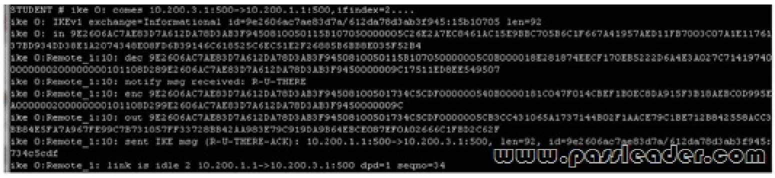
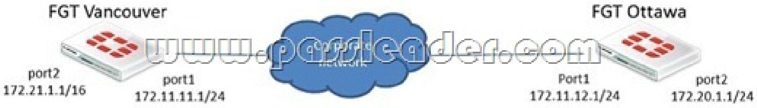
[2016-NEW! PassLeader NSE5 PDF And VCE Dumps For Free Download (Question 121 &ndash; Question 140)

Want to pass your NSE5 exam? Why not trying PassLeader's NSE5 VCE or PDF dumps? We PassLeader now are offering the accurate 240q NSE5 exam questions and answers, you can get all the real exam questions from our NSE5 exam dumps. All our 240q NSE5 practice tests are the newest and same with the real test. We ensure that you can pass NSE5 exam easily with our premium NSE5 study guide! Now visit passleader.com to get the valid NSE5 braindumps with free version VCE Player! keywords: NSE5 exam,240q NSE5 exam dumps,240q NSE5 exam questions,NSE5 pdf dumps,NSE5 vce dumps,NSE5 braindumps,NSE5 practice tests,NSE5 study guide,Fortinet Network Security Analyst Exam P.S. Download Free NSE5 PDF Dumps and Get Premium PassLeader NSE5 VCE Dumps At The End Of This Post!!! (Ctrl+End) QUESTION 121Examine the static route configuration shown below; then answer the question following it.config router staticedit 1set dst 172.20.1.0 255.255.255.0set device port1set gateway 172.11.12.1set distance 10set weight 5nextedit 2set dst 172.20.1.0 255.255.255.0set blackhole enableset distance 5set weight 10nextendWhich of the following statements correctly describes the static routing configuration provided? (Select all that apply.) A. All traffic to 172.20.1.0/24 will always be dropped by the FortiGate unit.B. As long as port1 is up, all the traffic to 172.20.1.0/24 will be routed by the static route number 1. If the interface port1 is down, the traffic will be routed using the blackhole route.C. The FortiGate unit will NOT create a session entry in the session table when the traffic is being routed by the blackhole route.D. The FortiGate unit will create a session entry in the session table when the traffic is being routed by the blackhole route.E. Traffic to 172.20.1.0/24 will be shared through both routes. Answer: AC QUESTION 122Review the IKE debug output for IPsec shown in the Exhibit below.

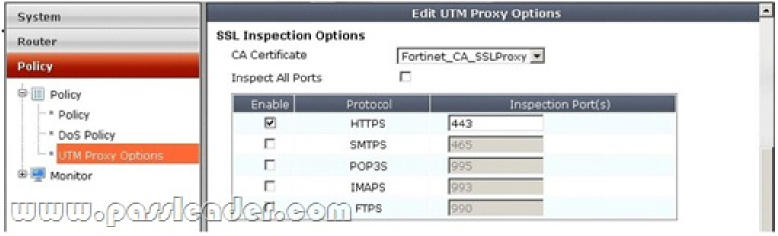


```
STUDENT # ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Informational id=9e2606ac7ae83d7a/612da78d3ab3f945:15b10705 len=92
ike 0: in 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C26E2A7EC8461AC15E9BBC705B6C1F667A41957AED11FB7003C07A1E11761
37BD934DD38E1A2074348E08FD6B39146C618525C6EC51E2F2468586BB8E035F52B4
ike 0:Remote_1:10: dec 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C0B000018E281874EECF170EB5222D6A4E3A027C71419740
000000020000000101108D289E2606AC7AE83D7A612DA78D3AB3F9450000009C17511ED8EE549507
ike 0:Remote_1:10: notify msg received: R-U-THERE
ike 0:Remote_1:10: enc 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF00000054080000181C047F014CBEF1B0EC8DA915F3B18AEBC0D995E
A00000020000000101108D299E2606AC7AE83D7A612DA78D3AB3F9450000009C
ike 0:Remote_1:10: out 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF0000005CB3CC431065A1737144B02F1AACE79C1BE712B842558ACC3
BB84E5FA7A967FE99C7B731057FF33728BB42AA983E79C919DA9B64EBCE087EF0A02666C1FB82C62F
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/612da78d3ab3f945:
734c5cdf
ike 0:Remote_1: link is idle 2 10.200.1.1->10.200.3.1:500 dpd=1 seqno=34
```

