CCNA Security v2.0 Final Exam Answers 100%

itexamanswers.net/ccna-security-v2-0-final-exam-answers.html

February 9, 2016

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

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.

Implementing Network Security (Version 2.0) – CCNAS Final Exam Answers Full 100% Scored

1. Which security implementation will provide control plane protection for a network device?

- encryption for remote access connections
- AAA for authenticating management access
- **routing protocol authentication**
- NTP for consistent timestamps on logging messages

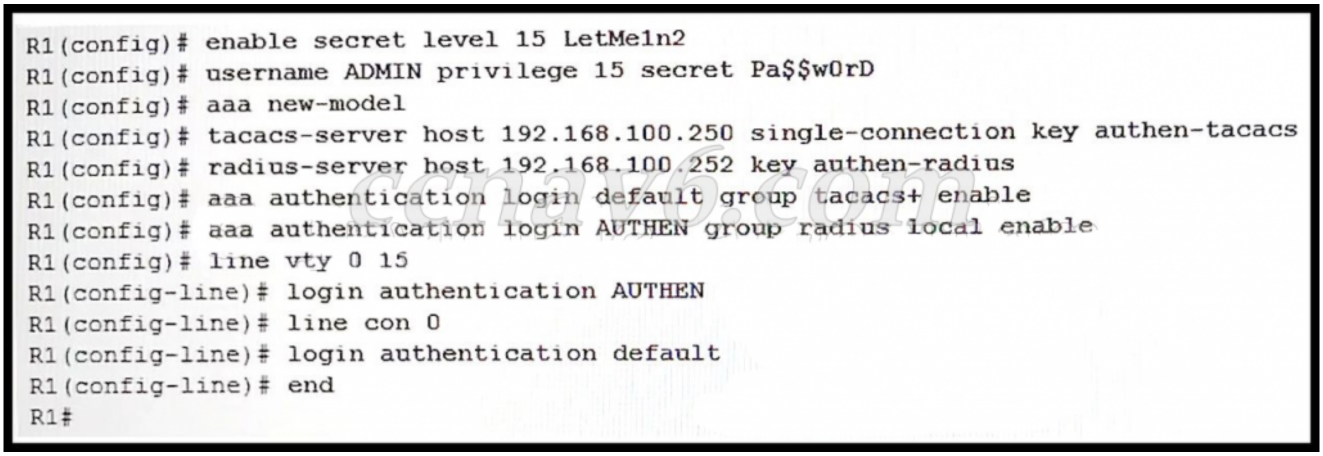
Explanation: Control plane traffic such as ARP messages or routing protocol advertisements are generated by a network device in order to support network operations. Routing protocol authentication provides an extra measure of security to authenticate the source of routing updates. Encrypting remote access connections, utilizing the NTP protocol, and using AAA, are all measures implemented to secure management plane traffic.

2. What is the one major difference between local AAA authentication and using the login local command when configuring device access authentication?

- **Local AAA authentication provides a way to configure backup methods of authentication, but login local does not.**
- The login local command requires the administrator to manually configure the usernames and passwords, but local AAA authentication does not.
- Local AAA authentication allows more than one user account to be configured, but login local does not.
- The login local command uses local usernames and passwords stored on the router, but local AAA authentication does not.

Explanation: Local AAA authentication works very similar to the login local command, except that it allows you to specify backup authentication methods as well. Both methods require that local usernames and passwords be manually configured on the router.

3. Refer to the exhibit. A network administrator configures AAA authentication on R1. The administrator then tests the configuration by telneting to R1. The ACS servers are configured and running. What will happen if the authentication fails?



```
R1(config)# enable secret level 15 LetMe1n2
R1(config)# username ADMIN privilege 15 secret Pa$$w0rD
R1(config)# aaa new-model
R1(config)# tacacs-server host 192.168.100.250 single-connection key authen-tacacs
R1(config)# radius-server host 192.168.100.252 key authen-radius
R1(config)# aaa authentication login default group tacacs+ enable
R1(config)# aaa authentication login AUTHEN group radius local enable
R1(config)# line vty 0 15
R1(config-line)# login authentication AUTHEN
R1(config-line)# line con 0
R1(config-line)# login authentication default
R1(config-line)# end
R1#
```

- The enable secret password could be used in the next login attempt.
- **The authentication process stops.**
- The username and password of the local user database could be used in the next login attempt.
- The enable secret password and a random username could be used in the next login attempt.

4. What are two tasks that can be accomplished with the Nmap and Zenmap network tools? (Choose two.)

- password recovery
- password auditing
- **identification of Layer 3 protocol support on hosts**
- **TCP and UDP port scanning**
- validation of IT system configuration

Explanation: Nmap is a low-level network scanner that is available to the public and which has the ability to perform port scanning, to identify open TCP and UDP ports, and perform system identification. It can also be used to identify Layer 3 protocols that are running on a system.

5. Which Cisco IOS subcommand is used to compile an IPS signature into memory?

- retired true
- event-action produce-alert
- **retired false**
- event-action deny-attacker-inline

Explanation: The Cisco IOS subcommand **retired** can be used to retire (not to compile into memory) or unretire (compile into memory) individual signatures or a group of signatures that belong to a signature category. The command **retired false** instructs IOS to compile an IPS signature into memory. The command **retired true** instructs IOS not to compile an IPS signature into memory. The commands event-action produce-alert and event-action deny-attacker-inline define the action when an enabled signature is matched.

6. Why are DES keys considered weak keys?

- They are more resource intensive.
- DES weak keys use very long key sizes.
- **They produce identical subkeys.**
- DES weak keys are difficult to manage.

Explanation: Weak keys, whether part of an existing encryption algorithm or manually generated, reveal regularities in encryption. This creates a shortcut by which a hacker can break the encryption. DES has four keys for which encryption is identical to decryption.

7. What is a benefit of using a next-generation firewall rather than a stateful firewall?

- reactive protection against Internet attacks
- **granularity control within applications**
- support of TCP-based packet filtering
- support for logging

Explanation: Stateful and next-generation firewalls provide better log information than packet filtering firewalls. Both stateful and next-generation firewalls defend against spoofing by filtering unwanted traffic. However, next-generation firewalls provide the following benefits over stateful firewalls:
– Granularity control within applications
– Website and application traffic filtering based on site reputation
– Proactive rather than reactive protection from Internet threat
– Enforcement of security policies based on multiple criteria
– Improved performance with NAT, VPN, and stateful inspections
– Integrated IPS

8. What is a result of securing the Cisco IOS image using the Cisco IOS Resilient Configuration feature?

- When the router boots up, the Cisco IOS image is loaded from a secured FTP location.
- **The Cisco IOS image file is not visible in the output of the show flash command.**
- The Cisco IOS image is encrypted and then automatically backed up to the NVRAM.
- The Cisco IOS image is encrypted and then automatically backed up to a TFTP server.

Explanation: When using the Cisco IOS Resilient Configuration feature, a secure copy of the IOS image is stored in flash and is hidden from view and and not included in any directory listings.

9. The corporate security policy dictates that the traffic from the remote-access VPN clients must be separated between trusted traffic that is destined for the corporate subnets and untrusted traffic destined for the public Internet. Which VPN solution should be implemented to ensure compliance with the corporate policy?

- MPLS
- hairpinning
- GRE
- **split tunneling**

Explanation: Hairpinning allows VPN traffic that is received on a single interface to be routed back out that same interface. Split tunneling allows traffic that originates from a remote-access client to be split according to whether the traffic must cross a VPN or the traffic is destined for the public Internet. MPLS and GRE are two types of Layer 3 VPNs.

10. Which two conditions must be met in order for a network administrator to be able to remotely manage multiple ASAs with Cisco ASDM? (Choose two.)

- **The ASAs must all be running the same ASDM version.**
- Each ASA must have the same enable secret password.
- Each ASA must have the same master passphrase enabled.
- The ASAs must be connected to each other through at least one inside interface.
- **ASDM must be run as a local application.**

Explanation: Cisco ASDM is a Java-based GUI tool that makes ASA configuration easier. In order to remotely manage multiple ASAs with Cisco ASDM, each ASA must have the same ASDM version. When ASDM is run as a local application, no browser is required and several ASA devices can be managed.

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

- **ISAKMP SA policy**

- DH groups
- interesting traffic
- transform sets

Explanation: 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

12. What are two benefits of using a ZPF rather than a Classic Firewall? (Choose two.)

- ZPF allows interfaces to be placed into zones for IP inspection.
- **The ZPF is not dependent on ACLs.**
- Multiple inspection actions are used with ZPF.
- **ZPF policies are easy to read and troubleshoot.**
- With ZPF, the router will allow packets unless they are explicitly blocked.

Explanation: There are several benefits of a ZPF:
– It is not dependent on ACLs.
– The router security posture is to block unless explicitly allowed.
– Policies are easy to read and troubleshoot with C3PL.
– One policy affects any given traffic, instead of needing multiple ACLs and inspection actions.

In addition, an interface cannot be simultaneously configured as a security zone member and for IP inspection.

13. Which security policy characteristic defines the purpose of standards?

- step-by-step details regarding methods to deploy company switches
- recommended best practices for placement of all company switches
- **required steps to ensure consistent configuration of all company switches**
- list of suggestions regarding how to quickly configure all company switches

Explanation: Standards help IT staff maintain consistency in the operations of the network. Guidelines are a list of suggestions on how to do things more efficiently and securely. They are similar to standards, but are more flexible and are not usually mandatory. Procedure documents are longer and more detailed than standards and guidelines. Procedure documents include implementation details that usually contain step-by-step instructions and graphics.

14. What algorithm is used to provide data integrity of a message through the use of a calculated hash value?

- RSA
- DH
- AES
- **HMAC**

Explanation: The IPsec framework uses various protocols and algorithms to provide data confidentiality, data integrity, authentication, and secure key exchange. To ensure that data is not intercepted and modified (data integrity), Hashed Message Authentication Code (HMAC) is used. AES is an encryption protocol and provides data confidentiality. DH (Diffie-Hellman) is an algorithm that is used for key exchange. RSA is an algorithm that is used for authentication.

