Fortinet

Exam Questions NSE4

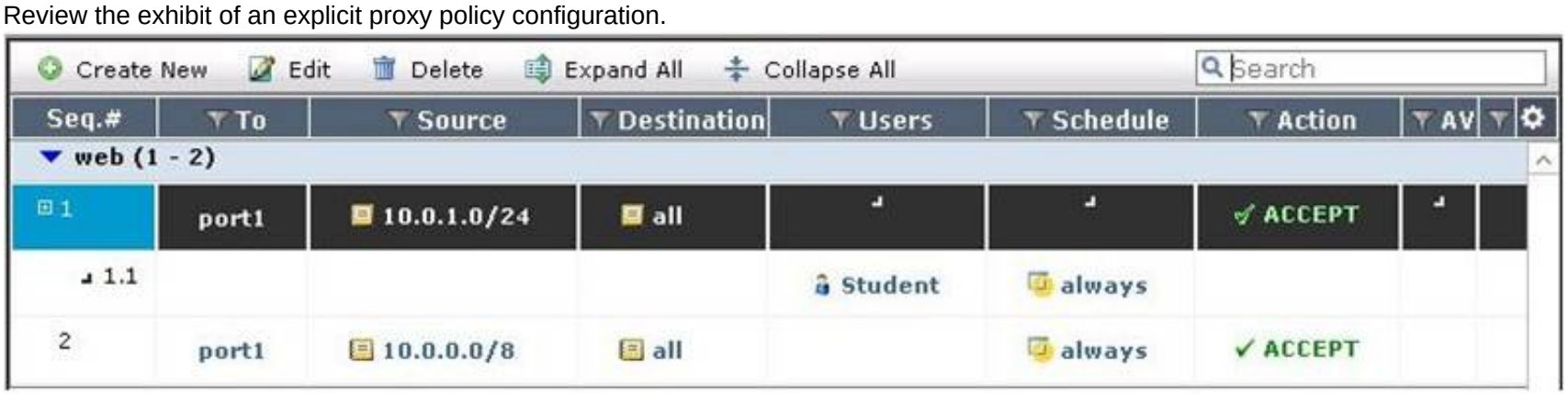
Fortinet Network Security Expert 4 Written Exam (400)

NEW QUESTION 1
What protocol cannot be used with the active authentication type?

A. Local
B. RADIUS
C. LDAP
D. RSSO

Answer: D

NEW QUESTION 2
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 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
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

Answer: ABE

NEW QUESTION 5
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 6
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 numbe

B. You must reconfigured the server to run on port 2.
C. To apply IPS to traffic to that server, you must configured FortiGate SMTP proxy to listen on port 2525
D. IPS will apply all SMTP signatures, regardless of whether they apply to clients or servers.
E. Protocol decoders automatically detect SMTP and scan for matches with appropriate IPS signature.

