in-the middle attacks

   to generate and share public keys

   to exchange shared secret keys over untrusted networks*

   The Diffie-Hellman (DH) algorithm is a modern key exchange method that allows the exchange of secret keys securely over an untrusted network.

3. **hen configuring SSH on a router to implement secure network management, a network engineer has issued the login local and transport input ssh line vty commands. What three additional configuration actions have to be performed to complete the SSH configuration? (Choose three.)**

   Configure role-based CLI access.

   Create a valid local username and password database.*

   Configure the correct IP domain name.*

   Manually enable SSH after the RSA keys are generated.

   Set the user privilege levels.

   Generate the asymmetric RSA keys.*

SSH is automatically enabled after the RSA keys are generated. Setting user privilege levels and configuring role-based CLI access are good security practices but are not a requirement of implementing SSH.

4. **Which functionality does the TACACS single-connection keyword provide to AAA services?**

maintains a single UDP connection for the life of the session

enhances the performance of the TCP connection*

encrypts the data transfer between the TACACS+ server and the AAA client

allows the use of differing keys between the TACACS+ server and the AAA client

The single-connection keyword enhances TCP performance with TACACS+ by maintaining a single TCP connection for the life of the session. Without the single-connection keyword, a TCP connection is opened and closed per session.

5. **In what situation would a network administrator most likely implement root guard?**

on all switch ports (used or unused)

on all switch ports that connect to a Layer 3 device

on all switch ports that connect to another switch that is not the root bridge*

on all switch ports that connect to another switch

on all switch ports that connect to host devices

Root guard in conjunction with PortFast, and BPDU guard is used to prevent an STP manipulation attack.

6. **What type of algorithms require sender and receiver to exchange a secret key that is used to ensure the confidentiality of messages?**

symmetric algorithms*

public key algorithms

hashing algorithms

asymmetric algorithms

Symmetric algorithms use the same key, a secret key, to encrypt and decrypt data. This key must be pre-shared before communication can occur. Asymmetric algorithms require more processing power and overhead on the communicating devices because these keys can be long in order to avoid being hacked.

7. **A network administrator is configuring an AAA server to manage TACACS+ authentication. What are two attributes of TACACS+ authentication? (Choose two.)**

encryption for only the password of a user

encryption for all communication*

separate processes for authentication and authorization*

single process for authentication and authorization

UDP port 1645

TCP port 40

TACACS+ authentication includes the following attributes:
Separates authentication and authorization processes
Encrypts all communication, not just passwords
Utilizes TCP port 49

8. **What is a characteristic of a role-based CLI view of router configuration?**

A CLI view has a command hierarchy, with higher and lower views.

When a superview is deleted, the associated CLI views are deleted.

A single CLI view can be shared within multiple superviews.*

Only a superview user can configure a new view and add or remove commands from the existing views.

A CLI view has no command hierarchy, and therefore, no higher or lower views. Deleting a superview does not delete the associated CLI views. Only a root view user can configure a new view and add or remove commands from the existing views.

9. **What service or protocol does the Secure Copy Protocol rely on to ensure that secure copy transfers are from authorized users?**

AAA*

RADIUS

IPsec

SNMP

Secure Copy Protocol (SCP) is used to securely copy IOS images and configuration files to a SCP server. To perform this, SCP will use SSH connections from users authenticated through AAA.

10. **Which three functions are provided under Cisco NAC framework solution? (Choose three.)**

secure connection to servers

VPN connection

AAA services*

intrusion prevention

remediation for noncompliant devices*

scanning for policy compliance*

The goal of both the Cisco NAC framework and the Cisco NAC Appliance is to ensure that only hosts that are authenticated and have their security posture examined and approved are permitted onto the network. They provide four important functions: authentication, authorization, and accounting; posture assessment (evaluating an incoming device against the security policies), quarantining of non-compliant systems, and remediation of noncompliant devices. They do not provide VPN connection or intrusion detection/prevention services.

