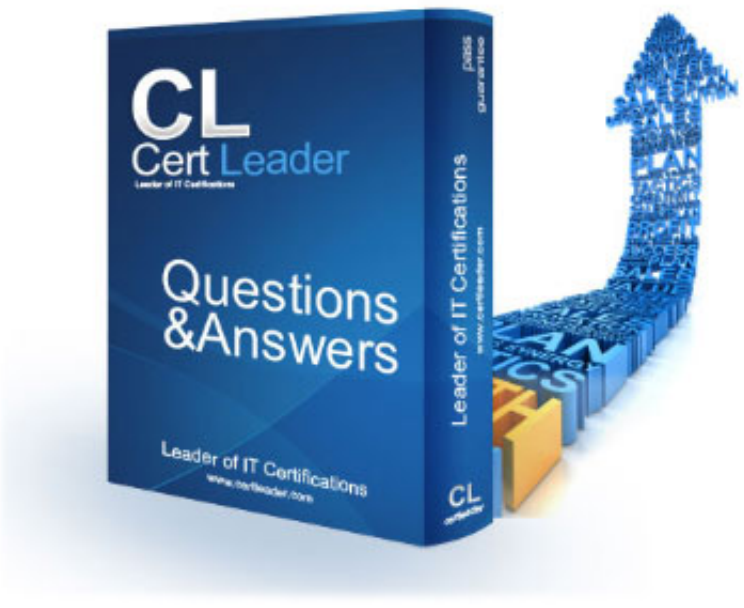
# NSE4 Dumps

# Fortinet Network Security Expert 4 Written Exam (400)

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



**NEW QUESTION 1**
Examine the two static routes to the same destination subnet 172.20.168.0/24 as shown below; then answer the question following it.

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

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

A. The FortiGate evenly shares the traffic to 172.20.168.0/24 through both routes.
B. The FortiGate shares the traffic to 172.20.168.0/24 through both routes, but the port2 route will carry approximately twice as much of the traffic.
C. The FortiGate sends all the traffic to 172.20.168.0/24 through port1.
D. Only the route that is using port1 will show up in the routing table.

**Answer:** C

**NEW QUESTION 2**
What protocol cannot be used with the active authentication type?

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

**Answer:** D

**NEW QUESTION 3**
How is traffic routed onto an SSL VPN tunnel from the FortiGate unit side?

A. A static route must be configured by the administrator using the ssl.root interface as the outgoing interface.
B. Assignment of an IP address to the client causes a host route to be added to the FortiGate unit's kernel routing table.
C. A route back to the SSLVPN IP pool is automatically created on the FortiGate unit.
D. The FortiGate unit adds a route based upon the destination address in the SSL VPN firewall policy.

**Answer:** B

**NEW QUESTION 4**
Which of the following settings can be configured per VDOM? (Choose three)

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

**Answer:** ABE

**NEW QUESTION 5**
Examine the exhibit; then answer the question below.


The Vancouver FortiGate initially had the following information in its routing table:
S 172.20.0.0/16 [10/0] via 172.21.1.2, port2
C 172.21.0.0/16 is directly connected, port2
C 172.11.11.0/24 is directly connected, port1
Afterwards, the following static route was added:

config router static edit 6
set dst 172.20.1.0 255.255.255.0
set priority 0
set device port1
set gateway 172.11.12.1 next
Since this change, the new static route is NOT showing up in the routing table. Given the information provided, which of the following describes the cause of this problem?

A. The subnet 172.20.1.0/24 is overlapped with the subnet of one static route that is already in the routing table (172.20.0.0/16), so, we need to enable allow-subnet-overlap first.
B. The 'gateway' IP address is NOT in the same subnet as the IP address of port1.
C. The priority is 0, which means that the route will remain inactive.
D. The static route configuration is missing the distance setting.

**Answer:** B

**NEW QUESTION 6**
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 7**
Files reported as "suspicious" were subject to which Antivirus check"?

