www.certifyguide.com

ExamCode: NSE4
ExamName: Fortinet Network Security Expert 4 Written Exam (400)
➢ Total Questions: 273

Question: 1

When creating FortiGate administrative users, which configuration objects specify the account rights?

A. Remote access profiles.
B. User groups.
C. Administrator profiles.
D. Local-in policies.

Answer: C

Question: 2

Which statements are true regarding the factory default configuration? (Choose three.)

A. The default web filtering profile is applied to the first firewall policy.
B. The 'Port1' or 'Internal' interface has the IP address 192.168.1.99.
C. The implicit firewall policy action is ACCEPT.
D. The 'Port1' or 'Internal' interface has a DHCP server set up and enabled (on device models that support DHCP servers).
E. Default login uses the username: admin (all lowercase) and no password.

Answer: B, D, E

Question: 3

What are valid options for handling DNS requests sent directly to a FortiGates interface IP? (Choose three.)

A. Conditional-forward.
B. Forward-only.
C. Non-recursive.
D. Iterative.
E. Recursive.

Answer: B, C, E

Question: 4

What logging options are supported on a FortiGate unit? (Choose two.)

A. LDAP
B. Syslog
C. FortiAnalyzer
D. SNMP

Answer: B, C

Question: 5

Regarding the header and body sections in raw log messages, which statement is correct?

A. The header and body section layouts change depending on the log type.
B. The header section layout is always the same regardless of the log type. The body section layout changes depending on the log type.
C. Some log types include multiple body sections.
D. Some log types do not include a body section.

Answer: B

Question: 6

Which is an advantage of using SNMP v3 instead of SNMP v1/v2 when querying a FortiGate unit?

A. MIB-based report uploads.
B. SNMP access limited by access lists.
C. Packet encryption.
D. Running SNMP service on a non-standard port is possible.

Answer: C

Question: 7

What is the maximum number of FortiAnalyzer/FortiManager devices a FortiGate unit can be configured to send logs to?

A. 1
B. 2
C. 3
D. 4

Answer: C

Question: 8

For traffic that does match any configured firewall policy, what is the default action taken by the FortiGate?

A. The traffic is allowed and no log is generated.
B. The traffic is allowed and logged.
C. The traffic is blocked and no log is generated.
D. The traffic is blocked and logged.

Answer: C

Question: 9

In which order are firewall policies processed on a FortiGate unit?

A. From top to down, according with their sequence number.
B. From top to down, according with their policy ID number.
C. Based on best match.
D. Based on the priority value.

Answer: A

Question: 10

Which firewall objects can be included in the Destination Address field of a firewall policy? (Choose three.)

A. IP address pool.
B. Virtual IP address.
C. IP address.
D. IP address group.
E. MAC address.

Answer: B, C, D

Question: 11

The order of the firewall policies is important. Policies can be re-ordered from either the GUI or the CLI. Which CLI command is used to perform this function?

A. set order
B. edit policy
C. reorder
D. move

Answer: D

Question: 12

Which header field can be used in a firewall policy for traffic matching?

A. ICMP type and code.
B. DSCP.
C. TCP window size.
D. TCP sequence number.

Answer: A

Question: 13

Examine the following CLI configuration:
config system session-ttl
  set default 1800
end
What statement is true about the effect of the above configuration line?

A. Sessions can be idle for no more than 1800 seconds.
B. The maximum length of time a session can be open is 1800 seconds.
C. After 1800 seconds, the end user must re-authenticate.
D. After a session has been open for 1800 seconds, the FortiGate sends a keepalive packet to both client and server.

Answer: A

Question: 14

Which statement regarding the firewall policy authentication timeout is true?

A. It is an idle timeout. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user’s source IP.
B. It is a hard timeout. The FortiGate removes the temporary policy for a user’s source IP address after this timer has expired.
C. It is an idle timeout. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user’s source MAC.
D. It is a hard timeout. The FortiGate removes the temporary policy for a user’s source MAC address after this timer has expired.

Answer: A

Question: 15

What methods can be used to deliver the token code to a user that is configured to use two-factor authentication? (Choose three.)

A. Browser pop-up window.
B. FortiToken.
C. Email.
D. Code books.
E. SMS phone message.

Answer: B, C, E

Question: 16

Which statements are true regarding local user authentication? (Choose two.)

A. Two-factor authentication can be enabled on a per user basis.
B. Local users are for administration accounts only and cannot be used to authenticate network users.
C. Administrators can create the user accounts is a remote server and store the user passwords locally in the FortiGate.
D. Both the usernames and passwords can be stored locally on the FortiGate

Answer: A, D

Question: 17

Which two statements are true regarding firewall policy disclaimers? (Choose two.)

A. They cannot be used in combination with user authentication.
B. They can only be applied to wireless interfaces.
C. Users must accept the disclaimer to continue.
D. The disclaimer page is customizable.

Answer: C, D

Question: 18

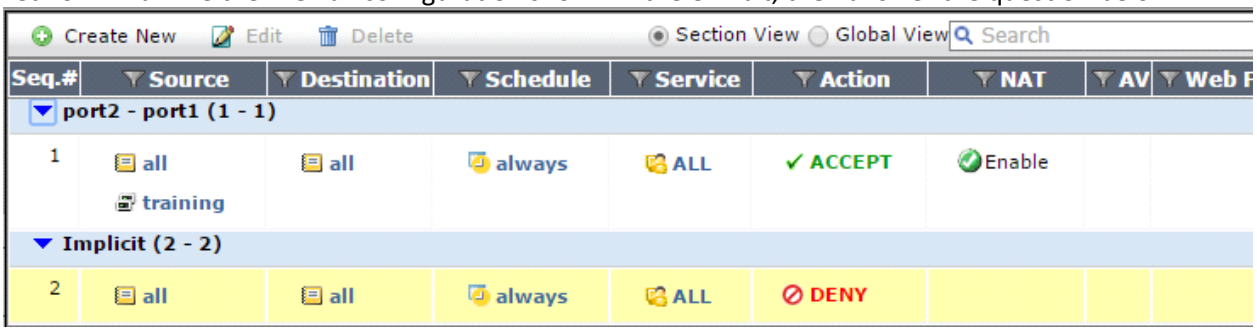
When firewall policy authentication is enabled, which protocols can trigger an authentication challenge? (Choose two.)

A. SMTP
B. POP3
C. HTTP
D. FTP

Answer: C, D

Question: 19

The FortiGate port1 is connected to the Internet. The FortiGate port2 is connected to the internal network. Examine the firewall configuration shown in the exhibit; then answer the question below.



Based on the firewall configuration illustrated in the exhibit, which statement is correct?

A. A user that has not authenticated can access the Internet using any protocol that does not trigger an authentication challenge.
B. A user that has not authenticated can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP.

C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access all Internet services.
D. DNS Internet access is always allowed, even for users that has not authenticated.

Answer: D

Question: 20

Regarding tunnel-mode SSL VPN, which three statements are correct? (Choose three.)

A. Split tunneling is supported.
B. It requires the installation of a VPN client.
C. It requires the use of an Internet browser.
D. It does not support traffic from third-party network applications.
E. An SSL VPN IP address is dynamically assigned to the client by the FortiGate unit.

Answer: A, B, E

Question: 21

Which two statements are true about IPsec VPNs and SSL VPNs? (Choose two.)

A. SSL VPN creates a HTTPS connection. IPsec does not.
B. Both SSL VPNs and IPsec VPNs are standard protocols.
C. Either a SSL VPN or an IPsec VPN can be established between two FortiGate devices.
D. Either a SSL VPN or an IPsec VPN can be established between an end-user workstation and a FortiGate device.

Answer: A, D

Question: 22

A user logs into a SSL VPN portal and activates the tunnel mode. The administrator has enabled split tunneling. The exhibit shows the firewall policy configuration:

Which static route is automatically added to the client's routing table when the tunnel mode is activated?

A. A route to a destination subnet matching the Internal_Servers address object.
B. A route to the destination subnet configured in the tunnel mode widget.
C. A default route.
D. A route to the destination subnet configured in the SSL VPN global settings.

Answer: A

Question: 23

When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

A. The remote user's virtual IP address.
B. The FortiGate unit's internal IP address.
C. The remote user's public IP address.
D. The FortiGate unit's external IP address.

Answer: B

Question: 24

Regarding the use of web-only mode SSL VPN, which statement is correct?

A. It supports SSL version 3 only.
B. It requires a Fortinet-supplied plug-in on the web client.
C. It requires the user to have a web browser that supports 64-bit cipher length.
D. The JAVA run-time environment must be installed on the client.

Answer: C

Question: 25

An administrator wants to create an IPsec VPN tunnel between two FortiGate devices.
Which three configuration steps must be performed on both units to support this scenario? (Choose three.)

A. Create firewall policies to allow and control traffic between the source and destination IP addresses.
B. Configure the appropriate user groups to allow users access to the tunnel.
C. Set the operating mode to IPsec VPN mode.
D. Define the phase 2 parameters.
E. Define the Phase 1 parameters.

Answer: A, D, E

Question: 26

You are the administrator in charge of a FortiGate acting as an IPsec VPN gateway using route-based mode. Users from either side must be able to initiate new sessions. There is only 1 subnet at either end and the FortiGate already has a default route.
Which two configuration steps are required to achieve these objectives? (Choose two.)

A. Create one firewall policy.
B. Create two firewall policies.
C. Add a route to the remote subnet.
D. Add two IPsec phases 2.

Answer: B, C

Question: 27

An administrator has configured a route-based site-to-site IPsec VPN. Which statement is correct regarding this IPsec VPN configuration?

A. The IPsec firewall policies must be placed at the top of the list.
B. This VPN cannot be used as part of a hub and spoke topology.
C. Routes are automatically created based on the quick mode selectors.
D. A virtual IPsec interface is automatically created after the Phase 1 configuration is completed.

Answer: D

Question: 28

What is IPsec Perfect Forwarding Secrecy (PFS)?.

A. A phase-1 setting that allows the use of symmetric encryption.
B. A phase-2 setting that allows the recalculation of a new common secret key each time the session key expires.
C. A 'key-agreement' protocol.
D. A 'security-association-agreement' protocol.

Answer: B

Question: 29

Which IPsec configuration mode can be used for implementing GRE-over-IPsec VPNs?.

A. Policy-based only.
B. Route-based only.
C. Either policy-based or route-based VPN.
D. GRE-based only.

Answer: B

Question: 30

Which antivirus and attack definition update options are supported by FortiGate units? (Choose two.)

A. Manual update by downloading the signatures from the support site.
B. Pull updates from the FortiGate.
C. Push updates from a FortiAnalyzer.
D. execute fortiguard-AV-AS command from the CLI.

Answer: A, B

Question: 31

Which antivirus inspection mode must be used to scan SMTP, FTP, POP3 and SMB protocols?

A. Proxy-based.

B. DNS-based.
C. Flow-based.
D. Man-in-the-middle.

Answer: C

Question: 32

Which statements regarding banned words are correct? (Choose two.)

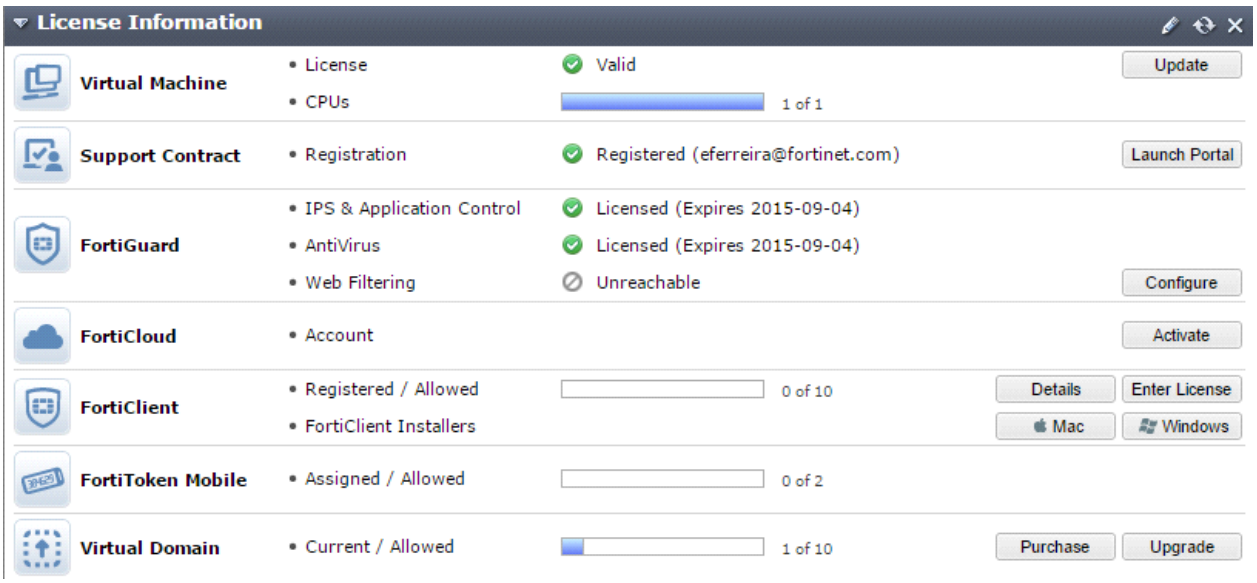
A. Content is automatically blocked if a single instance of a banned word appears.
B. The FortiGate updates banned words on a periodic basis.
C. The FortiGate can scan web pages and email messages for instances of banned words.
D. Banned words can be expressed as simple text, wildcards and regular expressions.

Answer: C, D

Question: 33

Examine the exhibit; then answer the question below

.



Which statement describes the green status indicators that appear next to the different FortiGuard Distribution Network services as illustrated in the exhibit?

A. They indicate that the FortiGate has the latest updates available from the FortiGuard Distribution Network.
B. They indicate that updates are available and should be downloaded from the FortiGuard Distribution Network to the FortiGate unit.

C. They indicate that the FortiGate is in the process of downloading updates from the FortiGuard Distribution Network.
D. They indicate that the FortiGate is able to connect to the FortiGuard Distribution Network.

Answer: D

Question: 34

A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, updates are not being received.
Which are two reasons for this problem? (Choose two.)

A. The FortiGate is connected to multiple ISPs.
B. There is a NAT device between the FortiGate and the FortiGuard Distribution Network.
C. The FortiGate is in Transparent mode.
D. The external facing interface of the FortiGate is configured to get the IP address from a DHCP server.

Answer: B, D

Question: 35

Which statements are true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

A. Only one proxy is supported.
B. Can be manually imported to the browser.
C. The browser can automatically download it from a web server.
D. Can include a list of destination IP subnets where the browser can connect directly to without using a proxy.

Answer: C, D

Question: 36

Examine the following FortiGate web proxy configuration; then answer the question below:

```
config web-proxy explicit
  set pac-file-server-status enable
  set pac-file-server-port 8080
  set pac-file-name wpad.dat
 end
```

Assuming that the FortiGate proxy IP address is 10.10.1.1, which URL must an Internet browser use to download the PAC file?

A. https://10.10.1.1:8080
B. https://10.10.1.1:8080/wpad.dat
C. http://10.10.1.1:8080/
D. http://10.10.1.1:8080/wpad.dat

Answer: D

Question: 37

Which two methods are supported by the web proxy auto-discovery protocol (WPAD) to automatically learn the URL where a PAC file is located? (Choose two.)

A. DHCP
B. BOOTP
C. DNS
D. IPv6 autoconfiguration

Answer: A, C

Question: 38

What is a valid reason for using session based authentication instead of IP based authentication in a FortiGate web proxy solution?

A. Users are required to manually enter their credentials each time they connect to a different web site.
B. Proxy users are authenticated via FSSO.
C. There are multiple users sharing the same IP address.
D. Proxy users are authenticated via RADIUS.

Answer: C

Question: 39

Which of the following regular expression patterns make the terms "confidential data" case insensitive?

A. [confidential data]
B. /confidential data/i
C. i/confidential data/
D. "confidential data"

Answer: B

Question: 40

Which two web filtering inspection modes inspect the full URL? (Choose two.)

A. DNS-based.
B. Proxy-based.
C. Flow-based.
D. URL-based.

Answer: B, C

Question: 41

Which web filtering inspection mode inspects DNS traffic?

A. DNS-based.
B. FQDN-based.
C. Flow-based.
D. URL-based.

Answer: A

Question: 42

How do you configure a FortiGate to apply traffic shaping to P2P traffic, such as BitTorrent?

A. Apply a traffic shaper to a BitTorrent entry in an application control list, which is then applied to a firewall policy.
B. Enable the shape option in a firewall policy with service set to BitTorrent.
C. Define a DLP rule to match against BitTorrent traffic and include the rule in a DLP sensor with traffic shaping enabled.
D. Apply a traffic shaper to a protocol options profile.

Answer: A

Question: 43

Which statements are true regarding traffic shaping that is applied in an application sensor, and associated with a firewall policy? (Choose two.)

A. Shared traffic shaping cannot be used.
B. Only traffic matching the application control signature is shaped.
C. Can limit the bandwidth usage of heavy traffic applications.
D. Per-IP traffic shaping cannot be used.

Answer: B, C

Question: 44

When does a FortiGate load-share traffic between two static routes to the same destination subnet?

A. When they have the same cost and distance.
B. When they have the same distance and the same weight.
C. When they have the same distance and different priority.
D. When they have the same distance and same priority.

Answer: D

Question: 45

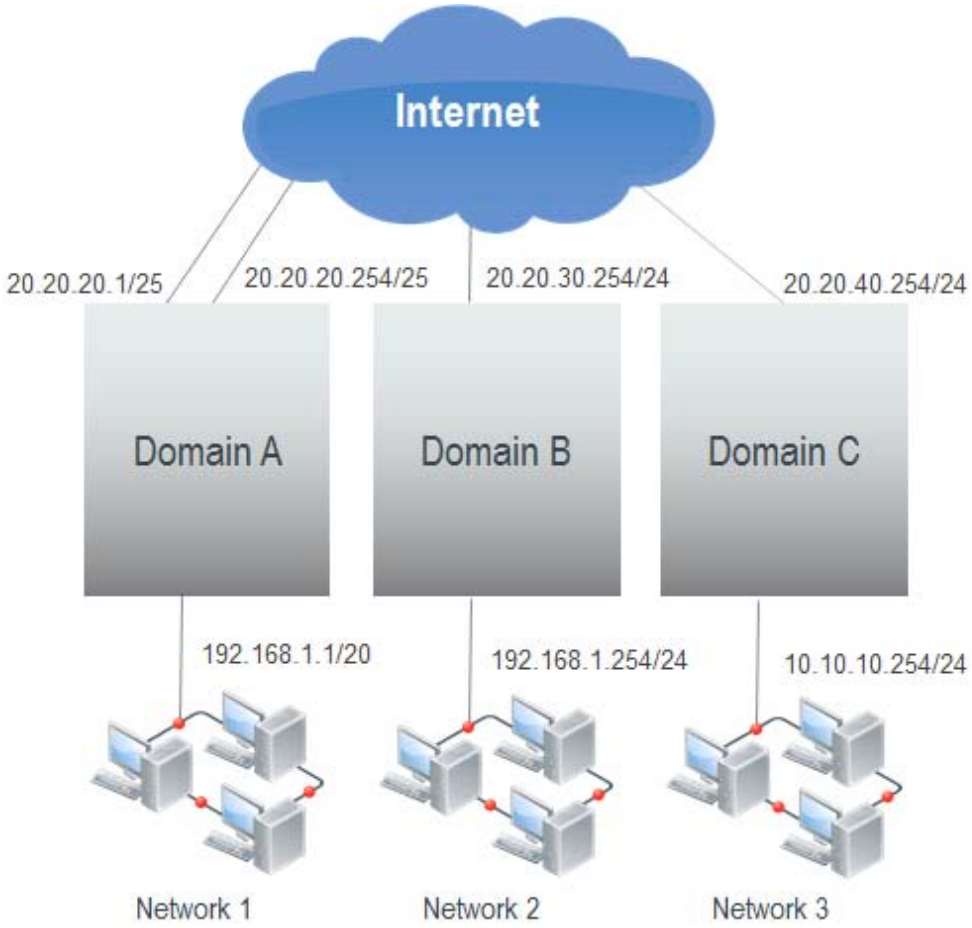
Which statements are correct regarding virtual domains (VDOMs)? (Choose two.)

A. VDOMs divide a single FortiGate unit into two or more virtual units that each have dedicated memory and CPUs.
B. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.
C. VDOMs share firmware versions, as well as antivirus and IPS databases.
D. Different time zones can be configured in each VDOM.

Answer: B, C

Question: 46

A FortiGate unit is configured with three Virtual Domains (VDOMs) as illustrated in the exhibit.



Which of the following statements are true if the network administrator wants to route traffic between all the VDOMs? (Choose three.)

A. The administrator can configure inter-VDOM links to avoid using external interfaces and routers.
B. As with all FortiGate unit interfaces, firewall policies must be in place for traffic to be allowed to pass through any interface, including inter-VDOM links.
C. This configuration requires a router to be positioned between the FortiGate unit and the Internet for proper routing.
D. Inter-VDOM routing is automatically provided if all the subnets that need to be routed are locally attached.
E. As each VDOM has an independent routing table, routing rules need to be set (for example, static routing, OSPF) in each VDOM to route traffic between VDOMs.

Answer: A, B, E

Question: 47

A FortiGate is configured with three virtual domains (VDOMs). Which of the following statements is correct regarding multiple VDOMs?

A. The FortiGate must be a model 1000 or above to support multiple VDOMs.
B. A license has to be purchased and applied to the FortiGate before VDOM mode could be enabled.
C. Changing the operational mode of a VDOM requires a reboot of the FortiGate.
D. The FortiGate supports any combination of VDOMs in NAT/Route and transparent modes.

Answer: D

Question: 48

A FortiGate administrator with the super_admin profile configures a virtual domain (VDOM) for a new customer. After creating the VDOM, the administrator is unable to reassign the dmz interface to the new VDOM as the option is greyed out in the GUI in the management VDOM.
What would be a possible cause for this problem?

A. The administrator does not have the proper permissions to reassign the dmz interface.
B. The dmz interface is referenced in the configuration of another VDOM.
C. Non-management VDOMs cannot reference physical interfaces.
D. The dmz interface is in PPPoE or DHCP mode.

Answer: B

Question: 49

Which statements are correct for port pairing and forwarding domains? (Choose two.)

A. They both create separate broadcast domains.
B. Port Pairing works only for physical interfaces.
C. Forwarding Domain only applies to virtual interfaces.
D. They may contain physical and/or virtual interfaces.

Answer: A, D

Question: 50

Examine the following spanning tree configuration on a FortiGate in transparent mode:

```
config system interface
  edit <interface name>
    set stp-forward enable
end
```

Which statement is correct for the above configuration?

A. The FortiGate participates in spanning tree.
B. The FortiGate device forwards received spanning tree messages.
C. Ethernet layer-2 loops are likely to occur.
D. The FortiGate generates spanning tree BPDU frames.

Answer: B

Question: 51

An administrator has formed a high availability cluster involving two FortiGate units.
[Multiple upstream Layer 2 switches] -- [FortiGate HA Cluster] -- [Multiple downstream Layer 2 switches]
The administrator wishes to ensure that a single link failure will have minimal impact upon the overall throughput of traffic through this cluster.
Which of the following options describes the best step the administrator can take?
The administrator should _____.

