Cisco

400-251 Exam

Cisco CCIE Security Exam

Questions & Answers
Demo

Version: 24.0

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

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

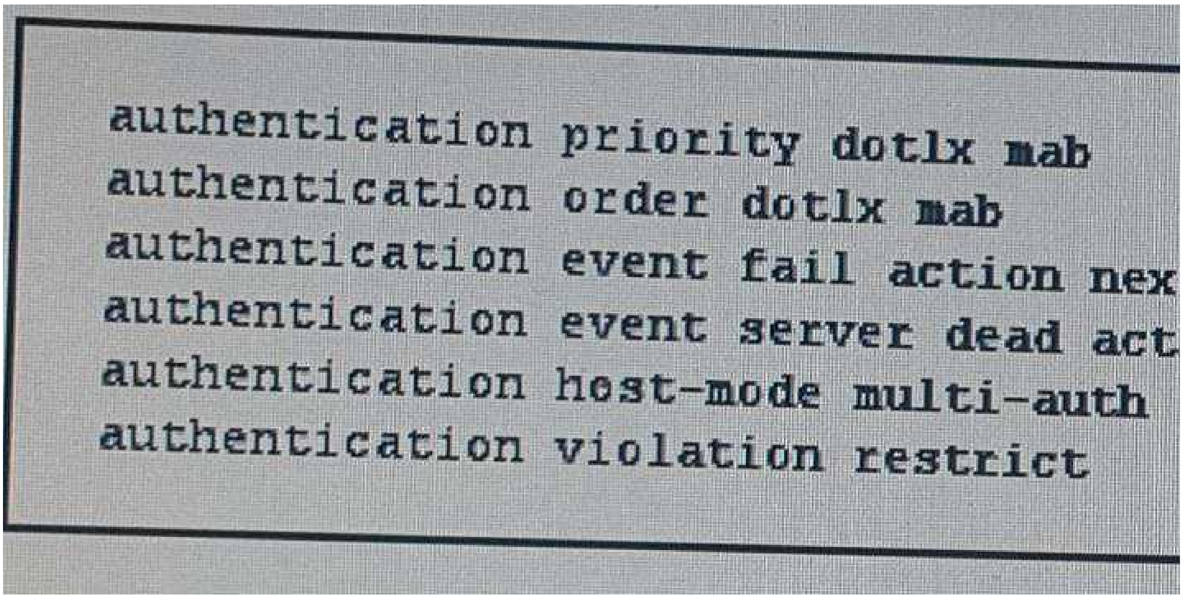
What are two features that helps to mitigate man-in-the-middle attacks? (Choose two.)

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.



```
authentication priority dotlx mab
authentication order dotlx mab
authentication event fail action nex
authentication event server dead act
authentication host-mode multi-auth
authentication violation restrict
```

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.html

Question: 10

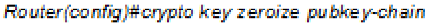
What are three features that are enabled by generating Change of Authorization (CoA) requests in a push
model? (Choose three.)

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

Answer: BCE

Question: 11

Refer to the exhibit.



```
Router(config)#crypto key zeroize pubkey-chain
```

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

Question: 12

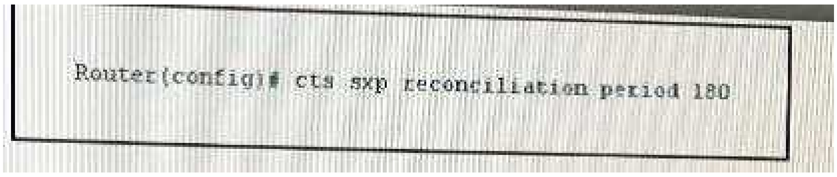
Which two statements about a wireless access point configured with the guest-mode command are true?
(Choose two.)

A. It can support more than one guest-mode SSID.
B. It supports associations by clients that perform passive scans.
C. It allows clients configured without SSIDs to associate.
D. It allows associated clients to transmit packets using its SSID.
E. If one device on a network is configure in guest-mode, clients can use the guest-mode SSID to connect
to any device in the same network.