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

**Answer:** D

**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.

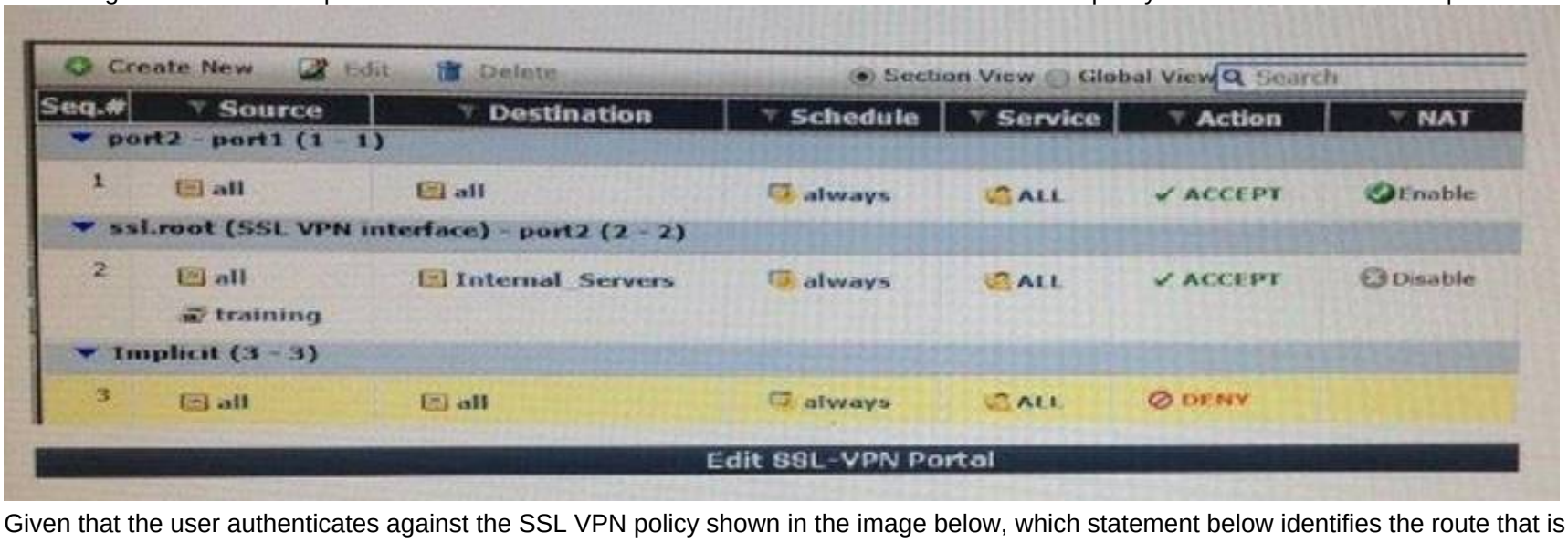
**Answer:** BD

**NEW QUESTION 9**
What methods can be used to deliver the token code to a user that is configured to use
two-factor authentication? (Choose three.)

A. Browser pop-up window.
B. FortiToken.
C. Email.
D. Code books.
E. SMS phone message.

**Answer:** BCE

**NEW QUESTION 10**
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:




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

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

**Answer:** AD

**NEW QUESTION 15**
Which of the following statements are true regarding application control? (Choose two.)

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

**Answer:** CD

**NEW QUESTION 19**
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 20**
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 21**
You are creating a custom signature. Which has incorrect syntax?

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

**Answer:** A

**NEW QUESTION 22**
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 25**
Which statement is not correct regarding SSL VPN Tunnel mode?

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

**Answer:** C

**NEW QUESTION 30**
Which of the following statements best describes what a Public Certificate Authority (CA) is?

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

**Answer:** D

**NEW QUESTION 35**
Which of the following statement correct describes the use of the "diagnose sys ha reset- uptime" command?

A. To force an HA failover when the HA override setting is disabled.

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

**Answer:** A

**NEW QUESTION 36**
What determines whether a log message is generated or not?

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

**Answer:** A

**NEW QUESTION 38**
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 43**
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 48**
Which of the following statements best describes what a Certificate Signing Request (CSR) is?

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

**Answer:** B

**NEW QUESTION 53**
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 58**
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 60**

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

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

**Answer:** AD

**NEW QUESTION 62**
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 67**
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 70**
Which is an advantage of using SNMP v3 instead of SNMP v1/v2 when querying a FortiGate unit?

A. MIB-based report uploads.
B. SNMP access limited by access lists.
C. Packet encryption.
D. Running SNMP service on a non-standard port is possible.

**Answer:** C

**NEW QUESTION 72**
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 77**
Which statement describes what the CLI command diagnose debug authd fsso list is used for?

