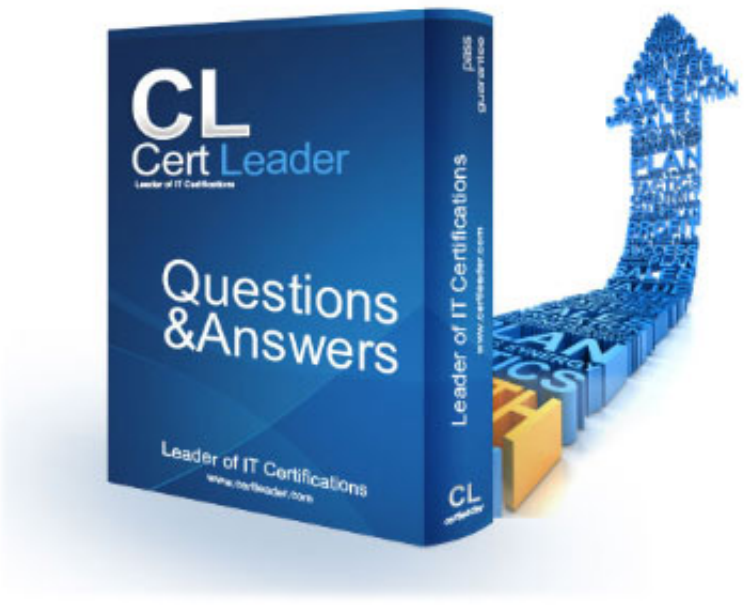
NSE4 Dumps

Fortinet Network Security Expert 4 Written Exam (400)

https://www.certleader.com/NSE4-dumps.html



NEW QUESTION 1
Which protocols can you use for secure administrative access to a FortiGate? (Choose two)

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

Answer: AD

NEW QUESTION 2
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

Answer: BC

NEW QUESTION 3
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.

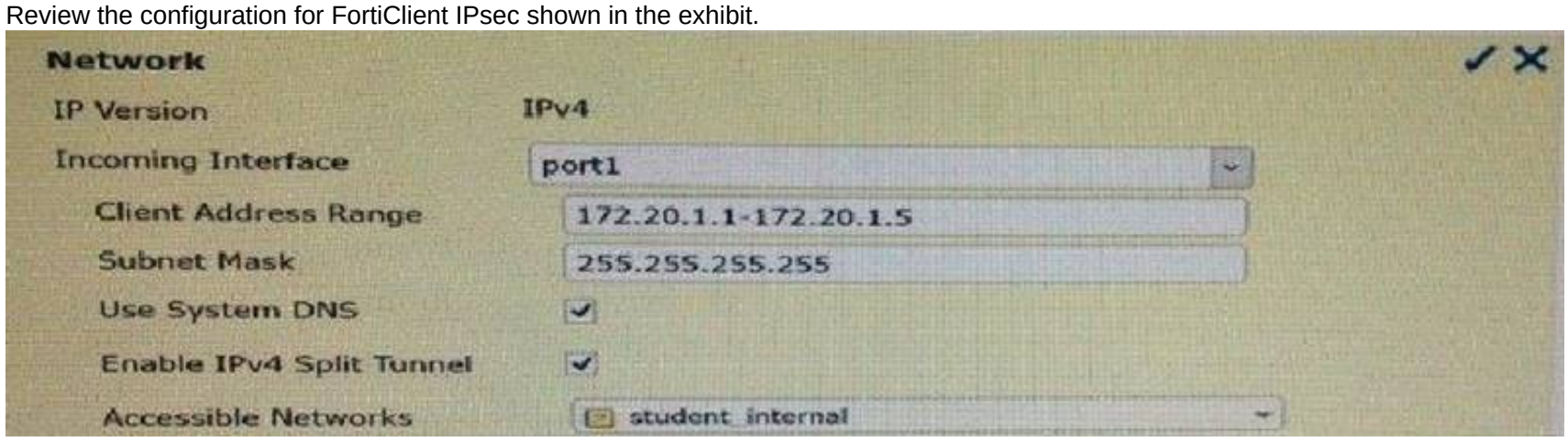
Answer: C

NEW QUESTION 4
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 5
Review the configuration for FortiClient IPsec shown in the exhibit.



Which statement is correct regarding this configuration?

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

Answer: A

NEW QUESTION 6
Review the output of the command get router info routing-table database shown in the exhibit below; then answer the question following it.

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

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

Which 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.