A. Increase the number of FortiGate units in the cluster and configure HA in active-active mode.
B. Enable monitoring of all active interfaces.
C. Set up a full-mesh design which uses redundant interfaces.
D. Configure the HA ping server feature to allow for HA failover in the event that a path is disrupted.

Answer: C

Question: 52

Which of the following sequences describes the correct order of criteria used for the selection of a master unit within a FortiGate high availability (HA) cluster when override is disabled?

A. 1. port monitor, 2. unit priority, 3. up time, 4. serial number.
B. 1. port monitor, 2. up time, 3. unit priority, 4. serial number.
C. 1. unit priority, 2. up time, 3. port monitor, 4. serial number.
D. 1. up time, 2. unit priority, 3. port monitor, 4. serial number.

Answer: B

Question: 53

Which IPsec mode includes the peer id information in the first packet?

A. Main mode.
B. Quick mode.
C. Aggressive mode.
D. IKEv2 mode.

Answer: C

Question: 54

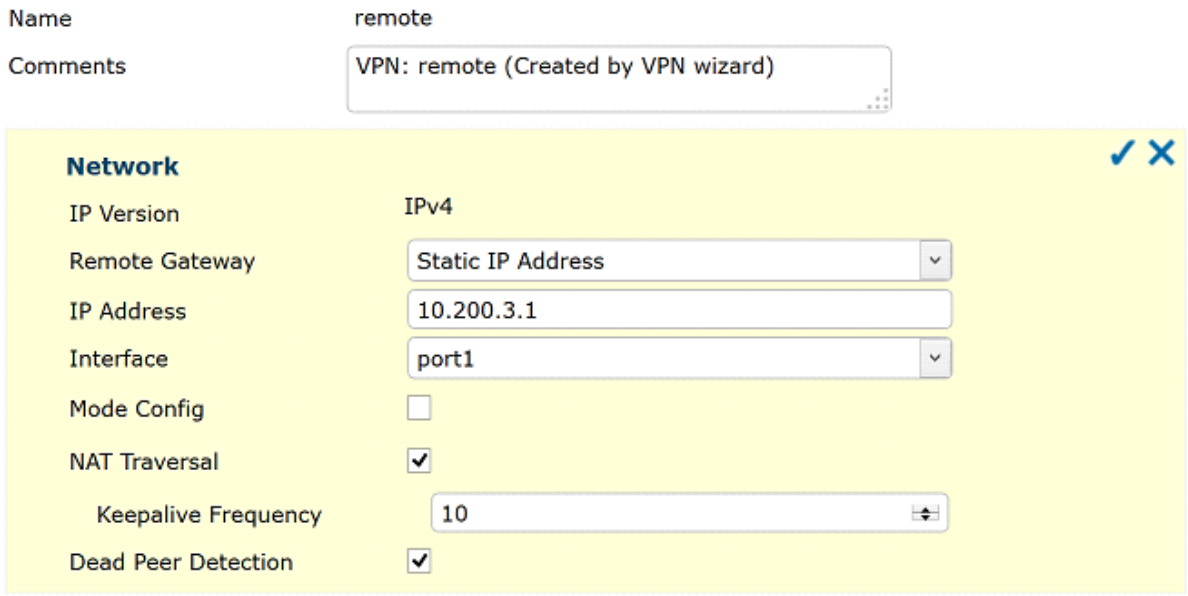
Which statements are correct properties of a partial mesh VPN deployment. (Choose two.)

A. VPN tunnels interconnect between every single location.
B. VPN tunnels are not configured between every single location.
C. Some locations are reached via a hub location.
D. There are no hub locations in a partial mesh.

Answer: B, C

Question: 55

Review the IPsec phase 1 configuration in the exhibit; then answer the question below.



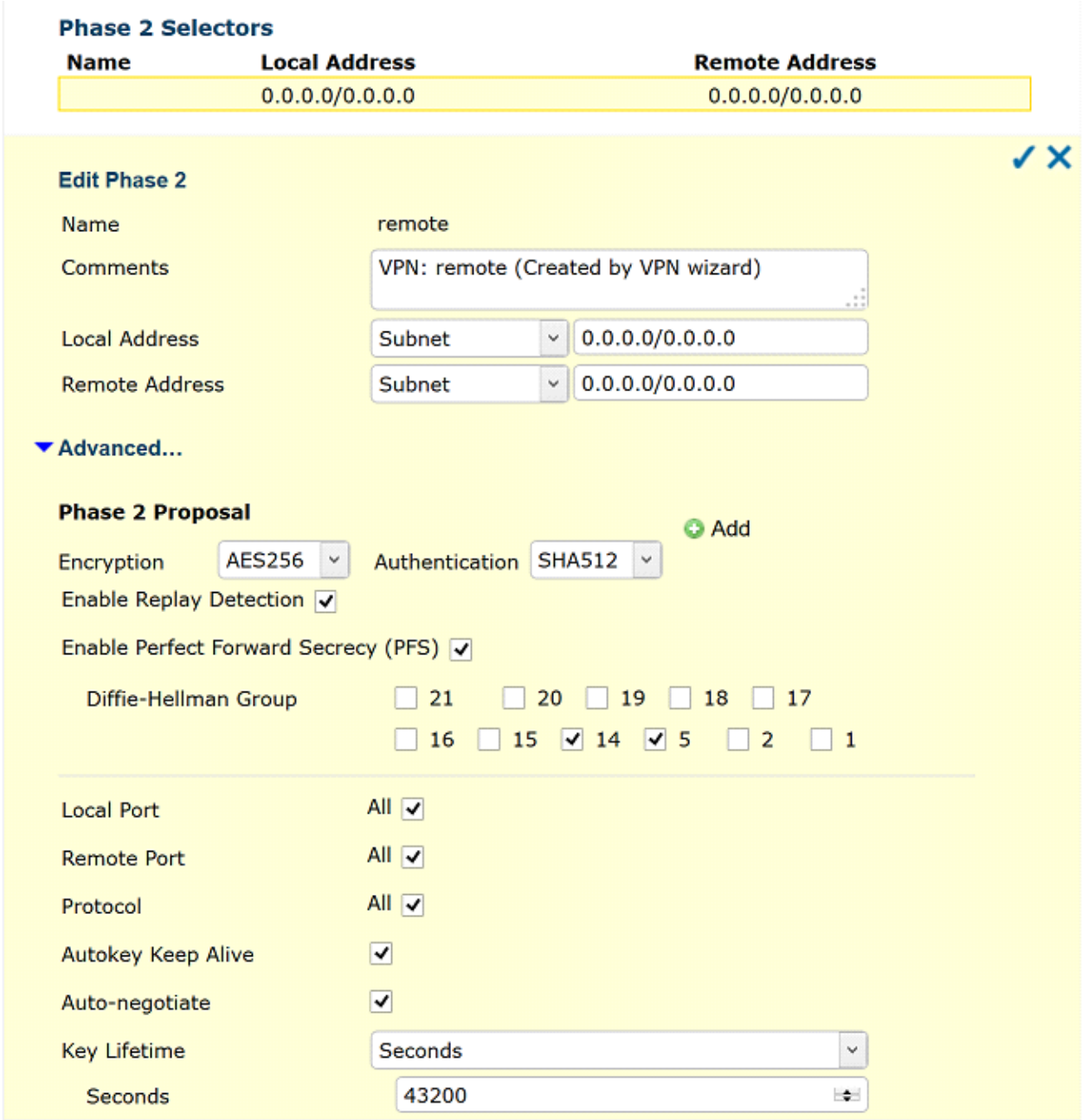
Which statements are correct regarding this configuration? (Choose two.)

A. The remote gateway address on 10.200.3.1.
B. The local IPsec interface address is 10.200.3.1.
C. The local gateway IP is the address assigned to port1.
D. The local gateway IP address is 10.200.3.1.

Answer: A, C

Question: 56

Review the IPsec phase 2 configuration shown in the exhibit; then answer the question below.



Which statements are correct regarding this configuration? (Choose two.).

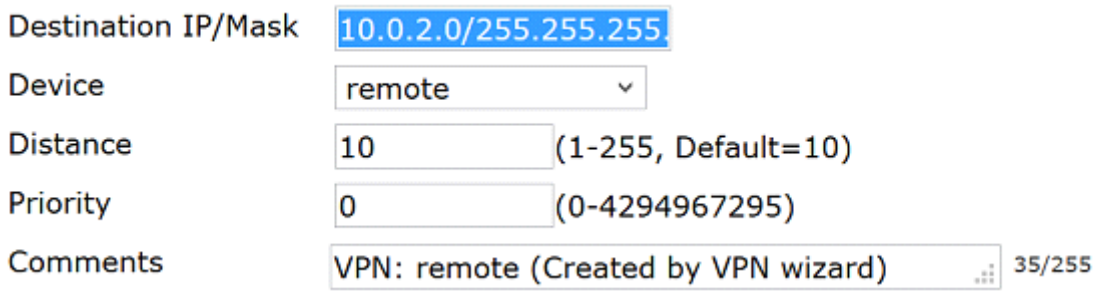
A. The Phase 2 will re-key even if there is no traffic.
B. There will be a DH exchange for each re-key.

C. The sequence number of ESP packets received from the peer will not be checked.
D. Quick mode selectors will default to those used in the firewall policy.

Answer: A, B

Question: 57

Review the static route configuration for IPsec shown in the exhibit; then answer the question below.



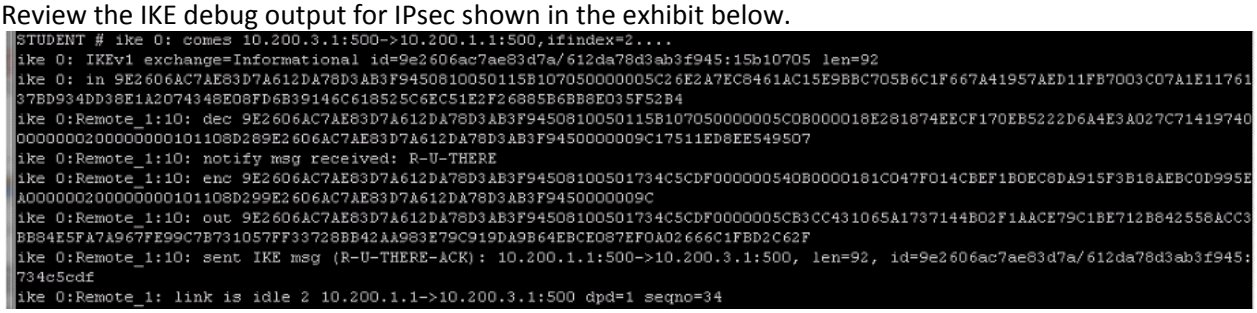
Which statements are correct regarding this configuration? (Choose two.)

A. Interface remote is an IPsec interface.
B. A gateway address is not required because the interface is a point-to-point connection.
C. A gateway address is not required because the default route is used.
D. Interface remote is a zone.

Answer: A, B

Question: 58

Review the IKE debug output for IPsec shown in the exhibit below.



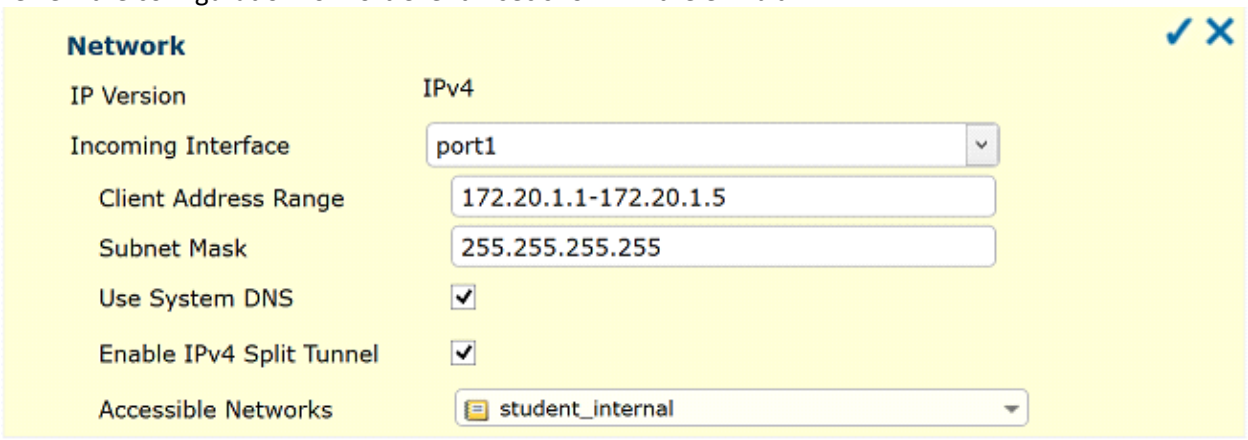
Which statements is correct regarding this output?

A. The output is a phase 1 negotiation.
B. The output is a phase 2 negotiation.
C. The output captures the dead peer detection messages.
D. The output captures the dead gateway detection packets.

Answer: C

Question: 59

Review the configuration for FortiClient IPsec shown in the exhibit.



Which statement is correct regarding this configuration?

A. The connecting VPN client will install a route to a destination corresponding to the student_internal address object.
B. The connecting VPN client will install a default route.
C. The connecting VPN client will install a route to the 172.20.1.[1-5] address range.
D. The connecting VPN client will connect in web portal mode and no route will be installed.

Answer: A

Question: 60

Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit below.

```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=FClient_0 ver=1 serial=3 10.200.1.1:4500->10.200.3.1:64916 lgwy=static tun=intf mode=dial_inst bound_if=2
parent=FClient index=0
proxyid_num=1 child_num=0 refcnt=8 ilast=2 olast=2
stat: rxp=59 txp=0 rxb=15192 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=10
natt: mode=keepalive draft=32 interval=10 remote_port=64916
proxyid=FClient proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:172.20.1.1-172.20.1.1:0
  SA: ref=3 options=00000006 type=00 soft=0 mtu=1280 expire=1717 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1791/1800
  dec: spi=a29046e9 esp=3des key=24 0525830c6fd67ca37e9d6dad174d175e24f97c3b87f428fa
       ah=sha1 key=20 982f8ba194f3f797773efc605c8321b728dabf1d
  enc: spi=19be4052 esp=3des key=24 da597cb7fec913528f8598d1aa7ecd17156a2a7a4afeeb4c
       ah=sha1 key=20 9e2c5d0fc055fa0149bc66024732e9a85bbe8016
------------------------------------------------------
```

Which statements are correct regarding this output? (Choose two.)

A. The connecting client has been allocated address 172.20.1.1.
B. In the Phase 1 settings, dead peer detection is enabled.
C. The tunnel is idle.
D. The connecting client has been allocated address 10.200.3.1.

Answer: A, B

Question: 61

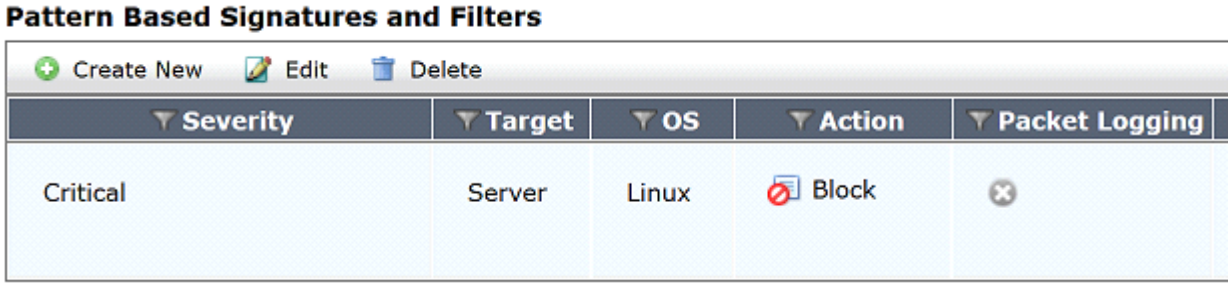
Which statement correctly describes the output of the command diagnose ips anomaly list?

A. Lists the configured DoS policy.
B. List the real-time counters for the configured DoS policy.
C. Lists the errors captured when compiling the DoS policy.
D. Lists the IPS signature matches.

Answer: B

Question: 62

Review the IPS sensor filter configuration shown in the exhibit



Based on the information in the exhibit, which statements are correct regarding the filter? (Choose two.)

A. It does not log attacks targeting Linux servers.
B. It matches all traffic to Linux servers.
C. Its action will block traffic matching these signatures.
D. It only takes effect when the sensor is applied to a policy.

Answer: C, D

Question: 63

Which statement describes what the CLI command diagnose debug authd fsso list is used for?

A. Monitors communications between the FSSO collector agent and FortiGate unit.
B. Displays which users are currently logged on using FSSO.
C. Displays a listing of all connected FSSO collector agents.
D. Lists all DC Agents installed on all domain controllers.

Answer: B

Question: 64

Which are two requirements for DC-agent mode FSSO to work properly in a Windows AD environment? [Choose two.]

A. DNS server must properly resolve all workstation names.
B. The remote registry service must be running in all workstations.
C. The collector agent must be installed in one of the Windows domain controllers.
D. A same user cannot be logged in into two different workstations at the same time.

Answer: A, B

Question: 65

Which statement is one disadvantage of using FSSO NetAPI polling mode over FSSO Security Event Log (WinSecLog) polling mode?

A. It requires a DC agent installed in some of the Windows DC.
B. It runs slower.
C. It might miss some logon events.
D. It requires access to a DNS server for workstation name resolution.

Answer: C

Question: 66

Bob wants to send Alice a file that is encrypted using public key cryptography.
Which of the following statements is correct regarding the use of public key cryptography in this scenario?

A. Bob will use his private key to encrypt the file and Alice will use her private key to decrypt the file.
B. Bob will use his public key to encrypt the file and Alice will use Bob's private key to decrypt the file.

C. Bob will use Alice's public key to encrypt the file and Alice will use her private key to decrypt the file.
D. Bob will use his public key to encrypt the file and Alice will use her private key to decrypt the file.

Answer: C

Question: 67

Which tasks fall under the responsibility of the SSL proxy in a typical HTTPS connection? (Choose two.)

A. The web client SSL handshake.
B. The web server SSL handshake.
C. File buffering.
D. Communication with the URL filter process.

Answer: A, B

Question: 68

When the SSL proxy is NOT doing man-in-the-middle interception of SSL traffic, which certificate field can be used to determine the rating of a website?

A. Organizational Unit.
B. Common Name.
C. Serial Number.
D. Validity.

Answer: B

Question: 69

In which process states is it impossible to interrupt/kill a process? (Choose two.)

A. S – Sleep
B. R – Running
C. D – Uninterruptable Sleep
D. Z – Zombie

Answer: C, D

Question: 70

Examine at the output below from the diagnose sys top command:
diagnose sys top 1
Run Time: 11 days, 3 hours and 29 minutes
0U, 0N, 1S, 99I; 971T, 528F, 160KF

sshd	123	S	1.9	1.2
ipsengine	61	S <	0.0	5.2
miglogd	45	S	0.0	4.9
pyfcgid	75	S	0.0	4.5
pyfcgid	73	S	0.0	3.9

Which statements are true regarding the output above? (Choose two.)

A. The sshd process is the one consuming most CPU.
B. The sshd process is using 123 pages of memory.
C. The command diagnose sys kill miglogd will restart the miglogd process.
D. All the processes listed are in sleeping state.

Answer: A, D

Question: 71

Examine the following output from the diagnose sys session list command:
session info: proto=6 proto_state=65 duration=3 expire=9 timeout=3600 flags=00000000 sockflag=00000000 sockport=443 av_idx=9 use=5
origin-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bps
reply-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bps
state=redir local may_dirty ndr npu nlb os rs
statistic(bytes/packets/allow_err): org=864/8/1 reply=2384/7/1 tuples=3
orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.17.87.3/10.1.10.1
hook=post dir=org act=snat 192.168.1.110:57999->74.201.86.29:443(172.17.87.16:57999)
hook=pre dir=reply act=dnat 74.201.86.29:443->172.17.87.16:57999(192.168.1.110:57999)
hook=post dir=reply act=noop 74.201.86.29:443->192.168.1.110:57999(0.0.0.0:0)
misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0/0
Which statements are true regarding the session above? (Choose two.)

A. Session Time-To-Live (TTL) was configured to 9 seconds.
B. FortiGate is doing NAT of both the source and destination IP addresses on all packets coming from the 192.168.1.110 address.
C. The IP address 192.168.1.110 is being translated to 172.17.87.16.
D. The FortiGate is not translating the TCP port numbers of the packets in this session.

Answer: C, D

Question: 72

Which statements are true regarding IPv6 anycast addresses? (Choose two.)

A. Multiple interfaces can share the same anycast address.
B. They are allocated from the multicast address space.
C. Different nodes cannot share the same anycast address.
D. An anycast packet is routed to the nearest interface.

Answer: A, D

Question: 73

What functions can the IPv6 Neighbor Discovery protocol accomplish? (Choose two.)

A. Negotiate the encryption parameters to use.
B. Auto-adjust the MTU setting.
C. Autoconfigure addresses and prefixes.
D. Determine other nodes reachability.

Answer: C, D

Question: 74

Which statements are correct regarding an IPv6 over IPv4 IPsec configuration? (Choose two.)

A. The source quick mode selector must be an IPv4 address.
B. The destination quick mode selector must be an IPv6 address.
C. The Local Gateway IP must be an IPv4 address.
D. The remote gateway IP must be an IPv6 address.

Answer: B, C

Question: 75

Which is one of the conditions that must be met for offloading the encryption and decryption of IPsec traffic to an NP6 processor?

A. No protection profile can be applied over the IPsec traffic.
B. Phase-2 anti-replay must be disabled.

C. Both the phase 1 and phases 2 must use encryption algorithms supported by the NP6.
D. IPsec traffic must not be inspected by any FortiGate session helper.

Answer: C

Question: 76

Two FortiGate units with NP6 processors form an active-active cluster. The cluster is doing security profile (UTM) inspection over all the user traffic. What statements are true regarding the sessions that the master unit is offloading to the slave unit for inspection? (Choose two.)

A. They are accelerated by hardware in the master unit.
B. They are not accelerated by hardware in the master unit.
C. They are accelerated by hardware in the slave unit.
D. They are not accelerated by hardware in the slave unit.

Answer: A, D

Question: 77

Which statements are true about offloading antivirus inspection to a Security Processor (SP)? (Choose two.)

A. Both proxy-based and flow-based inspection are supported.
B. A replacement message cannot be presented to users when a virus has been detected.
C. It saves CPU resources.
D. The ingress and egress interfaces can be in different SPs.

Answer: B, C

Question: 78

Which IP packets can be hardware-accelerated by a NP6 processor? (Choose two.)

A. Fragmented packet.
B. Multicast packet.
C. SCTP packet.
D. GRE packet.

Answer: B, C

Question: 79

FSSO provides a single sign on solution to authenticate users transparently to a FortiGate unit using credentials stored in Windows Active Directory.
Which of the following statements are correct regarding FSSO in a Windows domain environment when NTLM and Polling Mode are not used? (Select all that apply.)

A. An FSSO Collector Agent must be installed on every domain controller.
B. An FSSO Domain Controller Agent must be installed on every domain controller.
C. The FSSO Domain Controller Agent will regularly update user logon information on the FortiGate unit.
D. The FSSO Collector Agent will retrieve user information from the Domain Controller Agent and will send the user logon information to the FortiGate unit.
E. For non-domain computers, the only way to allow FSSO authentication is to install an FSSO client.