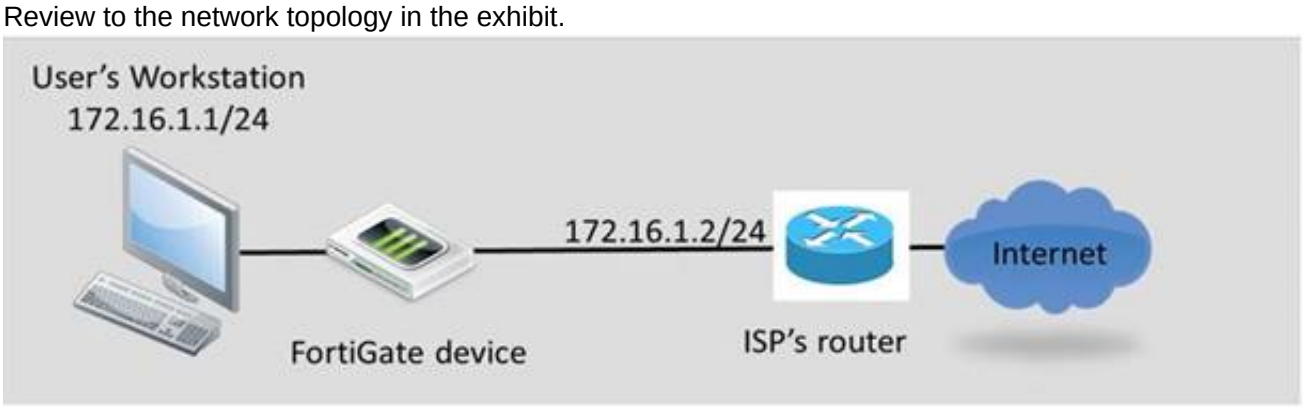
Answer: B

NEW QUESTION 7
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 8
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.

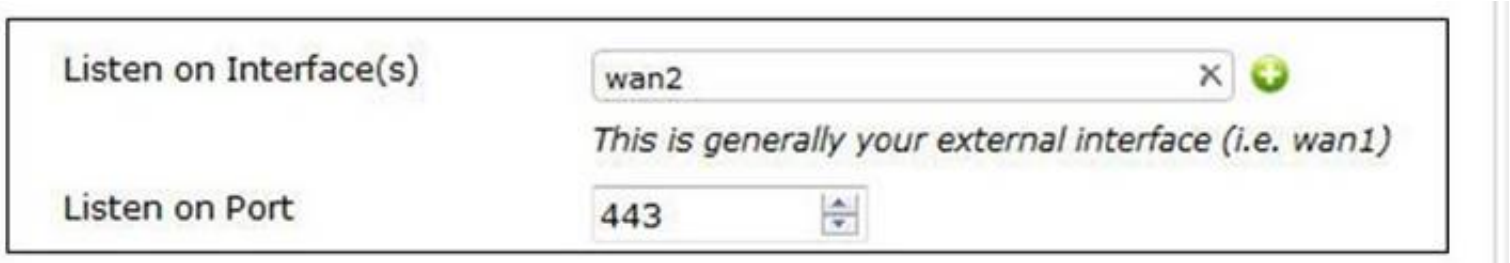
Answer: AD

NEW QUESTION 9
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.

Answer: BD

NEW QUESTION 10
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.



URL Path	Virtual Host	Max Concurrent U
Training		0
students		0

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/

Answer: BD

NEW QUESTION 10
Which two statements are true regarding firewall policy disclaimers? (Choose two.)

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

Answer: CD

NEW QUESTION 12
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 13
Which of the following protocols are defined in the IPsec Standard? (Choose two)

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

Answer: AD

NEW QUESTION 14
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.

Answer: AD

NEW QUESTION 19
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

Answer: C

NEW QUESTION 21
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.

Answer: B

NEW QUESTION 25
Which statements are true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

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

Answer: CD

NEW QUESTION 30
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

Answer: ABE

NEW QUESTION 34
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 38
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.

Answer: BC

NEW QUESTION 40
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 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.

Answer: A

NEW QUESTION 49
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

Answer: A

NEW QUESTION 52
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

Answer: D

NEW QUESTION 56
Regarding tunnel-mode SSL VPN, which three statements are correct? (Choose three.)

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

Answer: ABE

NEW QUESTION 57
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 60
Which is not a FortiGate feature?

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

Answer: A

NEW QUESTION 64
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)

Answer: B

NEW QUESTION 67
Which of the following are possible actions for FortiGuard web category filtering? (Choose three.)

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

Answer: ABD

NEW QUESTION 71
Examine the following spanning tree configuration on a FortiGate in transparent mode:
config system interface edit <interface name> set stp-forward enable end
Which statement is correct for the above configuration?

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

D. The FortiGate generates spanning tree BPDU frames.

Answer: B

NEW QUESTION 76
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

Answer: AD

NEW QUESTION 78
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 81
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 84
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.

