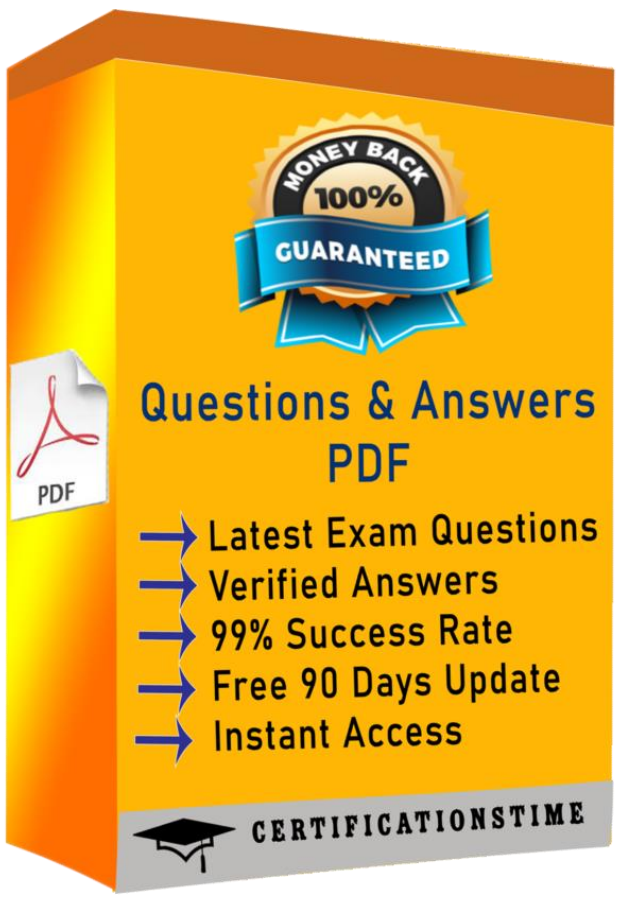
Cisco

Exam Questions 400-251

CCIE Security Written Exam

https://certificationstime.com/



Question: 1

Version: 24.0
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 airgapmode?
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 thatsecurity 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 passthe Web gateway.
Answer: BF

Question: 5

Which three statements about WCCP are true? (Choose three.)
A. The minimum WCCP-Fast Timers messages interval is 500 ms
B. Is a specific capability is missing from the Capabilities Info component, the router is assumed to support
the default capability
C. If the packet return method is missing from a packet return method advertisement, the web cache uses
the Layer 2 rewrite method
D. The router must receive a valid receive ID before it negotiates capabilities
E. The assignment method supports GRE encapsulation for sending traffic
F. The web cache transmits its capabilities as soon as it receives a receive ID from router
Answer: ACE
Explanation:
Web Cache Communication Protocol (WCCP)
http://www.cisco.com/c/en/us/td/docs/security/asa/special/wccp/guide/asa-wccp.html

Question: **6**

What are two featuresthat 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