Cisco

Exam Questions 400-251

CCIE Security Written Exam

Certshared now are offering 100% pass ensure 400-251 dumps!
https://www.certshared.com/exam/400-251/ (124 Q&As)
NEW QUESTION 1
- (Exam Topic 1)
Which two statements about MPP (Management Plane Protection) are true? (Choose two.)

A. It is supported on both distributed and hardware-switched platforms.
B. Only out-of-band management interfaces are supported.
C. Only virtual interfaces associated with physical interfaces are supported.
D. It is supported on both active and standby management interfaces.
E. Only in-band management interfaces are supported.
F. Only virtual interfaces associated with sub-interfaces are supported.

Answer: CE

NEW QUESTION 2
- (Exam Topic 1)
Which two statements about the Cisco AnyConnect VPN Client are true? (Choose two.)

A. It can use an SSL tunnel and a DTLS tunnel simultaneously.
B. It enables users to manage their own profiles.
C. It can be configured to download automatically without prompting the user.
D. By default, DTLS connections can fall back to TLS.
E. To improve security, keepalives are disabled by default.

Answer: AC

NEW QUESTION 3
- (Exam Topic 1)
Which statement about the Cisco AMP Virtual Private Cloud Appliance is true for deployments in air-gap mode?

A. The amp-sync tool syncs the threat-intelligence repository on the appliance directly with the AMP public cloud.
B. The appliance can perform disposition lookup against either the Protect DB or the AMP public cloud.
C. The appliance can perform disposition lookups against the Protect DB without an Internet connection.
D. The appliance evaluates files against the threat intelligence and disposition information residing on the Update Host.
E. The Update Host automatically downloads updates and deploys them to the Protect DB on a daily basis.

Answer: C

NEW QUESTION 4
- (Exam Topic 2)
Which two design options are best to reduce security concerns when adopting IoT into an organization? (Choose two.)

A. Ensure that application can gather and analyze data at the edge.
B. Implement video analytics on IP cameras.
C. Encrypt sensor data in transit.
D. Segment the Field Area Network from the Data Center network.
E. Encrypt data at rest on all devices in the IoT network.

Answer: CD

NEW QUESTION 5
- (Exam Topic 2)
Which two options are normal functionalities for ICMP? (Choose two)

A. host detection
B. packet filtering
C. relaying traffic statistics to applications
D. path MTU discovery
E. port scanning
F. router discovery

Answer: AD

NEW QUESTION 6
- (Exam Topic 2)
Refer to the exhibit.
For which type of user is this downloadable ACL appropriate?

A. management  
B. employees  
C. guest users  
D. network administrator  
E. outside contractors

**Answer:** C

**NEW QUESTION 7**

- (Exam Topic 2)

Which two functions of Cisco Content Security Management Appliance are true? (Choose two)

A. SMA is used for on-box management of WSAs  
B. SMA is used to configure NSAMP on the router  
C. SMA is a centralized system used to collectively manage and report the WSAs that are deployed in a network  
D. SMA is used for sandboxing functionality to perform malware analysis  
E. SMA is a unified management platform that manages web security, performs troubleshooting and maintains space for data storage.

**Answer:** CE

**NEW QUESTION 8**

- (Exam Topic 2)

Refer to the exhibit.

What are two functionalities of this configuration? (Choose two)

A. Traffic will not be able to pass on gigabitEthernet0/1.  
B. The ingress command is used for an IDS to send a reset on vlan 3 only.  
C. The source interface should always be a VLAN.  
D. The encapsulation command is used to do deep scan on dot1q encapsulation traffic  
E. Traffic will only be sent to gigabitEthernet 0/20

**Answer:** BE

**NEW QUESTION 9**

- (Exam Topic 2)

While a configuration audit is performed on a router, the set session-key command is found un crypto map applied to a WAN interface. Which three statements about this command are true? (Choose three)

A. This command sets a peer authentication string because the IPSec peer does not support automatic mutual authentication and a manual method is required  
B. When configuring the Crypto map, (ipsec-manual) must be defined as part of the parameters  
C. This command is used to encrypt traffic to another device which does not support internet key  
D. Exchange  
E. Another way of overcoming this issue is to use the crypto isakmp peer address command with a zeros wildcard address and mask combination  
F. Both peers must be configured for manual peer authentication for this configuration to work  
G. This command is used to manually configure an IPSec SA two entries are needed on each side to encrypt and decrypt traffic over the tunnel  
H. This command is used to manually configure an IPSec SA only one entry are needed on each side to encrypt and decrypt traffic over the tunnel.

**Answer:** BEF

**NEW QUESTION 10**

- (Exam Topic 2)

Which statement about Cisco ISE Guest portals is true?

A. To permit BYOD access, a Guest portal must use RADIUS authentication.  
B. If you delete a Guest portal without removing its authorization policy and profiles, they will be assigned automatically to the default Guest portal.  
C. The Hotspot Guest portal can be configured for password-only authentication.  
D. The Sponsored Guest portal allows guest users to create an account.  
E. The sponsored-Guest portal and Self-Registered Guest portal require a defined Endpoint Identity Group.  
F. When you make changes to an authorized Guest portal configuration, it must be reauthorized before the changes will take effect.

**Answer:**
NEW QUESTION 11
- (Exam Topic 2)
Which Cisco Firepower interface mode allows you to send inline traffic directly through the device and only inspect a copy of the traffic?

A. TAP mode
B. Automatic application bypass mode
C. Delay threshold mode
D. Fast-path mode

Answer: A

NEW QUESTION 12
- (Exam Topic 3)
Which of the following could be an evasion technique used by the attacker?

A. Port access using Dot1x
B. ACL implementation to drop unwanted traffic
C. TELNET to launch device administration session
D. Traffic encryption to bypass IPS detection
E. URL filtering to block malicious sites
F. NAT translations on routers and switches

Answer: D

NEW QUESTION 13
- (Exam Topic 3)
Which statement describes a pure SDN framework environment?

A. The control plane and data plane is pulled from the networking element and put in a SDN controller and SDN agent
B. The control plane function is split between a SDN controller and the networking element
C. The data plane is pulled from the networking element and put in a SDN controller
D. The data plane is controlled by a centralized SDN element
E. The control plane is pulled from the networking element and put in a SDN controller

Answer: E

NEW QUESTION 14
- (Exam Topic 3)
Which statement is true regarding securing connection using MACsec?

A. It secures connection between two supplicant clients
B. Switch uses session keys to calculate decrypted packet ICV value for the frame integrity check
C. Switch configured for MACSec can only accept MACSec frames from the MACSec client
D. It is implemented after a successful MAB authentication of supplicant
E. It provides network layer encryption on a wireless network
F. ISAKMP protocol is used to manage MACSec encryption keys

Answer: B

NEW QUESTION 15
- (Exam Topic 3)
What are the three configurations in which SSL VPN can be implemented? (Choose three.)

A. WebVPN
B. PVC TunnelMode
C. Interactive Mode
D. L2TP over IPSec
E. Thin-Client
F. AnyConnect TunnelMode
G. Clientless
H. CHAP

Answer: EFG

NEW QUESTION 16
- (Exam Topic 3)
Which of the following is true regarding ASA clustering requirements?

A. Only routed mode is allowed in the single context mode
B. Units in the cluster can be running different software version as long as they have identical hardware configuration
C. Units in the cluster can have different hardware configuration as long as they are running same software version
D. Units in the cluster can be in different geographical locations
E. Units in the cluster can be in different security context modes
F. Units in the cluster can have different amount of flash memory

Answer: B
NEW QUESTION 17
- (Exam Topic 3)
Which two options can be used to further harden a Cisco Email Security Appliance? (Choose two.)

A. Disable telnet
B. Rename the default administrator password
C. Disable HTTP and FTP services that are not required
D. Enable Cisco Discovery Protocol
E. Turn off TCP small services

Answer: AB

NEW QUESTION 18
- (Exam Topic 3)
Which statement about SenderBase reputation scoring on an ESA device is true?

A. Application traffic from known bad sites can be throttled or blocked
B. By default, all messages with a score below zero are dropped or throttled
C. Mail with scores in the medium range can be automatically routed for antimalware scanning
D. You can configure a custom score threshold for whitelisting messages
E. A high score indicates that a message is very likely to be spam
F. Sender reputation scores can be assigned to domains, IP addresses, and MAC addresses

Answer: D

NEW QUESTION 19
- (Exam Topic 3)
How would you best describe Jenkins?

A. An orchestration tool
B. Continuous integration and delivery application
C. Operations in a client/server model
D. Web-based repository hosting service
E. A REST client

Answer: B

NEW QUESTION 20
- (Exam Topic 3)
How many report templates does the Cisco Firepower Management Center support?

A. 5
B. 10
C. 50
D. 80
E. 100
F. Unlimited

Answer: F

NEW QUESTION 21
......
Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions
2nd - Questions and Answers in PDF Format

400-251 Practice Exam Features:

* 400-251 Questions and Answers Updated Frequently
* 400-251 Practice Questions Verified by Expert Senior Certified Staff
* 400-251 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
* 400-251 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click Order The 400-251 Practice Test Here