

**210-260.89q**

Number: 210-260  
Passing Score: 860  
Time Limit: 45 min  
File Version: 1



**VCE to PDF Converter :** <https://vceplus.com/vce-to-pdf/>

**Facebook:** <https://www.facebook.com/VCE.For.All.VN/>

**Twitter :** [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

**Google+ :** <https://plus.google.com/+Vcepluscom>

**LinkedIn :** <https://www.linkedin.com/company/vceplus>  
Cisco 210-260

VCE To PDF - Free Practice Exam

**Exam A****QUESTION 1**

Which SOURCEFIRE logging action should you choose to record the most detail about a connection?

- A. Enable logging at the beginning of the session
- B. Enable logging at the end of the session
- C. Enable alerts via SNMP to log events off-box
- D. Enable eStreamer to log events off-boxx

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 2**

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 3**

Which statement about communication over failover interfaces is true?

- A. All information that is sent over the failover interface is sent as clear text, but the stateful failover link is encrypted by default
- B. All information that is sent over the failover and stateful failover interfaces is encrypted by default
- C. All information that is sent over the failover and stateful failover interfaces is sent as clear text by default
- D. Usernames, password and preshared keys are encrypted by default when they are sent over the failover and stateful failover interfaces, but other information is

in clear text

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 4**

What features can protect the data plane? (Choose three)

- A. policing
- B. ACLs
- C. IPS
- D. antispoofing
- E. QoS
- F. DHCP-snooping

**Correct Answer:** BDF

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 5**

How many crypto map sets can you apply to a router interface?

- A. 3
- B. 2
- C. 4
- D. 1

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 6**

What is the transition order of STP states on a Layer 2 switch interface?

- A. listening, learning, blocking, forwarding, disabled
- B. listening, blocking, learning, forwarding, disabled
- C. blocking, listening, learning, forwarding, disabled
- D. forwarding, listening, learning, blocking, disabled

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 7**

Which sensor mode can deny attackers inline?

- A. IPS
- B. fail-close
- C. IDS
- D. fail=open

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 8**

Which options are filtering options used to display SDEE message types?

- A. stop
- B. none
- C. error
- D. all

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 9

When a company puts a security policy in place, what is the effect on the company's business?

- A. Minimizing risk
- B. Minimizing total cost of ownership
- C. Minimizing liability
- D. Maximizing compliance

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



### QUESTION 10

Refer to the exhibit.

```
authentication event fail action next-method
authentication event no-response action authorize vlan 101
authentication order mad dot1x webauth
authentication priority dot1x mab
authentication port-control auto
dot1x pae authenticator
```

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

- A. The switch will cycle through the configured authentication methods indefinitely
- B. The supplicant will fail to advance beyond the webauth method
- 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:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 11**

Which wildcard mask is associated with a subnet mask of /27?

- A. 0.0.0.31
- B. 0.0.0.27
- C. 0.0.0.224
- D. 0.0.0.225

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 12**

Which statements about reflexive access lists are true?

- A. Reflexive access lists create a permanent ACE
- B. Reflexive access lists approximate session filtering using the established keyword
- C. Reflexive access lists can be attached to standard named IP ACLs
- D. Reflexive access lists support UDP sessions
- E. Reflexive access lists can be attached to extended named IP ACLs
- F. Reflexive access lists support TCP sessions

**Correct Answer:** DEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 13**

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

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

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 14**

Which actions can a promiscuous IPS take to mitigate an attack? (Choose three)

- A. modifying packets
- B. requesting connection blocking
- C. denying packets
- D. resetting the TCP connection
- E. requesting host blocking
- F. denying frames

**Correct Answer:** BDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 15**

Which Cisco Security Manager application collects information about device status and uses it to generate notification and alerts?

- A. FlexConfig
- B. Device Manager
- C. Report Manager
- D. Health and Performance Monitor

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 16**

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 17**

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

**Correct Answer:** ABF



**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 18**

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 19**

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**

**Explanation/Reference:**

**QUESTION 20**

What are the two purposes of the Internet Key Exchange in an IPsec VPN? (Choose two)



<http://www.gratisexam.com/>

- A. The Internet Key Exchange protocol establishes security associations
- B. The Internet Key Exchange protocol provides data confidentiality
- C. The Internet Key Exchange protocol provides replay detection
- D. The internet Key Exchange protocol is responsible for mutual authentication

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 21**

Which protocol provides security to Secure Copy?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 22**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 23**

Which security zone is automatically defined by the system?

- A. The source zone
- B. The self zone
- C. The destination zone
- D. The inside zone

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 24**

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 25**

Which address block is reserved for locally assigned unique local addresses?

- A. 2002::/16
- B. FE00::/8
- C. 2001::/32
- D. FB00::/8

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 26**

What is a possible reason for the error message?