11. **A network administrator is configuring an AAA server to manage RADIUS authentication. Which two features are included in RADIUS authentication? (Choose two.)**

encryption for all communication

encryption for only the data

separate processes for authentication and authorization

hidden passwords during transmission*

single process for authentication and authorization*

RADIUS authentication supports the following features:
RADIUS authentication and authorization as one process
Encrypts only the password
Utilizes UDP
Supports remote-access technologies, 802.1X, and Session Initiation Protocol (SIP)

12. **What is the next step in the establishment of an IPsec VPN after IKE Phase 1 is complete?**

negotiation of the ISAKMP policy

detection of interesting traffic

authentication of peers

negotiation of the IPsec SA policy*

Establishing an IPsec tunnel involves five steps:
detection of interesting traffic defined by an ACL
IKE Phase 1 in which peers negotiate ISAKMP SA policy
IKE Phase 2 in which peers negotiate IPsec SA policy
Creation of the IPsec tunnel
Termination of the IPsec tunnel

13. **A security technician uses an asymmetric algorithm to encrypt messages with a private key and then forwards that data to another technician. What key must be used**

to decrypt this data?

The public key of the receiver.

The private key of the sender.

The public key of the sender.*

The private key of the receiver.

Asymmetric algorithms use two keys. if a public key encrypts the data, the matching private key decrypts the data. The opposite is also true. If a private key encrypts the data, the corresponding public key decrypts the data.

14. **Which IPS signature trigger type is based on a defined profile of normal network activity?**

pattern-based detection

policy-based detection

anomaly-based detection*

honeypot-based detection

There are four IPS trigger types:
pattern-based detection
anomaly-based detection
policy-based detection
honeypot-based detection
Anomaly-based detection compares network activity to a predefined profile of what is considered normal activity.

15. **Which condition describes a true positive IPS signature alarm?**

when an alarm is not generated in response to a known attack

when an alarm is not generated by normal traffic

when an alarm is generated in response to a known attack*

when an alarm is generated by normal traffic

There are four IPS alarms:
False positive – occurs when normal traffic triggers an alarm
False negative – occurs when known malicious traffic that should trigger an alarm does not
True positive – occurs when traffic that is known to be malicious triggers an attack
True negative – occurs when normal traffic does not trigger an alarm

16. **In the implementation of secure network management, what are two services or functions of the management plane of a Cisco router that should be configured? (Choose two.)**

secure logins and passwords*

secure SSH access*

Cisco Express Forwarding

traffic filtering with ACLs

Cisco IOS firewall inspection

Cisco Express Forwarding, traffic filtering with ACLs, and Cisco IOS firewall inspection are forwarding plane services that provide security. Management plane security includes these features:

legal notification using a banner

secure password and login functions

secure NTP

secure SSH access

TCP intercept services

17. **Which two characteristics describe a virus? (Choose two.)**

Malicious code that can remain dormant before executing an unwanted action.*

A self-replicating attack that is independently launched.

Malware that relies on the action of a user or a program to activate.*

Malware that executes arbitrary code and installs copies of itself in memory.

Program code specifically designed to corrupt memory in network devices.

A virus is malicious code that is attached to legitimate programs or executable files. Most viruses require end user activation, can lie dormant for an extended period, and then activate at a specific time or date. In contrast, a worm executes arbitrary code and installs copies of itself in the memory of the infected computer. The main purpose of a worm is automatic replication to spread quickly across a network. A worm does not require a host program to run.

18. **Which network attack is mitigated by enabling BPDU guard?**

MAC address spoofing

rogue switches on a network*

CAM table overflow attacks

rogue DHCP servers on a network

There are several recommended STP stability mechanisms to help mitigate STP manipulation attacks:

PortFast – used to immediately bring an interface configured as an access or trunk port to the forwarding state from a blocking state. Applied to all end-user ports.

BPDU guard – immediately error-disables a port that receives a BPDU. Applied to all end-

user ports.The receipt of BPDUs may be part of an unauthorized attempt to add a switch to the network.
Root guard – prevents a switch from becoming the root switch. Applied to all ports where the root switch should not be located.
Loop guard – detects unidirectional links to prevent alternate or root ports from becoming designated ports. Applied to all ports that are or can become nondesignated.

19. **When is a security association (SA) created if an IPsec VPN tunnel is used to connect between two sites?**

during both Phase 1 and 2*

after the tunnel is created, but before traffic is sent

only during Phase 2

only during Phase 1

As seen in the 8.4.1.1 Figure, an IPsec VPN connection creates two SAs: (1) at the completion of the IKE Phase 1 once the peers negotiate the IKE SA policy, and (2) at the end of IKE Phase 2 after the transform sets are negotiated.

