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
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 3
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 4
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.

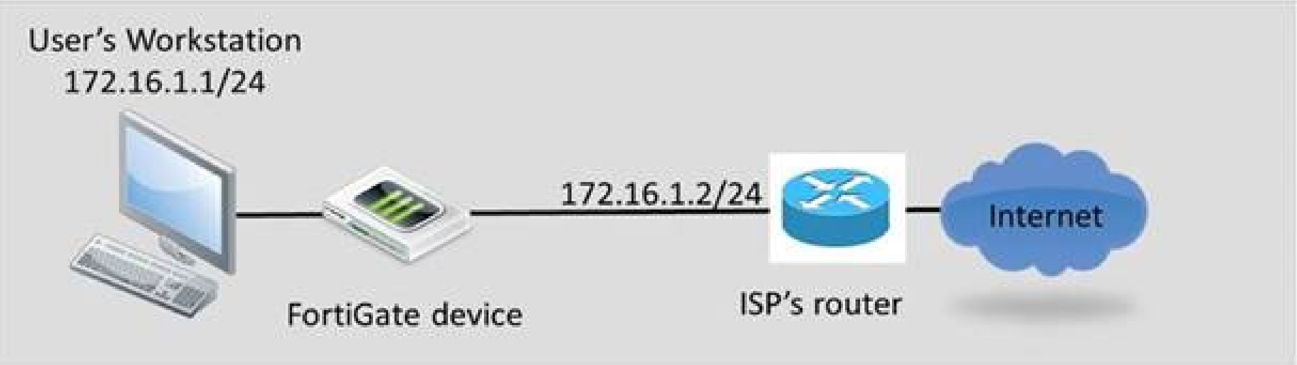
Answer: A

NEW QUESTION 5
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 6
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 7
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.

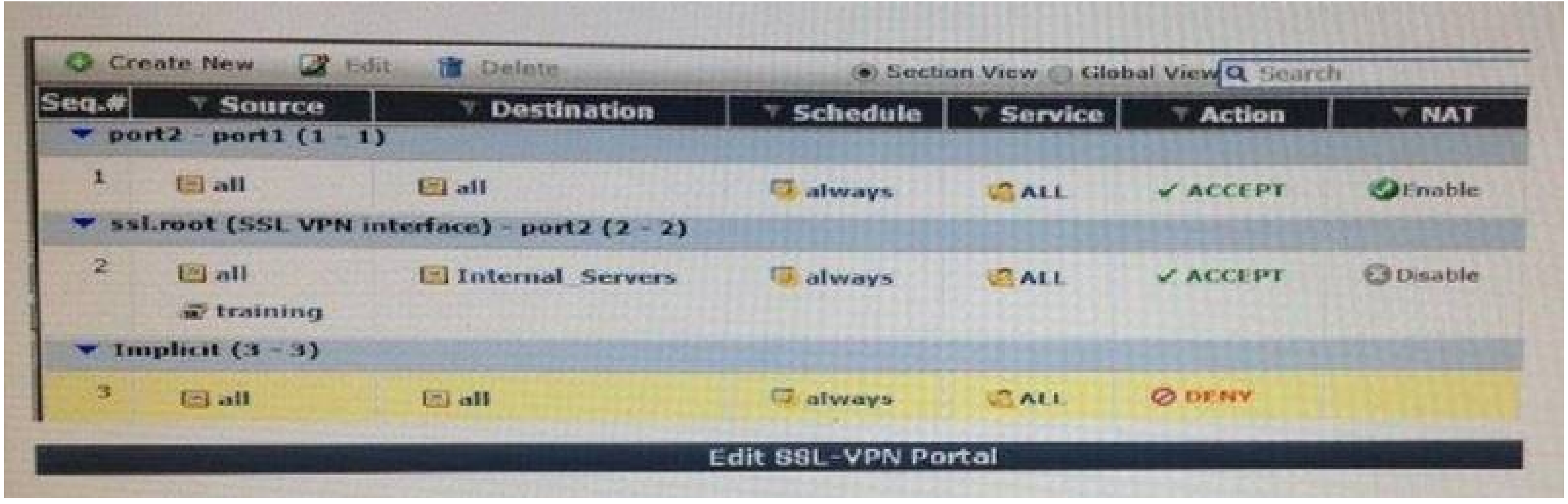
Answer: AD

NEW QUESTION 8
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 9
A user logs into a SSL VPN portal and activates the tunnel mode. The exhibit shows the firewall policy and the user's SSL VPN portal configuration:



Seq.#	Source	Destination	Schedule	Service	Action	NAT
port2 - port1 (1 - 1)						
1	all	all	always	ALL	✓ ACCEPT	Enable
ssl.root (SSL VPN interface) - port2 (2 - 2)						
2	all training	Internal_Servers	always	ALL	✓ ACCEPT	Disable
Implicit (3 - 3)						
3	all	all	always	ALL	DENY	

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

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

Answer: A

NEW QUESTION 10
The order of the firewall policies is important. Policies can be re-ordered from either the GUI or the CLI. Which CLI command is used to perform this function?

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

Answer: D

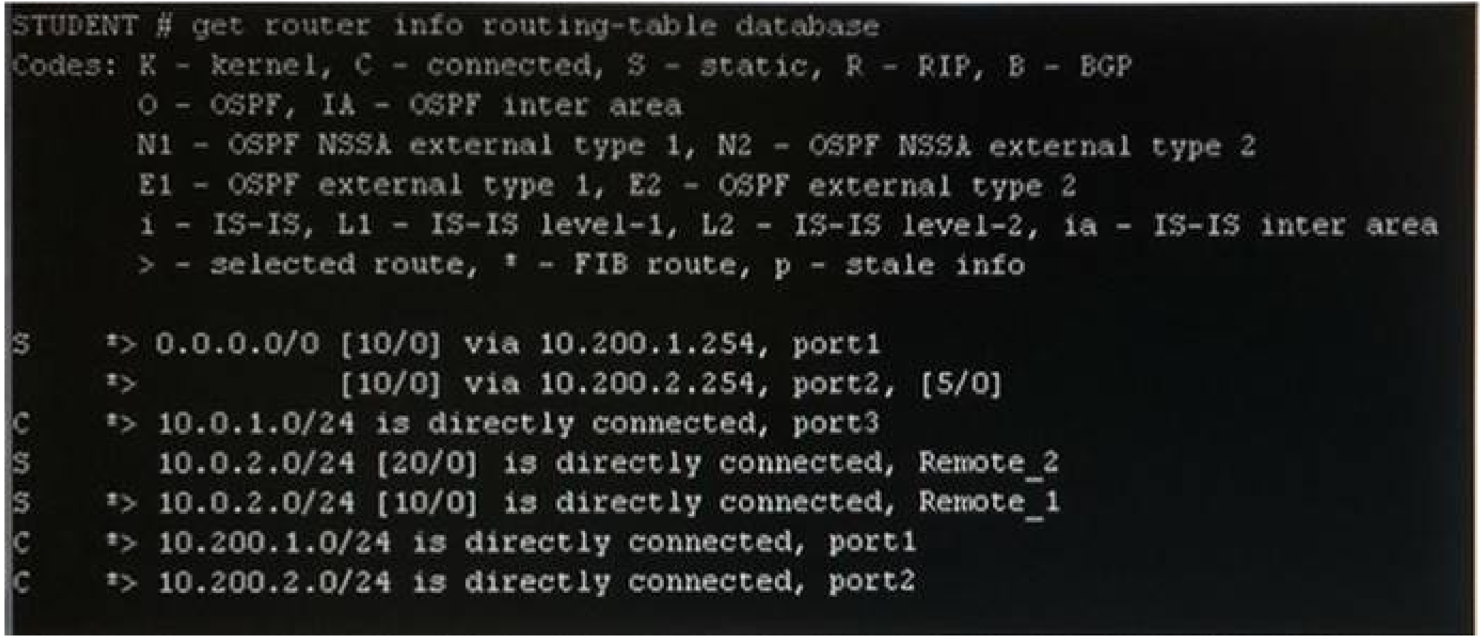
NEW QUESTION 10
With FSSO DC-agent mode, a domain user could authenticate either against the domain controller running the collector agent and domain controller agent, or a domain controller running only the domain controller agent.
If you attempt to authenticate with a domain controller running only the domain controller agent, which statements are correct? (Choose two.)

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

Answer: AC

NEW QUESTION 15

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 18
Which of the following fields contained in the IP/TCP/UDP headers can be used to make a routing decision when using policy-based routing? (Choose three)

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

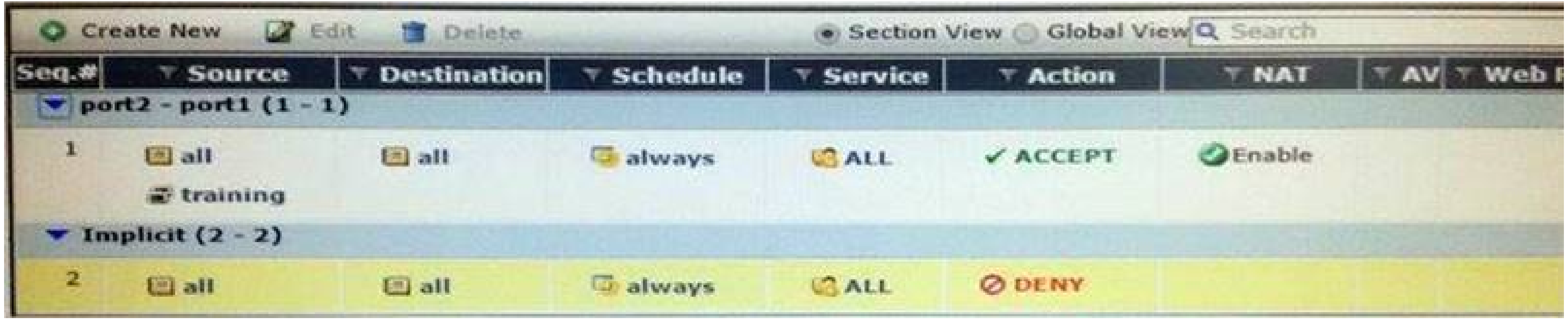
Answer: ACD

NEW QUESTION 22
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 23
The FortiGate port1 is connected to the Internet. The FortiGate port2 is connected to the internal network. Examine the firewall configuration shown in the exhibit; then answer the question below.