A. Monitors communications between the FSSO collector agent and FortiGate unit.
B. Displays which users are currently logged on using FSSO.
C. Displays are listing of all connected FSSO collector agents.
D. Lists all DC Agents installed on all domain controllers.

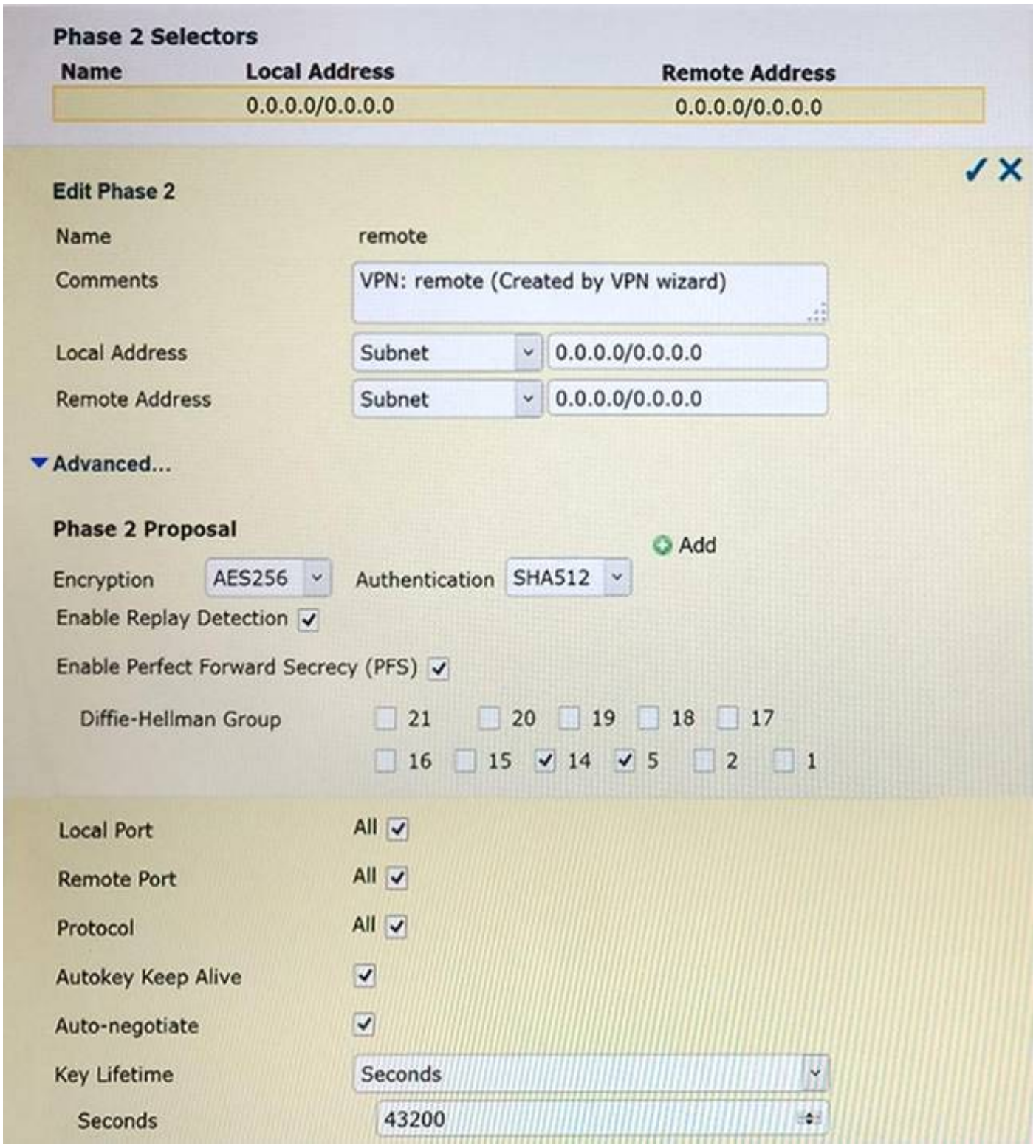
**Answer:** B

**NEW QUESTION 81**
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 86**
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 87**
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 89**
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 91**
Which statements regarding banned words are correct? (Choose two.)

A. Content is automatically blocked if a single instance of a banned word appears.
B. The FortiGate updates banned words on a periodic basis.

C. The FortiGate can scan web pages and email messages for instances of banned words.
D. Banned words can be expressed as simple text, wildcards and regular expressions.