Which one of the following 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 QUESTION 123In Transparent Mode, forward-domain is an attribute of ______________. A. an interfaceB. a firewall policyC. a static routeD. a virtual domain Answer: A QUESTION 124Examine the Exhibit shown below; then answer the question following it.



The Vancouver FortiGate unit initially had the following information in its routing table:S 172.20.0.0/16 [10/0] via 172.21.1.2, port2C 172.21.0.0/16 is directly connected, port2C 172.11.11.0/24 is directly connected, port1Afterwards, the following static route was added:config router staticedit 6set dst 172.20.1.0 255.255.255.0set pririoty 0set device port1set gateway 172.11.12.1nextend 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 QUESTION 125Examine the exhibit shown below then answer the question that follows it.



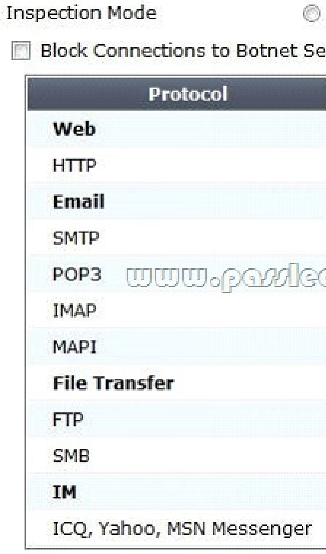
SSL Inspection Options

CA Certificate: Fortinet_CA_SSLProxy

Inspect All Ports ☐

Enable	Protocol	Inspection Port(s)
☑	HTTPS	443
☐	SMTPS	465
☐	POP3S	995
☐	IMAPS	993
☐	FTPS	990

Within the UTM Proxy Options, the CA certificate Fortinet_CA_SSLProxy defines which of the following: A. FortiGate unit's encryption certificate used by the SSL proxy.B. FortiGate unit's signing certificate used by the SSL proxy.C. FortiGuard's signing certificate used by the SSL proxy.D. FortiGuard's encryption certificate used by the SSL proxy. Answer: A QUESTION 126The eicar test virus is put into a zip archive, which is given the password of "Fortinet" in order to open the archive. Review the configuration in the exhibits shown below; then answer the question that follows.Exhibit A - Antivirus Profile:

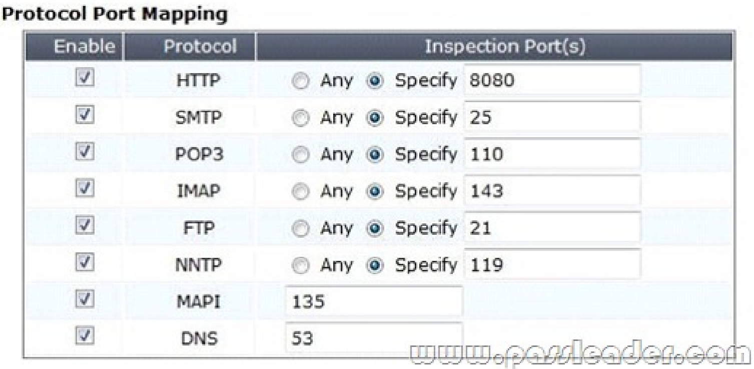


Inspection Mode ○

☐ Block Connections to Botnet Se

Protocol
Web
HTTP
Email
SMTP
POP3
IMAP
MAPI
File Transfer
FTP
SMB
IM
ICQ, Yahoo, MSN Messenger

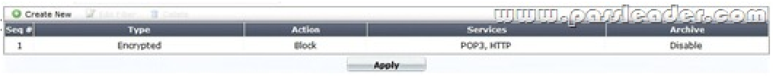
Exhibit B - Non-default UTM Proxy Options Profile:



Protocol Port Mapping

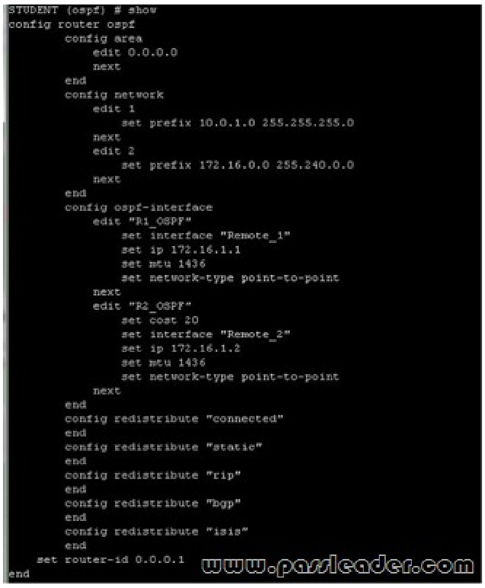
Enable	Protocol	Inspection Port(s)
☑	HTTP	○ Any ● Specify 8080
☑	SMTP	○ Any ● Specify 25
☑	POP3	○ Any ● Specify 110
☑	IMAP	○ Any ● Specify 143
☑	FTP	○ Any ● Specify 21
☑	NNTP	○ Any ● Specify 119
☑	MAPI	135
☑	DNS	53

Exhibit C - DLP Profile:



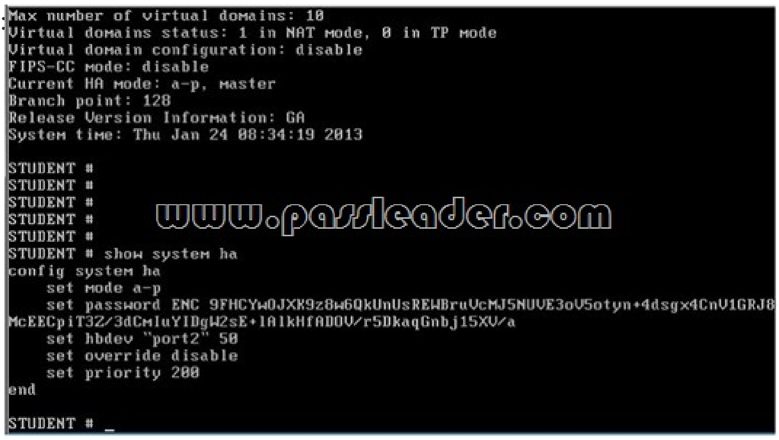
Seq #	Type	Action	Services	Archive
1	Encrypted	Block	POP3, HTTP	Disable

Which of one the following profiles could be enabled in order to prevent the file from passing through the FortiGate device over HTTP on the standard port for that protocol? A. Only Exhibit AB. Only Exhibit BC. Only Exhibit C with default UTM Proxy settings.D. All of the Exhibits (A, B and C)E. Only Exhibit C with non-default UTM Proxy settings (Exhibit B). Answer: C QUESTION 127Data Leak Prevention archiving gives the ability to store files and message data onto a FortiAnalyzer unit for which of the following types of network traffic? (Select all that apply.) A. SNMPB. IPSecC. SMTPD. POP3E. HTTP Answer: CDE QUESTION 128Review the output of the command config router ospf shown in the Exhibit below; then answer the question following it.



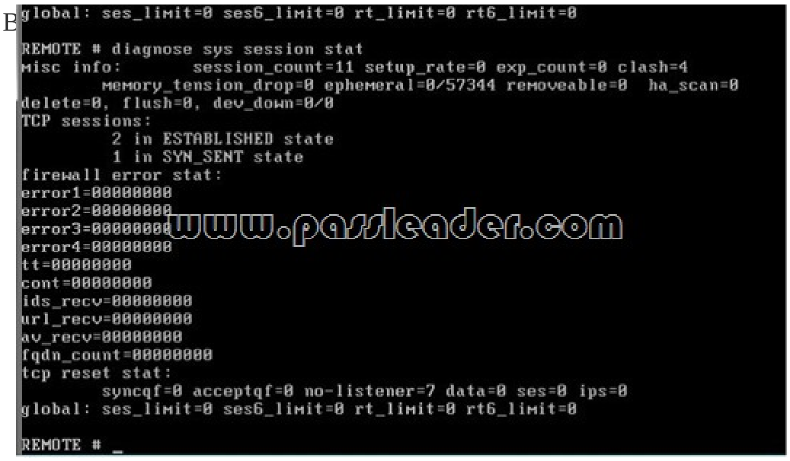
```
STUDENT (ospf) # show
config router ospf
        config area
            edit 0.0.0.0
            next
        end
        config network
            edit 1
                set prefix 10.0.1.0 255.255.255.0
            next
            edit 2
                set prefix 172.16.0.0 255.240.0.0
            next
        end
        config ospf-interface
            edit "R1_OSPF"
                set interface "Remote_1"
                set ip 172.16.1.1
                set mtu 1436
                set network-type point-to-point
            next
            edit "R2_OSPF"
                set cost 20
                set interface "Remote_2"
                set ip 172.16.1.2
                set mtu 1436
                set network-type point-to-point
            next
        end
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "rip"
        end
        config redistribute "bgp"
        end
        config redistribute "isis"
        end
    set router-id 0.0.0.1
end
```