Answer: B, D

Question: 80

Which of the following represents the correct order of criteria used for the selection of a Master unit within a FortiGate High Availability (HA) cluster when master override is disabled?

A. 1. port monitor, 2. unit priority, 3. up time, 4. serial number
B. 1. port monitor, 2. up time, 3. unit priority, 4. serial number
C. 1. unit priority, 2. up time, 3. port monitor, 4. serial number
D. 1. up time, 2. unit priority, 3. port monitor, 4. serial number

Answer: B

Question: 81

In a High Availability cluster operating in Active-Active mode, which of the following correctly describes the path taken by the SYN packet of an HTTP session that is offloaded to a subordinate unit?

A. Request: Internal Host; Master FortiGate; Slave FortiGate; Internet; Web Server
B. Request: Internal Host; Master FortiGate; Slave FortiGate; Master FortiGate; Internet; Web Server
C. Request: Internal Host; Slave FortiGate; Internet; Web Server
D. Request: Internal Host; Slave FortiGate; Master FortiGate; Internet; Web Server

Answer: A

Question: 82

Which of the following statements are correct regarding virtual domains (VDOMs)? (Select all that apply.)

A. VDOMs divide a single FortiGate unit into two or more virtual units that function as multiple, independent units.
B. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.
C. VDOMs share firmware versions, as well as antivirus and IPS databases.
D. Only administrative users with a 'super_admin' profile will be able to enter multiple VDOMs to make configuration changes.

Answer: A, B, C

Question: 83

What advantages are there in using a hub-and-spoke IPSec VPN configuration instead of a fully-meshed set of IPSec tunnels? (Select all that apply.)

A. Using a hub and spoke topology is required to achieve full redundancy.
B. Using a hub and spoke topology simplifies configuration because fewer tunnels are required.
C. Using a hub and spoke topology provides stronger encryption.
D. The routing at a spoke is simpler, compared to a meshed node.

Answer: B, D

Question: 84

Data Leak Prevention archiving gives the ability to store files and message data onto a FortiAnalyzer unit for which of the following types of network traffic? (Select all that apply.)

A. SNMP
B. IPSec
C. SMTP
D. POP3
E. HTTP

Answer: C, D, E

Question: 85

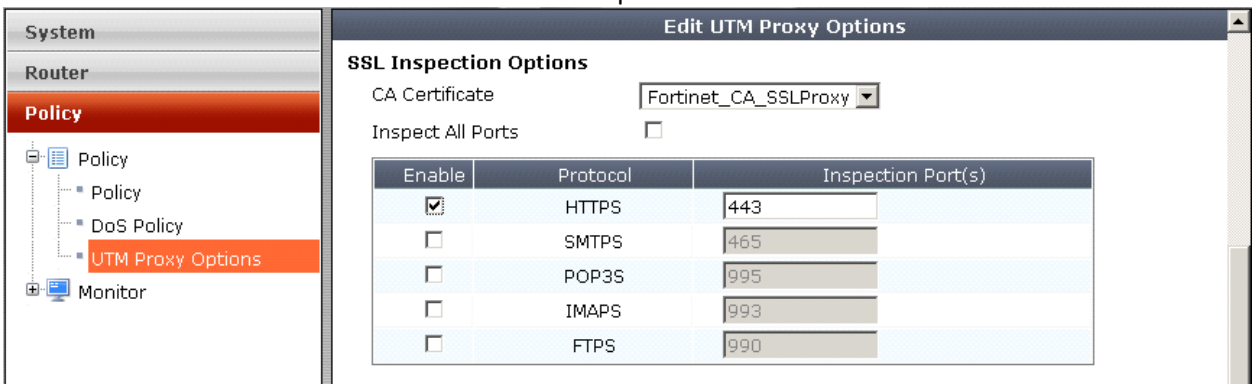
Which of the following statements are correct regarding Application Control?

A. Application Control is based on the IPS engine.
B. Application Control is based on the AV engine.
C. Application Control can be applied to SSL encrypted traffic.
D. Application Control cannot be applied to SSL encrypted traffic.

Answer: A, C

Question: 86

Examine the exhibit shown below then answer the question that follows it.



Within the UTM Proxy Options, the CA certificate Fortinet_CA_SSLProxy defines which of the following:

A. FortiGate unit's encryption certificate used by the SSL proxy.
B. FortiGate unit's signing certificate used by the SSL proxy.
C. FortiGuard's signing certificate used by the SSL proxy.
D. FortiGuard's encryption certificate used by the SSL proxy.

Answer: A

Question: 87

For Data Leak Prevention, which of the following describes the difference between the block and quarantine actions?

A. A block action prevents the transaction. A quarantine action blocks all future transactions, regardless of the protocol.
B. A block action prevents the transaction. A quarantine action archives the data.
C. A block action has a finite duration. A quarantine action must be removed by an administrator.
D. A block action is used for known users. A quarantine action is used for unknown users.

Answer: A

Question: 88

How can DLP file filters be configured to detect Office 2010 files? (Select all that apply.)

A. File TypE. Microsoft Office(msoffice)
B. File TypE. Archive(zip)
C. File TypE. Unknown Filetype(unknown)
D. File NamE. "*.ppt", "*.doc", "*.xls"
E. File NamE. "*.pptx", "*.docx", "*.xlsx"

Answer: B, E

Question: 89

Examine the Exhibits shown below, then answer the question that follows.
Review the following DLP Sensor (Exhibit 1):

Create New | Edit Filter | Delete

Seq #	Type	Action	Services	Archive
1	File Type	Log Only	SMTP, POP3, IMAP, HTTP, NNTP	Disable
2	File Type	Quarantine Interface	SMTP, POP3, IMAP, HTTP, NNTP	Disable
3	File Type	Block	SMTP, POP3, IMAP, HTTP, NNTP	Disable

Review the following File Filter list for rule #1 (Exhibit 2):

Create New | Edit Filter | Delete

Filter Type	Filter
File Type	Audio (mp3)
File Type	Audio (wma)
File Type	Audio (wav)

Review the following File Filter list for rule #2 (Exhibit 3):

Create New | Edit Filter | Delete

Filter Type	Filter
File Name Pattern	*.exe

Review the following File Filter list for rule #3 (Exhibit 4):

Create New | Edit Filter | Delete

Filter Type	Filter
File Type	Archive (arj)
File Type	Archive (bzip)
File Type	Archive (cab)
File Type	Archive (zip)

An MP3 file is renamed to 'workbook.exe' and put into a ZIP archive. It is then sent through the FortiGate device over HTTP. It is intercepted and processed by the configuration shown in the above Exhibits 1-4.
Assuming the file is not too large for the File scanning threshold, what action will the FortiGate unit take?

A. The file will be detected by rule #1 as an 'Audio (mp3)', a log entry will be created and it will be allowed to pass through.

B. The file will be detected by rule #2 as a "*.exe", a log entry will be created and the interface that received the traffic will be brought down.
C. The file will be detected by rule #3 as an Archive(zip), blocked, and a log entry will be created.
D. Nothing, the file will go undetected.

Answer: A

Question: 90

The eicar test virus is put into a zip archive, which is given the password of "Fortinet" in order to open the archive. Review the configuration in the exhibits shown below; then answer the question that follows.
Exhibit A – Antivirus Profile:

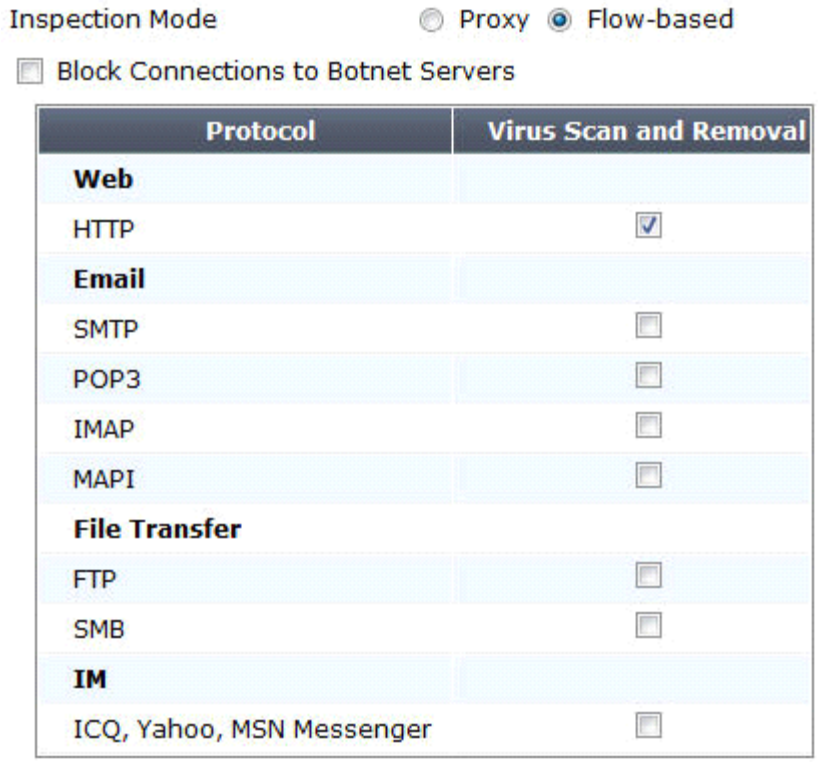


Exhibit B – Non-default UTM Proxy Options Profile:

Protocol Port Mapping

Enable	Protocol	Inspection Port(s)
☑	HTTP	○ Any ◉ Specify 8080
☑	SMTP	○ Any ◉ Specify 25
☑	POP3	○ Any ◉ Specify 110
☑	IMAP	○ Any ◉ Specify 143
☑	FTP	○ Any ◉ Specify 21
☑	NNTP	○ Any ◉ Specify 119
☑	MAPI	135
☑	DNS	53

Exhibit C – DLP Profile:

Which of one the following profiles could be enabled in order to prevent the file from passing through the FortiGate device over HTTP on the standard port for that protocol?

A. Only Exhibit A
B. Only Exhibit B
C. Only Exhibit C with default UTM Proxy settings.
D. All of the Exhibits (A, B and C)
E. Only Exhibit C with non-default UTM Proxy settings (Exhibit B).

Answer: C

Question: 91

With FSSO, a domain user could authenticate either against the domain controller running the Collector Agent and Domain Controller Agent, or a domain controller running only the Domain Controller Agent.
If you attempt to authenticate with the Secondary Domain Controller running only the Domain Controller Agent, which of the following statements are correct? (Select all that apply.)

A. The login event is sent to the Collector Agent.
B. The FortiGate unit receives the user information from the Domain Controller Agent of the Secondary Controller.
C. The Collector Agent performs the DNS lookup for the authenticated client's IP address.
D. The user cannot be authenticated with the FortiGate device in this manner because each Domain Controller Agent requires a dedicated Collector Agent.

Answer: A, C

Question:14
Select
the answer that describes what the CLI command diag debug authd fsso list is used for.

A. Monitors communications between the FSSO Collector Agent and FortiGate unit.
B. Displays which users are currently logged on using FSSO.
C. Displays a listing of all connected FSSO Collector Agents.
D. Lists all DC Agents installed on all Domain Controllers.

Answer: B

Question: 92

What are the requirements for a cluster to maintain TCP connections after device or link failover? (Select all that apply.)

A. Enable session pick-up.
B. Only applies to connections handled by a proxy.
C. Only applies to UDP and ICMP connections.
D. Connections must not be handled by a proxy.

Answer: A, D

Question: 93

Two devices are in an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of 'diag sys session stat' for the STUDENT device. Exhibit B shows the command output of 'diag sys session stat' for the REMOTE device.
Exhibit A:

```
STUDENT # diagnose sys session stat
misc info:       session_count=166 setup_rate=68 exp_count=0 clash=0
        memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
         8 in ESTABLISHED state
         3 in SYN_SENT state
         1 in FIN_WAIT state
         139 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=2 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

STUDENT # _
```

Exhibit B:

```
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # diagnose sys session stat
misc info:       session_count=11 setup_rate=0 exp_count=0 clash=4
        memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
         2 in ESTABLISHED state
         1 in SYN_SENT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=7 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # _
```

Given the information provided in the exhibits, which of the following statements are correct? (Select all that apply.)

A. STUDENT is likely to be the master device.

B. Session-pickup is likely to be enabled.
C. The cluster mode is definitely Active-Passive.
D. There is not enough information to determine the cluster mode.

Answer: A, D

Question: 94

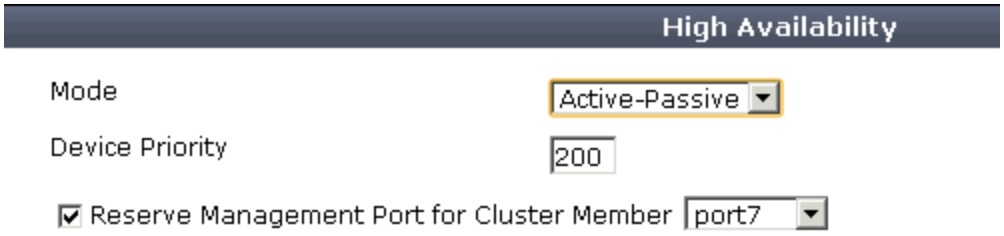
Which of the following statements are correct about the HA diag command diagnose sys ha reset-uptime? (Select all that apply.)

A. The device this command is executed on is likely to switch from master to slave status if master override is disabled.
B. The device this command is executed on is likely to switch from master to slave status if master override is enabled.
C. This command has no impact on the HA algorithm.
D. This command resets the uptime variable used in the HA algorithm so it may cause a new master to become elected.

Answer: A, D

Question: 95

In HA, the option Reserve Management Port for Cluster Member is selected as shown in the Exhibit below.



Which of the following statements are correct regarding this setting? (Select all that apply.)

A. Interface settings on port7 will not be synchronized with other cluster members.
B. The IP address assigned to this interface must not overlap with the IP address subnet assigned to another interface.
C. Port7 appears in the routing table.
D. A gateway address may be configured for port7.
E. When connecting to port7 you always connect to the master device.

Answer: A, D

Question: 96

In HA, what is the effect of the Disconnect Cluster Member command as given in the Exhibit.

A. The HA mode changes to standalone.
B. Port3 is configured with an IP address for management access.
C. The Firewall rules are purged on the disconnected unit.
D. All other interface IP settings are maintained.

Answer: A, B

Question: 97

Two FortiGate devices fail to form an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of 'show system ha' for the STUDENT device. Exhibit B shows the command output of 'show system ha' for the REMOTE device.
Exhibit A:

```
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:34:19 2013

STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT # show system ha
config system ha
    set mode a-p
    set password ENC 9FHCYwOJXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4dsgx4CnV1GRJ8
McEECpiT3Z/3dCmIuYIDgW2sE+lAlkHfADOV/r5DkaqGnbj15XV/a
    set hbdev "port2" 50
    set override disable
    set priority 200
end

STUDENT # _
```

Exhibit B

```
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # diagnose sys session stat
misc info:       session_count=11 setup_rate=0 exp_count=0 clash=4
        memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
         2 in ESTABLISHED state
         1 in SYN_SENT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=7 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # _
```

Which one of the following is the most likely reason that the cluster fails to form?

A. Password

B. HA mode
C. Hearbeat
D. Override

Answer: B

Question: 98

Examine the following log message for IPS and identify the valid responses below. (Select all that apply.)
2012-07-01 09:54:28 oid=2 log_id=18433 type=ips subtype=anomaly pri=alert vd=root severity="critical" src="192.168.3.168" dst="192.168.3.170" src_int="port2" serial=0 status="detected" proto=1 service="icmp" count=1 attack_name="icmp_flood" icmp_id="0xa8a4" icmp_type="0x08" icmp_code="0x00" attack_id=16777316 sensor="1" ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly: icmp_flood, 51 > threshold 50"

A. The target is 192.168.3.168.
B. The target is 192.168.3.170.
C. The attack was detected and blocked.
D. The attack was detected only.
E. The attack was TCP based.

Answer: B, D

Question: 99

Identify the statement which correctly describes the output of the following command:
diagnose ips anomaly list

A. Lists the configured DoS policy.
B. List the real-time counters for the configured DoS policy.
C. Lists the errors captured when compiling the DoS policy.

Answer: B

Question: 100

Review the CLI configuration below for an IPS sensor and identify the correct statements regarding this configuration from the choices below. (Select all that apply.)

```
config ips sensor
  edit "LINUX_SERVER"
    set comment ''
    set replacemsg-group ''
```

```
    set log enable
      config entries
        edit 1
          set action default
          set application all
          set location server
          set log enable
          set log-packet enable
          set os Linux
          set protocol all
          set quarantine none
          set severity all
          set status default
        next
      end
  next
end
```

A. The sensor will log all server attacks for all operating systems.
B. The sensor will include a PCAP file with a trace of the matching packets in the log message of any matched signature.
C. The sensor will match all traffic from the address object 'LINUX_SERVER'.
D. The sensor will reset all connections that match these signatures.
E. The sensor only filters which IPS signatures to apply to the selected firewall policy.

Answer: B, E

Question: 101

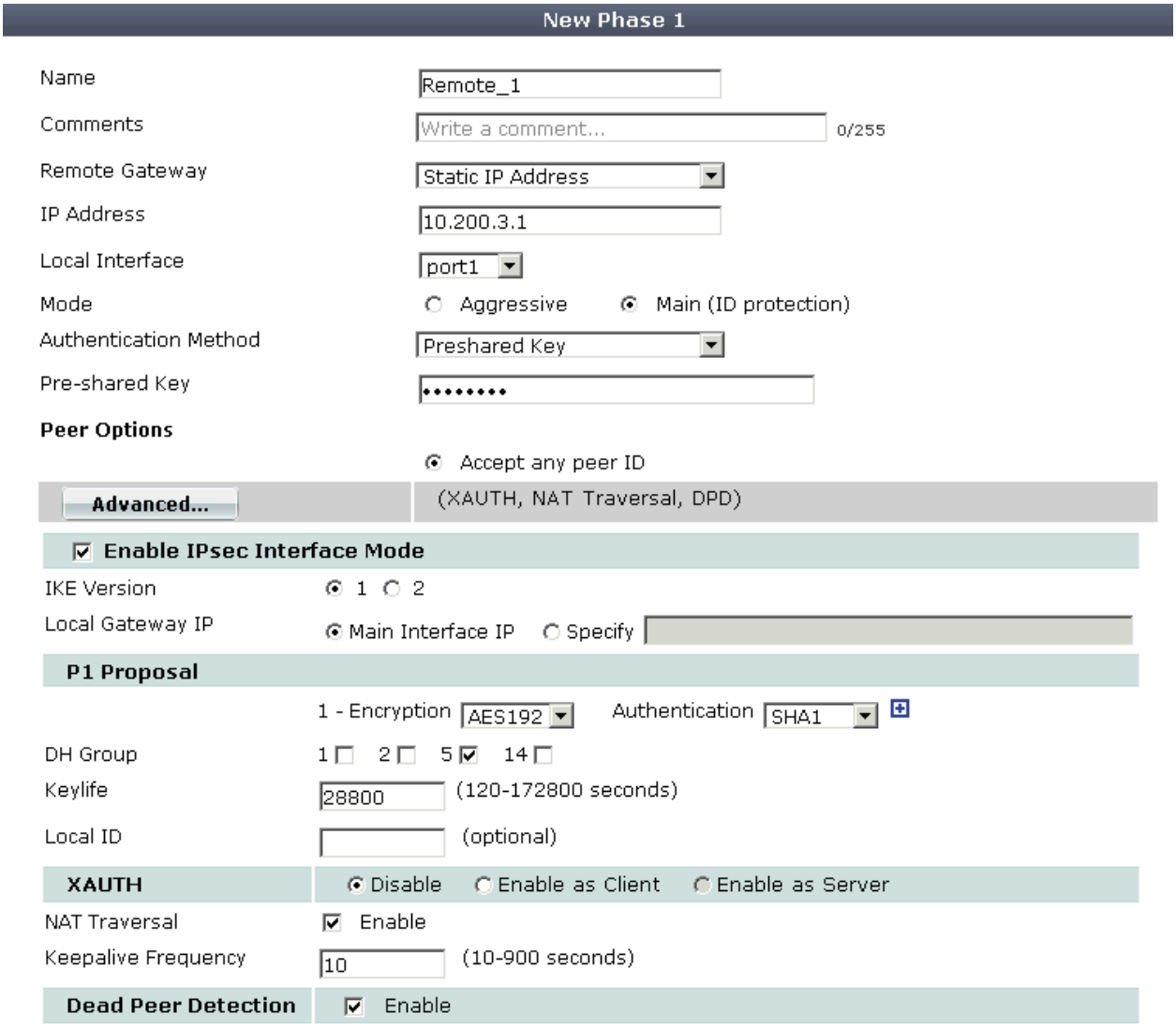
Identify the correct properties of a partial mesh VPN deployment:

A. VPN tunnels interconnect between every single location.
B. VPN tunnels are not configured between every single location.
C. Some locations are reached via a hub location.
D. There are no hub locations in a partial mesh.

Answer: B, C

Question: 102

Review the IPsec phase1 configuration in the Exhibit shown below; then answer the question following it.



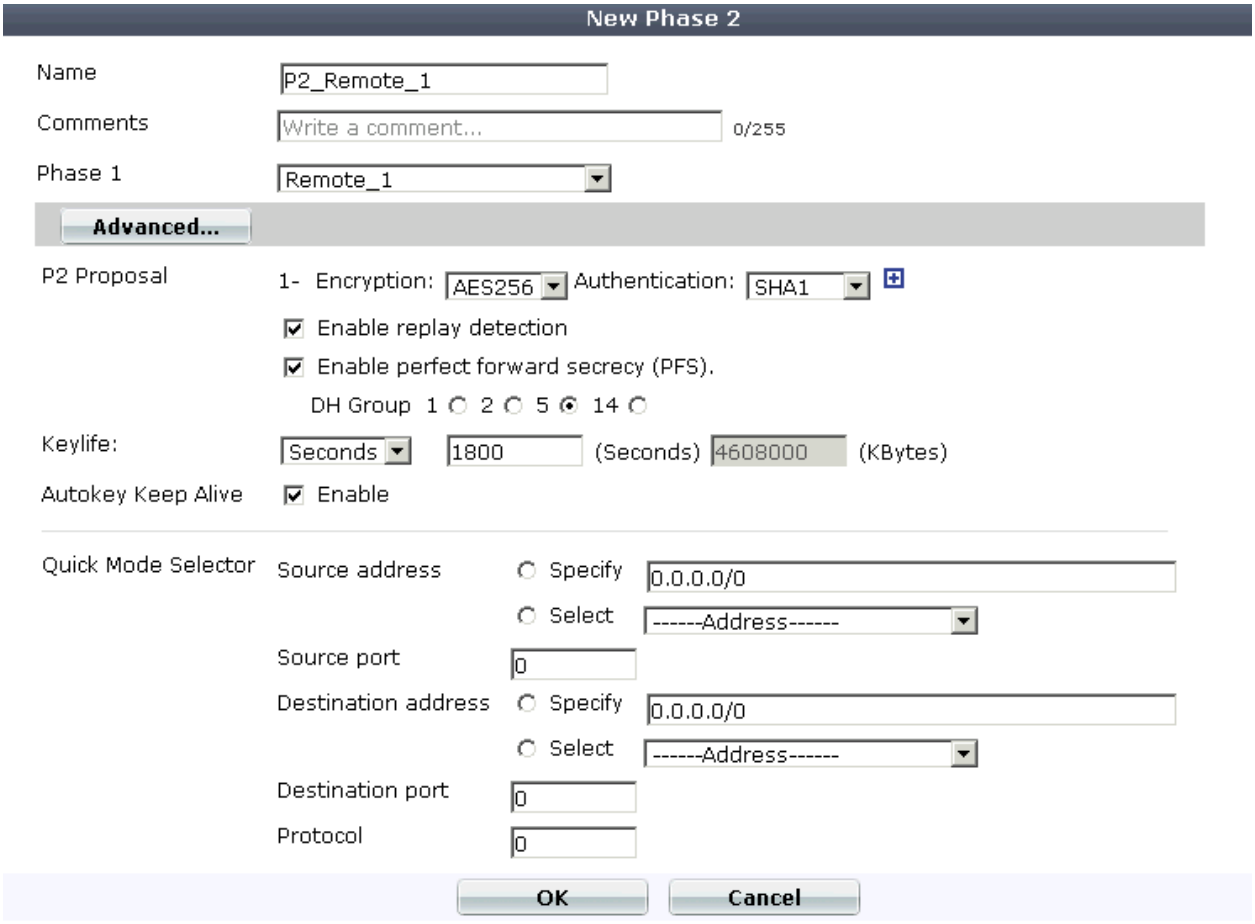
Which of the following statements are correct regarding this configuration? (Select all that apply).

A. The phase1 is for a route-based VPN configuration.
B. The phase1 is for a policy-based VPN configuration.
C. The local gateway IP is the address assigned to port1.
D. The local gateway IP address is 10.200.3.1.

Answer: A, C

Question: 103

Review the IPsec Phase2 configuration shown in the Exhibit; then answer the question following it.



Which of the following statements are correct regarding this configuration? (Select all that apply).

A. The Phase 2 will re-key even if there is no traffic.
B. There will be a DH exchange for each re-key.
C. The sequence number of ESP packets received from the peer will not be checked.
D. Quick mode selectors will default to those used in the firewall policy.

Answer: A, B

Question: 104

Review the static route configuration for IPsec shown in the Exhibit below; then answer the question following it.

Which of the following statements are correct regarding this configuration? (Select all that apply).

A. Remote_1 is a Phase 1 object with interface mode enabled
B. The gateway address is not required because the interface is a point-to-point connection
C. The gateway address is not required because the default route is used
D. Remote_1 is a firewall zone

Answer: A, B

Question: 105

Review the IKE debug output for IPsec shown in the Exhibit below.

```
STUDENT # ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Informational id=9e2606ac7ae83d7a/612da78d3ab3f945:15b10705 len=92
ike 0: in 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B10705000000 5C26E2A7EC8461AC15E9BBC705B6C1F667A41957AED11FB7003C07A1E11761
37BD934DD38E1A2074348E08FD6B39146C618525C6EC51E2F26885B6BB8E035F52B4
ike 0:Remote_1:10: dec 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B10705000000 5C0B000018E281874EECF17OEB5222D6A4E3AO27C71419740
0000000200000000101108D289E2606AC7AE83D7A612DA78D3AB3F9450000009C17511ED8EE549507
ike 0:Remote_1:10: notify msg received: R-U-THERE
ike 0:Remote_1:10: enc 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF000000540B0000181C047F014CBEF1B0EC8DA915F3B18AEBC0D995E
A0000002000000001011108D299E2606AC7AE83D7A612DA78D3AB3F94500000009C
ike 0:Remote_1:10: out 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF00000005CB3CC431065A1737144B02F1AACE79C1BE712B842558ACC3
BB84E5FA7A967FE99C7B731057FF33728BB42AA983E79C919DA9B64EBCE087EF0A02666C1FBD2C62F
ike 0:Remote_1:10: sent IKE msg (R-U-THERE-ACK): 10.200.1.1:500->10.200.3.1:500, len=92, id=9e2606ac7ae83d7a/612da78d3ab3f945:
734c5cdf
ike 0:Remote_1: link is idle 2 10.200.1.1->10.200.3.1:500 dpd=1 seqno=34
```

Which one of the following statements is correct regarding this output?

A. The output is a Phase 1 negotiation.
B. The output is a Phase 2 negotiation.
C. The output captures the Dead Peer Detection messages.
D. The output captures the Dead Gateway Detection packets.

Answer: C

Question: 106

Review the IPsec diagnostics output of the command diag vpn tunnel list shown in the Exhibit.

```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=Remote_1 ver=1 serial=1 10.200.1.1:0->10.200.3.1:0 lgwy=static tun=intf mode=auto bound_if=2
proxyid_num=1 child_num=0 refcnt=6 ilast=2 olast=2
stat: rxp=8 txp=8 rxb=960 txb=480
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=128
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=P2_Remote_1 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=0000000f type=00 soft=0 mtu=1412 expire=1486 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1753/1800
  dec: spi=b95a77fe esp=aes key=32 84ed410c1bb9f61e635a49563c4e7646e9e110628b79b0ac03482d05e3b6a0e6
       ah=sha1 key=20 6bddbfad7161237daa46c19725dd0292b062dda5
  enc: spi=9293e7d4 esp=aes key=32 951befd87860cdb59b98b170a17dcb75f77bd541bdc3a1847e54c78c0d43aa13
       ah=sha1 key=20 8a5bedd6a0ce0f8daf7593601acfe2c618a0d4e2
------------------------------------------------------
name=Remote_2 ver=1 serial=2 10.200.2.1:0->10.200.4.1:0 lgwy=static tun=intf mode=auto bound_if=3
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=P2_Remote_2 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=0000000f type=00 soft=0 mtu=1280 expire=1732 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1749/1800
  dec: spi=b95a77ff esp=aes key=32 582af59d71635b835c9208878e0e3f3fe31ba1dfd88ff83ca9bab1ed66ac325e
       ah=sha1 key=20 0d951e62a1bcb63232df6d0fb86df49ab714f53b
  enc: spi=9293e7d5 esp=aes key=32 eeeecacf3a58161f3390fa612b794c776654c86aef51fbc7542906223d56ebb3
       ah=sha1 key=20 09eaa3085bc30a59091f182eb3d11550385b8304
```

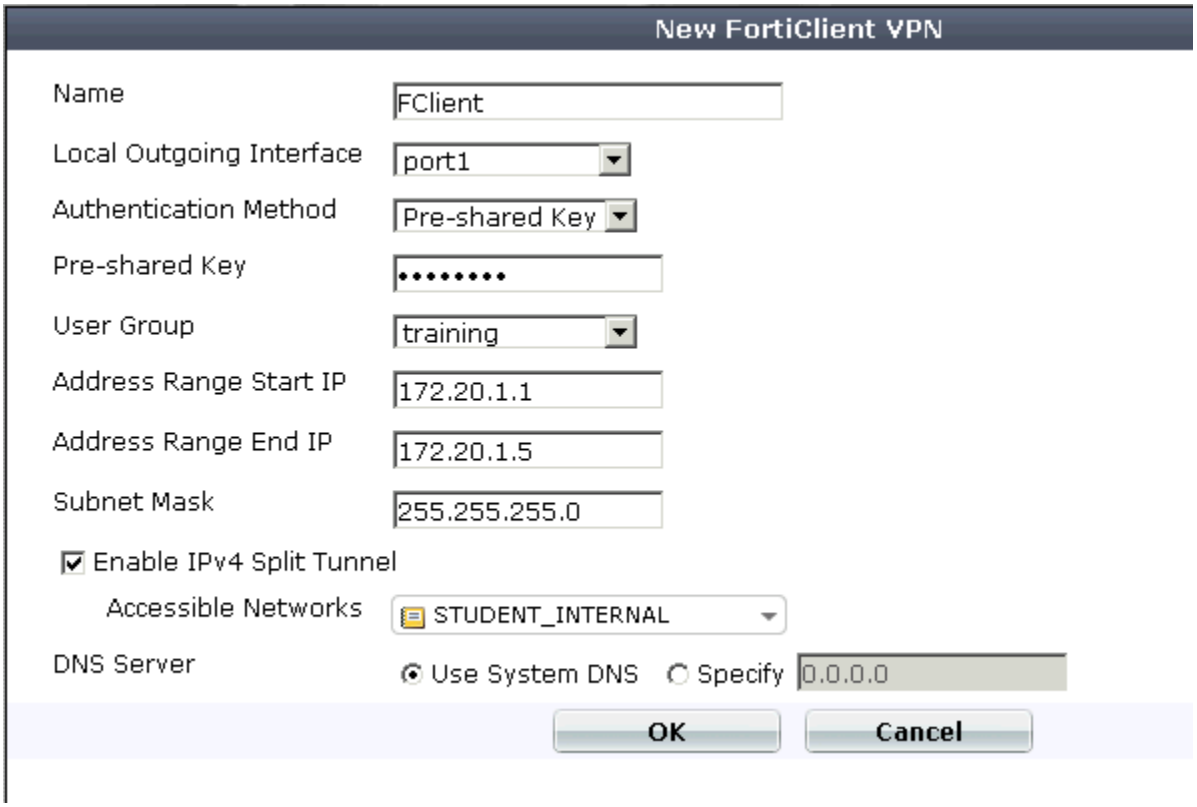
Which of the following statements is correct regarding this output? (Select one answer).

A. One tunnel is rekeying
B. Two tunnels are rekeying
C. Two tunnels are up
D. One tunnel is up

Answer: C

Question: 107

Review the configuration for FortiClient IPsec shown in the Exhibit below.



Which of the following statements is correct regarding this configuration?

A. The connecting VPN client will install a route to a destination corresponding to the STUDENT_INTERNAL address object
B. The connecting VPN client will install a default route
C. The connecting VPN client will install a route to the 172.20.1.[1-5] address range
D. The connecting VPN client will connect in web portal mode and no route will be installed

Answer: A

Question: 108

Review the IPsec diagnostics output of the command diag vpn tunnel list shown in the Exhibit below.

```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=FClient_0 ver=1 serial=3 10.200.1.1:4500->10.200.3.1:64916 lgwy=static tun=intf mode=dial_inst bound_if=2
parent=FClient index=0
proxyid_num=1 child_num=0 refcnt=8 ilast=2 olast=2
stat: rxp=59 txp=0 rxb=15192 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=10
natt: mode=keepalive draft=32 interval=10 remote_port=64916
proxyid=FClient proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:172.20.1.1-172.20.1.1:0
  SA: ref=3 options=00000006 type=00 soft=0 mtu=1280 expire=1717 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1791/1800
  dec: spi=a29046e9 esp=3des key=24 0525830c6fd67ca37e9d6dad174d175e24f97c3b87f428fa
       ah=sha1 key=20 982f8ba194f3f797773efc605c8321b728dabf1d
  enc: spi=19be4052 esp=3des key=24 da597cb7fec913528f8598d1aa7ecd17156a2a7a4afeeb4c
       ah=sha1 key=20 9e2c5d0fc055fa0149bc66024732e9a85bbe8016
------------------------------------------------------
```

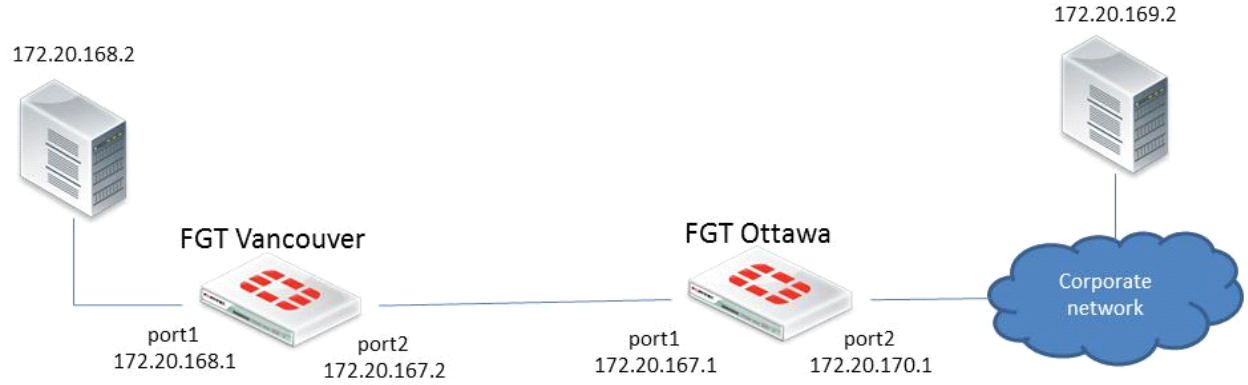
Which of the following statements are correct regarding this output? (Select all that apply.)

A. The connecting client has been allocated address 172.20.1.1.
B. In the Phase 1 settings, dead peer detection is enabled.
C. The tunnel is idle.
D. The connecting client has been allocated address 10.200.3.1.

Answer: A, B

Question: 109

Examine the Exhibit shown below; then answer the question following it.



In this scenario, the Fortigate unit in Ottawa has the following routing table:
S* 0.0.0.0/0 [10/0] via 172.20.170.254, port2
C 172.20.167.0/24 is directly connected, port1
C 172.20.170.0/24 is directly connected, port2
Sniffer tests show that packets sent from the Source IP address 172.20.168.2 to the Destination IP address 172.20.169.2 are being dropped by the FortiGate unit located in Ottaw
a. Which of the following correctly describes the cause for the dropped packets?
A. The forward policy check.
B. The reverse path forwarding check.
C. The subnet 172.20.169.0/24 is NOT in the Ottawa FortiGate unit's routing table.

D. The destination workstation 172.20.169.2 does NOT have the subnet 172.20.168.0/24 in its routing table.

Answer: B

Question: 110

Examine the two static routes to the same destination subnet 172.20.168.0/24 as shown below; then answer the question following it.

```
config router static
edit 1
set dst 172.20.168.0 255.255.255.0
set distance 20
set priority 10
set device port1
next
edit 2
set dst 172.20.168.0 255.255.255.0
set distance 20
set priority 20
set device port2
next
end
```

Which of the following statements correctly describes the static routing configuration provided above?

A. The FortiGate unit will evenly share the traffic to 172.20.168.0/24 through both routes.
B. The FortiGate unit will share the traffic to 172.20.168.0/24 through both routes, but the port2 route will carry approximately twice as much of the traffic.
C. The FortiGate unit will send all the traffic to 172.20.168.0/24 through port1.
D. Only the route that is using port1 will show up in the routing table.

Answer: C

Question: 111

Examine the Exhibit shown below; then answer the question following it.

The Vancouver FortiGate unit initially had the following information in its routing table:

S 172.20.0.0/16 [10/0] via 172.21.1.2, port2

C 172.21.0.0/16 is directly connected, port2
C 172.11.11.0/24 is directly connected, port1
Afterwards, the following static route was added:
config router static
edit 6
set dst 172.20.1.0 255.255.255.0
set pririoty 0
set device port1
set gateway 172.11.12.1
next
end
Since this change, the new static route is NOT showing up in the routing table. Given the information provided, which of the following describes the cause of this problem?

A. The subnet 172.20.1.0/24 is overlapped with the subnet of one static route that is already in the routing table (172.20.0.0/16), so, we need to enable allow-subnet-overlap first.
B. The 'gateway' IP address is NOT in the same subnet as the IP address of port1.
C. The priority is 0, which means that the route will remain inactive.
D. The static route configuration is missing the distance setting.

Answer: B

Question: 112

Examine the static route configuration shown below; then answer the question following it.
config router static
edit 1
set dst 172.20.1.0 255.255.255.0
set device port1
set gateway 172.11.12.1
set distance 10
set weight 5
next
edit 2
set dst 172.20.1.0 255.255.255.0
set blackhole enable
set distance 5
set weight 10
next
end
Which of the following statements correctly describes the static routing configuration provided? (Select all that apply.)

A. All traffic to 172.20.1.0/24 will always be dropped by the FortiGate unit.
B. As long as port1 is up, all the traffic to 172.20.1.0/24 will be routed by the static route number 1. If the interface port1 is down, the traffic will be routed using the blackhole route.

C. The FortiGate unit will NOT create a session entry in the session table when the traffic is being routed by the blackhole route.
D. The FortiGate unit will create a session entry in the session table when the traffic is being routed by the blackhole route.
E. Traffic to 172.20.1.0/24 will be shared through both routes.

Answer: A, C

Question: 113

In the case of TCP traffic, which of the following correctly describes the routing table lookups performed by a FortiGate unit when searching for a suitable gateway?

A. A look-up is done only when the first packet coming from the client (SYN) arrives.
B. A look-up is done when the first packet coming from the client (SYN) arrives, and a second is performed when the first packet coming from the server (SYNC/ACK) arrives.
C. A look-up is done only during the TCP 3-way handshake (SYNC, SYNC/ACK, ACK).
D. A look-up is always done each time a packet arrives, from either the server or the client side.

Answer: B

Question: 114

Shown below is a section of output from the debug command diag ip arp list.
index=2 ifname=port1 172.20.187.150 00:09:0f:69:03:7e state=00000004 use=4589 confirm=4589 update=2422 ref=1
In the output provided, which of the following best describes the IP address 172.20.187.150?

A. It is the primary IP address of the port1 interface.
B. It is one of the secondary IP addresses of the port1 interface.
C. It is the IP address of another network device located in the same LAN segment as the FortiGate unit's port1 interface.

Answer: C

Question: 115

Review the output of the command get router info routing-table database shown in the Exhibit below; then answer the question following it.

```
STUDENT # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

S     *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
      *>           [10/0] via 10.200.2.254, port2, [5/0]
C     *> 10.0.1.0/24 is directly connected, port3
S        10.0.2.0/24 [20/0] is directly connected, Remote_2
S     *> 10.0.2.0/24 [10/0] is directly connected, Remote_1
C     *> 10.200.1.0/24 is directly connected, port1
C     *> 10.200.2.0/24 is directly connected, port2
```

Which of the following statements are correct regarding this output? (Select all that apply).

A. There will be six routes in the routing table.
B. There will be seven routes in the routing table.
C. There will be two default routes in the routing table.
D. There will be two routes for the 10.0.2.0/24 subnet in the routing table.

Answer: A, C

Question: 116

Review the output of the command config router ospf shown in the Exhibit below; then answer the question following it.

```
STUDENT (ospf) # show
config router ospf
        config area
            edit 0.0.0.0
            next
        end
        config network
            edit 1
                set prefix 10.0.1.0 255.255.255.0
            next
            edit 2
                set prefix 172.16.0.0 255.240.0.0
            next
        end
        config ospf-interface
            edit "R1_OSPF"
                set interface "Remote_1"
                set ip 172.16.1.1
                set mtu 1436
                set network-type point-to-point
            next
            edit "R2_OSPF"
                set cost 20
                set interface "Remote_2"
                set ip 172.16.1.2
                set mtu 1436
                set network-type point-to-point
            next
        end
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "rip"
        end
        config redistribute "bgp"
        end
        config redistribute "isis"
        end
    set router-id 0.0.0.1
end
```

Which one of the following statements is correct regarding this output?

A. OSPF Hello packets will only be sent on interfaces configured with the IP addresses 172.16.1.1 and 172.16.1.2.
B. OSPF Hello packets will be sent on all interfaces of the FortiGate device.
C. OSPF Hello packets will be sent on all interfaces configured with an address matching the 10.0.1.0/24 and 172.16.0.0/12 networks.
D. OSPF Hello packets are not sent on point-to-point networks.

Answer: C

Question: 117

Review the output of the command get router info routing-table all shown in the Exhibit below; then answer the question following it.

```
STUDENT # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 10.200.1.254, port1
                  [10/0] via 10.200.2.254, port2, [5/0]
C       10.0.1.0/24 is directly connected, port3
O       10.0.2.0/24 [110/101] via 172.16.2.1, Remote_1, 00:00:21
                    [110/101] via 172.16.2.2, Remote_2, 00:00:21
C       10.200.1.0/24 is directly connected, port1
C       10.200.2.0/24 is directly connected, port2
C       172.16.1.1/32 is directly connected, Remote_1
C       172.16.1.2/32 is directly connected, Remote_2
C       172.16.2.1/32 is directly connected, Remote_1
C       172.16.2.2/32 is directly connected, Remote_2
```

Which one of the following statements correctly describes this output?

A. The two routes to the 10.0.2.0/24 subnet are ECMP routes and traffic will be load balanced based on the configured ECMP settings.
B. The route to the 10.0.2.0/24 subnet via interface Remote_1 is the active and the route via Remote_2 is the backup.
C. OSPF does not support ECMP therefore only the first route to subnet 10.0.1.0/24 is used.
D. 172.16.2.1 is the preferred gateway for subnet 10.0.2.0/24.

Answer: A

Question: 118

Which of the following statements correctly describe Transparent Mode operation? (Select all that apply.)

A. The FortiGate unit acts as transparent bridge and routes traffic using Layer-2 forwarding.
B. Ethernet packets are forwarded based on destination MAC addresses NOT IPs.
C. The device is transparent to network hosts.
D. Permits inline traffic inspection and firewalling without changing the IP scheme of the network.
E. All interfaces must be on different IP subnets.

Answer: A, B, C, D

Question: 119

In Transparent Mode, forward-domain is an attribute of _____.

A. an interface
B. a firewall policy
C. a static route
D. a virtual domain

Answer: A

Question: 120

Which of the following statements are TRUE for Port Pairing and Forwarding Domains? (Select all that apply.)

A. They both create separate broadcast domains.
B. Port Pairing works only for physical interfaces.
C. Forwarding Domains only apply to virtual interfaces.
D. They may contain physical and/or virtual interfaces.
E. They are only available in high-end models.

Answer: A, D

Question: 121

Which of the following is an advantage of using SNMP v3 instead of SNMP v1/v2 when querying the FortiGate unit?

A. Packet encryption
B. MIB-based report uploads
C. SNMP access limits through access lists
D. Running SNMP service on a non-standard port is possible

Answer: A

Question: 122

An administrator logs into a FortiGate unit using an account which has been assigned a super_admin profile. Which of the following operations can this administrator perform?

A. They can delete logged-in users who are also assigned the super_admin access profile.
B. They can make changes to the super_admin profile.
C. They can delete the admin account if the default admin user is not logged in.
D. They can view all the system configuration settings but can not make changes.
E. They can access configuration options for only the VDOMs to which they have been assigned.

Answer: C

Question: 123

The diag sys session list command is executed in the CLI. The output of this command is shown in the exhibit.

```
session info: proto=6 proto_state=11 duration=539 expire=3571 timeout=3600
flags=00000000 sockflag=00000000 sockport=80 av_idx=0 use=5
origin-shaper=guarantee-100kbps prio=1 guarantee 12288/sec max 134217728/sec
traffic 123/sec
reply-shaper=low-priority prio=3 guarantee 0/sec max 134217728/sec traffic 115/sec
per_ip_shaper=
ha_id=0 hakey=1335
policy_dir=0 tunnel=/
state=redir local may_dirty ndr os rs rem
statistic(bytes/packets/allow_err): org=3201/59/1 reply=2672/58/1 tuples=3
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9
gwy=76.27.192.1/192.168.203.2
hook=post dir=org act=snat 192.168.203.2:3196-
>128.100.58.53:80(76.27.195.147:58618)
hook=pre dir=reply act=dnat 128.100.58.53:80-
>76.27.195.147:58618(192.168.203.2:3196)
hook=post dir=reply act=noop 128.100.58.53:80->192.168.203.2:3196(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=10 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=00115cae tos=ff/ff app_list=2000 app=0
dd_type=0 dd_rule_id=0
per_ip_bandwidth meter: addr=192.168.203.2, bps=1351
```

Based on the output from this command, which of the following statements is correct?

A. This is a UDP session.
B. Traffic shaping is being applied to this session.

C. This is an ICMP session.
D. This traffic has been authenticated.
E. This session matches a firewall policy with ID 5.

Answer: B

Question: 124

A FortiGate unit is configured with multiple VDOMs. An administrative account on the device has been assigned a Scope value of VDOM:root.
Which of the following items would an administrator logging in using this account NOT be able to configure?

A. Firewall addresses
B. DHCP servers
C. FortiGuard Distribution Network configuration
D. PPTP VPN configuration

Answer: C

Question: 125

What is the effect of using CLI "config system session-ttl" to set session_ttl to 1800 seconds?

A. Sessions can be idle for no more than 1800 seconds.
B. The maximum length of time a session can be open is 1800 seconds.
C. After 1800 seconds, the end user must reauthenticate.
D. After a session has been open for 1800 seconds, the FortiGate unit will send a keepalive packet to both client and server.

Answer: A

Question: 126

Which of the following statements is correct about how the FortiGate unit verifies username and password during user authentication?

A. If a remote server is included in a user group, it will be checked before local accounts.
B. An administrator can define a local account for which the password must be verified by querying a remote server.
C. If authentication fails with a local password, the FortiGate unit will query the authentication server if the local user is configured with both a local password and an authentication server.

D. The FortiGate unit will only attempt to authenticate against Active Directory if Fortinet Server Authentication Extensions are installed and configured.

Answer: B

Question: 127

Which of the following statements are correct regarding the configuration of a FortiGate unit as an SSL VPN gateway? (Select all that apply.)

A. Tunnel mode can only be used if the SSL VPN user groups have at least one Host Check option enabled.
B. The specific routes needed to access internal resources through an SSL VPN connection in tunnel mode from the client computer are defined in the routing widget associated with the SSL VPN portal.
C. In order to apply a portal to a user, that user must belong to an SSL VPN user group.
D. The portal settings specify whether the connection will operate in web-only or tunnel mode.

Answer: C, D

Question: 128

Which of the following statements is correct about configuring web filtering overrides?

A. The Override option for FortiGuard Web Filtering is available for any user group type.
B. Admin overrides require an administrator to manually allow pending override requests which are listed in the Override Monitor.
C. The Override Scopes of User and User Group are only for use when Firewall Policy Authentication is also being used.
D. Using Web Filtering Overrides requires the use of Firewall Policy Authentication.

Answer: C

Question: 129

The FortiGate Server Authentication Extensions (FSAE) provide a single sign on solution to authenticate users transparently to a FortiGate unit using credentials stored in Windows Active Directory.
Which of the following statements are correct regarding FSAE in a Windows domain environment when NTLM is not used? (Select all that apply.)

A. An FSAE Collector Agent must be installed on every domain controller.
B. An FSAE Domain Controller Agent must be installed on every domain controller.
C. The FSAE Domain Controller Agent will regularly update user logon information on the FortiGate unit.

D. The FSAE Collector Agent will retrieve user information from the Domain Controller Agent and will send the user logon information to the FortiGate unit.
E. For non-domain computers, an FSAE client must be installed on the computer to allow FSAE authentication.

Answer: B, D

Question: 130

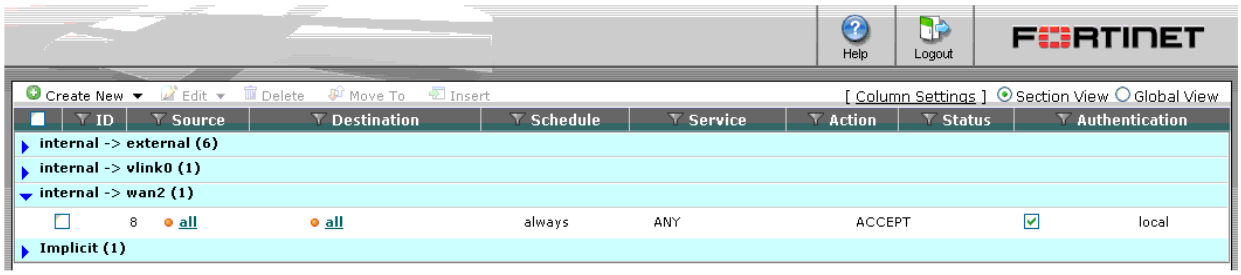
Bob wants to send Alice a file that is encrypted using public key cryptography.
Which of the following statements is correct regarding the use of public key cryptography in this scenario?

A. Bob will use his private key to encrypt the file and Alice will use her private key to decrypt the file.
B. Bob will use his public key to encrypt the file and Alice will use Bob's private key to decrypt the file.
C. Bob will use Alice's public key to encrypt the file and Alice will use her private key to decrypt the file.
D. Bob will use his public key to encrypt the file and Alice will use her private key to decrypt the file.
E. Bob will use Alice's public key to encrypt the file and Alice will use Bob's public key to decrypt the file.

Answer: C

Question: 131

Which of the following statements is correct based on the firewall configuration illustrated in the exhibit?



A. A user can access the Internet using only the protocols that are supported by user authentication.
B. A user can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP. These require authentication before the user will be allowed access.
C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access any services.
D. A user cannot access the Internet using any protocols unless the user has passed firewall authentication.

Answer: D

Question: 132

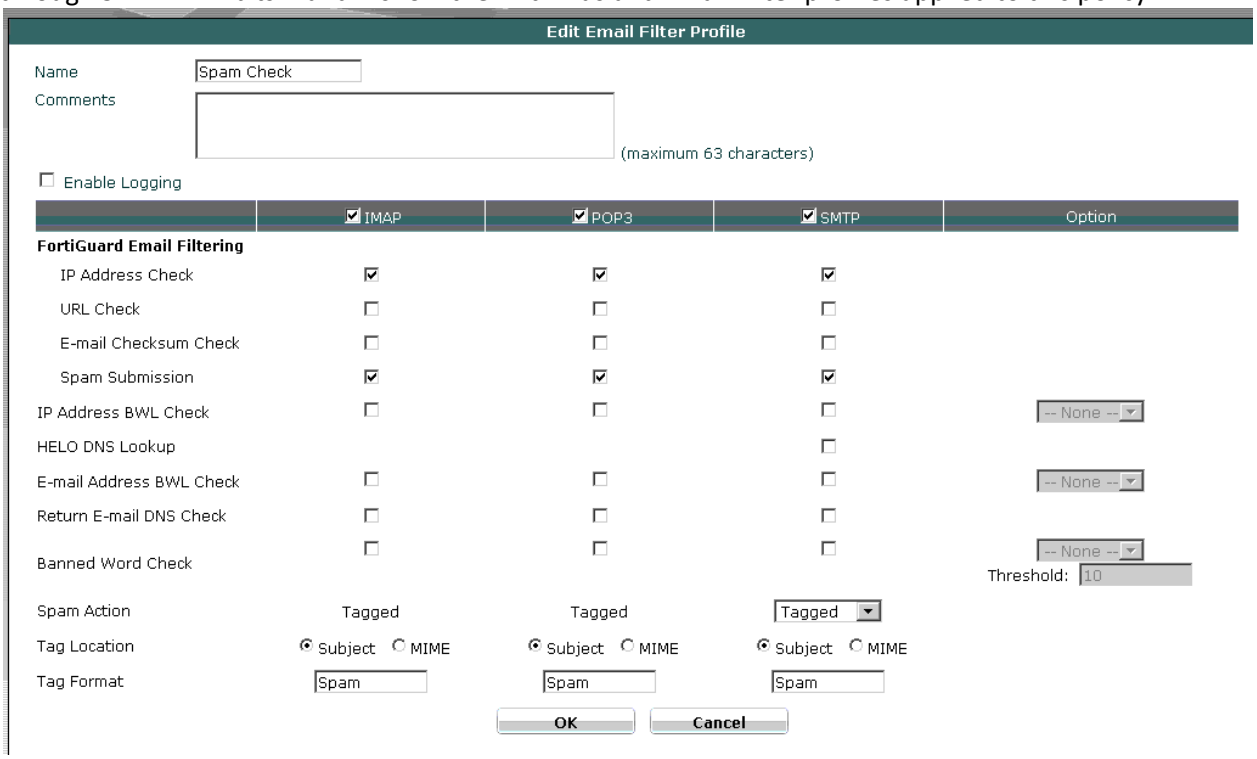
Which of the following statements is correct regarding the antivirus scanning function on the FortiGate unit?

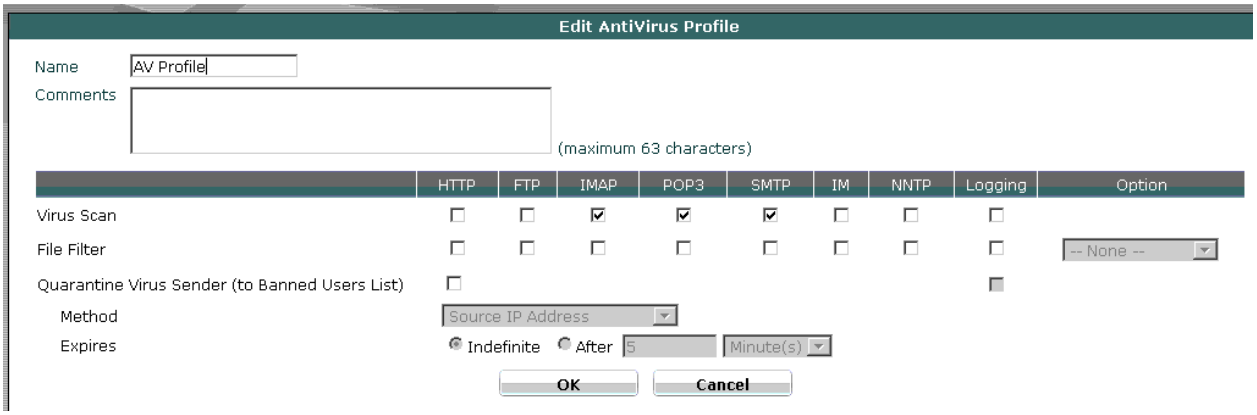
A. Antivirus scanning provides end-to-end virus protection for client workstations.
B. Antivirus scanning provides virus protection for the HTTP, Telnet, SMTP, and FTP protocols.
C. Antivirus scanning supports banned word checking.
D. Antivirus scanning supports grayware protection.

Answer: D

Question: 133

A firewall policy has been configured for the internal email server to receive email from external parties through SMTP. Exhibits A and B show the AntiVirus and Email Filter profiles applied to this policy.





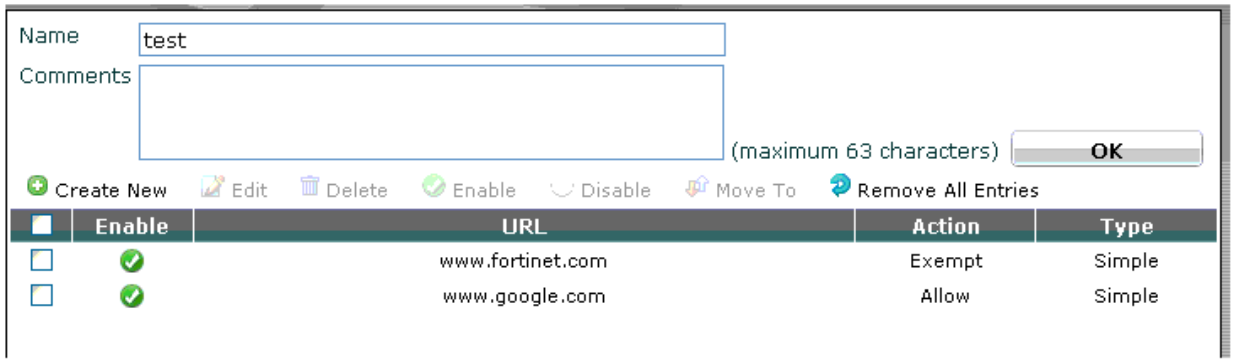
What is the correct behavior when the email attachment is detected as a virus by the FortiGate AntiVirus engine?

A. The FortiGate unit will remove the infected file and deliver the email with a replacement message to alert the recipient that the original attachment was infected.
B. The FortiGate unit will reject the infected email and notify both the sender and recipient.
C. The FortiGate unit will remove the infected file and add a replacement message. Both sender and recipient are notified that the infected file has been removed.
D. The FortiGate unit will reject the infected email and notify the sender.

Answer: A

Question: 134

Which of the following describes the best custom signature for detecting the use of the word "Fortinet" in chat applications?




```
MSN Messenger Service
  MSG 213 N 135\r\n
  MIME-Version: 1.0\r\n
  Content-Type: text/plain; charset=UTF-8\r\n
  X-MMS-IM-Format: FN=MS%20Shell%20Dlg%202; EF=; CO=0; CS=1; PF=0\r\n
  \r\n
  Fortinet
```

A. The sample packet trace illustrated in the exhibit provides details on the packet that requires detection.
F-SBID(--protocol tcp; --flow from_client; --pattern "X-MMS-IM-Format"; --pattern "fortinet"; --no_case;)
B. F-SBID(--protocol tcp; --flow from_client; --pattern "fortinet"; --no_case;)
C. F-SBID(--protocol tcp; --flow from_client; --pattern "X-MMS-IM-Format"; --pattern "fortinet"; --within 20; --no_case;)
D. F-SBID(--protocol tcp; --flow from_client; --pattern "X-MMS-IM-Format"; --pattern "fortinet"; --within 20;)

Answer: A

Question: 135

An administrator is examining the attack logs and notices the following entry:
type=ips subtype=signature pri=alert vd=root serial=1995 attack_id=103022611 src=69.45.64.22 dst=192.168.1.100 src_port=80 dst_port=4887 src_int=wlan dst_int=internal status=detected proto=6 service=4887/tcp user=N/A group=N/A msg=web_client: IE.IFRAME.BufferOverflow.B
Based on the information displayed in this entry, which of the following statements are correct? (Select all that apply.)

A. This is an HTTP server attack.
B. The attack was detected and blocked by the FortiGate unit.
C. The attack was against a FortiGate unit at the 192.168.1.100 IP address.
D. The attack was detected and passed by the FortiGate unit.

Answer: C, D

Question: 136

An administrator is examining the attack logs and notices the following entry:
device_id=FG100A3907508962 log_id=18432 subtype=anomaly type=ips timestamp=1270017358 pri=alert itime=1270017893 severity=critical src=192.168.1.52 dst=64.64.64.64 src_int=internal serial=0 status=clear_session proto=6 service=http vd=root count=1 src_port=35094 dst_port=80 attack_id=100663402 sensor=protect-servers ref=http://www.fortinet.com/ids/VID100663402 msg="anomaly: tcp_src_session, 2 > threshold 1" policyid=0 carrier_ep=N/A profile=N/A dst_int=N/A user=N/A group=N/A
Based solely upon this log message, which of the following statements is correct?

A. This attack was blocked by the HTTP protocol decoder.
B. This attack was caught by the DoS sensor "protect-servers".
C. This attack was launched against the FortiGate unit itself rather than a host behind the FortiGate unit.
D. The number of concurrent connections to destination IP address 64.64.64.64 has exceeded the configured threshold.

Answer: B

Question: 137

Which of the following items are considered to be advantages of using the application control features on the FortiGate unit?
Application control allows an administor to:

A. set a unique session-ttl for select applications.
B. customize application types in a similar way to adding custom IPS signatures.
C. check which applications are installed on workstations attempting to access the network.
D. enable AV scanning per application rather than per policy.

Answer: A

Question: 138

Which of the following features could be used by an administrator to block FTP uploads while still allowing FTP downloads?

A. Anti-Virus File-Type Blocking
B. Data Leak Prevention
C. Network Admission Control
D. FortiClient Check

Answer: B

Question: 139

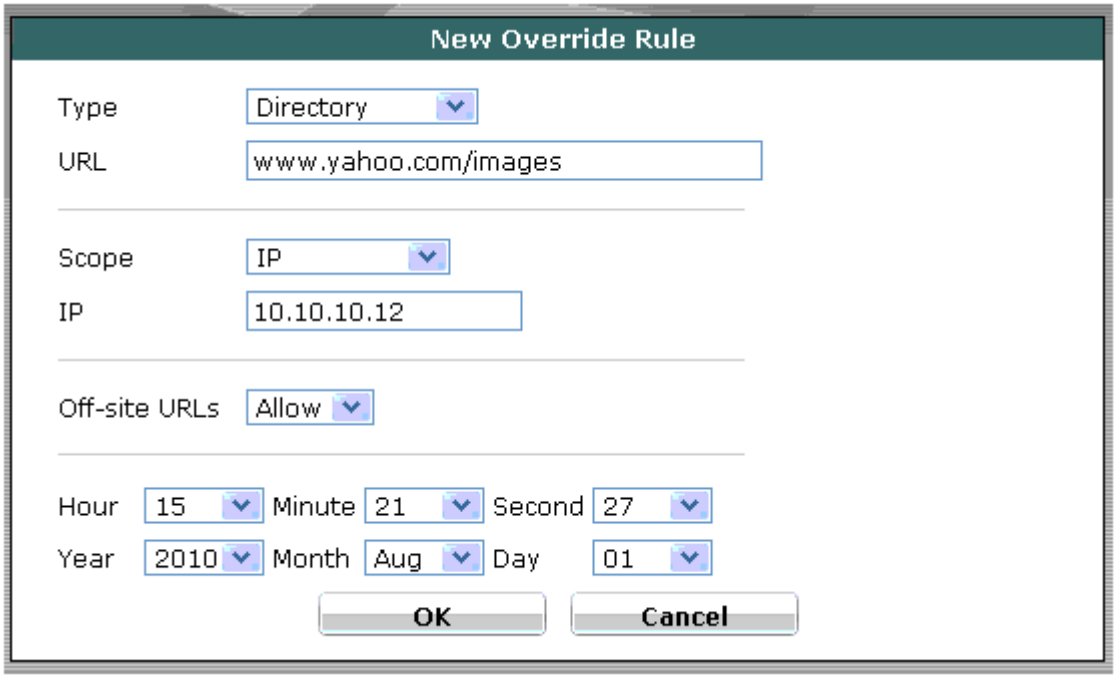
An organization wishes to protect its SIP Server from call flooding attacks. Which of the following configuration changes can be performed on the FortiGate unit to fulfill this requirement?

A. Apply an application control list which contains a rule for SIP and has the "Limit INVITE Request" option configured.
B. Enable Traffic Shaping for the appropriate SIP firewall policy.
C. Reduce the session time-to-live value for the SIP protocol by running the configure system session-ttl CLI command.
D. Run the set udp-idle-timer CLI command and set a lower time value.

Answer: A

Question: 140

Which of the following statements is correct regarding the FortiGuard Services Web Filtering Override configuration as illustrated in the exhibit?

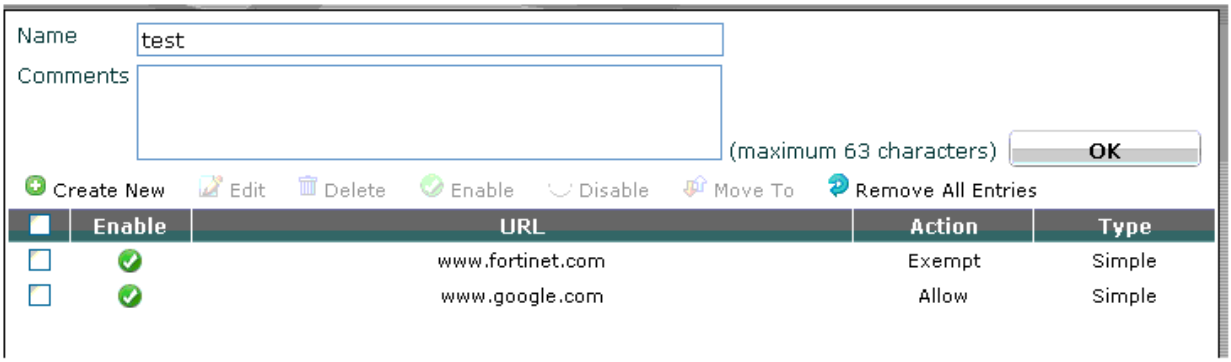


A. Any client on the same subnet as the authenticated user is allowed to access www.yahoo.com/images/.
B. A client with an IP of address 10.10.10.12 is allowed access to any subdirectory that is part of the www.yahoo.com web site.
C. A client with an IP address of 10.10.10.12 is allowed access to the www.yahoo.com/images/ web site and any of its offsite URLs.
D. A client with an IP address of 10.10.10.12 is allowed access to any URL under the www.yahoo.com web site, including any subdirectory URLs, until August 7, 2009.
E. Any client on the same subnet as the authenticated user is allowed to access www.yahoo.com/images/ until August 7, 2009.

Answer: C

Question: 141

Based on the web filtering configuration illustrated in the exhibit,



which one of the following statements is not a reasonable conclusion?

A. Users can access both the www.google.com site and the www.fortinet.com site.
B. When a user attempts to access the www.google.com site, the FortiGate unit will not perform web filtering on the content of that site.
C. When a user attempts to access the www.fortinet.com site, any remaining web filtering will be bypassed.
D. Downloaded content from www.google.com will be scanned for viruses if antivirus is enabled.

Answer: B

Question: 142

Which spam filter is not available on a FortiGate device?

A. Sender IP reputation database
B. URLs included in the body of known SPAM messages.
C. Email addresses included in the body of known SPAM messages.
D. Spam object checksums
E. Spam grey listing

Answer: E

Question: 143

Which part of an email message exchange is NOT inspected by the POP3 and IMAP proxies?

A. TCP connection
B. File attachments
C. Message headers
D. Message body

Answer: A

Question: 144

Which of the following statements best decribes the proxy behavior on a FortiGate unit during an FTP client upload when FTP splice is disabled?

A. The proxy buffers the entire file from the client, only sending the file to the server if the file is clean. One possible consequence of buffering is that the server could time out.
B. The proxy sends the file to the server while simultaneously buffering it.
C. The proxy removes the infected file from the server by sending a delete command on behalf of the client.
D. If the file being scanned is determined to be clean, the proxy terminates the connection and leaves the file on the server.

Answer: A

Question: 145

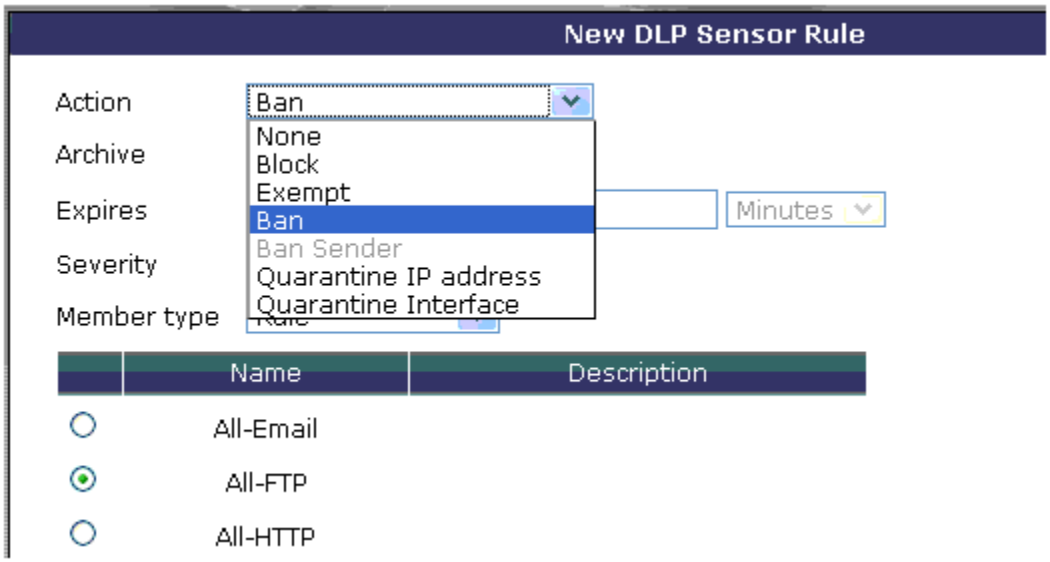
Which of the following describes the difference between the ban and quarantine actions?

A. A ban action prevents future transactions using the same protocol which triggered the ban. A qarantine action blocks all future transactions, regardless of the protocol.
B. A ban action blocks the transaction. A quarantine action archives the data.
C. A ban action has a finite duration. A quarantine action must be removed by an administrator.
D. A ban action is used for known users. A quarantine action is used for unknown users.

Answer: A

Question: 146

An administrator is configuring a DLP rule for FTP traffic. When adding the rule to a DLP sensor,



the administrator notes that the Ban Sender action is not available (greyed-out), as shown in the exhibit. Which of the following is the best explanation for the Ban Sender action NOT being available?

A. The Ban Sender action is never available for FTP traffic.
B. The Ban Sender action needs to be enabled globally for FTP traffic on the FortiGate unit before configuring the sensor.
C. Firewall policy authentication is required before the Ban Sender action becomes available.
D. The Ban Sender action is only available for known domains. No domains have yet been added to the domain list.

Answer: A

Question: 147

When viewing the Banned User monitor in Web Config, the administrator notes the entry illustrated in the exhibit.

#	Ban key	Application Protocol	Cause or rule	Created	Expires
1	192.168.203.2	HTTP-get	http-get-put	Fri Jun 11 15:25:38 2010	Indefinite

Which of the following statements is correct regarding this entry?

A. The entry displays a ban that has been added as a result of traffic triggering a configured DLP rule.
B. The entry displays a ban that was triggered by HTTP traffic matching an IPS signature. This client is banned from receiving or sending any traffic through the FortiGate.
C. The entry displays a quarantine, which could have been added by either IPS or DLP.
D. This entry displays a ban entry that was added manually by the administrator on June11th.

Answer: A

Question: 148

The following ban list entry is displayed through the CLI.
get user ban list
id cause src-ip-addr dst-ip-addr expires created
531 protect_client 10.177.0.21 207.1.17.1 indefinite Wed Dec 24 :21:33 2008
Based on this command output, which of the following statements is correct?

A. The administrator has specified the Attack and Victim Address method for the quarantine.
B. This diagnostic entry results from the administrator running the diag ips log test command. This command has no effect on traffic.
C. A DLP rule has been matched.
D. An attack has been repeated more than once during the holddown period; the expiry time has been reset to indefinite.

Answer: A

Question: 149

Which of the following statements is correct regarding the NAC Quarantine feature?

A. With NAC quarantine, files can be quarantined not only as a result of antivirus scanning, but also for other forms of content inspection such as IPS and DLP.
B. NAC quarantine does a client check on workstations before they are permitted to have administrative access to FortiGate.
C. NAC quarantine allows administrators to isolate clients whose network activity poses a security risk.
D. If you chose the quarantine action, you must decide whether the quarantine type is NAC quarantine or File quarantine.

Answer: C

Question: 150

Which of the following DLP actions will override any other action?

A. Exempt
B. Quarantine Interface
C. Block
D. None

Answer: A

Question: 151

Which of the following DLP actions will always be performed if it is selected?

A. Archive
B. Quarantine Interface
C. Ban Sender
D. Block
E. None
F. Ban
G. Quarantine IP Address

Answer: A

Question: 152

The transfer of encrypted files or the use of encrypted protocols between users and servers on the internet can frustrate the efforts of administrators attempting to monitor traffic passing through the FortiGate unit and ensuring user compliance to corporate rules.
Which of the following items will allow the administrator to control the transfer of encrypted data through the FortiGate unit? (Select all that apply.)

A. Encrypted protocols can be scanned through the use of the SSL proxy.
B. DLP rules can be used to block the transmission of encrypted files.
C. Firewall authentication can be enabled in the firewall policy, preventing the use of encrypted communications channels.
D. Application control can be used to monitor the use of encrypted protocols; alerts can be sent to the administrator through email when the use of encrypted protocols is attempted.

Answer: A, B, D

Question: 153

A DLP rule with an action of Exempt has been matched against traffic passing through the FortiGate unit. Which of the following statements is correct regarding how this transaction will be handled by the FortiGate unit?

A. Any other matched DLP rules will be ignored with the exception of Archiving.
B. Future files whose characteristics match this file will bypass DLP scanning.
C. The traffic matching the DLP rule will bypass antivirus scanning.
D. The client IP address will be added to a white list.

Answer: A

Question: 154

The following diagnostic output is displayed in the CLI:
diag firewall auth list
policy iD. 9, srC. 192.168.3.168, action: accept, timeout: 13427
user: forticlient_chk_only, group:
flag (80020): auth timeout_ext, flag2 (40): exact
group iD. 0, av group: 0
----- 1 listed, 0 filtered ------
Based on this output, which of the following statements is correct?

A. Firewall policy 9 has endpoint compliance enabled but not firewall authentication.
B. The client check that is part of an SSL VPN connection attempt failed.
C. This user has been associated with a guest profile as evidenced by the group id of 0.
D. An auth-keepalive value has been enabled.

Answer: A

Question: 155

Which of the following cannot be used in conjunction with the endpoint compliance check?

A. HTTP Challenge Redirect to a Secure Channel (HTTPS) in the Authentication Settings.
B. Any form of firewall policy authentication.
C. WAN optimization.
D. Traffic shaping.

Answer: A

Question: 156

SSL Proxy is used to decrypt the SSL-encrypted traffic. After decryption, where is the traffic buffered in preparation for content inspection?

A. The file is buffered by the application proxy.
B. The file is buffered by the SSL proxy.
C. In the upload direction, the file is buffered by the SSL proxy. In the download direction, the file is buffered by the application proxy.

D. No file buffering is needed since a stream-based scanning approach is used for SSL content inspection.

Answer: A

Question: 157

Which of the following statements correctly describes the deepscan option for HTTPS?

A. When deepscan is disabled, only the web server certificate is inspected; no decryption of content occurs.
B. Enabling deepscan will perform further checks on the server certificate.
C. Deepscan is only applicable to mail protocols, where all IP addresses in the header are checked.
D. With deepscan enabled, archived files will be decompressed before scanning for a more comprehensive file inspection.

Answer: A

Question: 158

Which of the following tasks fall under the responsibility of the SSL proxy in a typical HTTPS connection? (Select all that apply.)

A. The web client SSL handshake.
B. The web server SSL handshake.
C. File buffering.
D. Communication with the urlfilter process.

Answer: A, B

Question: 159

When the SSL proxy inspects the server certificate for Web Filtering only in SSL Handshake mode, which certificate field is being used to determine the site rating?

A. Common Name
B. Organization
C. Organizational Unit
D. Serial Number
E. Validity

Answer: A

Question: 160

When performing a log search on a FortiAnalyzer, it is generally recommended to use the Quick Search option.
What is a valid reason for using the Full Search option, instead?

A. The search items you are looking for are not contained in indexed log fields.
B. A quick search only searches data received within the last 24 hours.
C. You want the search to include the FortiAnalyzer's local logs.
D. You want the search to include content archive data as well.

Answer: A

Question: 161

Both the FortiGate and FortiAnalyzer units can notify administrators when certain alert conditions are met.
Considering this, which of the following statements is NOT correct?

A. On a FortiGate device, the alert condition is based either on the severity level or on the log type, but not on a combination of the two.
B. On a FortiAnalyzer device, the alert condition is based either on the severity level or on the log type, but not on a combination of the two.
C. Only a FortiAnalyzer device can send the alert notification in the form of a syslog message.
D. Both the FortiGate and FortiAnalyzer devices can send alert notifications in the form of an email alert.

Answer: B

Question: 162

Which of the following report templates must be used when scheduling report generation?

A. Layout Template
B. Data Filter Template
C. Output Template
D. Chart Template

Answer: A

Question: 163

In which of the following report templates would you configure the charts to be included in the report?

A. Layout Template
B. Data Filter Template
C. Output Template
D. Schedule Template

Answer: A

Question: 164

An administrator wishes to generate a report showing Top Traffic by service type. They notice that web traffic overwhelms the pie chart and want to exclude the web traffic from the report.
Which of the following statements best describes how to do this?

A. In the Service field of the Data Filter, type 80/tcp and select the NOT checkbox.
B. Add the following entry to the Generic Field section of the Data Filter: service="!web".
C. When editing the chart, uncheck wlog to indicate that Web Filtering data is being excluded when generating the chart.
D. When editing the chart, enter 'http' in the Exclude Service field.

Answer: A

Question: 165

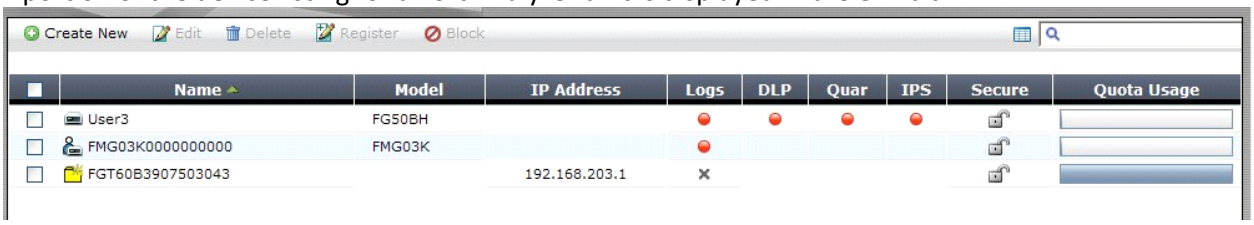
An administrator wishes to generate a report showing Top Traffic by service type, but wants to exclude SMTP traffic from the report.
Which of the following statements best describes how to do this?

A. In the Service field of the Data Filter, type 25/smtp and select the NOT checkbox.
B. Add the following entry to the Generic Field section of the Data Filter: service="!smtp".
C. When editing the chart, uncheck mlog to indicate that Mail Filtering data is being excluded when generating the chart.
D. When editing the chart, enter 'dns' in the Exclude Service field.

Answer: A

Question: 166

A portion of the device listing for a FortiAnalyzer unit is displayed in the exhibit.



Which of the following statements best describes the reason why the FortiGate 60B unit is unable to archive data to the FortiAnalyzer unit?

A. The FortiGate unit is considered an unregistered device.
B. The FortiGate unit has been blocked from sending archive data to the FortiAnalyzer device by the administrator.
C. The FortiGate unit has insufficient privileges. The administrator should edit the device entry in the FortiAnalyzer and modify the privileges.
D. The FortiGate unit is being treated as a syslog device and is only permitted to send log data.

Answer: A

Question: 167

In order to load-share traffic using multiple static routes, the routes must be configured with ...

A. the same distance and same priority.
B. the same distance and the same weight.
C. the same distance but each of them must be assigned a unique priority.
D. a distance equal to its desired weight for ECMP but all must have the same priority.

Answer: A

Question: 168

A static route is configured for a FortiGate unit from the CLI using the following commands:
config router static
edit 1
set device "wan1"
set distance 20
set gateway 192.168.100.1
next
end
Which of the following conditions is NOT required for this static default route to be displayed in the FortiGate unit's routing table?

A. The Administrative Status of the wan1 interface is displayed as Up.
B. The Link Status of the wan1 interface is displayed as Up.
C. All other default routes should have an equal or higher distance.
D. You must disable DHCP client on that interface.

Answer: D

Question: 169

If Routing Information Protocol (RIP) version 1 or version 2 has already been configured on a FortiGate unit, which of the following statements is correct if the routes learned through RIP need to be advertised into Open Shortest Path First (OSPF)?

A. The FortiGate unit will automatically announce all routes learned through RIP v1 or v2 to its OSPF neighbors.
B. The FortiGate unit will automatically announce all routes learned only through RIP v2 to its OSPF neighbors.
C. At a minimum, the network administrator needs to enable Redistribute RIP in the OSPF Advanced Options.
D. The network administrator needs to configure a RIP to OSPF announce policy as part of the RIP settings.
E. At a minimum, the network administrator needs to enable Redistribute Default in the OSPF Advanced Options.

Answer: C

Question: 170

If Open Shortest Path First (OSPF) has already been configured on a FortiGate unit, which of the following statements is correct if the routes learned through OSPF need to be announced by Border Gateway Protocol (BGP)?

A. The FortiGate unit will automatically announce all routes learned through OSPF to its BGP peers if the FortiGate unit is configured as an OSPF Autonomous System Boundary Router (ASBR).
B. The FortiGate unit will automatically announce all routes learned through OSPF to its BGP peers if the FortiGate unit is configured as an OSPF Area Border Router (ABR).
C. At a minimum, the network administrator needs to enable Redistribute OSPF in the BGP settings.
D. The BGP local AS number must be the same as the OSPF area number of the routes learned that need to be redistributed into BGP.
E. By design, BGP cannot redistribute routes learned through OSPF.

Answer: C

Question: 171

An administrator has formed a High Availability cluster involving two FortiGate 310B units.
[Multiple upstream Layer 2 switches] -- [FortiGate HA Cluster] -- [Multiple downstream Layer 2 switches]
The administrator wishes to ensure that a single link failure will have minimal impact upon the overall throughput of traffic through this cluster.
Which of the following options describes the best step the administrator can take?
The administrator should...

A. set up a full-mesh design which uses redundant interfaces.
B. increase the number of FortiGate units in the cluster and configure HA in Active-Active mode.
C. enable monitoring of all active interfaces.
D. configure the HA ping server feature to allow for HA failover in the event that a path is disrupted.

Answer: A

Question: 172

In a High Availability configuration operating in Active-Active mode, which of the following correctly describes the path taken by a load-balanced HTTP session?

A. Request: Internal Host -> Master FG -> Slave FG -> Internet -> Web Server
B. Request: Internal Host -> Master FG -> Slave FG -> Master FG -> Internet -> Web Server
C. Request: Internal Host -> Slave FG -> Internet -> Web Server
D. Request: Internal Host -> Slave FG -> Master FG -> Internet -> Web Server

Answer: A

Question: 173

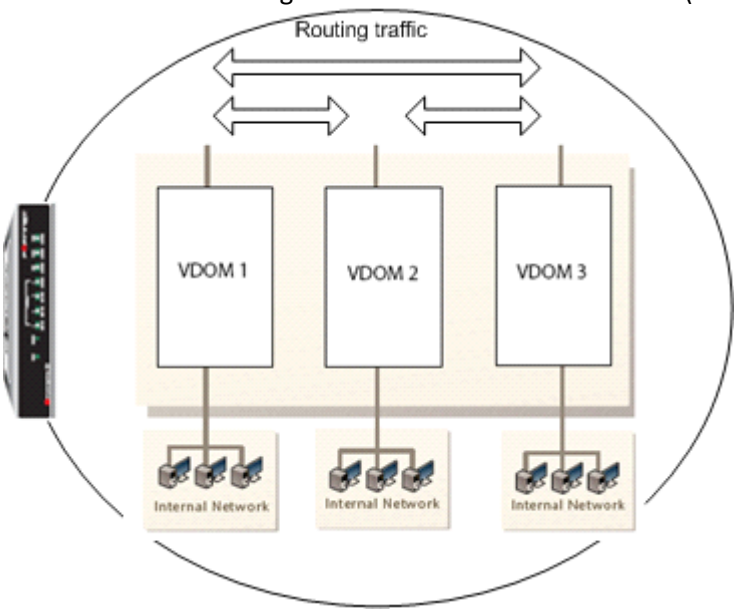
Which of the following statements is not correct regarding virtual domains (VDOMs)?

A. VDOMs divide a single FortiGate unit into two or more virtual units that function as multiple, independent units.
B. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.
C. A backup management VDOM will synchronize the configuration from an active management VDOM.
D. VDOMs share firmware versions, as well as antivirus and IPS databases.
E. Only administrative users with a super_admin profile will be able to enter all VDOMs to make configuration changes.

Answer: C

Question: 174

A FortiGate unit is configured with three Virtual Domains (VDOMs) as illustrated in the exhibit.



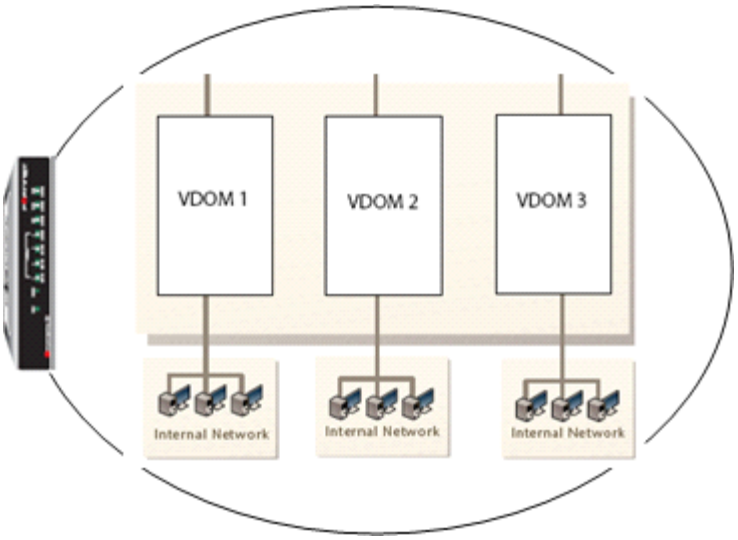
Which of the following statements are true if the network administrator wants to route traffic between all the VDOMs? (Select all that apply.)

A. The administrator should configure inter-VDOM links to avoid using external interfaces and routers.
B. As with all FortiGate unit interfaces, firewall policies must be in place for traffic to be allowed to pass through any interface, including inter-VDOM links. This provides the same level of security internally as externally.
C. This configuration requires the use of an external router.
D. Inter-VDOM routing is automatically provided if all the subnets that need to be routed are locally attached.
E. As each VDOM has an independant routing table, routing rules need to be set (for example, static routing, OSPF) in each VDOM to route traffic between VDOMs.

Answer: A, B, E

Question: 175

A FortiGate unit is configured with three Virtual Domains (VDOMs) as illustrated in the exhibit.



Which of the following statements are correct regarding these VDOMs? (Select all that apply.)

A. The FortiGate unit supports any combination of these VDOMs in NAT/Route and Transparent modes.
B. The FortiGate unit must be a model 1000 or above to support multiple VDOMs.
C. A license had to be purchased and applied to the FortiGate unit before VDOM mode could be enabled.
D. All VDOMs must operate in the same mode.
E. Changing a VDOM operational mode requires a reboot of the FortiGate unit.
F. An admin account can be assigned to one VDOM or it can have access to all three VDOMs.

Answer: A, F

Question: 176

A FortiGate administrator configures a Virtual Domain (VDOM) for a new customer. After creating the VDOM, the administrator is unable to reassign the dmz interface to the new VDOM as the option is greyed out in Web Config in the management VDOM.
What would be a possible cause for this problem?

A. The dmz interface is referenced in the configuration of another VDOM.
B. The administrator does not have the proper permissions to reassign the dmz interface.
C. Non-management VDOMs can not reference physical interfaces.
D. The dmz interface is in PPPoE or DHCP mode.
E. Reassigning an interface to a different VDOM can only be done through the CLI.

Answer: A

Question: 177

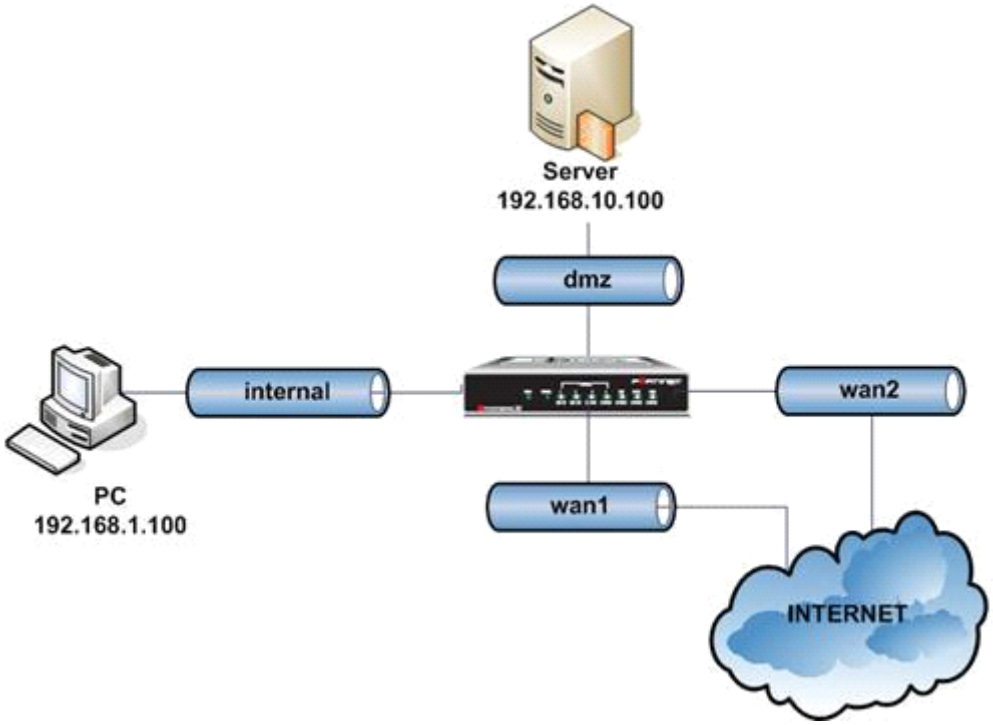
A FortiGate unit is operating in NAT/Route mode and is configured with two Virtual LAN (VLAN) sub-interfaces added to the same physical interface.
Which of the following statements is correct regarding the VLAN IDs in this scenario?

A. The two VLAN sub-interfaces can have the same VLAN ID only if they have IP addresses in different subnets.
B. The two VLAN sub-interfaces must have different VLAN IDs.
C. The two VLAN sub-interfaces can have the same VLAN ID only if they belong to different VDOMs.
D. The two VLAN sub-interfaces can have the same VLAN ID if they are connected to different L2 IEEE 802.1Q compliant switches.

Answer: B

Question: 178

An intermittent connectivity issue is noticed between two devices located behind the FortiGate dmz and internal interfaces. A continuous sniffer trace is run on the FortiGate unit that the administrator will convert into a .cap file for an off-line analysis with a sniffer application.



Given the high volume of global traffic on the network, which of the following CLI commands will best allow the administrator to perform this troubleshooting operation?

A. diagnose sniffer packet any
B. diagnose sniffer packet dmz "" 3
C. diagnose sniffer packet any "host 192.168.1.100 and host 192.168.10.100 " 3
D. diagnose sniffer packet any "host 192.168.1.100 and host 192.168.10.100 “ 4

Answer: C

Question: 179

The Host Check feature can be enabled on the FortiGate unit for SSL VPN connections. When this feature is enabled, the FortiGate unit probes the remote host computer to verify that it is "safe" before access is granted.
Which of the following items is NOT an option as part of the Host Check feature?

A. FortiClient Antivirus software
B. Microsoft Windows Firewall software
C. FortiClient Firewall software
D. Third-party Antivirus software

Answer: B

Question: 180

In the Tunnel Mode widget of the web portal, the administrator has configured an IP Pool and enabled split tunneling.
Which of the following statements is true about the IP address used by the SSL VPN client?

A. The IP pool specified in the SSL-VPN Tunnel Mode Widget Options will override the IP address range defined in the SSL-VPN Settings.
B. Because split tunneling is enabled, no IP address needs to be assigned for the SSL VPN tunnel to be established.
C. The IP address range specified in SSL-VPN Settings will override the IP address range in the SSL-VPN Tunnel Mode Widget Options.

Answer: A

Question: 181

An issue could potentially occur when clicking Connect to start tunnel mode SSL VPN. The tunnel will start up for a few seconds, then shut down.
Which of the following statements best describes how to resolve this issue?

A. This user does not have permission to enable tunnel mode. Make sure that the tunnel mode widget has been added to that user's web portal.
B. This FortiGate unit may have multiple Internet connections. To avoid this problem, use the appropriate CLI command to bind the SSL VPN connection to the original incoming interface.

C. Check the SSL adaptor on the host machine. If necessary, uninstall and reinstall the adaptor from the tunnel mode portal.
D. Make sure that only Internet Explorer is used. All other browsers are unsupported.

Answer: B

Question: 182

You are the administrator in charge of a FortiGate unit which acts as a VPN gateway. You have chosen to use Interface Mode when configuring the VPN tunnel and you want users from either side to be able to initiate new sessions. There is only 1 subnet at either end and the FortiGate unit already has a default route.
Which of the following configuration steps are required to achieve these objectives? (Select all that apply.)

A. Create one firewall policy.
B. Create two firewall policies.
C. Add a route for the remote subnet.
D. Add a route for incoming traffic.
E. Create a phase 1 definition.
F. Create a phase 2 definition.

Answer: B, C, E, F

Question: 183

An administrator configures a VPN and selects the Enable IPSec Interface Mode option in the phase 1 settings.
Which of the following statements are correct regarding the IPSec VPN configuration?

A. To complete the VPN configuration, the administrator must manually create a virtual IPSec interface in Web Config under System > Network.
B. The virtual IPSec interface is automatically created after the phase1 configuration.
C. The IPSec policies must be placed at the top of the list.
D. This VPN cannot be used as part of a hub and spoke topology.
E. Routes were automatically created based on the address objects in the firewall policies.

Answer: B

Question: 184

What advantages are there in using a hub-and-spoke IPSec VPN configuration instead of a fully-meshed set of IPSec tunnels? (Select all that apply.)

A. Using a hub and spoke topology is required to achieve full redundancy.
B. Using a hub and spoke topology simplifies configuration.
C. Using a hub and spoke topology provides stronger encryption.
D. Using a hub and spoke topology reduces the number of tunnels.

Answer: B, D

Question: 185

What advantages are there in using a fully Meshed IPSec VPN configuration instead of a hub and spoke set of IPSec tunnels?

A. Using a hub and spoke topology is required to achieve full redundancy.
B. Using a full mesh topology simplifies configuration.
C. Using a full mesh topology provides stronger encryption.
D. Full mesh topology is the most fault-tolerant configuration.

Answer: D

Question: 186

A network administrator needs to implement dynamic route redundancy between a FortiGate unit located in a remote office and a FortiGate unit located in the central office.
The remote office accesses central resources using IPSec VPN tunnels through two different Internet providers.
What is the best method for allowing the remote office access to the resources through the FortiGate unit used at the central office?

A. Use two or more route-based IPSec VPN tunnels and enable OSPF on the IPSec virtual interfaces.
B. Use two or more policy-based IPSec VPN tunnels and enable OSPF on the IPSec virtual interfaces.
C. Use route-based VPNs on the central office FortiGate unit to advertise routes with a dynamic routing protocol and use a policy-based VPN on the remote office with two or more static default routes.
D. Dynamic routing protocols cannot be used over IPSec VPN tunnels.

Answer: A

Question: 187

A FortiClient fails to establish a VPN tunnel with a FortiGate unit.

The following information is displayed in the FortiGate unit logs:
msg="Initiator: sent 192.168.11.101 main mode message #1 (OK)"
msg="Initiator: sent 192.168.11.101 main mode message #2 (OK)"
msg="Initiator: sent 192.168.11.101 main mode message #3 (OK)"
msg="Initiator: parsed 192.168.11.101 main mode message #3 (DONE)"
msg="Initiator: sent 192.168.11.101 quick mode message #1 (OK)"
msg="Initiator: tunnel 192.168.1.1/192.168.11.101 install ipsec sa"
msg="Initiator: sent 192.168.11.101 quick mode message #2 (DONE)"
msg="Initiator: tunnel 192.168.11.101, transform=ESP_3DES, HMAC_MD5"
msg="Failed to acquire an IP address
Which of the following statements is a possible cause for the failure to establish the VPN tunnel?

A. An IPSec DHCP server is not enabled on the external interface of the FortiGate unit.
B. There is no IPSec firewall policy configured for the policy-based VPN.
C. There is a mismatch between the FortiGate unit and the FortiClient IP addresses in the phase 2 settings.
D. The phase 1 configuration on the FortiGate unit uses Aggressive mode while FortiClient uses Main mode.

Answer: A

Question: 188

An administrator sets up a new FTP server on TCP port 2121. A FortiGate unit is located between the FTP clients and the server. The administrator has created a policy for TCP port 2121.
Users have been complaining that when downloading data they receive a 200 Port command successful message followed by a 425 Cannot build data connection message.
Which of the following statements represents the best solution to this problem?

A. Create a new session helper for the FTP service monitoring port 2121.
B. Enable the ANY service in the firewall policies for both incoming and outgoing traffic.
C. Place the client and server interface in the same zone and enable intra-zone traffic.
D. Disable any protection profiles being applied to FTP traffic.

Answer: A

Question: 189

Which of the following Session TTL values will take precedence?

A. Session TTL specified at the system level for that port number
B. Session TTL specified in the matching firewall policy
C. Session TTL dictated by the application control list associated with the matching firewall policy
D. The default session TTL specified at the system level

Answer: C

Question: 190

Which of the following items is NOT a packet characteristic matched by a firewall service object?

A. ICMP type and code
B. TCP/UDP source and destination ports
C. IP protocol number
D. TCP sequence number

Answer: D

Question: 191

When configuring a server load balanced virtual IP, which of the following is the best distribution algorithm to be used in applications where the same physical destination server must be maintained between sessions?

A. Static
B. Round robin
C. Weighted round robin
D. Least connected

Answer: A

Question: 192

A network administrator connects his PC to the INTERNAL interface on a FortiGate unit. The administrator attempts to make an HTTPS connection to the FortiGate unit on the VLAN1 interface at the IP address of 10.0.1.1, but gets no connectivity.
The following troubleshooting commands are executed from the DOS prompt on the PC and from the CLI.
C:\>ping 10.0.1.1
Pinging 10.0.1.1 with 32 bytes of data:
Reply from 10.0.1.1: bytes=32 time=1ms TTL=255
Reply from 10.0.1.1: bytes=32 time<1ms TTL=255
Reply from 10.0.1.1: bytes=32 time<1ms TTL=255
Reply from 10.0.1.1: bytes=32 time<1ms TTL=255
user1 # get system interface
== [internal]

namE. internal modE. static ip: 10.0.1.254 255.255.255.128 status: up
netbios-forwarD. disable typE. physical mtu-overridE. disable
== [vlan1]
namE. vlan1 modE. static ip: 10.0.1.1 255.255.255.128 status: up netb
ios-forwarD. disable typE. vlan mtu-overridE. disable
user1 # diagnose debug flow trace start 100
user1 # diagnose debug ena
user1 # diagnose debug flow filter daddr 10.0.1.1 10.0.1.1
id=20085 trace_id=274 msg="vd-root received a packet(proto=6, 10.0.1.130:47927->10.0.1.1:443) from internal."
id=20085 trace_id=274 msg="allocate a new session-00000b1b"
id=20085 trace_id=274 msg="find SNAT: IP-10.0.1.1, port-43798"
id=20085 trace_id=274 msg="iprope_in_check() check failed, drop"
Based on the output from these commands, which of the following explanations is a possible cause of the problem?

A. The Fortigate unit has no route back to the PC.
B. The PC has an IP address in the wrong subnet.
C. The PC is using an incorrect default gateway IP address.
D. The FortiGate unit does not have the HTTPS service configured on the VLAN1 interface.
E. There is no firewall policy allowing traffic from INTERNAL-> VLAN1.

Answer: D

Question: 193

A network administrator connects his PC to the INTERNAL interface on a FortiGate unit. The administrator attempts to make an HTTPS connection to the FortiGate unit on the VLAN1 interface at the IP address of 10.0.1.1, but gets no connectivity.
The following troubleshooting commands are executed from the CLI:
user1 # get system interface
== [internal]
namE. internal modE. static ip: 10.0.1.254 255.255.255.128 status: up
netbios-forwarD. disable typE. physical mtu-overridE. disable
== [vlan1]
namE. vlan1 modE. static ip: 10.0.1.1 255.255.255.128 status: up netb
ios-forwarD. disable typE. vlan mtu-overridE. disable
user1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
S 10.0.0.0/8 [10/0] is a summary, Null
C 10.0.1.0/25 is directly connected, vlan1

C 10.0.1.128/25 is directly connected, internal
user1 # diagnose debug flow trace start 100
user1 # diagnose debug ena
user1 # diagnose debug flow filter daddr 10.0.1.1 10.0.1.1
id=20085 trace_id=277 msg="vd-root received a packet(proto=6, 10.0.1.130
:47922->10.0.1.1:443) from internal."
id=20085 trace_id=277 msg="allocate a new session-00000b21"
id=20085 trace_id=277 msg="iprope_in_check() check failed, drop"
Based on the output from these commands, which of the following is a possible cause of the problem?

A. The FortiGate unit has no route back to the PC.
B. The PC has an IP address in the wrong subnet.
C. The PC is using an incorrect default gateway IP address.
D. There is no firewall policy allowing traffic from INTERNAL -> VLAN1.

Answer: D

Question: 194

WAN optimization is configured in Active/Passive mode. When will the remote peer accept an attempt to initiate a tunnel?

A. The attempt will be accepted when the request comes from a known peer and there is a matching WAN optimization passive rule.
B. The attempt will be accepted when there is a matching WAN optimization passive rule.
C. The attempt will be accepted when the request comes from a known peer.
D. The attempt will be accepted when a user on the remote peer accepts the connection request.

Answer: A

Question: 195

Which of the following methods does the FortiGate unit use to determine the availability of a web cache using Web Cache Communication Protocol (WCCP)?

A. The FortiGate unit receives periodic "Here I am" messages from the web cache.
B. The FortiGate unit polls all globally-defined web cache servers at a regular intervals.
C. The FortiGate using uses the health check monitor to verify the availability of a web cache server.
D. The web cache sends an "I see you" message which is captured by the FortiGate unit.

Answer: C

Question: 196

Which of the following must be configured on a FortiGate unit to redirect content requests to remote web cache servers?

A. WCCP must be enabled on the interface facing the Web cache.
B. You must enabled explicit Web-proxy on the incoming interface.
C. WCCP must be enabled as a global setting on the FortiGate unit.
D. WCCP must be enabled on all interfaces on the FortiGate unit through which HTTP traffic is passing.

Answer: A

Question: 197

Which of the following represents the method used on a FortiGate unit running FortiOS version 4.2 to apply traffic shaping to P2P traffic, such as BitTorrent?

A. Apply a Traffic Shaper to a BitTorrent entry in an Application Control List.
B. Enable the Shape option in a Firewall policy with a Service set to BitTorrent.
C. Define a DLP Rule to match against BitTorrent traffic and include the rule in a DLP Sensor with Traffic Shaping enabled.
D. Specify the amount of Rate Limiting to be applied to BitTorrent traffic through the P2P settings of the Firewall Policy Protocol Options.

Answer: A

Question: 198

Which of the following authentication types are supported by FortiGate units? (Select all that apply.)

A. Kerberos
B. LDAP
C. RADIUS
D. Local Users

Answer: B, C, D

Question: 199

Which of the following are valid authentication user group types on a FortiGate unit? (Select all that apply.)

A. Firewall
B. Directory Service
C. Local
D. LDAP
E. PKI

Answer: A, B

Question: 200

Users may require access to a web site that is blocked by a policy. Administrators can give users the ability to override the block.
Which of the following statements regarding overrides are correct? (Select all that apply.)

A. A protection profile may have only one user group defined as an override group.
B. A firewall user group can be used to provide override privileges for FortiGuard Web Filtering.
C. Authentication to allow the override is based on a user's membership in a user group.
D. Overrides can be allowed by the administrator for a specific period of time.

Answer: B, C, D

Question: 201

Users may require access to a web site that is blocked by a policy. Administrators can give users the ability to override the block.
Which of the following statements regarding overrides is NOT correct?

A. A web filter profile may only have one user group defined as an override group.
B. A firewall user group can be used to provide override privileges for FortiGuard Web Filtering.
C. When requesting an override, the matched user must belong to a user group for which the override capabilty has been enabled.
D. Overrides can be allowed by the administrator for a specific period of time.

Answer: A

Question: 202

An administrator has configured a FortiGate unit so that end users must authenticate against the firewall using digital certificates before browsing the Internet.

What must the user have for a successful authentication? (Select all that apply.)

A. An entry in a supported LDAP Directory.
B. A digital certificate issued by any CA server.
C. A valid username and password.
D. A digital certificate issued by the FortiGate unit.
E. Membership in a firewall user group.

Answer: B, E

Question: 203

The FortiGate unit can be configured to allow authentication to a RADIUS server. The RADIUS server can use several different authentication protocols during the authentication process.
Which of the following are valid authentication protocols that can be used when a user authenticates to the RADIUS server? (Select all that apply.)

A. MS-CHAP-V2 (Microsoft Challenge-Handshake Authentication Protocol v2)
B. PAP (Password Authentication Protocol)
C. CHAP (Challenge-Handshake Authentication Protocol)
D. MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol v1)
E. FAP (FortiGate Authentication Protocol)

Answer: A, B, C, D

Question: 204

Which of the following are valid components of the Fortinet Server Authentication Extensions (FSAE)? (Select all that apply.)

A. Domain Local Security Agent.
B. Collector Agent.
C. Active Directory Agent.
D. User Authentication Agent.
E. Domain Controller Agent.

Answer: B, E

Question: 205

A client can create a secure connection to a FortiGate using SSL VPN in web-only mode.
Which one of the following statements is correct regarding the use of web-only mode SSL VPN?

A. Web-only mode supports SSL version 3 only.
B. A Fortinet-supplied plug-in is required on the web client to use web-only mode SSL VPN.
C. Web-only mode requires the user to have a web browser that supports 64-bit cipher length.
D. The JAVA run-time environment must be installed on the client to be able to connect to a web-only mode SSL VPN.

Answer: C

Question: 206

A FortiGate unit can create a secure connection to a client using SSL VPN in tunnel mode.
Which of the following statements are correct regarding the use of tunnel mode SSL VPN? (Select all that apply.)

A. Split tunneling can be enabled when using tunnel mode SSL VPN.
B. Software must be downloaded to the web client to be able to use a tunnel mode SSL VPN.
C. Users attempting to create a tunnel mode SSL VPN connection must be members of a configured user group on the FortiGate unit.
D. Tunnel mode SSL VPN requires the FortiClient software to be installed on the user's computer.
E. The source IP address used by the client for the tunnel mode SSL VPN is assigned by the FortiGate unit.

Answer: A, B, C, E

Question: 207

In an IPSec gateway-to-gateway configuration, two FortiGate units create a VPN tunnel between two separate private networks.
Which of the following configuration steps must be performed on both FortiGate units to support this configuration? (Select all that apply.)

A. Create firewall policies to control traffic between the IP source and destination address.
B. Configure the appropriate user groups on the Fortigate units to allow users access to the IPSec VPN connection.
C. Set the operating mode of the FortiGate unit to IPSec VPN mode.
D. Define the Phase 2 parameters that the FortiGate unit needs to create a VPN tunnel with the remote peer.
E. Define the Phase 1 parameters that the FortiGate unit needs to authenticate the remote peers.

Answer: A, D, E

Question: 208

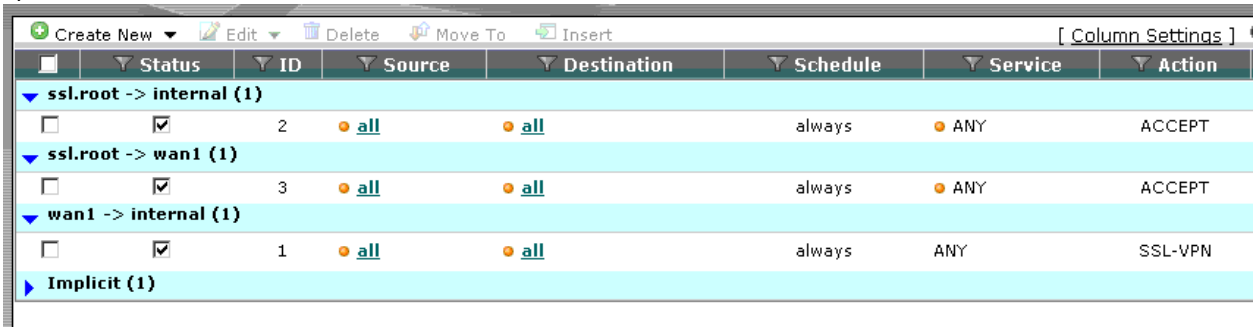
How is traffic routed onto an SSL VPN tunnel from the FortiGate unit side?

A. A static route must be configured by the administrator using the ssl.root interface as the outgoing interface.
B. Assignment of an IP address causes a host route to be added to the FortiGate routing table.
C. A route back to the client is automatically created on the FortiGate to match the SSLVPN IP pool from which the IP address assignment was made.
D. The FortiGate adds a route based upon the destination address in the SSL VPN firewall policy.

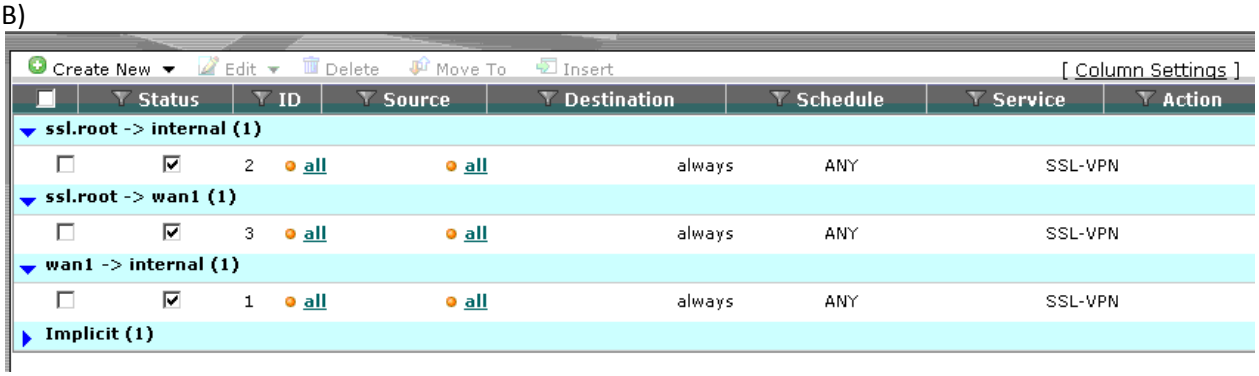
Answer: A

Question: 209

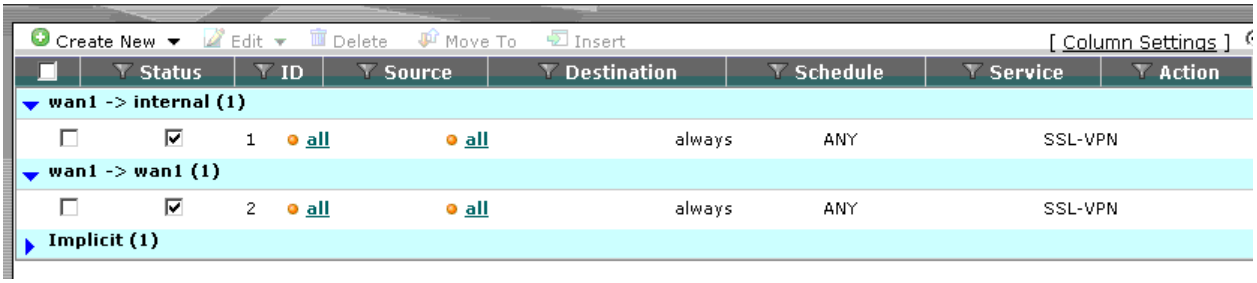
An end user logs into the SSL VPN portal and selects the Tunnel Mode option by clicking on the "Connect" button. The administrator has not enabled split tunneling and so the end user must access the Internet through the SSL VPN Tunnel.
Which firewall policies are needed to allow the end user to not only access the internal network but also reach the Internet?
A)



B)



C)



D)

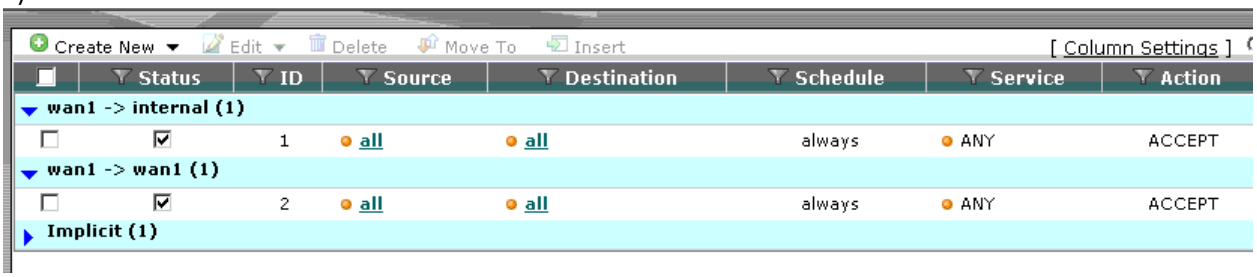


Exhibit A
Exhibit B
Exhibit C
Exhibit D

Answer: A

Question: 210

Which of the following antivirus and attack definition update features are supported by FortiGate units? (Select all that apply.)

A. Manual, user-initiated updates from the FortiGuard Distribution Network.
B. Hourly, daily, or weekly scheduled antivirus and attack definition and antivirus engine updates from the FortiGuard Distribution Network.
C. Push updates from the FortiGuard Distribution Network.
D. Update status including version numbers, expiry dates, and most recent update dates and times.

Answer: A, B, C, D

Question: 211

By default the Intrusion Protection System (IPS) on a FortiGate unit is set to perform which action?

A. Block all network attacks.
B. Block the most common network attacks.
C. Allow all traffic.
D. Allow and log all traffic.

Answer: C

Question: 212

A FortiGate unit can scan for viruses on which types of network traffic? (Select all that apply.)

