



Vendor: Cisco

Exam Code: 400-251

Exam Name: CCIE Security Written Exam v5.1

Version: Demo

QUESTION 1

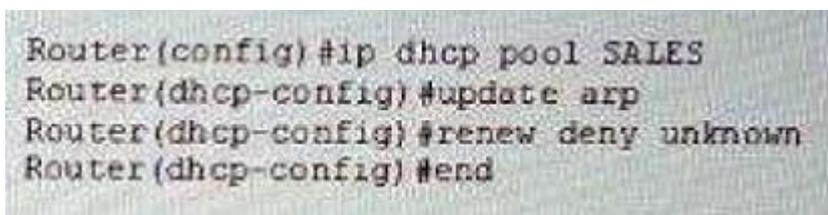
Which two statements about the Cognitive Threat Analytics feature of Cisco AMP for Web Security are true? (Choose two.)

- A. It can locate and identify indicators of prior malicious activity on the network and preserve information for forensic analysis.
- B. It can identify potential data exfiltration.
- C. It uses a custom virtual appliance to perform reputation-based evaluation and blocking of incoming files.
- D. It can perform file analysis by sandboxing known malware and comparing unknown files to a local repository of threats.
- E. It can identify anomalous traffic passing through the Web gateway by comparing it to an established baseline of expected activity.
- F. It can identify anomalous traffic within the network by comparing it to an established baseline of expected activity.

Correct Answer: BF

QUESTION 2

Refer to the exhibit. What feature does the given configuration implement?



```
Router(config)#ip dhcp pool SALES
Router(dhcp-config)#update arp
Router(dhcp-config)#renew deny unknown
Router(dhcp-config)#end
```

- A. DHCP Secured IP Address Assignment
- B. DHCP snooping
- C. dynamic ARP learning
- D. ARP probing

Correct Answer: A

QUESTION 3

Which statement about Health Monitoring on the Firepower System is true?

- A. When you delete a health policy that is applied to a device, the device reverts to the default health policy.
- B. If you apply a policy without active modules to a device, the previous health policy remains in

- effect unless you delete it.
- C. Health events are generated even when the health monitoring status is disabled.
 - D. Descendant domains in a multi-domain deployment can view, edit, and apply policies from ancestor domains.
 - E. The administrator of a descendant domain is unable to edit or delete blacklists applied by the administrator of an ancestor domain.
 - F. The default health policy is automatically applied to all managed devices.

Correct Answer: C

QUESTION 4

Which tunnel type does the Cisco Unified Wireless solution use to map a provisioned guest WLAN to an anchor WLC?

- A. EoIP
- B. TLS
- C. EAPoL
- D. PEAP
- E. GRE
- F. IPsec

Correct Answer: A

QUESTION 5

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.

Correct Answer: A

QUESTION 6

A client computer at 10.10.7.4 is trying to access a Linux server(11.0.1.9) that is running a Tomcat Server application. What TCP dump filter would be best to verify that traffic is reaching the Linux Server eth0 interface?

- A. tcpdump -l eth0 host 10.10.7.4 and host 11.0.1.9 and port 8080.
- B. tcpdump -l eth0 host 10.10.7.4 and 11.0.1.9.
- C. tcpdump -l eth0 dst 11.0.1.9 and dst port 8080.
- D. tcpdump -l eth0 src 10.10.7.4 and dst 11.0.1.9 and dst port 8080

Correct Answer: D

QUESTION 7

AMP for Endpoint is supported on which of these platforms?

- A. Windows, MAC, ANDROID
- B. Windows, MAC, LINUX (SuSE, UBUNTU), ANDROID
- C. Windows, ANDROID, LINUX (SuSE, REDHAT)
- D. Windows, ANDROID, LINUX (REDHA, CentOS), MAC

Correct Answer: D

QUESTION 8

Which three EAP protocols are supported in WPA and WPA2? (Choose three.)

- A. EAP-PSK
- B. EAP-EKE
- C. EAP-FAST
- D. EAP-AKA
- E. EAP-SIM
- F. EAP-EEE

Correct Answer: CDE

QUESTION 9

Which three statements about VXLAN are true? (Choose three.)

- A. It can converge topology without STP.
- B. It enables up to 24 million VXLAN segments to coexist in the same administrative domain.

- C. It uses encrypted TCP/IP packets to transport data over the physical network.
- D. The VTEP encapsulates and de-encapsulates VXLAN traffic by adding or removing several fields, including a 16-bit VXLAN header.
- E. It uses a 24-bit VXLAN network identifier to provide layer 2 isolation between LAN segments.
- F. It can migrate a virtual machine from one Layer 2 domain to another over a Layer 3 network.

Correct Answer: ADE

QUESTION 10

Refer to the exhibit. Which service of feature must be enabled on 209.165.200.255 to produce the given output?

```

r1#telnet 209.165.200.225 19
Trying 209.165.200.225, 19 ...
Open
abcdefghijklmnopqrstuvwxyz{|~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHI
bcdefghijklmnopqrstuvwxyz{|~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJ
cdefghijklmnopqrstuvwxyz{|~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJK
defghijklmnopqrstuvwxyz{|~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKL
efghijklmnopqrstuvwxyz{|~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLM
fghijklmnopqrstuvwxyz{|~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMN
ghijklmnopqrstuvwxyz{|~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNO
hijklmnopqrstuvwxyz{|~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNQP
ijklmnopqrstuvwxyz{|~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNQPQ
jklmnopqrstuvwxyz{|~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNQPQR
    
```

- A. the Finger service
- B. a BOOTP server
- C. a TCP small server
- D. the PAD service

Correct Answer: C

QUESTION 11

When you use the Firepower Management Center to deploy an access control policy to a managed device, which process is restarted?

- A. kupdate
- B. snort
- C. crond
- D. reportd
- E. mysqld

Correct Answer: B

QUESTION 12

Which statement about the Firepower Security Intelligence feature is true?

- A. It uses user-configured ACLs to blacklist and whitelist traffic
- B. It can override custom whitelists to provide greater security against emerging threats
- C. It filters traffic after policy-based inspection is complete and before the default action is taken
- D. Blacklisted traffic is blocked without further inspection
- E. It filters traffic after policy-based inspection is completed and the default action is taken

Correct Answer: D

QUESTION 13

Which three statements about communication between Cisco VSG and the VEM are true?

(Choose three.)

- A. In Layer 3 mode, fragmentation with vPath is not supported.
- B. vPath handled fragmentation for all adjacencies between Cisco VSG and the VEM.
- C. If vPath encapsulation of a packet in Layer 2 mode causes the packet to exceed the interface MTU size, it will be dropped.
- D. Layer 3 adjacency between Cisco VSG and the VEM requires communication through a VMkernel interface on the VEM.
- E. vPath encapsulation of incoming packets can increase the frame size by up to 94 bytes.
- F. Cisco VSG and VEM should be adjacent at Layer 3 when minimal latency is required.

Correct Answer: ADE

QUESTION 14

Which statement about Password Authentication Protocol is true?

- A. RADIUS -based PAP authentication logs successful authentication attempts only.
- B. Its password is encrypted with a certificate.
- C. It offers strong protection against brute force attacks.
- D. RADIUS -based PAP authentication is based on the RADIUS Password attribute
- E. It is the most secure authentication method supported for authentication against the internal Cisco ISE database
- F. It uses a two-way handshake with an encrypted password

Correct Answer: D