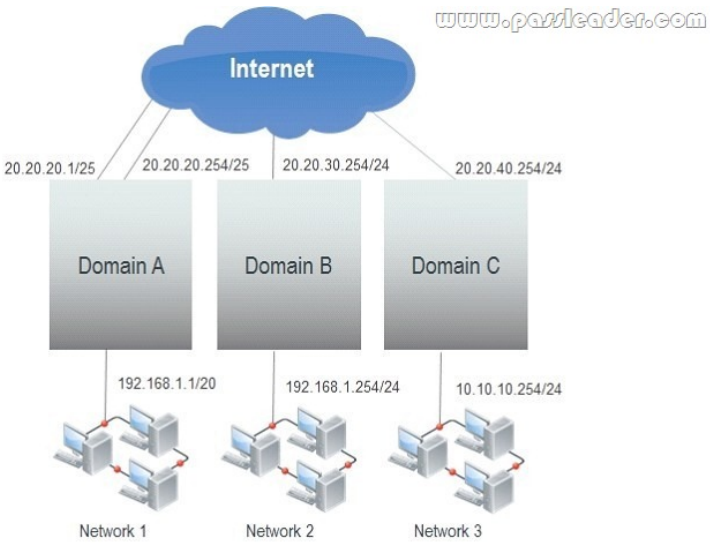
100% Valid Fortinet NSE4 Dumps with VCE and PDF shared by PassLeader (Question 26 - Question 50)

PassLeader just published the NEWEST Fortinet NSE4 exam dumps! And, PassLeader offer two types of the NSE4 dumps -- NSE4 VCE dumps and NSE4 PDF dumps, both VCE and PDF contain the NEWEST NSE4 exam questions, they will help you PASSING the Fortinet NSE4 exam easily! Now, get the NEWEST NSE4 dumps in VCE and PDF from PassLeader -- http://www.passleader.com/nse4.html (562 Q&As Dumps)
What's more, part of that PassLeader NSE4 dumps now are free -- https://drive.google.com/open?id=0B-ob6L_QjGLpWVVnQl8wTTd0NW8
QUESTION 26
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
QUESTION 27
Which statements are correct regarding virtual domains (VDOMs)? (Choose two.)
A. VDOMs divide a single FortiGate unit into two or more virtual units that each have dedicated memory and CPUs.
B. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.
C. VDOMs share firmware versions, as well as antivirus and IPS databases.
D. Different time zones can be configured in each VDOM.
Answer: BC
QUESTION 28
A FortiGate is configured with multiple VDOMs. An administrative account on the device has been assigned a Scope value of VDOM:root. Which of the following settings will this administrator be able to configure? (Choose two.)
A. Firewall addresses.
B. DHCP servers.
C. FortiGuard Distribution Network configuration.
D. System hostname.
Answer: AB
QUESTION 29
A FortiGate administrator with the super_admin profile configures a virtual domain (VDOM) for a new customer. After creating the VDOM, the administrator is unable to reassign the dmz interface to the new VDOM as the option is greyed out in the GUI in the management VDOM. What would be a possible cause for this problem?
A. The administrator does not have the proper permissions to reassign the dmz interface.
B. The dmz interface is referenced in the configuration of another VDOM.
C. Non-management VDOMs cannot reference physical interfaces.
D. The dmz interface is in PPPoE or DHCP mode.
Answer: B
QUESTION 30
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

QUESTION 31

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

QUESTION 32

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

QUESTION 33

In transparent mode, forward-domain is an CLI setting associate with ____.

A. a static route.

B. a firewall policy.

C. an interface.

D. a virtual domain.

Answer: C

QUESTION 34

Which statements correctly describe transparent mode operation? (Choose three.)

A. The FortiGate acts as transparent bridge and forwards traffic at Layer-2.

B. Ethernet packets are forwarded based on destination MAC addresses, NOT IP addresses.

C. The transparent FortiGate is clearly visible to network hosts in an IP trace route.

D. Permits inline traffic inspection and firewalling without changing the IP scheme of the network.

E. All interfaces of the transparent mode FortiGate device must be on different IP subnets.

Answer: ABD

QUESTION 35

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

QUESTION 36

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 is executed on is likely to switch from master to slave status if 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 37

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.

