Fortinet

Exam Questions NSE4

Fortinet Network Security Expert 4 Written Exam (400)

NEW QUESTION 1
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 authenticat
B. Traffic from the user Student will be allowed by the policy #1. Traffic from any other user will be allowed by the policy #2.
C. User is not prompted to authenticat
D. The connection is allowed by the proxy policy #2.
E. User is not prompted to authenticat
F. The connection will be allowed by the proxy policy #1.
G. User is prompted to authenticat
H. Only traffic from the user Student will be allowe
I. Traffic from any other user will be blocked.

Answer: D

NEW QUESTION 2
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

Answer: BC

NEW QUESTION 3
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.

Answer: B

NEW QUESTION 4
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.

Answer: B

NEW QUESTION 5
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.

Answer: B

NEW QUESTION 6
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 configuratio
B. 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.
C. No settings are preserve
D. You must completely reconfigure.
E. No settings are preserve
F. After the upgrade, you must upload a configuration backup fil
G. FortiOS will ignore any commands that are not valid in the new O
H. In those cases, you must reconfigure settings that are not compatible with the new firmware.
I. You must use FortiConverter to convert a backup configuration file into the syntax required by the new FortiOS, then upload it to FortiGate.

Answer: A

NEW QUESTION 7
For traffic that does match any configured firewall policy, what is the default action taken by the FortiGate?

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

Answer: C

NEW QUESTION 8
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.

Answer: A

NEW QUESTION 9
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.

Answer: C

NEW QUESTION 10
Which statements are correct for port pairing and forwarding domains? (Choose two.)

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

Answer: AD

NEW QUESTION 10
What methods can be used to deliver the token code to a user that is configured to use two-factor authentication? (Choose three.)

A. Browser pop-up window.
B. FortiToken.
C. Email.

D. Code books.
E. SMS phone message.

Answer: BCE

NEW QUESTION 12
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

Answer: ABD

NEW QUESTION 13
Which statements are correct regarding virtual domains (VDOMs)? (Choose two)

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

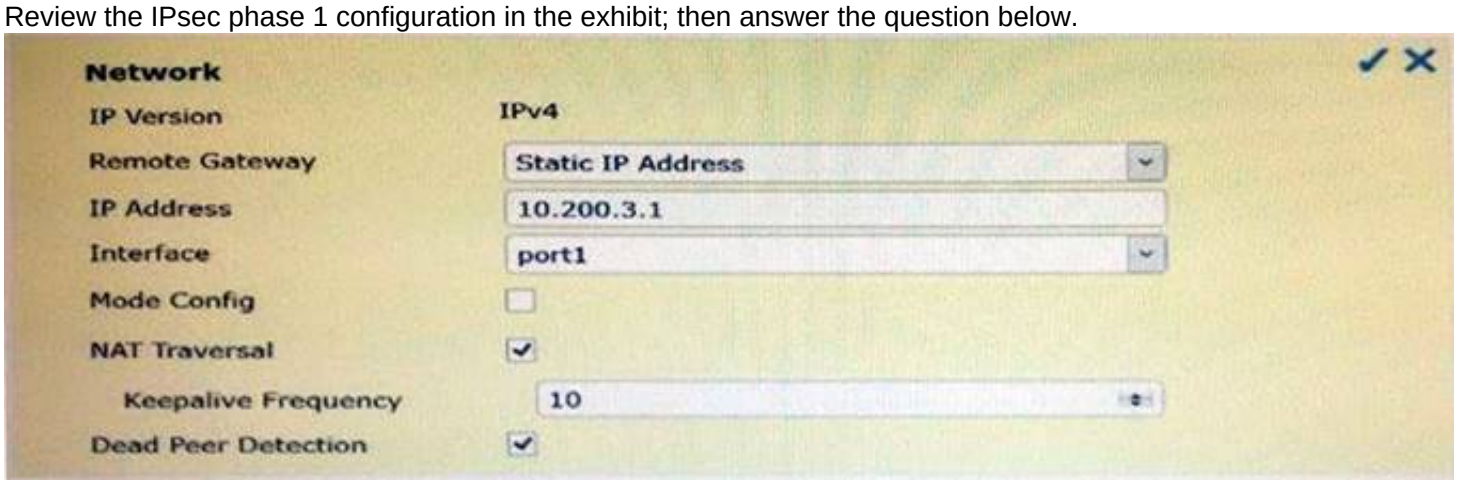
Answer: BC

NEW QUESTION 15
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.