Answer: AC

NEW QUESTION 7
What is the maximum number of different virus databases a FortiGate can have?

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

Answer: B

NEW QUESTION 8
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.

Answer: D

NEW QUESTION 9
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

Answer: AD

NEW QUESTION 10
What capabilities can a FortiGate provide? (Choose three)

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

Answer: BCD

NEW QUESTION 10
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 14
Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit below.

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

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

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

Answer: AB

NEW QUESTION 18
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 22
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 25
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

Answer: CD

NEW QUESTION 27
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.

Answer: D

NEW QUESTION 28
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 30
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.

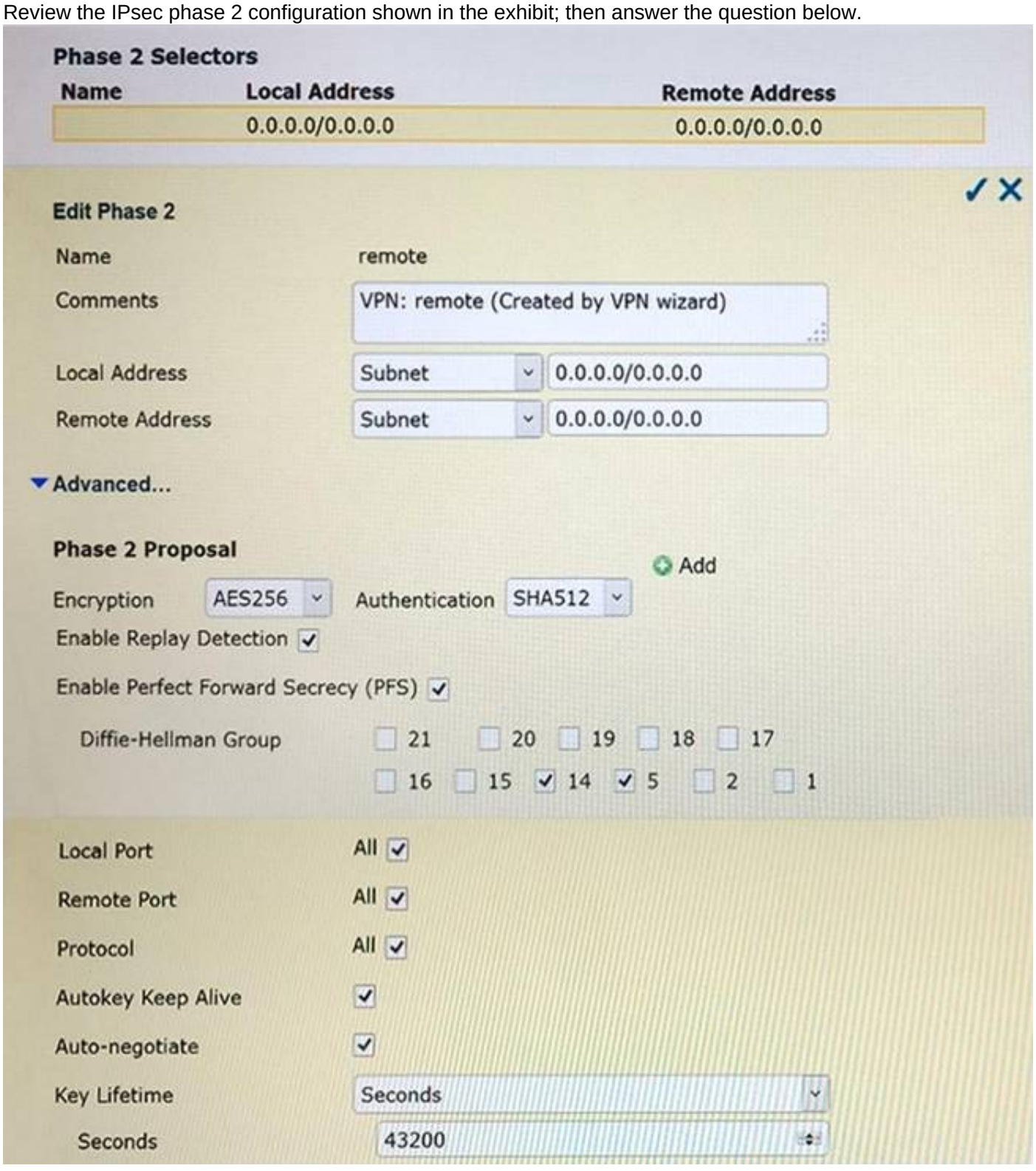
Answer: B

NEW QUESTION 31
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.