Router(config)#aaa server?% Unrecognized command

- A. The command syntax requires a space after the word "server"
- B. The command is invalid on the target device
- C. The router is already running the latest operating system
- D. The router is a new device on which the aaa new-model command must be applied before continuing

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 27**

Which statements about smart tunnels on a Cisco firewall are true? (Choose two)

- A. Smart tunnels can be used by clients that do not have administrator privileges
- B. Smart tunnels support all operating systems
- C. Smart tunnels offer better performance than port forwarding
- D. Smart tunnels require the client to have the application installed locally

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 28

Which option describes information that must be considered when you apply an access list to a physical interface?

- A. Protocol used for filtering
- B. Direction of the access class
- C. Direction of the access group
- D. Direction of the access list



**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 29

Which source port does IKE use when NAT has been detected between two VPN gateways?

- A. TCP 4500
- B. TCP 500
- C. UDP 4500
- D. UDP 500

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 30**

Which of the following are features of IPsec transport mode? (Choose three)

- A. IPsec transport mode is used between end stations
- B. IPsec transport mode is used between gateways
- C. IPsec transport mode supports multicast
- D. IPsec transport mode supports unicast
- E. IPsec transport mode encrypts only the payload
- F. IPsec transport mode encrypts the entire packet

**Correct Answer:** ADE

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 31**

Which command causes a Layer 2 switch interface to operate as a Layer 3 interface?

- A. no switchport nonnegotiate
- B. switchport
- C. no switchport mode dynamic auto
- D. no switchport

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 32**

Which command verifies phase 1 of an IPsec VPN on a Cisco router?

- A. show crypto map
- B. show crypto ipsec sa
- C. show crypto isakmp sa
- D. show crypto engine connection active

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 33

What is the purpose of a honeypot IPS?

- A. To create customized policies
- B. To detect unknown attacks
- C. To normalize streams
- D. To collect information about attacks

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 34

Which type of firewall can act on behalf of the end device?

- A. Stateful packet
- B. Application
- C. Packet
- D. Proxy

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 35**

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 issue 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 36**

What type of attack was the Stuxnet virus?

- A. cyber warfare
- B. hactivism
- C. botnet
- D. social engineering

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 37**

Which type of secure connectivity does an extranet provide?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 38**

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 39**

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 40

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



<http://www.gratisexam.com/>



- A. NAT traversal
- B. Hairpinning
- C. split tunneling
- D. NAT

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 41

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

- A. The user must approve the locking action
- B. The ISE agent must be installed on the device
- C. The organization must implement an acceptable use policy allowing device locking

D. The device must be connected to the network when the lock command is executed

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 42**

Refer to the exhibit. What type of firewall would use the given configuration line?

UPD outside 209.165.201.225:53 inside 10.0.0.10:52464, idle 0:00:01, bytes 226 flags -

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 43**

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

- A. To enable the use of multicast routing and QoS through the firewall
- B. To separate different departments and business units
- C. To enable the use of VFRs on routers that are adjacently connected
- D. To provide redundancy and high availability within the organization

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 44**

Which FirePOWER preprocessor engine is used to prevent SYN attacks?

- A. Portscan Detection
- B. IP Defragmentation
- C. Inline Normalization
- D. Rate-Based Prevention

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 45**

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

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

**Correct Answer:** CF

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 46**

What is the effect of the given command sequence?

```
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
```

- 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 47**

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

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



**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 48**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 49**

Which statement about application blocking is true?

- A. It blocks access to files with specific extensions
- B. It blocks access to specific network addresses
- C. It blocks access to specific programs
- D. It blocks access to specific network services

**Correct Answer: C**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 50**

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 51**

When is the best time to perform an anti-virus signature update?

- A. Every time a new update is available

- B. When the system detects a browser hook
- C. When a new virus is discovered in the wild
- D. When the local scanner has detected a new virus

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 52

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 53

What Statement about personal firewalls is true?

- A. They can protect the network against attacks
- B. They can protect a system by denying probing requests
- C. They are resilient against kernel attacks

D. They can protect email messages and private documents in a similar way to a VPN

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 54

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

```
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 compr. failed: 0,
#pkts decompress failed: 0, # send errors 0, #rcv errors 0
local_crypto_endpt.: 10.1.1.1, remote_crypto_endpt.: 10.1.1.5
```

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 55

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

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



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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 56**

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

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

**Correct Answer:** ADF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 57**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 58**

Refer to the exhibit. Which statement about the device time is true?

```
R1> show clock detail
.22:22:35.123 UTC Tue Feb 26 2013
Time source is NTP
```

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 59**

In what type of attack does an attacker virtually change a device's burned in address in an attempt to circumvent access list 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 60**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 61

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 62

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 63

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

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

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



### QUESTION 64

Which two features do CoPP and CPPR use to protect the control plane? (Choose two)

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

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 65**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 66**

Refer to the exhibit. What is the effect of the given command sequence?