20. **How is asymmetric encryption used to provide confidentiality for VPN traffic?**

A sender encrypts traffic with the public key of the receiver and the receiver decrypts the data using the private key of the receiver.*

A sender encrypts traffic with the private key of the receiver and the receiver decrypts the data using the private key of the sender.

A sender encrypts traffic with the private key of the receiver and the receiver decrypts the data using the public key of the sender.

A sender encrypts traffic with the public key of the receiver and the receiver decrypts the data using the public key of the sender.

21. **Which AAA component can be established using token cards?**

authorization

auditing

accounting

authentication*

The authentication component of AAA is established using username and password combinations, challenge and response questions, and token cards. The authorization component of AAA determines which resources the user can access and which operations the user is allowed to perform. The accounting and auditing component of AAA keeps track of how network resources are used.

22. **In the implementation of network security, how does the deployment of a Cisco ASA firewall differ from a Cisco IOS router?**

ASA devices do not support an implicit deny within ACLs.

ASA devices use ACLs configured with a wildcard mask.

ASA devices support interface security levels.*

ASA devices use ACLs that are always numbered.

The differences between ASA devices and Cisco IOS routers include the following:
An ASA device configured with ACLs is configured with a subnet mask.
An ASA device supports interface security levels.
An ASA device configured with an ACL is always named.
ASA devices and Cisco IOS routers are similar in that they both support an implicit deny within an ACL.

23. **What function is performed by the class maps configuration object in the Cisco modular policy framework?**

restricting traffic through an interface

identifying interesting traffic*

applying a policy to an interface

applying a policy to interesting traffic

There are three configuration objects in the MPF; class maps, policy maps, and service policy. The class maps configuration object uses match criteria to identify interesting traffic.

24. **In the implementation of security on multiple devices, how do ASA ACLs differ from Cisco IOS ACLs?**

Cisco IOS routers utilize both named and numbered ACLs and Cisco ASA devices utilize only numbered ACLs.

Cisco IOS ACLs are configured with a wildcard mask and Cisco ASA ACLs are configured with a subnet mask.*

Cisco IOS ACLs are processed sequentially from the top down and Cisco ASA ACLs are not processed sequentially.

Cisco IOS ACLs utilize an implicit deny all and Cisco ASA ACLs end with an implicit permit all.

The Cisco IOS ACLs are configured with a wildcard mask and the Cisco ASA ACLs are configured with a subnet mask. Both devices use an implicit deny, top down sequential processing, and named or numbered ACLs.

25. **In configuring a Cisco router to prepare for IPS and VPN features, a network administrator opens the file realm-cisco.pub.key.txt, and copies and pastes the contents to the router at the global configuration prompt. What is the result after this configuration step?**

The router is authenticated with the Cisco secure IPS resource web server.

A pair of public/secret keys is created for the router to serve as an SSH server.

A crypto key is created for IOS IPS to verify the master signature file.*

A pair of public/secret keys is created for IPsec VPN operation.

The third step in implementing IOS IPS is to configure the Cisco IOS IPS public key that is located in the realm-cisco.pub.key.txt file. This public key is used to verify digital signature for the master signature file, and can be downloaded from cisco.com. To configure the IOS IPS crypto key, open the text file, and copy and paste the contents to the router at the global configuration prompt. Public/private key pairs for IPsec VPN and SSH server are generated using different methods.

26. **When dynamic NAT on an ASA is being configured, what two parameters must be specified by network objects? (Choose two.)**

the outside NAT interface

the interface security level

a range of private addresses that will be translated*

the inside NAT interface

the pool of public global addresses*

On an ASA, both the pool of addresses that will be used as inside global address and the range of internal private addresses that should be translated are configured through network objects.

27. **A system analyst is configuring and tuning a recently deployed IPS appliance. By examining the IPS alarm log, the analyst notices that the IPS does not generate alarms for a few known attack packets. Which term describes the lack of alarms by the IPS?**

false negative*

true positive

true negative

false positive

The alarms generated by an IPS can be classified into 4 types:

A false positive occurs when an IPS generates an alarm on normal user traffic that should not have triggered an alarm.

A false negative occurs when an IPS fails to generate an alarm after processing attack traffic

the IPS is configured to detect.
A true positive occurs when an IPS generates an alarm in response to known attack traffic.
A true negative occurs when normal network traffic does not generate an alarm.

