NSE4.examcollection.premium.exam.301q

Number: NSE4
Passing Score: 800
Time Limit: 120 min
File Version: 8.0

ExamCollection
free practice exam collection

NSE4

Fortinet Network Security Expert 4

Version 8.0

Exam A

QUESTION 1
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://kb.fortinet.com/kb/documentLink.do?externalID=FD36492

QUESTION 2
Which statements are correct regarding URL filtering on a FortiGate unit? (Choose two.)

A. The allowed actions for URL filtering include allow, block, monitor and exempt.
B. The allow actions for URL filtering and Allow and Block only.
C. URL filters may be based on patterns using simple text, wildcards and regular expressions.
D. URL filters are based on simple text only and require an exact match.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Examine the following log message for IPS:

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"

Which statement is correct about the above log? (Choose two.)

A. The target is 192.168.3.168.
B. The target is 192.168.3.170.
C. The attack was NOT blocked.
D. The attack was blocked.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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. Third-party network applications cannot send IP traffic through the tunnel.
E. An SSL VPN IP address is dynamically assigned to the client by the FortiGate unit.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/1952/fortigate-sslvpn.pdf page 10

QUESTION 5
Examine the output below from the `diagnose sys top` command:

```
# diagnose sys top 1
Run time: 11 days, 3 hours and 29 minutes
OU,   ON,   1S,   99I;   971T,  528F,  160 KF
sshd          123          S      1.9     1.2
ipsendjine    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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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?

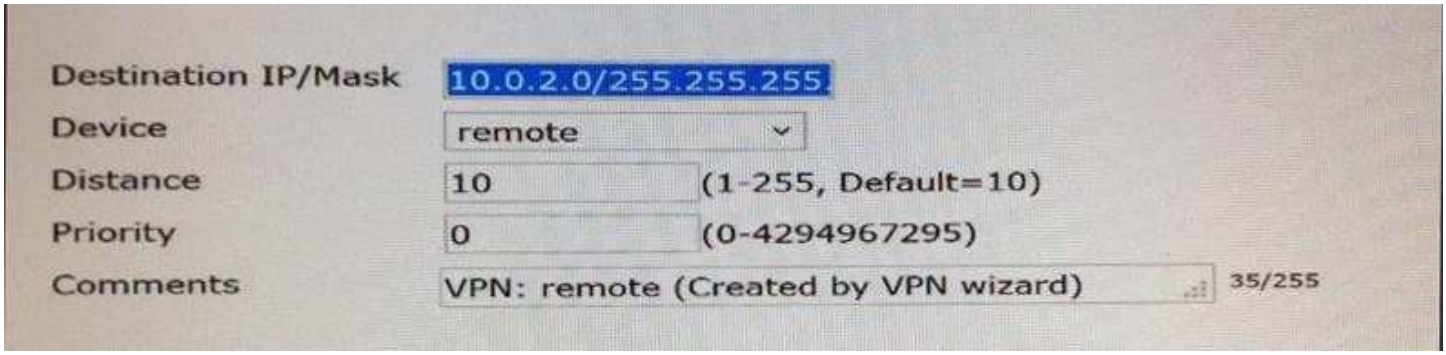
A. The administrator does not have the proper permissions the dmz interface.
B. The dmz interface is referenced in the configuration of another VDOM.
C. Non-management VDOMs cannot reference physical interfaces

D. The dmz interface is in PPPoE or DHCP mode.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Review the static route configuration for IPsec shown in the exhibit; then answer the question below.



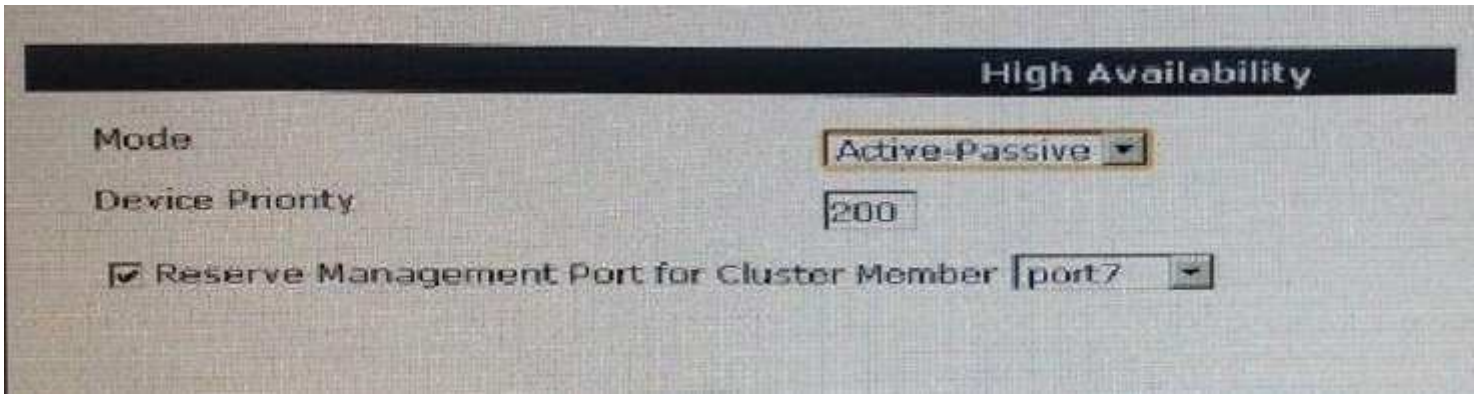
Which statements are correct regarding this configuration? (Choose two.)

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.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
In HA, the option Reserve Management Port for Cluster Member is selected as shown in the exhibit below.



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

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. When connecting to port7 you always connect to the master device.
D. A gateway address may be configured for port7.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/1881/fortigate-ipsecvpn-52.pdf page 23

QUESTION 10
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.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which statements are true regarding traffic shaping that is applied in an application sensor, and associated with the 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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
What are valid options for handling DNS requests sent directly to a FortiGate's interface IP? (Choose three.)

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

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, they are not being received.
Which is one reason for this problem?

A. The FortiGate is connected to multiple ISPs.
B. FortiGuard scheduled updates are enabled in the FortiGate configuration.
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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 in 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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
What methods can be used to access the FortiGate CLI? (Choose two.)

A. Using SNMP.
B. A direct connection to the serial console port.
C. Using the CLI console widget in the GUI.
D. Using RCP.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
When firewall policy authentication is enabled, which protocols can trigger an authentication challenge? (Choose two.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/1063/fortigate-authentication-40-mr2.pdf page 48

QUESTION 17
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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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. Phase 2 must have an encryption algorithm supported by the NP6.
D. IPsec traffic must not be inspected by any FortiGate session helper.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
With FSSO DC-agent mode, 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 a domain controller running only the domain controller agent, which statements are correct? (Choose two.)

A. The login event is sent to a collector agent by the DC agent.
B. the login event is sent to the FortiGate by the DC agent.
C. The domain collector agent may perform a DNS lookup for the authenticated client's IP address.
D. The user cannot be authenticated with the FortiGate in this manner because each domain controller agent requires a dedicated collector agent.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22

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

A. It support 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 suppports 64-bit cipher length.
D. The JAVA run-time environment must be installed on the client.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR1/Fortigate-SSLVPN's_FortiOS_Handbook_4.0_MR1.pdf page 18

QUESTION 23
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=sta
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 replayt
  life: type=01 bytes=0/0 timeout=1791/1800
  dec: spi=a29046e9 esp=3des key=24 0525830c6fd67ca37e9d6dad174d175e24f9
       ah=sha1 key=20 982f8ba194f3f797773efc605c8321b728dabf1d
  enc: spi=19be4052 esp=3des key=24 da597cb7fec913528f8598d1aa7ecd17156a
       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.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

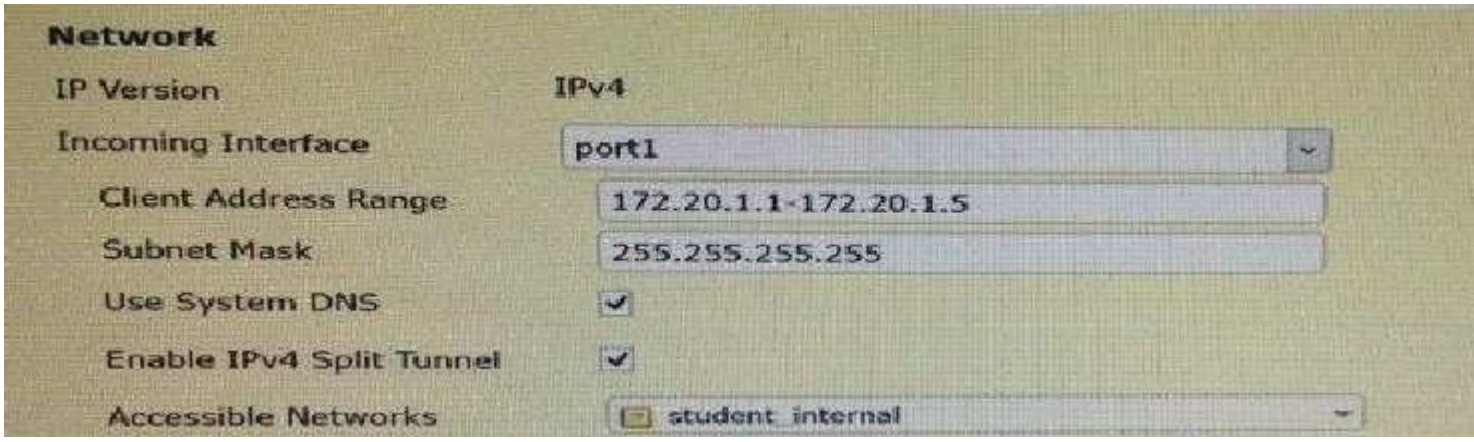
QUESTION 24
If there are no changes in the routing table and in the case of TCP traffic, which of the following correctly describes the routing table lookups performed by a FortiGate in NAT /Route mode, when searching for a suitable gateway?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which IPSec mode includes the *peer id* information in the first packet?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
A FortiGate is operating in NAT/Route mode and configured with two virtual LAN (VLAN) sub-interfaces added to the same physical interface.
Which one 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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 are listing of all connected FSSO collector agents.
D. Lists all DC Agents installed on all domain controllers.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

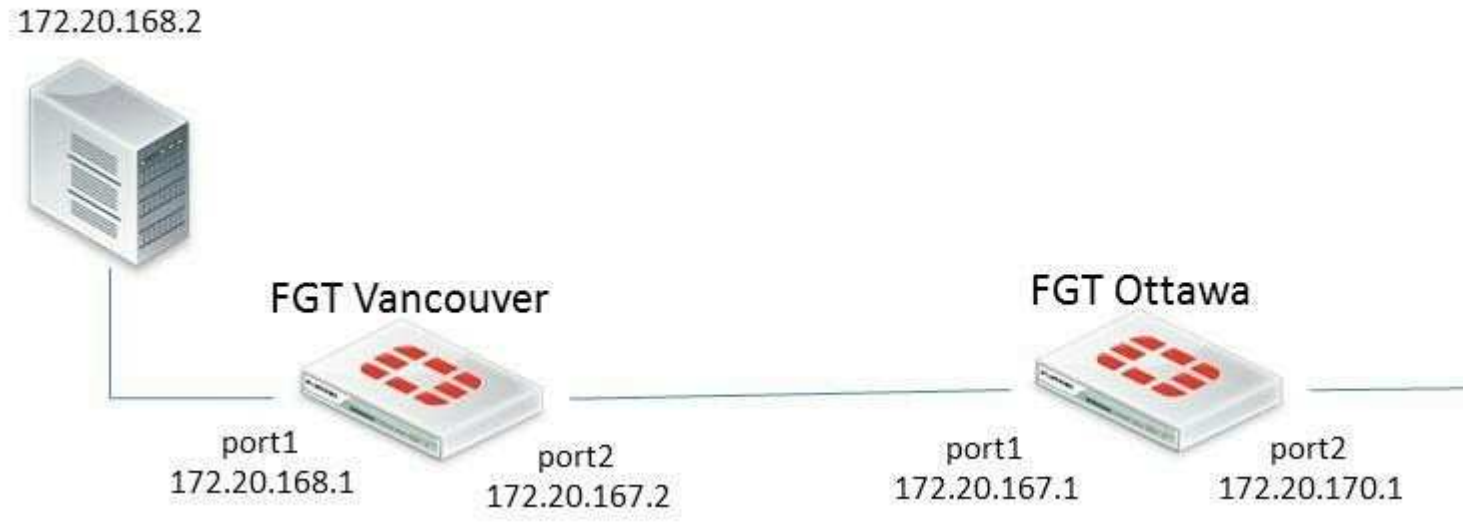
QUESTION 31
You are the administrator in charge of a point-to-point IPsec VPN between two FortiGate units using route based mode. Users from either side must be able to initiate new sessions with no restrictions. There is only 1 subnet at either end and the FortiGate already has a default route.
Which two configuration steps are required in each FortiGate 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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Examine the exhibit 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 170.20.168.2 to the destination IP address 172.20.169.2 are being dropped by the FortiGate located in Ottawa. Which of the following correctly describes the cause for the dropped packets?

A. The forward policy check.
B. The reserve path forwarding check.
C. The subnet 172.20.169.0/24 is NOT in the Ottawa FortiGate'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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
In which order are firewall policies processed on a FortiGate unit?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
What logging options are supported on a FortiGate unit? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
What is 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
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. FortiGuard pull updates.
C. Push updates from a FortiAnalyzer.
D. execute fortiguard-AV-AS command from the CLI.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
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? (Choose three.)

A. POP3
B. SNMP
C. IPsec
D. SMTP

E. HTTP

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which statements correctly describe transparent mode operation? (Choose three.)

A. The FortiGate acts as transparent bridge and forwards traffic at Layer-2.
B. Ethernet packets are forwarded based on destination MAC addresses, NOT IP addresses.
C. The transparent FortiGate ia clearly visible to network hosts in an IP trace route.
D. Permits inline traffic inspection and firewalling without changing the IP scheme of the network.
E. All interfaces of the transparent mode FortiGate device most be on different IP subnets.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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 offloaded to the NP6 in the master unit.
B. They are not offloaded to the NP6 in the master unit.
C. They are offloaded to the NP6 in the slave unit.
D. They are not offloaded to the NP6 in the slave unit.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

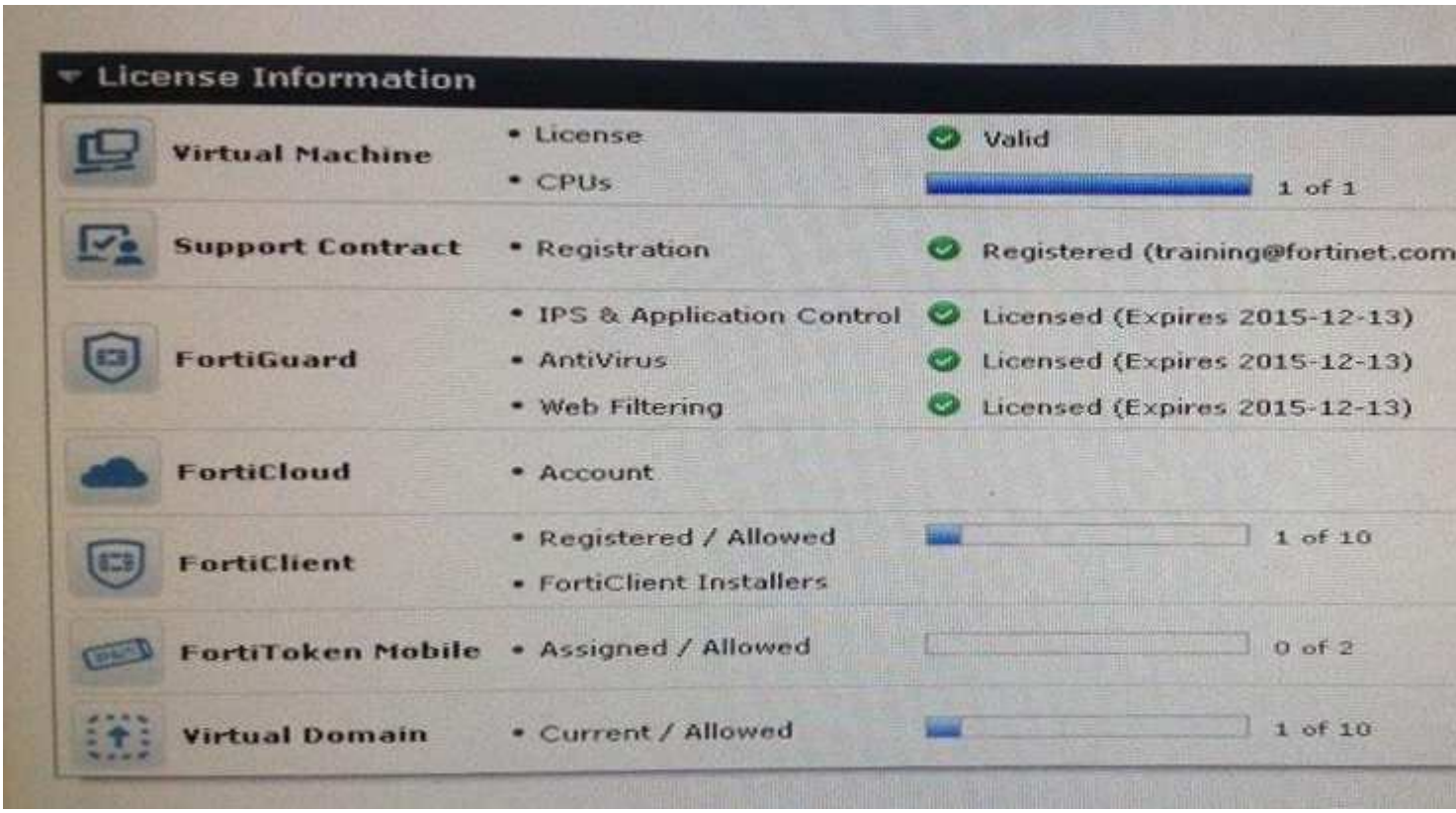
QUESTION 40
Which two methods are supported by the web proxy auto-discovery protocol (WPAD) to automatically learn the URL where a PAC file is located? (Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
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 FortyGate is able to connect to the FortiGuard Distribution Network.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
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
```

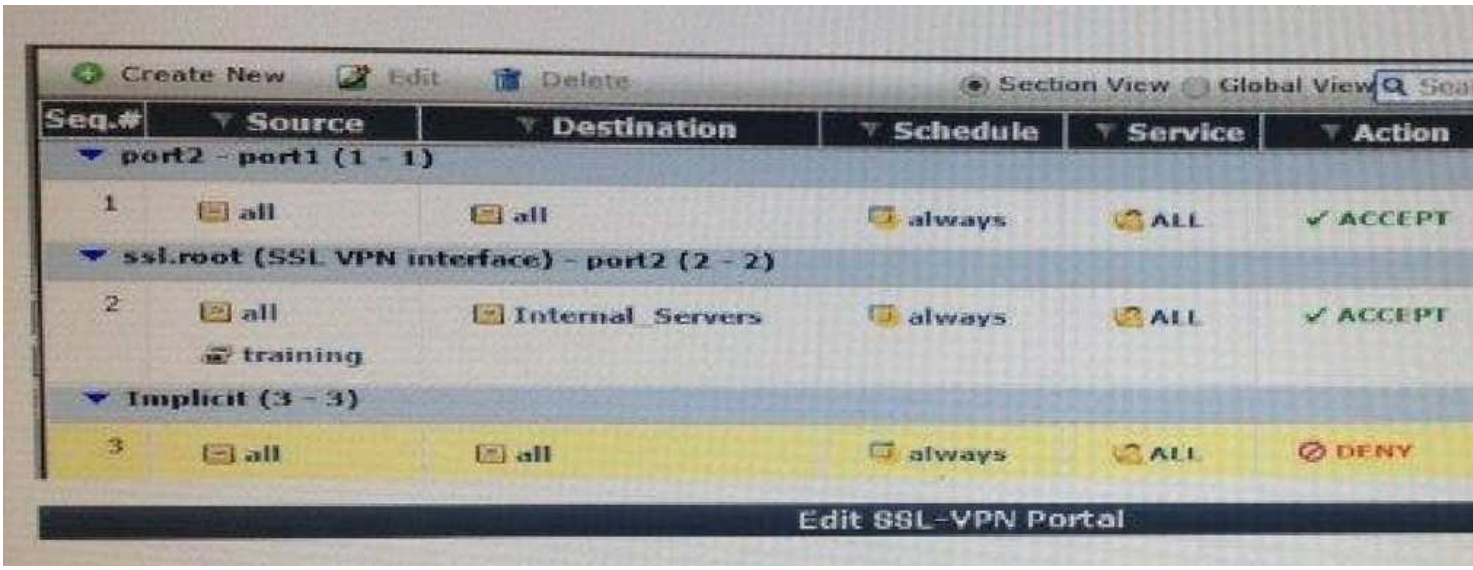
Which of the following statements correctly describes the static routing configuration provided? (Choose two.)

