[Updated Constantly]

HERE

CCNA Security v2.0 Practice 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 three areas of router security must be maintained to secure an edge router at the network perimeter? (Choose three.)**
   - **physical security***
   - flash security
   - remote access security
   - **operating system security***
   - zone isolation
   - **router hardening***

   There are three areas of router security to maintain:
   1) physical security
   2) router hardening
   3) operating system security

2. **What is the purpose of AAA accounting?**
   - to prove users are who they say they are
   - to determine which operations the user can perform
   - to determine which resources the user can access
   - **to collect and report data usage***

   AAA accounting collects and reports usage data. This data can be used for such purposes as auditing or billing. AAA authentication is the process of verifying users are who they say they are. AAA authorization is what the users can and cannot do on the network after they are authenticated.

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

- **AAA***
- IPsec

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

4. **Which statement accurately describes Cisco IOS Zone-Based Policy Firewall operation?**
   - **The pass action works in only one direction.**
   - Service policies are applied in interface configuration mode.
   - A router interface can belong to multiple zones.
   - Router management interfaces must be manually assigned to the self zone.
5. **Which two statements describe the use of asymmetric algorithms? (Choose two.)**
   - Public and private keys may be used interchangeably.
   - If a public key is used to encrypt the data, a public key must be used to decrypt the data.
   - **If a private key is used to encrypt the data, a public key must be used to decrypt the data.***
   - **If a public key is used to encrypt the data, a private key must be used to decrypt the data.***
   - If a private key is used to encrypt the data, a private key must be used to decrypt the data.

Asymmetric algorithms use two keys: a public key and a private key. Both keys are capable of the encryption process, but the complementary matched key is required for decryption. If a public key encrypts the data, the matching private key decrypts the data. The opposite is also true. If a private key encrypts the data, the corresponding public key decrypts the data.

6. **Refer to the exhibit. Based on the output generated by the show monitor session 1 command, how will SPAN operate on the switch?**

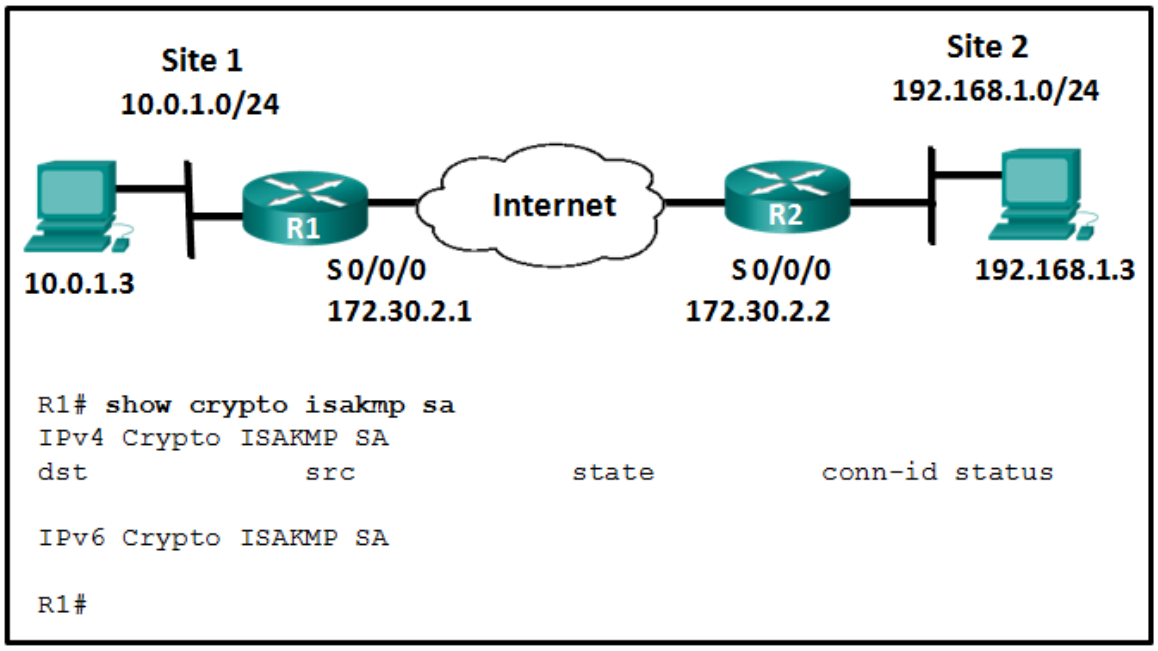
```
S1# show monitor session 1
Session 1
------------
Type                          : Local Session
Source VLANs                  :
    RX Only                   : 10
    TX Only                   : 20
Destination Ports             : Fa0/1
    Encapsulation             : Native
         Ingress              : Disabled
```