Answer: D

NEW QUESTION 32
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 33
Which traffic can match a firewall policy's "Services" setting? (Choose three.)

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

Answer: ACE

NEW QUESTION 38
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

Answer: A

NEW QUESTION 42
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 47
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.

Answer: C

NEW QUESTION 52
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 54
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 55
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 59
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.

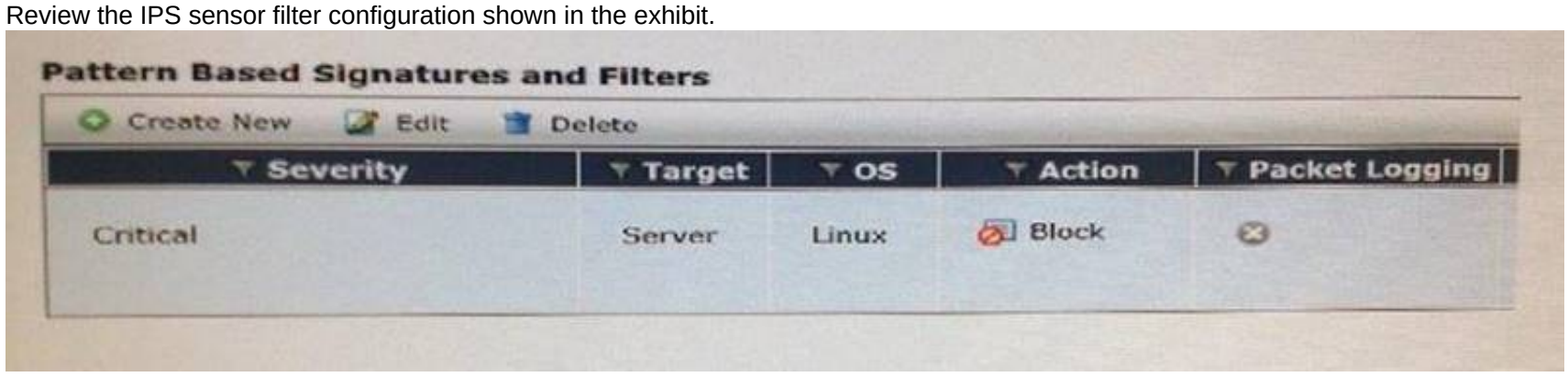
Answer: AC

NEW QUESTION 61
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 63
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.

Answer: CD

NEW QUESTION 66
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

Answer: D

NEW QUESTION 71
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 73
Which network protocols are supported for administrative access to a FortiGate unit? (Choose three.)

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

Answer: CDE

NEW QUESTION 77
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 78
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.

Answer: AB

NEW QUESTION 79
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.

Answer: B

NEW QUESTION 84
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 86
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.

Answer: B

NEW QUESTION 88
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 89
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.

Answer: BD

NEW QUESTION 90
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 93
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 95
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.

Answer: A

NEW QUESTION 97
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 99
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.

Answer: AC

NEW QUESTION 101
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 106
Which does FortiToken use as input when generating a token code? (Choose two.)