15. On which port should Dynamic ARP Inspection (DAI) be configured on a switch?

- **an uplink port to another switch**
- on any port where DHCP snooping is disabled
- any untrusted port
- access ports only

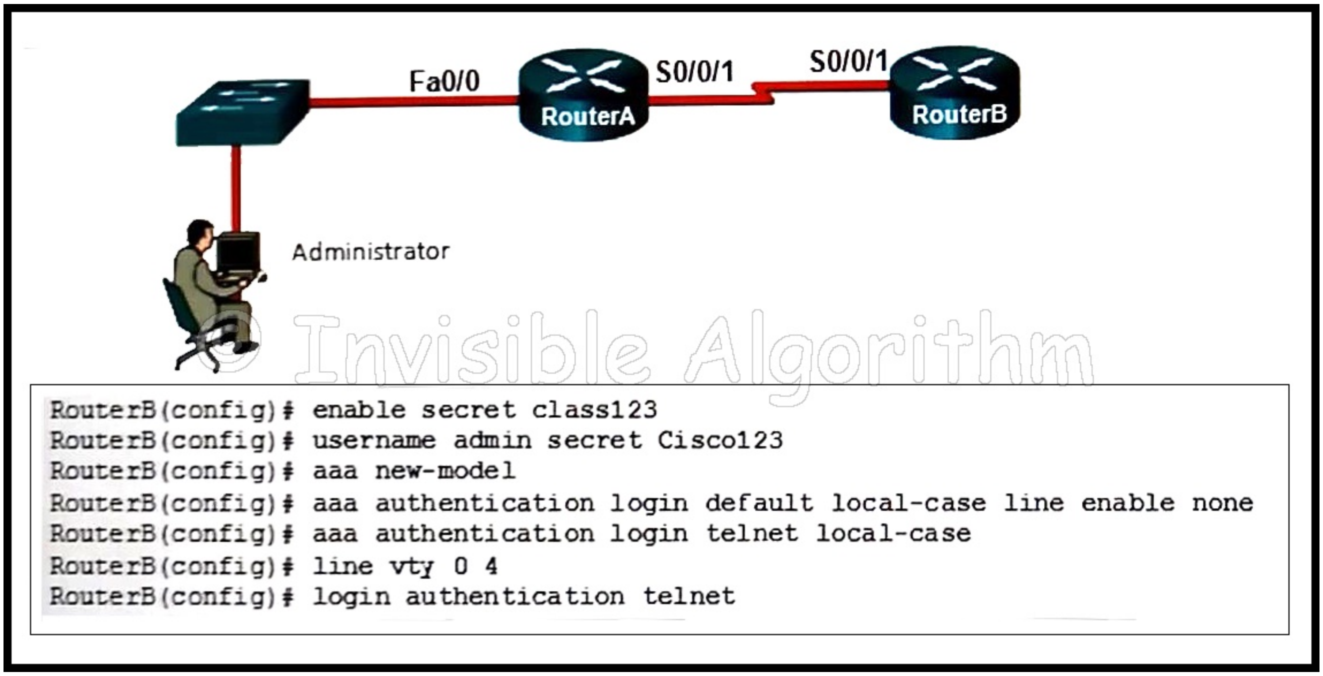
Explanation: DHCP snooping must be enabled on a port where DAI is configured, because DAI requires the DHCP snooping table to operate. Only a trusted interface, such as an uplink port between switches, is configured to implement DAI. All access ports are untrusted.

16. What is a feature of a Cisco IOS Zone-Based Policy Firewall?

- **A router interface can belong to only one zone at a time.**
- Service policies are applied in interface configuration mode.
- Router management interfaces must be manually assigned to the self zone.
- The pass action works in multiple directions.

Explanation: The pass action allows traffic in only one direction. Interfaces automatically become members of the self zone. Interfaces are assigned to a zone in interface configuration mode, but most configuration takes place in global configuration mode and associated submodes. An interface can belong to only one zone at a time.

17. Refer to the exhibit. The administrator can ping the S0/0/1 interface of RouterB but is unable to gain Telnet access to the router by using the password cisco123. What is a possible cause of the problem?



```
RouterB(config)# enable secret class123
RouterB(config)# username admin secret Cisco123
RouterB(config)# aaa new-model
RouterB(config)# aaa authentication login default local-case line enable none
RouterB(config)# aaa authentication login telnet local-case
RouterB(config)# line vty 0 4
RouterB(config)# login authentication telnet
```

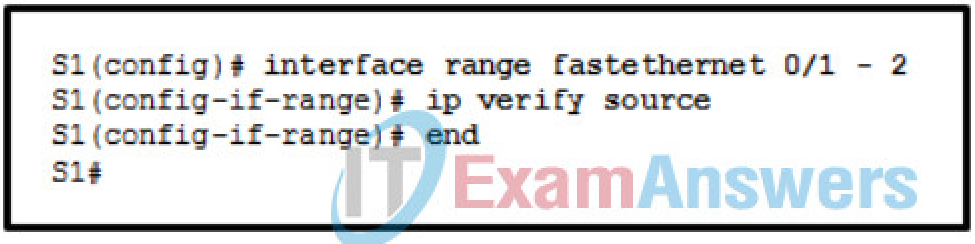
- The Telnet connection between RouterA and RouterB is not working correctly.
- **The password cisco123 is wrong.**
- The administrator does not have enough rights on the PC that is being used.
- The enable password and the Telnet password need to be the same.

Other case:

- AAA authorization is not configured.
- The administrator does not have enough rights on the PC that is being used.
- **The administrator has used the wrong password.**
- The wrong vty lines are configured.

Explanation: To authenticate and log in using a Telnet vty line, the network administrator is required to use the local username and password that has been configured on the local router. This is evidenced by the application of the **aaa authentication login telnet local-case** command. The administrator must use a capital C in Cisco123 to match the applied configuration.

18. Refer to the exhibit. The ip verify source command is applied on untrusted interfaces. Which type of attack is mitigated by using this configuration?

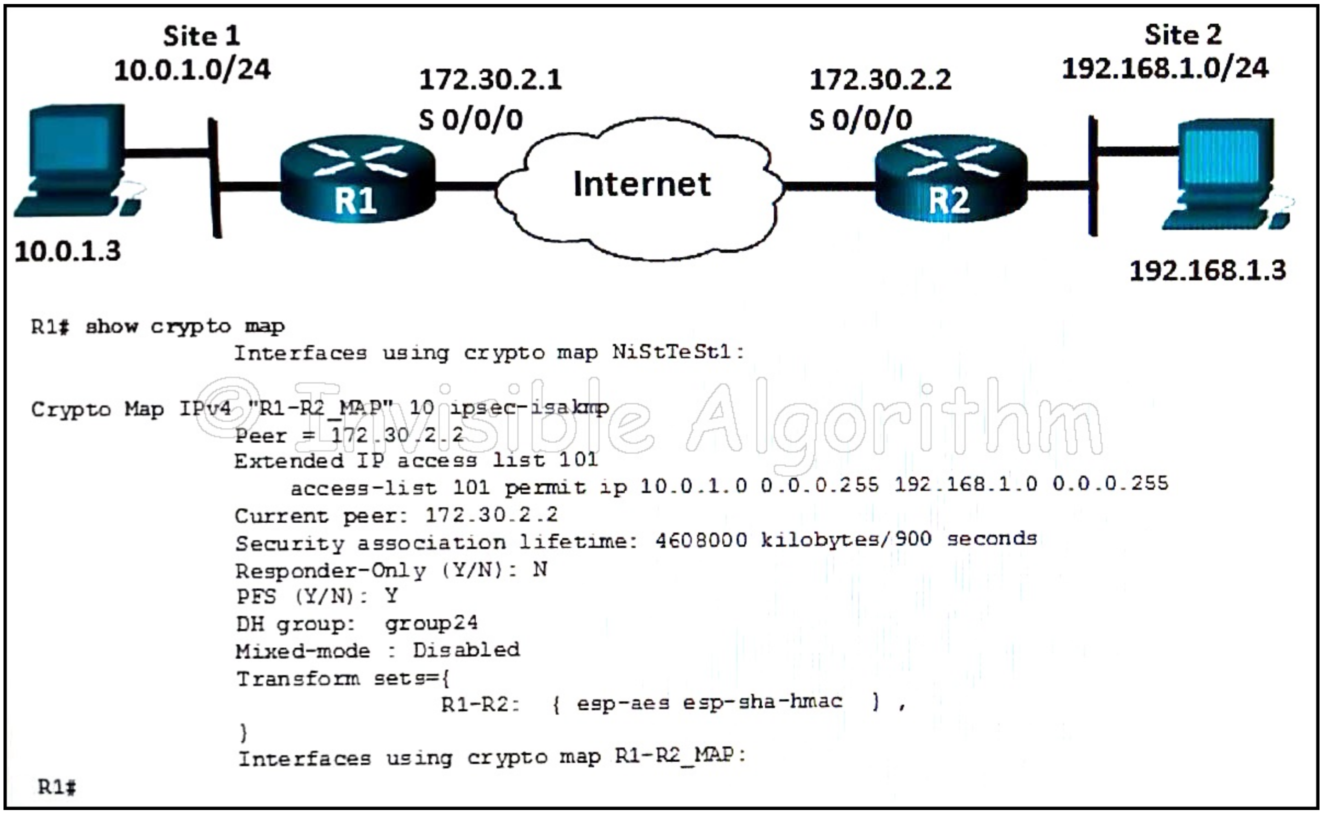


```
S1(config)# interface range fastethernet 0/1 - 2
S1(config-if-range)# ip verify source
S1(config-if-range)# end
S1#
```

- DHCP spoofing
- DHCP starvation
- STP manipulation
- **MAC and IP address spoofing**

Explanation: To protect against MAC and IP address spoofing, apply the IP Source Guard security feature, using the **ip verify source** command, on untrusted ports.

19. Refer to the exhibit. Which conclusion can be made from the show crypto map command output that is shown on R1?



```
R1# show crypto map
                Interfaces using crypto map NiStTeSt1:

Crypto Map IPv4 "R1-R2_MAP" 10 ipsec-isakmp
                Peer = 172.30.2.2
                Extended IP access list 101
                    access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255
                Current peer: 172.30.2.2
                Security association lifetime: 4608000 kilobytes/900 seconds
                Responder-Only (Y/N): N
                PFS (Y/N): Y
                DH group:  group24
                Mixed-mode : Disabled
                Transform sets={
                                R1-R2:  { esp-aes esp-sha-hmac  } ,
                }
                Interfaces using crypto map R1-R2_MAP:
R1#
```

- **The crypto map has not yet been applied to an interface.**
- The current peer IP address should be 172.30.2.1.
- There is a mismatch between the transform sets.
- The tunnel configuration was established and can be tested with extended pings.