Answer: D

NEW QUESTION 17
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

Answer: AC

NEW QUESTION 21
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

Answer: ABC

NEW QUESTION 24
Which antivirus inspection mode must be used to scan SMTP, FTP, POP3 and SMB protocols?

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

D. Man-in-the-middle.

Answer: C

NEW QUESTION 26
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.

Answer: D

NEW QUESTION 29
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.

Answer: C

NEW QUESTION 32
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 typ
C. The body section layout changes depending on the log type.
D. Some log types include multiple body sections.
E. Some log types do not include a body section.

Answer: B

NEW QUESTION 36
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)

Answer: ACE

NEW QUESTION 39
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.

Answer: C

NEW QUESTION 44
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

Answer: CDE

NEW QUESTION 47
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.

Answer: C

NEW QUESTION 49
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. There are no hub locations in a partial mesh.

Answer: BC

NEW QUESTION 50
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.

Answer: B

NEW QUESTION 52
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 application
B. Configured DLP to block HTTP GET request with credit card numbers.
C. Enable IPS signatures for Linux servers with HTTP, TCP and SSL protocols and Apache application
D. Configure DLP to block HTTP GET with credit card number
E. Also configure a DoS policy to prevent TCP SYn floods and port scans.
F. Non
G. FortiGate 60D is a desktop model, which does not support IPS.
H. Enable IPS signatures for Linux and windows servers with FTP, HTTP, TCP, and SSL protocols and Apache and PHP applications.

Answer: D

NEW QUESTION 56
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.

Answer: CD

NEW QUESTION 61
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.

Answer: D

NEW QUESTION 63
Which of the following are possible actions for static URL filtering? (Choose three.)

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

Answer: ABC

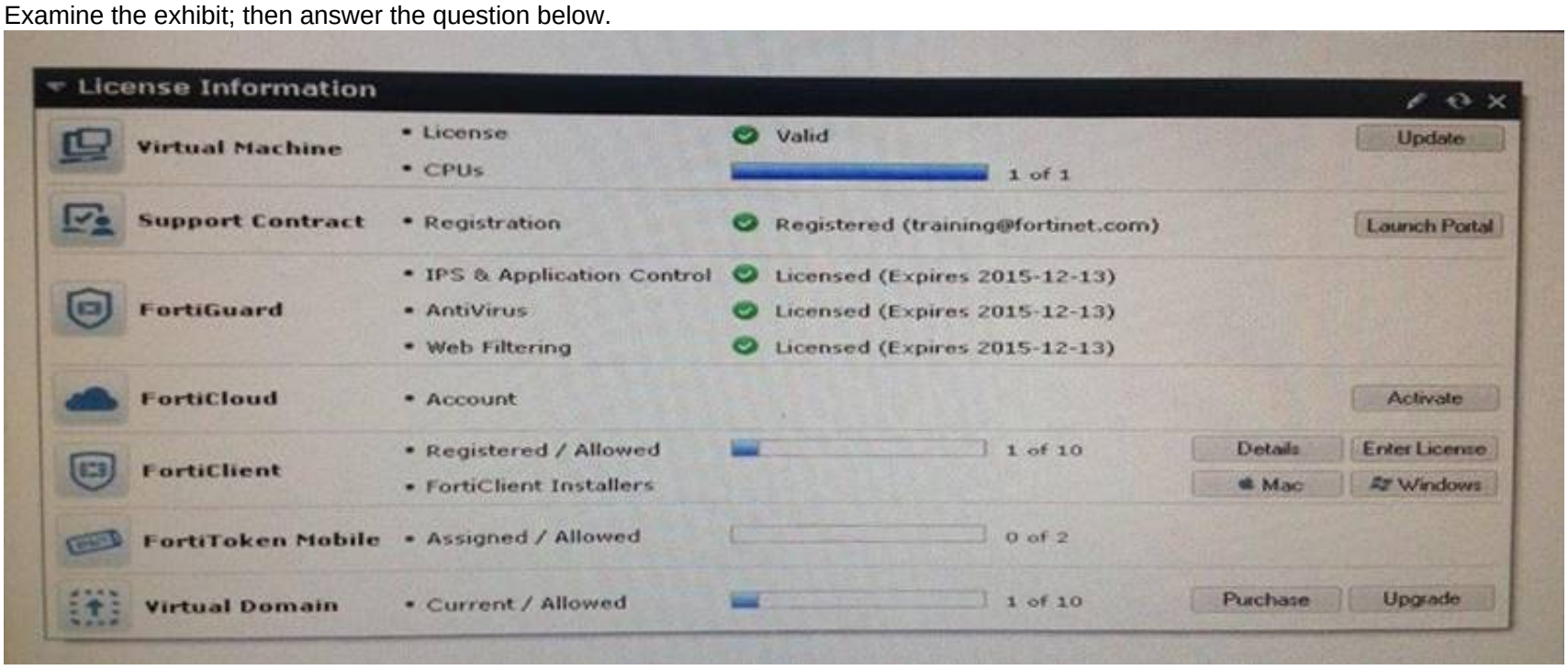
NEW QUESTION 65
Which statement describes what the CLI command diagnose debug authd fsso list is used for?