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

Answer: AD

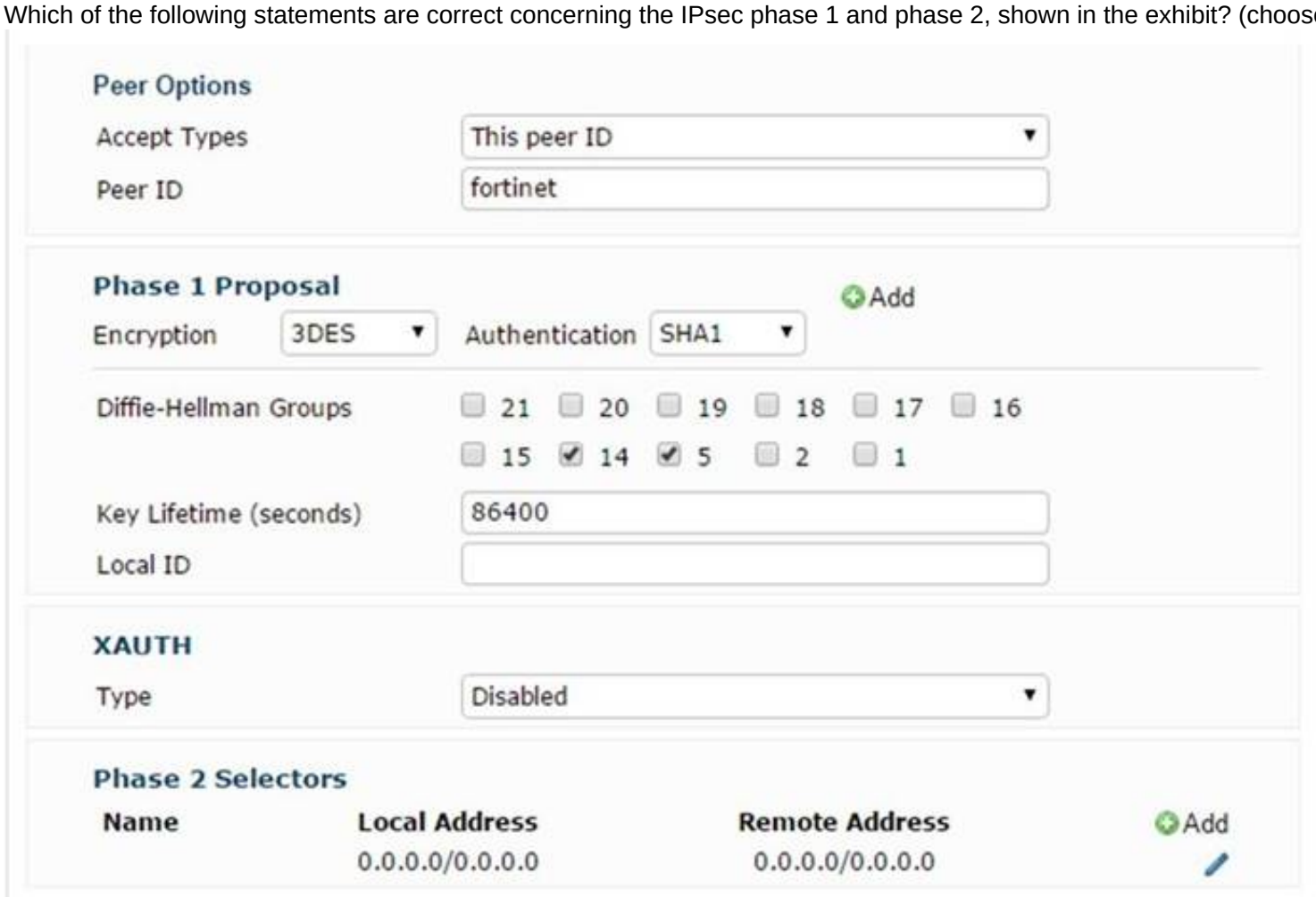
Explanation:
The token passcode is generated using a combination of the time and a secret key which is known only by the token and the FortiAuthenticator device. The token password changes at regular time intervals, and the FortiAuthenticator unit is able to validate the entered passcode using the time and the secret seed information for that token.

NEW QUESTION 110
Which of the following items is NOT a packet characteristic matched by a firewall service object?

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

Answer: D

NEW QUESTION 111
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 tunnel
E. A FortiGate tunnel requires a different configuration.

Answer: CD

NEW QUESTION 113
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 114
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.

Answer: ACE

NEW QUESTION 116
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

Answer: D

NEW QUESTION 121
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 126
A FortiGate is configured with multiple VDOMs. An administrative account on the device has been assigned a Scope value of VDOM: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.

Answer: AB

NEW QUESTION 131
What functions can the IPv6 Neighbor Discovery Protocol accomplish? (Choose two.)

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

Answer: CD

NEW QUESTION 132
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.

Answer: D

NEW QUESTION 134
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 137
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.

Answer: ADE

NEW QUESTION 140
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

Answer: D

NEW QUESTION 145
Bob wants to send Alice a file that is encrypted using public key cryptography.
Which of the following statements is correct regarding the use of public key cryptography in this scenario?

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

Answer: C

NEW QUESTION 147
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.

Answer: BC

NEW QUESTION 149
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 152
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

Answer: AD

NEW QUESTION 153

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 FortiGat
C. Via the local console, during the boot loader, use the menu to format the flash disk and reinstall the firmwar
D. Then you can log in with the default password.
E. Power off the FortiGat
F. After several seconds, restart i
G. 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.
H. Reboot the FortiGat
I. 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.

Answer: C

NEW QUESTION 155
What actions are possible with Application Control? (Choose three.)