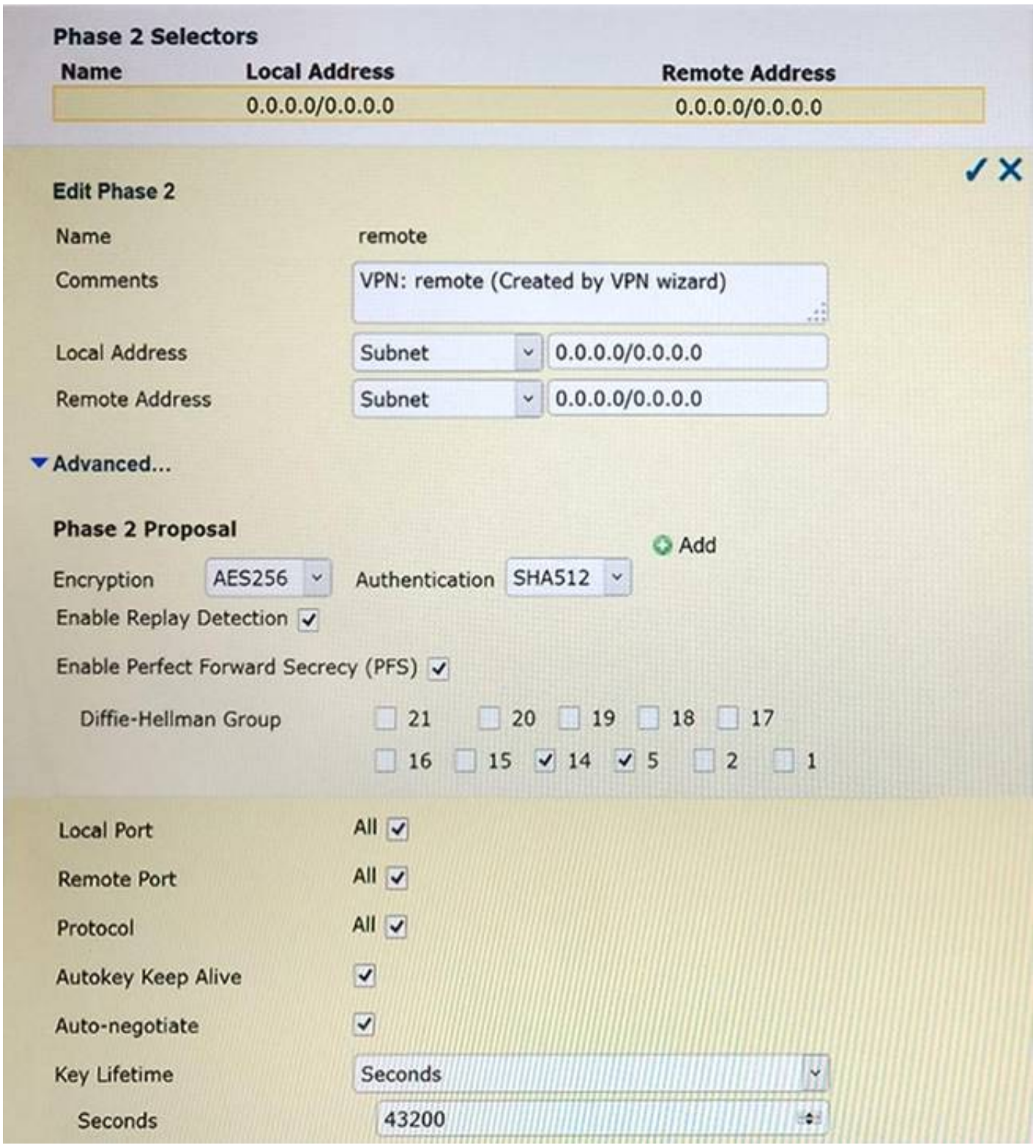
Answer: D

NEW QUESTION 87
Which statements are correct regarding an IPv6 over IPv4 IPsec configuration? (Choose two.)

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

Answer: BC

NEW QUESTION 89
Review the IPsec phase 2 configuration shown in the exhibit; then answer the question below.