**Answer:** CD

**NEW QUESTION 93**
Which operating system vulnerability can you protect when selecting signatures to include in an IPS sensor? (choose three)

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

**Answer:** CDE

**NEW QUESTION 96**
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 101**
Which of the following statements are correct concerning IPsec dialup VPN configurations for FortiGate devices? (Choose two)

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

**Answer:** CD

**NEW QUESTION 103**
In a FSSO agent mode solution, how does the FSSO collector agent learn each IP address?

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

**Answer:** D

**NEW QUESTION 105**
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 109**
Which statement describes how traffic flows in sessions handled by a slave unit in an active-active HA cluster?

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

**Answer:** D

**NEW QUESTION 112**
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 113**
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 115**
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 120**
Which statement best describes what a Fortinet System on a Chip (SoC) is?

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

**Answer:** B

**NEW QUESTION 122**
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 124**
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 128**
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 132**
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 135**
Which of the following statements are true regarding traffic accelerated by an NP processor? (Choose two.)

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

**Answer:** AD

**NEW QUESTION 140**
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 145**
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

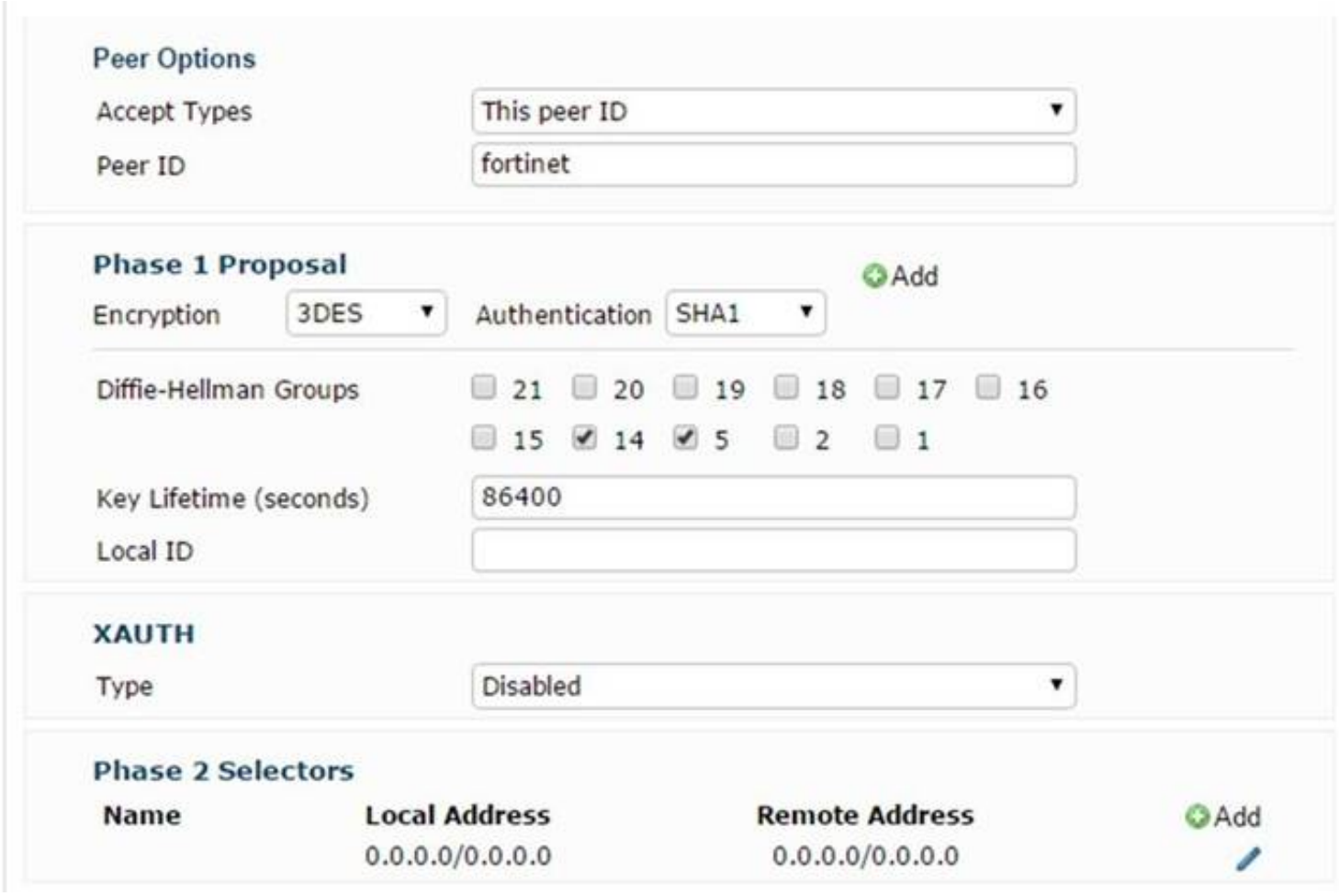
**Answer:** D

**NEW QUESTION 148**
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 153**
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 155**
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 158**
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 161**
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 8a5bedd6a0ce0f8daf759360lacfe2c618a0d4e2
------------------------------------------------------
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 582af59d71635b835c92O8878e0e3f3fe31ba1dfd88ff83ca9bab1ed66ac325e
       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 166**
Which of the following statements are correct concerning layer 2 broadcast domains in transparent mode VDOMs?(Choose two)

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

**Answer:** BC

**NEW QUESTION 171**
Which IP packets can be hardware-accelerated by a NP6 processor? (Choose two.)

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

**Answer:** BC

**NEW QUESTION 175**
Which of the following statements are correct about the HA command diagnose sys ha reset-uptime? (Choose two.)

A. The device this command is executed on is likely to switch from master to slave status if override is disabled.
B. The device this command executed on is likely to switch from master to slave status if override is enabled.
C. The command has no impact on the HA algorithm.
D. This commands resets the uptime variable used in the HA algorithm so it may cause a new master to become elected.

**Answer:** AD

**NEW QUESTION 178**
How many packets are interchanged between both IPSec ends during the negotiation of a main-mode phase 1?

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

**Answer:** D

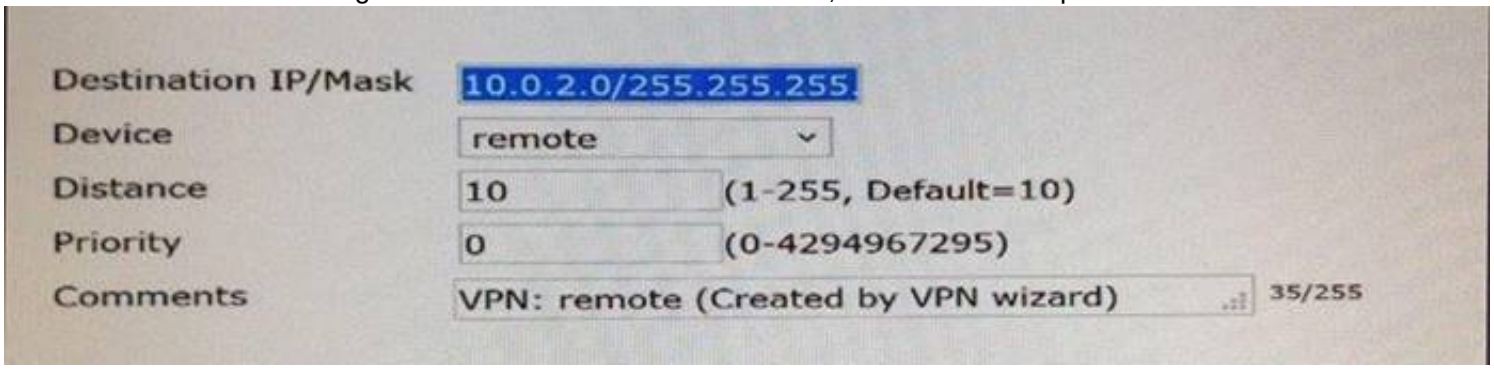
**NEW QUESTION 180**

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

A. Policy-based VPN only
B. Both policy-based and route-based VPN.
C. Route-based VPN only.
D. IPSec VPNs are not supported when the FortiGate is running in NAT mode.

**Answer:** B

**NEW QUESTION 182**
Review the static route configuration for IPsec shown in the exhibit; then answer the question below.