Explanation: According to the **show crypto map** command output, all required SAs are in place, but no interface is currently using the crypto map. To complete the tunnel configuration, the crypto map has to be applied to the outbound interface of each router.

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

- **symmetric algorithms**
- hashing algorithms

- asymmetric algorithms
- public key algorithms

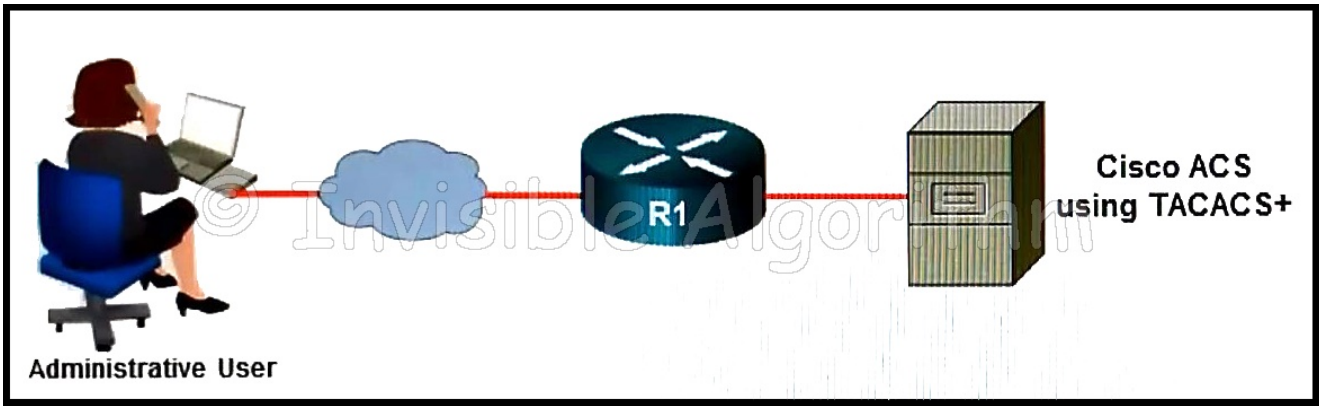
Explanation: Symmetric algorithms use the same key, a secret key, to encrypt and decrypt data. This key must be pre-shared before communication can occur. Asymmetric algorithms require more processing power and overhead on the communicating devices because these keys can be long in order to avoid being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

21. What is an advantage in using a packet filtering firewall versus a high-end firewall appliance?

- **Packet filters perform almost all the tasks of a high-end firewall at a fraction of the cost.**
- Packet filters provide an initial degree of security at the data-link and network layer.
- Packet filters represent a complete firewall solution.
- Packet filters are not susceptible to IP spoofing.

Explanation: There are several advantages of using a packet filtering firewall:
– allows for implementing simple permit or deny rule sets.
– has a low impact on network performance
– is easy to implement, and is supported by most routers
– provides an initial degree of security at the network layer
– performs almost all the tasks of a high-end firewall at a much lower cost

22. Refer to the exhibit. In the network that is shown, which AAA command logs the use of EXEC session commands?



- aaa accounting network start-stop group tacacs+
- aaa accounting network start-stop group radius
- aaa accounting connection start-stop group radius
- aaa accounting exec start-stop group radius
- aaa accounting connection start-stop group tacacs+
- **aaa accounting exec start-stop group tacacs+**

Explanation: The aaa accounting exec start-stop group tacacs+ command is used to configure the router to log the use of EXEC commands.

23. A network administrator enters the single-connection command. What effect does this command have on AAA operation?

- allows a new TCP session to be established for every authorization request
- authorizes connections based on a list of IP addresses configured in an ACL on a Cisco ACS server
- **allows a Cisco ACS server to minimize delay by establishing persistent TCP connections**
- allows the device to establish only a single connection with the AAA-enabled server

Explanation: By default, TACACS+ establishes a new TCP session for every authorization request. This can lead to delays.To improve performance, Cisco Secure ACS supports persistent TCP sessions configured with the **single-connection** command.

24. Which two practices are associated with securing the features and performance of router operating systems? (Choose two.)

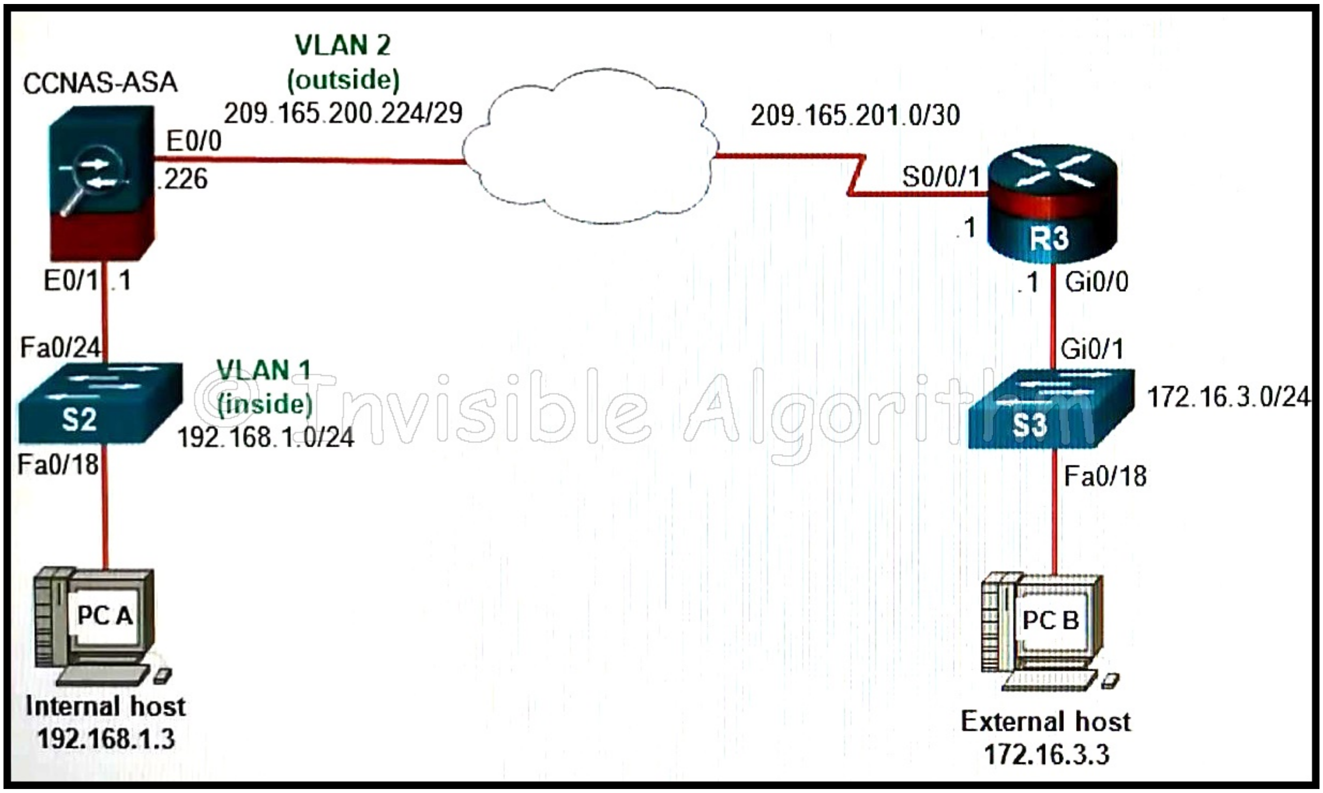
- Install a UPS.
- **Keep a secure copy of router operating system images.**
- **Configure the router with the maximum amount of memory possible.**
- Disable default router services that are not necessary.
- Reduce the number of ports that can be used to access the router.

Explanation: Configuring a router with maximum available memory allows support for the widest range of security services and can help to protect against certain DoS attacks. Secure copies of router operating system images and configuration files provide backups needed for device recovery. Installing a UPS device provides physical security for networking devices but does not affect the security of their operating systems. Disabling unnecessary ports and services is part of the process of router hardening, and does not specifically involve the router operating system.

25. Which statement describes a characteristic of the IKE protocol?

- **It uses UDP port 500 to exchange IKE information between the security gateways.**
- IKE Phase 1 can be implemented in three different modes: main, aggressive, or quick.
- It allows for the transmission of keys directly across a network.
- The purpose of IKE Phase 2 is to negotiate a security association between two IKE peers.

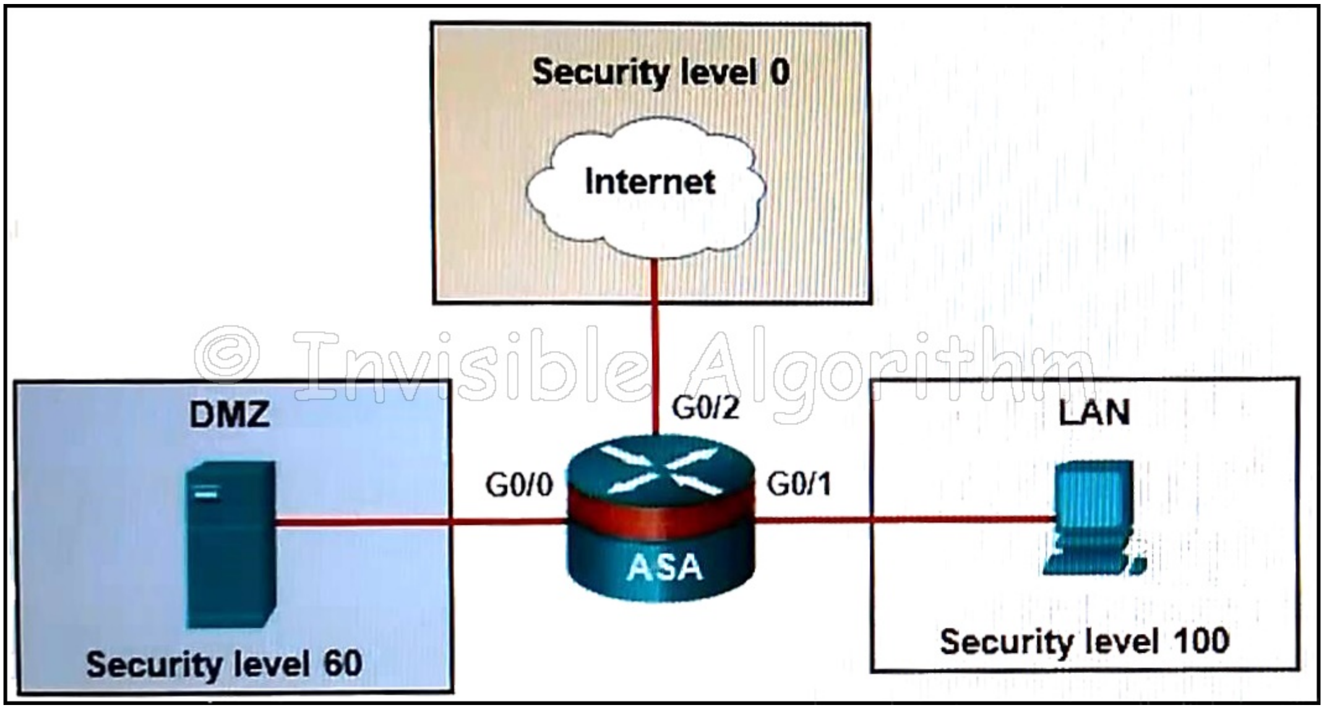
26. Refer to the exhibit. If a network administrator is using ASDM to configure a site-to-site VPN between the CCNAS-ASA and R3, which IP address would the administrator use for the peer IP address textbox on the ASA if data traffic is to be encrypted between the two remote LANs?