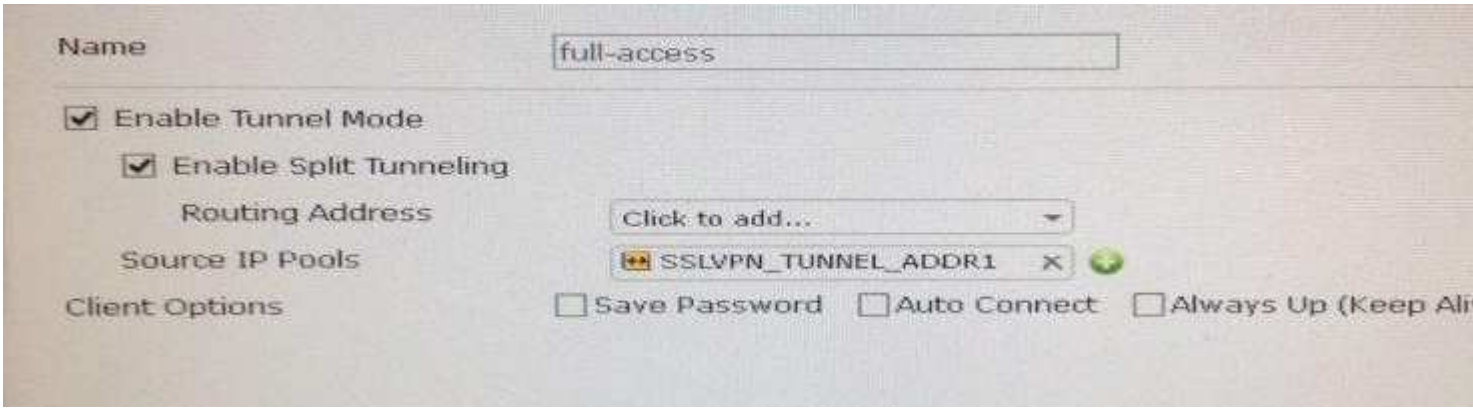
A. All traffic to 172.20.1.0/24 is dropped by the FortiGate.
B. As long as port1 is up, all traffic to 172.20.1.0/24 is routed by the static route number 1. if the interface port1 is down, the traffic is routed using the blackhole route.
C. The FortiGate unit does NOT create a session entry in the session table when the traffic is being routed by the blackhole route.
D. The FortiGate unit creates a session entry in the session table when the traffic is being routed by the blackhole route.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A user logs into a SSL VPN portal and activates the tunnel mode. The exhibit shows the firewall policy and the user's SSL VPN portal 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
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 are required for this static default route to be displayed in the FortiGate unit's routing table? (Choose two.)

A. The administrative status of the wan1 interface is displayed as down.
B. The link status of the wan1 interface is displayed as up.
C. All other default routers should have a lower distance.
D. The wan1 interface address and gateway address are on the same subnet.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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 slave unit?

A. Client - > slave FortiGate - > master FortiGate - > web server.
B. Client - > slave FortiGate - > web server.
C. Client - > master FortiGate - > slave FortiGate - > master FortiGate - >web server.
D. Client - > master FortiGate - >slave FortiGate - > web server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
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 DC-agent mode is used? (Choose two.)

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 receive user logon information from the domain controller agent and will send it to the FortiGate unit.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
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.

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which network protocols are supported for administrative access to a FortiGate unit? (Choose three.)

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

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
What is the FortiGate password recovery process?

A. Interrupt 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 seconds of physically power cycling the FortiGate.
C. Hold down the CTRL + Esc (Escape) keys during reboot, then reset the admin password.
D. Interrupt the boot sequence and restore a configuration file for which the password has been modified.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which two web filtering inspection modes inspect the full URL? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Which of the following statements are correct about the HA command `diagnose sys ha reset-`uptime? (Choose two.)

A. The device this command is executed on is likely to switch from master to slave status if `override` is disabled.
B. The device this command executed on is likely to switch from master to slave status if override is enabled.

C. The command has no impact on the HA algorithm.
D. This commands resets the uptime variable used in the HA algorithm so it may cause a new master to become elected.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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 location may be reachable via a hub location.
D. It cannot contain redundant VPN tunnels.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
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 affect when the sensor is applied to a policy.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Two devices are in an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of `diagnose sys session stat` for the STUDENT device. Exhibit B shows the command output of `diagnose sys session stat` for the REMOTE device.

Exhibit A:

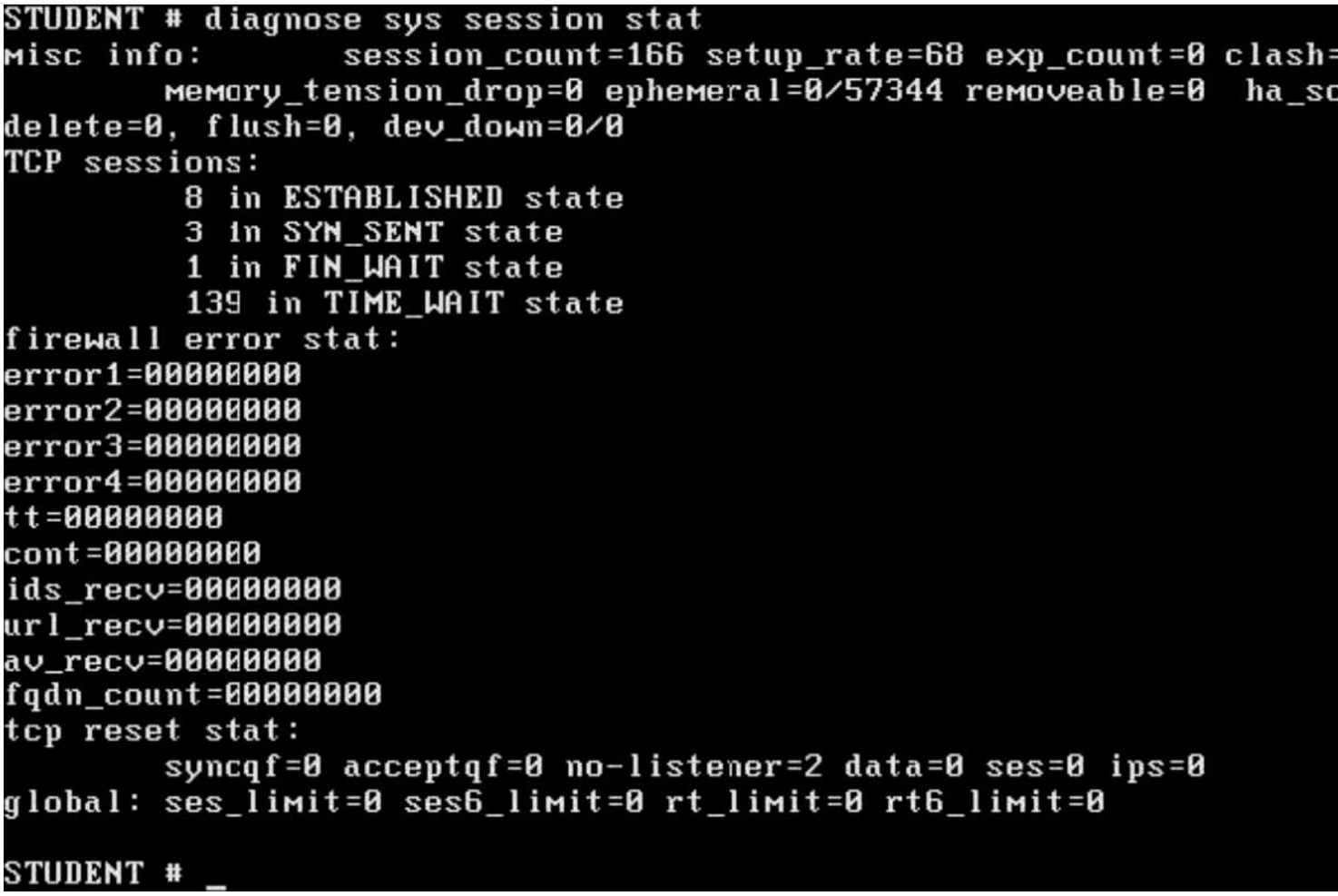


Exhibit B:

```
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
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? (Choose two.)

A. STUDENT is likely to be the master device.
B. Session-pickup is likely to be enabled.
C. The cluster mode is active-passive.
D. There is not enough information to determine the cluster mode.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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.

Correct Answer: BC
Section: (none)

Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/2712/fortigate-ipv6-54.pdf

QUESTION 61
Which is not a FortiGate feature?

A. Database auditing
B. Intrusion prevention
C. Web filtering
D. Application control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
When an administrator attempts to manage FortiGate from an IP address that is not a trusted host, what happens?

A. FortiGate will still subject that person's traffic to firewall policies; it will not bypass them.
B. FortiGate will drop the packets and not respond.
C. FortiGate responds with a block message, indicating that it will not allow that person to log in.
D. FortiGate responds only if the administrator uses a secure protocol. Otherwise, it does not respond

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
A backup file begins with this line:

#config-version=FGVM64-5.02-FW-build589-140613:opmode=0:vdom=0:user=admin
#conf_file_ver=3881503152630288414 #buildno=0589 #global_vdom=1

Can you restore it to a FortiWiFi 60D?

A. Yes
B. Yes, but only if you replace the "#conf_file_ver" line so that it contains the serial number of that specific FortiWiFi 60D.
C. Yes, but only if it is running the same version of FortiOS, or a newer compatible version.
D. No

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Acme Web Hosting is replacing one of their firewalls with a FortiGate. It must be able to apply port forwarding to their back-end web servers while blocking virus uploads and TCP SYN floods from attackers. Which operation mode is the best choice for these requirements?

A. NAT/route
B. NAT mode with an interface in one-arm sniffer mode
C. Transparent mode
D. No appropriate operation mode exists

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
You have configured the DHCP server on a FortiGate's port1 interface (or internal, depending on the model) to offer IPs in a range of 192.168.1.65-192.168.1.253.

When the first host sends a DHCP request, what IP will the DHCP offer?

A. 192.168.1.99
B. 192.168.1.253
C. 192.168.1.65
D. 192.168.1.66

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
You have created a new administrator account, and assign it the prof_admin profile. Which is false about that account's permissions?

A. It cannot upgrade or downgrade firmware.
B. It can create and assign administrator accounts to parts of its own VDOM.
C. It can reset forgotten passwords for other administrator accounts such as "admin".
D. It has a smaller permissions scope than accounts with the "super_admin" profile.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can select **prof_admin**, a special access profile used by the admin administrator account. However, selecting this access profile will **not** confer all of the same permissions of the admin administrator. For example, the new administrator would not be able to reset lost administrator passwords.
Reference: http://help.fortinet.com/fweb/550/Content/FortiWeb/fortiweb-admin/administrators.htm

QUESTION 67
Which UTM feature sends a UDP query to FortiGuard servers each time FortiGate scans a packet (unless the response is locally cached)?

A. Antivirus
B. VPN
C. IPS
D. Web Filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A new version of FortiOS firmware has just been released. When you upload new firmware, which is true?

A. If you upload the firmware image via the boot loader's menu from a TFTP server, it will not preserve the configuration. But if you upload new firmware via the GUI or CLI, as long as you are following a supported upgrade path, FortiOS will attempt to convert the existing configuration to be valid with any new or changed syntax.
B. No settings are preserved. You must completely reconfigure.
C. No settings are preserved. After the upgrade, you must upload a configuration backup file. FortiOS will ignore any commands that are not valid in the new OS. In those cases, you must reconfigure settings that are not compatible with the new firmware.
D. You must use FortiConverter to convert a backup configuration file into the syntax required by the new FortiOS, then upload it to FortiGate.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which protocols can you use for secure administrative access to a FortiGate? (Choose two)

A. SSH
B. Telnet
C. NTLM
D. HTTPS

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
If you have lost your password for the "admin" account on your FortiGate, how should you reset it?

A. Log in with another administrator account that has "super_admin" profile permissions, then reset the

password for the "admin" account.

B. Reboot the FortiGate. Via the local console, during the boot loader, use the menu to format the flash disk and reinstall the firmware. Then you can log in with the default password.
C. Power off the FortiGate. After several seconds, restart it. Via the local console, within 30 seconds after booting has completed, log in as "maintainer" and enter the CLI commands to set the password for the "admin" account.
D. Reboot the FortiGate. Via the local console, during the boot loader, use the menu to log in as "maintainer" and enter the CLI commands to set the password for the "admin" account.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
What are the ways FortiGate can monitor logs? (Choose three.)

A. MIB
B. SMS
C. Alert Emails
D. SNMP
E. FortiAnalyzer
F. Alert Message Console

Correct Answer: CDF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
To which remote device can the FortiGate send logs? (Choose three.)

A. Syslog
B. FortiAnalyzer
C. Hard drive
D. Memory
E. FortiCloud

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
In a Crash log, what does a status of 0 indicate?

A. Abnormal termination of a process
B. A process closed for any reason
C. Scanunitd process crashed

D. Normal shutdown with no abnormalities
E. DHCP process crashed

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
There are eight (8) log severity levels that indicate the importance of an event. Not including Debug, which is only needed to log diagnostic data, what are both the lowest AND highest severity levels?

A. Notification, Emergency
B. Information, Critical
C. Error, Critical
D. Information, Emergency
E. Information, Alert

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Examine this log entry.

What does the log indicate? (Choose three.)

date=2013-12-04 time=09:30:18 logid=0100032001 type=event subtype=system level=information vd="root" user="admin" ui=http(192.168.1.112) action=login status=success reason=none profile="super_admin" msg="Administrator admin logged in successfully from http(192.168.1.112)"

A. In the GUI, the log entry was located under “Log & Report > Event Log > User”.
B. In the GUI, the log entry was located under “Log & Report > Event Log > System”.
C. In the GUI, the log entry was located under “Log & Report > Traffic Log > Local Traffic”.
D. The connection was encrypted.
E. The connection was unencrypted.
F. The IP of the FortiGate interface that “admin” connected to was 192.168.1.112.
G. The IP of the computer that “admin” connected from was 192.168.1.112.

Correct Answer: BEG
Section: (none)
Explanation

Explanation/Reference:

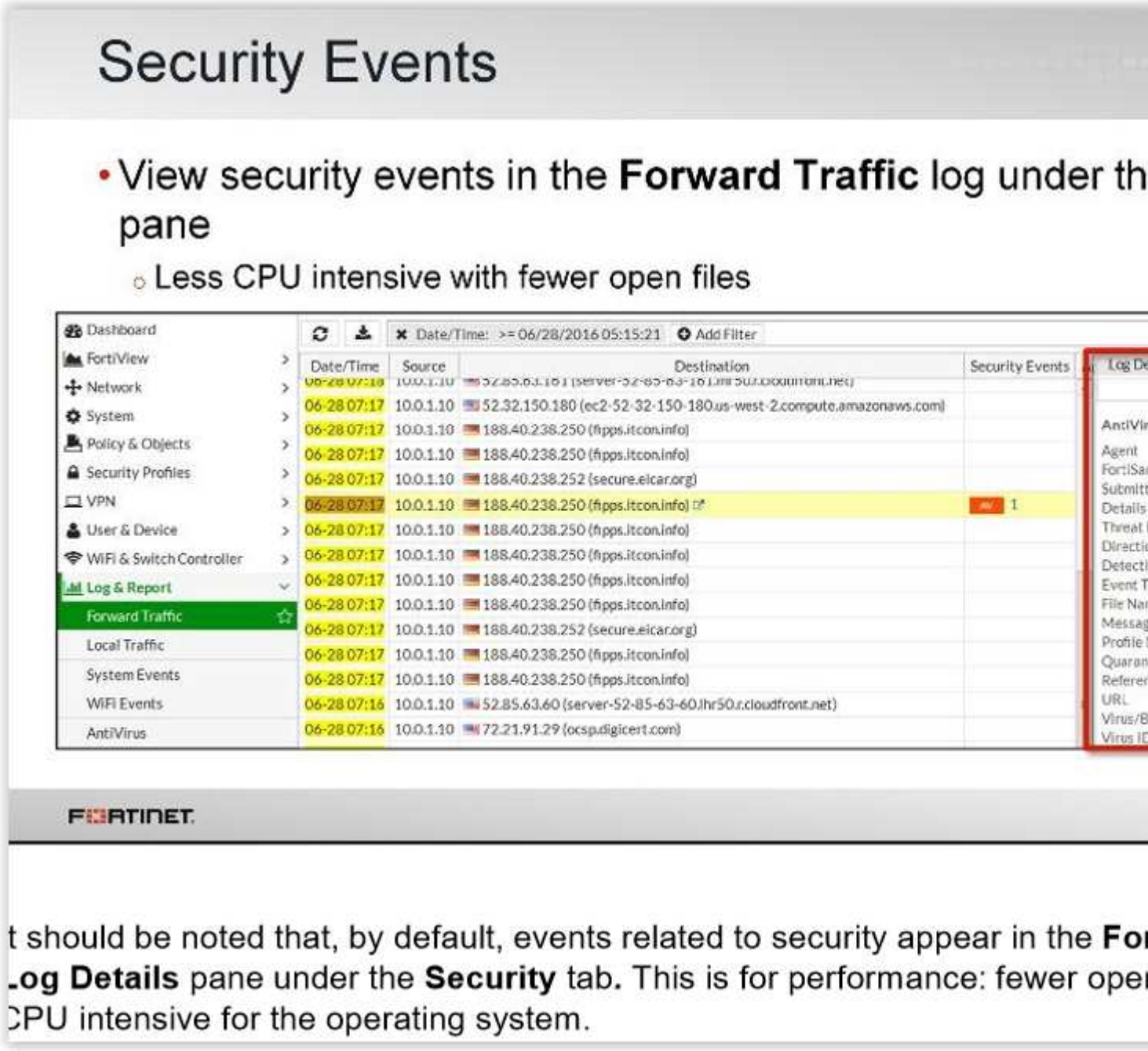
QUESTION 76
Where are most of the security events logged?

A. Security log

B. Forward Traffic log
C. Event log
D. Alert log
E. Alert Monitoring Console

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:



QUESTION 77

What determines whether a log message is generated or not?

A. Firewall policy setting
B. Log Settings in the GUI
C. 'config log' command in the CLI
D. Syslog
E. Webtrends

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which of the following are considered log types? (Choose three.)

A. Forward log
B. Traffic log
C. Syslog
D. Event log
E. Security log

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
What attributes are always included in a log header? (Choose three.)

A. policyid
B. level
C. user
D. time
E. subtype
F. duration

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
What log type would indicate whether a VPN is going up or down?

A. Event log
B. Security log
C. Forward log

D. Syslog

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which correctly define "Section View" and "Global View" for firewall policies? (Choose two.)

A. Section View lists firewall policies primarily by their interface pairs.
B. Section View lists firewall policies primarily by their sequence number.
C. Global View lists firewall policies primarily by their interface pairs.
D. Global View lists firewall policies primarily by their policy sequence number.
E. The 'any' interface may be used with Section View.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
In "diag debug flow" output, you see the message “Allowed by Policy-1: SNAT”. Which is true?

A. The packet matched the topmost policy in the list of firewall policies.
B. The packet matched the firewall policy whose policy ID is 1.
C. The packet matched a firewall policy, which allows the packet and skips UTM checks
D. The policy allowed the packet and applied session NAT.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which is NOT true about the settings for an IP pool type port block allocation?

A. A Block Size defines the number of connections.
B. Blocks Per User defines the number of connection blocks for each user.
C. An Internal IP Range defines the IP addresses permitted to use the pool.
D. An External IP Range defines the IP addresses in the pool.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which define device identification? (Choose two.)

A. Device identification is enabled by default on all interfaces.
B. Enabling a source device in a firewall policy enables device identification on the source interfaces of that policy.
C. You cannot combine source user and source device in the same firewall policy.
D. FortiClient can be used as an agent based device identification technique.
E. Only agentless device identification techniques are supported.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which is true of FortiGate's session table?

A. NAT/PAT is shown in the central NAT table, not the session table.
B. It shows TCP connection states.
C. It shows IP, SSL, and HTTP sessions.
D. It does not show UDP or ICMP connection state codes, because those protocols are connectionless.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which is true about incoming and outgoing interfaces in firewall policies?

A. A physical interface may not be used.
B. A zone may not be used.
C. Multiple interfaces may not be used for both incoming and outgoing.
D. Source and destination interfaces are mandatory.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
For FortiGate devices equipped with Network Processor (NP) chips, which are true? (Choose three.)

A. For each new IP session, the first packet always goes to the CPU.
B. The kernel does not need to program the NPU. When the NPU sees the traffic, it determines by itself whether it can process the traffic
C. Once offloaded, unless there are errors, the NP forwards all subsequent packets. The CPU does not process them.

D. When the last packet is sent or received, such as a TCP FIN or TCP RST signal, the NP returns this session to the CPU for tear down.
E. Sessions for policies that have a security profile enabled can be NP offloaded.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which traffic can match a firewall policy's "Services" setting? (Choose three.)

A. HTTP
B. SSL
C. DNS
D. RSS
E. HTTPS

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which is NOT true about source matching with firewall policies?

A. A source address object must be selected in the firewall policy.
B. A source user/group may be selected in the firewall policy.
C. A source device may be defined in the firewall policy.
D. A source interface must be selected in the firewall policy.
E. A source user/group and device must be specified in the firewall policy.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
If you enable the option "Generate Logs when Session Starts", what effect does this have on the number of traffic log messages generated for each session?

A. No traffic log message is generated.
B. One traffic log message is generated.
C. Two traffic log messages are generated.
D. A log message is only generated if there is a security event.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which best describes the authentication timeout?

A. How long FortiGate waits for the user to enter his or her credentials.
B. How long a user is allowed to send and receive traffic before he or she must authenticate again.
C. How long an authenticated user can be idle (without sending traffic) before they must authenticate again.
D. How long a user-authenticated session can exist without having to authenticate again.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which authentication scheme is not supported by the RADIUS implementation on FortiGate?

A. CHAP
B. MSCHAP2
C. PAP
D. FSSO

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which are valid replies from a RADIUS server to an ACCESS-REQUEST packet from a FortiGate? (Choose two.)

A. ACCESS-CHALLENGE
B. ACCESS-RESTRICT
C. ACCESS-PENDING
D. ACCESS-REJECT

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
What protocol cannot be used with the active authentication type?

A. Local
B. RADIUS

C. LDAP
D. RSSO

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
When configuring LDAP on the FortiGate as a remote database for users, what is not a part of the configuration?

A. The name of the attribute that identifies each user (Common Name Identifier).
B. The user account or group element names (user DN).
C. The server secret to allow for remote queries (Primary server secret).
D. The credentials for an LDAP administrator (password).

Correct Answer: C
Section: (none)
Explanation

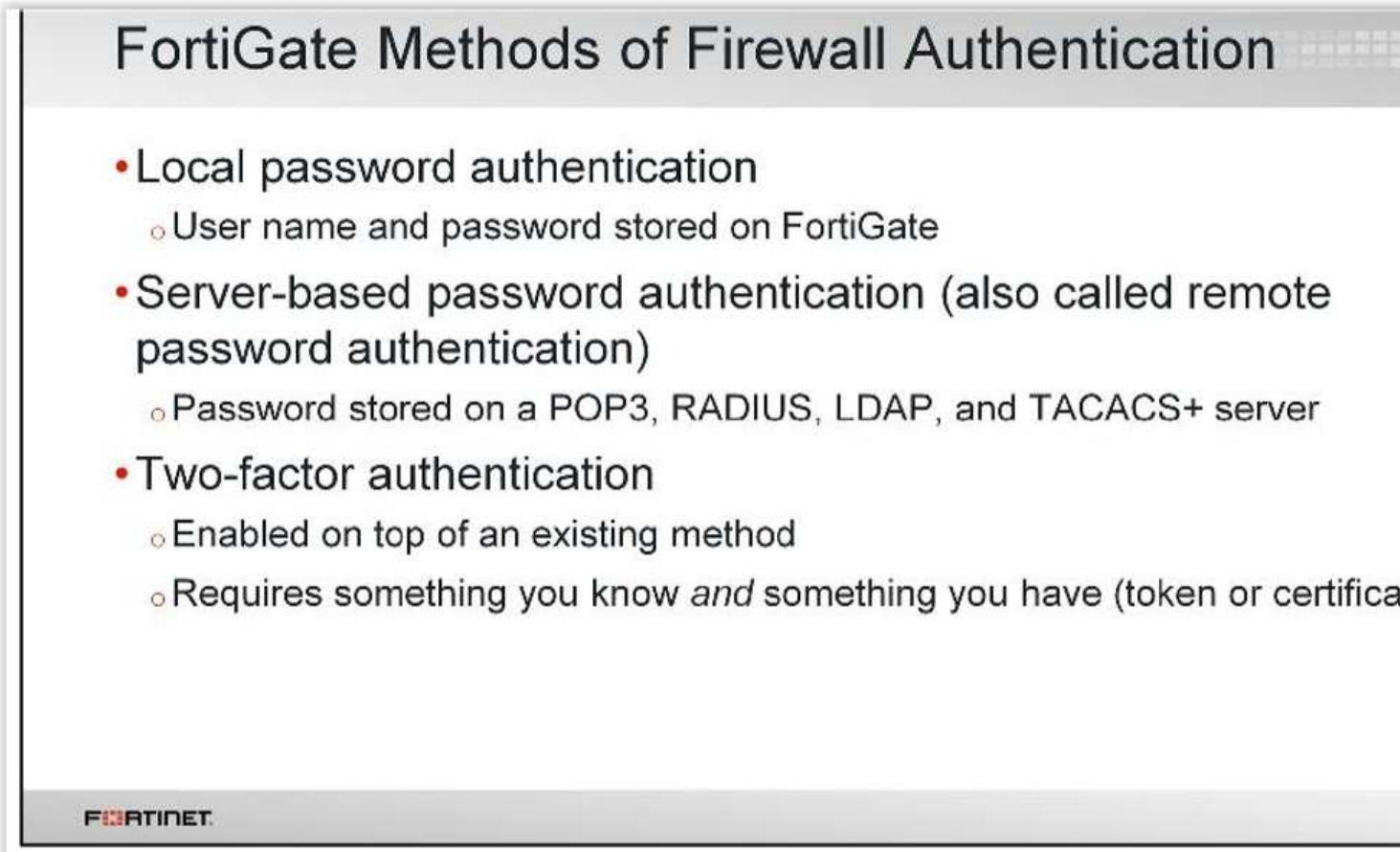
Explanation/Reference:

QUESTION 96
Which authentication methods does FortiGate support for firewall authentication? (Choose two.)

A. Remote Authentication Dial in User Service (RADIUS)
B. Lightweight Directory Access Protocol (LDAP)
C. Local Password Authentication
D. POP3
E. Remote Password Authentication

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:



FortiGate includes three types of firewall authentication:

- Local password authentication
- Server-based password authentication (also called remote password authentication)
- Two-factor authentication. This is a method of authentication that is enabled on top of an

QUESTION 97
Which methods can FortiGate use to send a One Time Password (OTP) to Two-Factor Authentication users? (Choose three.)

A. Hardware FortiToken
B. Web Portal
C. Email
D. USB Token
E. Software FortiToken (FortiToken mobile)

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98

Which user group types does FortiGate support for firewall authentication? (Choose three.)

A. RSSO
B. Firewall
C. LDAP
D. NTLM
E. FSSO

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which does FortiToken use as input when generating a token code? (Choose two.)

A. User password
B. Time
C. User name
D. Seed

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The token passcode is generated using a combination of the time and a secret key which is known only by the token and the FortiAuthenticator device. The token password changes at regular time intervals, and the FortiAuthenticator unit is able to validate the entered passcode using the time and the secret seed information for that token.
Reference: http://docs.fortinet.com/uploaded/files/2030/FortiAuthenticator-3.1-Admin-Guide.pdf

QUESTION 100
What is not true of configuring disclaimers on the FortiGate?

A. Disclaimers can be used in conjunction with captive portal.
B. Disclaimers appear before users authenticate.
C. Disclaimers can be bypassed through security exemption lists.
D. Disclaimers must be accepted in order to continue to the authentication login or originally intended destination.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which statement best describes what SSL.root is?

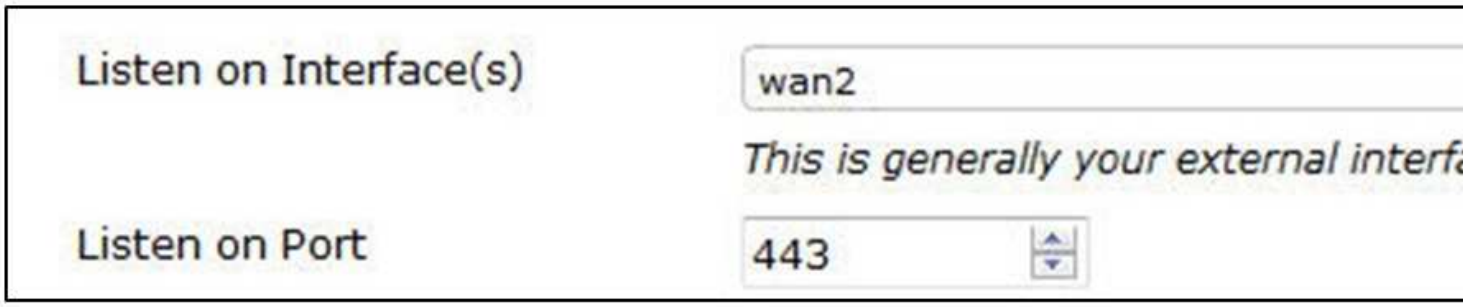
A. The name of the virtual network adapter required in each user's PC for SSL VPN Tunnel mode.

B. The name of a virtual interface in the root VDOM where all the SSL VPN user traffic comes from.
C. A Firewall Address object that contains the IP addresses assigned to SSL VPN users.
D. The virtual interface in the root VDOM that the remote SSL VPN tunnels connect to.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
A FortiGate is configured with the 1.1.1.1/24 address on the wan2 interface and HTTPS Administrative Access, using the default tcp port, is enabled for that interface. Given the SSL VPN settings in the exhibit.



Which of the following SSL VPN login portal URLs are valid? (Choose two.)

A. http://1.1.1.1:443/Training
B. https://1.1.1.1:443/STUDENTS
C. https://1.1.1.1/login
D. https://1.1.1.1/

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Which of the following statements are correct regarding SSL VPN Web-only mode? (Choose two.)

A. It can only be used to connect to web services.
B. IP traffic is encapsulated over HTTPS.

C. Access to internal network resources is possible from the SSL VPN portal.
D. The standalone FortiClient SSL VPN client CANNOT be used to establish a Web-only SSL VPN.
E. It is not possible to connect to SSH servers through the VPN.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Which of the following authentication methods can be used for SSL VPN authentication? (Choose three.)

A. Remote Password Authentication (RADIUS, LDAP)
B. Two-Factor Authentication
C. Local Password Authentication
D. FSSO
E. RSSO

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Which statement best describes what SSL VPN Client Integrity Check does?

A. Blocks SSL VPN connection attempts from users that has been blacklisted.
B. Detects the Windows client security applications running in the SSL VPN client's PCs.
C. Validates the SSL VPN user credential.
D. Verifies which SSL VPN portal must be presented to each SSL VPN user.
E. Verifies that the latest SSL VPN client is installed in the client's PC.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
Which statement is not correct regarding SSL VPN Tunnel mode?

A. IP traffic is encapsulated over HTTPS.
B. The standalone FortiClient SSL VPN client can be used to establish a Tunnel mode SSL VPN.
C. A limited amount of IP applications are supported.
D. The FortiGate device will dynamically assign an IP address to the SSL VPN network adapter.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
What action does an IPsec Gateway take with the user traffic routed to an IPsec VPN when it does not match any phase 2 quick mode selector?

A. Traffic is dropped
B. Traffic is routed across the default phase 2.
C. Traffic is routed to the next available route in the routing table.
D. Traffic is routed unencrypted to the interface where the IPsec VPN is terminating.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
Which of the following authentication methods are supported in an IPsec phase 1? (Choose two.)

A. Asymmetric Keys
B. CA root digital certificates
C. RSA signature
D. Pre-shared keys

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Which of the following IPsec configuration modes can be used for implementing L2TP-over-IPSec VPNs?

A. Policy-based IPsec only.
B. Route-based IPsec only.
C. Both policy-based and route-based VPN.
D. L2TP-over-IPSec is not supported by FortiGate devices.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Which of the following IPsec configuration modes can be used when the FortiGate is running in NAT mode?

A. Policy-based VPN only
B. Both policy-based and route-based VPN.
C. Route-based VPN only.

D. IPSec VPNs are not supported when the FortiGate is running in NAT mode.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Which of the following statements is true regarding the differences between route-based and policy-based IPsec VPNs? (Choose two.)

A. The firewall policies for policy-based are bidirectional. The firewall policies for route-based are unidirectional.
B. In policy-based VPNs the traffic crossing the tunnel must be routed to the virtual IPsec interface. In route-based, it does not.
C. The action for firewall policies for route-based VPNs may be Accept or Deny, for policy-based VPNs it is Encrypt.
D. Policy-based VPN uses an IPsec interface, route-based does not.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Which portion of the configuration does an administrator specify the type of IPsec configuration (either policy-based or route-based)?

A. Under the IPsec VPN global settings.
B. Under the phase 2 settings.
C. Under the phase 1 settings.
D. Under the firewall policy settings.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Firewall policies allow IP traffic to pass between interfaces on a FortiGate unit. You can limit communication to particular traffic by specifying source address and destination addresses.
Policy-based and route-based VPNs require different firewall policies.
• A policy-based VPN requires an IPsec firewall policy. You specify the interface to the private network, the interface to the remote peer and the VPN tunnel. A single policy can enable traffic inbound, outbound, or in both directions.
• A route-based VPN requires an Accept firewall policy for each direction. As source and destination interfaces, you specify the interface to the private network and the virtual IPsec interface (phase 1 configuration) of the VPN. The IPsec interface is the destination interface for the outbound policy and the source interface for the inbound policy

Reference: http://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR1/fortigate-ipsec-40-mr1.pdf

QUESTION 113
Which of the following options best defines what Diffie-Hellman is?

A. A symmetric encryption algorithm.
B. A "key-agreement" protocol.
C. A "Security-association-agreement" protocol.
D. An authentication algorithm.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
How many packets are interchanged between both IPSec ends during the negotiation of a main-mode phase 1?

A. 5
B. 3
C. 2
D. 6

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Which of the following IKE modes is the one used during the IPsec phase 2 negotiation?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Which of the following statements are true about IPsec VPNs? (Choose three.)

A. IPsec increases overhead and bandwidth.
B. IPsec operates at the layer 2 of the OSI model.
C. End-user's network applications must be properly pre-configured to send traffic across the IPsec VPN.
D. IPsec protects upper layer protocols.
E. IPsec operates at the layer 3 of the OSI model.

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
Which of the following statements is true regarding the TCP SYN packets that go from a client, through an implicit web proxy (transparent proxy), to a web server listening at TCP port 80? (Choose three.)

A. The source IP address matches the client IP address.
B. The source IP address matches the proxy IP address.
C. The destination IP address matches the proxy IP address.
D. The destination IP address matches the server IP addresses.
E. The destination TCP port number is 80.

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which of the following statements is true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

A. More than one proxy is supported.
B. Can contain a list of destinations that will be exempt from the use of any proxy.
C. Can contain a list of URLs that will be exempted from the FortiGate web filtering inspection.
D. Can contain a list of users that will be exempted from the use of any proxy.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
An Internet browser is using the WPAD DNS method to discover the PAC file's URL. The DNS server replies to the browser's request with the IP address 10.100.1.10. Which URL will the browser use to download the PAC file?

A. http://10.100.1.10/proxy.pac
B. https://10.100.1.10/
C. http://10.100.1.10/wpad.dat
D. https://10.100.1.10/proxy.pac

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

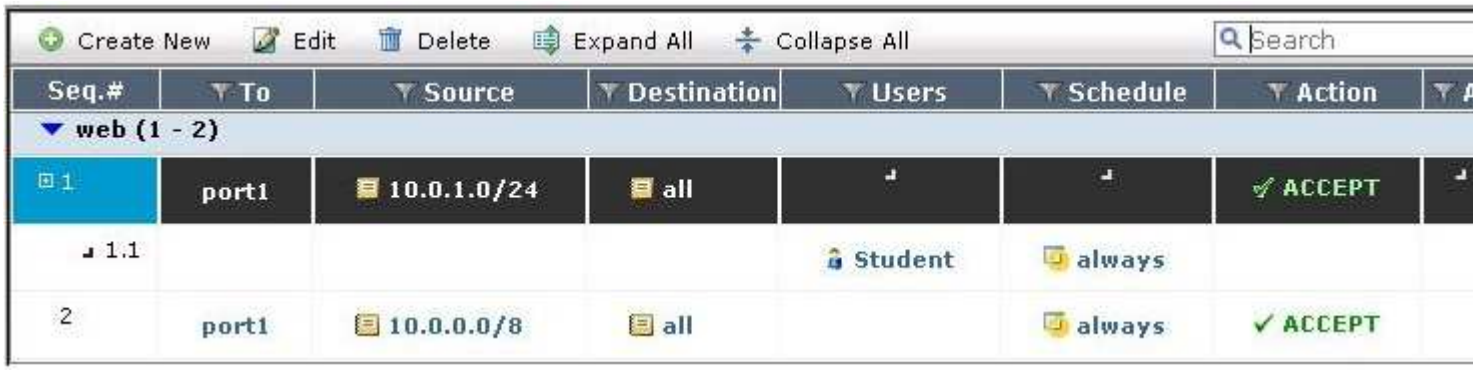
QUESTION 120
Which of the following are benefits of using web caching? (Choose three.)

A. Decrease bandwidth utilization
B. Reduce server load
C. Reduce FortiGate CPU usage
D. Reduce FortiGate memory usage
E. Decrease traffic delay

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
Review the exhibit of an explicit proxy policy configuration.



If there is a proxy connection attempt coming from the IP address 10.0.1.5, and from a user that has not authenticated yet, what action does the FortiGate proxy take?

A. User is prompted to authenticate. Traffic from the user Student will be allowed by the policy #1. Traffic from any other user will be allowed by the policy #2.
B. User is not prompted to authenticate. The connection is allowed by the proxy policy #2.
C. User is not prompted to authenticate. The connection will be allowed by the proxy policy #1.
D. User is prompted to authenticate. Only traffic from the user Student will be allowed. Traffic from any other user will be blocked.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
Which protocol can an Internet browser use to download the PAC file with the web proxy configuration?

A. HTTPS
B. FTP
C. TFTP

D. HTTP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
Which are the three different types of Conserve Mode that can occur on a FortiGate device? (Choose three.)

A. Proxy
B. Operating system
C. Kernel
D. System
E. Device

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
What is longest length of time allowed on a FortiGate device for the virus scan to complete?

A. 20 seconds
B. 30 seconds
C. 45 seconds
D. 10 seconds

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Files reported as "suspicious" were subject to which Antivirus check"?

A. Grayware
B. Virus
C. Sandbox
D. Heuristic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
Which type of conserve mode writes a log message immediately, rather than when the device exits conserve mode?

A. Kernel
B. Proxy
C. System
D. Device

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

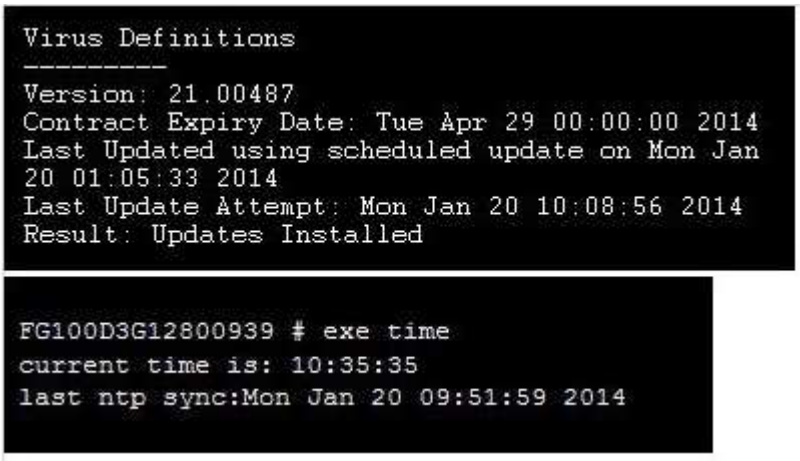
QUESTION 127
Files that are larger than the oversized limit are subjected to which Antivirus check?

A. Grayware
B. Virus
C. Sandbox
D. Heuristic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
A FortiGate device is configure to perform an AV & IPS scheduled update every hour.



Given the information in the exhibit, when will the next update happen?

A. 01:00
B. 02:05
C. 11:00
D. 11:08

Correct Answer: D
Section: (none)
Explanation

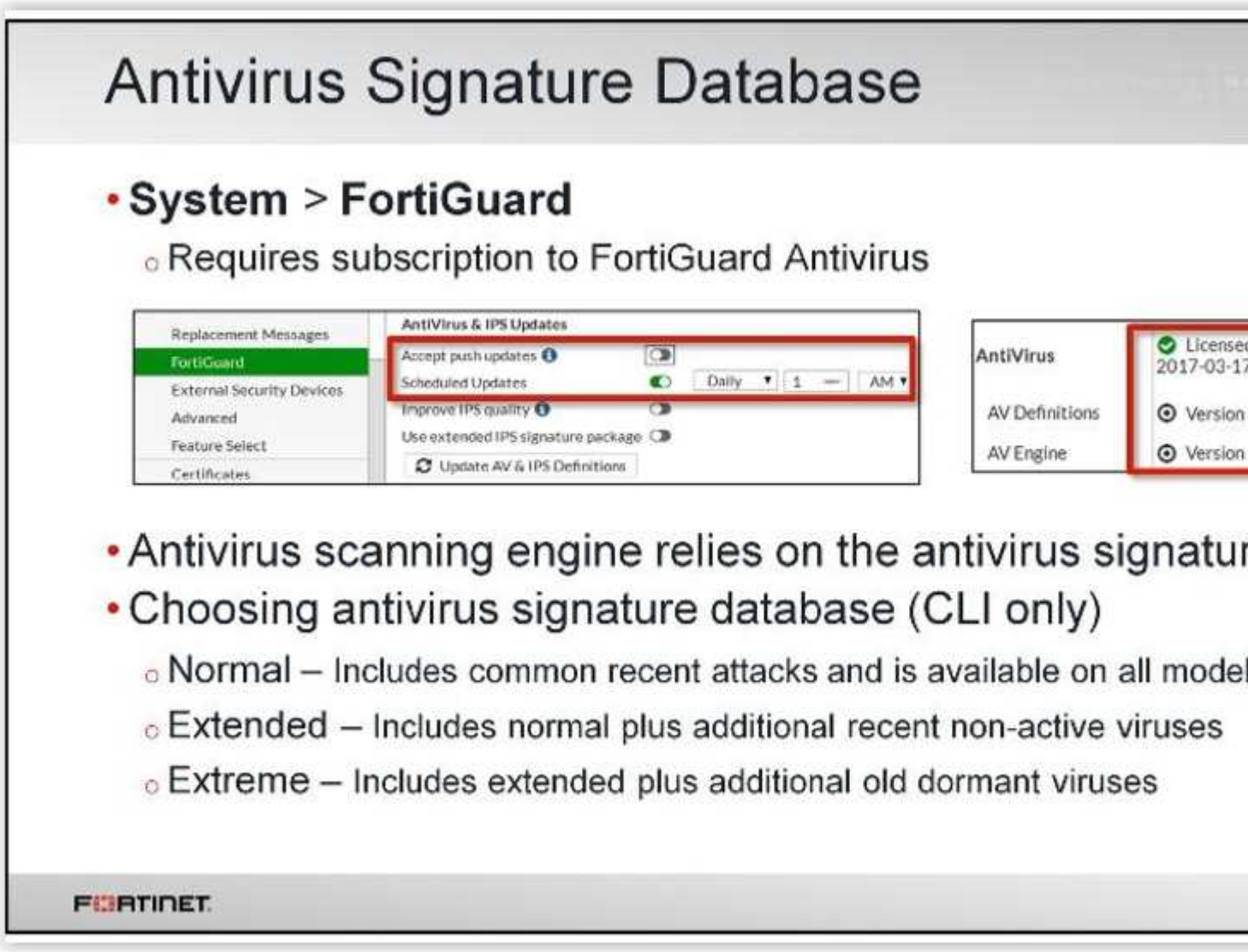
Explanation/Reference:

QUESTION 129
What is the maximum number of different virus databases a FortiGate can have?

A. 5
B. 2
C. 3
D. 4

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:



QUESTION 130
Which of the following are possible actions for static URL filtering? (Choose three.)

A. Allow
B. Block
C. Exempt
D. Warning
E. Shape

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
Which of the following statements are true regarding the web filtering modes? (Choose two.)

A. Proxy based mode allows for customizable block pages to display when sites are prevented.
B. Proxy based mode requires more resources than flow-based.
C. Flow based mode offers more settings under the advanced configuration section of the GUI.
D. Proxy based mode offers higher throughput than flow-based mode.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
Which of the following web filtering modes can inspect the full URL? (Choose two.)

A. Proxy based
B. DNS based
C. Policy based
D. Flow based

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
Examine the following log message attributes and select two correct statements from the list below. (Choose two.)

hostname=www.youtube.com profiletype="Webfilter_Profile" profile="default" status="passthrough" msg="URL belongs to a category with warnings enabled"

A. The traffic was blocked.
B. The user failed authentication.
C. The category action was set to warning.
D. The website was allowed

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
Which of the following are possible actions for FortiGuard web category filtering? (Choose three.)

A. Allow
B. Block
C. Exempt
D. Warning
E. Shape

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
Which of the following actions can be used with the FortiGuard quota feature? (Choose three.)

A. Allow
B. Block
C. Monitor
D. Warning
E. Authenticate

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
Which of the following statements are true regarding application control? (Choose two.)

A. Application control is based on TCP destination port numbers.
B. Application control is proxy based.
C. Encrypted traffic can be identified by application control.
D. Traffic shaping can be applied to the detected application traffic.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
The exhibit is a screen shot of an Application Control profile.

Different settings are circled and numbered. Select the number identifying the setting which will provide additional information about YouTube access, such as the name of the video watched.

A. 1
B. 2
C. 3
D. 4
E. 5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
How do application control signatures update on a FortiGate device?

A. Through FortiGuard updates.
B. Upgrade the FortiOS firmware to a newer release.
C. By running the Application Control auto-learning feature.
D. Signatures are hard coded to the device and cannot be updated.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139

Which answer best describes what an "Unknown Application" is?

A. All traffic that matches the internal signature for unknown applications.
B. Traffic that does not match the RFC pattern for its protocol.
C. Any traffic that does not match an application control signature
D. A packet that fails the CRC check.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
What actions are possible with Application Control? (Choose three.)

A. Warn
B. Allow
C. Block
D. Traffic Shaping
E. Quarantine

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
Which is the following statement are true regarding application control? (choose two)

A. Application control is based on TCP destination port numbers.
B. Application control is proxy based.
C. Encrypted traffic can be identified by application control.
D. Traffic Shaping can be applied to the detected application traffic.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

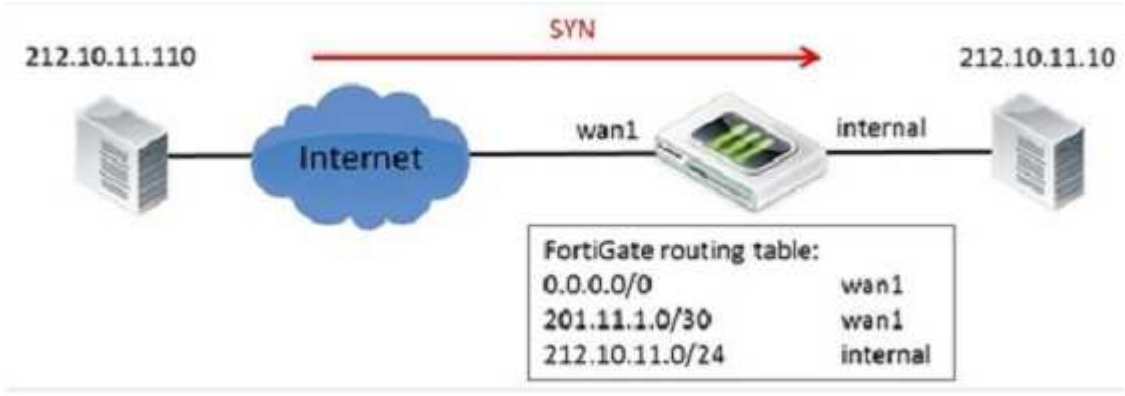
QUESTION 142
Which of the following fields contained in the IP/TCP/UDP headers can be used to make a routing decision when using policy-based routing? (Choose three)

A. Source IP address.
B. TCP flags
C. Source TCP/UDP ports
D. Type of service.
E. Checksum

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
Examine the network topology diagram in the exhibit; the workstation with the IP address 212.10.11.110 sends a TCP SYN packet to the workstation with the IP address 212.10.11.20.



Which of the following sentences best describes the result of the reverse path forwarding (RFP) check executed by the FortiGate on the SYN packets? (Choose two).

A. Packets is allowed if RPF is configured as loose.
B. Packets is allowed if RPF is configured as strict.
C. Packets is blocked if RPF is configured as loose.
D. Packets is blocked if RPF is configured as strict.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
Which of the following statements best describe what a FortiGate does when packets match a black hole route?

A. Packets are dropped.
B. Packets are routed based on the information in the policy-based routing table.
C. An ICMP error message is sent back to the originator.
D. Packet are routed back to the originator.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
The exhibit shows two static routes to the same destinations subnet 172.20.168.0/24.