Seq.#	Source	Destination	Schedule	Service	Action	NAT	AV	Web F
port2 - port1 (1 - 1)								
1	all training	all	always	ALL	✓ ACCEPT	Enable		
Implicit (2 - 2)								
2	all	all	always	ALL	DENY			

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

A. A user that has not authenticated can access the Internet using any protocol that does not trigger an authentication challenge.
B. A user that has not authenticated can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP.
C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access all Internet services.
D. DNS Internet access is always allowed, even for users that have not authenticated.

Answer: D

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

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

Answer: BC

NEW QUESTION 26
Which of the following statements is true regarding a FortiGate device operating in transparent mode? (Choose three.)

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

Answer: ACE

NEW QUESTION 27
What is the maximum number of different virus databases a FortiGate can have?

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

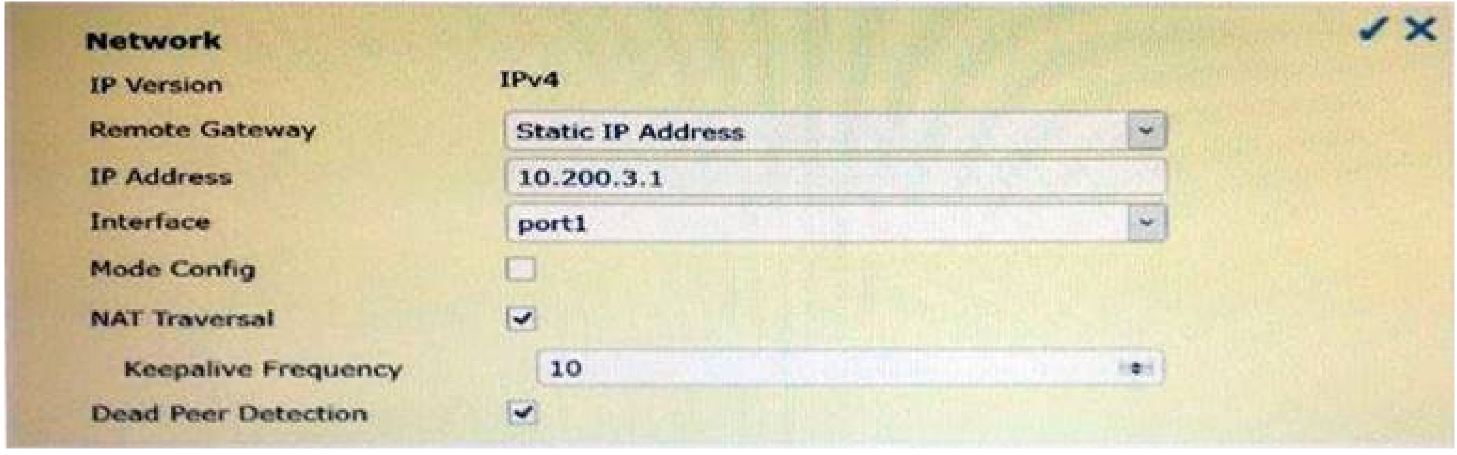
Answer: B

NEW QUESTION 31
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 34
Review the IPsec phase 1 configuration in the exhibit; then answer the question below.



Network
IP Version IPv4
Remote Gateway Static IP Address
IP Address 10.200.3.1
Interface port1
Mode Config □
NAT Traversal ☑
Keepalive Frequency 10
Dead Peer Detection ☑

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

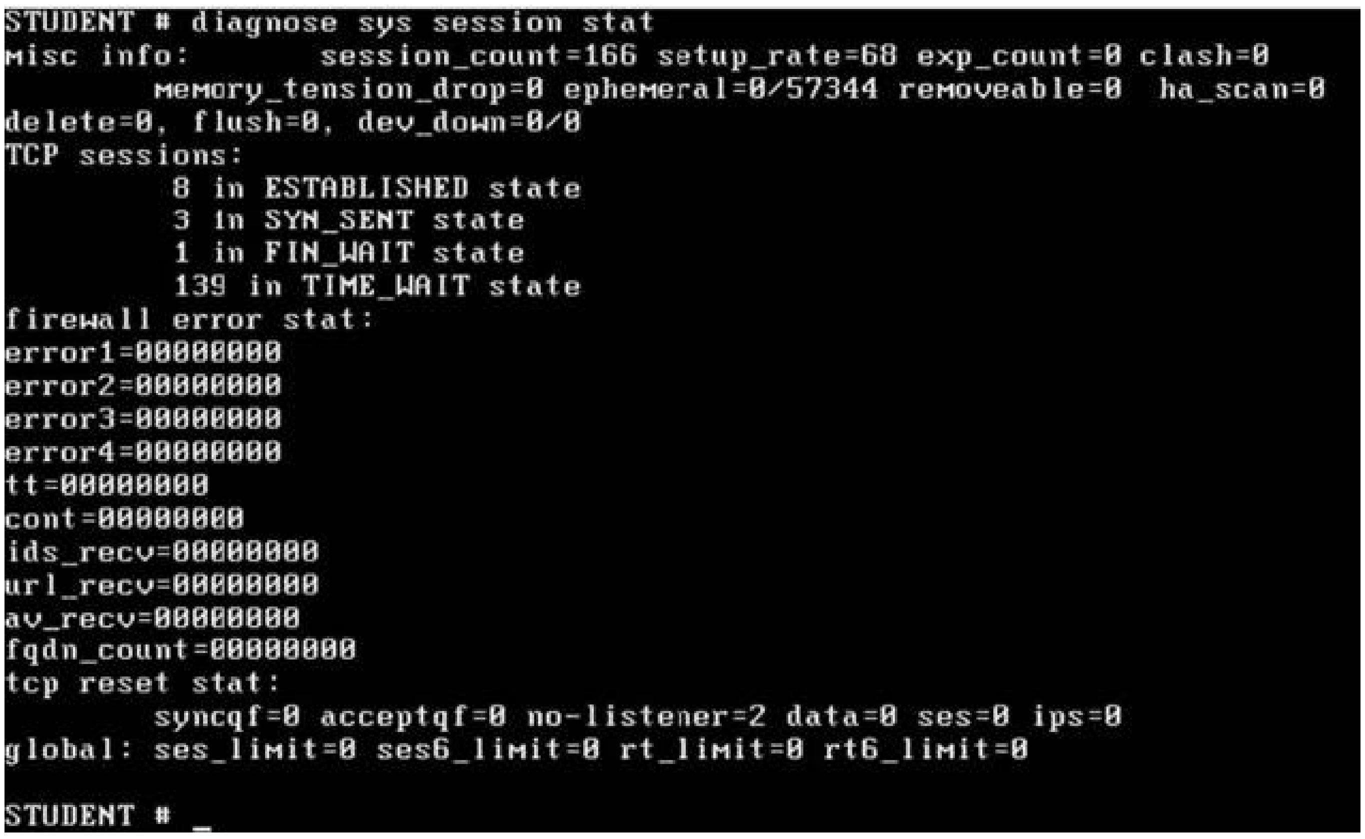
Answer: AC

NEW QUESTION 35
Which of the following statements are correct regarding a master HA unit? (Choose two)

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

Answer: AB

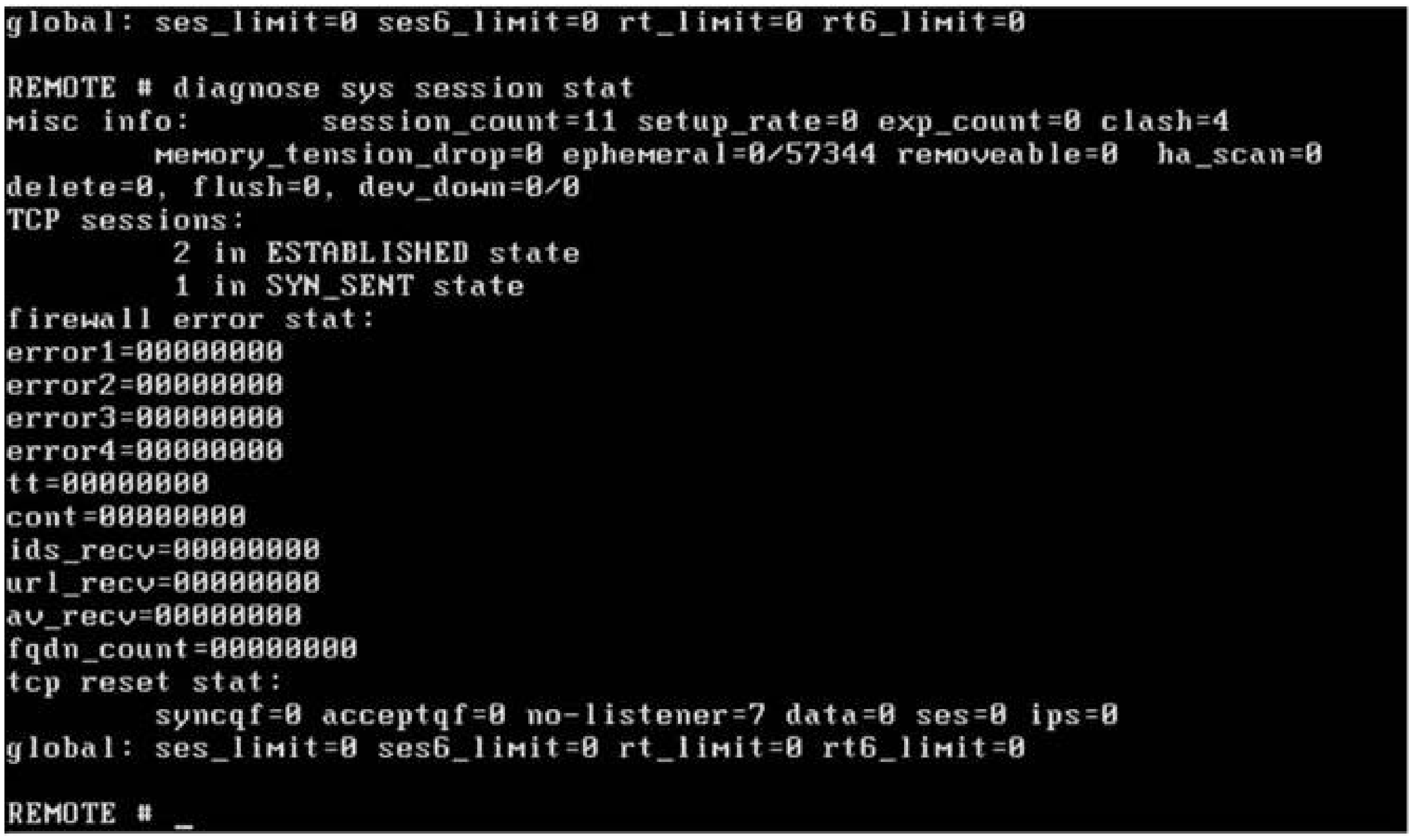
NEW QUESTION 40
Two devices are in an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of diagnose sys session stat for the STUDENT device. Exhibit B shows the command output of diagnose sys session stat for the REMOTE device.
Exhibit A:



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

STUDENT # _
```

Exhibit B:



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

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

REMOTE # _
```

Given the information provided in the exhibits, which of the following statements are correct? (Choose two.)

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

Answer: AD

NEW QUESTION 42
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 44
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 49
What log type would indicate whether a VPN is going up or down?

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

Answer: A

NEW QUESTION 53
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 57
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.

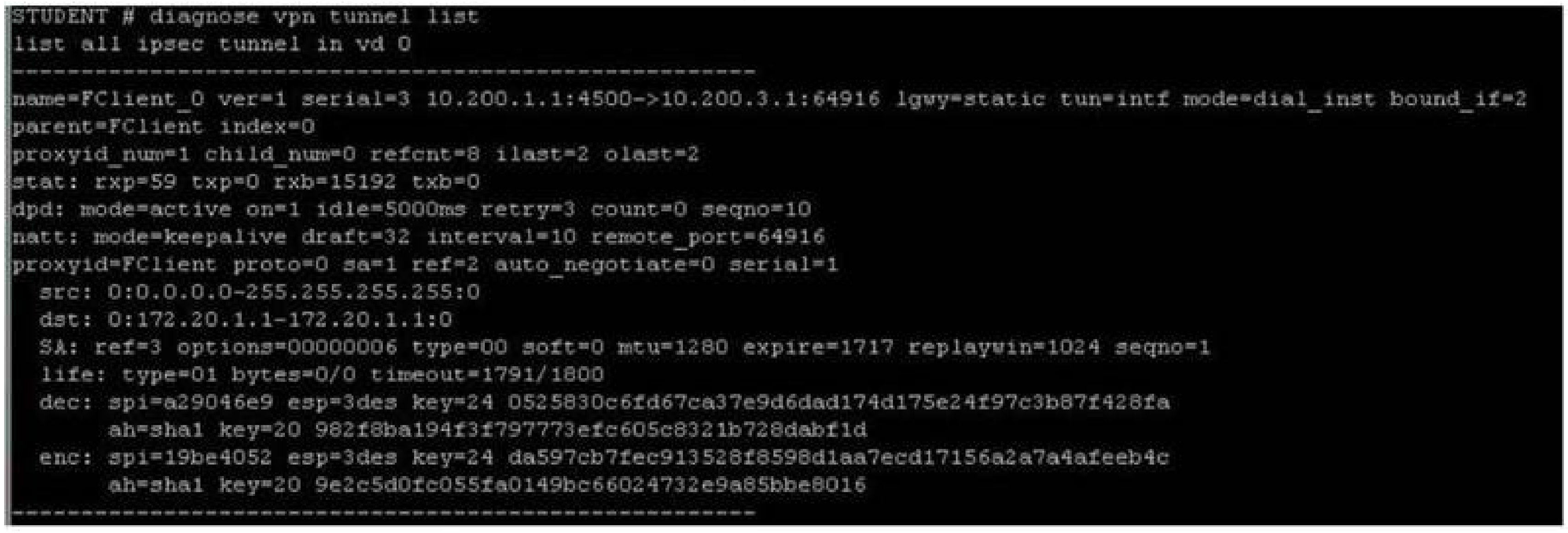
Answer: B

NEW QUESTION 61
How do application control signatures update on a FortiGate device?

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

Answer: A

NEW QUESTION 66
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 70
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 71
What is the FortiGate password recovery process?

A. Interrupt boot sequence, modify the boot registry and reboo
B. After changing thepassword, reset the boot registry.
C. Log in through the console port using the ''maintainer'' account within several seconds of physically power cycling the FortiGate.
D. Hold down the CTRL + Esc (Escape) keys during reboot, then reset the admin password.
E. Interrupt the boot sequence and restore a configuration file for which the password has been modified.

Answer: B

NEW QUESTION 75
Which is one of the conditions that must be met for offloading the encryption and decryption of IPsec traffic to an NP6 processor?

A. no protection profile can be applied over the IPsec traffic.
B. Phase-2 anti-replay must be disabled.
C. Phase 2 must have an encryption algorithm supported by the NP6.
D. IPsec traffic must not be inspected by any FortiGate session helper.

Answer: C

NEW QUESTION 77
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 79
Which two methods are supported by the web proxy auto-discovery protocol (WPAD) to automatically learn the URL where a PAC file is located? (Choose two.)

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

Answer: AC

NEW QUESTION 80
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 85
When an administrator attempts to manage FortiGate from an IP address that is not a trusted host, what happens?

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

Answer: B

NEW QUESTION 89
When configuring LDAP on the FortiGate as a remote database for users, what is not a part of the configuration?

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

Answer: C

NEW QUESTION 90

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 92
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 96
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 97
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 98
Which is not a FortiGate feature?

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

Answer: A

NEW QUESTION 101
What attributes are always included in a log header? (Choose three.)

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

Answer: BDE

NEW QUESTION 104
A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, they are not being received.
Which of the following statements are possible reasons for this?
A FortiGate unit is configured to receive push updates from the FortiGuard Distribution Network, however, updates are not being received. Which of the following statements are possible reasons for this? (Select all that apply.)

A. The external facing interface of the FortiGate unit is configured to use DHCP.
B. The FortiGate unit has not been registered.
C. There is a NAT device between the FortiGate unit and the FortiGuard Distribution Network and no override push IP is configured.
D. The FortiGate unit is in Transparent mode which does not support push updates.

Answer: ABC

NEW QUESTION 107
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 109
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 112
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 113
Which changes to IPS will reduce resource usage and improve performance? (Choose three)

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

Answer: ABD

NEW QUESTION 118
Which of the following items does NOT support the Logging feature?

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

Answer: C

NEW QUESTION 119
In transparent mode, forward-domain is a CLI setting associated with .

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

Answer: C

NEW QUESTION 122
What action does an IPsec Gateway take with the user traffic routed to an IPsec VPN when it does not match any phase 2 quick mode selector?

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

Answer: A

NEW QUESTION 126
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 128
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.

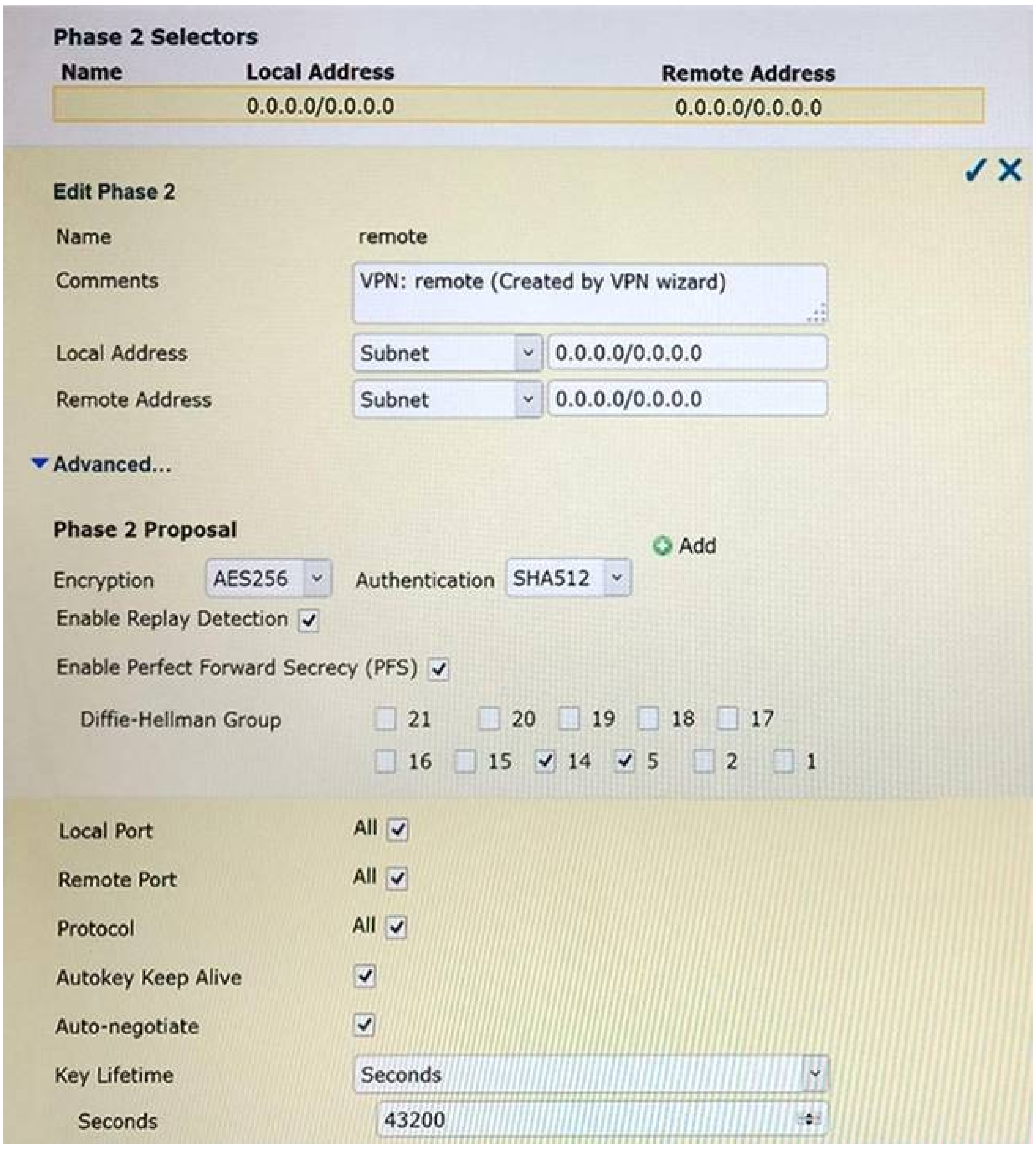
Answer: D

NEW QUESTION 129
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 132
Review the IPsec phase 2 configuration shown in the exhibit; then answer the question below.