- **All traffic received on VLAN 10 or transmitted from VLAN 20 is forwarded to FastEthernet 0/1.***
- Native VLAN traffic transmitted from VLAN 10 or received on VLAN 20 is forwarded to FastEthernet 0/1.
- All traffic transmitted from VLAN 10 or received on VLAN 20 is forwarded to FastEthernet 0/1.
- Native VLAN traffic received on VLAN 10 or transmitted from VLAN 20 is forwarded to FastEthernet 0/1.

The show monitor session command is used to verify how SPAN is configured (what ports are involved in the traffic mirroring)

7. **Refer to the exhibit. The ISAKMP policy for the IKE Phase 1 tunnel was configured, but the tunnel does not yet exist. Which action should be taken next before IKE Phase 1**

negotiations can begin?



- Configure the set of encryption and hashing algorithms that will be used to transform the data sent through the IPsec tunnel.
- Bind the transform set with the rest of the IPsec policy in a crypto map.
- Configure the IPsec tunnel lifetime.
- **Configure an ACL to define interesting traffic.***

Although the ISAKMP policy for the IKE Phase 1 tunnel is configured, the tunnel does not yet exist as verified with the show crypto isakmp sa command. Interesting traffic must be detected before IKE Phase 1 negotiations can begin. To define interesting traffic, each router has to be configured with an ACL to permit traffic from the local LAN to the remote LAN.

8. **What ports can receive forwarded traffic from an isolated port that is part of a PVLAN?**
   - other isolated ports and community ports
   - **only promiscuous ports***
   - all other ports within the same community
   - only isolated ports

PVLANs are used to provide Layer 2 isolation between ports within the same broadcast domain. The level of isolation can be specified
with three types of PVLAN ports:
Promiscuous ports that can forward traffic to all other ports
Isolated ports that can only forward traffic to promiscuous ports
Community ports that can forward traffic to other community ports and promiscuous ports

9. **What is the next step in the establishment of an IPsec VPN after IKE Phase 1 is complete?**
   - negotiation of the ISAKMP policy
   - **negotiation of the IPsec SA policy***
   - detection of interesting traffic
   - authentication of peers

   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

10. **What is an advantage of HIPS that is not provided by IDS?**
    - **HIPS protects critical system resources and monitors operating system processes.***
    - HIPS deploys sensors at network entry points and protects critical network segments.
    - HIPS provides quick analysis of events through detailed logging.
    - HIPS monitors network processes and protects critical files.

    Network-based IDS (NIDS) sensors are typically deployed in offline mode. They do not protect individual hosts. Host-based IPS (HIPS) is software installed on a single host to monitor and analyze suspicious activity. It can monitor and protect operating system and critical system processes that are specific to that host. HIPS can be thought of as a combination of antivirus software, antimalware software, and a firewall.

11. **Which interface setting can be configured in ASDM through the Device Setup tab?**
    - port-security
    - EtherChannel
    - NAT
    - **security level***

    In the Device Setup tab, the ASA Layer 3 interfaces can be created, edited, or deleted. Name, security level, and IP address are some of the settings that can be configured on an interface. There is no NAT, port security, or EtherChannel configuration in this tab.

12. **A security technician uses an asymmetric algorithm to encrypt messages with a private key and then forwards that data to another technician. What key must be used to decrypt this data?**
    - The public key of the receiver.

- **The public key of the sender.***
- The private key of the receiver.
- The private key of the sender.

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

13. **On what switch ports should PortFast be enabled to enhance STP stability?**
    - only ports that are elected as designated ports
    - only ports that attach to a neighboring switch
    - all trunk ports that are not root ports
    - **all end-user ports***

PortFast will immediately bring an interface configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states. If configured on a trunk link, immediately transitioning to the forwarding state could lead to the formation of Layer 2 loops.

14. **What is the function of the Hashed Message Authentication Code (HMAC) algorithm in setting up an IPsec VPN?**
    - authenticates the IPsec peers
    - **guarantees message integrity***
    - protects IPsec keys during session negotiation
    - creates a secure channel for key negotiation

The IPsec framework uses various protocols and algorithms to provide data confidentiality, data integrity, authentication, and secure key exchange. The Hashed Message Authentication Code (HMAC) is a data integrity algorithm that uses a hash value to guarantee the integrity of a message.

15. **What are three characteristics of the RADIUS protocol? (Choose three.)**
    - utilizes TCP port 49
    - **is an open IETF standard AAA protocol***
    - **uses UDP ports for authentication and accounting***
    - **is widely used in VOIP and 802.1X implementations***
    - separates authentication and authorization processes
    - encrypts the entire body of the packet

RADIUS is an open-standard AAA protocol using UDP port 1645 or 1812 for authentication and UDP port 1646 or 1813 for accounting. It combines authentication and authorization into

one process; thus, a password is encrypted for transmission while the rest of the packet will be sent in plain text. RADIUS offers the expedited service and more comprehensive accounting desired by remote-access providers but provides lower security and less potential for customization than TACACS+.

16. **A network administrator is configuring an AAA server to manage TACACS+ authentication. What are two attributes of TACACS+ authentication? (Choose two.)**
    - UDP port 1645
    - encryption for only the password of a user
    - **encryption for all communication***
    - TCP port 40
    - single process for authentication and authorization
    - **separate processes for authentication and authorization***

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

17. **What technology is used to separate physical interfaces on the ASA 5505 device into different security zones?**
    - Network Address Translation
    - quality of service
    - **virtual local-area networks***
    - access control lists

    For an ASA 5505, common deployments use a specific VLAN with a higher security level for an inside network and a separate VLAN with a lower security level for the outside network.

18. **How are Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) components used conjunctively?**
    - The IDS blocks offending traffic and the IPS verifies that offending traffic was blocked.
    - The IPS will send alert messages when the IDS sends traffic through that is marked as malicious.
    - The IPS will block all traffic that the IDS does not mark as legitimate.
    - **The IDS will send alert messages about “gray area” traffic while the IPS will block malicious traffic.***

    IDS sensors are typically deployed in offline mode. Although they do not stop the triggered packets immediately, they have no impact on network performance and hence can be

configured to identify a broader scope of activities. IPS sensors can be configured to perform a packet drop to stop the trigger packet. However, because they are deployed inline, inspection of heavy traffic flow could have a negative impact on network performance. IDS and IPS technologies can complement each other. For example, an IDS can be implemented to validate IPS operation because the IDS can be configured for deeper packet inspection offline. This allows the IPS to focus on fewer but more critical traffic patterns inline.

19. **What is the result of a DHCP starvation attack?**
    - **Legitimate clients are unable to lease IP addresses.***
    - The IP addresses assigned to legitimate clients are hijacked.
    - The attacker provides incorrect DNS and default gateway information to clients.
    - Clients receive IP address assignments from a rogue DHCP server.

    DCHP starvation attacks are launched by an attacker with the intent to create a DoS for DHCP clients. To accomplish this goal, the attacker uses a tool that sends many DHCPDISCOVER messages to lease the entire pool of available IP addresses, thus denying them to legitimate hosts.

20. **Which router component determines the number of signatures and engines that can be supported in an IPS implementation?**
    - USB availability
    - **available memory***
    - number of interfaces
    - CPU speed

    The number of signatures and engines that can be adequately supported depends on the amount of available memory .

21. **What algorithm is used with IPsec to provide data confidentiality?**
    - **AES***
    - RSA
    - MD5
    - Diffie-Hellman
    - SHA

    The IPsec framework uses various protocols and algorithms to provide data confidentiality, data integrity, authentication, and secure key exchange. Two popular algorithms that are used to ensure that data is not intercepted and modified (data integrity) are MD5 and SHA. 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.

22. **When configuring SSH on a router to implement secure network management, a network engineer has issued the login local and transport input ssh line vty commands. What three additional configuration actions have to be performed to complete the SSH configuration? (Choose three.)**
    - **Create a valid local username and password database.***
    - **Generate the asymmetric RSA keys.***
    - Set the user privilege levels.
    - Configure role-based CLI access.
    - **Configure the correct IP domain name.***
    - Manually enable SSH after the RSA keys are generated.

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

23. **What can be used as an alternative to HMAC?**
    - SHA
    - MD5
    - symmetric encryption algorithms
    - **digital signatures***

    Both HMAC and digital signatures are used to guarantee that messages are authentic. MD5 and SHA are considered legacy algorithms that should be avoided because they have security flaws. Encryption algorithms ensure data confidentiality rather than authentication.