28. **An administrator is comparing multiple implementations of AAA. Which AAA method is server-based and considered the most secure?**
enable
RADIUS
local-case
TACACS+*

Server-based implementations of AAA include both RADIUS and TACACS+. TACACS+ is considered more secure because the entire protocol exchange is encrypted whereas RADIUS will only encrypt the password of the user.

29. **What can be implemented to help mitigate the threat of a rogue switch becoming the root bridge in an STP domain?**
Source Guard
root guard*
BPDU guard
loop guard

There are several recommended STP stability mechanisms to help mitigate STP manipulation attacks:
PortFast – Used to immediately bring an interface configured as an access or trunk port to the forwarding state from a blocking state. Applied to all end-user ports.
BPDU guard – Immediately error-disables a port that receives a BPDU. Applied to all end-user ports.
Root guard – Prevents a switch from becoming the root switch. Applied to all ports where root switch should not be located.
Loop guard – Detects unidirectional links to prevent alternate or root ports from becoming designated ports. Applied to all ports that are or can become non-designated.

30. **Consider the following configuration on a Cisco ASA:**
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
What is the purpose of this command?
to define the ISAKMP parameters that are used to establish the tunnel
to define the encryption and integrity algorithms that are used to build the IPsec tunnel*

to define what traffic is allowed through and protected by the tunnel

to define only the allowed encryption algorithms

The transform set is negotiated during Phase 2 of the IPsec VPN connection process. The purpose of the transform set is to define what encryption and authentication schemes can be used. The device doing the VPN initiation offers the acceptable transform sets in order of preference, in this case, ESP authentication using DES for encryption or ESP authentication using SHA-HMAC authentication and integrity for the data payload. Remember that ESP provides confidentiality with encryption and integrity with authentication. The ESP-DES-SHA is the name of the transform set. The parameters that follow (esp-des and esp-sha-hmac) are the specific types of encryption or authentication that is supported by the ASA for the VPN tunnel that uses this transform set.

31. **What is negotiated in the establishment of an IPsec tunnel between two IPsec hosts during IKE Phase 1?**

interesting traffic

ISAKMP SA policy*

transform sets

DH groups

Establishing an IPsec tunnel involves five steps:
Detection of interesting traffic defined by an ACL
IKE Phase 1 in which peers negotiate ISAKMP SA policy
IKE Phase 2 in which peers negotiate IPsec SA policy
Creation of the IPsec tunnel
Termination of the IPsec tunnel

32. **Which type of IPS signature alarm occurs from normal traffic that should not have triggered an alarm?**

true negative

false negative

true positive

false positive*

There are four IPS alarms:
False positive – occurs when normal traffic triggers an alarm
False negative – occurs when known malicious traffic that should trigger an alarm does not
True positive – occurs when traffic that is known to be malicious triggers an attack
True negative – occurs when normal traffic does not trigger an alarm

33. **Which two options provide secure remote access to a router? (Choose two.)**

HTTP

HTTPS*

CHAP

Telnet

SSH*

For security, all traffic between the administrator computer and the router should be encrypted by using HTTPS or SSH instead of HTTP or Telnet.

34. **What action can a network administrator take to help mitigate the threat of VLAN hopping attacks?**

Disable automatic trunking negotiation.*

Disable VTP.

Enable PortFast on all switch ports.

Configure all switch ports to be members of VLAN 1.

There are two methods for mitigating VLAN hopping attacks:
disabling automatic trunking negotiation on switchports
turning trunking off on all unused nontrunk switchport

35. **What type of data does the DLP feature of Cisco Email Security Appliance scan in order to prevent customer data from being leaked outside of the company?**

messages stored on a client device

messages stored on the email server

outbound messages*

inbound messages

Cisco ESAs control outbound messages through data-loss prevention (DLP), email encryption, and optional integration with the RSA Enterprise Manager. This control helps ensure that the outbound messages comply with industry standards and are protected in transit.

36. **A security specialist configures an IPS so that it will generate an alert when an attack is first detected. Alerts for the subsequent detection of the same attack are suppressed for a pre-defined period of time. Another alert will be generated at the end of the period indicating the number of the attack detected. Which IPS alert monitoring mechanism is configured?**

atomic alert

summary alert*

correlation alert

composite alert

Alerts generated by an IPS should be monitored closely to ensure proper actions are taken against malicious attacks. IPS solutions incorporate two types of alerts, atomic alerts and summary alerts. Atomic alerts are generated every time a signature triggers. A summary alert is a single alert that indicates multiple occurrences of the same signature from the same source address or port. With a summary alter, the first detection of the attack triggers a normal alert. Subsequent detection of the same attack is counted until the end of the signature summary interval. When the length of time specified by the summary interval has elapsed, a summary alarm is sent, indicating the number of alarms that occurred during the time interval.