Phase 2 Selectors

Name	Local Address	Remote Address
	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: remote
Comments: VPN: remote (Created by VPN wizard)
Local Address: Subnet 0.0.0.0/0.0.0.0
Remote Address: Subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal

Encryption: AES256 Authentication: SHA512 Add
Enable Replay Detection ☑
Enable Perfect Forward Secrecy (PFS) ☑
Diffie-Hellman Group: □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 ☑ 14 ☑ 5 □ 2 □ 1

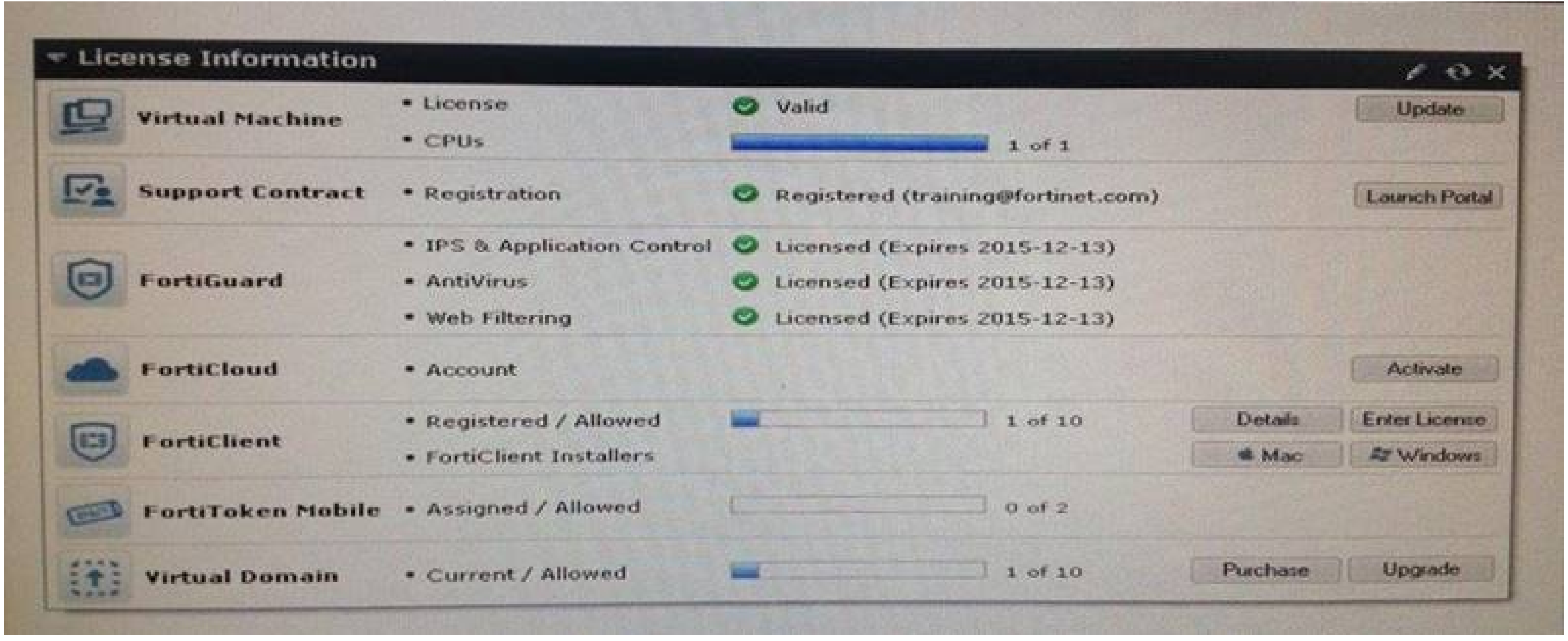
Local Port: All ☑
Remote Port: All ☑
Protocol: All ☑
Autokey Keep Alive: ☑
Auto-negotiate: ☑
Key Lifetime: Seconds
Seconds: 43200

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 137
Examine the exhibit; then answer the question below.



License Information

Virtual Machine	• License • CPUs	Valid 1 of 1		Update
Support Contract	• Registration	Registered (training@fortinet.com)		Launch Portal
FortiGuard	• IPS & Application Control • AntiVirus • Web Filtering	Licensed (Expires 2015-12-13) Licensed (Expires 2015-12-13) Licensed (Expires 2015-12-13)		
FortiCloud	• Account			Activate
FortiClient	• Registered / Allowed • FortiClient Installers	1 of 10	Details Mac	Enter License Windows
FortiToken Mobile	• Assigned / Allowed	0 of 2		
Virtual Domain	• Current / Allowed	1 of 10	Purchase	Upgrade

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.

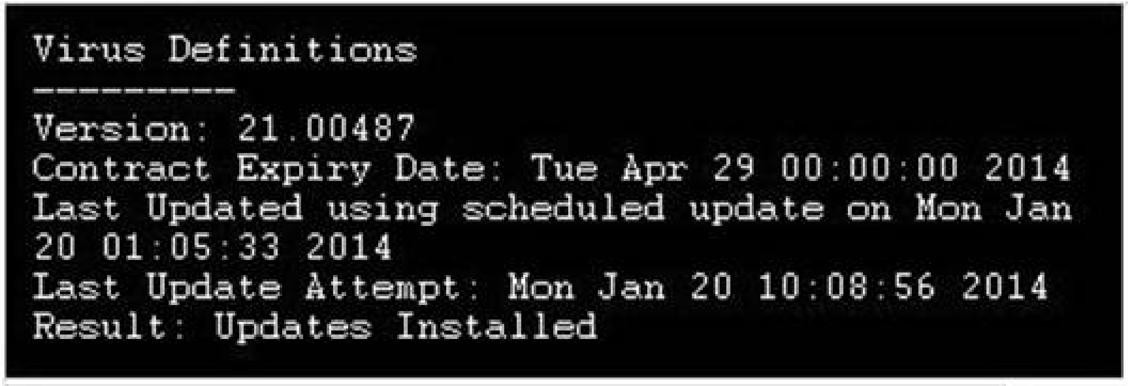
Answer: D

NEW QUESTION 139
Which traffic can match a firewall policy's "Services" setting? (Choose three.)

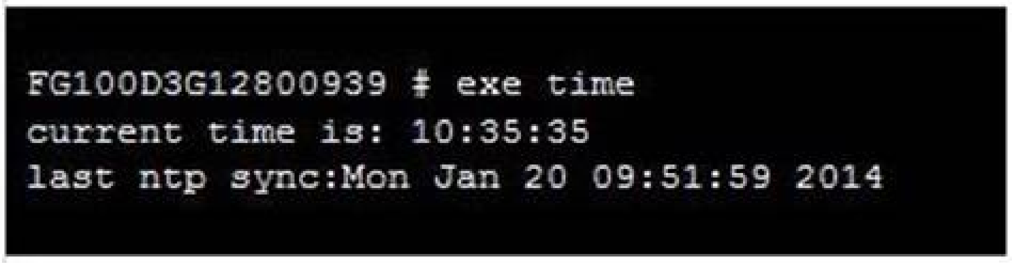
A. HTTP
B. SSL
C. DNS
D. RSS
E. HTTPS

Answer: ACE

NEW QUESTION 143
A FortiGate device is configure to perform an AV & IPS scheduled update every hour.



```
Virus Definitions
---------
Version: 21.00487
Contract Expiry Date: Tue Apr 29 00:00:00 2014
Last Updated using scheduled update on Mon Jan
20 01:05:33 2014
Last Update Attempt: Mon Jan 20 10:08:56 2014
Result: Updates Installed
```



```
FG100D3G12800939 # exe time
current time is: 10:35:35
last ntp sync:Mon Jan 20 09:51:59 2014
```

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

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

Answer: D

NEW QUESTION 146
Which of the following statements describe some of the differences between symmetric and asymmetric cryptography? (Choose two.)

A. In symmetric cryptography, the keys are publicly availabl
B. In asymmetric cryptography, the keys must be kept secret.
C. Asymmetric cryptography can encrypt data faster than symmetric cryptography
D. Symmetric cryptography uses one pre-shared ke
E. Asymmetric cryptography uses a pair or keys
F. Asymmetric keys can be sent to the remote peer via digital certificate
G. Symmetric keys cannot

Answer: CD

NEW QUESTION 148
Which of the following IPsec configuration modes can be used for implementing L2TP- over-IPSec VPNs?

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

Answer: A

NEW QUESTION 149
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 154
Which of the following statements best describes the role of a DC agents in an FSSO DC?