24. **How can DHCP spoofing attacks be mitigated?**
    - by disabling DTP negotiations on nontrunking ports
    - by implementing port security
    - by the application of the ip verify source command to untrusted ports
    - **by implementing DHCP snooping on trusted ports***

    One of the procedures to prevent a VLAN hopping attack is to disable DTP (auto trunking) negotiations on nontrunking ports. DHCP spoofing attacks can be mitigated by using DHCP snooping on trusted ports. The ip verify source interface configuration command is used to enable IP Source Guard on untrusted ports to protect against MAC and IP address spoofing.

25. **A network administrator is configuring an AAA server to manage RADIUS authentication. Which two features are included in RADIUS authentication? (Choose two.)**
    - **single process for authentication and authorization***

- **hidden passwords during transmission***
- encryption for only the data
- encryption for all communication
- separate processes for authentication and authorization

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

26. **A syslog server has received the message shown.**
***Mar 1 00:07:18.783: %SYS-5-CONFIG_I: Configured from console by vty0 (172.16.45.1)**
What can be determined from the syslog message?

- The message is a normal notification and should not be reviewed.
- **The message informs the administrator that a user with an IP address of 172.16.45.1 configured this device remotely.***
- The message is a Log_Alert notification message.
- The message description displays that the console line was accessed locally.

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

27. **What is the default preconfigured security level for the outside network interface on a Cisco ASA 5505?**

- 255
- 1
- **0***
- 100

By default the Cisco ASA ships with two interfaces preconfigured: interface VLAN 1 for the inside network with a security level of 100 and VLAN 2 for outside network with a security level of 0.

28. **What term describes a set of rules used by an IDS or IPS to detect typical intrusion activity?**

- definition
- trigger
- **signature***
- event file

A signature is a set of rules that an IDS and an IPS use to detect typical intrusion activity, such as DoS attacks. These signatures uniquely identify specific worms, viruses, protocol anomalies, and malicious traffic.

29. **Which type of VLAN-hopping attack may be prevented by designating an unused VLAN as the native VLAN?**
    - **VLAN double-tagging***
    - DHCP starvation
    - DHCP spoofing
    - DTP spoofing

Spoofing DTP messages forces a switch into trunking mode as part of a VLAN-hopping attack, but VLAN double tagging works even if trunk ports are disabled. Changing the native VLAN from the default to an unused VLAN reduces the possibility of this type of attack. DHCP spoofing and DHCP starvation exploit vulnerabilities in the DHCP message exchange.

30. **Which statement describes the Cisco Cloud Web Security?**
    - It is a secure web server specifically designed for cloud computing.
    - **It is a cloud-based security service to scan traffic for malware and policy enforcement.***
    - It is an advanced firewall solution to guard web servers against security threats.
    - It is a security appliance that provides an all-in-one solution for securing and controlling web traffic.

The Cisco Cloud Web Security (CWS) is a cloud-based security service that uses web proxies in the Cisco cloud environment to scan traffic for malware and policy enforcement. It is not a firewall or web server solution. The Cisco Web Security Appliance (WSA) combines multiple security solutions to provide an all-in-one solution on a single platform to address the challenges of securing and controlling web traffic.

31. **Why is Diffie-Hellman algorithm typically avoided for encrypting data?**
    - DH runs too quickly to be implemented with a high level of security.
    - Most data traffic is encrypted using asymmetrical algorithms.
    - **The large numbers used by DH make it too slow for bulk data transfers.***
    - DH requires a shared key which is easily exchanged between sender and receiver.

Diffie-Hellman (DH) is an asymmetric mathematical algorithm that is too slow for encrypting large amounts of data. The longer key length and complexity of DH make it ideal for generating the keys used by symmetric algorithms. Symmetric algorithms typically encrypt the data, whereas DH creates the keys they use.

32. **What information does the SIEM network security management tool provide to network administrators?**
    - **real time reporting and analysis of security events***
    - assessment of system security configurations
    - a map of network systems and services
    - detection of open TCP and UDP ports

    SIEM, which is a combination of Security Information Management and Security Event Management products, is used for forensic analysis and provides real-time reporting of security events.

33. **What can be configured as part of a network object?**
    - interface type
    - **IP address and mask***
    - upper layer protocol
    - source and destination MAC address

    There are two types of objects that can be configured on the Cisco ASA 5505: network objects and service objects. Network objects can be configured with an IP address and mask. Service objects can be configured with a protocol or port ranges.