37. **Which transform set provides the best protection?**

crypto ipsec transform-set ESP-DES-SHA esp-aes esp-des esp-sha-hmac

crypto ipsec transform-set ESP-DES-SHA esp-3des esp-sha-hmac

crypto ipsec transform-set ESP-DES-SHA esp-aes-256 esp-sha-hmac*

crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac

DES uses 56-bit keys. 3DES uses 56-bit keys, but encrypts three times. AES uses 128-bit keys. AES-256 uses 256-bit keys and is the strongest.

38. **A syslog server has received the message shown.**

***Mar 1 00:07:18.783: %SYS-5-CONFIG_I: Configured from console by vty0 (172.16.45.1)**

What can be determined from the syslog message?

The message is a normal notification and should not be reviewed.

The message is a Log_Alert notification message.

The message informs the administrator that a user with an IP address of 172.16.45.1 configured this device remotely.*

The message description displays that the console line was accessed locally.

The message shown is a level 5 Log_Notice and displays that a user with an IP address of 172.16.45.1 has configured this device remotely.

39. **What are three attributes of IPS signatures? (Choose three.)**

action*

length

trigger*

type*

depth

function

IPS signatures have three distinctive attributes:

• type

• trigger (alarm)

• action

40. **What mitigation plan is best for thwarting a DoS attack that is creating a switch buffer overflow?**

Enable port security.*

Disable STP.

Disable DTP.

Place unused ports in an unused VLAN.

A MAC address (CAM) table overflow attack, buffer overflow, and MAC address spoofing can all be mitigated by configuring port security. A network administrator would typically not want to disable STP because it prevents Layer 2 loops. DTP is disabled to prevent VLAN hopping. Placing unused ports in an unused VLAN prevents unauthorized wired connectivity.

41. **What mitigation method is effective against CAM table overflow attacks?**

port security*

DHCP snooping

Dynamic ARP Inspection

Source Guard

Port security is the most effective method for preventing CAM table overflow attacks. Port security gives an administrator the ability to manually specify what MAC addresses should be seen on given switch ports. It provides a method for limiting the number of MAC addresses that can be dynamically learned over a switch port.

42. **An administrator assigned a level of router access to the user ADMIN using the commands below.**

Router(config)# privilege exec level 14 show ip route

Router(config)# enable algorithm-type scrypt secret level 14 cisco-level-10

Router(config)# username ADMIN privilege 14 algorithm-type scrypt secret cisco-level-10

Which two actions are permitted to the user ADMIN? (Choose two.)

The user can issue all commands because this privilege level can execute all Cisco IOS commands.

The user can only execute the subcommands under the show ip route command.

The user can issue the show version command.*

The user can execute all subcommands under the show ip interfaces command.*

The user can issue the ip route command.

Assigning a command such as show ip route to a specific privilege level automatically assigns all commands associated with the first few keywords to the specified privilege level. So, the show and the show ip commands are automatically set to the privilege level where show ip route is set, which is necessary because the show ip route command cannot be executed without access to the show and show ip commands. Assigning the show ip route command allows the user to issue all show commands, such as show version.

43. **What is an effective deployment of IPS and IDS appliances in a corporate network?**

Place an IPS between the border router and the internal network and an IDS in the same LAN.*

Place an IPS between the border router and the internal network and an IDS between the border router and the ISP.

Place both an IPS and an IDS inside the DMZ network.

Place an IDS between the border router and the internal network and an IPS inside the DMZ network.

An IPS is deployed in inline mode whereas an IDS is deployed in promiscuous mode. An effective deployment of IPS/IDS is to place an IPS right behind the border router to filter the traffic inbound to and outbound from the corporate internal network. IPS and IDS technologies can complement each other. Although an IDS will not stop an intrusion attack immediately, it can be used to validate IPS operation because the IDS can be configured for deeper packet inspection offline. This allows the IPS to focus on fewer but more critical traffic patterns inline. Placing IPS and IDS in the DMZ network will not protect the corporate internal network.