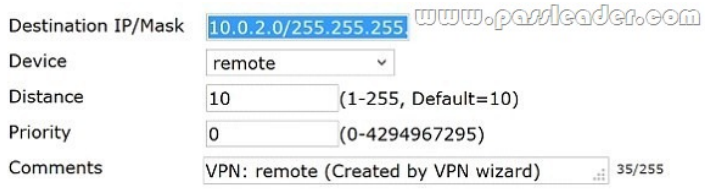
C. Connections must be UDP or ICMP.

D. Connections must not be handled by a proxy.

Answer: AD

QUESTION 38

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.

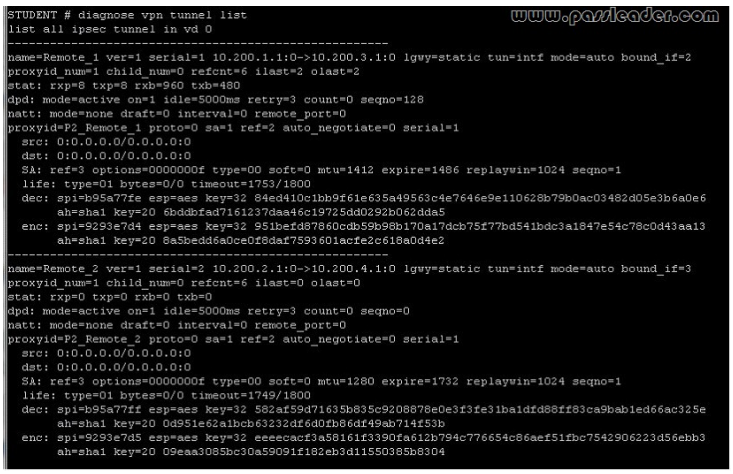
C. A gateway address is not required because the default route is used.

D. Interface remote is a zone.

Answer: AB

QUESTION 39

Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit.



Which of the following statements is correct regarding this output? (Select one answer).

A. One tunnel is rekeying.

B. Two tunnels are rekeying.

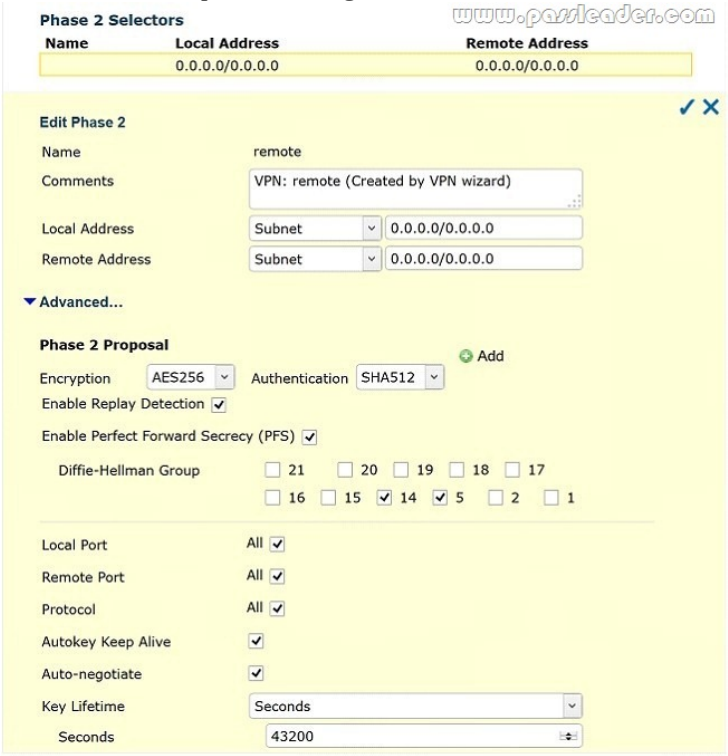
C. Two tunnels are up.

D. One tunnel is up.

Answer: C

QUESTION 40

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

QUESTION 41

Which statement is an 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

QUESTION 42

Review the IKE debug output for IPsec shown in the exhibit below.

Which statements is correct regarding this output?