- **209.165.201.1**
- 192.168.1.3
- 172.16.3.1
- 172.16.3.3
- 192.168.1.1

Explanation: When ASDM is used to configure an ASA, the peer address is the IP address of the other site for the VPN. In this instance R3 has the outside IP address of 209.165.201.1, so that must be the peer IP address for the ASA. Conversely, R3 will have to be configured with a peer IP address of 209.165.200.226.

27. Refer to the exhibit. Based on the security levels of the interfaces on the ASA, what statement correctly describes the flow of traffic allowed on the interfaces?



- Traffic that is sent from the LAN and the Internet to the DMZ is considered inbound.
- Traffic that is sent from the DMZ and the Internet to the LAN is considered outbound.
- Traffic that is sent from the LAN to the DMZ is considered inbound.
- Traffic that is sent from the LAN to the DMZ is considered is considered inbound.
- **Traffic that is sent from the DMZ and the LAN to the Internet is considered outbound.**

Explanation: When traffic moves from an interface with a higher security level to an interface with a lower security level, it is considered outbound traffic. Conversely, traffic that moves from an interface with a lower security level to an interface with a higher security level is considered inbound traffic.

28. What two assurances does digital signing provide about code that is downloaded from the Internet? (Choose two.)

- The code contains no errors.
- The code contains no viruses.
- **The code has not been modified since it left the software publisher.**
- **The code is authentic and is actually sourced by the publisher.**
- The code was encrypted with both a private and public key.

Explanation: Digitally signing code provides several assurances about the code:
The code is authentic and is actually sourced by the publisher.
The code has not been modified since it left the software publisher.
The publisher undeniably published the code. This provides nonrepudiation of the act of publishing.

29. Which interface option could be set through ASDM for a Cisco ASA?

- default route
- access list
- **VLAN ID**
- NAT/PAT

Explanation: To assign a VLAN number to an interface, choose Configuration > Device Setup > Interfaces and add or select an interface. Choose the Advanced tab to assign a VLAN. Other options that can be assigned to an interface include an IP address, mask, and security level.

30. What are two characteristics of a stateful firewall? (Choose two.)

- **uses connection information maintained in a state table**
- uses static packet filtering techniques
- **analyzes traffic at Layers 3, 4 and 5 of the OSI model**
- uses complex ACLs which can be difficult to configure
- prevents Layer 7 attacks

Explanation: Stateful firewalls are the most versatile and the most common firewall technologies in use. Stateful firewalls provide stateful packet filtering by using connection information maintained in a state table. Stateful filtering is a firewall architecture that is classified at the network layer. It also analyzes traffic at OSI Layers 4 and 5. Stateful firewalls cannot prevent application layer attacks because they do not examine the actual contents of an HTTP connection.

31. What are three characteristics of SIEM? (Choose three.)

- **can be implemented as software or as a service**
- Microsoft port scanning tool designed for Windows
- **examines logs and events from systems and applications to detect security threats**
- **consolidates duplicate event data to minimize the volume of gathered data**
- uses penetration testing to determine most network vulnerabilities
- provides real-time reporting for short-term security event analysis

Explanation: Security Information Event Management (SIEM) is a technology that provides real-time reporting and long-term analysis of security events. SIEM provides the ability to search logs and events from disparate systems or applications to detect threats. SIEM aggregates duplicate events to reduce the volume of event data. SIEM can be implemented as software or as a managed.service. SuperScan is a Microsoft Windows port scanning tool that runs on most versions of Windows.Tools, such as Nmap and SuperScan, can provide effective penetration testing on a network and determine network vulnerabilities while helping to anticipate possible attack mechanisms.

32. Which type of traffic is subject to filtering on an ASA 5505 device?

- public Internet to inside
- public Internet to DMZ
- **inside to DMZ**
- DMZ to inside

Explanation: Filtering only applies to traffic traveling in the direction from a higher security level to a lower security level.

33. Which IDS/IPS signature alarm will look for packets that are destined to or from a particular port?

- honey pot-based
- anomaly-based
- **signature-based**
- policy-based

Explanation: Cisco IDS and IPS sensors can use four types of signature alarms or triggers:

– **Pattern-based detection** – also known as signature-based detection, searches for a specific and pre-defined pattern. In most cases, the pattern is matched to the signature only if the suspect packet is associated with a particular service or destined to or from particular ports.
– **Anomaly-based detection** – also known as profile-based detection, involves first defining a profile of what is considered normal for the network or host. After defining normal activity, the signature triggers an action if excessive activity occurs beyond a specified threshold that is not included in the normal profile.
– **Policy-based detection** – also known as behavior-based detection, is similar to pattern-based detection, but instead of trying to define specific patterns, the administrator defines behaviors that are suspicious based on historical analysis.
– **Honey pot-based detection** – uses a dummy server to attract attacks.

34. Which three actions can the Cisco IOS Firewall IPS feature be configured to take when an intrusion activity is detected? (Choose three.)

- reset UDP connection
- **reset TCP connection**
- **alert**
- isolate

- inoculate
- **drop**

Explanation: In IPS implementation, when a signature detects a matching activity, the signature triggers one or more of these actions:
– Generates an alert
– Logs the activity
– Drops or prevent the activity
– Resets a TCP connection
– Blocks future activity
– Allows the activity

35. Which two protocols can be selected using the Cisco AnyConnect VPN Wizard to protect the traffic inside a VPN tunnel? (Choose two.)

- Telnet
- SSH
- **SSL**
- ESP
- **IPsec**

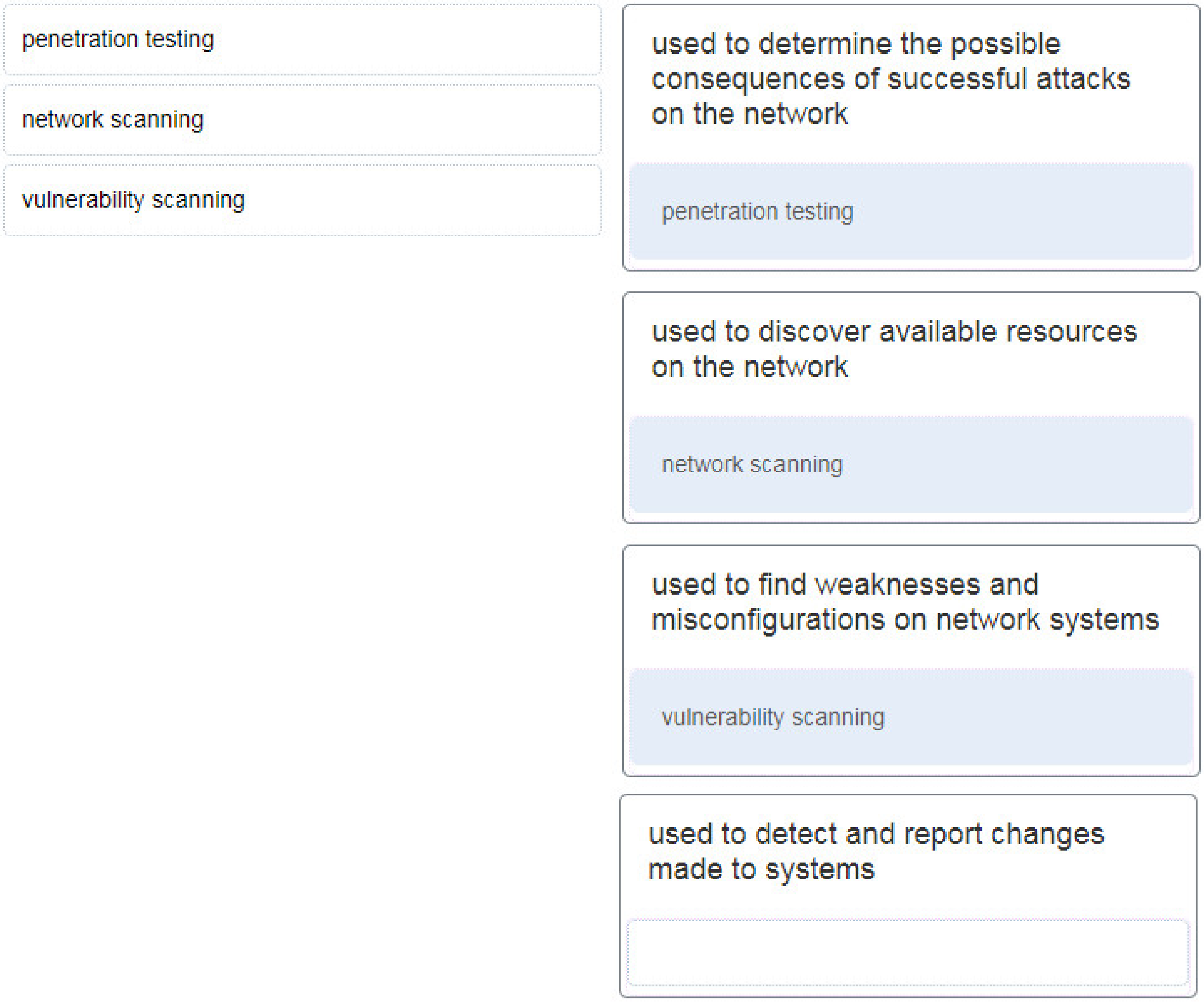
Explanation: When a full tunnel is creating using the Cisco AnyConnect VPN Wizard, the VPN protocols should be selected to protect the traffic inside the tunnel. The VPN protocol choices are SSL and/or IPsec. Otherwise, a third-party certificate can be configured. Initially SSL and IPsec are selected.