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.

Answer: B

NEW QUESTION 70
Examine the exhibit; then answer the question below.



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

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

Answer: D

NEW QUESTION 71
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

Answer: CD

NEW QUESTION 76
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.

Answer: D

NEW QUESTION 77
Which two statements are true about IPsec VPNs and SSL VPNs? (Choose two.)

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

Answer: AD

NEW QUESTION 79
Examine the following FortiGate web proxy configuration; then answer the question below:
config web-proxy explicit
set pac-file-server-status enable set pac-file-server-port 8080
set pac-file-name wpad.dat end
Assuming that the FortiGate proxy IP address is 10.10.1.1, which URL must an Internet browser use to download the PAC file?

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

D. http://10.10.1.1:8080/wpad.dat

Answer: D

NEW QUESTION 83
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

Answer: CDE

NEW QUESTION 85
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

Answer: A

NEW QUESTION 88
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.

Answer: AD

NEW QUESTION 92
Which two web filtering inspection modes inspect the full URL? (Choose two.)

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

Answer: BC

NEW QUESTION 93
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 NP
C. When the NPU sees the traffic, it determines by itself whether it can process the traffic
D. Once offloaded, unless there are errors, the NP forwards all subsequent packet
E. The CPU does not process them.
F. 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.
G. Sessions for policies that have a security profile enabled can be NP offloaded.

Answer: ACD

NEW QUESTION 95
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 addres
C. Only workstation names are known by the collector agent.
D. The collector agent frequently polls the AD domain controllers to get each user IP address.
E. 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.

Answer: D

NEW QUESTION 97
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.

Answer: D

NEW QUESTION 98
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

Answer: CD

NEW QUESTION 102
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.

Answer: BD

NEW QUESTION 107
Which statements are true regarding the factory default configuration? (Choose three.)