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

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

Answer: AB

NEW QUESTION 94
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 95
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 100
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 protoco
D. Otherwise, it could accidentally match lower-layer protocols.
E. It is not supported by Fortinet Technical Support.

Answer: A

NEW QUESTION 104
Data leak prevention archiving gives the ability to store session transaction data on a FortiAnalyzer unit for which of the following types of network traffic? (Choose three.)

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

Answer: ADE

NEW QUESTION 108
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 113
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.

Answer: B

NEW QUESTION 114
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

Answer: AB

NEW QUESTION 116
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

Answer: BC

NEW QUESTION 117
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.

Answer: CDE

NEW QUESTION 121
Which IPsec configuration mode can be used for implementing GRE-over-IPsec VPNs?

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

Answer: B

NEW QUESTION 122
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 123
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.

Answer: AC

NEW QUESTION 127
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

Answer: A

NEW QUESTION 129
Which firewall objects can be included in the Destination Address field of a firewall policy? (Choose three.)

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

Answer: BCD

NEW QUESTION 133
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.

Answer: A

NEW QUESTION 135
Files that are larger than the oversized limit are subjected to which Antivirus check?

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

Answer: C

NEW QUESTION 140
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.

Answer: D

NEW QUESTION 143
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.

Answer: AB

NEW QUESTION 148
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.

Answer: A

NEW QUESTION 149
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.

Answer: AD

NEW QUESTION 153
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.