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

Answer: C

NEW QUESTION 156
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 157
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 162
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

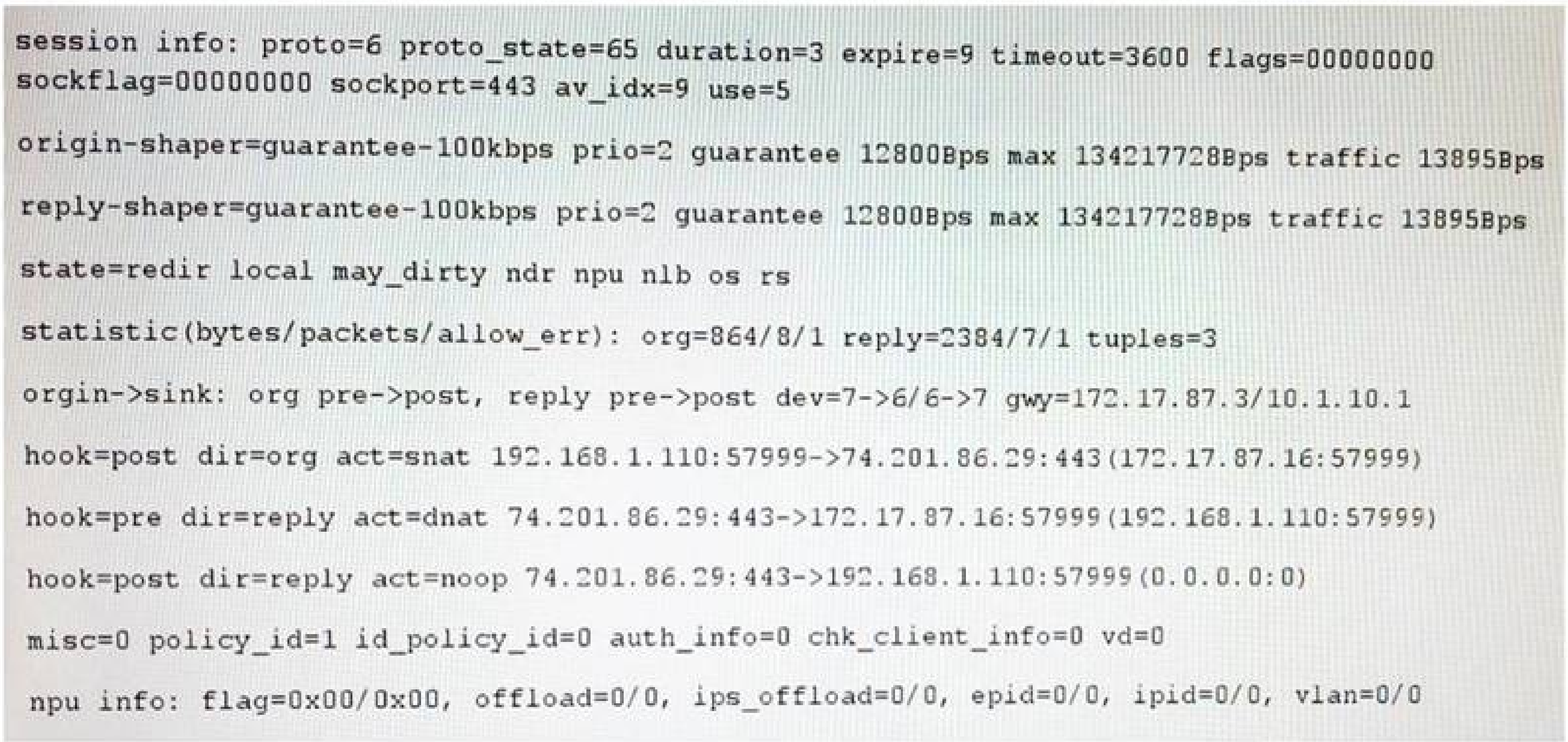
Answer: A

NEW QUESTION 165
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 167
Examine the following output from the diagnose sys session list command:



```
session info: proto=6 proto_state=65 duration=3 expire=9 timeout=3600 flags=00000000
sockflag=00000000 sockport=443 av_idx=9 use=5

origin-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bps

reply-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bps

state=redir local may_dirty ndr npu nlb os rs

statistic(bytes/packets/allow_err): org=864/8/1 reply=2384/7/1 tuples=3

orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.17.87.3/10.1.10.1

hook=post dir=org act=snat 192.168.1.110:57999->74.201.86.29:443(172.17.87.16:57999)

hook=pre dir=reply act=dnat 74.201.86.29:443->172.17.87.16:57999(192.168.1.110:57999)

hook=post dir=reply act=noop 74.201.86.29:443->192.168.1.110:57999(0.0.0.0:0)

misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0

npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0/0
```

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

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

Answer: CD

NEW QUESTION 170
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 171
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 172
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 174
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 176
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 180
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 185
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 189
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 192
Which antivirus and attack definition update options are supported by FortiGate units? (Choose two.)

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

Answer: ABC

NEW QUESTION 196
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 199
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 200
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 202
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 204
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 205
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 207
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 208
In FortiOS session table output, what are the two possible 'proto_state' values for a UDP session? (Choose two.)

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

Answer: AC

NEW QUESTION 213
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 216
Which statements are true about offloading antivirus inspection to a Security Processor (SP)? (Choose two.)

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

Answer: BC

NEW QUESTION 219
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 223
What types of troubleshooting can you do when uploading firmware? (Choose two.)

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

Answer: AD

NEW QUESTION 224
Which of the following FSSO modes must be used for Novell eDirectory networks?

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

Answer: C

NEW QUESTION 227
Examine the following log message attributes and select two correct statements from the list below. (Choose two.)
hostname=www.youtube.com profiletype="Webfilter_Profile" profile="default" status="passthrough" msg="URL belongs to a category with warnings enabled"

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

Answer: CD

NEW QUESTION 228
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

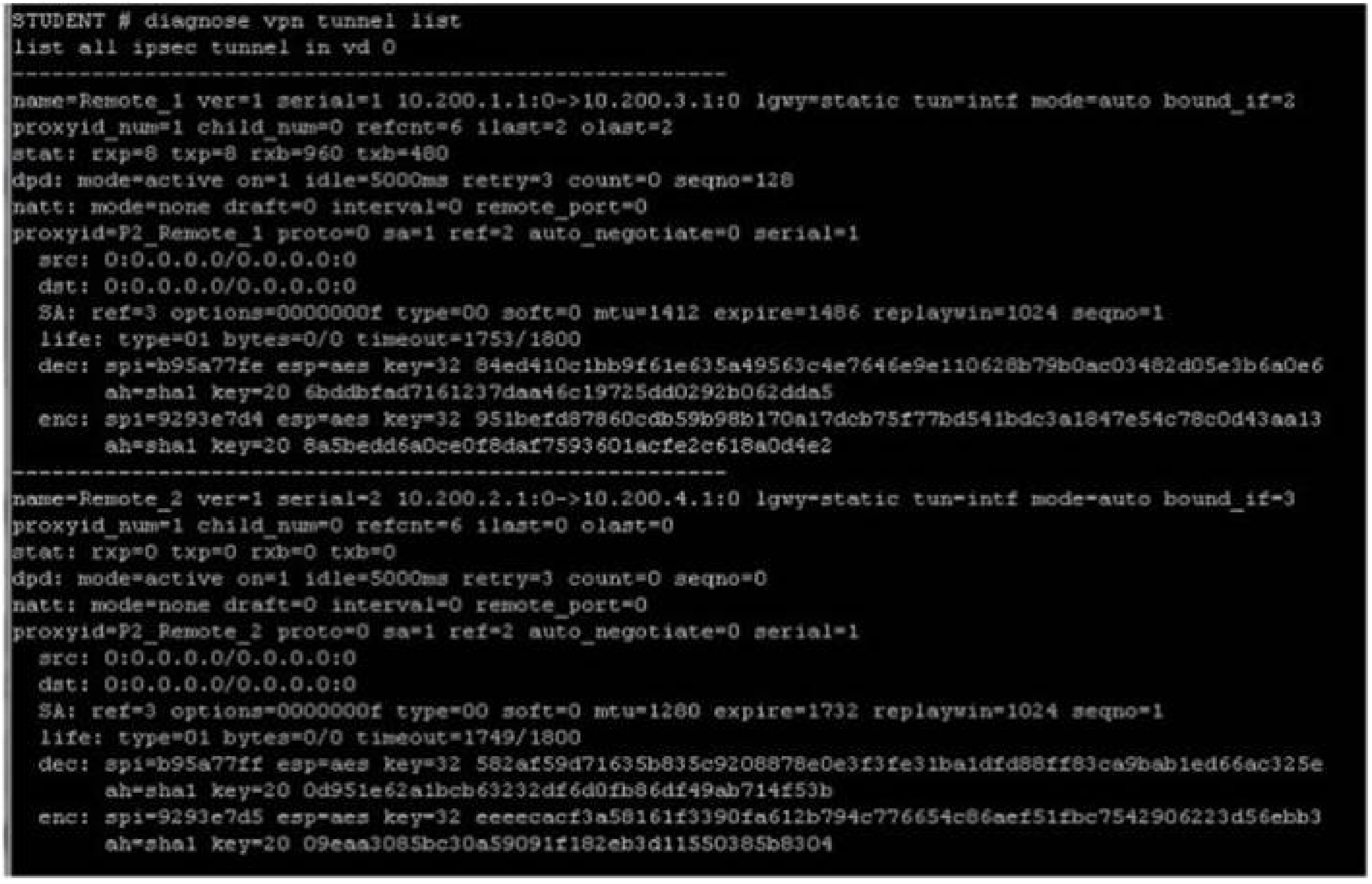
Answer: ABD

NEW QUESTION 232
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 237
Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit.



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

Which statements is correct regarding this output?

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

Answer: C

NEW QUESTION 242
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 246
Which of the following actions that can be taken by the Data Leak Prevention scanning? (Choose three.)

