**[Updated Constantly]**

**HERE**

## CCNA Security v2.0 Final 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. **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

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.

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

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

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.

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

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.

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***

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.***

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

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.

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

14. **What algorithm is used to provide data integrity of a message through the use of a calculated hash value?**
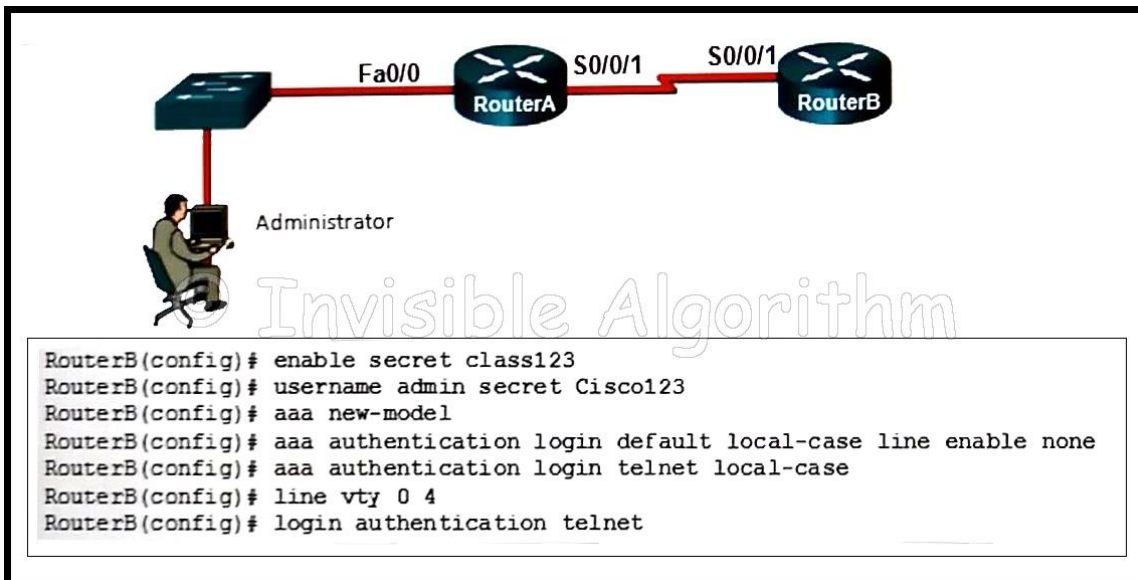    - RSA
    - DH
    - AES
    - **HMAC***

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

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.

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.

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***

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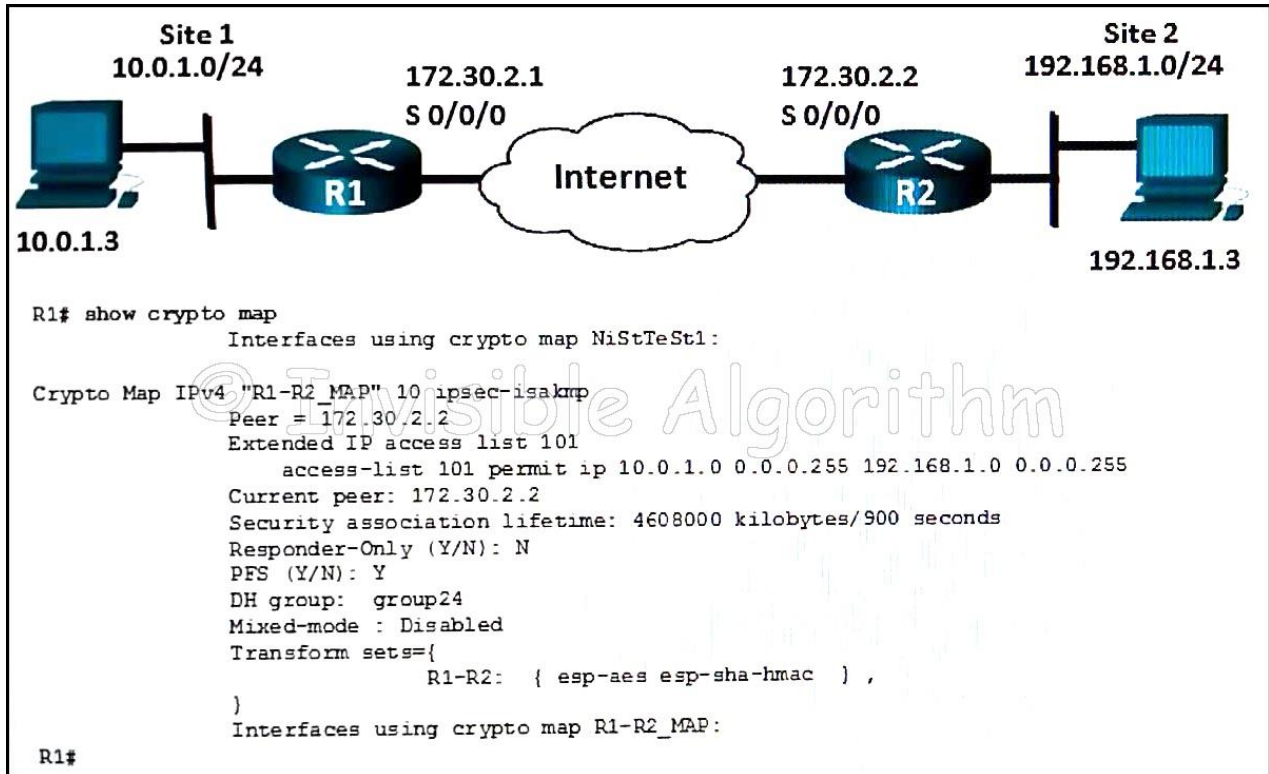


- **The crypto map has not yet been applied to an interface.***
- The current peer IP address should be 172.30.2.1.
- There is a mismatch between the transform sets.
- The tunnel configuration was established and can be tested with extended pings.

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

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.

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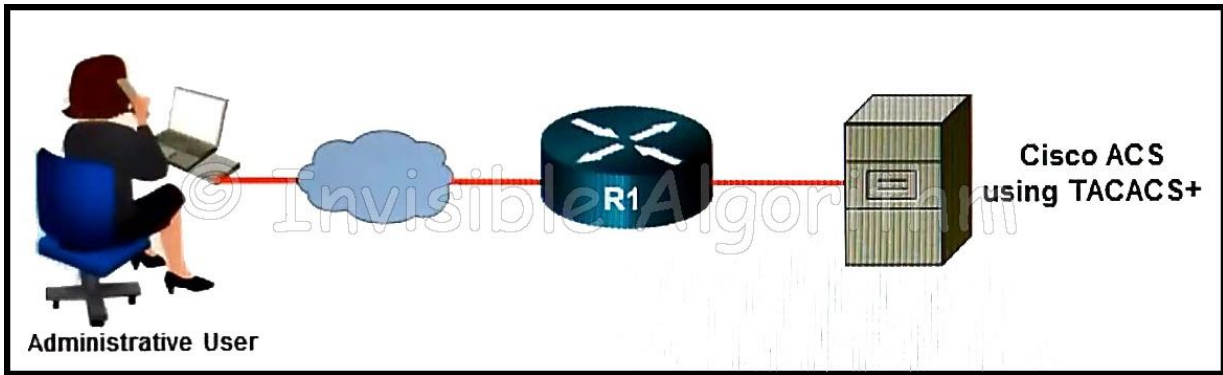


- aaa accounting network start-stop group tacacs+
- aaa accounting network start-stop group radius
- aaa accounting connection start-stop group radius
- aaa accounting exec start-stop group radius
- aaa accounting connection start-stop group tacacs+
- **aaa accounting exec start-stop group tacacs+***

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

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.

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?**
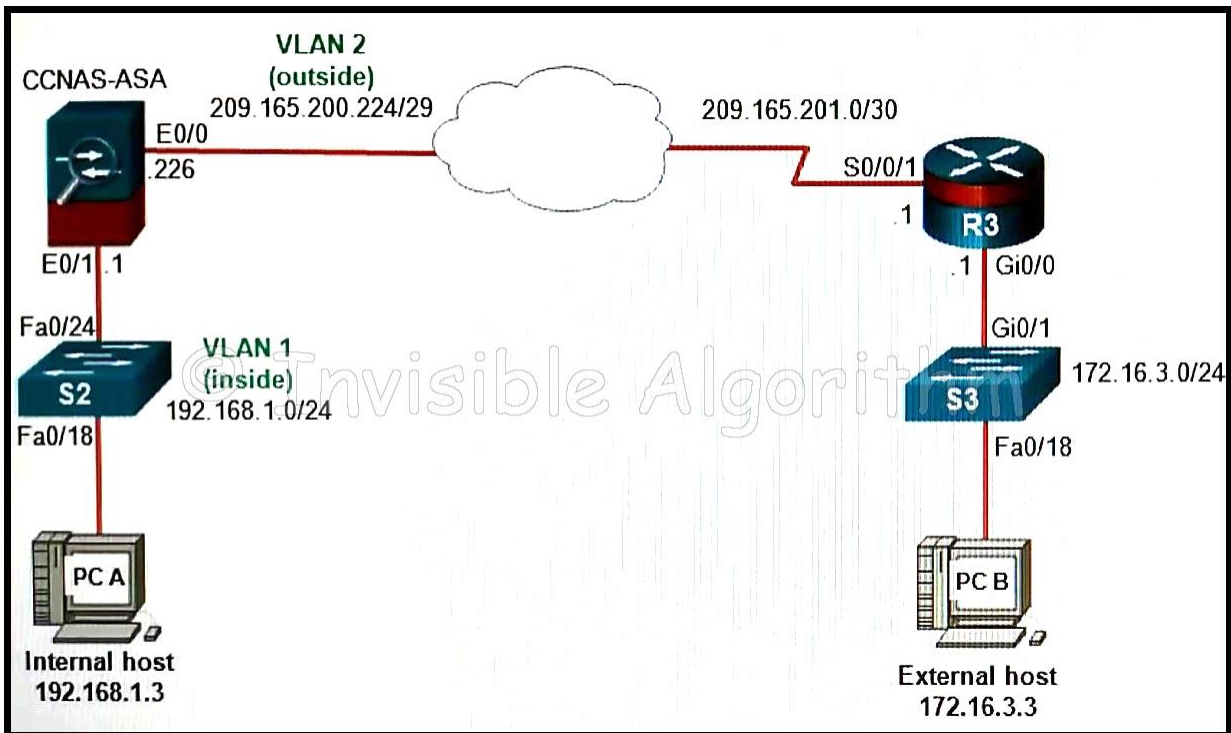


- **209.165.201.1***
- 192.168.1.3
- 172.16.3.1
- 172.16.3.3
- 192.168.1.1

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?**
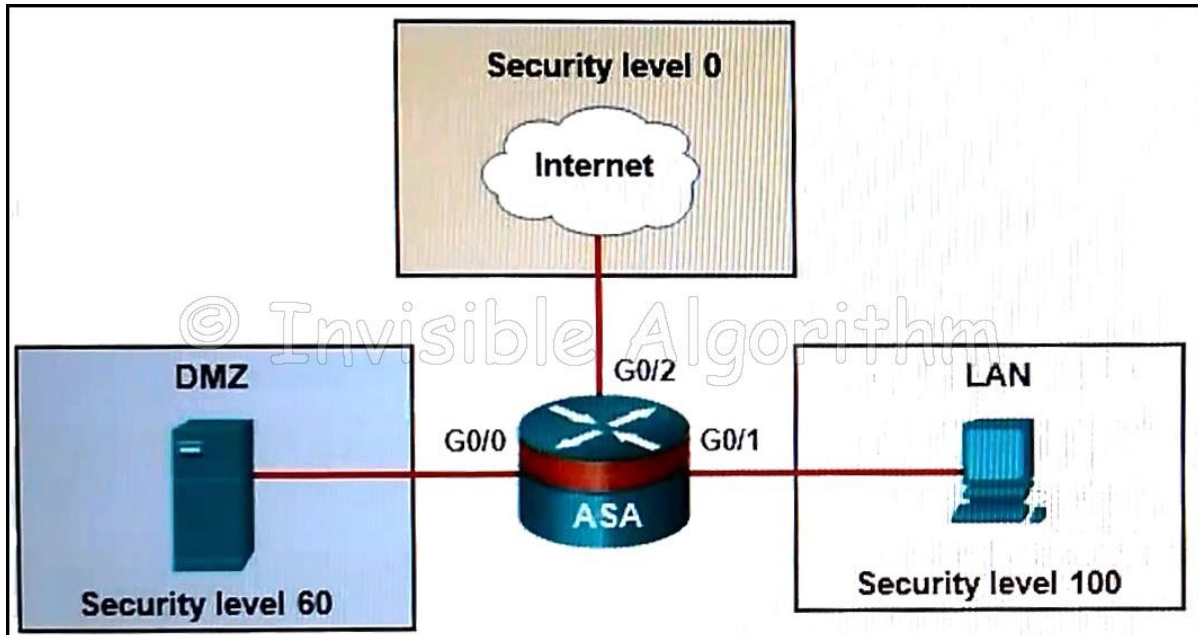


- ▪ Traffic that is sent from the LAN and the Internet to the DMZ is considered inbound.
- ▪ Traffic that is sent from the DMZ and the Internet to the LAN is considered outbound.
- ▪ Traffic that is sent from the LAN to the DMZ is considered is considered inbound.
- ▪ **Traffic that is sent from the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

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.

29. **Which interface option could be set through ASDM for a Cisco ASA?**
- ▪ default route
- ▪ access list
- ▪ **VLAN ID***
- ▪ NAT/PAT

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

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

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

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

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***

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***

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.

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



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

| penetration testing | | used to determine the possible consequences of successful attacks on the network |
| network scanning | | used to discover available resources on the network |
| vulnerability scanning | | used to find weaknesses and misconfigurations on network systems |
| | | 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***.

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.

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.

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.

41. **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 execute all subcommands under the show ip interfaces command.
   - **The user can issue the show version command.***
   - **The user can only execute the subcommands under the show ip route 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.

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***

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

44. **What Layer 2 attack is mitigated by disabling Dynamic Trunking Protocol?**
    - DHCP spoofing
    - ARP spoofing
    - **VLAN hopping***
    - ARP poisoning

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

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.

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***

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 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.

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***

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.

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.

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. [adef]

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***

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.***

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***

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.

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.***

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

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.***

61. **What function is provided by the Tripwire network security tool?**
   - password recovery
   - **security policy compliance***
   - IDS signature development
   - logging of security events

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

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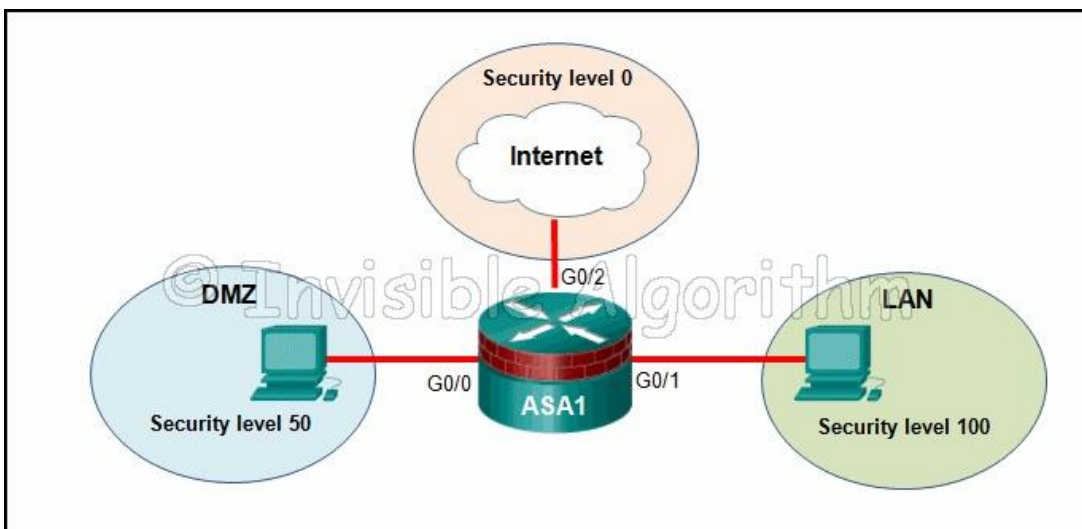


   - Traffic from the Internet and LAN can access the DMZ.
   - Traffic from the Internet and DMZ can access the LAN.

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

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

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

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.

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

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

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.

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***

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

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

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***

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

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.

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

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