Number: 210-260
Passing Score: 800
Time Limit: 120 min
File Version: 5.0

210-260

Implementing Cisco Network Security

Version 5.0

Exam A

QUESTION 1
Which two services define cloud networks? (Choose two.)

A. Infrastructure as a Service
B. Platform as a Service
C. Security as a Service
D. Compute as a Service
E. Tenancy as a Service

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
In which two situations should you use out-of-band management? (Choose two.)

A. when a network device fails to forward packets
B. when you require ROMMON access
C. when management applications need concurrent access to the device
D. when you require administrator access from multiple locations
E. when the control plane fails to respond

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
In which three ways does the TACACS protocol differ from RADIUS? (Choose three.)

A. TACACS uses TCP to communicate with the NAS.
B. TACACS can encrypt the entire packet that is sent to the NAS.
C. TACACS supports per-command authorization.

D. TACACS authenticates and authorizes simultaneously, causing fewer packets to be transmitted.
E. TACACS uses UDP to communicate with the NAS.
F. TACACS encrypts only the password field in an authentication packet.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
According to Cisco best practices, which three protocols should the default ACL allow on an access port to enable wired BYOD devices to supply valid credentials and connect to the network? (Choose three.)

A. BOOTP
B. TFTP
C. DNS
D. MAB
E. HTTP
F. 802.1x

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which two next-generation encryption algorithms does Cisco recommend? (Choose two.)

A. AES
B. 3DES
C. DES
D. MD5
E. DH-1024
F. SHA-384

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which three ESP fields can be encrypted during transmission? (Choose three.)

A. Security Parameter Index
B. Sequence Number
C. MAC Address
D. Padding
E. Pad Length
F. Next Header

Correct Answer: DEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
What are two default Cisco IOS privilege levels? (Choose two.)

A. 0
B. 1
C. 5
D. 7
E. 10
F. 15

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which two authentication types does OSPF support? (Choose two.)

A. plaintext
B. MD5
C. HMAC
D. AES 256
E. SHA-1
F. DES

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which two features do CoPP and CPPr use to protect the control plane? (Choose two.)

A. QoS
B. traffic classification
C. access lists
D. policy maps
E. class maps
F. Cisco Express Forwarding

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which two statements about stateless firewalls are true? (Choose two.)

A. They compare the 5-tuple of each incoming packet against configurable rules.
B. They cannot track connections.

C. They are designed to work most efficiently with stateless protocols such as HTTP or HTTPS.
D. Cisco IOS cannot implement them because the platform is stateful by nature.
E. The Cisco ASA is implicitly stateless because it blocks all traffic by default.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which three statements about host-based IPS are true? (Choose three.)

A. It can view encrypted files.
B. It can have more restrictive policies than network-based IPS.
C. It can generate alerts based on behavior at the desktop level.
D. It can be deployed at the perimeter.
E. It uses signature-based policies.
F. It works with deployed firewalls.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
What three actions are limitations when running IPS in promiscuous mode? (Choose three.)

A. deny attacker
B. deny packet
C. modify packet
D. request block connection
E. request block host
F. reset TCP connection

Correct Answer: ABC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
When an IPS detects an attack, which action can the IPS take to prevent the attack from spreading?

A. Deny the connection inline.
B. Perform a Layer 6 reset.
C. Deploy an antimalware system.
D. Enable bypass mode.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
What is an advantage of implementing a Trusted Platform Module for disk encryption?

A. It provides hardware authentication.
B. It allows the hard disk to be transferred to another device without requiring re-encryption.dis
C. It supports a more complex encryption algorithm than other disk-encryption technologies.
D. It can protect against single points of failure.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
What is the purpose of the Integrity component of the CIA triad?

A. to ensure that only authorized parties can modify data

B. to determine whether data is relevant
C. to create a process for accessing data
D. to ensure that only authorized parties can view data

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
In a security context, which action can you take to address compliance?

A. Implement rules to prevent a vulnerability.
B. Correct or counteract a vulnerability.
C. Reduce the severity of a vulnerability.
D. Follow directions from the security appliance manufacturer to remediate a vulnerability.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which type of secure connectivity does an extranet provide?