44. **Which antispoofing technology is used to mitigate DoS attacks?**

encryption

port scanning

switched infrastructure

switch port-security*

strong authentication

Implementing switch port-security will assist in mitigating DoS attacks. In order to mitigate reconnaissance attacks, it is best to use strong authentication, a switched infrastructure, antisniffer software, and encryption.

45. **A network administrator notices that unsuccessful login attempts have caused a router to enter quiet mode. How can the administrator maintain remote access to the networks even during quiet mode?**

Quiet mode behavior will only prevent specific user accounts from attempting to authenticate.

Quiet mode behavior can be enabled via an ip access-group command on a physical interface.

Quiet mode behavior can be disabled by an administrator by using SSH to connect.

Quiet mode behavior can be overridden for specific networks by using an ACL.*

Quiet mode prevents any further login attempts for a period of time. Quiet mode is enabled via the login quiet-mode access-class command. Quiet mode behavior can be overridden for specific networks by building and implementing an access control list (ACL).

46. **Which statement describes the function of the SPAN tool used in a Cisco switch?**

It provides interconnection between VLANs over multiple switches.

It is a secure channel for a switch to send logging to a syslog server.

It copies the traffic from one switch port and sends it to another switch port that is connected to a monitoring device.*

It supports the SNMP trap operation on a switch.

To analyze network traffic passing through a switch, switched port analyzer (SPAN) can be used. SPAN can send a copy of traffic from one port to another port on the same switch where a network analyzer or monitoring device is connected. SPAN is not required for syslog or SNMP. SPAN is used to mirror traffic, while syslog and SNMP are configured to send data directly to the appropriate server.

47. **What function is provided by the Cisco IOS Resilient Configuration feature?**

It locks down the management plane and the forwarding plane services and functions of a router.

It allows administrators to create different views of router configurations for different users.

It maintains a secure copy of the IOS image and running configuration that can be used for fast recovery if flash or NVRAM is erased.*

It identifies attacks and security policy violations that are occurring on the network.

The Cisco IOS Resilient Configuration feature allows a secure copy of the IOS and running configuration file to be stored locally on a router. If flash memory or NVRAM is inadvertently or maliciously erased, the router can be quickly restored using the stored files.

48. **What does the TACACS+ protocol provide in a AAA deployment?**

compatibility with previous TACACS protocols

password encryption without encrypting the packet

AAA connectivity via UDP

authorization on a per-user or per-group basis*

TACACS+ utilizes TCP port 49, provides authorization on a per-user or per-group basis, encrypts the entire packet, and does not provide compatibility with previous TACACS protocols.

49. **Which two UDP port numbers may be used for server-based AAA RADIUS authentication? (Choose two.)**

1812*

1645*

1813

1646

49

RADIUS authentication and accounting utilize the following UDP port numbers:
UDP port 1645 or 1812 for authentication
UDP port 1646 or 1813 for accounting
TACACS+ uses TCP port 49.

50. **Which two options can limit the information discovered from port scanning? (Choose two.)**

intrusion prevention system*

firewall*

authentication

passwords

encryption

Using an intrusion prevention system (IPS) and firewall can limit the information that can be discovered with a port scanner. Authentication, encryption, and passwords provide no protection from loss of information from port scanning.

51. **What function is provided by the RADIUS protocol?**

RADIUS provides encryption of the complete packet during transfer.

RADIUS provides separate AAA services.

RADIUS provides separate ports for authorization and accounting.*

RADIUS provides secure communication using TCP port 49.

When an AAA user is authenticated, RADIUS uses UDP port 1645 or 1812 for authentication and UDP port 1646 or 1813 for accounting. TACACS provides separate authorization and

accounting services. When a RADIUS client is authenticated, it is also authorized. TACACS provides secure connectivity using TCP port 49. RADIUS hides passwords during transmission and does not encrypt the complete packet.

52. **What is the role of the Cisco NAC Agent in implementing a secure networking infrastructure?**

to provide the ability for company employees to create guest accounts

to perform deep inspection of device security profiles*

to provide post-connection monitoring of all endpoint devices

to assess and enforce security policy compliance in the NAC environment

to define role-based user access and endpoint security policies

Cisco NAC is used in the Cisco Borderless Network Architecture to authenticate users and ensure user devices are compliant with security policies. The Cisco NAC Agent is optional agent software that runs on endpoints and performs deep inspection of the security profile of that device.