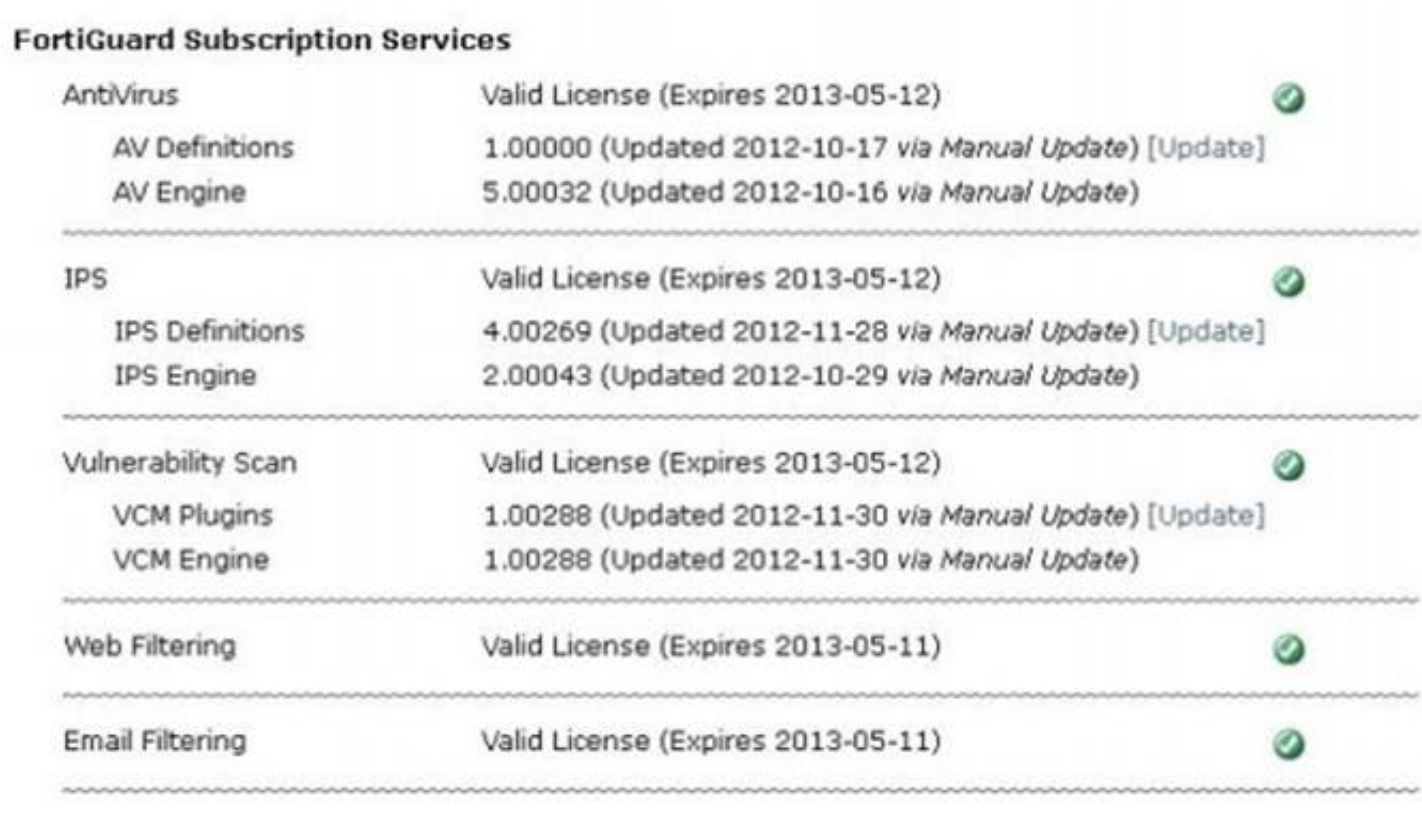
Answer: D

NEW QUESTION 158
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.

Answer: BD

NEW QUESTION 160
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 165
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 170
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.

Answer: BC

NEW QUESTION 172
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.

Answer: C

NEW QUESTION 173
Examine the following CLI configuration:
config system session -ttl set default 1800
end
What statement is true about the effect of the above configuration line?

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

Answer: A

NEW QUESTION 178
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

Answer: AC

NEW QUESTION 180
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

Answer: D

NEW QUESTION 182
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

Answer: C

NEW QUESTION 185
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 188
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:0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7: sent IKE msg (quick_r1send): 172.20.186.222:500->172.20.187.114:500, len=356
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

Answer: BD

NEW QUESTION 189
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.

Answer: B

NEW QUESTION 190
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.

Answer: AC

NEW QUESTION 191
Which authentication scheme is not supported by the RADIUS implementation on FortiGate?

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

Answer: D

NEW QUESTION 192
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.

Answer: BEG

NEW QUESTION 193
Which statement is one disadvantage of using FSSO NetAPI polling mode over FSSO Security Event Log (WinSecLog) polling mode?

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

Answer: C

NEW QUESTION 197
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 VP
B. Side B: aggressive mode, remote Gateway as static IP address policy-based VPN.
C. Side A:main mode, remote gateway as static IP address, policy based VP
D. Side B: main mode, remote gateway as static IP address, route-based VPN
E. Side A:main mode, remote gateway as static IP address, policy based VP
F. Side B: main mode, remote gateway as dialup, route-based VPN.
G. Side A: main mode, remote gateway as dialup policy based VPN, Side B: main mode, remote gateway as dialup, policy based VPN.

Answer: BC

NEW QUESTION 199
Which of the following are considered log types? (Choose three.)

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

Answer: BDE

NEW QUESTION 200
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 202
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

Answer: CD

NEW QUESTION 204
What actions are possible with Application Control? (Choose three.)

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

Answer: BCD

NEW QUESTION 206
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.