34. **A user complains about not being able to gain access to the network. What command would be used by the network administrator to determine which AAA method list is being used for this particular user as the user logs on?**
    - debug aaa accounting
    - debug aaa authorization
    - **debug aaa authentication***
    - debug aaa protocol

    In the debug aaa authenticationcommand output, to quickly identify which method list is being used, look for the GETUSER and GETPASS status messages.

35. **What is a limitation to using OOB management on a large enterprise network?**
    - Production traffic shares the network with management traffic.
    - Terminal servers can have direct console connections to user devices needing management.
    - OOB management requires the creation of VPNs.
    - **All devices appear to be attached to a single management network.***

    OOB management provides a dedicated management network without production traffic. Devices within that network, such as terminal servers, have direct console access for

management purposes. Because in-band management runs over the production network, secure tunnels or VPNs may be needed. Failures on the production network may not be communicated to the OOB network administrator because the OOB management network may not be affected

36. **A company deploys a network-based IPS. Which statement describes a false negative alarm that is issued by the IPS sensor?**
    - A normal user packet passes and no alarm is generated.
    - A normal user packet passes and an alarm is generated.
    - An attack packet passes and an alarm is generated.
    - **An attack packet passes and no alarm is generated.***

    The four IDS/IPS alarm types are:
    False Positive – A normal user packet passes and an alarm is generated.
    False Negative – An attack packet passes and no alarm is generated.
    True Positive – An attack packet passes and an alarm is generated.
    True Negative – A normal user packet passes and no alarm is generated.

37. **What type of ACL offers greater flexibility and control over network access?**
    - flexible
    - named standard
    - **extended***
    - numbered standard

    The two types of ACLs are standard and extended. Both types can be named or numbered, but extended ACLs offer greater flexibility.

38. **Which security document includes implementation details, usually with step-by-step instructions and graphics?**
    - overview document
    - **procedure document***
    - guideline document
    - standard document

    Of the three types of security policy documents (standards, guidelines, and procedures), it is the procedure document that includes details such as step-by-step instructions and graphics.

39. **What is a characteristic of a DMZ zone?**
    - Traffic originating from the inside network going to the DMZ network is not permitted.
    - **Traffic originating from the outside network going to the DMZ network is selectively permitted.***

- Traffic originating from the DMZ network going to the inside network is permitted.
- Traffic originating from the inside network going to the DMZ network is selectively permitted.

The characteristics of a DMZ zone are as follows:
Traffic originating from the inside network going to the DMZ network is permitted.
Traffic originating from the outside network going to the DMZ network is selectively permitted.
Traffic originating from the DMZ network going to the inside network is denied.

40. **Which type of ASDM connection would provide secure remote access for remote users into corporate networks?**
- ASDM Launcher
- **AnyConnect SSL VPN***
- site-to-site VPN
- Java Web Start VPN

The ASDM Launcher is an option used to run Cisco ASDM as a local application instead of through a browser. The other option is to run ASDM as a Java Web Start application through a browser. The site-to-site VPN option is used to connect an ASA to a remote ASA or ISR router. Cisco AnyConnect SSL VPN provides remote users with secure access to corporate networks.

41. **Which three forwarding plane services and functions are enabled by the Cisco AutoSecure feature?** (Choose three.)
- secure SSH access
- **Cisco IOS firewall inspection***
- **Cisco Express Forwarding (CEF)***
- **traffic filtering with ACLs***
- secure password and login functions
- legal notification using a banner

Cisco Express Forwarding, traffic filtering using ACLs, and Cisco IOS firewall inspection are forwarding plane services and functions. Secure SSH, secure password and login functions, and legal notification using a banner are management plane services and functions.

42. **Which feature of the Cisco Network Foundation Protection framework prevents a route processor from being overwhelmed by unnecessary traffic?**
- **Control Plane Policing***
- IP Source Guard
- port security

- access control lists

Control Plane Policing provides a method for an administrator to control the amount of traffic that is being handled by the route processor. This security measure prevents a route processor from being overwhelmed by unnecessary traffic. IP Source Guard and access control lists are used to secure the data plane of network devices.