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

Answer: BDE

NEW QUESTION 109
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

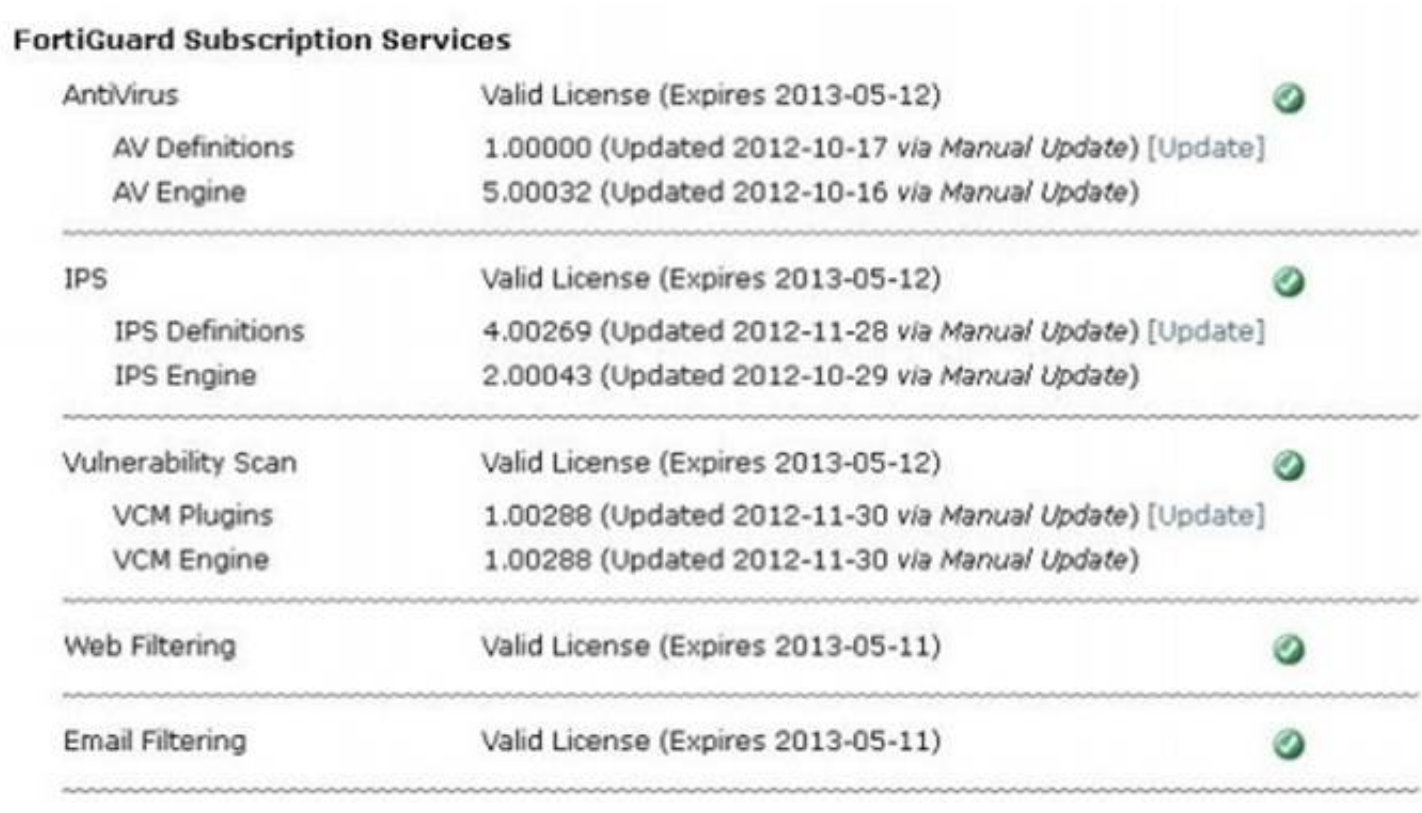
Answer: ABD

NEW QUESTION 110
You are the administrator in charge of a FortiGate acting as an IPsec VPN gateway using routebased mode. Users from either side must be able to initiate new sessions. There is only 1 subnet at either end and the FortiGate already has a default route.
Which two configuration steps are required to achieve these objectives? (Choose two.)

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

Answer: BC

NEW QUESTION 112
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.

Answer: A

NEW QUESTION 116
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

Answer: D

NEW QUESTION 119
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.

Answer: BC

NEW QUESTION 124
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.

Answer: AD

NEW QUESTION 128
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

Answer: ABD

NEW QUESTION 130
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'

Answer: D

NEW QUESTION 135
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”

Answer: B

NEW QUESTION 139
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.

Answer: BC

NEW QUESTION 143
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.

Answer: BC

NEW QUESTION 146
How do you configure a FortiGate to apply traffic shaping to P2P traffic, such as BitTorrent?

