Cisco

400-251 Exam

Cisco CCIE Security Exam

Thank you for Downloading 400-251 exam PDF Demo

You can Buy Latest 400-251 Full Version Download

https://www.certkillers.net/Exam/400-251

Version: 8.0

Question: 1

A server with IP address 209.165.202.150 is protected behind the inside interface of a Cisco ASA and the Internet on the outside interface. User on the Internet need to access the server ay any time, but the firewall administrator does not want to apply NAT to the address of the server because it is currently a public address. Which three of the following commands can be used to accomplish this? (Choose three.)

A. static (outside, inside) 209.165.202.150.209.165.202.150 netmask 255.255.255.255
B. nat (inside) 1 209.165.202.150 255.255.255.255
C. static (inside, outside) 209.165.202.150.209.165.202.150 netmask 255.255.255.255
D. no nat-control
E. access-list no-nat permit ip host 209.165.202.150 any
nat (inside) 0 access-list no-nat
F. nat (inside) 0 209.165.202.150 255.255.255.255

Answer: CEF

Question: 2

Which statement about the Cisco AMP Virtual Private Cloud Appliance is true for deployments in air-gapmode?

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

Question: 3

What are the most common methods that security auditors use to access an organization's security processes? (Choose two.)

A. physical observation
B. social engineering attempts
C. penetration testing
D. policy assessment
E. document review
F. interviews

Answer: AF

Question: 4

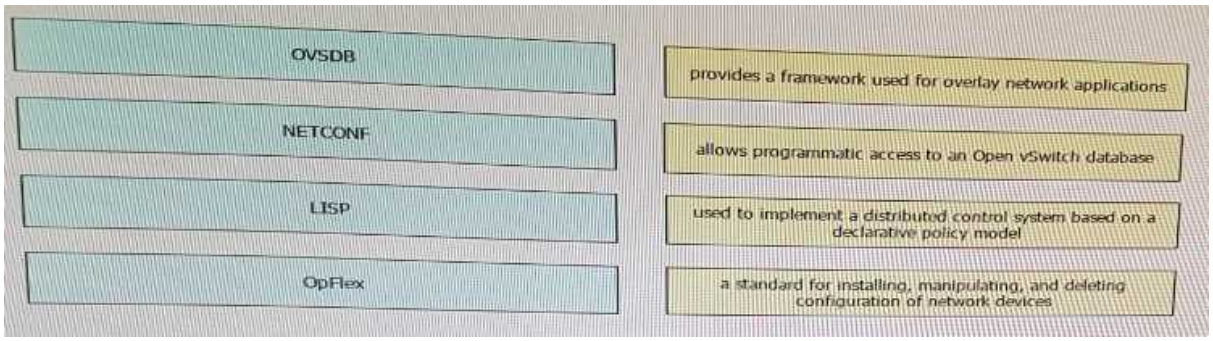
Which two statements about Cisco AMP for Web Security are true? (Choose two.)

A. It can prevent malicious data exfiltration by blocking critical files from exiting through the Web gateway.
B. It can perform reputation-based evaluation and blocking by uploading the fingerprint of incoming files to a cloud-based threat intelligence network.
C. It can detect and block malware and other anomalous traffic before it passes through the Web gateway.
D. It can perform file analysis by sandboxing known malware and comparing unknown files to a local repository of the threats.
E. It can identify anomalous traffic passing through the Web gateway by comparing it to an established of
expected activity.
F. It continues monitoring files after they pass the Web gateway.

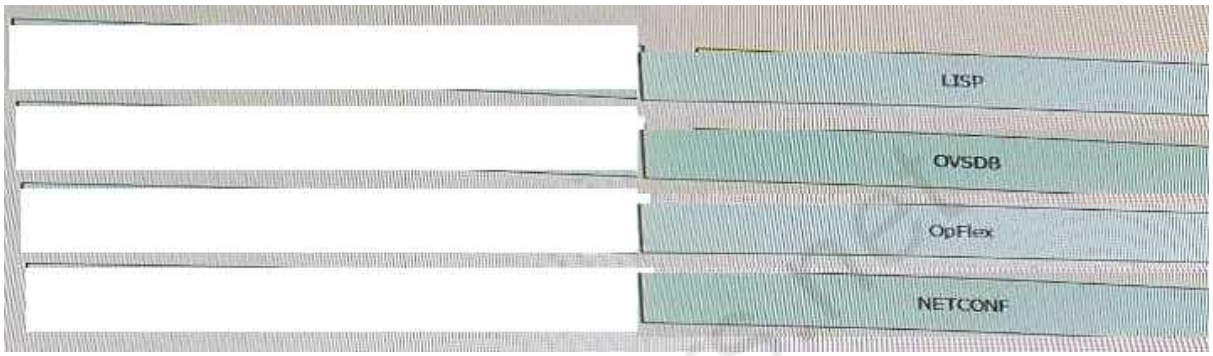
Answer: BF

Question: 5

DRAG DROP
Drag and drop the protocol on the left onto their description on the right:



Answer:



Question: 6

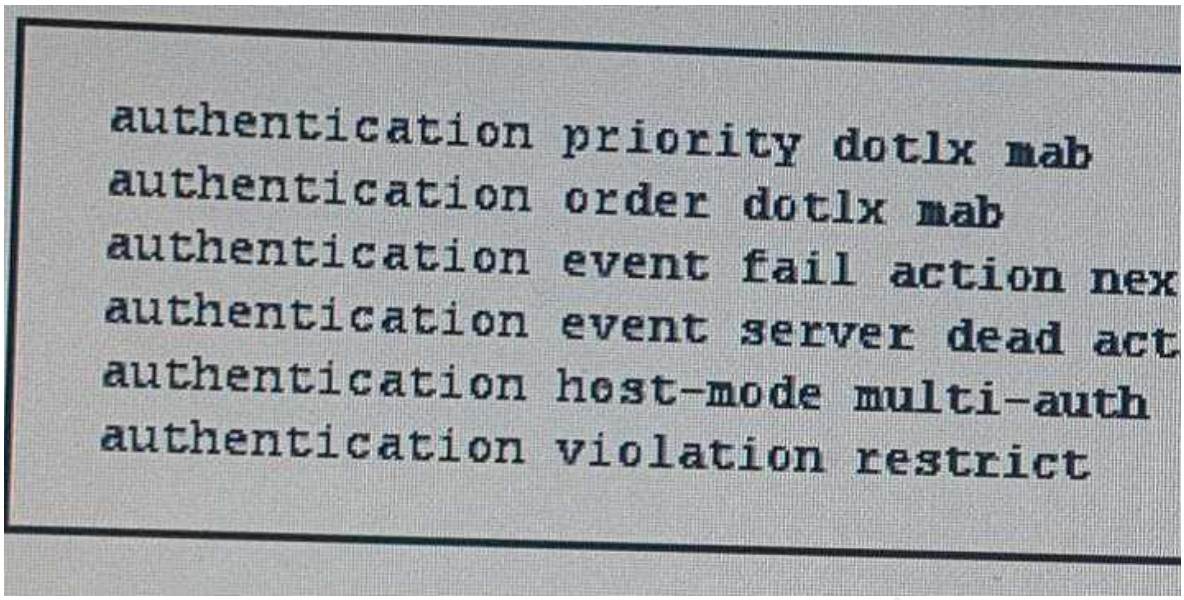
What are two features that helps to mitigate man-in-the-middle attacks? (Choose two.)

A. DHCP snooping
B. ARP spoofing
C. destination MAC ACLs
D. dynamic ARP inspection
E. ARP sniffing on specific ports

Answer: AD

Question: 7

Refer to the exhibit.



Which two effects of this configuration are true? (Choose two.)

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

Answer: CF

Question: 8

Which two statements about 6to4 tunneling are true? (Choose two.)

A. It provides a /128 address block.
B. It supports static and BGPV4 routing.
C. It provides a /48 address block.
D. It supports managed NAT along the path of the tunnel.
E. The prefix address of the tunnel is determined by the IPv6 configuration of the interface.
F. It supports multihoming.

Answer: BC

Question: 9

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

A. It detects rogue access points that are connected to the wired network.
B. It can detect rogue APs that use WPA encryption.
C. It can detect rogue APs operating only on 5 GHz.
D. It can detect rogue APs that use WEP encryption.
E. The AP is unable to serve clients while the RLDP process is active.
F. Active Rogue Containment can be initiated manually against rogue devices detected on the wired network.

Answer: AEF

Explanation:
Rogue Location Discovery Protocol (RLDP)
http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70987-rogue-detect

Question: 10

What are three features that are enabled by generating Change of Authorization (CoA) requests in a push model? (Choose three.)

A. session reauthentication
B. session identification
C. host reauthentication
D. MAC identification
E. session termination
F. host termination

Answer: BCE

Thank You for trying 400-251 PDF Demo

To Buy Latest 400-251 Full Version Download visit link below

https://www.certkillers.net/Exam/400-251

Start Your 400-251 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your 400-251 preparation with actual exam questions.