A. The output is a phase 1 negotiation.

B. The output is a phase 2 negotiation.

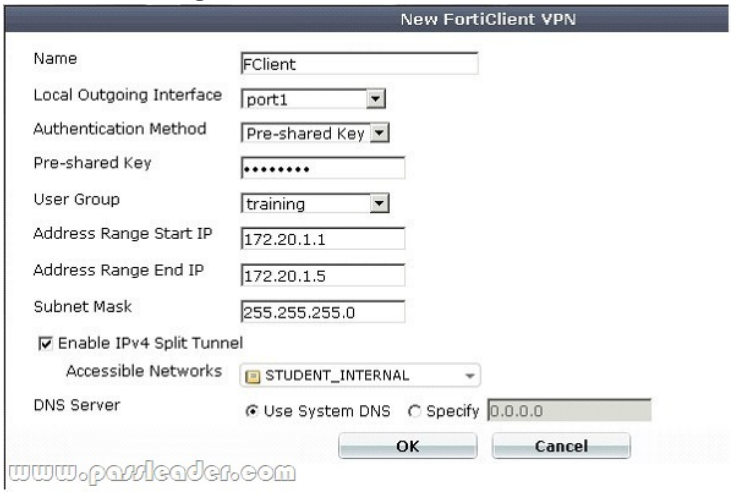
C. The output captures the dead peer detection messages.

D. The output captures the dead gateway detection packets.

Answer: C

QUESTION 43

Review the configuration for FortiClient IPsec shown in the exhibit.



Which statement is correct regarding this configuration?

A. The connecting VPN client will install a route to a destination corresponding to the student_internal address object.

B. The connecting VPN client will install a default route.

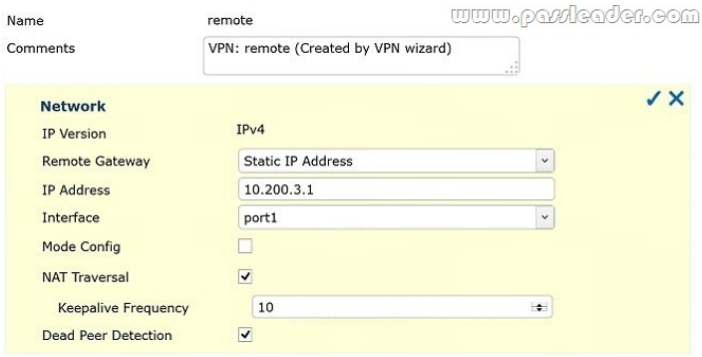
C. The connecting VPN client will install a route to the 172.20.1.[1-5] address range.

D. The connecting VPN client will connect in web portal mode and no route will be installed.

Answer: A

QUESTION 44

Review the IPsec phase 1 configuration in the exhibit; then answer the question below.



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

A. The remote gateway address on 10.200.3.1.

B. The local IPsec interface address is 10.200.3.1.

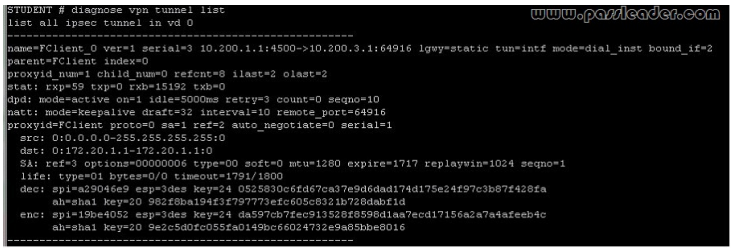
C. The local gateway IP is the address assigned to port1.

D. The local gateway IP address is 10.200.3.1.

Answer: AC

QUESTION 45

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



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

QUESTION 46

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

QUESTION 47

Which statements are correct properties of a partial mesh VPN deployment. (Choose two.)

A. VPN tunnels interconnect between every single location.

B. VPN tunnels are not configured between every single location.

C. Some locations are reached via a hub location.

D. There are no hub locations in a partial mesh.

Answer: BC

QUESTION 48

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 49

Identify 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.
D. Lists the IPS signature matches.

Answer: B

QUESTION 50

Review the IPS sensor filter configuration shown in the exhibit.

Based on the information in the exhibit, which statements are correct regarding the filter? (Choose two.)

A. It does not log attacks targeting Linux servers.
B. It matches all traffic to Linux servers.
C. Its action will block traffic matching these signatures.
D. It only takes effect when the sensor is applied to a policy.

Answer: CD