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

- When a superview is deleted, the associated CLI views are deleted.
- **A single CLI view can be shared within multiple superviews.**
- A CLI view has a command hierarchy, with higher and lower views.
- Only a superview user can configure a new view and add or remove commands from the existing views.

Explanation: 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.

37. Match the network security testing technique with how it is used to test network security. (Not all options are used)?



penetration testing

network scanning

vulnerability scanning

used to determine the possible consequences of successful attacks on the network

penetration testing

used to discover available resources on the network

network scanning

used to find weaknesses and misconfigurations on network systems

vulnerability scanning

used to detect and report changes made to systems

- Penetration testing = **used to determine the possible consequences of successful attacks on the network**.
- Vulnerability scanning = **used to find weaknesses and misconfigurations on network systems**.
- Network scanning = **used to discover available resources on the network**.

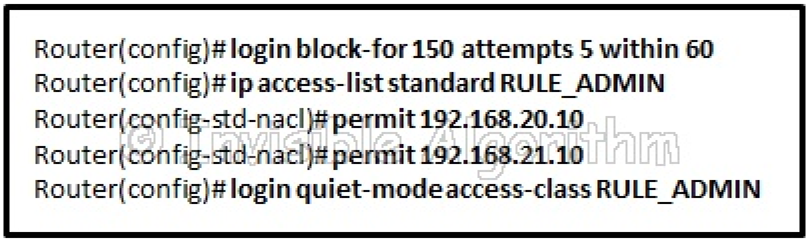
Explanation: Network scanning tools are used to probe network devices, servers and hosts for open TCP or UDP ports. Vulnerability scanning tools are used to discover security weaknesses in a network or computer system. Penetration testing tools are used to determine the possible outcome of a successful attack on a network or computer system.

38. Which statement describes the use of certificate classes in the PKI?

- **A class 5 certificate is more trustworthy than a class 4 certificate.**
- Email security is provided by the vendor, not by a certificate.
- The lower the class number, the more trusted the certificate.
- A vendor must issue only one class of certificates when acting as a CA.

Explanation: The higher the certificate number, the more trustworthy the certificate. Class 1 certificates are for individuals, with a focus on email verification. An enterprise can act as its own CA and implement PKI for internal use. In that situation, the vendor can issue certificates as needed for various purposes.

39. 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
```

- Because the login delay command was not used, a one-minute delay between login attempts is assumed.
- **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.
- These enhancements apply to all types of login connections.

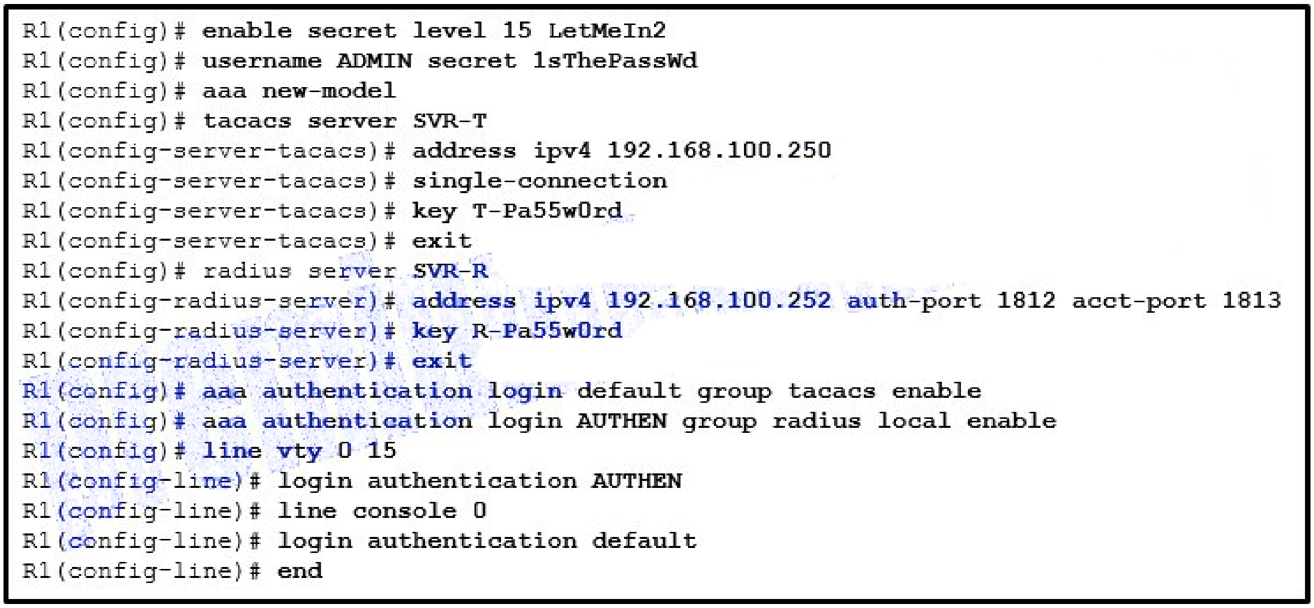
Explanation: When the **login block-for** command is implemented, it automatically invokes a one-second delay between login attempts. The **login block-for** command that is presented means that login will be disabled for 150 seconds, if more than 5 login failures occur within 60 seconds. These enhancements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

40. A company deploys a Cisco ASA with the Cisco CWS connector enabled as the firewall on the border of corporate network. An employee on the internal network is accessing a public website. What should the employee do in order to make sure the web traffic is protected by the Cisco CWS?

- Register the destination website on the Cisco ASA.
- Use the Cisco AnyConnect Secure Mobility Client first.
- **Use a web browser to visit the destination website.**
- First visit a website that is located on a web server in the Cisco CWS infrastructure.

Explanation: Once the connector is enabled on the Cisco ASA device, users on the internal network can connect to the Cisco CWS transparently when they access external websites. The Cisco CWS serves as a proxy for the web access to scan traffic for malware and policy enforcement. Users visit external websites by accessing the URLs directly on the web browsers.

41. Refer to the exhibit. A network administrator configures AAA authentication on router R1. The ACS servers are configured and running. The administrator tests the configuration by telneting to R1. What will happen if the administrator attempts to authenticate through the RADIUS server using incorrect credentials?



```
R1(config)# enable secret level 15 LetMeIn2
R1(config)# username ADMIN secret 1sThePassWd
R1(config)# aaa new-model
R1(config)# tacacs server SVR-T
R1(config-server-tacacs)# address ipv4 192.168.100.250
R1(config-server-tacacs)# single-connection
R1(config-server-tacacs)# key T-Pa55w0rd
R1(config-server-tacacs)# exit
R1(config)# radius server SVR-R
R1(config-radius-server)# address ipv4 192.168.100.252 auth-port 1812 acct-port 1813
R1(config-radius-server)# key R-Pa55w0rd
R1(config-radius-server)# exit
R1(config)# aaa authentication login default group tacacs enable
R1(config)# aaa authentication login AUTHEN group radius local enable
R1(config)# line vty 0 15
R1(config-line)# login authentication AUTHEN
R1(config-line)# line console 0
R1(config-line)# login authentication default
R1(config-line)# end
```

- **The authentication process stops.**
- The enable secret password could be used in the next login attempt.
- The enable secret password and a random username could be used in the next login attempt.
- The username and password of the local user database could be used in the next login attempt.

Explanation: The authentication for Telnet connections is defined by AAA method list AUTHEN. The AUTHEN list defines that the first authentication method is through an ACS server using the RADIUS protocol (or RADIUS server), the second authentication method is to use the local user database, and the third method is to use the enable password. In this scenario, however, because the administrator fails to pass the authentication by the first method, the authentication process stops and no other authentication methods are allowed.

42. What mechanism is used by an ASA 5505 device to allow inspected outbound traffic to return to the originating sender who is on an inside network?

- Network Address Translation
- access control lists
- security zones

- **stateful packet inspection**

Explanation: Stateful packet inspection allows return traffic that is sourced on the outside network to be received by the originating sender on the internal network.

43. Which two end points can be on the other side of an ASA site-to-site VPN configured using ASDM? (Choose two.)

- DSL switch
- Frame Relay switch
- **ISR router**
- **another ASA**
- multilayer switch

Explanation: ASDM supports creating an ASA site-to-site VPN between two ASAs or between an ASA and an ISR router.

44. What Layer 2 attack is mitigated by disabling Dynamic Trunking Protocol?

- DHCP spoofing
- ARP spoofing
- **VLAN hopping**
- ARP poisoning

Explanation: Mitigating a VLAN hopping attack can be done by disabling Dynamic Trunking Protocol (DTP) and by setting the native VLAN of trunk links to VLANs not in use.

45. In an AAA-enabled network, a user issues the configure terminal command from the privileged executive mode of operation. What AAA function is at work if this command is rejected?

- **authorization**
- authentication
- auditing
- accounting

Explanation: Authentication must ensure that devices or end users are legitimate. Authorization is concerned with allowing and disallowing authenticated users access to certain areas and programs on the network. The configure terminal command is rejected because the user is not authorized to execute the command.

46. An organization has configured an IPS solution to use atomic alerts. What type of response will occur when a signature is detected?

- A counter starts and a summary alert is issued when the count reaches a preconfigured number.
- The TCP connection is reset.
- **An alert is triggered each time a signature is detected.**
- The interface that triggered the alert is shutdown.

Explanation: 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. Deny packet and deny flow actions do not automatically cause TCP reset actions to occur. Atomic alerts do not shut down interfaces.

47. What two algorithms can be part of an IPsec policy to provide encryption and hashing to protect interesting traffic? (Choose two.)

- PSK
- DH
- RSA
- **AES**
- **SHA**

Explanation: The IPsec framework uses various protocols and algorithms to provide data confidentiality, data integrity, authentication, and secure key exchange. Two algorithms that can be used within an IPsec policy to protect interesting traffic are AES, which is an encryption protocol, and SHA, which is a hashing algorithm.

48. Fill in the blank.?

A stateful signature is also known as a **Composite?** signature.

49. Why is hashing cryptographically stronger compared to a cyclical redundancy check (CRC)?

- Hashes are never sent in plain text.
- It is easy to generate data with the same CRC.
- It is difficult to generate data with the same CRC.
- **It is virtually impossible for two different sets of data to calculate the same hash output.**
- Hashing always uses a 128-bit digest, whereas a CRC can be variable length.

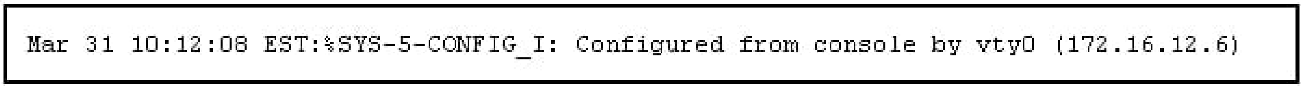
Explanation: When assuring integrity with CRC values, it is easy to generate data with the same CRC. With hash functions, it is computationally infeasible for two different sets of data to come up with the same hash output. Hashing can use many bit values depending on the algorithm. These characteristics make hashing much stronger cryptographically.

50. A network analyst wants to monitor the activity of all new interns. Which type of security testing would track when the interns sign on and sign off the network?

- vulnerability scanning
- password cracking
- network scanning
- **integrity checker**

Explanation: An integrity checking system can report login and logout activities. Network scanning can detect user names, groups, and shared resources by scanning listening TCP ports. Password cracking is used to test and detect weak passwords. Vulnerability scanning can detect potential weaknesses in a system, such as misconfigurations, default passwords, or DoS attack targets.

51. Refer to the exhibit. What two pieces of information can be gathered from the generated message? (Choose two.)



```
Mar 31 10:12:08 EST:%SYS-5-CONFIG_I: Configured from console by vty0 (172.16.12.6)
```

- **This message is a level five notification message.**
- **This message indicates that service timestamps have been globally enabled.**
- This message indicates that enhanced security was configured on the vty ports.
- This message appeared because a major error occurred that requires immediate action.
- This message appeared because a minor error occurred that requires further investigation.

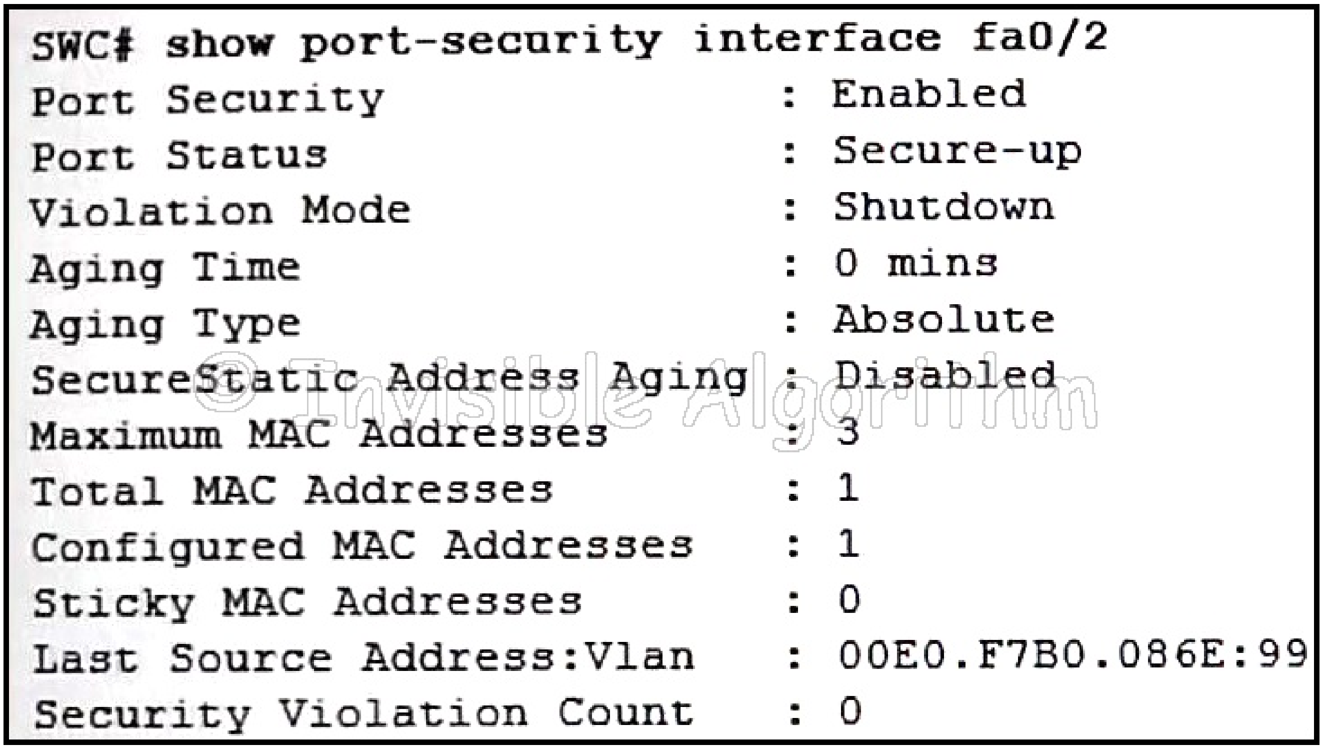
Explanation: A Cisco router log message consists for three parts:
1) the timestamp
2) the log message and severity level
3) the message text

52. What is required for auto detection and negotiation of NAT when establishing a VPN link?

- Both VPN end devices must be configured for NAT.
- No ACLs can be applied on either VPN end device.
- **Both VPN end devices must be NAT-T capable.**
- Both VPN end devices must be using IPv6.

Explanation: Establishing a VPN between two sites has been a challenge when NAT is involved at either end of the tunnel. The enhanced version of original IKE, IKE version 2, now supports NAT Traversal (NAT-T). NAT-T has the ability to encapsulate ESP packets inside UDP. During IKE version 2 Phase 1, the VPN end devices can detect whether the other device is NAT-T capable and whether either device is connecting through a NAT-enabled device in order to establish the tunnel.

53. Refer to the exhibit. The network administrator is configuring the port security feature on switch SWC. The administrator issued the command show port-security interface fa 0/2 to verify the configuration. What can be concluded from the output that is shown? (Choose three.)



```
SWC# show port-security interface fa0/2
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode               : Shutdown
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 3
Total MAC Addresses          : 1
Configured MAC Addresses     : 1
Sticky MAC Addresses         : 0
Last Source Address:Vlan     : 00E0.F7B0.086E:99
Security Violation Count     : 0
```

- Three security violations have been detected on this interface.
- **This port is currently up.**
- The port is configured as a trunk link.
- **Security violations will cause this port to shut down immediately.**
- There is no device currently connected to this port.
- **The switch port mode for this interface is access mode.**

Explanation: Because the security violation count is at 0, no violation has occurred. The system shows that 3 MAC addresses are allowed on port fa0/2, but only one has been configured and no sticky MAC addresses have been learned. The port is up because of the port status of secure-up. The violation mode is what happens when an unauthorized device is attached to the port. A port must be in access mode in order to activate and use port security.

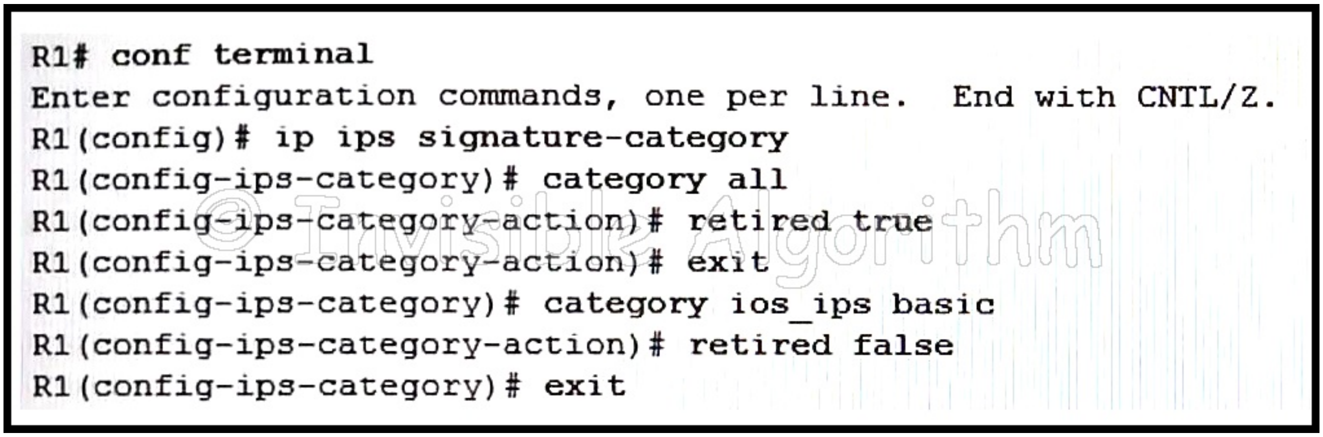
54. In which two instances will traffic be denied as it crosses the ASA 5505 device? (Choose two.)

- traffic originating from the inside network going to the DMZ network

- traffic originating from the inside network going to the outside network
- traffic originating from the outside network going to the DMZ network
- **traffic originating from the DMZ network going to the inside network**
- **traffic originating from the outside network going to the inside network**

Explanation: When an ASA 5505 device is being utilized, traffic is denied as it travels from a lower security zone to a higher security zone. The highest security zone is the internal network, the DMZ is usually the next highest, and the outside network is the lowest. Traffic is only allowed to move from a lower security level to a higher if it is in response to originating traffic within the higher security zone.

55. Refer to the exhibit. Based on the configuration that is shown, which statement is true about the IPS signature category?



```
R1# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category)# exit
```

- Only signatures in the ios_ips advanced category will be compiled into memory for scanning.
- All signatures categories will be compiled into memory for scanning, but only those signatures within the ios ips advanced
- category will be used for scanning purposes.
- All signature categories will be compiled into memory for scanning, but only those signatures in the ios_ips basic category will be used for scanning purposes.
- **Only signatures in the ios_ips basic category will be compiled into memory for scanning.**

Explanation: When a signature category is marked as retired by using the command **retired true**, then the IPS does not compile signatures that are part of that category into memory for inspection (scanning). The **retired false** command does the opposite. This command instructs the IPS to include those signatures that are part of that category into memory for scanning.

56. Which two ports can send and receive Layer 2 traffic from a community port on a PVLAN? (Choose two.)

- community ports belonging to other communities
- **promiscuous ports**
- isolated ports within the same community
- PVLAN edge protected ports
- **community ports belonging to the same community**

Explanation: Community ports can send and receive information with ports within the same community, or with a promiscuous port. Isolated ports can only communicate with promiscuous ports. Promiscuous ports can talk to all interfaces. PVLAN edge protected ports only forward traffic through a Layer 3 device to other protected ports.

57. What is a feature of the TACACS+ protocol?

- It utilizes UDP to provide more efficient packet transfer.
- It combines authentication and authorization as one process.
- **It encrypts the entire body of the packet for more secure communications.**
- It hides passwords during transmission using PAP and sends the rest of the packet in plaintext.

Explanation: TACACS+ has the following features:separates authentication and authorization encrypts all communication uses TCP port 49

58. Which security measure is best used to limit the success of a reconnaissance attack from within a campus area network?

- Implement restrictions on the use of ICMP echo-reply messages.
- Implement a firewall at the edge of the network.
- Implement access lists on the border router.
- **Implement encryption for sensitive traffic.**

Explanation: The implementation of an access list may provide extra security by permitting denying a flow of traffic, but it will not provide a direct response to limit the success of the attack. The implementation of a firewall on the network edge may prevent reconnaissance attacks from the Internet, but attacks within the local network are not prevented. By implementing restrictions on the sending of ICMP echo-reply messages within a local network, devices may not respond to ping messages, but port scans are not prevented and clear-text data sent on the network are still vulnerable. The best security measure is to encrypt as much network traffic as possible, both user data and network management traffic.

59. What is the benefit of the network-based IPS (NIPS) over host-based IPS (HIPS) deployment models?

- NIPS provides individual host protection.
- NIPS relies on centrally managed software agents.

- **NIPS monitors network segments.**
- NIPS monitors all operations within an operating system.

Explanation: The network-based IPS (NIPS) is deployed in a network to monitor traffic in the network. Different from the host-based IPS (HIPS), NIPS does not provides protection to specific individual hosts. The operation of NIPS does not rely on the operating system of individual hosts nor centrally managed software agents.

60. What represents a best practice concerning discovery protocols such as CDP and LLDP on network devices?

- LLDP on network devices?
- Enable CDP on edge devices, and enable LLDP on interior devices.
- Use the default router settings for CDP and LLDP.
- Use the open standard LLDP rather than CDP.
- **Disable both protocols on all interfaces where they are not required.**

Explanation: Both discovery protocols can provide hackers with sensitive network information. They should not be enabled on edge devices, and should be disabled globally or on a per-interface basis if not required. CDP is enabled by default.

61. What function is provided by the Tripwire network security tool?

- password recovery
- **security policy compliance**
- IDS signature development
- logging of security events

Explanation: Tripwire is a network security testing tool that can be used by administrators to assess if network devices are compliant with company network security policies.

62. What is the function of a policy map configuration when an ASA firewall is being configured?

- **binding class maps with actions**
- identifying interesting traffic
- binding a service policy to an interface
- using ACLs to match traffic

Explanation: Policy maps are used to bind class maps with actions Class maps are configured to identify Layer 3 and 4 traffic. Service policies are configured to attach the policy map to an interface.

63. If a network administrator wants to track the usage of FTP services, which keyword or keywords should be added to the aaa accounting command?

- exec default
- connection
- **exec**
- network

64. What is indicated by the use of the local-case keyword in a local AAA authentication configuration command sequence?

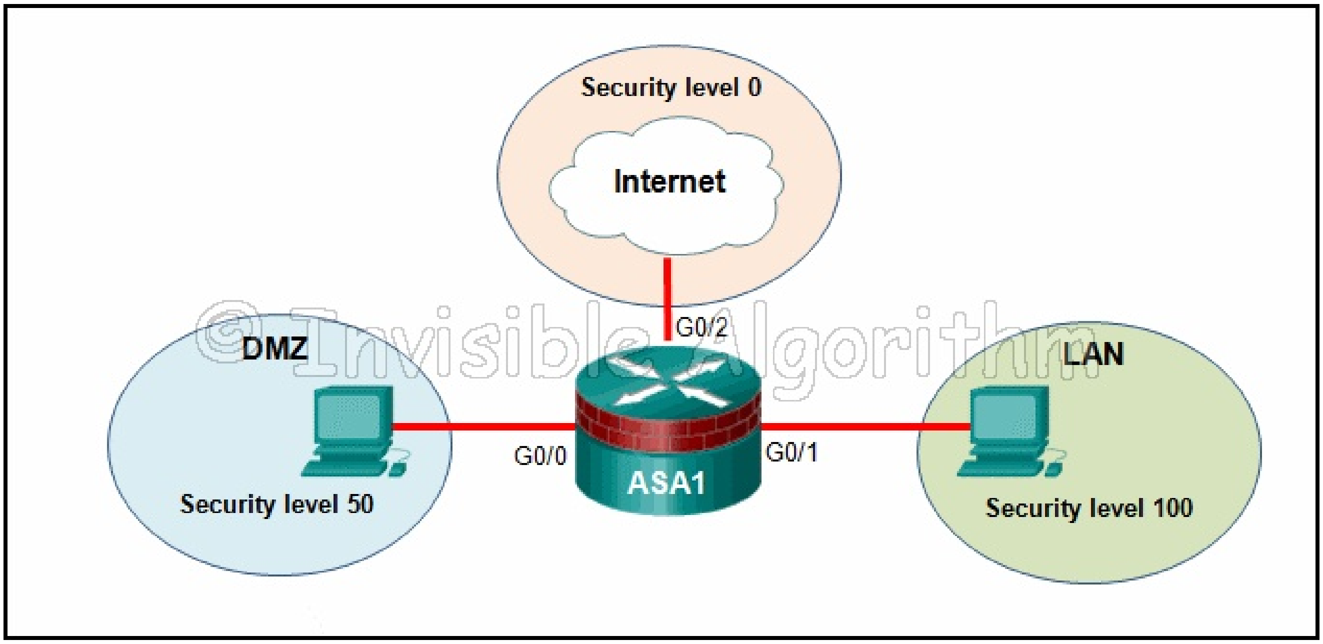
- that user access is limited to vty terminal lines
- that passwords and usernames are case-sensitive
- that AAA is enabled globally on the router
- that a default local database AAA authentication is applied to all lines

Explanation: The use of the local-case keyword means that the authentication is case-sensitive. It does not enable or apply the AAA configuration to router interfaces or lines.

65. What is the purpose of a local username database if multiple ACS servers are configured to provide authentication services?

- Clients using internet services are authenticated by ACS servers, whereas local clients are authenticated through a local username database.
- Each ACS server must be configured with a local username database in order to provide authentication services.
- A local username database is required when creating a method list for the default login.
- **A local username database provides redundancy if ACS servers become unreachable. [adef]**

66. 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 Internet and LAN can access the DMZ.
- Traffic from the Internet and DMZ can access the LAN.
- Traffic from the Internet can access both the DMZ and the LAN.
- **Traffic from the LAN and DMZ can access the Internet.**

Explanation: 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.

67. What are two reasons to enable OSPF routing protocol authentication on a network? (Choose two.)

- to ensure more efficient routing
- **to prevent data traffic from being redirected and then discarded**
- to ensure faster network convergence
- **to prevent redirection of data traffic to an insecure link?**
- to provide data security through encryption

Explanation: The reason to configure OSPF authentication is to mitigate against routing protocol attacks like redirection of data traffic to an insecure link, and redirection of data traffic to discard it. OSPF authentication does not provide faster network convergence, more efficient routing, or encryption of data traffic.

68. A security awareness session is best suited for which topic?

- required steps when reporting a breach of security
- the primary purpose and use of password policies
- steps used to configure automatic Windows updates
- **how to install and maintain virus protection?**

69. What provides both secure segmentation and threat defense in a Secure Data Center solution?

- Cisco Security Manager software
- AAA server
- **Adaptive Security Appliance**
- intrusion prevention system

70. Which two features should be configured on end-user ports in order to prevent STP manipulation attacks(Choose two.)?

- root guard
- UDLD
- **BPDU guard**
- loop guard
- PortFast

71. What is a characteristic of most modern viruses?

- They are usually found attached to online games.
- **Email viruses are the most common type of them.**
- They replicate themselves and locate new targets.
- They are responsible for some of the most destructive internet attacks.

72. Which statement describes a characteristic of the Security Device Event Exchange (SDEE) feature supported by the Cisco IOS IPS?

- **SDEE notification is disabled by default. It does not receive and process events from the Cisco IOS IPS unless SDEE notification is enabled.**
- SDEE notification is enabled by default. It receives and processes events from the Cisco IOS IPS and sends them to a syslog server.
- SDEE notification is enabled by default. It receives and processes events from the Cisco IOS IPS and stores them in a buffer.
- SDEE notification is disabled by default. It starts receiving and processing events from the Cisco IOS IPS as soon as an attack signature is detected.

73. Which network security tool allows an administrator to test and detect weak passwords?

- **L0phtcrack**

- Tripwire
- Nessus
- Metasploit

Explanation: L0phtcrack can be used to perform password auditing and recovery. Nessus can scan systems for software vulnerabilities. Metasploit is used for penetration testing and IDS signature development. Tripwire is used to assess if network devices are compliant with network security policies.

74. What is an advantage of logging packets that are seen by an IPS device?

- Packets from the IP address that triggered the logging are denied once logging begins.
- **Administrators can decide what actions can be taken in the future.**
- Administrators can use the brief summary that is generated to quickly determine how to handle the packets.
- Attacker packets can be stopped immediately.

75. Which procedure is recommended to mitigate the chances of ARP spoofing?

- **Enable DHCP snooping on selected VLANs.**
- Enable IP Source Guard on trusted ports.
- Enable DAI on the management VLAN.
- Enable port security globally.

Explanation: To mitigate the chances of ARP spoofing, these procedures are recommended:
– Implement protection against DHCP spoofing by enabling DHCP snooping globally.
– Enable DHCP snooping on selected VLANs.
– Enable DAI on selected VLANs.
– Configure trusted interfaces for DHCP snooping and ARP inspection. Untrusted ports are configured by default.

76. In a server-based AAA implementation, which protocol will allow the router to successfully communicate with the AAA server?

- **RADIUS**
- 802.1x
- SSH
- TACACS

Explanation: With a server-based method, the router accesses a central AAA server using either the Remote Authentication Dial-In User (RADIUS) or Terminal Access Controller Access Control System (TACACS+) protocol. SSH is a protocol used for remote login. 802.1x is a protocol used in port-based authentication. TACACS is a legacy protocol and is no longer used.

77. A network technician is attempting to resolve problems with the NAT configuration on anASA. The technician generates a ping from an inside host to an outside host. Whichcommand verifies that addresses are being translated on the ASA?

- show ip nat translation
- show running-config
- **show xlate**
- show ip address

78. What are three components of a technical security policy? (Choose three.)

- human resource policy
- **acceptable use policy**
- **remote access policy**
- identity policy
- **network access policy**
- end user policy

79. Which security policy outlines the overall security goals for managers and technical personnel within an organization and includes the consequences of noncompliance with the policy?

- end-user policy
- application policy
- **governing policy**
- technical policy

80. What is a secure configuration option for remote access to a network device?

- Configure 802.1x.
- Configure Telnet.
- **Configure SSH.**
- Configure an ACL and apply it to the VTY lines.

81. On what switch ports should BPDU guard be enabled to enhance STP stability?

- only ports that attach to a neighboring switch
- **all PortFast-enabled ports**
- all trunk ports that are not root ports

- only ports that are elected as designated ports

Explanation: End-user ports should connect only to end-user devices and not to other switches. To prevent a switch from being added to the network on an end-user port, BPDU guard will immediately put the port into the error disabled state if a BPDU is received on that port. However, if PortFast is not configured on an end-user port, BPDU guard is not activated on that port.

82. Which feature is specific to the Security Plus upgrade license of an ASA 5505 and provides increased availability?

- **redundant ISP connections**
- routed mode
- transparent mode
- stateful packet inspection

83. A company deploys a hub-and-spoke VPN topology where the security appliance is the hub and the remote VPN networks are the spokes. Which VPN method should be used in order for one spoke to communicate with another spoke through the single public interface of the security appliance?

- split tunneling
- MPLS
- GRE
- **Hairpinning**

84. What are two drawbacks in assigning user privilege levels on a Cisco router? (Choose two.)

- Privilege levels must be set to permit access control to specific device interfaces, ports, or slots.
- **Assigning a command with multiple keywords allows access to all commands using those keywords.**
- Only a root user can add or remove commands.
- **Commands from a lower level are always executable at a higher level.**
- AAA must be enabled.

Explanation: Privilege levels may not provide desired flexibility and specificity because higher levels always inherit commands from lower levels, and commands with multiple keywords give the user access to all commands available for each keyword. Privilege levels cannot specify access control to interfaces, ports, or slots. AAA is not required to set privilege levels, but is required in order to create role-based views. The role of root user does not exist in privilege levels.

85. Which two types of hackers are typically classified as grey hat hackers? (Choose two.)

- script kiddies
- **vulnerability brokers**
- cyber criminals
- state-sponsored hackers
- **hacktivists**

Explanation: Grey hat hackers may do unethical or illegal things, but not for personal gain or to cause damage. Hacktivists use their hacking as a form of political or social protest, and vulnerability brokers hack to uncover weaknesses and report them to vendors. Depending on the perspective one possesses, state-sponsored hackers are either white hat or black hat operators. Script kiddies create hacking scripts to cause damage or disruption. Cyber criminals use hacking to obtain financial gain by illegal means.

86. What is the default preconfigured interface for the outside network on a Cisco ASA 5505?

- **VLAN 2**
- Ethernet 0/2
- Ethernet 0/1
- VLAN 1

87. A user successfully logs in to a corporate network via a VPN connection. Which part of the AAA process records that a certain user performed a specific operation at a particular date and time?

- authentication
- **accounting**
- access
- authorization

Explanation: The three parts of the AAA process are authentication, authorization, and accounting. The accounting function records information such as who logged in, when the user logged in and out, and what the user did with network resources.

88. What determines which switch becomes the STP root bridge for a given VLAN?

- **the lowest bridge ID**
- the highest MAC address
- the highest priority
- the lowest IP address

Explanation: STP uses a root bridge as a central point for all spanning tree calculations. To select a root bridge, STP conducts an election process. All switches in the broadcast domain participate in the election process. The switch with the lowest bridge ID, or BID, is elected as the root bridge. The BID is made up of a priority value, an extended system ID, and the MAC address of the switch.

89. What is a function of the GRE protocol?

- to configure the set of encryption and hashing algorithms that will be used to transform the data sent through the IPsec tunnel
- to provide encryption through the IPsec tunnel
- to configure the IPsec tunnel lifetime
- **to encapsulate multiple OSI Layer 3 protocol packet types inside an IP tunnel**

Explanation: The transform set is the set of encryption and hashing algorithms that will be used to transform the data sent through the IPsec tunnel. GRE supports multiprotocol tunneling. It can encapsulate multiple OSI Layer 3 protocol packet types inside an IP tunnel. Routing protocols that are used across the tunnel enable dynamic exchange of routing information in the virtual network. GRE does not provide encryption.

90. What is used to determine the root bridge when the priority of the switches are the same?

- the MAC address with the highest hexadecimal value
- the lowest ip address
- **the layer 2 address with the lowest hexadecimal value**
- the highest BID

91. What is algorithm-type to protect the data in transit?
Hashing algorithm

92. What type of ACL is designed for use in the configuration of an ASA to support filtering for clientless SSL VPN's?

- **Webtype**
- Standard
- Ethertype
- Extended

Explanation: Webtype access lists are used in ASA configurations to support filtering for clientless SSL VPNs. Standard ACLs used in ASA configurations typically identify destination IPs in OSPF routes. Extended ACLs are the most common type of ACL, and are not specifically designed for use with clientless SSL VPNs. Ethertype ACLs can only be configured if the ASA is running in transparent mode.

93. The following authentication configuration is applied to a router.
aaa authentication login default tacacs+ local enable none
Several days later the TACACS+ server goes off-line. Which method will be used to authenticate users?

- **none**
- manually configured vty line password
- local username/password database
- default

94. A security technician is evaluating a new operations security proposal designed to limit access to all servers. What is an advantage of using network security testing to evaluate the new proposal?

- **Network security testing proactively evaluates the effectiveness of the proposal before any real threat occurs.**
- Network security testing is most effective when deploying new security proposals.
- Network security testing is specifically designed to evaluate administrative tasks involving server and workstation access.
- Network security testing is simple because it requires just one test to evaluate the new proposal.

Explanation: Network security testing can evaluate the effectiveness of an operations security solution without having to wait for a real threat to take place. However, this type of testing should be conducted periodically, versus just once. It is effective to evaluate many different tasks when it is conducted during both the implementation and operational stages.

95. Which security implementation will provide management plane protection for a network device?

- **role-based access control**
- antispoofing
- routing protocol authentication
- access control lists

Explanation: Management plane processes typically use protocols such as Telnet and SSH. Role-based access control ensures that only authorized users have management privileges. ACLs perform packet filtering and antispoofing functions on the data plane to secure packets generated by users. Routing protocol authentication on the control plane ensures that a router does not accept false routing updates from neighbor routers.

96. What two new features are offered by Cisco ASA 5500-X with FirePOWER service when compared with the original ASA 5500 series? (Choose two.)

- IPsec VPN
- **advanced malware protection**
- security level settings
- stateful firewall
- **application control and URL filtering**

Explanation: The Cisco ASA 5500-X series with FirePOWER service merges the ASA 5500 series appliances with some new features such as advanced malware protection as well as application control and URL filtering. The stateful firewall, IPsec VPN, and security level settings are functions common to both ASA 5500 and ASA 5500-X series devices.

97. Which two statements describe the 8 Ethernet ports in the backplane of a Cisco ASA 5506-X device? (Choose two.)

- **These ports all require IP addresses.**
- They all can be configured as routed ports or switch ports.
- **They are all routed ports.**
- Port 1 is a routed port and the rest are switch ports.
- Three of them are routed ports and 5 of them are switch ports.

Explanation: Unlike the ASA 5505, the ASA 5506-X does not use switch ports. All Ethernet ports in the backplane are routed and require IP addresses.

98. An administrator workstation connects to a switch that connects to the Fa0/0 port of RouterA. RouterA connects to RouterB through serial interfaces labeled S0/0/1 on both routers. The following configuration is applied to RouterB.