A. POP3
B. FTP
C. SMTP
D. SNMP
E. NetBios

Answer: A, B, C

Question: 213

Which of the following statements regarding Banned Words are correct? (Select all that apply.)

A. The FortiGate unit can scan web pages and email messages for instances of banned words.
B. When creating a banned word list, an administrator can indicate either specific words or patterns.
C. Banned words can be expressed as wildcards or regular expressions.
D. Content is automatically blocked if a single instance of a banned word appears.
E. The FortiGate unit includes a pre-defined library of common banned words.

Answer: A, B, C

Question: 214

Which statement is correct regarding virus scanning on a FortiGate unit?

A. Virus scanning is enabled by default.
B. Fortinet Customer Support enables virus scanning remotely for you.
C. Virus scanning must be enabled in a protection profile and the protection profile must be assigned to a firewall policy.
D. Enabling virus scanning in a protection profile enables virus scanning for all traffic flowing through the FortiGate.

Answer: C

Question: 215

Which of the following statements are correct regarding URL Filtering on the FortiGate unit? (Select all that apply.)

A. The allowed actions for URL Filtering include Allow, Block and Exempt.
B. The allowed actions for URL Filtering are Allow and Block.
C. The FortiGate unit can filter URLs based on patterns using text and regular expressions.
D. Any URL accessible by a web browser can be blocked using URL Filtering.
E. Multiple URL Filter lists can be added to a single protection profile.

Answer: A, C

Question: 216

Which of the following statements is correct regarding URL Filtering on the FortiGate unit?

A. The available actions for URL Filtering are Allow and Block.
B. Multiple URL Filter lists can be added to a single Web filter profile.
C. A FortiGuard Web Filtering Override match will override a block action in the URL filter list.
D. The available actions for URL Filtering are Allow, Block and Exempt.

Answer: D

Question: 217

Which of the following statements is correct regarding URL Filtering on the FortiGate unit?

A. The FortiGate unit can filter URLs based on patterns using text and regular expressions.
B. The available actions for URL Filtering are Allow and Block.
C. Multiple URL Filter lists can be added to a single Web filter profile.
D. A FortiGuard Web Filtering Override match will override a block action in the URL filter list.

Answer: A

Question: 218

Which of the following Regular Expression patterns will make the term "bad language" case insensitive?

A. [bad language]

B. /bad language/i
C. i/bad language/
D. "bad language"
E. /bad language/c

Answer: B

Question: 219

Which of the following spam filtering methods are supported on the FortiGate unit? (Select all that apply.)

A. IP address check.
B. Open Relay Database List (ORDBL).
C. Black/White list.
D. Return email DNS check.
E. Email checksum check.

Answer: A, B, C, D, E

Question: 220

Which of the following email spam filtering features is not supported on a FortiGate unit?

A. Multipurpose Internet Mail Extensions (MIME) header check
B. HELO DNS lookup
C. Email quarantine
D. Banned word

Answer: C

Question: 221

SSL content inspection is enabled on the FortiGate unit. Which of the following steps is required to prevent a user from being presented with a web browser warning when accessing an SSL-encrypted website?

A. The root certificate of the FortiGate SSL proxy must be imported into the local certificate store on the user's workstation.
B. Disable the strict server certificate check in the web browser under Internet Options.
C. Enable transparent proxy mode on the FortiGate unit.

D. Enable NTLM authentication on the FortiGate unit. NTLM authentication suppresses the certificate warning messages in the web browser.

Answer: A

Question: 222

Which of the following statements describes the method of creating a policy to block access to an FTP site?

A. Enable Web Filter URL blocking and add the URL of the FTP site to the URL Block list.
B. Create a firewall policy with destination address set to the IP address of the FTP site, the Service set to FTP, and the Action set to Deny.
C. Create a firewall policy with a protection profile containing the Block FTP option enabled.
D. None of the above.

Answer: B

Question: 223

UTM features can be applied to which of the following items?

A. Firewall policies
B. User groups
C. Policy routes
D. Address groups

Answer: A

Question: 224

Each UTM feature has configurable UTM objects such as sensors, profiles or lists that define how the feature will function.
How are UTM features applied to traffic?

A. One or more UTM features are enabled in a firewall policy.
B. In the system configuration for that UTM feature, you can identify the policies to which the feature is to be applied.
C. Enable the appropriate UTM objects and identify one of them as the default.
D. For each UTM object, identify which policy will use it.

Answer: A

Question: 225

If no firewall policy is specified between two FortiGate interfaces and zones are not used, which of the following statements describes the action taken on traffic flowing between these interfaces?

A. The traffic is blocked.
B. The traffic is passed.
C. The traffic is passed and logged.
D. The traffic is blocked and logged.

Answer: A

Question: 226

In which order are firewall policies processed on the FortiGate unit?

A. They are processed from the top down as they appear in Web Config.
B. They are processed based on the policy ID number shown in the left hand column of the policy window.
C. They are processed using a policy hierarchy scheme that allows for multiple decision branching.
D. They are processed based on a priority value assigned through the priority column in the policy window.

Answer: A

Question: 227

File blocking rules are applied before which of the following?

A. Firewall policy processing
B. Virus scanning
C. Web URL filtering
D. White/Black list filtering

Answer: B

Question: 228

Which of the following pieces of information can be included in the Destination Address field of a firewall policy?

A. An IP address pool, a virtual IP address, an actual IP address, and an IP address group.
B. A virtual IP address, an actual IP address, and an IP address group.
C. An actual IP address and an IP address group.
D. Only an actual IP address.

Answer: B

Question: 229

The ordering of firewall policies is very important. Policies can be re-ordered within the FortiGate Web Config and also using the CLI. The command used in the CLI to perform this function is _____.

Answer: move

Question: 230

FortiGate units are preconfigured with four default protection profiles. These protection profiles are used to control the type of content inspection to be performed.
What action must be taken for one of these profiles to become active?

A. The protection profile must be assigned to a firewall policy.
B. The "Use Protection Profile" option must be selected in the Web Config tool under the sections for AntiVirus, IPS, WebFilter, and AntiSpam.
C. The protection profile must be set as the Active Protection Profile.
D. All of the above.

Answer: A

Question: 231

A FortiGate 60 unit is configured for your small office. The DMZ interface is connected to a network containing a web server and email server. The Internal interface is connected to a network containing 10 user workstations and the WAN1 interface is connected to your ISP.
You want to configure firewall policies so that your users can send and receive email messages to the email server on the DMZ network. You also want the email server to be able to retrieve email messages from an email server hosted by your ISP using the POP3 protocol.
Which policies must be created for this communication? (Select all that apply.)

A. Internal > DMZ
B. DMZ > Internal
C. Internal > WAN1

D. WAN1 > Internal
E. DMZ > WAN1
F. WAN1 > DMZ

Answer: A, E

Question: 232

The ordering of firewall policies is very important. Policies can be re-ordered within the FortiGate Web Config and also using the CLI. The command used in the CLI to perform this function is _____.

A. set order
B. edit policy
C. reorder
D. move

Answer: D

Question: 233

Which of the following network protocols can be used to access a FortiGate unit as an administrator?

A. HTTPS, HTTP, SSH, TELNET, PING, SNMP
B. FTP, HTTPS, NNTP, TCP, WINS
C. HTTP, NNTP, SMTP, DHCP
D. Telnet, FTP, RLOGIN, HTTP, HTTPS, DDNS
E. Telnet, UDP, NNTP, SMTP

Answer: A

Question: 234

Which of the following statements is correct regarding a FortiGate unit operating in NAT/Route mode?

A. The FortiGate unit requires only a single IP address for receiving updates and configuring from a management computer.
B. The FortiGate unit must use public IP addresses on both the internal and external networks.
C. The FortiGate unit commonly uses private IP addresses on the internal network but hides them using network address translation.
D. The FortiGate unit uses only DHCP-assigned IP addresses on the internal network.

Answer: C

Question: 235

Which of the following statements correctly describes how a FortiGate unit functions in Transparent mode?

A. To manage the FortiGate unit, one of the interfaces must be designated as the management interface. This interface may not be used for forwarding data.
B. An IP address is used to manage the FortiGate unit but this IP address is not associated with a specific interface.
C. The FortiGate unit must use public IP addresses on the internal and external networks.
D. The FortiGate unit uses private IP addresses on the internal network but hides them using address translation.

Answer: B

Question: 236

The Idle Timeout setting on a FortiGate unit applies to which of the following?

A. Web browsing
B. FTP connections
C. User authentication
D. Administrator access
E. Web filtering overrides.

Answer: D

Question: 237

You wish to create a firewall policy that applies only to traffic intended for your web server. The server has an IP address of 192.168.2.2 and belongs to a class C subnet.
When defining the firewall address for use in this policy, which one of the following addressing formats is correct?

A. 192.168.2.0 / 255.255.255.0
B. 192.168.2.2 / 255.255.255.0
C. 192.168.2.0 / 255.255.255.255
D. 192.168.2.2 / 255.255.255.255

Answer: D

Question: 238

If a FortiGate unit has a dmz interface IP address of 210.192.168.2 with a subnet mask of 255.255.255.0, what is a valid dmz DHCP addressing range?

A. 172.168.0.1 - 172.168.0.10
B. 210.192.168.3 - 210.192.168.10
C. 210.192.168.1 - 210.192.168.4
D. All of the above.

Answer: B

Question: 239

A FortiGate unit can act as which of the following? (Select all that apply.)

A. Antispam filter
B. Firewall
C. VPN gateway
D. Mail relay
E. Mail server

Answer: A, B, C

Question: 240

Which of the following components are contained in all FortiGate units from the FG50 models and up? (Select all that apply.)

A. FortiASIC content processor.
B. Hard Drive.
C. Gigabit network interfaces.
D. Serial console port.

Answer: A, D

Question: 241

Which of the following methods can be used to access the CLI? (Select all that apply.)

A. By using a direct connection to a serial console.
B. By using the CLI console window in Web Config.
C. By using an SSH connection.
D. By using a Telnet connection.

Answer: A, B, C, D

Question: 242

The _____CLI command is used on the FortiGate unit to run static commands such as ping or to reset the FortiGate unit to factory defaults.

Answer: execute

Question: 243

The command structure of the FortiGate CLI consists of commands, objects, branches, tables, and parameters.
Which of the following items describes user?

A. A command.
B. An object.
C. A table.
D. A parameter.

Answer: B

Question: 244

The command structure of the CLI on a FortiGate unit consists of commands, objects, branches, tables and parameters.
Which of the following items describes port1?

A. A command.
B. An object.
C. A table.
D. A parameter.

Answer: C

Question: 245

When backing up the configuration file on a FortiGate unit, the contents can be encrypted by enabling the encrypt option and supplying a password.
If the password is forgotten, the configuration file can still be restored using which of the following methods?

A. Selecting the recover password option during the restore process.
B. Having the password emailed to the administrative user by selecting the Forgot Password option.
C. Sending the configuration file to Fortinet support for decryption.
D. If the password is forgotten, there is no way to use the file.

Answer: D

Question: 246

When creating administrative users, the assigned _____determines user rights on the FortiGate unit.

Answer: access profile

Question: 247

Each UTM feature has configurable UTM objects such as sensors, profiles or lists that define how the feature will function.
An administrator must assign a set of UTM features to a group of users.
Which of the following is the correct method for doing this?

A. Enable a set of unique UTM features under "Edit User Group".
B. The administrator must enable the UTM features in an identify-based policy applicable to the user group.
C. When defining the UTM objects, the administrator must list the user groups which will use the UTM object.
D. The administrator must apply the UTM features directly to a user object.

Answer: B

Question: 248

Which of the following items represent the minimum configuration steps an administrator must perform to enable Data Leak Prevention for traffic flowing through the FortiGate unit? (Select all that apply.)

A. Assign a DLP sensor in a firewall policy.
B. Apply one or more DLP rules to a firewall policy.
C. Enable DLP globally using the config sys dlp command in the CLI.
D. Define one or more DLP rules.
E. Define a DLP sensor.
F. Apply a DLP sensor to a DoS sensor policy.

Answer: A, D, E

Question: 249

Because changing the operational mode to Transparent resets device (or vdom) to all defaults, which precautions should an Administrator take prior to performing this? (Select all that apply.)

A. Backup the configuration.
B. Disconnect redundant cables to ensure the topology will not contain layer 2 loops.
C. Set the unit to factory defaults.
D. Update IPS and AV files.

Answer: A, B

Question: 250

Which of the following is true regarding Switch Port Mode?

A. Allows all internal ports to share the same subnet.
B. Provides separate routable interfaces for each internal port.
C. An administrator can select ports to be used as a switch.
D. Configures ports to be part of the same broadcast domain.

Answer: A

Question: 251

What is the FortiGate unit password recovery process?

A. Interupt boot sequence, modify the boot registry and reboot. After changing the password, reset the boot registry.
B. Log in through the console port using the maintainer account within several minutes of a reboot.
C. Hold CTRL + break during reboot and reset the admin password.
D. The only way to regain access is to interrupt boot sequence and restore a configuration file for which the password has been modified.

Answer: B

Question: 252

The FortiGate Web Config provides a link to update the firmware in the System > Status window. Clicking this link will perform which of the following actions?

A. It will connect to the Fortinet support site where the appropriate firmware version can be selected.
B. It will send a request to the FortiGuard Distribution Network so that the appropriate firmware version can be pushed down to the FortiGate unit.
C. It will present a prompt to allow browsing to the location of the firmware file.
D. It will automatically connect to the Fortinet support site to download the most recent firmware version for the FortiGate unit.

Answer: C

Question: 253

Which of the following statements correctly describes how a push update from the FortiGuard Distribution Network (FDN) works?

A. The FDN sends push updates only once.
B. The FDN sends package updates automatically to the FortiGate unit without requiring an update request.
C. The FDN continues to send push updates until the FortiGate unit sends an acknowledgement.
D. The FDN sends a message to the FortiGate unit that there is an update available and that the FortiGate unit should download the update.

Answer: D

Question: 254

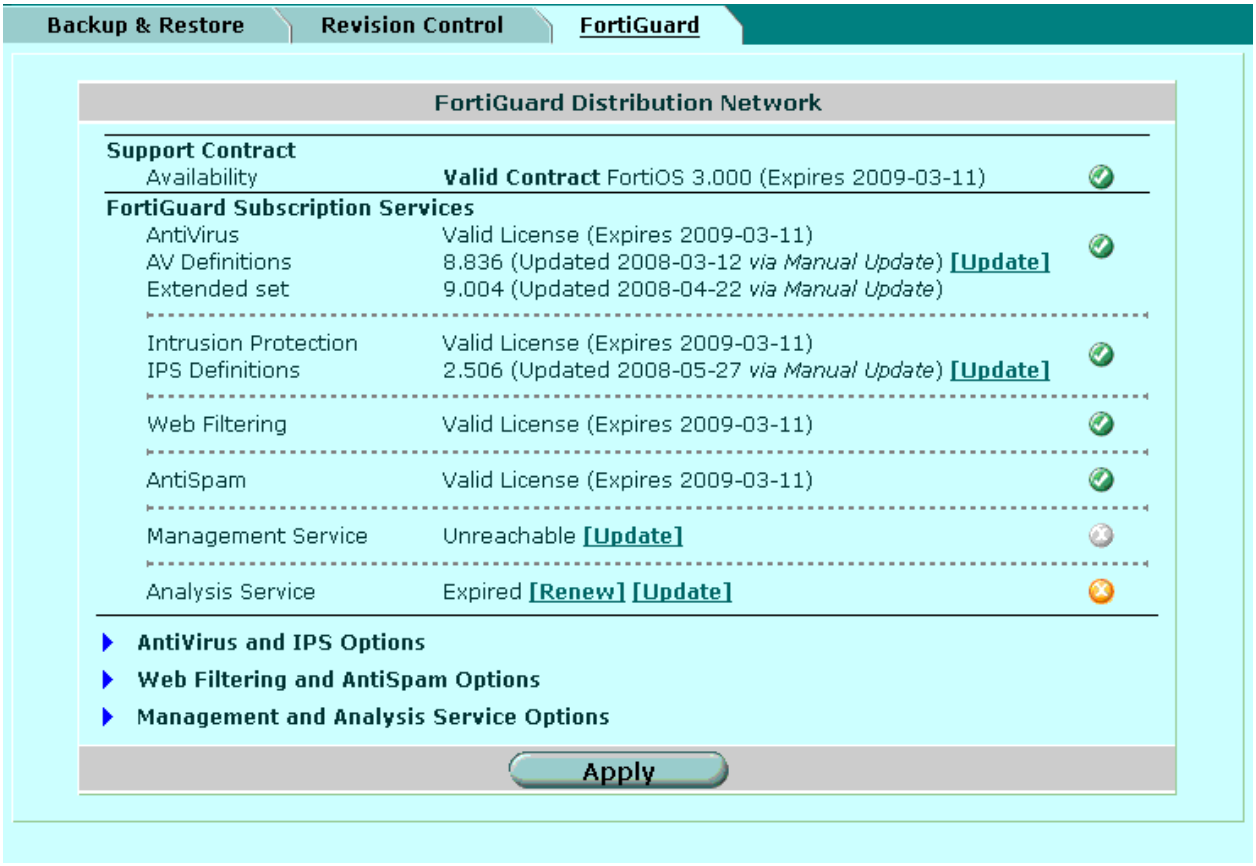
Which of the following options can you use to update the virus definitions on a FortiGate unit? (Select all that apply.)

A. Push update
B. Scheduled update
C. Manual update
D. FTP update

Answer: A, B, C

Question: 255

Which of the following statements best describes the green status indicators that appear next to different FortiGuard Distribution Network services as illustrated in the exhibit?



A. They indicate that the FortiGate unit is able to connect to the FortiGuard Distribution Network.
B. They indicate that the FortiGate unit has the latest updates that are available from the FortiGuard Distribution Network.
C. They indicate that updates are available and should be downloaded from the FortiGuard Distribution Network to the FortiGate unit.
D. They indicate that the FortiGate unit is in the process of downloading updates from the FortiGuard Distribution Network.

Answer: A

Question: 256

A FortiGate 100 unit is configured to receive push updates from the FortiGuard Distribution Network, however, updates are not being received.
Which of the following statements are possible reasons for this? (Select all that apply.)

A. The external facing interface of the FortiGate unit is configured to use DHCP.
B. The FortiGate unit has not been registered.
C. There is a NAT device between the FortiGate unit and the FortiGuard Distribution Network.
D. The FortiGate unit is in Transparent mode.

Answer: A, B, C

Question: 257

In addition to AntiVirus services, the FortiGuard Subscription Services provide IPS, Web Filtering, and _____ services.

Answer: antispam

Question: 258

Caching improves performance by reducing FortiGate unit requests to the FortiGuard server.
Which of the following statements are correct regarding the caching of FortiGuard responses? (Select all that apply.)

A. Caching is available for web filtering, antispam, and IPS requests.
B. The cache uses a small portion of the FortiGate system memory.
C. When the cache is full, the least recently used IP address or URL is deleted from the cache.
D. An administrator can configure the number of seconds to store information in the cache before the FortiGate unit contacts the FortiGuard server again.
E. The size of the cache will increase to accomodate any number of cached queries.

Answer: B, C, D

Question: 259

Which of the following products is designed to manage multiple FortiGate devices?

A. FortiGate
B. FortiAnalyzer
C. FortiClient
D. FortiManager
E. FortiMail
F. FortiBridge

Answer: D

Question: 260

Which of the following products provides dedicated hardware to analyze log data from multiple FortiGate devices?

A. FortiGate
B. FortiAnalyzer
C. FortiClient
D. FortiManager
E. FortiMail
F. FortiBridge

Answer: B

Question: 261

Which of the following products can be installed on a computer running Windows XP to provide personal firewall protection, antivirus protection, web and mail filtering, spam filtering, and VPN functionality?

A. FortiGate
B. FortiAnalyzer
C. FortiClient
D. FortiManager
E. FortiReporter

Answer: C

Question: 262

A FortiAnalyzer device could use which security method to secure the transfer of log data from FortiGate devices?

A. SSL
B. IPSec
C. direct serial connection
D. S/MIME

Answer: B

Question: 263

Which of the following Fortinet products can receive updates from the FortiGuard Distribution Network? (Select all that apply.)

A. FortiGate
B. FortiClient
C. FortiMail
D. FortiAnalyzer

Answer: A, B, C

Question: 264

Which Fortinet products & features could be considered part of a comprehensive solution to monitor and prevent the leakage of senstive data? (Select all that apply.)

A. Archive non-compliant outgoing e-mails using FortiMail.
B. Restrict unofficial methods of transferring files such as P2P using Application Control lists on a FortiGate.
C. Monitor database activity using FortiAnalyzer.
D. Apply a DLP sensor to a firewall policy.
E. Configure FortiClient to prevent files flagged as sensitive from being copied to a USB disk.

Answer: A, B, D

Question: 265

Which of the following logging options are supported on a FortiGate unit? (Select all that apply.)

A. LDAP
B. Syslog
C. FortiAnalyzer
D. Local

Answer: B, C, D

Question: 266

Which of the following statements are correct regarding logging to memory on a FortiGate unit? (Select all that apply.)

A. When the system has reached its capacity for log messages, the FortiGate unit will stop logging to memory.
B. When the system has reached its capacity for log messages, the FortiGate unit overwrites the oldest messages.
C. If the FortiGate unit is reset or loses power, log entries captured to memory will be lost.
D. None of the above.

Answer: B, C

Question: 267

An administrator configures a FortiGate unit in Transparent mode on the 192.168.11.0 subnet. Automatic Discovery is enabled to detect any available FortiAnalyzers on the network.
Which of the following FortiAnalyzers will be detected? (Select all that apply.)

A. 192.168.11.100
B. 192.168.11.251
C. 192.168.10.100
D. 192.168.10.251

Answer: A, B

Question: 268

Which of the following items does NOT support the Logging feature?

A. File Filter
B. Application control
C. Session timeouts
D. Administrator activities
E. Web URL filtering

Answer: C

Question: 269

DLP archiving gives the ability to store session transaction data on a FortiAnalyzer unit for which of the following types of network traffic? (Select all that apply.)

A. SNMP
B. IPSec
C. SMTP
D. POP3
E. HTTP

Answer: C, D, E

Question: 270

Alert emails enable the FortiGate unit to send email notifications to an email address upon detection of a pre-defined event type.
Which of the following are some of the available event types in Web Config? (Select all that apply.)

A. Intrusion detected.
B. Successful firewall authentication.
C. Oversized file detected.
D. DHCP address assigned.
E. FortiGuard Web Filtering rating error detected.

Answer: A

Question: 271

Which network protocols are supported for administrative access to a FortiGate unit? (Choose three.)

A. SNMP
B. WINS
C. HTTP
D. Telnet
E. SSH

Answer: C, D, E

Question: 272

What capabilities can a FortiGate provide? (Choose three.)

A. Mail relay.
B. Email filtering.
C. Firewall.
D. VPN gateway.
E. Mail server.

Answer: B, C, D

Question: 273

Which of the following must be configured on a FortiGate unit to redirect content requests to remote web cache servers?

A. WCCP must be enabled on the interface facing the Web cache.
B. You must enabled explicit Web-proxy on the incoming interface.
C. WCCP must be enabled as a global setting on the FortiGate unit.
D. WCCP must be enabled on all interfaces on the FortiGate unit through which HTTP traffic is passing.

Answer: A

www.certifyguide.com

Thanks for Using Our Product

We Accept PayPal™