```
#config router static
    edit 1
      set dst 172.20.168.0 255.255.255.0
      set distance 10
       set priority 20
      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 this static routing configuration? (choose two)

A. Both routes will show up in the routing table.
B. The FortiGate unit will evenly share the traffic to 172.20.168.0/24 between routes.
C. Only one route will show up in the routing table.
D. The FortiGate will route the traffic to 172.20.168.0/24 only through one route.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
Which of the following statements are true regarding WAN Link Load Balancing? (Choose two).

A. There can be only one virtual WAN Link per VDOM.
B. FortiGate can measure the quality of each link based on latency, jitter, or packets percentage.
C. Link health checks can be performed over each link member if the virtual WAN interface.
D. Distance and priority values are configured in each link member if the virtual WAN interface.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
In the debug command output shown in the exhibit, which of the following best described the MAC address 00:09:0f:69:03:7e ?

```
# diagnose 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
```

A. It is one of the secondary MAC addresses of the port1 interface.
B. It is the primary MAC address of the port interface.
C. It is the MAC address of another network devices located in the same LAN segment as the FortiGate unit's port1 interface.
D. It is the HA virtual MAC address.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
Which action does the FortiGate take when link health monitor times out?

A. All routes to the destination subnet configured in the link health monitor are removed from the routing table.
B. The distance values of all routes using interface configured in the link health monitor are increased.
C. The priority values of all routes using configured in the link health monitor are increased.
D. All routes using the next-hop gateway configured in the link health monitor are removed from the routing table.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
What must be configured in order to keep two static routes to the same destination in the routing table?

A. The same priority.
B. The same distance and same priority.
C. The same distance.
D. The same metric.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
The exhibit shoes three static routes.

```
config router static
    edit 1
      set dst 172.20.168.0 255.255.255.0
      set distance 10
      set priority 10
     set device port1
    next
    edit 2
      set dst 172.20.0.0 255.255.0.0
      set distance 5
      set priority 20
      set device port2
    next
    edit 3
      set dst 172.20.0.0 255.255.0.0
      set distance 5
      set priority 20
      set device port3
    next
end
```

Which routes will be used to route the packets to the destination IP address 172.20.168.1?

A. The route with the ID number 2 and 3.
B. Only the route with the ID number 3.
C. Only the route with the ID number 2.
D. Only the route with the ID number 1.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
The exhibit shows a FortiGate routing table.

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default
O*E2  0.0.0.0/0 [110/10] via 192.168.11.254, wan1, 01:29:24
C        172.16.78.0/24 is directly connected, wan2
O        192.168.1.0/24 [110/200] via 192.168.11.59, internal, 01:30
C        192.168.3.0/24 is directly connected, dmz
C        192.168.11.0/24 is directly connected, internal
```

Which of the following statements are correct?(Choose two)

A. There is only one active default route.
B. The distance values for the route to 192.168.1.0/24 is 200
C. An IP address in the subnet 172.16.78.0/24 has been assigned to the dmz interface.
D. The FortiGate will route the traffic to 172.17.1.2 to next hop with the IP address 192.168.11.254

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
A FortiGate devices has two VDOMs in NAT/route mode. Which of the following solutions can be implemented by a network administrator to route traffic between the two VDOMs.(Choose two)

A. Use the inter-VDOMs links automatically created between all VDOMS.
B. Manually create and configured an inter-VDOM link between yours.
C. Interconnect and configure an external physical interface in one VDOM to another physical interface in the second VDOM.
D. Configure both VDOMs to share the same table.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
A FortiGate device is configured with two VDOMs. The management VDOM is 'root' , and is configured in transparent mode,'vdom1' is configured as NAT/route mode. Which traffic is generated only by 'root' and not 'vdom1'? (Choose three.)

A. SNMP traps

B. FortiGaurd
C. ARP
D. NTP
E. ICMP redirect

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
Which of the following settings can be configured per VDOM? (Choose three)

A. Operating mode (NAT/route or transparent)
B. Static routes
C. Hostname
D. System time
E. Firewall Policies

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
Which of the following statements are correct regarding FortiGate virtual domains (VDOMs)? (Choose two)

A. VDOMs divide a single FortiGate unit into two or more independent firewall.
B. A management VDOM handles SNMP. logging, alert email and FortiGuard updates.
C. Each VDOM can run different firmware versions.
D. Administrative users with a 'super_admin' profile can administrate only one VDOM.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
Which of the following statements is correct concerning multiple vdoms configured in a FortiGate device?

A. FortiGate devices,from the FGT/FWF 60D and above, all support VDOMS.
B. All FortiGate devices scale to 250 VDOMS.
C. Each VDOM requires its own FortiGuard license.
D. FortiGate devices support more NAT/route VDOMs than Transparent Mode VDOMs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
A FortiGate unit has multiple VDOMs in NAT/route mode with multiple VLAN interfaces in each VDOM. Which of the following statements is correct regarding the IP addresses assigned to each VLAN interface?

A. Different VLANs can share the same IP address as long as they have different VLAN IDs.
B. Different VLANs can share the same IP address as long as they are in different physical interface.
C. Different VLANs can share the same IP address as long as they are in different VDOMs.
D. Different VLANs can never share the same IP addresses.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
A FortiGate unit operating in NAT/route mode and configured with two sub-interface on the same physical interface. Which of the following statement is correct regarding the VLAN IDs in this scenario?

A. The two VLAN sub-interfaces can have the same VLAN IDs 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 VLAN ID only if they belong to different VDOMs.
D. The two VLAN sub-interfaces can have the same VLAN if they are connected to different L2 IEEE 802.1Q complaint switches.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
A FortiGate devices is configured with four VDOMs: 'root' and 'vdom1' are in NAT/route mode; 'vdom2' and 'vdom2' are in transparent mode. The management VDOM is 'root'. Which of the following statements are true? (Choose two.)

A. An inter-VDOM link between 'root' and 'vdom1' can be created.
B. An inter-VDOM link between 'vdom1' and vdom2' can created.
C. An inter-VDOM link between 'vdom2' and vdom3' can created.
D. Inter-VDOM link links must be manually configured for FortiGuard traffic.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
Which of the following statements is true regarding a FortiGate device operating in transparent mode?

(Choose three.)

A. It acts as a layer 2 bridge
B. It acts as a layer 3 router
C. It forwards frames using the destination MAC address.
D. It forwards packets using the destination IP address.
E. It can perform content inspection (antivirus, web filtering, etc)

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
Which of the following statements are correct concerning IPsec dialup VPN configurations for FortiGate devices? (Choose two)

A. Main mode mist be used when there is no more than one IPsec dialup VPN configured on the same FortiGate device.
B. A FortiGate device with an IPsec VPN configured as dialup can initiate the tunnel connection to any remote IP address.
C. Peer ID must be used when there is more than one aggressive-mode IPsec dialup VPN on the same FortiGate device.
D. The FortiGate will automatically add a static route to the source quick mode selector address received from each remote peer.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
Which of the following combinations of two FortiGate device configurations (side A and side B), can be used to successfully establish an IPsec VPN between them? (choose two)

A. Side A:main mode, remote gateway as static IP address, policy based VPN. Side B: aggressive mode, remote Gateway as static IP address policy-based VPN.
B. Side A:main mode, remote gateway as static IP address, policy based VPN. Side B: main mode, remote gateway as static IP address, route-based VPN
C. Side A:main mode, remote gateway as static IP address, policy based VPN. Side B: main mode, remote gateway as dialup, route-based VPN.
D. Side A: main mode, remote gateway as dialup policy based VPN, Side B: main mode, remote gateway as dialup, policy based VPN.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163

Which of the following statements are correct differences between NAT/route and transparent mode? (Choose two.)

A. In transparent mode, interfaces do not have IP addresses.
B. Firewall polices are only used in NAT/ route mode.
C. Static routers are only used in NAT/route mode.
D. Only transparent mode permits inline traffic inspection at layer 2.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

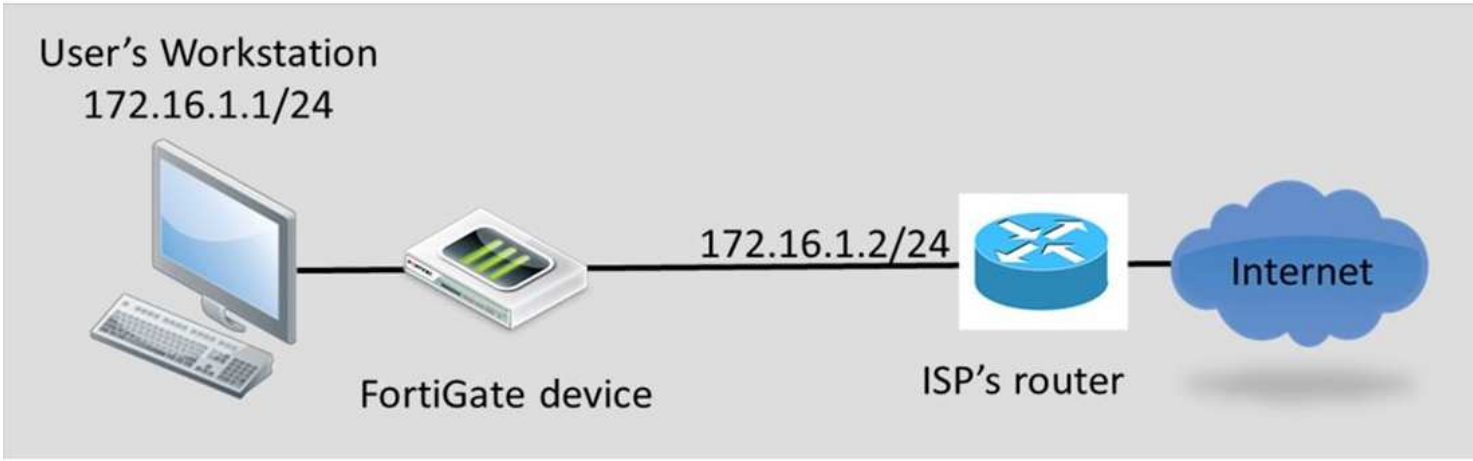
QUESTION 164
Which of the following are operating mode supported in FortiGate devices? (Choose two)

A. Proxy
B. Transparent
C. NAT/route
D. Offline inspection

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
Review to the network topology in the exhibit.



The workstation, 172.16.1.1/24, connects to port2 of the FortiGate device, and the ISP router, 172.16.1.2, connects to port1. Without changing IP addressing, which configuration changes are required to properly forward users traffic to the Internet?(Choose two)

A. At least one firewall policy from port2 to port1 to allow outgoing traffic.
B. A default route configured in the FortiGuard devices pointing to the ISP's router.
C. Static or dynamic IP addresses in both ForitGate interfaces port1 and port2.

D. The FortiGate devices configured in transparent mode.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
Which of the following statement correct describes the use of the "diagnose sys ha reset-uptime" command?

A. To force an HA failover when the HA override setting is disabled.
B. To force an HA failover when the HA override setting is enabled.
C. To clear the HA counters.
D. To restart a FortiGate unit that is part of an HA cluster.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
What are required to be the same for two FortiGate units to form an HA cluster? (Choose two)

A. Firmware.
B. Model.
C. Hostname.
D. System time zone.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
Which of the following statements describes the objectives of the gratuitous ARP packets sent by an HA cluster?

A. To synchronize the ARp tables in all the FortiGate Unis that are part of the HA cluster.
B. To notify the network switches that a new HA master unit has been elected.
C. To notify the master unit that the slave devices are still up and alive.
D. To notify the master unit about the physical MAC addresses of the slave units.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169

Which of the following statements are correct regarding a master HA unit? (Choose two)

A. There should be only one master unit is each HA virtual cluster.
B. The Master synchronizes cluster configuration with slaves.
C. Only the master has a reserved management HA interface.
D. Heartbeat interfaces are not required on a master unit.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
Which statement describes how traffic flows in sessions handled by a slave unit in an active-active HA cluster?

A. Packet are sent directly to the slave unit using the slave physical MAC address.
B. Packets are sent directly to the slave unit using the HA virtual MAC address.
C. Packets arrived at both units simultaneously, but only the salve unit forwards the session.
D. Packets are first sent to the master unit, which then forwards the packets to the slave unit.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
Which of the following statements are correct concerning the FortiGate session life support protocol? (Choose two)

A. By default, UDP sessions are not synchronized.
B. Up to four FortiGate devices in standalone mode are supported.
C. only the master unit handles the traffic.
D. Allows per-VDOM session synchronization.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
What is the default criteria for selecting the HA master unit in a HA cluster?

A. port monitor, priority, uptime, serial number
B. Port monitor, uptime, priority, serial number
C. Priority, uptime, port monitor, serial number
D. uptime, priority, port monitor, serial number

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

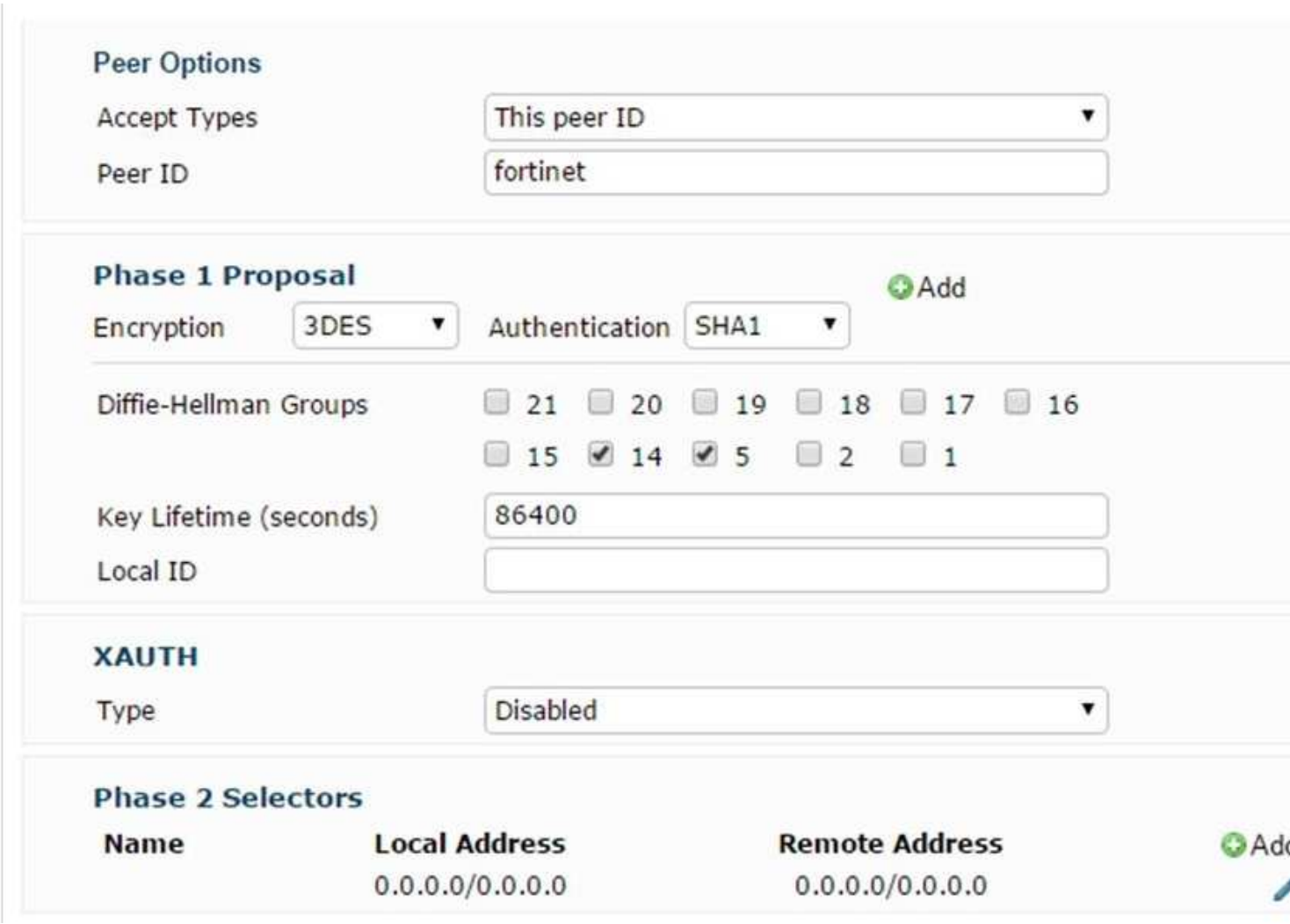
QUESTION 173
What information is synchronized between two FortiGate units that belong to the same HA cluster? (Choose three)

A. IP addresses assigned to DHCP enabled interface.
B. The master devices hostname.
C. Routing configured and state.
D. Reserved HA management interface IP configuration.
E. Firewall policies and objects.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
Which of the following statements are correct concerning the IPsec phase 1 and phase 2, shown in the exhibit? (choose two)



A. The quick mode selector in the remote site must also be 0.0.0.0/0 for the source and destination addresses.
B. Only remote peers with the peer ID 'fortinet' will be able to establish a VPN.
C. The FortiGate device will automatically add a static route to the source quick mode selector address received from each remote VPN peer.
D. The configuration will work only to establish FortiClient-to-FortiGate tunnels. A FortiGate tunnel requires a different configuration.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
The exhibit shows a part output of the diagnostic command 'diagnose debug application ike 255', taken during establishment of a VPN. Which of the following statement are correct concerning this output? (choose two)