Answer: BC

Question: 13

Refer to the exhibit.



```
Router(config)# cts sxp reconciliation period 180
```

Which two statements about a device with this configuration are true? (Choose two.)

A. When a peer establishes a new connection to the device, CTS retains all existing SGT mapping entries
for 3 minutes.
B. If a peer reconnects to device within 120 seconds of terminating a CTS-SXP connection, the reconciliation timer stats.

C. When a peer re-establishes a previous connection to the device, CTS retains all existing SGT mapping
entries for 3 minutes.
D. If a peer reconnects to device within 180 seconds of terminating a CTS-SXP connection, the reconciliation timer stats.
E. If a peer re-establishes a connection to the device before the hold-down timer expires, the device retains the SGT mapping entries it learned during the previous connection for an additional 3 minutes.
F. It sets the internal hold-down timer of the device to 3 minutes.

Answer: BE

Question: 14

Which option is a data modeling language used to model configuration and state data of network elements?

A. RESTCONF
B. SNMPv4
C. NETCONF
D. YANG

Answer: D

Question: 15

Which statement about MDM with the Cisco ISE is true?

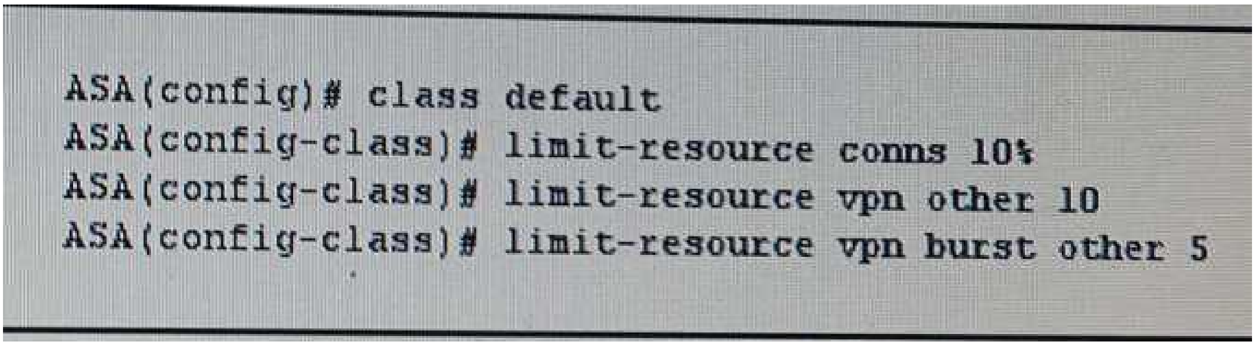
A. The MDM's server certificate must be imported into the Cisco ISE Certificate Store before the MDM and
ISE can establish a connection.
B. MDM servers can generate custom ACLs for the Cisco ISE to apply to network devices.
C. The Cisco ISE supports a built-in list of MDM dictionary attributes it can use in authorization policies.
D. The Cisco ISE supports limited built-in MDM functionality.
E. If a mobile endpoint fails posture compliance, both the user and the administrator are notified immediately.
F. When a mobile endpoint becomes compliant the Cisco ISE records the updated device status in its internal database.

Answer: A

Explanation:
Mobile Device Management
https://meraki.cisco.com/blog/tag/mobile-device-management/

Question: 16

Refer to the exhibit.



```
ASA(config)# class default
ASA(config-class)# limit-resource conns 10%
ASA(config-class)# limit-resource vpn other 10
ASA(config-class)# limit-resource vpn burst other 5
```

What is the maximum number of site-to-site VPNs allowed by this configuration?

A. 10
B. unlimited
C. 5
D. 0
E. 1
F. 15

Answer: F

Question: 17

When applying MD5 route authentication on routers running RIP or EIGRP, which two important key chain considerations should be accounted for? (Choose two.)