A. other company networks to your company network
B. remote branch offices to your company network
C. your company network to the Internet
D. new networks to your company network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which tool can an attacker use to attempt a DDoS attack?

A. botnet
B. Trojan horse
C. virus
D. adware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
What type of security support is provided by the Open Web Application Security Project?

A. Education about common Web site vulnerabilities.
B. A Web site security framework.
C. A security discussion forum for Web site developers.
D. Scoring of common vulnerabilities and exposures.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
What type of attack was the Stuxnet virus?

A. cyber warfare
B. hacktivism
C. botnet
D. social engineering

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
What type of algorithm uses the same key to encrypt and decrypt data?

A. a symmetric algorithm
B. an asymmetric algorithm
C. a Public Key Infrastructure algorithm
D. an IP security algorithm

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Refer to the exhibit.

```
R1#show snmp
Chassis: FTX123456789
0 SNMP packets input
   6 Bad SNMP version errors
   3 Unknown community name
   9 Illegal operation for community name supplied
   4 Encoding errors
   2 Number of requested variables
   0 Number of altered variables
   98 Get-request PDUs
   12 Get-next PDUs
   2 Set-request PDUs
   0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
   0 Too big errors (Maximum packet size 1500)
   0 No such name errors
   0 Bad values errors
   0 General errors
   31 Response PDUs
   1 Trap PDUs
```

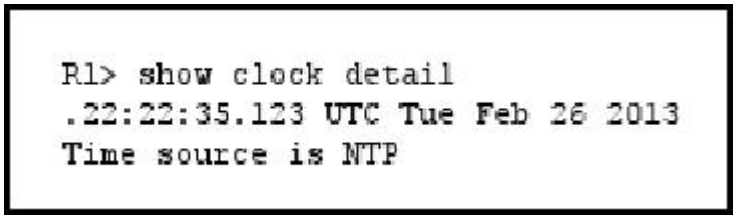
How many times was a read-only string used to attempt a write operation?

A. 9
B. 6
C. 4
D. 3
E. 2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Refer to the exhibit.



Which statement about the device time is true?

A. The time is authoritative, but the NTP process has lost contact with its servers.
B. The time is authoritative because the clock is in sync.
C. The clock is out of sync.
D. NTP is configured incorrectly.
E. The time is not authoritative.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
How does the Cisco ASA use Active Directory to authorize VPN users?

A. It queries the Active Directory server for a specific attribute for the specified user.
B. It sends the username and password to retrieve an ACCEPT or REJECT message from the Active Directory server.
C. It downloads and stores the Active Directory database to query for future authorization requests.
D. It redirects requests to the Active Directory server defined for the VPN group.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which statement about Cisco ACS authentication and authorization is true?

A. ACS servers can be clustered to provide scalability.
B. ACS can query multiple Active Directory domains.
C. ACS uses TACACS to proxy other authentication servers.
D. ACS can use only one authorization profile to allow or deny requests.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Refer to the exhibit.

```
authentication event fail action next-method
authentication event no-response action authorize vlan 101
authentication order mab dotlx webauth
authentication priority dotlx mab
authentication port-control auto
dotlx pae authenticator
```

If a supplicant supplies incorrect credentials for all authentication methods configured on the switch, how will the switch respond?

A. The supplicant will fail to advance beyond the webauth method.
B. The switch will cycle through the configured authentication methods indefinitely.
C. The authentication attempt will time out and the switch will place the port into the unauthorized state.
D. The authentication attempt will time out and the switch will place the port into VLAN 101.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which EAP method uses Protected Access Credentials?

A. EAP-FAST
B. EAP-TLS
C. EAP-PEAP
D. EAP-GTC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
What is one requirement for locking a wired or wireless device from ISE?

A. The ISE agent must be installed on the device.
B. The device must be connected to the network when the lock command is executed.
C. The user must approve the locking action.
D. The organization must implement an acceptable use policy allowing device locking.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
What VPN feature allows traffic to exit the security appliance through the same interface it entered?