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

Answer: ADE

NEW QUESTION 251
What configuration objects are automatically added when using the FortiGate's FortiClient VPN Configurations Wizard?(Choose two)

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

Answer: BD

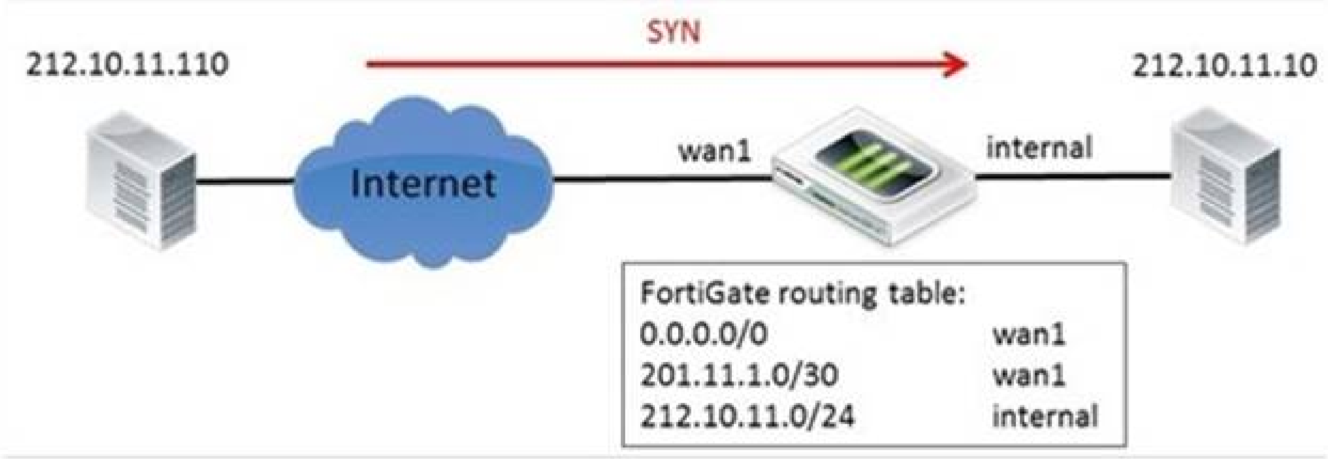
NEW QUESTION 253
Examine the following CLI configuration:
config system session -ttl set default 1800
end
What statement is true about the effect of the above configuration line?

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 256
Examine the network topology diagram in the exhibit; the workstation with the IP address 212.10.11.110 sends a TCP SYN packet to the workstation with the IP address 212.10.11.20.



FortiGate routing table:

0.0.0.0/0	wan1
201.11.1.0/30	wan1
212.10.11.0/24	internal

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

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

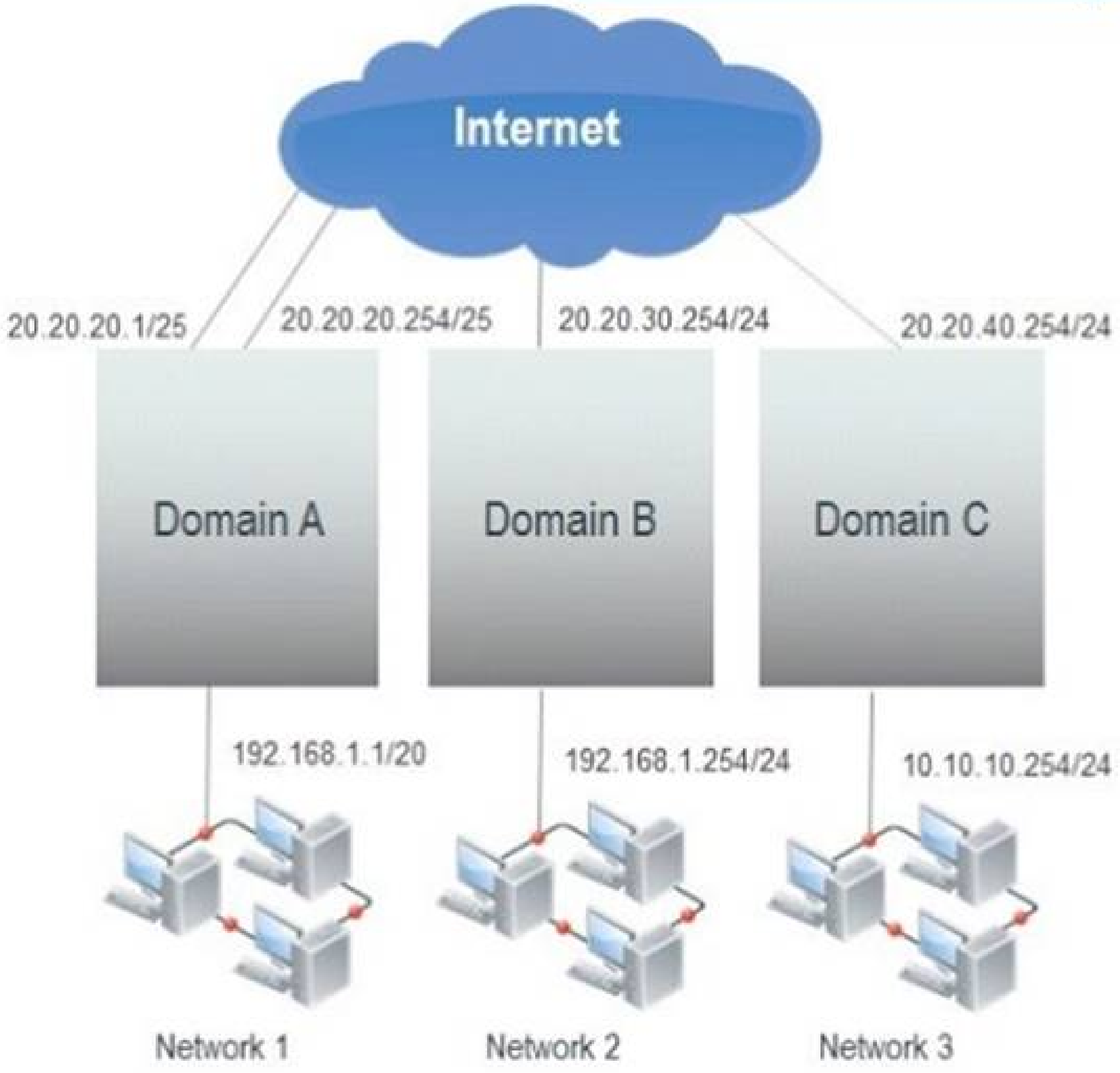
Answer: AD

NEW QUESTION 257
Which statement correctly describes the output of the command diagnose ips anomaly list?

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

Answer: B

NEW QUESTION 258
A FortiGate unit is configured with three Virtual Domains (VDOMs) as illustrated in the exhibit.



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

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

Answer: ABE

NEW QUESTION 259
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 263
Regarding the use of web-only mode SSL VPN, which statement is correct?

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

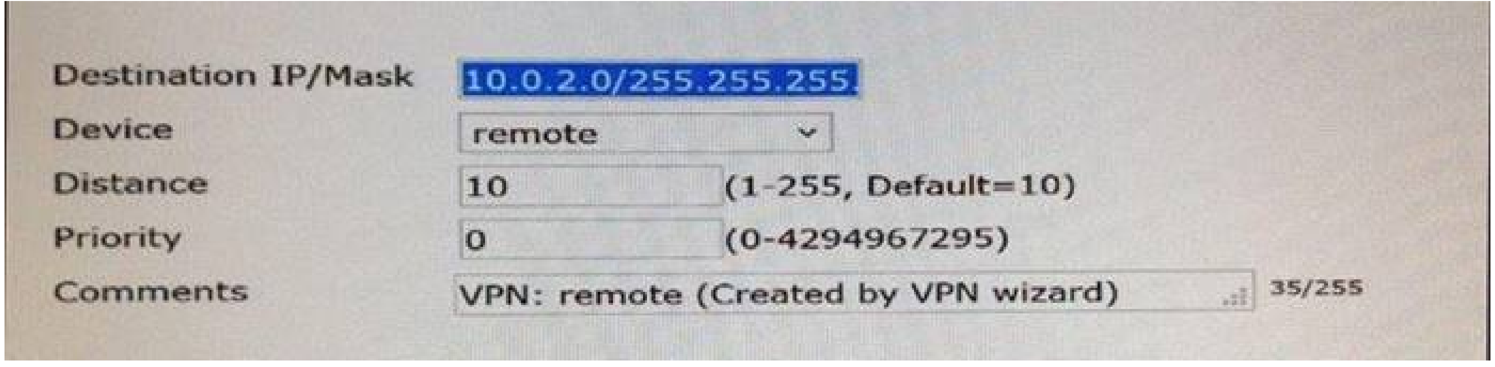
Answer: C

NEW QUESTION 264
Which web filtering inspection mode inspects DNS traffic?

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

Answer: A

NEW QUESTION 267
Review the static route configuration for IPsec shown in the exhibit; then answer the question below.



Destination IP/Mask	10.0.2.0/255.255.255.	
Device	remote	
Distance	10	(1-255, Default=10)
Priority	0	(0-4294967295)
Comments	VPN: remote (Created by VPN wizard)	35/255

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

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

Answer: AB

NEW QUESTION 271
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

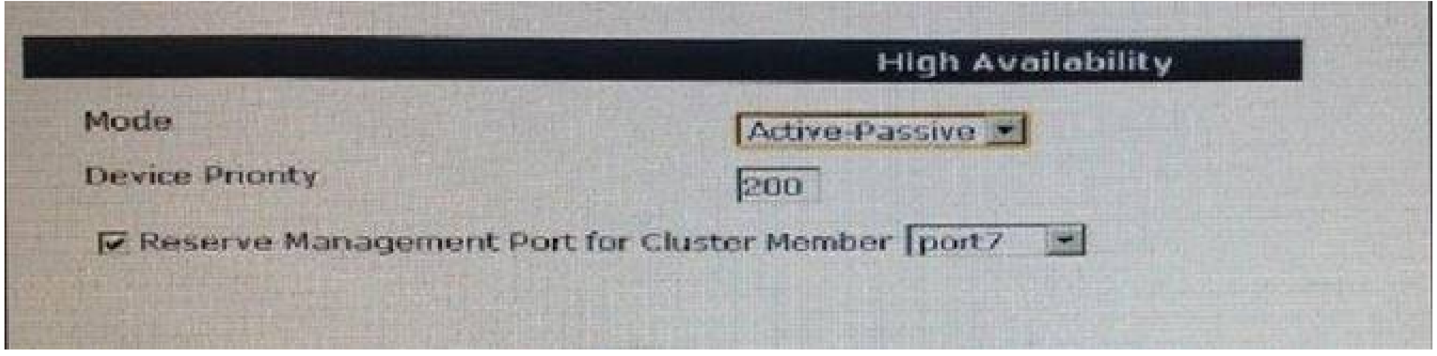
NEW QUESTION 272
Which of the following statements are correct differences between NAT/route and transparent mode? (Choose two.)