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

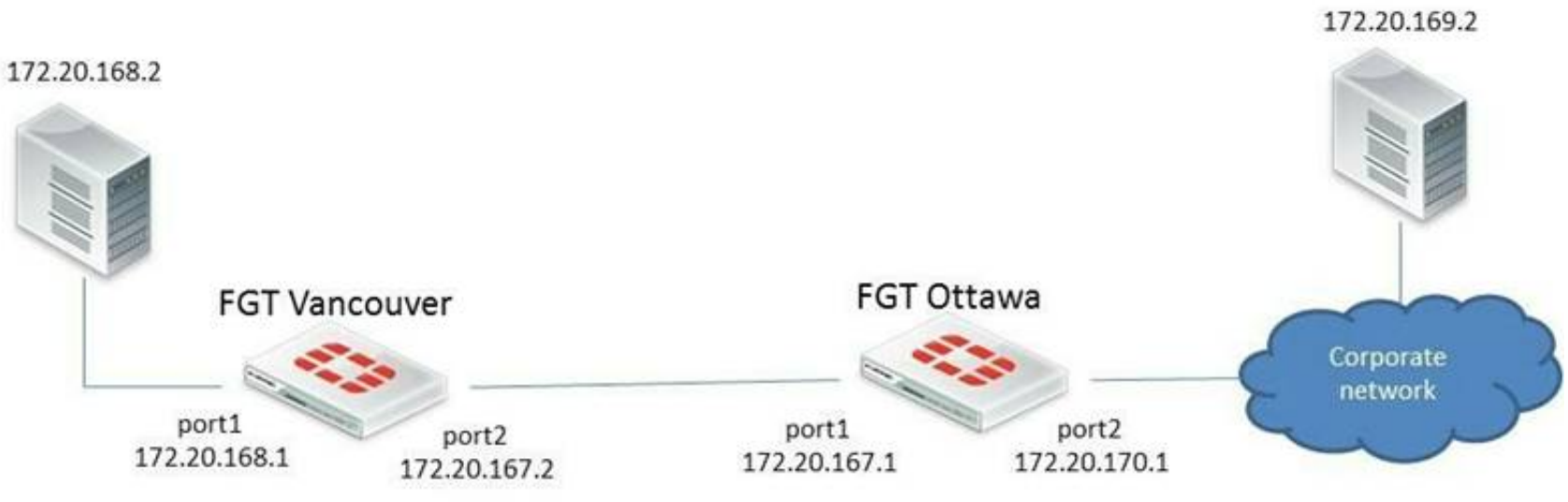
Answer: A

NEW QUESTION 149
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.

Answer: ABC

NEW QUESTION 154
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
c172.20.167.0/24 is directly connected, port1 c172.20.170.0/24 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.

Answer: B

NEW QUESTION 159
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.

Answer: A

NEW QUESTION 160
What actions are possible with Application Control? (Choose three.)

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

Answer: BCD

NEW QUESTION 164
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.

Answer: BCD

NEW QUESTION 166
Two FortiGate devices fail to form an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of show system ha for the STUDENT device. Exhibit B shows the command output of show system ha for the REMOTE device.
Exhibit A:

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

STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT # show system ha
config system ha
    set mode a-p
    set password ENC 9FHCYwOJXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4dsgx4CnV1GRJ8
McEECpiT3Z/3dCmIuYIDgW2sE+lA1kHfADOV/r5DkaqGnbj15XV/a
    set hbdev "port2" 50
    set override disable
    set priority 200
end

STUDENT # _
```

Exhibit B:

```
Log hard disk: Available
Hostname: REMOTE
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-a, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:41:46 2013

REMOTE # show system ha
config system ha
    set mode a-a
    set password ENC 9FHCYwOJXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4ds7YGvl2Cir+8
B6Mf/rGXhOu5lygP+yPgI5SDnSMEz4JlNv4E09skIO0mBQbcgxhSE
    set hbdev "port2" 50
    set session-pickup enable
    set override disable
    set priority 100
end