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

Answer: BCD

NEW QUESTION 157
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

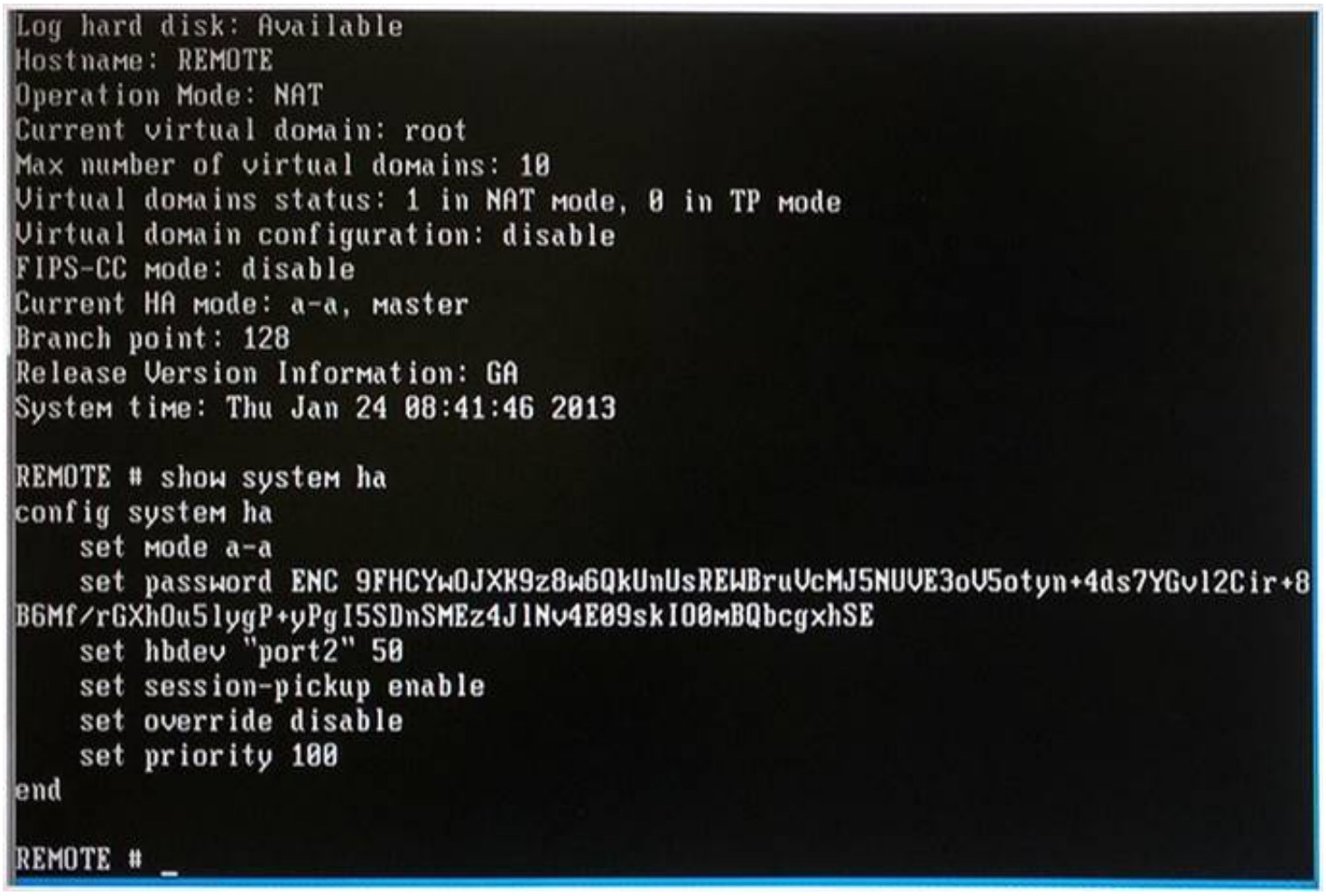
NEW QUESTION 162
Two FortiGate devices fail to form an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of show system ha for the STUDENT device. Exhibit B shows the command output of show system ha for the REMOTE device.
Exhibit A:

```
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 165
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 167
Which of the following Fortinet products can receive updates from the FortiGuard Distribution Network?

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

Answer: ABC

NEW QUESTION 171
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 174
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 176
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.

Answer: AB

NEW QUESTION 180
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 182
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE4 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE4-dumps.html