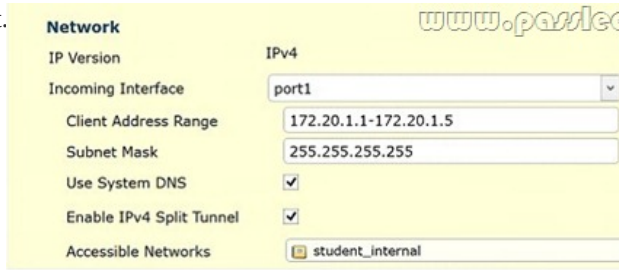
[Mar-2016 Update Reliable 222q NSE4 Exam Dumps From PassLeader For Free Download (41-60)

Free Download New NSE4 Exam Dumps: PassLeader now supplying the new version of NSE4 VCE dumps, we ensure our 222q NSE4 exam questions are the most authoritative and valid compared with others', which will ensure your NSE4 exam 100% passing, and now we are offering the free new version VCE Player along with the VCE format 222q NSE4 braindumps, also the PDF format NSE4 practice test is available now, welcome to choose. keywords: NSE4 exam,222q NSE4 exam dumps,222q NSE4 exam questions,NSE4 pdf dumps,NSE4 vce dumps,NSE4 practice test,NSE4 study guide,NSE 4 -- Fortinet Network Security Professional Exam

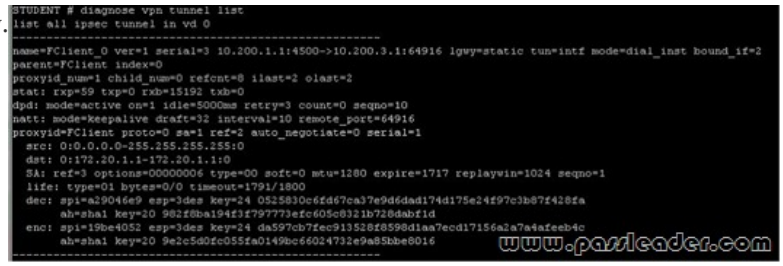
QUESTION 41Which statement is an advantage of using a hub and spoke IPsec VPN configuration instead of a fully-meshed set of IPsec tunnels? A. Using a hub and spoke topology provides full redundancy.B. Using a hub and spoke topology requires fewer tunnels.C. Using a hub and spoke topology uses stronger encryption protocols.D. Using a hub and spoke topology requires more routes. Answer: B QUESTION 42Review 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 43Review 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 44Review 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 45Review 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 46Which 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 47Which 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 48Examine 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: BC QUESTION 49Which 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 QUESTION 50Review the IPS sensor filter configuration shown in the exhibit: **Pattern Based Signatures and Filters**

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

http://www.passleader.com/nse4.html QUESTION 51With FSSO, 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 the 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 QUESTION 52FSSO 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 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 QUESTION 53Which statement is one disadvantage of using FSSO NetAPI polling mode over FSSO Security Event Log (WinSecLog) polling mode? A. It requires a DC agent installed in some of the Windows DC.B. It runs slower.C. It might miss some logon events.D. It requires access to a DNS server for workstation name resolution. Answer: C QUESTION 54Which are two requirements for DC-agent mode FSSO to work properly in a Windows AD environment? [Choose two.] A. DNS server must properly resolve all workstation names.B. The remote registry service must be running in all workstations.C. The collector agent must be installed in one of the Windows domain controllers.D. A same user cannot be logged in into two different workstations at the same time. Answer: AB QUESTION 55Which 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 a listing of all connected FSSO collector agents.D. Lists all DC Agents installed on all domain controllers. Answer: B QUESTION 56When the SSL proxy is NOT doing man-in-the-middle interception of SSL traffic, which certificate field can be used to determine the rating of a website? A. Organizational Unit.B. Common Name. C. Serial Number.D. Validity. Answer: B QUESTION 57Which tasks fall under the responsibility of the SSL proxy in a typical HTTPS connection? (Choose two.) A. The web client SSL handshake.B. The web server SSL handshake.C. File buffering.D. Communication with the URL filter process. Answer: AB QUESTION 58Bob 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 QUESTION 59Which Fortinet products & features could be considered part of a comprehensive solution to monitor and prevent the leakage of senstive data? (Select all that apply.) A. Archive non-compliant outgoing e-mails using FortiMail.B. Restrict unofficial methods of transferring files such as P2P using Application Control lists on a FortiGate.C. Monitor database activity using FortiAnalyzer.D. Apply a DLP sensor to a firewall policy.E. Configure FortiClient to prevent files flagged as sensitive from being copied to a USB disk. Answer: ABD QUESTION 60For data leak prevention, which statement describes the difference between the block and quarantine actions? A. A block action prevents the transaction. A quarantine action blocks all future transactions, regardless of the protocol.B. A block action prevents the transaction. A quarantine action archives the data.C. A block action has a finite duration. A quarantine action must be removed by an administrator.D. A block action is used for known users. A quarantine action is used for unknown users. Answer: A

http://www.passleader.com/nse4.html