REMOTE # _
```

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

A. Password
B. HA mode
C. Hearbeat
D. Override

Answer: B

NEW QUESTION 171
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 UTM security profile enables virus scanning for all traffic flowing through the FortiGate device.

Answer: C

NEW QUESTION 175
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

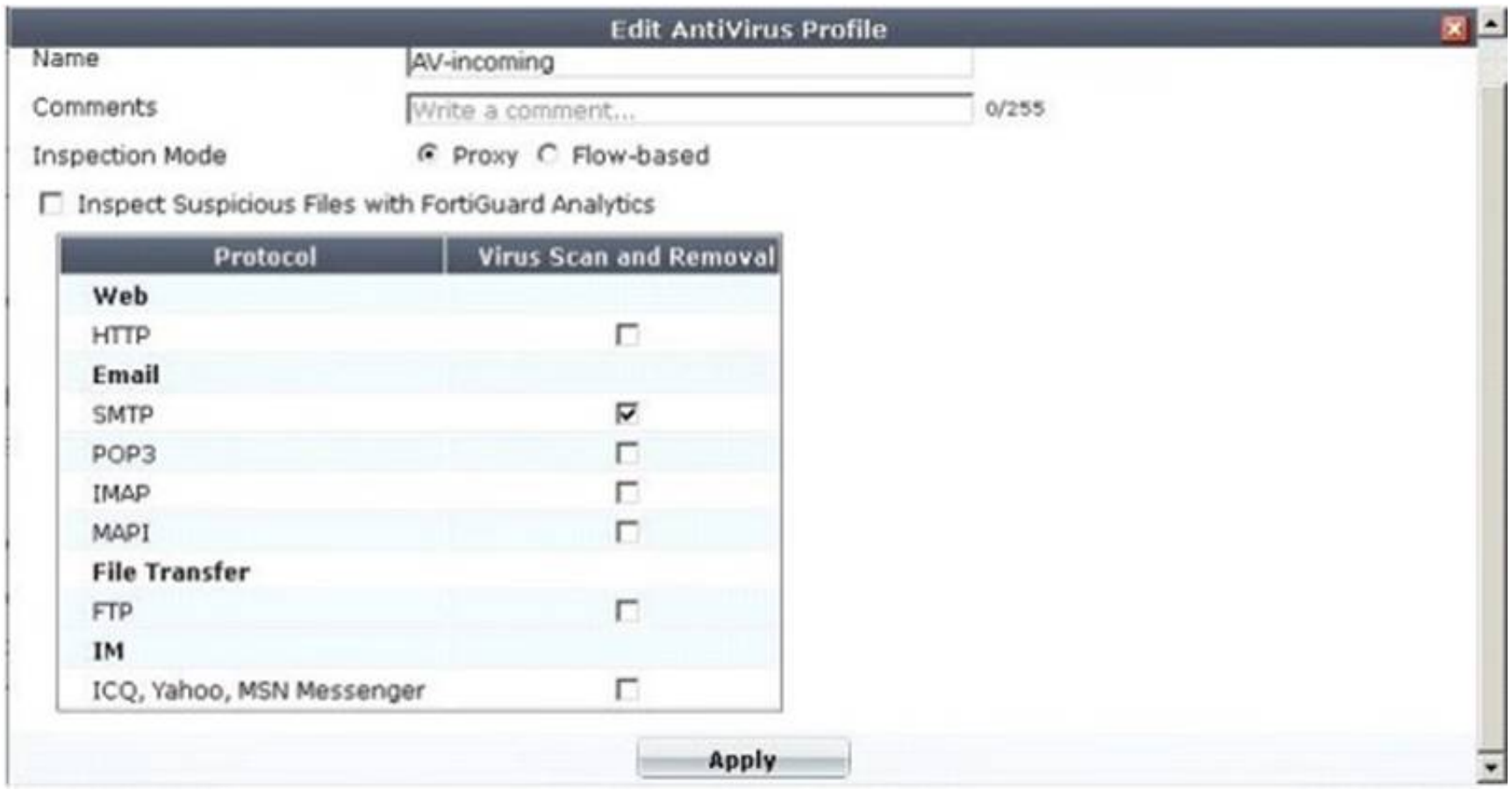


Exhibit B:

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 messag
D. Both sender and recipient are notified that the infected file has been removed.
E. The FortiGate unit will reject the infected email and notify the sender.

Answer: B

NEW QUESTION 179
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.

Answer: AD

NEW QUESTION 183
An administrator has formed a high availability cluster involving two FortiGate units.
[Multiple upstream Layer 2 switches] – [FortiGate HA Cluster] – [Multiple downstream Layer 2 Switches]
The administrator wishes to ensure that a single link failure will have minimal impact upon the overall throughput of traffic through this cluster.
Which of the following options describes the best step the administrator can take? The administrator should

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

Answer: C

NEW QUESTION 184
To which remote device can the FortiGate send logs? (Choose three.)

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

Answer: ABE

NEW QUESTION 185
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.

Answer: CD

NEW QUESTION 187
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.

Answer: ADE

NEW QUESTION 188
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE4 Practice Exam Features:

* NSE4 Questions and Answers Updated Frequently

* NSE4 Practice Questions Verified by Expert Senior Certified Staff

* NSE4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year