Answer: AB

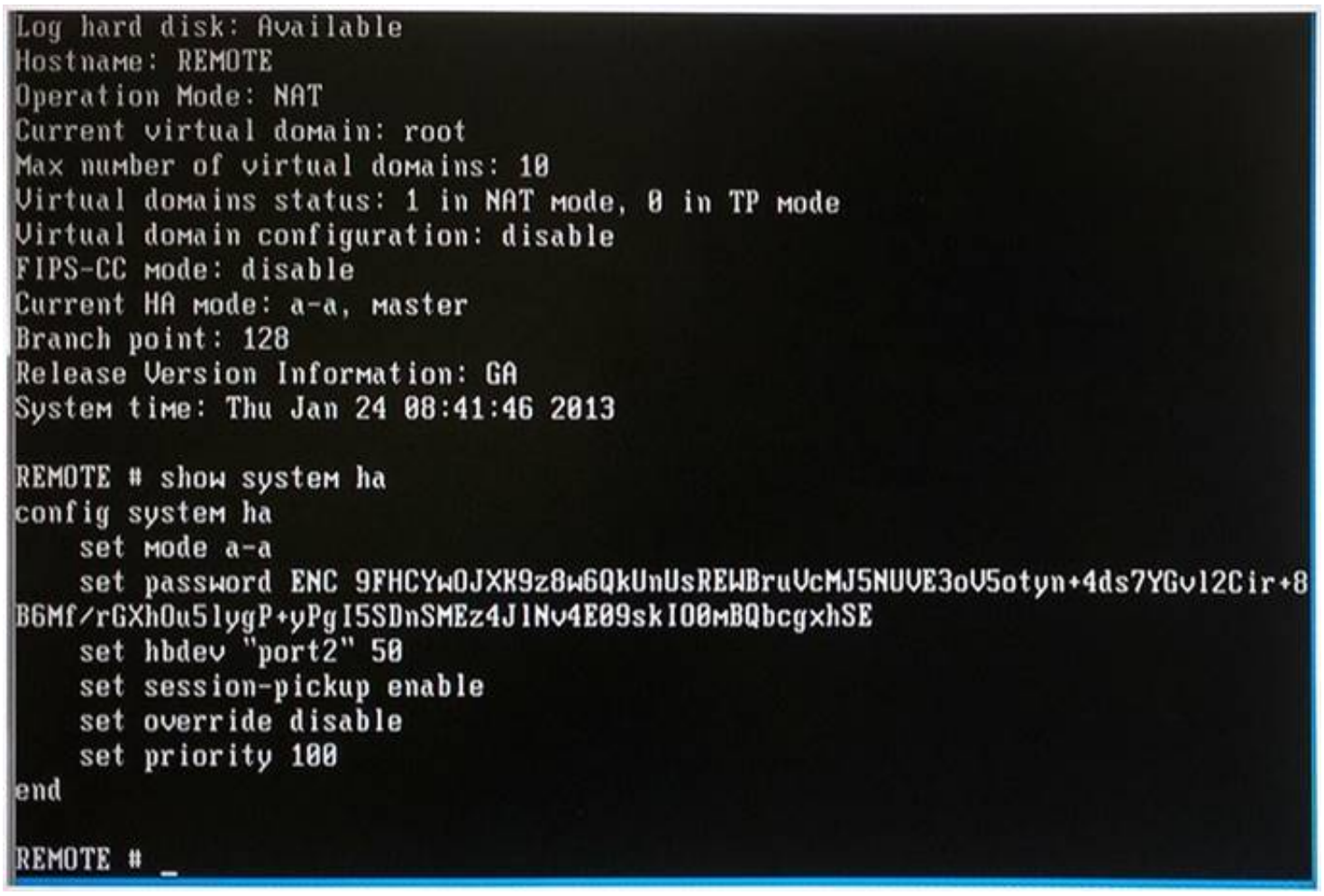
NEW QUESTION 207
Two FortiGate devices fail to form an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of show system ha for the STUDENT device. Exhibit B shows the command output of show system ha for the REMOTE device.
Exhibit A:

```
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 # show system ha
config system ha
    set mode a-p
    set password ENC 9FHCYwOJXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4dsgx4CnV1GRJ8
McEECpiT32/3dCmluYIDgW2sE+lA1kHfADOV/r5DkaqGnbj15XV/a
    set hbdev "port2" 50
    set override disable
    set priority 200
end

STUDENT # _
```

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

Answer: B

NEW QUESTION 212
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

Answer: C

NEW QUESTION 213
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.

Answer: AC

NEW QUESTION 215
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.

Answer: C

NEW QUESTION 219
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.

Answer: ABCD

NEW QUESTION 222

.....

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