```
Ike 0:Remote:7:22: responder received first quick-mode message
ike 0:Remote:7:22: peer proposal is: peer:0:0.0.0.0-255.255.255.255:0, me:0:0.0.
ike 0:Remote:7: sent IKE msg (quick_r1send): 172.20.186.222:500->172.20.187.114:
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:7:P2:22: replay protection enabled
ike 0:Remote:7:P2:22: SA life soft seconds=1750.
ike 0:Remote:7:P2:22: SA life hard seconds=1800.
ike 0:Remote:7:P2:22: IPsec SA selectors #src=1 #dst=1
ike 0:Remote:7:P2:22: src 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7:P2:22: dst 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7:P2:22: add IPsec SA: SPIs=6e13ca19/8f1ce9ae
ike 0:Remote:7:P2:22: added IPsec SA: SPIs=6e13ca19/8f1ce9ae
ike 0:Remote:7:P2:22: sending SNMP tunnel UP trap
```

A. The quick mode selectors negotiated between both IPsec VPN peers is 0.0.0.0/32 for both source and destination addresses.
B. The output corresponds to a phase 2 negotiation
C. NAT-T enabled and there is third device in the path performing NAT of the traffic between both IPsec VPN peers.
D. The IP address of the remote IPsec VPN peer is 172.20.187.114

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
What is required in a FortiGate configuration to have more than one dialup IPsec VPN using aggressive mode?

A. All the aggressive mode dialup VPNs MUST accept connections from the same peer ID.
B. Each peer ID MUST match the FQDN of each remote peer.
C. Each aggressive mode dialup MUST accept connections from different peer ID.
D. The peer ID setting must NOT be used.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
Which of the following statements are correct concerning IKE mode config? (Choose two)

A. It can dynamically assign IP addresses to IPsec VPN clients.
B. It can dynamically assign DNS settings to IPsec VPN clients.
C. It uses the ESP protocol.
D. It can be enabled in the phase 2 configuration.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
Which statement is correct concerning an IPsec VPN with the remote gateway setting configured as 'Dynamic DNS'?

A. The FortiGate will accept IPsec VPN connection from any IP address.
B. The FQDN resolution of the local FortiGate IP address where the VPN is terminated must be provided by a dynamic DNS provider.
C. The FortiGate will Accept IPsec VPN connections only from IP addresses included on a dynamic DNS access list.
D. The remote gateway IP address can change dynamically.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
Which of the following protocols are defined in the IPsec Standard? (Choose two)

A. AH
B. GRE
C. SSL/TLS
D. ESP

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
What configuration objects are automatically added when using the FortiGate's FortiClient VPN Configurations Wizard?(Choose two)

A. Static route
B. Phase 1
C. Users group
D. Phase 2

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
Which of the following statements are correct concerning layer 2 broadcast domains in transparent mode VDOMs?(Choose two)

A. The whole VDOM is a single broadcast domain even when multiple VLAN are used.
B. Each VLAN is a separate broadcast domain.
C. Interfaces configured with the same VLAN ID can belong to different broadcast domains.
D. All the interfaces in the same broadcast domain must use the same VLAN ID.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.firewallshop.com/download/fortinet/FortiGate_VLANs_and_VDOMs_Guide.pdf

QUESTION 182
Which of the following statements is correct regarding FortiGate interfaces and spanning tree protocol? (Choose Two)

A. Only FortiGate switch interfaces Participate in spanning tree.
B. All FortiGate interfaces in transparent mode VDOMs participate in spanning tree.
C. All FortiGate interfaces in NAT/route mode VDOMs Participate in spanning tree.
D. All FortiGate interfaces in transparent mode VDOMs may block or forward BPDUs.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
On your FortiGate 60D, you've configured firewall policies. They port forward traffic to your Linux Apache web server. Select the best way to protect your web server by using the IPS engine.

A. Enable IPS signatures for Linux servers with HTTP, TCP and SSL protocols and Apache applications. Configured DLP to block HTTP GET request with credit card numbers.
B. Enable IPS signatures for Linux servers with HTTP, TCP and SSL protocols and Apache applications. Configure DLP to block HTTP GET with credit card numbers. Also configure a DoS policy to prevent TCP SYn floods and port scans.
C. None. FortiGate 60D is a desktop model, which does not support IPS.
D. Enable IPS signatures for Linux and windows servers with FTP, HTTP, TCP, and SSL protocols and Apache and PHP applications.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/2181/fortigate-security-profiles-guide-524.pdf

QUESTION 184
Which changes to IPS will reduce resource usage and improve performance? (Choose three)

A. In custom signature, remove unnecessary keywords to reduce how far into the signature tree that FortiGate must compare in order to determine whether the packet matches.
B. In IPS sensors, disable signatures and rate based statistics (anomaly detection) for protocols, applications and traffic directions that are not relevant.
C. In IPS filters, switch from 'Advanced' to 'Basic' to apply only the most essential signatures.
D. In firewall policies where IPS is not needed, disable IPS.
E. In firewall policies where IPS is used, enable session start logs.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
Which statement concerning IPS is false?

A. IPS packages contain an engine and signatures used by both IPS and other flow-based scans.
B. One-arm topology with sniffer mode improves performance of IPS blocking.
C. IPS can detect zero-day attacks.
D. The status of the last service update attempt from FortiGuard IPS is shown on System>Config>FortiGuard and in output from 'diag autoupdate version'

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
Which best describes the mechanism of a TCP SYN flood?

A. The attackers keeps open many connections with slow data transmission so that other clients cannot start new connections.
B. The attackers sends a packets designed to sync with the FortiGate
C. The attacker sends a specially crafted malformed packet, intended to crash the target by exploiting its parser.
D. The attacker starts many connections, but never acknowledges to fully form them.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
Which profile could IPS engine use on an interface that is in sniffer mode? (Choose three)

A. Antivirus (flow based
B. Web filtering (PROXY BASED)
C. Intrusion Protection
D. Application Control

E. Endpoint control

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.fortinet.com/sites/default/files/productdatasheets/fortios-5-4-datasheet_2.pdf (page 10 - offline inspection)

QUESTION 188
Which operating system vulnerability can you protect when selecting signatures to include in an IPS sensor? (choose three)

A. Irix
B. QNIX
C. Linux
D. Mac OS
E. BSD

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/1082/fortigate-security_profiles-50.pdf (page 59)

QUESTION 189
You are creating a custom signature. Which has incorrect syntax?

A. F-SBID(--attack_id 1842,--name "Ping.Death";--protocol icmp; --data_size>32000;)
B. F-SBID(--name "Block.SMTP.VRFY.CMD";--pattern "vrfy";-- service SMTP; --no_case;--context header;)
C. F-SBID(--name "Ping.Death";--protocol icmp;--data_size>32000;)
D. F-SBID(--name "Block".HTTP.POST"; --protocol tcp;-- service HTTP;-- flow from_client; --pattern "POST"; --context uri;--within 5,context;)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://forum.fortinet.com/tm.aspx?m=110493

QUESTION 190
Which best describe the mechanism of a TCP SYN flood?

A. The attacker keeps open many connections with slow data transmission so that other clients cannot start new connections.
B. The attacker sends a packet designed to "sync" with the FortiGate.
C. The attacker sends a specially crafted malformed packet, intended to crash the target by exploiting its parser.
D. The attacker starts many connections, but never acknowledges to fully form them.

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 191
Which statement is correct concerning creating a custom signature?

A. It must start with the name
B. It must indicate whether the traffic flow is from the client or the server.
C. It must specify the protocol. Otherwise, it could accidentally match lower-layer protocols.
D. It is not supported by Fortinet Technical Support.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
Your Linux email server runs on a non-standard port number, port 2525. Which statement is true?

A. IPS cannot scan that traffic for SMTP anomalies because of the non-standard port number. You must reconfigured the server to run on port 2.
B. To apply IPS to traffic to that server, you must configured FortiGate SMTP proxy to listen on port 2525
C. IPS will apply all SMTP signatures, regardless of whether they apply to clients or servers.
D. Protocol decoders automatically detect SMTP and scan for matches with appropriate IPS signature.

Correct Answer: B
Section: (none)
Explanation

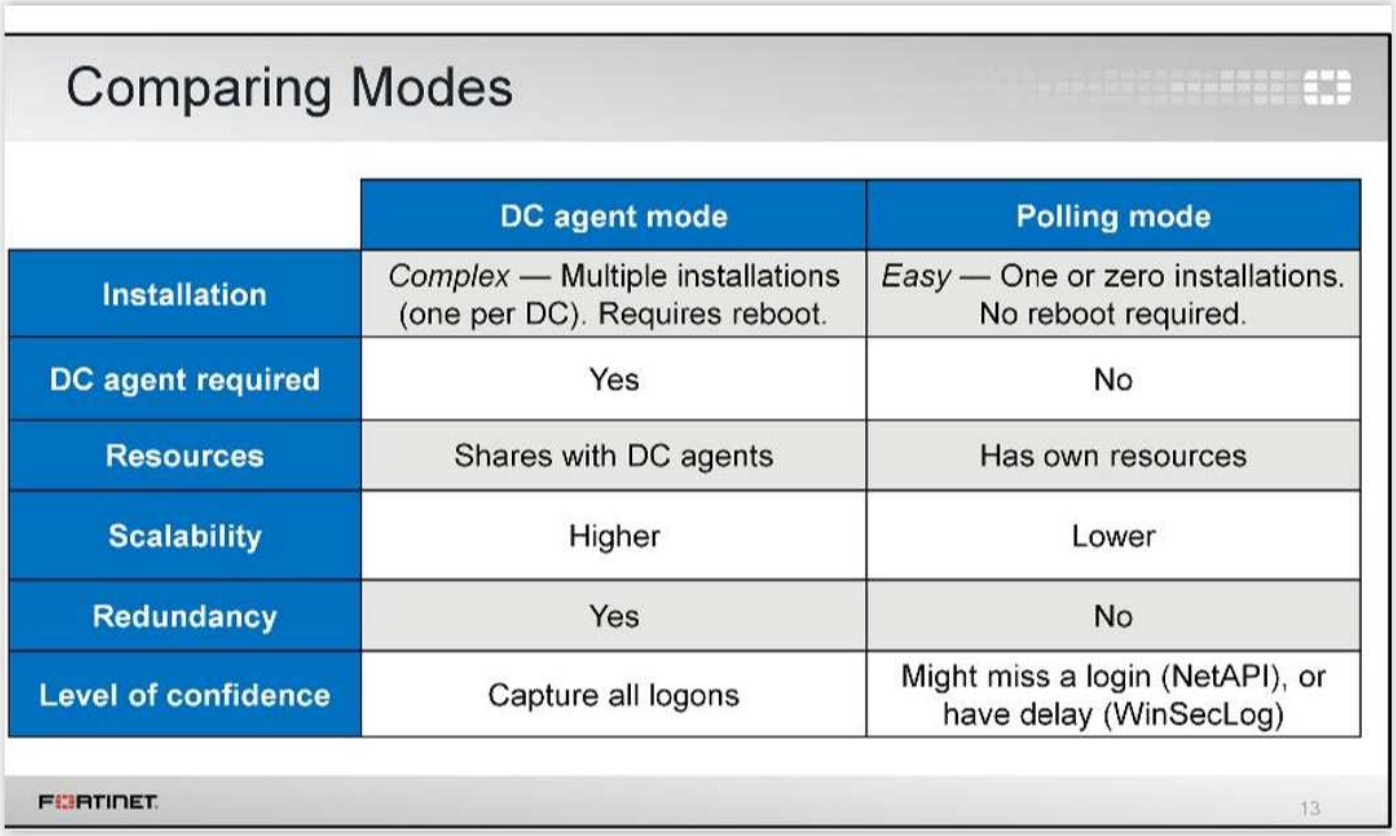
Explanation/Reference:

QUESTION 193
What are the advantages of FSSO DC mode over polling mode?

A. Redundancy in the collector agent.
B. Allows transparent authentication.
C. DC agents are not required in the AD domain controllers.
D. Scalability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference:

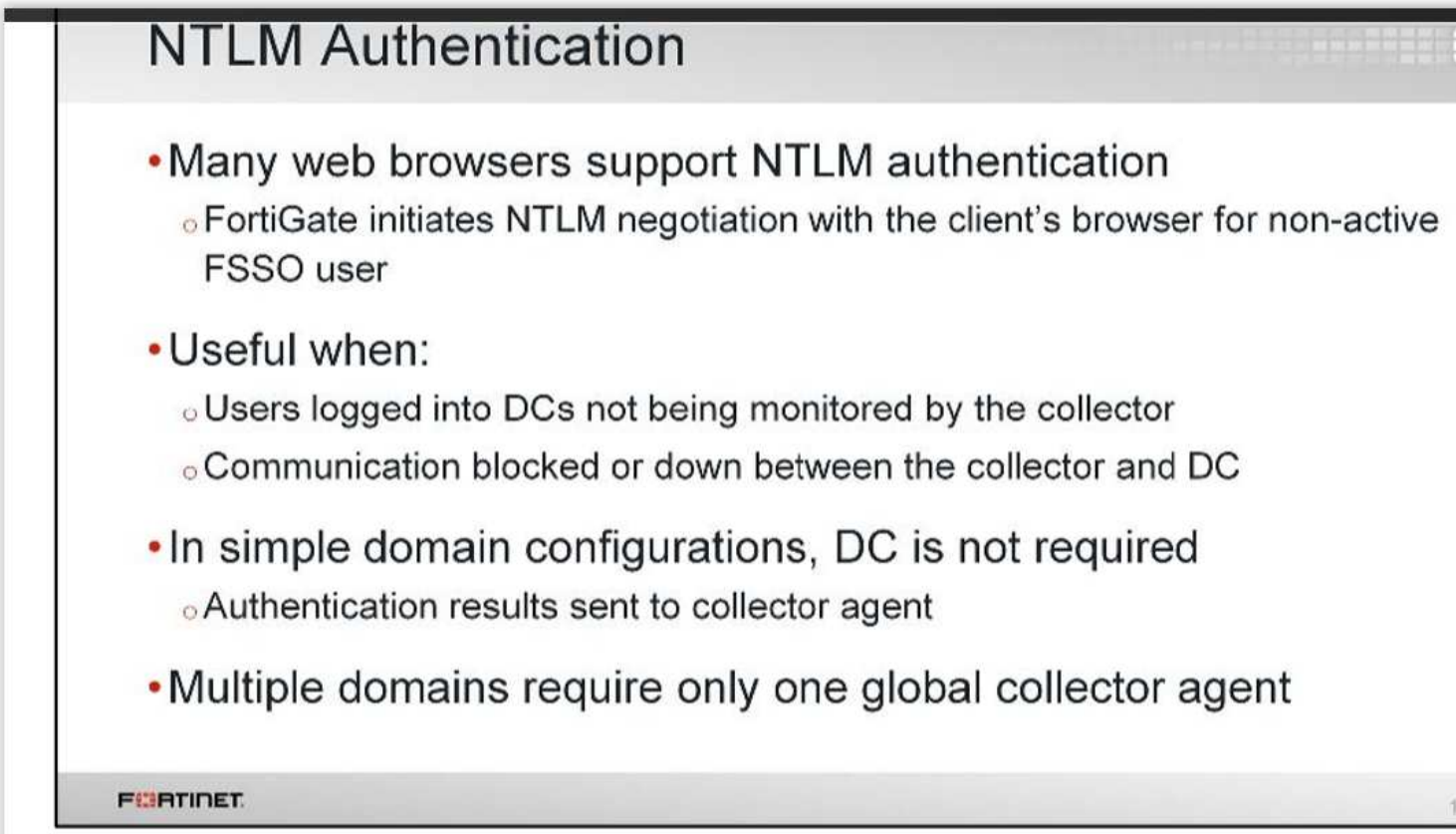


QUESTION 194
Which of the following statements are correct about NTLM authentication? (Choose three)

A. NTLM negotiation starts between the FortiGate device and the user's browser.
B. It must be supported by the user's browser.
C. It must be supported by the domain controllers.
D. It does not require a collector agent.
E. It does not require DC agents.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:



NTLM authentication does not require DC agents, but it is not fully invisible to users: they must
heir credentials during NTLM negotiation. NTLM authentication is a Microsoft-proprietary solut
it can only be implemented in a Windows network.

NTLM is most useful when users log in to DCs that, for some reason, can't be monitored by the
collector agent, or when there is a communication problem between the collector agent and on

QUESTION 195
Which of the following statements best describes how the collector agent learns that a user has logged off from the network?

A. The workstation fails to reply to the polls frequently done by the collector agent.
B. The DC agent captures the log off event from the event logs, which it forwards to the collector agent.
C. The work station notifies the DC agent that the user has logged off.
D. The collector agent gets the logoff events when polling the respective domain controller.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
Which of the following statements best describes the role of a DC agents in an FSSO DC?

A. Captures the login events and forward them to the collector agent.
B. Captures the user IP address and workstation name and forward that information to the FortiGate devices.
C. Captures the login and logoff events and forward them to the collector agent.
D. Captures the login events and forward them to the FortiGate devices.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
Which of the following FSSO modes must be used for Novell eDirectory networks?

A. Agentless polling
B. LDAP agent
C. eDirectory agent
D. DC agent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/1041/fortigate-authentication-40-mr3.pdf (page 140)

QUESTION 198
In a FSSO agentless polling mode solution, where must the collector agent be?

A. In any Windows server
B. In any of the AD domain controllers
C. In the master AD domain controller
D. The FortiGate device polls the AD domain controllers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

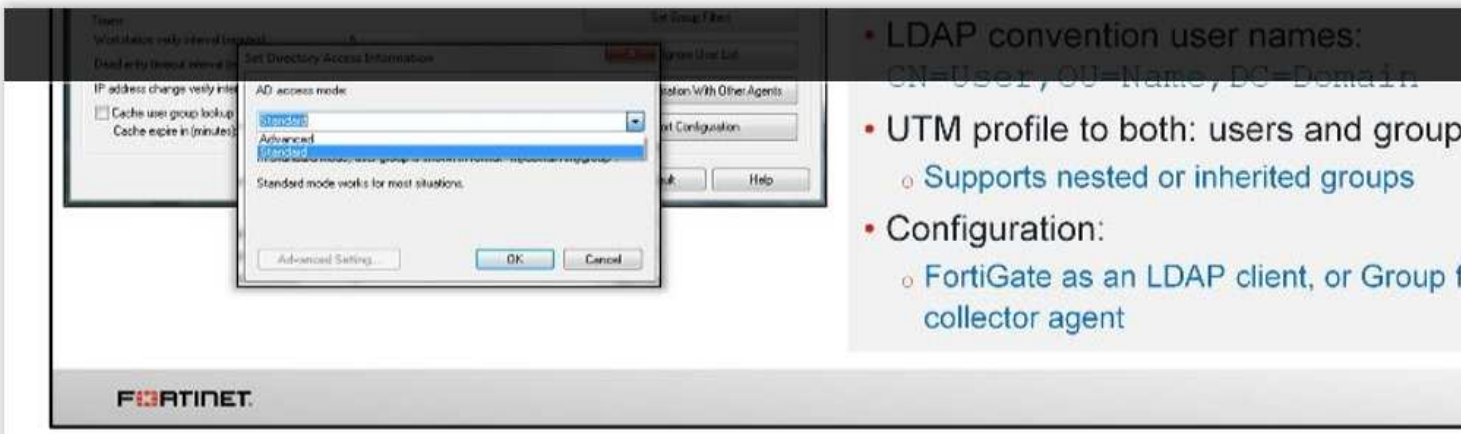
QUESTION 199
Which of the following statements are characteristics of a FSSO solution using advanced access mode? (Choose three.)

A. Protection profiles can be applied to both individual users and user groups
B. Nested or inherited groups are supported
C. Usernames follow the LDAP convention: CN=User, OU=Name, DC=Domain
D. Usernames follow the Windows convention: Domain\username
E. Protection profiles can be applied to user groups only.

Correct Answer: ABC
Section: (none)

Explanation

Explanation/Reference:
Explanation:



Another important FSSO setting is the AD access mode. You can set the AD access mod
Set Directory Access Information. It specifies how the collector agent accesses and co
user and user group information. There are two modes that can be used to access AD us
information: standard and advanced.

The main difference in both modes include the naming convention used:

- standard mode uses the Windows convention - NetBios: Domain\Username, while
- advanced mode uses the LDAP convention: `CN=User, OU=Name, DC=Domain.`

Also, advanced mode supports nested or inherited groups; that is, users can be members
subgroups that belong to monitored *parent* groups. Additionally, in advanced mode FortiG
apply protection profiles to individual users, user groups, and organizational units (OUs).

QUESTION 200
Which of the following FSSO agents are required for a DC agent mode solution? (Choose two.)

A. FSSO agent
B. DC agent
C. Collector agent
D. Radius server

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201
In a FSSO agent mode solution, how does the FSSO collector agent learn each IP address?

A. The DC agents get each user IP address from the event logs and forward that information to the collector agent
B. The collector agent does not know, and does not need, each user IP address. Only workstation names are known by the collector agent.
C. The collector agent frequently polls the AD domain controllers to get each user IP address.
D. The DC agent learns the workstation name from the event logs and DNS is then used to translate those names to the respective IP addresses.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
Which FSSO agents are required for a FSSO agent-based polling mode solution?

A. Collector agent and DC agents
B. Polling agent only
C. Collector agent only
D. DC agents only

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
Which of the following statements are true about Man-in-the-middle SSL Content Inspection? (Choose three.)

A. The FortiGate device “re-signs” all the certificates coming from the HTTPS servers
B. The FortiGate device acts as a sub-CA
C. The local service certificate of the web server must be installed in the FortiGate device
D. The FortiGate device does man-in-the-middle inspection.
E. The required SSL Proxy certificate must first be requested to a public certificate authority (CA).

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
Which of the following statements describe some of the differences between symmetric and asymmetric cryptography? (Choose two.)

A. In symmetric cryptography, the keys are publicly available. In asymmetric cryptography, the keys must be kept secret.

B. Asymmetric cryptography can encrypt data faster than symmetric cryptography
C. Symmetric cryptography uses one pre-shared key. Asymmetric cryptography uses a pair or keys
D. Asymmetric keys can be sent to the remote peer via digital certificates. Symmetric keys cannot

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205
Which of the following statements best describes what a Public Certificate Authority (CA) is?

A. A service that provides a digital certificate each time a user is authenticating
B. An entity that certifies that the information contained in a digital certificate is valid and true.
C. The FortiGate process in charge of generating digital certificates on the fly for SSL inspection purposes
D. A service that validates digital certificates for certificate-based authentication purposes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206
Which of the following statements are true about the SSL Proxy certificate that must be used for SSL Content Inspection? (Choose two.)

A. It cannot be signed by a private CA
B. It must have either the field “CA=True” or the filed “Key Usage=KeyCertSign”
C. It must be installed in the FortiGate device
D. The subject filed must contain either the FQDN, or the IP address of the FortiGate device

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
Which of the following statements are true about PKI users created in a FortiGate device? (Choose two.)

A. Can be used for token-based authentication
B. Can be used for two-factor authentication
C. Are used for certificate-based authentication
D. Cannot be members of user groups

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

Reference: http://docs.fortinet.com/uploaded/files/1937/fortigate-authentication-52.pdf (page 14)

QUESTION 208
Which of the following statements best describes what a Certificate Signing Request (CSR) is?

A. A message sent by the Certificate Authority (CA) that contains a signed digital certificate.
B. An enquiry submitted to a Certificate Authority (CA) to request a root CA certificate
C. An enquiry submitted to a Certificate Authority (CA) to request a signed digital certificate
D. An enquiry submitted to a Certificate Authority (CA) to request a Certificate Revocation List (CRL)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
Which of the following actions can be used to back up the keys and digital certificates in a FortiGate device? (Choose two.)

A. Taking a full backup of the FortiGate configuration
B. Uploading a PKCS#10 file to a USB drive
C. Manually uploading the certificate information to a Certificate authority (CA)
D. Uploading a PKCS#12 file to a TFTP server

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210
Which of the following statements must be true for a digital certificate to be valid? (Choose two.)

A. It must be signed by a “trusted” CA
B. It must be listed as valid in a Certificate Revocation List (CRL)
C. The CA field must be “TRUE”
D. It must be still within its validity period

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211
Of the following information, what can be recorded by a Data Leak Prevention sensor configured to do a summary archiving? (Choose three.)

A. Visited URL (for the case of HTTP traffic)
B. Sender email address (for the case of SMTP traffic)
C. Recipient email address (for the case of SMTP traffic)

D. Attached file (for the case of SMTP traffic)
E. Email body (for the case of SMTP traffic)

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/1084/fortigate-loggingreporting-509.pdf

QUESTION 212
Which of the following statements best describes what the Document Fingerprinting feature is for?

A. Protects sensitive documents from leakage
B. Appends a fingerprint signature to all documents sent by users
C. Appends a fingerprint signature to all the emails sent by users
D. Validates the fingerprint signature in users' emails

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/2181/fortigate-security-profiles-guide-524.pdf (133)

QUESTION 213
Which action is taken by the FortiGate device when a file matches more than one rule in a Data Leak Prevention sensor?

A. The actions specified by the rule that most specifically matched the file
B. The actions specified in the first rule from top to bottom
C. All actions specified by all the matched rules.
D. The actions specified in the rule with the higher priority number

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214
Which of the following statements are true regarding DLP File Type Filtering? (Choose two.)

A. Filters based on file extension
B. Filters based on fingerprints
C. Filters based on file content
D. File types are hard coded in the FortiOS

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: http://kb.fortinet.com/kb/documentLink.do?externalID=FD35108

QUESTION 215
Which of the following actions that can be taken by the Data Leak Prevention scanning? (Choose three.)

A. Block
B. Reject
C. Tag
D. Log only
E. Quarantine IP address

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/2181/fortigate-security-profiles-guide-524.pdf (131)

QUESTION 216
Which of the following network protocols can be inspected by the Data Leak Prevention scanning? (Choose three.)

A. SMTP
B. HTTP-POST
C. AIM
D. MAPI
E. ICQ

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 217
What types of troubleshooting can you do when uploading firmware? (Choose two.)

A. Investigate corrupted firmware
B. Investigate current runtime state
C. Investigate damaged hardware
D. Investigate configuration history

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218
Which are outputs for the command 'diagnose hardware deviceinfo nic'? (Choose two.)

A. ARP cache
B. Physical MAC address
C. Errors and collisions

D. Listening TCP ports

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/1067/fortigate-troubleshooting-40-mr2.pdf (page 28)

QUESTION 219
In FortiOS session table output, what is the correct 'proto_state' number for an established, non-proxied TCP connection?

A. 00
B. 11
C. 01
D. 05

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220
Which commands are appropriate for investigating high CPU? (Choose two.)

A. diag sys top
B. diag hardware sysinfo mem
C. diag debug flow
D. get system performance status

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/1067/fortigate-troubleshooting-40-mr2.pdf (109)

QUESTION 221
What are examples of correct syntax for the session table diagnostics command? (Choose two.)

A. diagnose sys session filter clear
B. diagnose sys session src 10.0.1.254
C. diagnose sys session filter
D. diagnose sys session filter list dst.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docs.fortinet.com/uploaded/files/1067/fortigate-troubleshooting-40-mr2.pdf (33. 34)

QUESTION 222

Which TCP states does the global setting 'tcp-half-open-timer' applies to? (Choose two.)

A. SYN SENT
B. SYN & SYN/ACK
C. FIN WAIT
D. TIME WAIT

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223
In FortiOS session table output, what are the two possible 'proto_state' values for a UDP session? (Choose two.)

A. 00
B. 11
C. 01
D. 05

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
Which statement best describes what the FortiGate hardware acceleration processors main task is?

A. Offload traffic processing tasks from the main CPU.
B. Offload management tasks from the main CPU.
C. Compress and optimize the network traffic.
D. Increase maximum bandwidth available in a FortiGate interface.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

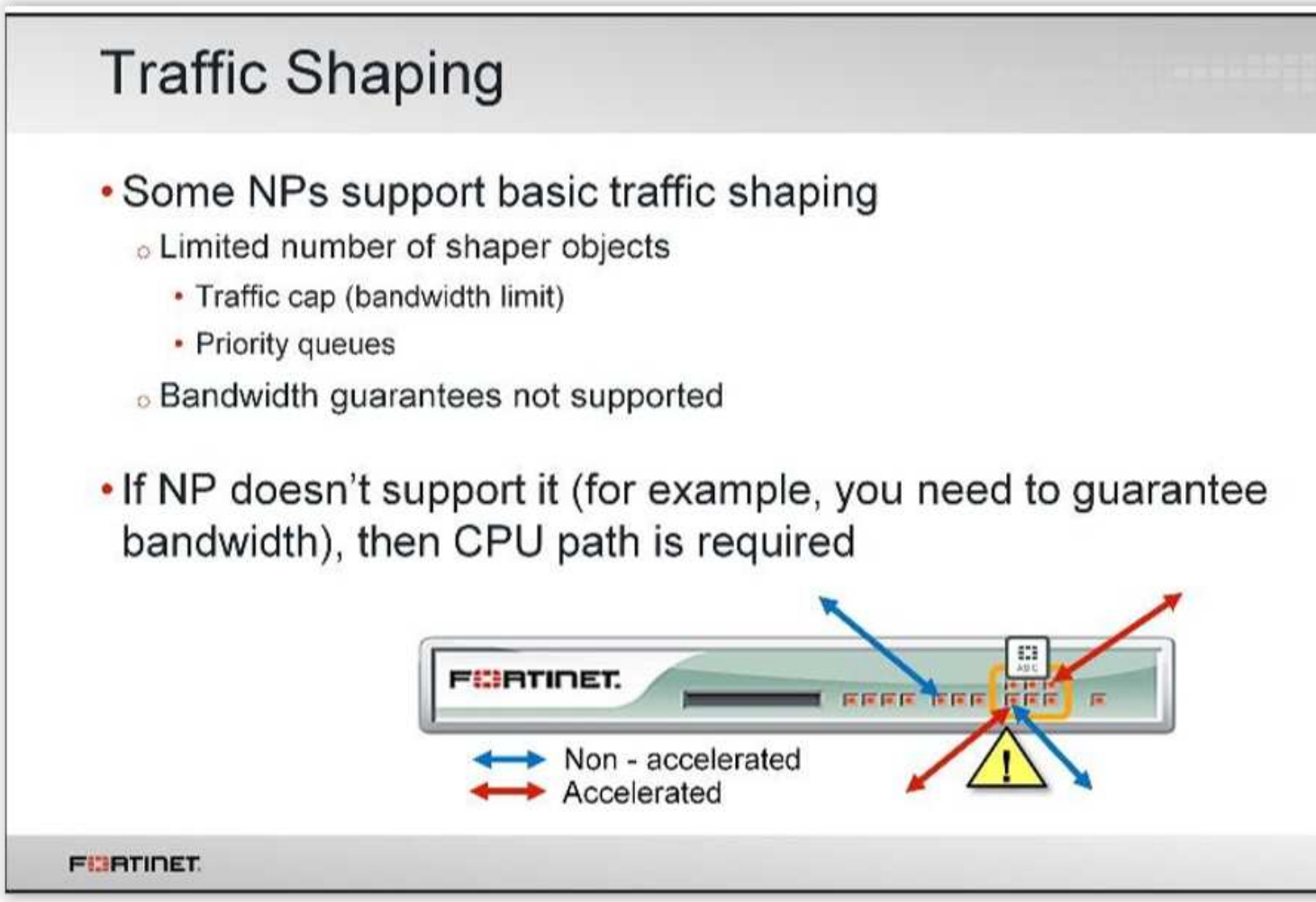
QUESTION 225
Which of the following traffic shaping functions can be offloaded to a NP processor? (Choose two.)

A. Que prioritization
B. Traffic cap (bandwidth limit)
C. Differentiated services field rewriting
D. Guarantee bandwidth

Correct Answer: AB
Section: (none)

Explanation

Explanation/Reference:
Explanation:



QUESTION 226
Which of the following statements best describe the main requirements for a traffic session to be offload eligible to an NP6 processor? (Choose three.)

A. Session packets do NOT have an 802.1Q VLAN tag.
B. It is NOT multicast traffic.
C. It does NOT require proxy-based inspection.
D. Layer 4 protocol must be UDP, TCP, SCTP or ICMP.
E. It does NOT require flow-based inspection.

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227

Which statement best describes what a Fortinet System on a Chip (SoC) is?

A. Low-power chip that provides general purpose processing power
B. Chip that combines general purpose processing power with Fortinet's custom ASIC technology
C. Light-version chip (with fewer features) of an SP processor
D. Light-version chip (with fewer features) of a CP processor

Correct Answer: B
Section: (none)
Explanation

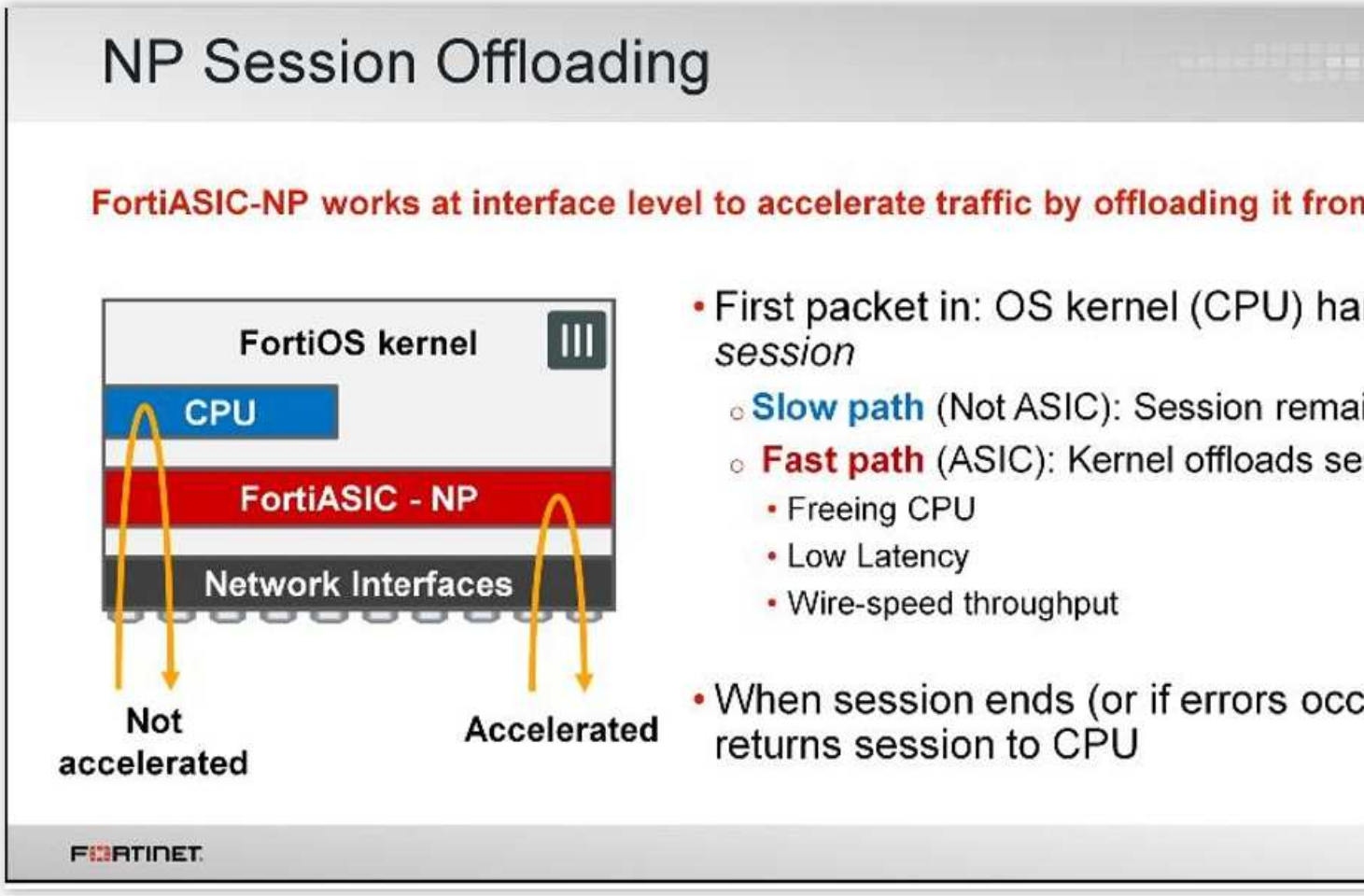
Explanation/Reference:
Reference: http://www.fortinet.com/press_releases/100713.html

QUESTION 228
Which of the following statements are true regarding traffic accelerated by an NP processor? (Choose two.)

A. TCP SYN packets are always handled by the NP Processor
B. The initial packets go to the NP Processor, where a decision is taken on if the session can be offloaded or not.
C. Packets for a session termination are always handled by the CPU.
D. The initial packets go to the CPU, where a decision is taken on if the session can be offloaded or not.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:



QUESTION 229
Which statement best describes the objective of the SYN proxy feature available in SP processors?

A. Accelerate the TCP 3-way handshake
B. Collect statistics regarding traffic sessions
C. Analyze the SYN packet to decide if the new session can be offloaded to the SP processor
D. Protect against SYN flood attacks.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://kb.fortinet.com/kb/viewContent.do?externalId=FD33596

QUESTION 230
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 have not authenticated.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231
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.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232
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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 234
What capabilities can a FortiGate provide? (Choose three)

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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235
For data leak prevention, which statement 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.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 236
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 a 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 237
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 238
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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 239
What 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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 240
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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241
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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242
What is IPsec Perfect Forwarding Secresy (PFS)?

A. A phase-1 setting that allows the use of symmetric encryption.
B. A phase-2 setting that forces the use of Diffie Helman each time new phase-2 SA keys must be generated.
C. A 'key-agreement' protocol.
D. A 'security-assotiation- agreement' protocol.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 243
An administrator wants to form 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. Configure the 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

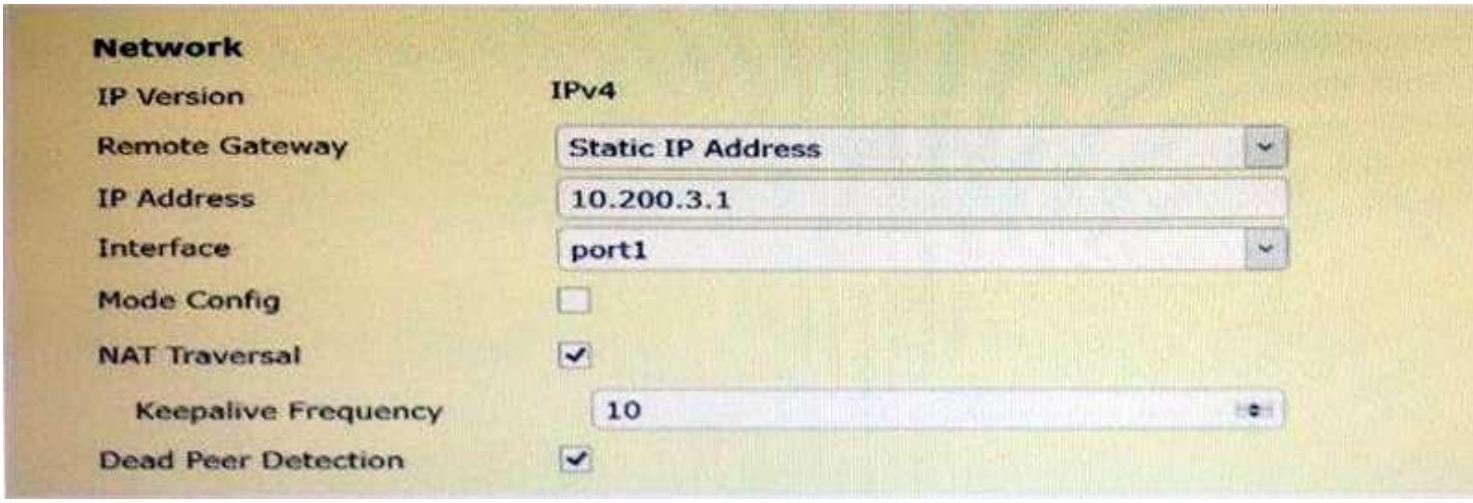
QUESTION 244
Which two statements are true about IPsec VPNs and SSL VPNs? (Choose two.)

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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245
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 is 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 is 10.200.3.1

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247
What are the requirements for a HA cluster to maintain TCP connections after device or link failover? (Choose two.)

A. Enable session pick-up.
B. Enable override.
C. Connections must be UDP or ICMP.
D. Connections must not be handled by a proxy.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 248
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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 249
Which of the following regular expression patterns makes the terms “confidential data” case insensitive?

A. [confidential data]
B. /confidential data/i
C. i/confidential data/
D. “confidential data”

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 250
A FortiGate is configured with multiple VDOMs. An administrative account on the device is assigned to the administrator profile *prof_admin* and to the virtual domain *root*.
Which of the following settings will this administrator be able to configure? (Choose two.)

A. Firewall addresses
B. DHCP servers
C. FortiGuard Distribution Network configuration.
D. System hostname.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

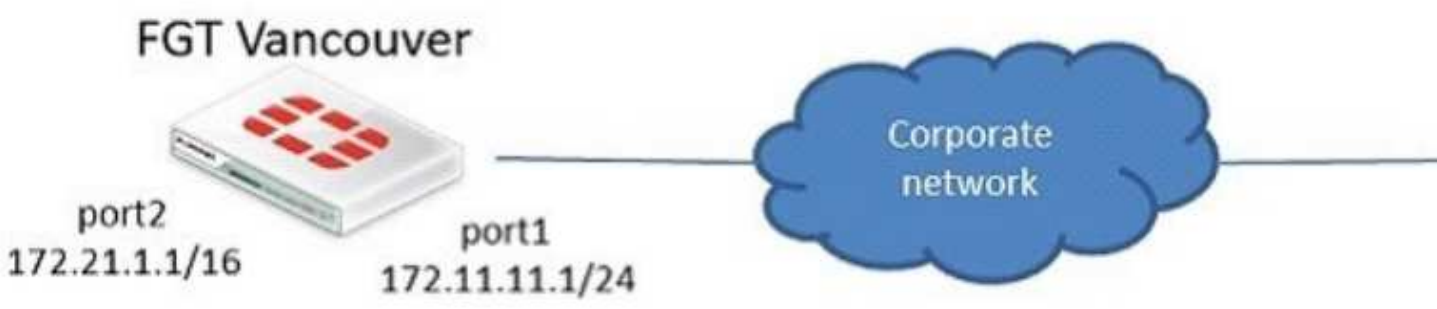
QUESTION 252
Which statement correctly describes the output of the command `diagnose ips anomaly list`?

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253
Examine the exhibit; then answer the question below.



The Vancouver FortiGate 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 priority 0
```

```
      set device port1
      set gateway 172.11.12.1
next
```