43. **What three tasks can a network administrator accomplish with the Nmap and Zenmap security testing tools? (Choose three.)**
    - **open UDP and TCP port detection***
    - **operating system fingerprinting***
    - password recovery
    - security event analysis and reporting
    - **assessment of Layer 3 protocol support on hosts***
    - development of IDS signatures

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

44. **Which two end points can be on the other side of an ASA site-to-site VPN configured using ASDM? (Choose two.)**
    - **another ASA***
    - Frame Relay switch
    - multilayer switch
    - DSL switch
    - **ISR router***

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

45. **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?**
    - **hairpinning***
    - GRE
    - split tunneling
    - MPL

46. **Which two types of hackers are typically classified as grey hat hackers? (Choose two.)**
    - script kiddies
    - **hacktivists***
    - state-sponsored hackers
    - **vulnerability brokers***
    - cyber criminals

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.

47. **Which security implementation will provide management plane protection for a network device?**
    - antispoofing
    - routing protocol authentication
    - **role-based access control***
    - access control lists

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.

48. **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 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.
    - Network security testing is most effective when deploying new security proposals.
    - **Network security testing proactively evaluates the effectiveness of the proposal before any real threat occurs.***

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.

49. **Which feature is specific to the Security Plus upgrade license of an ASA 5505 and provides increased availability?**
    - **redundant ISP connections***
    - transparent mode
    - routed mode
    - stateful packet inspection

50. **What is a characteristic of an ASA site-to-site VPN?**
    - ASA site-to-site VPNs create a secure single-user-to-LAN connection.
    - **The IPsec protocol protects the data transmitted through the site-to-site tunnel.***
    - ASA site-to-site VPNs can only be established between ASA devices.
    - The first echo request packet sent to test the establishment of the tunnel always succeeds.

    An ASA site-to-site VPN creates a secure LAN-to-LAN connection. The VPN can be established with another ASA or ISR router. Pings can be issued to test the tunnel established between devices. The first echo request packet sent to the remote host fails, but then the others succeed because the devices must negotiate the tunnel parameters.

51. **What is a result of enabling the Cisco IOS image resilience feature?**
    - Secured files can be viewed in the output of a CLI-issued command.
    - Multiple primary bootset files can be accessed.
    - **The feature can only be disabled through a console session.***
    - Images on a TFTP server can be secured.

    The Cisco IOS image resilience feature creates a copy of the IOS image and running configuration (primary bootset) and stores them locally in a hidden file. Once the feature is enabled, it can only be disabled through a console session. Images that are loaded from a remote location, such as a TFTP server, cannot be secured. The Cisco IOS file system prevents secured files from being listed in command output.

52. **What does the keyword default specify when used with the aaa authentication login command?**
    - Authentication must be specifically set for all lines, otherwise access is denied and no authentication is performed.
    - Authentication is automatically enabled for the vty lines utilizing the enable password.
    - The local username/password database is accessed for authentication.
    - **Authentication is automatically applied to the con 0, aux, and vty lines.***

The default keyword applies AAA authentication to all console, aux, and vty lines. AAA authentication can be configured to use a AAA server or local usernames/passwords to authenticate users.

53. **What are two protocols that are used by AAA to authenticate users against a central database of usernames and password? (Choose two.)**
    - **RADIUS***
    - SSH
    - HTTPS
    - CHAP
    - NTP
    - **TACACS+***

By using TACACS+ or RADIUS, AAA can authenticate users from a database of usernames and passwords stored centrally on a server such as a Cisco ACS server.

54. **Which service should be disabled on a router to prevent a malicious host from falsely responding to ARP requests with the intent to redirect the Ethernet frames?**
    - LLDP
    - reverse ARP
    - **proxy ARP***
    - CDP

Proxy ARP is a technique used on a device on a network to answer ARP queries for a device on another network. This service should be disabled on a router and the correct default gateway address should be configured (manually or by DHCP) for the normal process of remote network access. CDP and LLDP are device discovery protocols. Reverse ARP is used to resolve IP addresses.

55. **What is a characteristic of asymmetric algorithms?**
    - Key management is more difficult with asymmetric algorithms than it is with symmetric algorithms.
    - **Very long key lengths are used.***
    - Both the sender and the receiver know the key before communication is shared.
    - Asymmetric algorithms are easier for hardware to accelerate.

Asymmetric algorithms do not require a preshared key, which makes key management simpler. The longer key lengths that are used by asymmetric algorithms result in slower execution by devices.

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

- Only a root user can add or remove commands.
- 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.***
- **Commands from a lower level are always executable at a higher level.***
- AAA must be enabled.

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.