A. Key 0 of all key chains must match for all routers in the autonomous system.
B. The lifetimes of the keys in the chain should overlap.
C. Routers should be configured for NTP to synchronize their clocks.
D. No more than three keys should be configured in any single chain.
E. Link compression techniques should be disabled on links transporting any MD5 hash.

Answer: BC

Question: 18

Which description of SaaS is true?

A. a service offering on-demand licensed applications for end users
B. a service offering that allowing developers to build their own applications
C. a service offering on-demand software downloads
D. a service offering a software environment in which applications can be build and deployed.

Answer: A

Question: 19

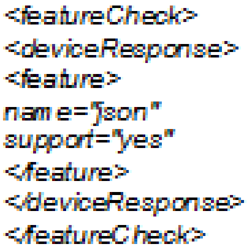
Which two statements about ICMP redirect messages are true? (Choose two.)

A. Redirects are only punted to the CPU if the packets are also source-routed.
B. The messages contain an ICMP Type 3 and ICMP code 7.
C. By default, configuring HSRP on the interface disables ICMP redirect functionality.
D. They are generated when a packet enters and exits the same route interface.
E. They are generated by the host to inform the router of an temate route to the destination.

Answer: CD

Question: 20

Refer to the exhibit.



```
<featureCheck>
<deviceResponse>
<feature>
name="json"
support="yes"
</feature>
</deviceResponse>
</featureCheck>
```

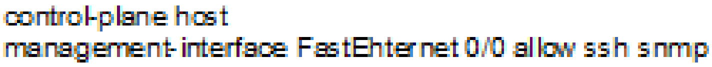
Which data format is used in this script?

A. JSON
B. YANG
C. API
D. XML
E. JavaScript

Answer: D

Question: 21

Refer to the exhibit.



```
control-plane host
management-interface FastEhternet 0/0 allow ssh snmp
```

What is the effect of the given command?
control-plane host
management-interface FastEhternet 0/0 allow ssh snmp

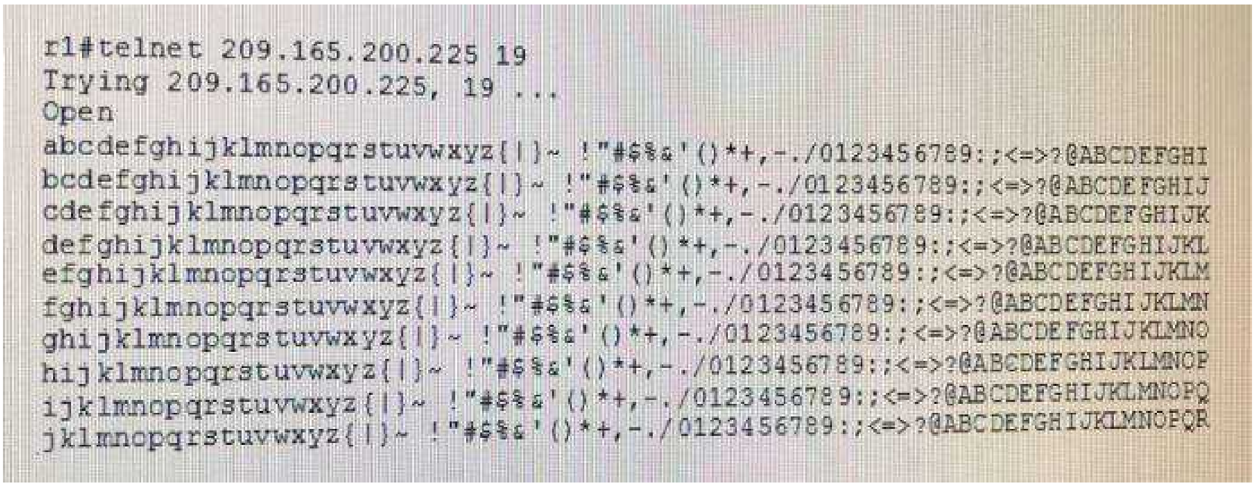
A. It enables CoPP on the FastEthernet 0/0 interface for SSH and SNMP management traffic.
B. It enables QoS policing on the control plane of the FastEthernet 0/0 interface.
C. It enables MPP on the FastEthernet 0/0 interface, allowing only SSH and SNMP management

traffic.
D. It enables MPP on the FastEthernet 0/0 interface by enforcing rate-limiting for SSH and SNMP management traffic.
E. It enables MPP on the FastEthernet 0/0 interface for SNMP management traffic and CoPP for all other
protocols.