Which one of the following statements is correct regarding this output? A. OSPF Hello packets will only be sent on interfaces configured with the IP addresses 172.16.1.1 and 172.16.1.2.B. OSPF Hello packets will be sent on all interfaces of the FortiGate device.C. OSPF Hello packets will be sent on all interfaces configured with an address matching the 10.0.1.0/24 and 172.16.0.0/12 networks.D. OSPF Hello packets are not sent on point-to-point networks. Answer: C QUESTION 129In a High Availability cluster operating in Active-Active mode, which of the following correctly describes the path taken by the SYN packet of an HTTP session that is offloaded to a subordinate unit? A. Request: Internal Host; Master FortiGate; Slave FortiGate; Internet; Web Server B. Request: Internal Host; Master FortiGate; Slave FortiGate; Master FortiGate; Internet; Web ServerC. Request: Internal Host; Slave FortiGate; Internet; Web ServerD. Request: Internal Host; Slave FortiGate; Master FortiGate; Internet; Web Server Answer: A QUESTION 130Two 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:



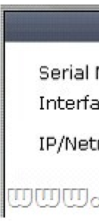
```
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:34:19 2013

STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT # show system ha
config system ha
    set mode a-p
    set password ENC 9FHCYw0JXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4dsgx4CnV1GRJ8
McEECpiT3Z/3dCmIuYIDgW2sE+1A1kHfADOV/r5DkaqGnbj15XV/a
    set hbdev "port2" 50
    set override disable
    set priority 200
end

STUDENT # _
```

Exhibit B

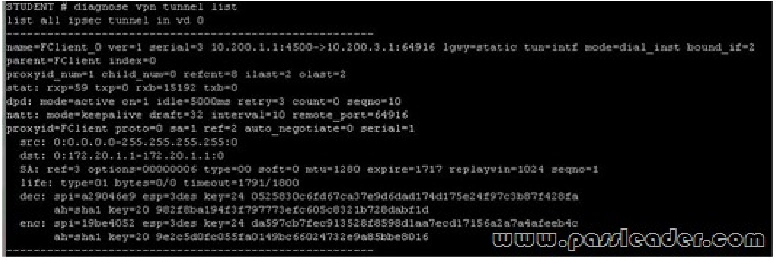


```
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

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 # _
```

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 QUESTION 131 In HA, what is the effect of the Disconnect Cluster Member command as given in the Exhibit.

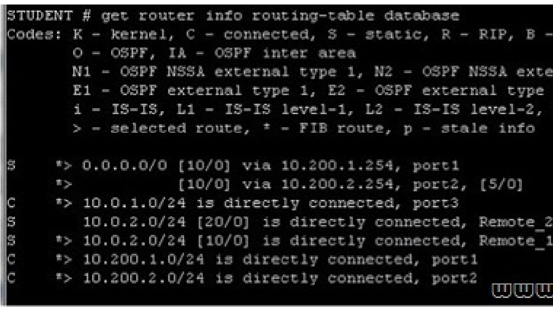


A. The HA mode changes to standalone. B. Port3 is configured with an IP address for management access. C. The Firewall rules are purged on the disconnected unit. D. All other interface IP settings are maintained. Answer: AB QUESTION 132 Which of the following statements are correct about the HA diag command diagnose sys ha reset-uptime? (Select all that apply.) A. The device this command is executed on is likely to switch from master to slave status if master override is disabled. B. The device this command is executed on is likely to switch from master to slave status if master override is enabled. C. This command has no impact on the HA algorithm. D. This command resets the uptime variable used in the HA algorithm so it may cause a new master to become elected. Answer: AD QUESTION 133 Review the IPsec diagnostics output of the command diag vpn tunnel list shown in the Exhibit below.