A. hairpinning

B. NAT
C. NAT traversal
D. split tunneling

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
What VPN feature allows Internet traffic and local LAN/WAN traffic to use the same network connection?

A. split tunneling
B. hairpinning
C. tunnel mode
D. transparent mode

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Refer to the exhibit.

```
crypto ikev1 policy 1
encryption aes
hash md5
authentication pre-share
group 2
lifetime 14400
```

What is the effect of the given command sequence?

A. It configures IKE Phase 1.
B. It configures a site-to-site VPN tunnel.
C. It configures a crypto policy with a key size of 14400.
D. It configures IPSec Phase 2.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Refer to the exhibit.

```
crypto map mymap 20 match address 201
access-list 201 permit ip 10.10.10.0 255.255.255.0 10.100.100.0 255.255.255.0
```

What is the effect of the given command sequence?

A. It defines IPSec policy for traffic sourced from 10.10.10.0/24 with a destination of 10.100.100.0/24.
B. It defines IPSec policy for traffic sourced from 10.100.100.0/24 with a destination of 10.10.10.0/24.
C. It defines IKE policy for traffic sourced from 10.10.10.0/24 with a destination of 10.100.100.0/24.
D. It defines IKE policy for traffic sourced from 10.100.100.0/24 with a destination of 10.10.10.0/24.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Refer to the exhibit.

```
dst          src          state       conn-id     slot
10.10.10.2   10.1.1.5     QM_IDLE     1           0
```

While troubleshooting site-to-site VPN, you issued the show crypto isakmp sa command. What does the given output show?

A. IPSec Phase 1 is established between 10.10.10.2 and 10.1.1.5.
B. IPSec Phase 2 is established between 10.10.10.2 and 10.1.1.5.
C. IPSec Phase 1 is down due to a QM_IDLE state.
D. IPSec Phase 2 is down due to a QM_IDLE state.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Refer to the exhibit.

```
current_peer: 10.1.1.5
   PERMIT, flags={origin_is_acl,}
  #pkts encaps: 1205, #pkts encrypt: 1205, #pkts digest 1205
  #pkts decaps: 1168, #pkts decrypt: 1168, #pkts verify 1168
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0,
  #pkts decompress failed: 0, #send errors 0, #recv errors 0
   local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.1.1.5
```

While troubleshooting site-to-site VPN, you issued the show crypto ipsec sa command. What does the given output show?

A. IPSec Phase 2 is established between 10.1.1.1 and 10.1.1.5.
B. ISAKMP security associations are established between 10.1.1.5 and 10.1.1.1.

C. IKE version 2 security associations are established between 10.1.1.1 and 10.1.1.5.
D. IPSec Phase 2 is down due to a mismatch between encrypted and decrypted packets.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Refer to the exhibit.

```
Username HelpDesk privilege 9 password 0 helpdesk
Username Monitor privilege 8 password 0 watcher
Username Admin password checkme
Username Admin privilege 6 autocommand show running
Privilege exec level 6 configure terminal
```

The Admin user is unable to enter configuration mode on a device with the given configuration. What change can you make to the configuration to correct the problem?

A. Remove the autocommand keyword and arguments from the Username Admin privilege line.
B. Change the Privilege exec level value to 15.
C. Remove the two Username Admin lines.
D. Remove the Privilege exec line.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
After reloading a router, you issue the dir command to verify the installation and observe that the image file appears to be missing. For what reason

could the image file fail to appear in the dir output?

A. The secure boot-image command is configured.
B. The secure boot-comfit command is configured.
C. The confreg 0x24 command is configured.
D. The reload command was issued from ROMMON.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
What is the effect of the send-lifetime local 23:59:00 31 December 31 2013 infinite command?