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 274
In HA, the option Reserve Management Port for Cluster Member is selected as shown in the exhibit below.



High Availability

Mode Active-Passive

Device Priority 200

☑ Reserve Management Port for Cluster Member port7

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

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

Answer: AD

NEW QUESTION 275
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 278
Two FortiGate units with NP6 processors form an active-active cluster. The cluster is doing security profile (UTM) inspection over all the user traffic.
What statements are true regarding the sessions that the master unit is offloading to the slave unit for inspection? (Choose two.)

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

Answer: AD

NEW QUESTION 283
Which of the following are operating mode supported in FortiGate devices? (Choose two)

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

Answer: BC

NEW QUESTION 285
Which of the following statements is correct regarding FortiGate interfaces and spanning tree protocol? (Choose Two)

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

Answer: BD

NEW QUESTION 290
Which user group types does FortiGate support for firewall authentication? (Choose three.)

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

Answer: ABE

NEW QUESTION 295
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 299
Of the following information, what can be recorded by a Data Leak Prevention sensor configured to do a summary archiving? (Choose three.)

A. Visited URL (for the case of HTTP traffic)
B. Sender email address (for the case of SMTP traffic)
C. Recipient email address (for the case of SMTP traffic)
D. Attached file (for the case of SMTP traffic)
E. Email body (for the case of SMTP traffic)

Answer: BCE

NEW QUESTION 302
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 305
Which of the following statements is true regarding the TCP SYN packets that go from a client, through an implicit web proxy (transparent proxy), to a web server listening at TCP port 80? (Choose three.)

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

Answer: ADE

NEW QUESTION 309
Which IPSec mode includes the peer id information in the first packet?

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

Answer: C

NEW QUESTION 310
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 315
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.

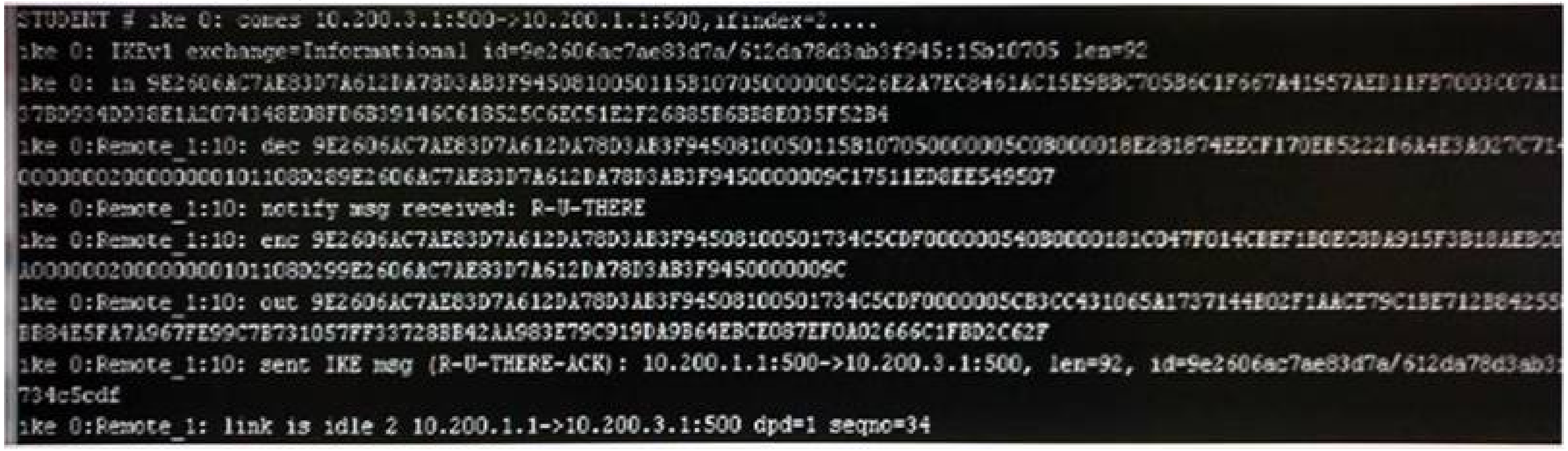
Answer: ABC

NEW QUESTION 318
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 320
Review the IKE debug output for IPsec shown in the exhibit below.



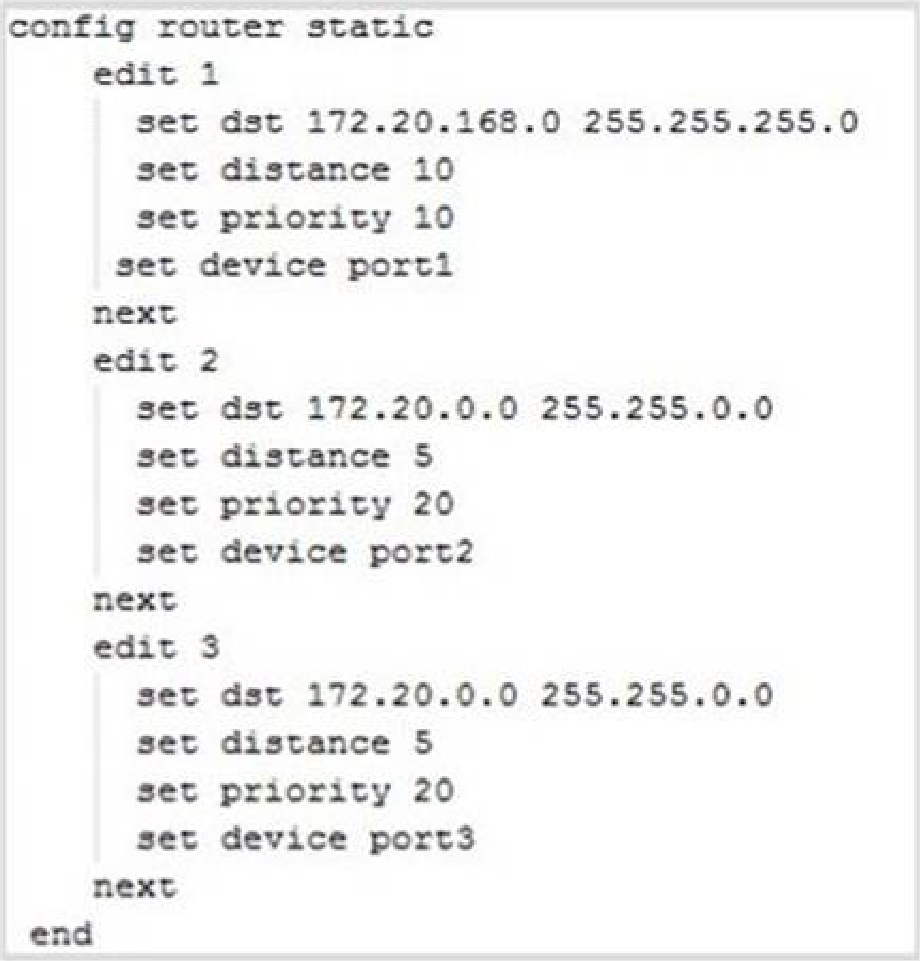
```
STUDENT # ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Informational id=9e2606ac7ae83d7a/612da78d3ab3f945:15b10705 len=92
ike 0: in 9E2606AC7AE83D7A612DA78D3AB3F94508100501158107050000005C26E2A7EC8461AC15E9BBC705B6C1F667A41957AED11FB7003C07A1
37BD934DD38E1A2074348E08FD6B39146C618525C6EC51E2F26885B6BB8E035F52B4
ike 0:Remote_1:10: dec 9E2606AC7AE83D7A612DA78D3AB3F94508100501158107050000005C08000018E281874EECF170EB522206A4E3A027C71
0000000200000000101108D289E2606AC7AE83D7A612DA78D3AB3F9450000009C17511ED8EE549507
ike 0:Remote_1:10: notify msg received: R-U-THERE
ike 0:Remote_1:10: enc 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF00000054080000181C047F014CBEF1B0EC8DA915F3B18AEBC0
A000000200000000101108D299E2606AC7AE83D7A612DA78D3AB3F9450000009C
ike 0:Remote_1:10: out 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF0000005CB3CC431065A1737144B02F1AACE79C1BE712B84255
BB84E5FA7A967FE99C7B731057FF33728BB42AA983E79C919DA9B64EBCE087EF0A02666C1FBD2C62F
ike 0:Remote_1:10: sent IKE msg (R-U-THERE-ACK): 10.200.1.1:500->10.200.3.1:500, len=92, id=9e2606ac7ae83d7a/612da78d3ab3
734c5cdf
ike 0:Remote_1: link is idle 2 10.200.1.1->10.200.3.1:500 dpd=1 seqno=34
```

Which statements is correct regarding this output?

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

Answer: C

NEW QUESTION 325
The exhibit shoes three static routes.



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

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

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

Answer: D

NEW QUESTION 329
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 332
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 336
A FortiGate is configured with three virtual domains (VDOMs). Which of the following statements is correct regarding multiple VDOMs?