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

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

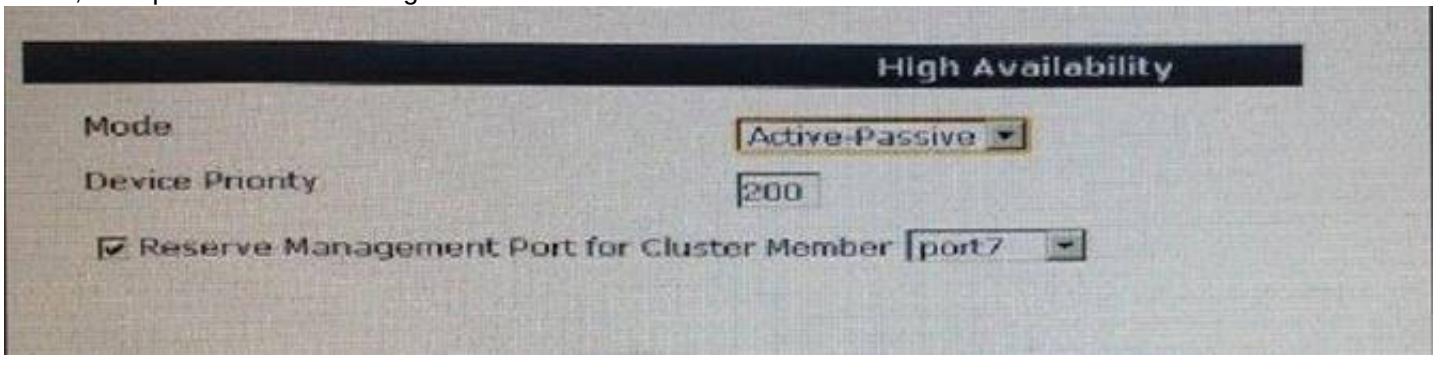
**Answer:** AB

**NEW QUESTION 186**
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 187**
In HA, the option Reserve Management Port for Cluster Member is selected as shown in the exhibit below.




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

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

**Answer:** AD

**NEW QUESTION 188**
Which of the following statements are characteristics of a FSSO solution using advanced access mode? (Choose three.)

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

**Answer:** BCE

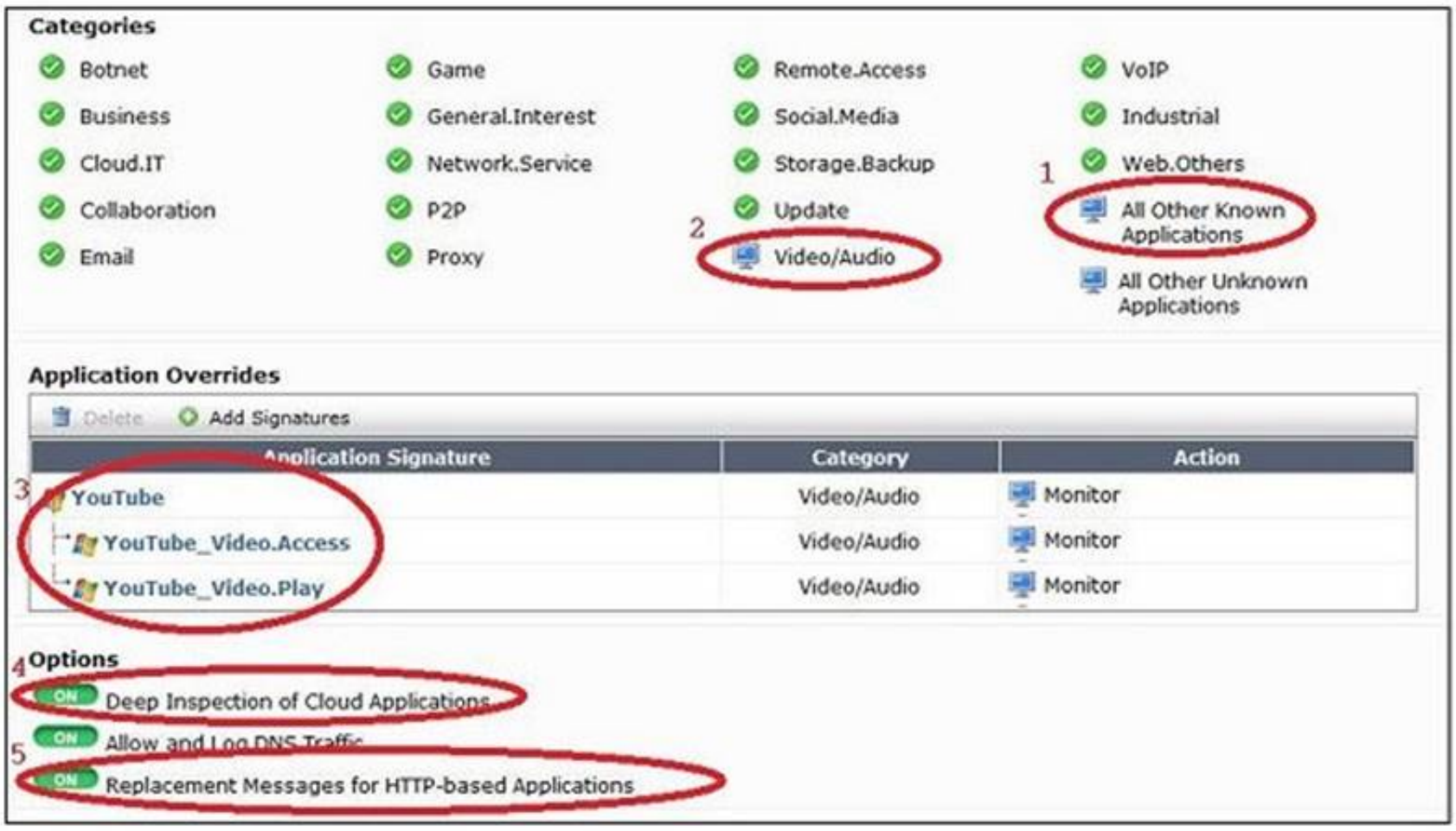
**NEW QUESTION 190**
Which of the following statements are correct regarding FortiGate virtual domains (VDOMs)? (Choose two)