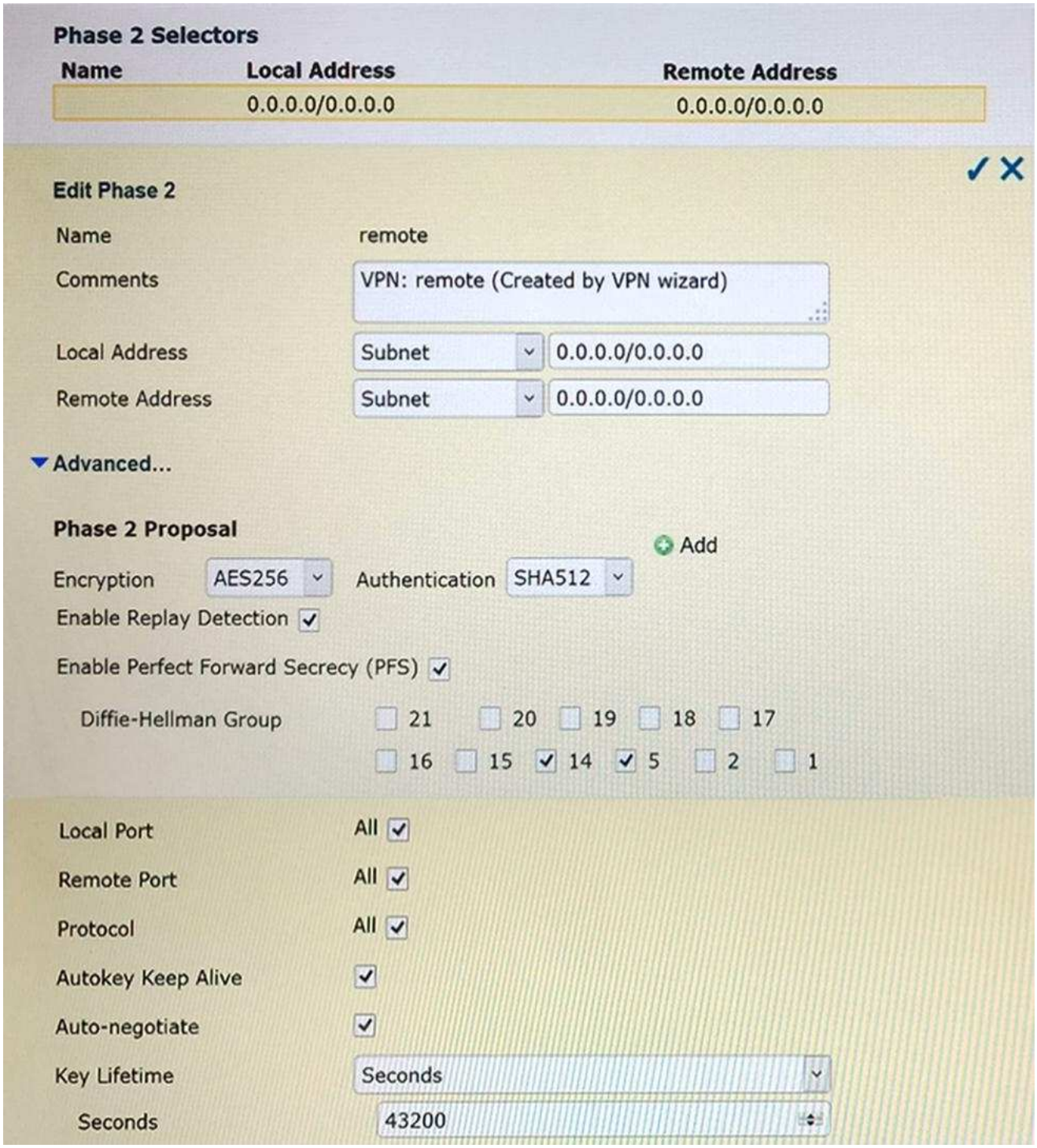
Since this change, the new static route is NOT showing up in the routing table. Given the information provided, which of the following describes the cause of this problem?