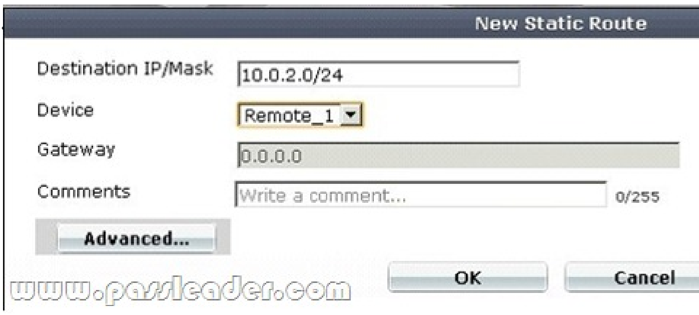
```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=FClient_0 ver=1 serial=3 10.200.1.1:4500->10.200.3.1:64916 lgwy=static tun=intf mode=dial_inst bound_if=2
parent=FClient index=0
proxyid_num=1 child_num=0 refcnt=8 ilast=2 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 of the following statements are correct regarding this output? (Select all that apply.) 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 QUESTION 134 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 -
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA exte
       E1 - OSPF external type 1, E2 - OSPF external type
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       > - 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 of the following statements are correct regarding this output? (Select all that apply). 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 QUESTION 135 Review the static route configuration for IPsec shown in the Exhibit below; then answer the question following it.



New Static Route

Destination IP/Mask: 10.0.2.0/24

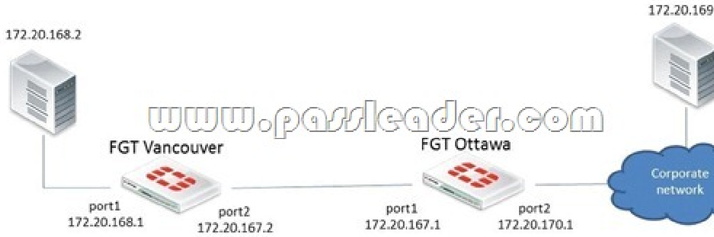
Device: Remote_1

Gateway: 0.0.0.0

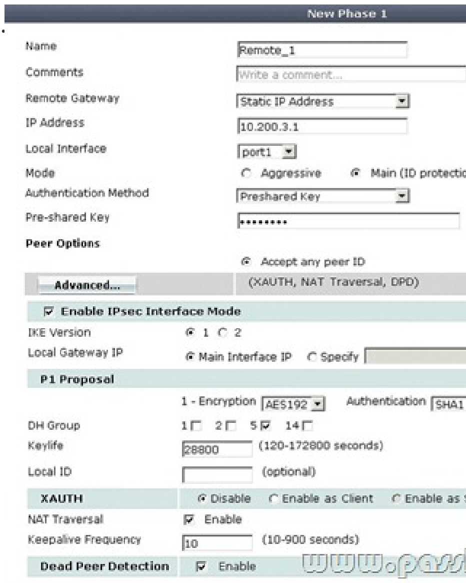
Comments: Write a comment... 0/255

Which of the following statements are correct regarding this configuration? (Select all that apply). A. Remote_1 is a Phase 1 object with interface mode enabled B. The gateway address is not required because the interface is a point-to-point connection C.

The gateway address is not required because the default route is usedD. Remote_1 is a firewall zone Answer: AB QUESTION 136 Examine the Exhibit shown below; then answer the question following it.

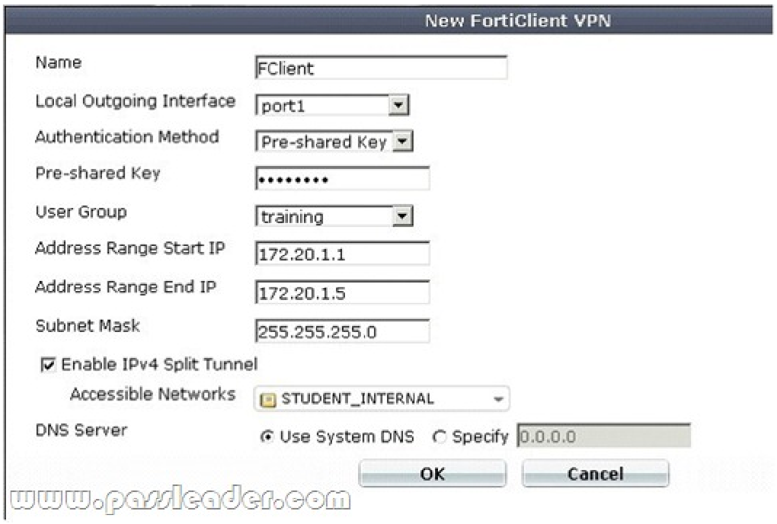


In this scenario, the Fortigate unit in Ottawa has the following routing table:S* 0.0.0.0/0 [10/0] via 172.20.170.254, port2C 172.20.167.0/24 is directly connected, port1C 172.20.170.0/24 is directly connected, port2Sniffer tests show that packets sent from the Source IP address 172.20.168.2 to the Destination IP address 172.20.169.2 are being dropped by the FortiGate unit located in Ottawa. Which of the following correctly describes the cause for the dropped packets? A. The forward policy check.B. The reverse path forwarding check.C. The subnet 172.20.169.0/24 is NOT in the Ottawa FortiGate unit's routing table.D. The destination workstation 172.20.169.2 does NOT have the subnet 172.20.168.0/24 in its routing table. Answer: B QUESTION 137 Examine the following log message for IPS and identify the valid responses below. (Select all that apply.)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" A. The target is 192.168.3.168.B. The target is 192.168.3.170.C. The attack was detected and blocked.D. The attack was detected only.E. The attack was TCP based. Answer: BD QUESTION 138Review the IPsec phase1 configuration in the Exhibit shown below; then answer the question following it.