53. **What level of syslog is associated with Log_Alert?**

1*

2

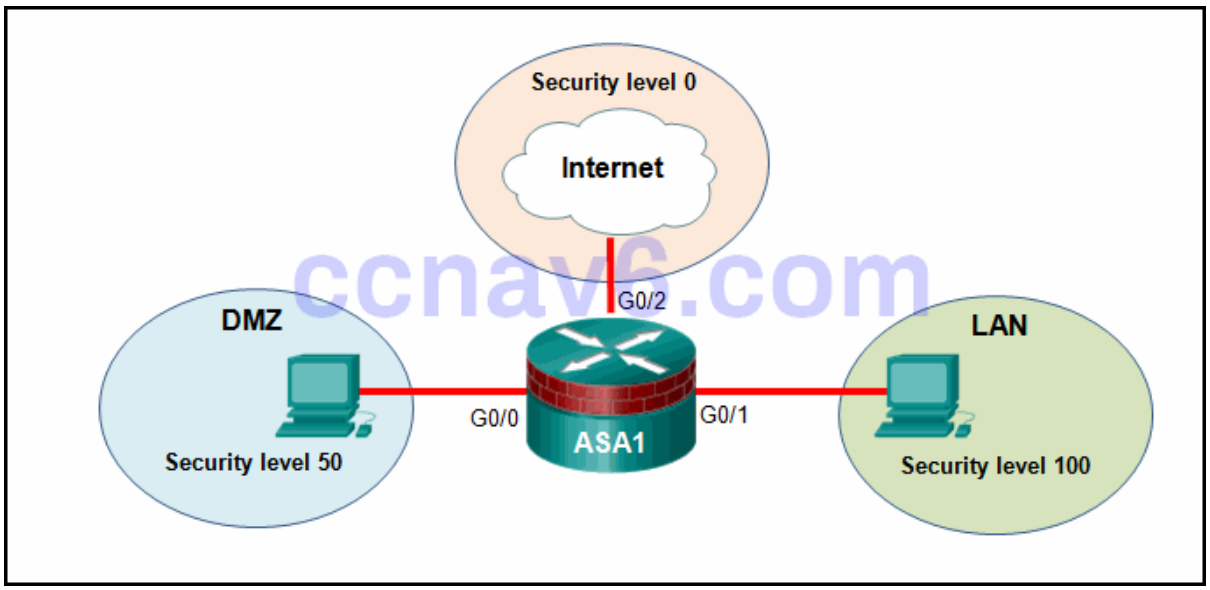
4

0

3

Syslog levels range from 0 to 7:
Level 0 is Log_Emerg
Level 1 is Log_Alert
Level 2 is Log_Crit
Level 3 is Log_Err
Level 4 is Log_Warning
Level 5 is Log_Notice
Level 6 is Log_Info
Level 7 is Log_Debug

54. **Refer to the exhibit. Based on the security levels of the interfaces on ASA1, what traffic will be allowed on the interfaces?**



Traffic from the LAN and DMZ can access the Internet.*

Traffic from the Internet and LAN can access the DMZ.

Traffic from the Internet can access both the DMZ and the LAN.

Traffic from the Internet and DMZ can access the LAN.

ASA devices have security levels assigned to each interface that are not part of a configured ACL. These security levels allow traffic from more secure interfaces, such as security level 100, to access less secure interfaces, such as level 0. By default, they allow traffic from more secure interfaces (higher security level) to access less secure interfaces (lower security level). Traffic from the less secure interfaces is blocked from accessing more secure interfaces.

55. **Refer to the exhibit. An administrator issues these IOS login enhancement commands to increase the security for login connections. What can be concluded about them?**

```
Router(config)# login block-for 150 attempts 5 within 60
Router(config)# ip access-list standard RULE_ADMIN
Router(config-std-nacl)# permit 192.168.20.10
Router(config-std-nacl)# permit 192.168.21.10
Router(config)# login quiet-mode access-class RULE_ADMIN
```

These enhancements apply to all types of login connections.

The hosts that are identified in the ACL will have access to the device.*

The login block-for command permits the attacker to try 150 attempts before being stopped to try again.

Because the login delay command was not used, a one-minute delay between login attempts is assumed.

When the login block-for command is implemented, it automatically invokes a one-second delay between login attempts. The login block-for command that is presented means that login will be disabled for 150 seconds, if more than 5 login failures occur within 60 seconds. These enhancements do not apply to console connections. When quiet mode is enabled, all login attempts are denied except for the hosts permitted in the ACL.