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 254



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.

Correct Answer: AB
Section: (none)

Explanation

Explanation/Reference:

QUESTION 255
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256
Which IP packets can be hardware-accelerated by a NP6 processor? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

Reference: http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-hardware-acceleration-52/NP6.htm

QUESTION 257
Which statements are true regarding the factory default configuration for low-end models? (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.

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 258
Which web filtering inspection mode inspects DNS traffic?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 259
In transparent mode, forward-domain is a CLI setting associated with _____ .

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260
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.

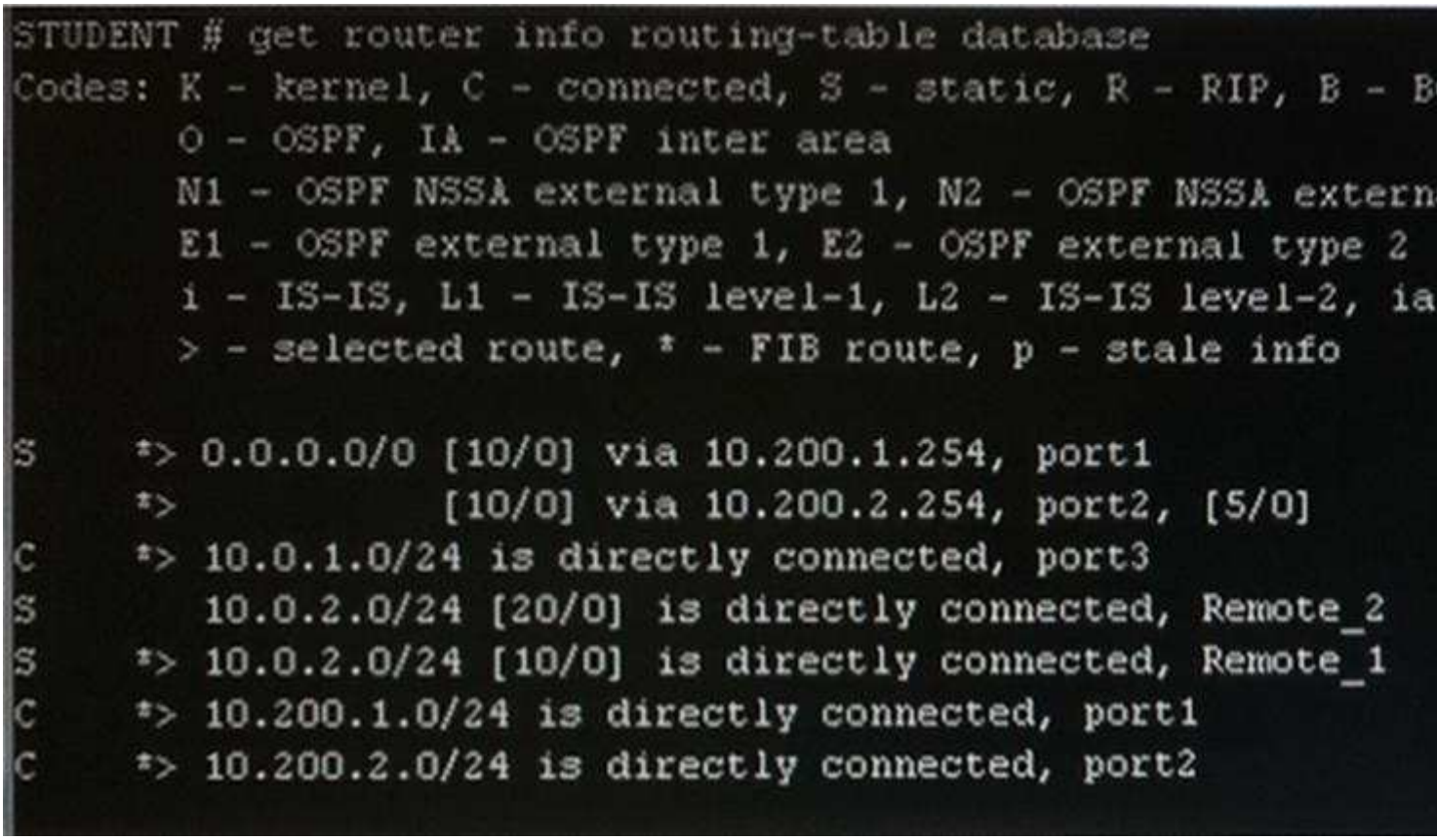
C. It is an idle timeout. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user's source MAC.

D. It is a hard timeout. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261
Review the output of the command `get router info routing-table database` shown in the exhibit below; then answer the question following it.



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

A. There will be six routes in the routing table.

B. There will be seven routes in the routing table.

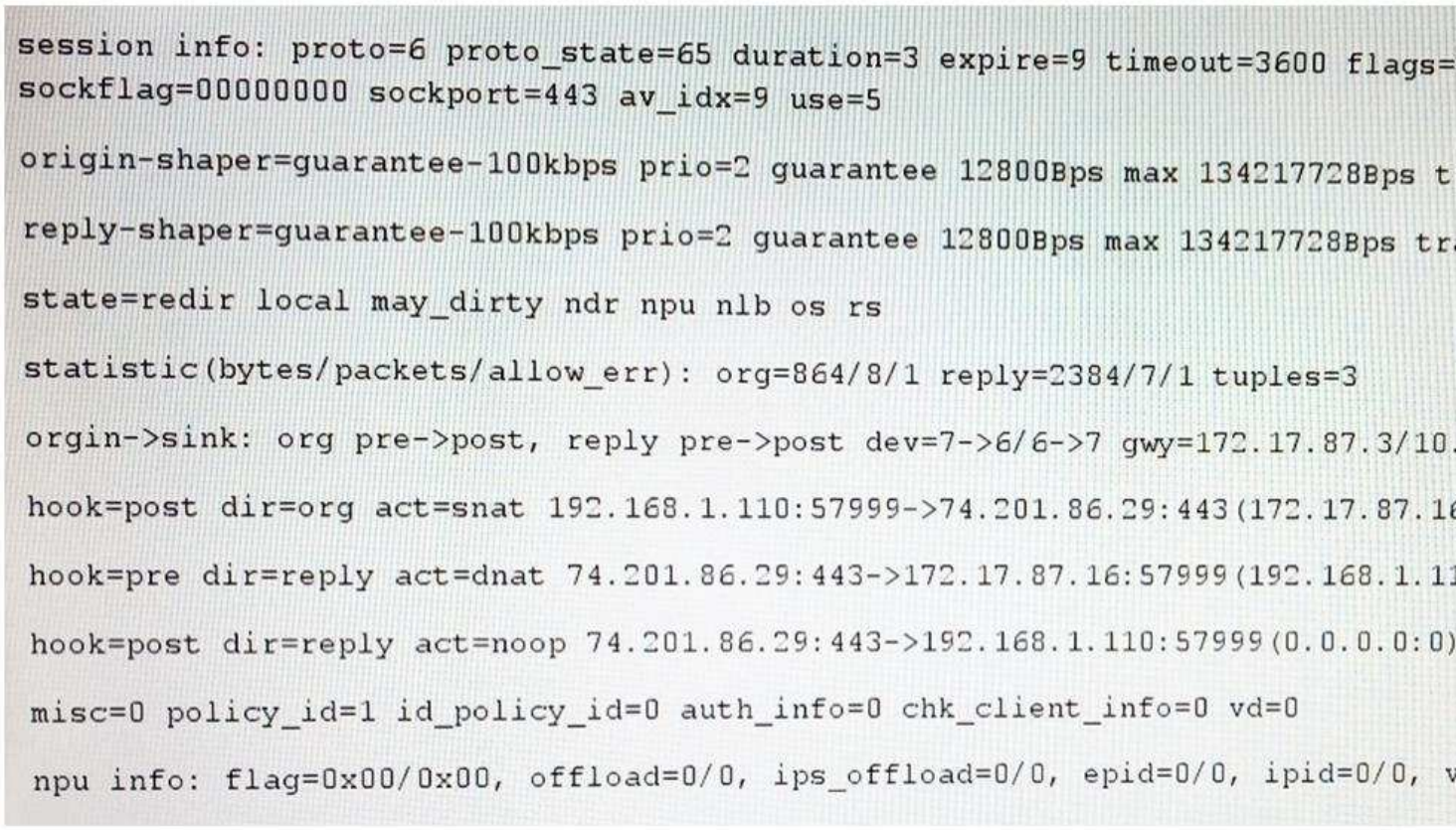
C. There will be two default routes in the routing table.