```
RouterB(config)# enable secret class123
RouterB(config)# username admin secret Cisco123
RouterB(config)# aaa new-model
RouterB(config)# aaa authentication login default local-case line enable none
RouterB(config)# aaa authentication login telnet local-case
RouterB(config)# line vty 0 4
RouterB(config)# login authentication telnet
```

Refer to the exhibit. The administrator can ping the S0/0/1 interface of RouterB but is unable to gain Telnet access to the router by using the password cisco123. What is a possible cause of the problem?

- The wrong vty lines are configured.
- AAA authorization is not configured.
- The administrator has used the wrong password.

- The administrator does not have enough rights on the PC that is being used.
- Navigation Ba

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

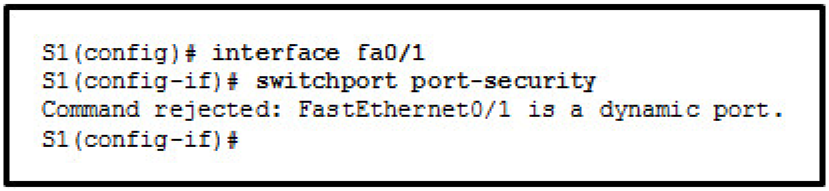
```
Router(config)# privilege exec level 14 show ip route
Router(config)# enable algorithm-type scrypt secret level 14 cisco-level-10
Router(config)# username ADMIN privilege 14 algorithm-type scrypt secret cisco-level-
10
```

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

- The user can only execute the subcommands under the **show ip route**command.
- **The user can execute all subcommands under the show ip interfaces command.**
- The user can issue all commands because this privilege level can execute all Cisco IOS commands.
- The user can issue the **ip route**command.
- **The user can issue the show version command.**

Explanation: 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**.

100. Refer to the exhibit. The administrator wants to enable port security on an interface on switch S1, but the command was rejected. Which conclusion can be drawn?



```
S1(config)# interface fa0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)#
```

- The interface must be initially configured with the switchport mode trunk command.
- The interface needs to be configured initially with an IP address.
- The interface needs to be previously configured with the no shutdown command.
- **The interface must be initially configured with the switchport mode access command.**

Explanation: To enable port security, use the switchport port-security interface configuration command on an access port. By default, Layer 2 switch ports are set to dynamic auto (trunking on); therefore, the port must be initially configured as an access port before port security can be enabled.