A. It configures the device to begin transmitting the authentication key to other devices at 00:00:00 local time on January 1, 2014 and continue using the key indefinitely.
B. It configures the device to begin transmitting the authentication key to other devices at 23:59:00 local time on December 31, 2013 and continue using the key indefinitely.
C. It configures the device to begin accepting the authentication key from other devices immediately and stop accepting the key at 23:59:00 local time on December 31, 2013.
D. It configures the device to generate a new authentication key and transmit it to other devices at 23:59:00 local time on December 31, 2013.
E. It configures the device to begin accepting the authentication key from other devices at 23:59:00 local time on December 31, 2013 and continue accepting the key indefinitely.
F. It configures the device to begin accepting the authentication key from other devices at 00:00:00 local time on January 1, 2014 and continue accepting the key indefinitely.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
What type of packet creates and performs network operations on a network device?

A. control plane packets

B. data plane packets
C. management plane packets
D. services plane packets

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
An attacker installs a rogue switch that sends superior BPDUs on your network. What is a possible result of this activity?

A. The switch could offer fake DHCP addresses.
B. The switch could become the root bridge.
C. The switch could be allowed to join the VTP domain.
D. The switch could become a transparent bridge.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
In what type of attack does an attacker virtually change a device's burned-in address in an attempt to circumvent access lists and mask the device's true identity?

A. gratuitous ARP
B. ARP poisoning
C. IP spoofing
D. MAC spoofing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
What command can you use to verify the binding table status?

A. show ip dhcp snooping database
B. show ip dhcp snooping binding
C. show ip dhcp snooping statistics
D. show ip dhcp pool
E. show ip dhcp source binding
F. show ip dhcp snooping

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
If a switch receives a superior BPDU and goes directly into a blocked state, what mechanism must be in use?

A. root guard
B. EtherChannel guard
C. loop guard
D. BPDU guard

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which statement about a PVLAN isolated port configured on a switch is true?

A. The isolated port can communicate only with the promiscuous port.
B. The isolated port can communicate with other isolated ports and the promiscuous port.
C. The isolated port can communicate only with community ports.

D. The isolated port can communicate only with other isolated ports.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
If you change the native VLAN on the trunk port to an unused VLAN, what happens if an attacker attempts a double-tagging attack?

A. The trunk port would go into an error-disabled state.
B. A VLAN hopping attack would be successful.
C. A VLAN hopping attack would be prevented.
D. The attacked VLAN will be pruned.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
What is a reason for an organization to deploy a personal firewall?

A. To protect endpoints such as desktops from malicious activity.
B. To protect one virtual network segment from another.
C. To determine whether a host meets minimum security posture requirements.
D. To create a separate, non-persistent virtual environment that can be destroyed after a session.
E. To protect the network from DoS and syn-flood attacks.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which statement about personal firewalls is true?

A. They can protect a system by denying probing requests.
B. They are resilient against kernel attacks.
C. They can protect email messages and private documents in a similar way to a VPN.
D. They can protect the network against attacks.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Refer to the exhibit.

```
UDP outside  209.165.201.225:53 inside  10.0.0.10:52464, idle 0:00:01, bytes 266, flags -
```

What type of firewall would use the given configuration line?

A. a stateful firewall
B. a personal firewall
C. a proxy firewall
D. an application firewall
E. a stateless firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
What is the only permitted operation for processing multicast traffic on zone-based firewalls?

A. Only control plane policing can protect the control plane against multicast traffic.
B. Stateful inspection of multicast traffic is supported only for the self-zone.
C. Stateful inspection for multicast traffic is supported only between the self-zone and the internal zone.
D. Stateful inspection of multicast traffic is supported only for the internal zone.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
How does a zone-based firewall implementation handle traffic between interfaces in the same zone?

A. Traffic between two interfaces in the same zone is allowed by default.
B. Traffic between interfaces in the same zone is blocked unless you configure the same-security permit command.
C. Traffic between interfaces in the same zone is always blocked.
D. Traffic between interfaces in the same zone is blocked unless you apply a service policy to the zone pair.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which two statements about Telnet access to the ASA are true? (Choose two).

A. You may VPN to the lowest security interface to telnet to an inside interface.
B. You must configure an AAA server to enable Telnet.
C. You can access all interfaces on an ASA using Telnet.
D. You must use the command virtual telnet to enable Telnet.
E. Best practice is to disable Telnet and use SSH.

Correct Answer: AE
Section: (none)
Explanation