D. There will be two routes for the 10.0.2.0/24 subnet in the routing table.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 262
Examine the following output from the `diagnose sys session list` command:



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 address 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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 263
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:

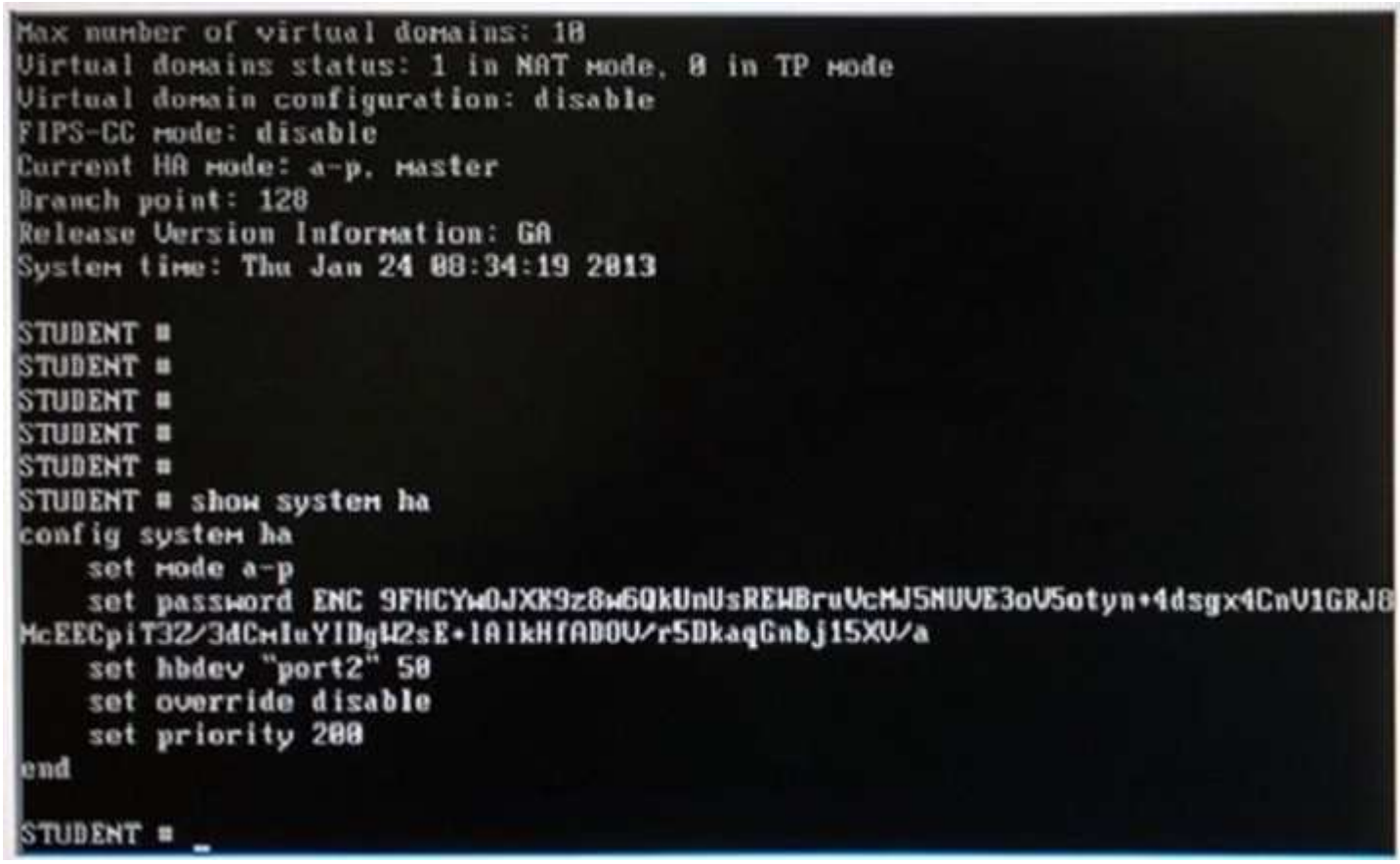
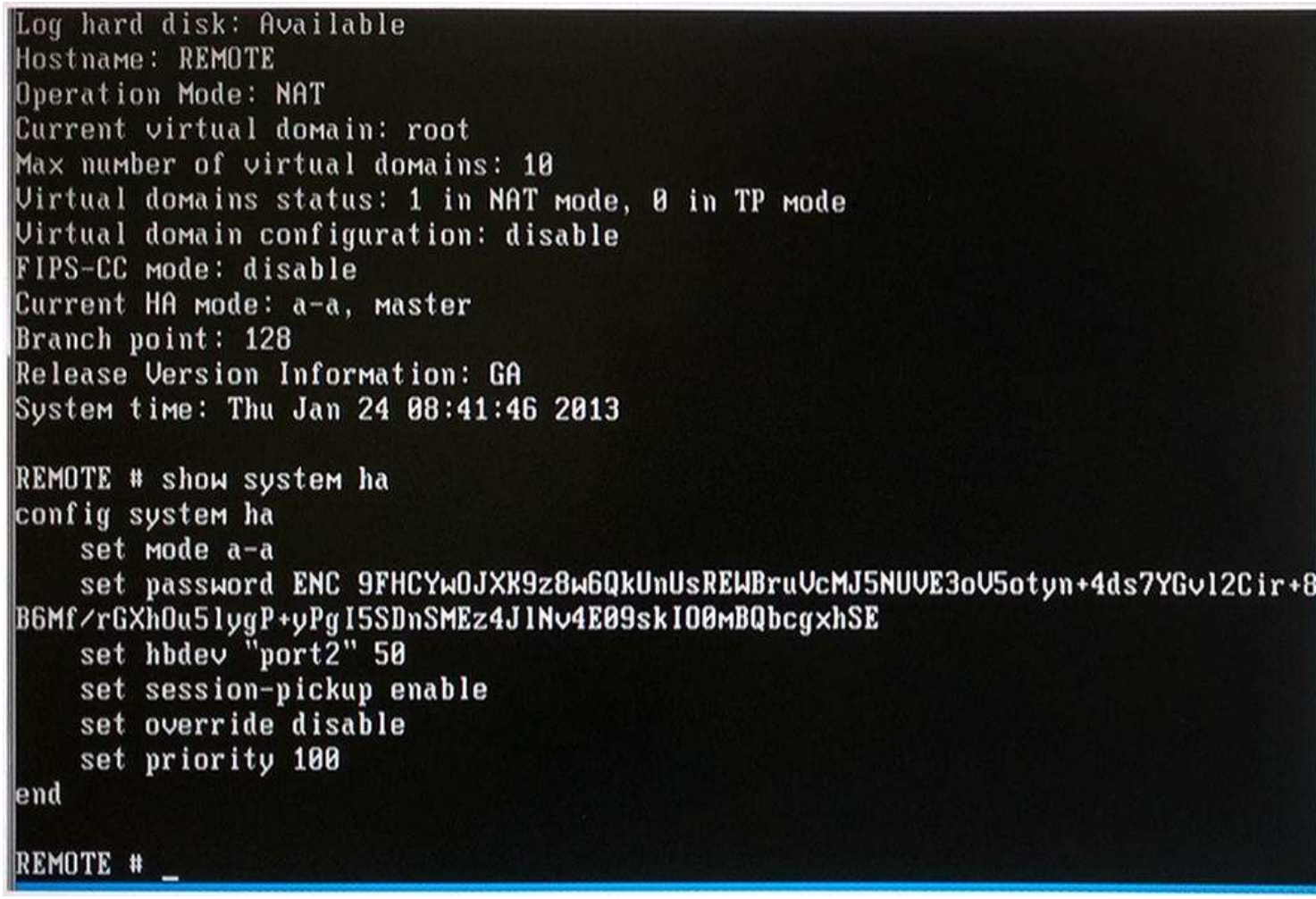


Exhibit B:



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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 264
Which statements are correct regarding application control? (Choose two.)

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

Correct Answer: AC

Section: (none)
Explanation

Explanation/Reference:

QUESTION 265
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 security profile, which must be applied to a firewall policy.
D. Enabling virus scanning in a security profile enables virus protection for all traffic flowing through the FortiGate.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 266
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 267
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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

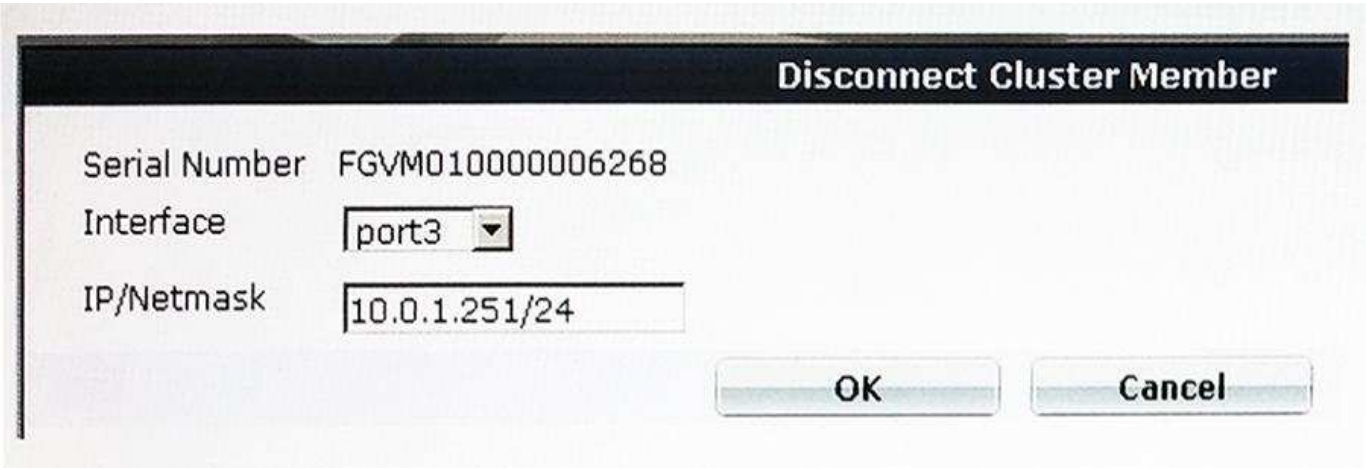
QUESTION 268
Which statement is in advantage of using a hub and spoke IPsec VPN configuration instead of a fully-meshed set of IPsec tunnels?

A. Using a hub and spoke topology provides full redundancy.
B. Using a hub and spoke topology requires fewer tunnels.
C. Using a hub and spoke topology uses stronger encryption protocols.
D. Using a hub and spoke topology requires more routes.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 269
The exhibit shows the Disconnect Cluster Member command in a FortiGate unit that is part of a HA cluster with two HA members.



What is the effect of the Disconnect Cluster Member command as given in the exhibit. (Choose two.)

A. Port3 is configured with an IP address management access.
B. The firewall rules are purged on the disconnected unit.
C. The HA mode changes to standalone.
D. The system hostname is set to the unit serial number.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

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?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 271
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.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 272
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 273
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
```

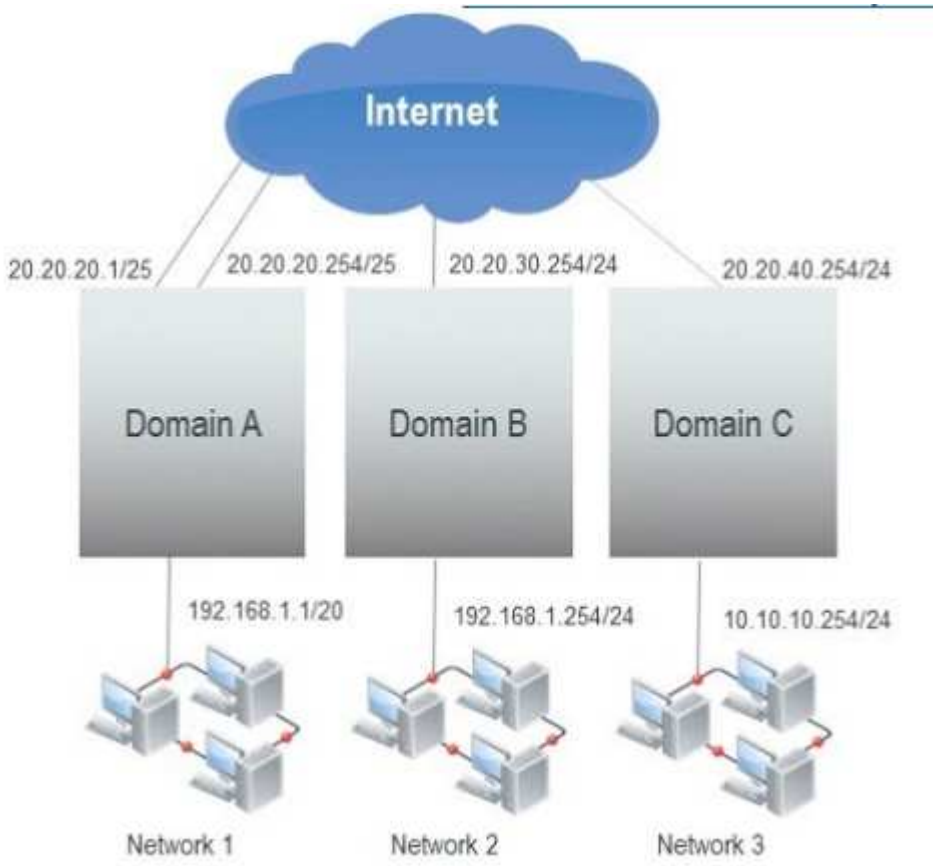
Which of the following statements correctly describes the static routing configuration provided above?

A. The FortiGate evenly shares the traffic to 172.20.168.0/24 through both routes.
B. The FortiGate shares 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 sends 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 274
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.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 275
Review the IPsec diagnostics output of the command diagnose 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 582af59d71635b835c92086878e0e3f3fe31ba1dfd88ff83ca9bab1ed66ac325e
       ah=sha1 key=20 0d951e62a1bcb63232df6d0fb86df49ab714f53b
  enc: spi=9293e7d5 esp=aes key=32 eeeecacf3a58161f3390fa612b794c776654c86aef51fbc7542906223d56ebb3
       ah=sha1 key=20 09eaa3085bc30a59091f182eb3d11550385b8304
```

Which statements is correct regarding this output?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 276
Which Fortinet products & features could be considered part of a comprehensive solution to monitor and prevent the leakage of sensitive data?

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.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 277
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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 278
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 279
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 280
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 281
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 slave unit?

A. Request: internal host; slave FortiGate; master FortiGate; Internet; web server.
B. Request: internal host; slave FortiGate; Internet; web server.
C. Request: internal host; slave FortiGate; master FortiGate; Internet; web server.
D. Request: internal host; master FortiGate; slave FortiGate; Internet; web server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 282
A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, they are not being received.
Which of the following statements are possible reasons for this?

A FortiGate 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 and no override push IP is configured.
D. The FortiGate unit is in Transparent mode which does not support push updates.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 283
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 device
C. Push updates from the FortiGuard Distribution Network.
D. execute fortiguard-AV-AS command from the CLI.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 284
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 285
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 286
When firewall policy authentication is enabled, which protocols can trigger an authentication challenge? (Choose two.)

A. SMTP
B. SSH
C. HTTP
D. FTP
E. SCP

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 287
A client can create a secure connection to a FortiGate device 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 288
A client can establish a secure connection to a corporate network 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. Client software is required to be able to use a tunnel mode SSL VPN.
C. Users attempting to create a tunnel mode SSL VPN connection must be authenticated by at least one SSL VPN policy.
D. The source IP address used by the client for the tunnel mode SSL VPN is assigned by the FortiGate unit.

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 289
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?

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.

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 290
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 to the client causes a host route to be added to the FortiGate unit's kernel routing table.
C. A route back to the SSLVPN IP pool is automatically created on the FortiGate unit.
D. The FortiGate unit adds a route based upon the destination address in the SSL VPN firewall policy.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 291
An end user logs into the full-access SSL VPN portal and selects the Tunnel Mode option by clicking on the "Connect" button. The administrator has enabled split tunneling.

Given that the user authenticates against the SSL VPN policy shown in the image below, which statement below identifies the route that is added to the client's routing table.

A. A route to destination matching the `WIN2K3' address object.
B. A route to the destination matching the `all' address object.
C. A default route.
D. No route is added.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 292
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 293
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?

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 294
Which of the following statements are correct regarding logging to memory on a FortiGate unit?

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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 295
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

Correct Answer: ABCDE
Section: (none)
Explanation

Explanation/Reference:

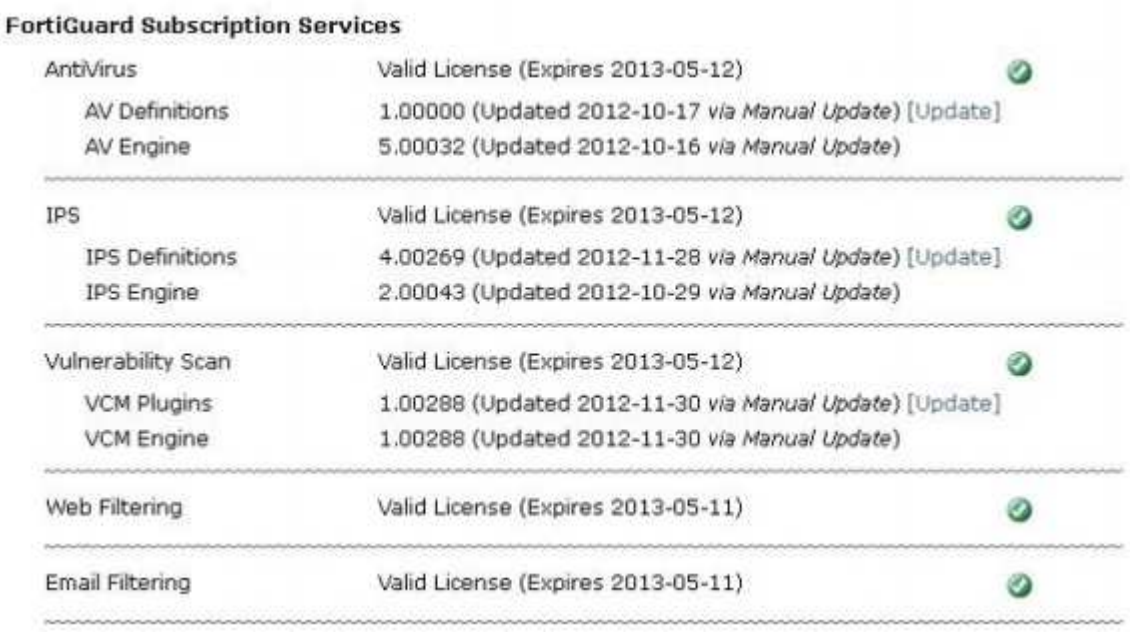
QUESTION 296
Which of the following email spam filtering features is NOT supported on a FortiGate unit?

A. Multipurpose Internet Mail Extensions (MIME) Header Check
B. HELO DNS Lookup
C. Greylisting
D. Banned Word

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 297
Examine the exhibit shown below; then answer the question following it.



Which of the following statements best 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 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 298
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.

Exhibit A

Exhibit B:

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 the sender will receive a failed delivery message.
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 299
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?

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 accommodate any number of cached queries.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 300
Which of the following Fortinet products can receive updates from the FortiGuard Distribution Network?

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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 301
How can DLP file filters be configured to detect Office 2010 files?

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"

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference: