Cisco Exam Questions 400-251
CCIE Security Written Exam
NEW QUESTION 1
- (Exam Topic 1)
Which three statements about VRF-Aware Cisco Firewall are true? (Choose three.)

A. It supports both global and per-VRF commands and DoS parameters.
B. It enables service providers to deploy firewalls on customer devices.
C. It can generate syslog messages that are visible only to individual VPNs.
D. It can support VPN networks with overlapping address ranges without NAT.
E. It enables service providers to implement firewalls on PE devices.
F. It can run as more than one instance.

Answer: CEF

NEW QUESTION 2
- (Exam Topic 1)
Which three statements about Cisco AnyConnect SSL VPN with the ASA are true? (Choose three)

A. DTLS can fall back to TLS without enabling dead peer detection.
B. By default, the VPN connection connects with DTLS.
C. Real-time application performance improves if DTLS is implemented
D. Cisco AnyConnect connections use IKEv2 by default when it is configure as the primary protocol on the client.
E. By default, the ASA uses the Cisco AnyConnect Essentials license.
F. The ASA will verify the remote HTTPS certificate.

Answer: CDE

NEW QUESTION 3
- (Exam Topic 1)
Refer to the exhibit.

Which effect of this command is true?

A. The route immediately deletes its current public key from the cache and generates a new one.
B. The public key of the remote peer is deleted from the router cache.
C. The CA revokes the public key certificate of the router.
D. The current public key of the router is deleted from the cache when the router reboots, and the router generates a new one.
E. The router sends a request to the CA to delete the router certificate from its configuration.

Answer: B

NEW QUESTION 4
- (Exam Topic 1)
What are three technologies that can be used to trace the source of an attack in a network environment with multiple exit/entry points? (Choose three.)

A. ICMP Unreachable messages
B. Sinkholes
C. A honey pot
D. Remotely-triggered destination-based black holing
E. Traffic scrubbing

Answer: ADE

NEW QUESTION 5
- (Exam Topic 1)
Which two statements about the MACsec security protocol are true? (Choose two.)

A. When switch-to-switch link security is configured in manual mode, the SAP operation mode must be set to GCM.
B. MACsec is not supported in MDA mode.
C. Stations broadcast an MKA heartbeat that contains the key server priority.
D. MKA heartbeats are sent at a default interval of 3 seconds.
E. The SAK is secured by 128 bit AES-GCM by default.

Answer: CE

NEW QUESTION 6
- (Exam Topic 2)
Which two statements about the Cisco FireAMP solution are true? (Choose two.)

A. It can perform dynamic analysis in the Fire AMP Private Cloud.
B. The FireAMP Connector can detect malware in network traffic and when files are downloaded.
C. The FireAMP Private Cloud provides an on-premises option for file disposition lookups and retrospection generation.
D. The FireAMP Connector is compatible with antivirus software on the endpoint, but you must configure exclusion to prevent the Connector from scanning the antivirus directory.
E. The FireAMP Connector can provide information about potentially malicious network connections.
F. The FireAMP Private cloud can act as an anonymized proxy to transport endpoint event data to the public cloud for disposition lookups.
G. When a FireAMP Connector detects malware in network traffic, it generates a malware event and a threat.

Answer: AC

NEW QUESTION 7
- (Exam Topic 2)
1821 How does the Cisco Firepower Decrypt-known method perform SSI decryption on inbound traffic?

A. The system identifies the server certificate during the SSL handshake and downloads the associate private key from the CA to decrypt the traffic.
B. The system matches the incoming server certificate to a previously stored certificate on the server and uses the private key to decrypt the traffic.
C. The system uses a CA certificate on the server to resign the exchanges server certificate then uses the private key of the CA certificate to decrypt the traffic.
D. The system uses a CA certificate on the server to resign the exchanges server certificate then uses separate private key to decrypt the traffic.

Answer: C

NEW QUESTION 8
- (Exam Topic 2)
Which two statements about MACsec are true? (Choose two)

A. It maintains network intelligence as it applied to router uplinks and downlinks.
B. It works in conjunction with IEEE 802.1X -2010 port-based access control.
C. It uses symmetric-key encryption to protect data confidentiality.
D. It encrypts packets at Layer 3, which allows devices to handle packets in accordance with network policies.
E. It can be enabled on individual port at Layer 3 to allow MACsec devices to access the network.
F. It can use IEEE 802.1x master keys to encrypt wired and wireless links.

Answer: BC

NEW QUESTION 9
- (Exam Topic 2)
Which two statements about AMP. The Grid are true? (Choose two)

A. It can transmit suspected malware to the public AMP I threat Grid cloud for deeper analysis.
B. It provides two separate on premises appliances to support powerful malware analysis and threat intelligence features.
C. It provides dynamic analysis reports and generates threat scores.
D. It supports real-time threat and behavioral analysis.
E. It can be installed on individual endpoints to inspect local files for malware.
F. It can act as an anonymized proxy to transport endpoint event data to the public AMP I threat Grid cloud for threat detection.

Answer: BC

NEW QUESTION 10
- (Exam Topic 2)
Which difference between DomainKeys and DKIM in Cisco ESA deployment is true?

A. Only Domain Keys support incoming-mail authentication.
B. AsyncOS supports mail signing for DKIM only.
C. Bounce and delay messages can use DKIM only.
D. AsyncOS supports email authentication for DomainKeys only.
E. If DomainKeys and DKIM are associated to mail flow, AsyncOS uses only DKIM to sign outgoing messages.
F. Only DKIM supports incoming-mail verifications.

Answer: D

NEW QUESTION 11
- (Exam Topic 2)
Which two statements about internal detectors in the Cisco Firepower System are true? (Choose two)

A. They are built in to the Firepower system and delivered automatically with firepower updates.
B. They can be activated manually or configured to activate automatically under specific conditions.
C. They can be modified for use as custom detectors.
D. They can detect client and application traffic.
E. They can detect only web-based application activity in FTTP traffic.
F. They can be deactivated manually or by VDB updates.

Answer: AE

NEW QUESTION 12
- (Exam Topic 2)
Which two parameters must be identical per interface while configuring virtual port channels? (Choose two)

Guaranteed success with Our exam guides
visit - https://www.certshared.com
A. network access control  
B. IP sourceguard  
C. Protocol independent multicast  
D. Bridge Assurance setting  
E. maximum transmission unit

Answer: DE

NEW QUESTION 13  
- (Exam Topic 3)  
Which statement about the TLS security protocol is true?

A. TLS version 1.0 is less secure then SSL version 3.0  
B. The TLS and SSL versions can interoperate in the client-server handshake  
C. It is always recommended to disable TLS version 1.0 in the browser so that it only supports SSL for better security  
D. You need to replace SSL certificate with TLS certificate for successful TLS operation  
E. There are differences between TLS and SSL version 2 and 3  
F. It only supports data authentication for the client-server session using a browser

Answer: E

NEW QUESTION 14  
- (Exam Topic 3)  
Which description of a hybrid SDN framework is true?

A. The control plane and data plane are pulled from the networking element and put in an 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 an SDN controller.  
D. The control plane is pulled from the networking element and put in an SDN controller

Answer: B

NEW QUESTION 15  
- (Exam Topic 3)  
Which statement is true regarding x.509 certificate?

A. The version number in the certificate is the OS version of CA  
B. The Subject Distinguished Name in the certificate is of the entity who issued the certificate  
C. The algorithm in the certificate is used by the issuer to sign the certificate  
D. The serial number in the certificate is common across the certificates issued by the same CA  
E. The algorithm in the certificate is used by the subject to encrypt the traffic  
F. The Issuer Distinguished Name in the certificate is of the entity to which the certificate is issued

Answer: C

NEW QUESTION 16  
- (Exam Topic 3)  
Refer to the exhibit. Which two effects of this configuration are true? (Choose two.)  
Case Study Title (Case Study):
authentication priority dot1x mab authentication order dot1x mab authentication event fail action next-method authentication event server dead action reinitialize vlan 50 authentication host-mode multi-auth  
authentication violation restrict

A. If the TACACS+ server is unreachable, the switch places hosts on critical ports in VLAN 50  
B. The device allows multiple authenticated sessions for a single MAC address in the voice domain  
C. If multiple hosts have authenticated to the same port, each can be in their own assigned VLAN  
D. If the authentication priority is changed the order in which authentication is performed also changes  
E. The switch periodically sends an EAP-Identity-Request to the endpoint supplicant  
F. The port attempts 802.1x authentication first, and then falls back to MAC authentication bypass

Answer: A

NEW QUESTION 17  
- (Exam Topic 3)  
Transmission control protocol, src port: 649999(64999), Dst Port:49086(49086),Seq:2,Ack:2,Len: Refer to the exhibit.
Refer to the exhibit. The ASA at 150.1.7.43 is configured to receive the IP address to SGT mapping from ISE at 161.1.7.14. Which statement about this packet capture from Wireshark is true?

A. The TACACS connection keep alive using UDP originated from ASA
B. The SXP message uses TCP port 64999 for connection termination
C. The RADIUS connection keep alive using TCP originated from ISE
D. The SXP message uses MD5 for authentication and integrity check.
E. The ISE keep alive message for NDAC connection using TCP originated from ASA
F. The NTP keep alive message using UDP originated from ISE
G. The SXP keep alive message for SXP connection using UDP originated from ASA

Answer: D

NEW QUESTION 18
- (Exam Topic 3)
What would describe Cisco Virtual Topology System?

A. Package that contains an entire runtime environment
B. An agent that resides on physical devices
C. Web server hosting for NX-OS
D. Overlay provisioning and management solution

Answer: D

NEW QUESTION 19
- (Exam Topic 3)
A network architect has been tasked to migrate a customer's legacy infrastructure switches from Nexus 9000 platform. Which peers will help him achieve his milestone?

A. Create a container providing separate execution space
B. Manage software upgrades via guest shell
C. Setup a Web-based interface for configuration management.
D. Allow guests temporary access to the CLI without logging in.

Answer: A

NEW QUESTION 20
- (Exam Topic 3)
Which description of a Dockers file is true?

A. repository for Docker images
B. software used to manage containers
C. message daemon files
D. text document used to build an image

Answer: D

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 First Try
* 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