A. VDOMs divide a single FortiGate unit into two or more independent firewall.
B. A management VDOM handles SNM

C. logging, alert email and FortiGuard updates.
D. Each VDOM can run different firmware versions.
E. Administrative users with a 'super_admin' profile can administrate only one VDOM.

**Answer:** AB

**NEW QUESTION 195**
The exhibit is a screen shot of an Application Control profile.




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

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

**Answer:** D

**NEW QUESTION 200**
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 201**
Which of the following sequences describes the correct order of criteria used for the selection of a master unit within a FortiGate high availability (HA) cluster when override is disabled?

A. 1. port monitor, 2. unit priority, 3. up time, 4. serial number.
B. 1. port monitor, 2. up time, 3. unit priority, 4. serial number.
C. 1. unit priority, 2. up time, 3. port monitor, 4. serial number.
D. 1. up time, 2. unit priority, 3. port monitor, 4. serial number.

**Answer:** B

**NEW QUESTION 205**
Examine this log entry.
What does the log indicate? (Choose three.)
date=2013-12-04 time=09:30:18 logid=0100032001 type=event subtype=system level=information vd="root" user="admin" ui=http(192.168.1.112) action=login status=success reason=none profile="super_admin" msg="Administrator admin logged in successfully from http(192.168.1.112)"

A. In the GUI, the log entry was located under “Log & Report > Event Log > User”.
B. In the GUI, the log entry was located under “Log & Report > Event Log > System”.
C. In the GUI, the log entry was located under “Log & Report > Traffic Log > Local Traffic”.
D. The connection was encrypted.

E. The connection was unencrypted.
F. The IP of the FortiGate interface that “admin” connected to was 192.168.1.112.
G. The IP of the computer that “admin” connected from was 192.168.1.112.

**Answer:** BEG

**NEW QUESTION 209**
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 214**
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 218**
What is the default criteria for selecting the HA master unit in a HA cluster?

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

**Answer:** B

**NEW QUESTION 221**
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 224**
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 227**
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 229**
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 230**
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