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 67**

A specific URL has been identified as containing malware. What action can you take to block users from accidentally visiting the URL and becoming infected with malware?

- A. Enable URL filtering on the perimeter firewall and add the URLs you want to allow to the routers local URL list
- B. Enable URL filtering on the perimeter router and add the URLs you want to allow to the firewalls local URL list
- C. Create a blacklist that contains the URL you want to block and activate the blacklist on the perimeter router
- D. Enable URL filtering on the perimeter router and add the URLs you want to block to the routers local URL list
- E. Create a whitelist that contains the URLs you want to allow and activate the whitelist on the perimeter router

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 68**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 69**

What is an advantage of placing an IPS on the inside of a network?

- A. It can provide higher throughput
- B. It receives traffic that has already been filtered

- C. It receives every inbound packet
- D. It can provide greater security

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 70**

Which tasks is the session management path responsible for? (Choose three)

- A. Verifying IP checksums
- B. Performing route lookup
- C. Performing session lookup
- D. Allowing NAT translations
- E. Checking TCP sequence numbers
- F. Checking packets against the access list

**Correct Answer:** BDF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 71**

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

- A. services plane packets
- B. control plane packets
- C. data plane packets
- D. management plane packets

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 72**

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

- A. They are designed to work most efficiently with stateless protocols such as HTTP or HTTPS.
- B. They compare the 5-tuple of each incoming packet against configurable rules.
- C. Cisco IOS cannot implement them because the platform is stateful by nature.
- D. They cannot track connections.
- E. The Cisco ASA is implicitly stateless because it blocks all traffic by default.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 73**

Which syslog severity level is level number 7?

- A. Warning
- B. Debugging
- C. Informational
- D. Notification

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 74**

Which alert protocol is used with Cisco IPS Manager Express to support up to 10 sensors?

- A. CSM



- B. SDEE
- C. Syslog
- D. SNMP

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 75**

Which components does HMAC use to determine the authenticity and integrity of a message?

- A. The password
- B. The hash
- C. The key
- D. The transform set

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 76**

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

- A. BPDU guard
- B. loop guard
- C. root guard
- D. Etherchannel guard

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 77**

Which RADIUS server authentication protocols are supported on Cisco ASA firewalls? (Choose three)

- A. EAP
- B. ASCII
- C. PAP
- D. PEAP
- E. MS-CHAPv2
- F. MS-CHAPv1

**Correct Answer:** CEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 78**

Which command initializes a lawful intercept view?

- A. username cisco1 view lawful-intercept password cisco
- B. parser view cisco li-view
- C. li-view cisco user cisco1 password cisco
- D. parser view li-view inclusive

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 79**

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

- A. Port security
- B. CoPP

- C. CPPr
- D. Access control lists
- E. Parser views

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 80

Which statement about extended access lists is true?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 81

Which type of address translation should be used when a Cisco ASA is in transparent mode?

- A. Dynamic PAT
- B. Static NAT
- C. Overload
- D. Dynamic NAT

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 82**

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. HTTP
- F. HTTPS

**Correct Answer:** BF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 83**

What are the primary attack methods of VLAN hopping? (Choose two)

- A. VoIP hopping
- B. CAM-table overflow
- C. Switch spoofing
- D. Double tagging

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 84**

What is the default timeout interval during which a router waits for responses from a TACACS server before declaring a timeout failure?

- A. 20 seconds
- B. 5 seconds

- C. 15 seconds
- D. 10 seconds

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 85**

How can the administrator enable permanent client installation in a Cisco AnyConnect VPN firewall configuration?

- A. Issue the command anyconnect keep-installer installed under the group policy or username webvpn mode
- B. Issue the command anyconnect keep-installer installed in the global configuration
- C. Issue the command anyconnect keep-installer under the group policy or username webvpn mode
- D. Issue the command anyconnect keep-installer under the group policy or username webvpn mode

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 86**

What is the FirePOWER impact flag used for?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 87**

What can the SMTP preprocessor in a FirePOWER normalize?

- A. It can look up the email sender
- B. It uses the Traffic Anomaly Detector
- C. It can extract and decode email attachments in client to server traffic
- D. It compares known threats to the email sender
- E. It can forward the SMTP traffic to an email filter server

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 88**

You want to allow all of your companies users to access the internet without allowing other Web servers to collect the IP addresses of individual users. What two solutions can you use? (Choose two)

- A. Install a Web content filter to hid users local IP addresses
- B. Configure a firewall to use Port Address Translation
- C. Assign the same IP addresses to all users
- D. Configure a proxy server to hide users local IP addresses
- E. Assign unique IP addresses to all users

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 89**

Refer to the exhibit. 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?

```
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
```

- 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:**