

# Cisco

## Exam 210-260

### Implementing Cisco Network Security

Version: 12.0

[ Total Questions: 186 ]

**Question No : 1**

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.

**Answer: A**

**Question No : 2**

Which command is needed to enable SSH support on a Cisco Router?

- A. crypto key lock rsa
- B. crypto key generate rsa
- C. crypto key zeroize rsa
- D. crypto key unlock rsa

**Answer: B**

**Question No : 3**

A clientless SSL VPN user who is connecting on a Windows Vista computer is missing the menu option for Remote Desktop Protocol on the portal web page. Which action should you take to begin troubleshooting?

- A. Ensure that the RDP2 plug-in is installed on the VPN gateway
- B. Reboot the VPN gateway
- C. Instruct the user to reconnect to the VPN gateway
- D. Ensure that the RDP plug-in is installed on the VPN gateway

**Answer: D**

**Question No : 4**

Which two features are commonly used CoPP and CPPr 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

**Answer: A,B**

**Question No : 5**

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

**Answer: A**

**Question No : 6**

Which protocols use encryption to protect the confidentiality of data transmitted between two parties? (Choose two.)

- A. FTP
- B. SSH
- C. Telnet
- D. AAA
- E. HTTPS
- F. HTTP

**Answer: B,E**

**Question No : 7**

What is the FirePOWER impact flag used for?

- A. A value that indicates the potential severity of an attack.
- B. A value that the administrator assigns to each signature.
- C. A value that sets the priority of a signature.
- D. A value that measures the application awareness.

**Answer: A**

**Question No : 8**

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

**Answer: D**

**Question No : 9**

If a router configuration includes the line `aaa authentication login default group tacacs+ enable`, which events will occur when the TACACS+ server returns an error? (Choose two.)

- A. The user will be prompted to authenticate using the enable password
- B. Authentication attempts to the router will be denied
- C. Authentication will use the router's local database
- D. Authentication attempts will be sent to the TACACS+ server

**Answer: A,B**

**Question No : 10**

If a switch port goes directly into a blocked state only when a superior BPDU is received, what mechanism must be in use?

- A. STP BPDU guard
- B. loop guard
- C. STP Root guard
- D. EtherChannel guard

**Answer: A**

**Question No : 11**

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.

**Answer: A**

**Question No : 12**

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

**Answer: A**

**Question No : 13**

What are two uses of SIEM software? (Choose two.)

- A. collecting and archiving syslog data
- B. alerting administrators to security events in real time
- C. performing automatic network audits
- D. configuring firewall and IDS devices
- E. scanning email for suspicious attachments

**Answer: A,B**

**Question No : 14**

Which statement about extended access lists is true?

- A. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the destination
- B. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the source
- C. Extended access lists perform filtering that is based on destination and are most effective when applied to the source
- D. Extended access lists perform filtering that is based on source and are most effective when applied to the destination

**Answer: B**

**Question No : 15**

For what reason would you configure multiple security contexts on the ASA firewall?

- A. To separate different departments and business units.

- B. To enable the use of VRFs on routers that are adjacently connected.
- C. To provide redundancy and high availability within the organization.
- D. To enable the use of multicast routing and QoS through the firewall.

**Answer: A**

**Question No : 16**

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, #recverrors 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.

**Answer: A**

**Question No : 17**

What is a valid implicit permit rule for traffic that is traversing the ASA firewall?

- A. ARPs in both directions are permitted in transparent mode only.
- B. Unicast IPv4 traffic from a higher security interface to a lower security interface is permitted in routed mode only.
- C. Unicast IPv6 traffic from a higher security interface to a lower security interface is permitted in transparent mode only.
- D. Only BPDUs from a higher security interface to a lower security interface are permitted

in transparent mode.

E. Only BPDUs from a higher security interface to a lower security interface are permitted in routed mode.

**Answer: A**

**Question No : 18**

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

**Answer: A,B**

**Question No : 19**

Which security measures can protect the control plane of a Cisco router? (Choose two.)

- A. CCPr
- B. Parser views
- C. Access control lists
- D. Port security
- E. CoPP

**Answer: A,E**

**Question No : 20**

In the router ospf 200 command, what does the value 200 stand for?

- A. process ID
- B. area ID
- C. administrative distance value



D. ABR ID

**Answer: A**

**Question No : 21**

Which protocol provides security to Secure Copy?

- A. IPsec
- B. SSH
- C. HTTPS
- D. ESP

**Answer: B**

**Question No : 22**

Which technology can be used to rate data fidelity and to provide an authenticated hash for data?

- A. file reputation
- B. file analysis
- C. signature updates
- D. network blocking

**Answer: A**

**Question No : 23**

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.

**Answer: B**

**Question No : 24**

Which type of mirroring does SPAN technology perform?

**A.** Remote mirroring over Layer 2

**B.** Remote mirroring over Layer 3

**C.** Local mirroring over Layer 2

**D.** Local mirroring over Layer 3

**Answer: C**

**Question No : 25**

If a packet matches more than one class map in an individual feature type's policy map, how does the ASA handle the packet?

**A.** The ASA will apply the actions from only the first matching class map it finds for the feature type.

**B.** The ASA will apply the actions from only the most specific matching class map it finds for the feature type.

**C.** The ASA will apply the actions from all matching class maps it finds for the feature type.

**D.** The ASA will apply the actions from only the last matching class map it finds for the feature type.

**Answer: A**

**Question No : 26**