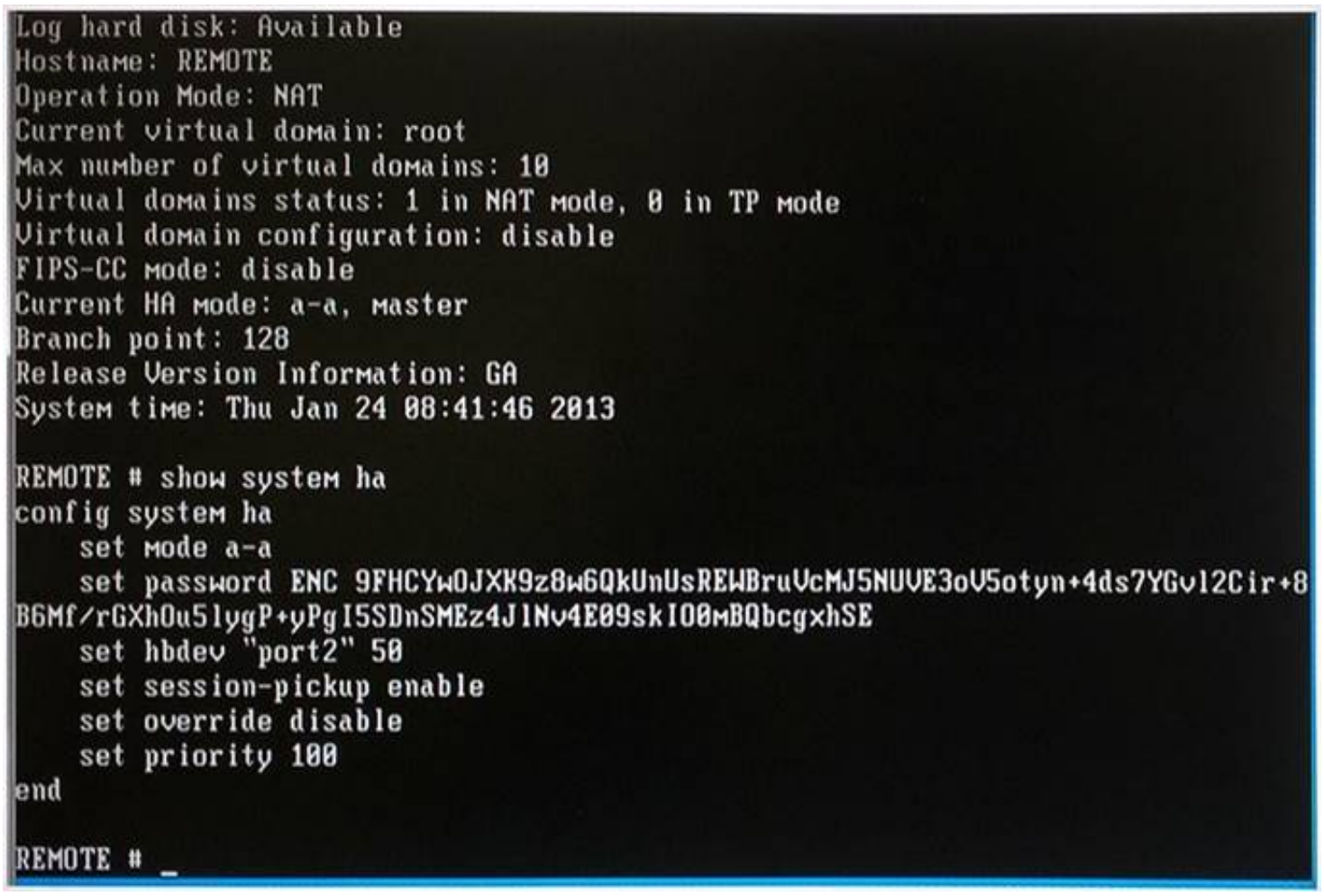
**NEW QUESTION 233**
Two FortiGate devices fail to form an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of show system ha for the STUDENT device. Exhibit B shows the command output of show system ha for the REMOTE device.
Exhibit A:

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

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

STUDENT #
```

Exhibit B:




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 235**
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 238**
An administrator wants to create an IPsec VPN tunnel between two FortiGate devices.
Which three configuration steps must be performed on both units to support this scenario? (Choose three.)

A. Create firewall policies to allow and control traffic between the source and destination IP addresses.
B. Configure the appropriate user groups to allow users access to the tunnel.
C. Set the operating mode to IPsec VPN mode.
D. Define the phase 2 parameters.
E. Define the Phase 1 parameters.

**Answer:** ADE

**NEW QUESTION 240**
Which of the following options best defines what Diffie-Hellman is?

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

**Answer:** B

**NEW QUESTION 241**
To which remote device can the FortiGate send logs? (Choose three.)

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

**Answer:** ABE

**NEW QUESTION 242**
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 247**
What are the ways FortiGate can monitor logs? (Choose three.)

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

**Answer:** CDF

**NEW QUESTION 249**
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 253**
Which of the following statements are true about PKI users created in a FortiGate device? (Choose two.)

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

**Answer:** AB

**NEW QUESTION 255**
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 259**
.....

# 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