New Phase 1

Name: Remote_1
Comments: Write a comment...
Remote Gateway: Static IP Address
IP Address: 10.200.3.1
Local Interface: port1
Mode: ○ Aggressive ● Main (ID protectio
Authentication Method: Preshared Key
Pre-shared Key: ••••••••
Peer Options
● Accept any peer ID
Advanced... (XAUTH, NAT Traversal, DPD)
☑ **Enable IPsec Interface Mode**
IKE Version: ● 1 ○ 2
Local Gateway IP: ● Main Interface IP ○ Specify
P1 Proposal
1 - Encryption: AES192 Authentication: SHA1
DH Group: 1 ☐ 2 ☐ 5 ☑ 14 ☐
Keylife: 28800 (120-172800 seconds)
Local ID: (optional)
XAUTH: ● Disable ○ Enable as Client ○ Enable as
NAT Traversal: ☑ Enable
Keepalive Frequency: 10 (10-900 seconds)
Dead Peer Detection: ☑ Enable

Which of the following statements are correct regarding this configuration? (Select all that apply). A. The phase1 is for a route-based VPN configuration.B. The phase1 is for a policy-based VPN configuration.C. The local gateway IP is the address assigned to port1.D. The local gateway IP address is 10.200.3.1. Answer: AC QUESTION 139Review the configuration for FortiClient IPsec shown in the Exhibit below.



New FortiClient VPN

Name: FClient
Local Outgoing Interface: port1
Authentication Method: Pre-shared Key
Pre-shared Key: ••••••••
User Group: training
Address Range Start IP: 172.20.1.1
Address Range End IP: 172.20.1.5
Subnet Mask: 255.255.255.0
☑ Enable IPv4 Split Tunnel
Accessible Networks: STUDENT_INTERNAL
DNS Server: ● Use System DNS ○ Specify 0.0.0.0

Which of the following statements is correct regarding this configuration? A. The connecting VPN client will install a route to a destination corresponding to the STUDENT_INTERNAL address objectB. The connecting VPN client will install a default route C. The connecting VPN client will install a route to the 172.20.1.[1-5] address rangeD. The connecting VPN client will connect in web portal mode and no route will be installed Answer: A QUESTION 140Identify the statement which correctly describes the output of the following 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. Answer: B Download Free NSE5 PDF Dumps From Google Drive: https://drive.google.com/open?id=0B-ob6L_QjGLpU0FrbTh1X3JMSmM Download New NSE5 VCE Dumps From PassLeader: http://www.passleader.com/nse5.html (New Questions Are 100% Available and Wrong Answers Have Been Corrected!!!)