Answer: C

Question: 22

Refer to the exhibit.



```
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:;<=>?@ABCDEFGHIJKLMNOP
ijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQ
jklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQR
```

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

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

Answer: C

Question: 23

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

Question: 24

Which OpenStack project has orchestration capabilities?

A. Cinder
B. Horizon
C. Sahara
D. Heat

Answer: D

Question: 25

Which feature does Cisco VSG use to redirect traffic in a Cisco Nexus 1000v Series Switch?

A. VEM
B. VPC
C. VDC
D. vPath

Answer: D

Question: 26

What is the purpose of the BGP TTL security check?

A. to check for a TTL value in packet header of less than or equal to for successful peering
B. to protect against routing table corruption
C. to use for iBGP session
D. to protect against CPU utilization-based attacks
E. to authenticate a peer

Answer: D

Question: 27

Which three of these are properties of RC4? (Choose three.)

A. It is a block cipher.
B. It is a stream cipher.
C. It is used in AES.
D. It is a symmetric cipher.
E. It is used in SSL.
F. It is an asymmetric cipher.

Answer: BDE

Question: 28

Which two statements about role-based access control are true? (Choose two.)

A. The user profile on an AAA server is configured with the roles that grant user privileges.
B. If the same user name is used for a local user account and a remote user account, the roles defined in
the remote user account override the local user account.
C. Server profile administrators have read and write access to all system logs by default.
D. A view is created on the Cisco IOS device to leverage role-based access controls.
E. Network administrators have read and write access to all system logs by default.

Answer: AD

Question: 29

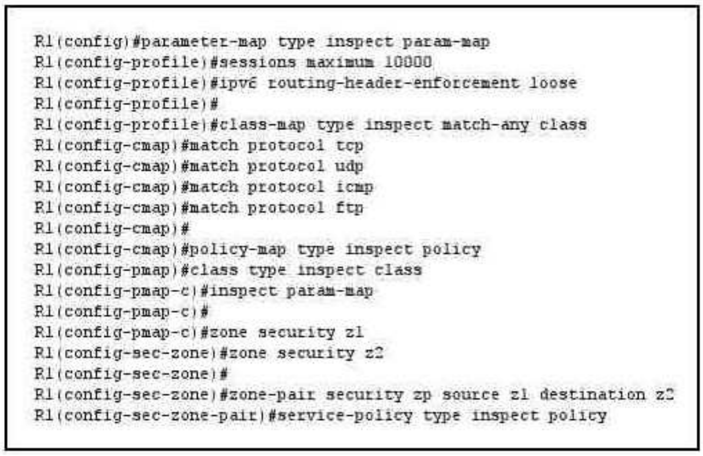
What is an example of a stream cipher?

A. RC4
B. RC5
C. DES
D. Blowfish

Answer: A

Question: 30

Refer to the exhibit.



```
R1(config)#parameter-map type inspect param-map
R1(config-profile)#sessions maximum 10000
R1(config-profile)#ipv6 routing-header-enforcement loose
R1(config-profile)#
R1(config-profile)#class-map type inspect match-any class
R1(config-cmap)#match protocol tcp
R1(config-cmap)#match protocol udp
R1(config-cmap)#match protocol icmp
R1(config-cmap)#match protocol ftp
R1(config-cmap)#
R1(config-cmap)#policy-map type inspect policy
R1(config-pmap)#class type inspect class
R1(config-pmap-c)#inspect param-map
R1(config-pmap-c)#
R1(config-pmap-c)#zone security z1
R1(config-sec-zone)#zone security z2
R1(config-sec-zone)#
R1(config-sec-zone)#zone-pair security zp source z1 destination z2
R1(config-sec-zone-pair)#service-policy type inspect policy
```

d

Which two statements about the given IPv6 ZBF configuration are true? (Choose two.)