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

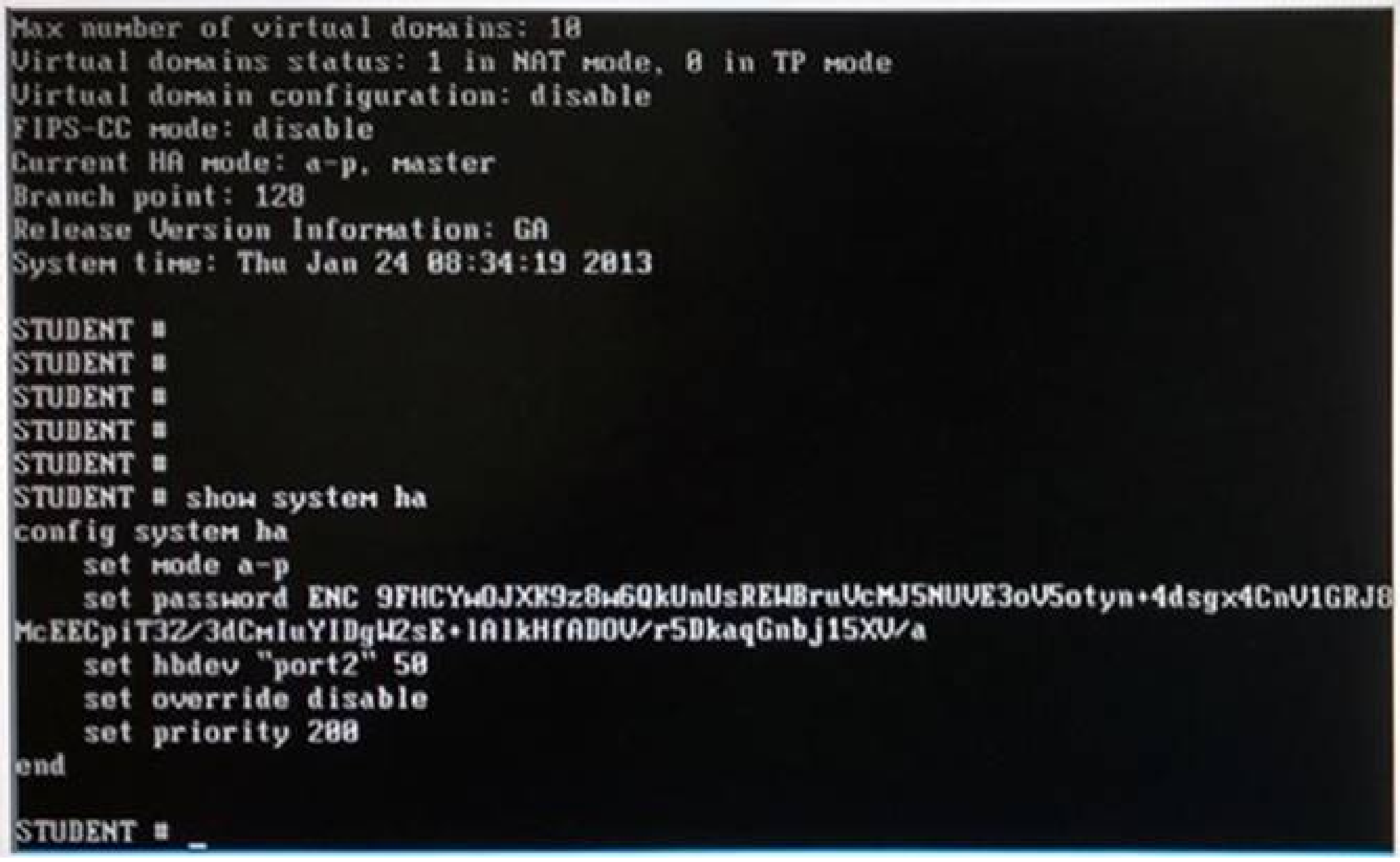
Answer: D

NEW QUESTION 339
Two FortiGate units with NP6 processors form an active-active cluster. The cluster is doing security profile (UTM) inspection over all the user traffic. What statements are true regarding the sessions that the master unit is offloading to the slave unit for inspection? (Choose two.)

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

Answer: BC

NEW QUESTION 340
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:

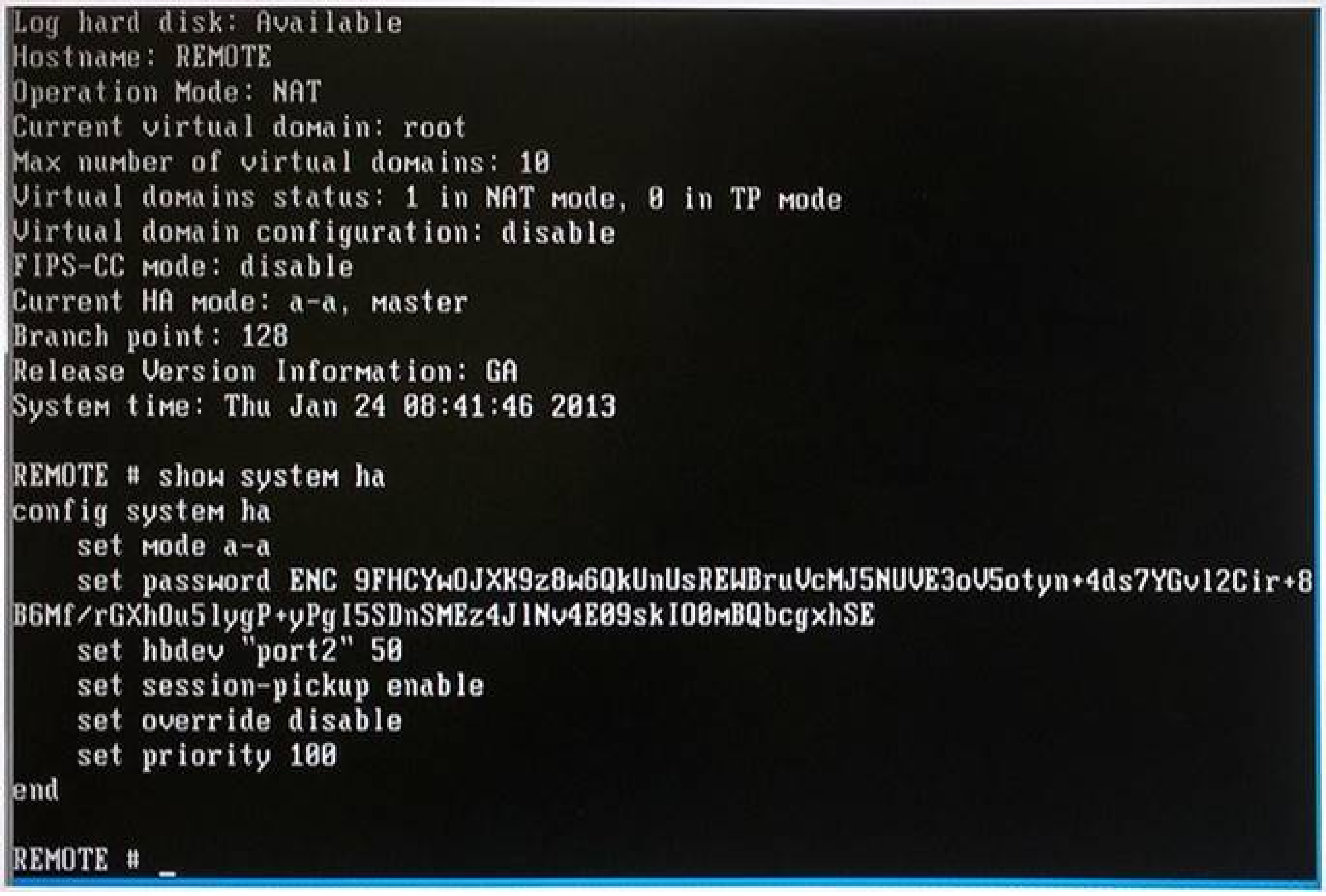


```
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:34:19 2013

STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT # show system ha
config system ha
    set mode a-p
    set password ENC 9FHCYwOJXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4dsgx4CnV1GRJ8
McEECpiT32/3dCmIuYIDgW2sE+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+yPgI5SDnSMEz4JlNv4E09skI00mBQbcgxhSE
    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 341
Which of the following statements is true regarding the differences between route-based and policy-based IPsec VPNs? (Choose two.)

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

Answer: AC

NEW QUESTION 343
When firewall policy authentication is enabled, which protocols can trigger an authentication challenge? (Choose two.)

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

Answer: CD

NEW QUESTION 345
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.

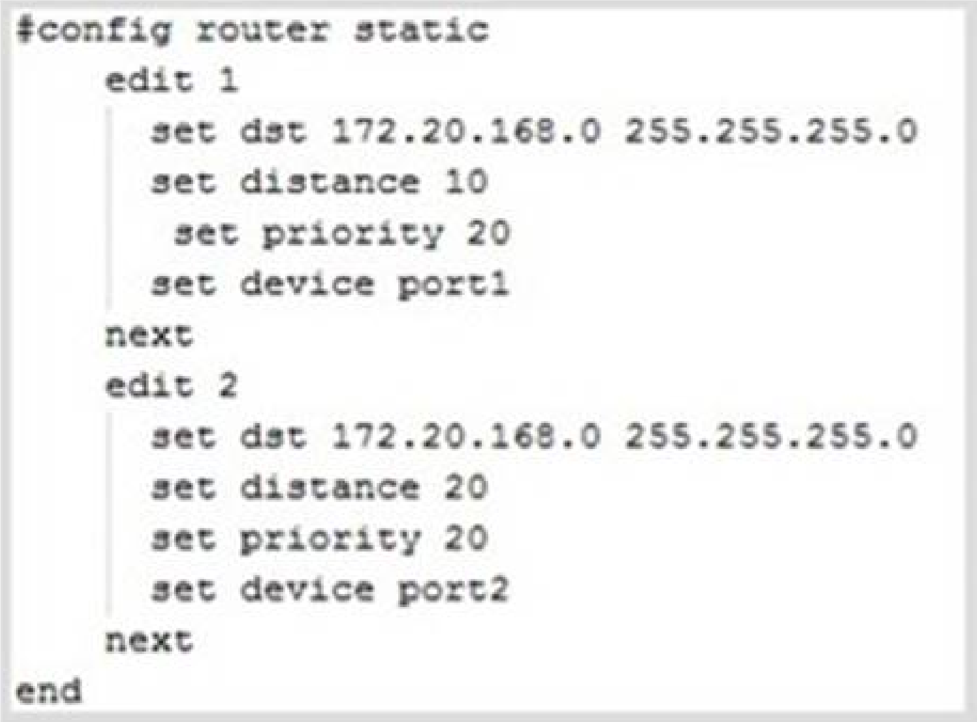
Answer: AB

NEW QUESTION 350
What is IPsec Perfect Forwarding Secrecy (PFS)?

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

Answer: B

NEW QUESTION 353
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 355
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 357
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 360
What is longest length of time allowed on a FortiGate device for the virus scan to complete?

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

Answer: B

NEW QUESTION 363
......