A. It inspects TCP, UDP, ICMP, and FTP traffic from z1 to z2.
B. It provides backward compatibility with legacy IPv4 inspection.
C. It inspects TCP, UDP, ICMP, and FTP traffic from z2 to z1.
D. It passes TCP, UDP, ICMP, and FTP traffic in both directions between z1 and z2.
E. It provides backward compatibility with legacy IPv6 inspection.
F. It passes TCP, UDP, ICMP, and FTP traffic from z1 to z2.

Answer: AE

Question: 31

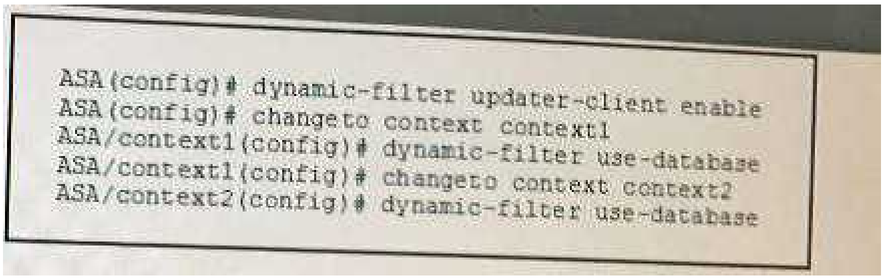
Which three options are fields in a CoA Request Response code packet? (Choose three.)

A. Length
B. Acct-session-ID
C. Calling-station-ID
D. Identifier
E. Authenticator
F. State

Answer: BCF

Question: 32

Refer to the exhibit.



```
ASA(config)# dynamic-filter updater-client enable
ASA(config)# changeto context context1
ASA/context1(config)# dynamic-filter use-database
ASA/context1(config)# changeto context context2
ASA/context2(config)# dynamic-filter use-database
```

What are two effects of the given configuration? (Choose two.)

A. It enables the ASA to download the static botnet filter database.
B. It enables the ASA to download the dynamic botnet filter database.
C. It enables botnet filtering in single context mode.
D. It enables botnet filtering in mutiple context mode.
E. It enables multiple context mode.
F. It enables single context mode.

Answer: BD

Question: 33

What are the three scanning engines that the Cisco IronPort dynamic vectoring and streaming engine can
use to protect against malware? (Choose three.)

A. McAfee
B. TrendMicro
C. Sophos
D. Webroot
E. F-Secure
F. Symantec

Answer: ACD

Question: 34

Which option best describes RPL?

A. RPL stands for Routing over low priority links that use link-state LSAs to determine the best route between two root border routers.
B. RPL stands for Routing over low priority links that use distance vector DOGAG to determine the best
route between two root border routers.
C. RPL stands for Routing over Low-power Lossy Networks that use link-state LSAs to determine the best
route between leaves and the root border router.
D. RPL stands for Routing over Low-power Lossy Networks that use distance vector DOGAG to determine
the best route between leaves and the root border router.

Answer: D

Question: 35

Which command sequence do you enter to add the host 10.2.1.0 to the CISCO object group?

A. object-group network CISCO
group-object 10.2.1.0
B. object network CISCO
network-object object 10.2.1.0
C. object-group network CISCO
network-object host 10.2.1.0
D. object network CISCO
group-object 10.2.1.0

Answer: C

Question: 36

Which two options are benefits of network summarization? (Choose two.)

A. It prevents unnecessary routing updates at the summarization boundary if one of the routes in the summary is unstable.
B. It can increase the convergence of the network.
C. It can summarize discontiguous IP addresses.
D. It can easily be added to existing networks.
E. It reduces the number of routes.

Answer: AE