

[2016-NEW! Free PassLeader NSE5 VCE and PDF Dumps With New Update Exam Questions (Question 141 & Question 160)]

PassLeader helps you to get well prepared for the NSE5 exam! Try PassLeader's new 240q NSE5 exam dumps with VCE test software or PDF braindumps now and you will get your NSE5 certification quickly. PassLeader's 240q NSE5 exam questions with all new NSE5 exam questions is the best study materials for preparing exam, we ensure that our full version NSE5 VCE dumps and PDF dumps will help you 100 percent passing NSE5 exam. First try the PassLeader valid NSE5 braindumps and first pass exam! 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 141 Which of the following statements correctly describe Transparent Mode operation? (Select all that apply.)

- A. The FortiGate unit acts as transparent bridge and routes traffic using Layer-2 forwarding.
- B. Ethernet packets are forwarded based on destination MAC addresses NOT IPs.
- C. The device is transparent to network hosts.
- D. Permits inline traffic inspection and firewalling without changing the IP scheme of the network.
- E. All interfaces must be on different IP subnets.

Answer: ABCD

QUESTION 142 How can DLP file filters be configured to detect Office 2010 files? (Select all that apply.)

- A. File TypeE. Microsoft Office(msoffice)
- B. File TypeE. Archive(zip)
- C. File TypeE. Unknown Filetype(unknown)
- D. File NameE. "*.ppt", "*.doc", "*.xls"
- E. File NameE. "*.pptx", "*.docx", "*.xlsx"

Answer: BE

QUESTION 143 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 unit will evenly share the traffic to 172.20.168.0/24 through both routes.
- B. The FortiGate unit will share 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 unit will send 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

QUESTION 144 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? (Select all that apply.)

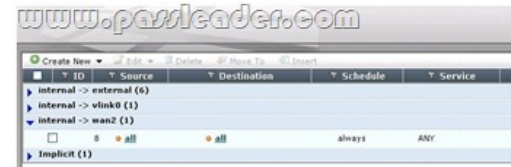
- A. The administrator should configure inter-VDOM links to avoid using external interfaces and routers.
- B. As with all FortiGate unit interfaces, firewall policies must be in place for traffic to be allowed to pass through any interface, including inter-VDOM links. This provides the same level of security internally as externally.
- C. This configuration requires the use of an external router.
- 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 145 A FortiGate administrator 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 Web Config in the management VDOM. What would be a possible cause for this problem?

- A. The dmz interface is referenced in the configuration of another VDOM.
- B. The administrator does not have

the proper permissions to reassign the dmz interface. C. Non-management VDOMs can not reference physical interfaces. D. The dmz interface is in PPPoE or DHCP mode. E. Reassigning an interface to a different VDOM can only be done through the CLI. Answer: A QUESTION 146 Which of the following statements is correct based on the firewall configuration illustrated in the exhibit?



A. A user can access the Internet using only the protocols that are supported by user authentication. B. A user can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP. These require authentication before the user will be allowed access. C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access any services. D. A user cannot access the Internet using any protocols unless the user has passed firewall authentication. Answer: D QUESTION 147 Which of the following features could be used by an administrator to block FTP uploads while still allowing FTP downloads? A. Anti-Virus File-Type Blocking B. Data Leak Prevention C. Network Admission Control D. FortiClient Check Answer: B QUESTION 148 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. E. Bob will use Alice's public key to encrypt the file and Alice will use Bob's public key to decrypt the file. Answer: C QUESTION 149 An administrator has formed a High Availability cluster involving two FortiGate 310B units. [Multiple upstream Layer 2 switches] -- [FortiGate HA Cluster] -- [Multiple downstream Layer 2 switches] The administrator wishes to ensure that a single link failure will have minimal impact upon the overall throughput of traffic through this cluster. Which of the following options describes the best step the administrator can take? The administrator should _____. A. set up a full-mesh design which uses redundant interfaces. B. increase the number of FortiGate units in the cluster and configure HA in Active-Active mode. C. enable monitoring of all active interfaces. D. configure the HA ping server feature to allow for HA failover in the event that a path is disrupted. Answer: A QUESTION 150 Which of the following statements best describes the proxy behavior on a FortiGate unit during an FTP client upload when FTP splice is disabled? A. The proxy buffers the entire file from the client, only sending the file to the server if the file is clean. One possible consequence of buffering is that the server could time out. B. The proxy sends the file to the server while simultaneously buffering it. C. The proxy removes the infected file from the server by sending a delete command on behalf of the client. D. If the file being scanned is determined to be clean, the proxy terminates the connection and leaves the file on the server. Answer: A QUESTION 151 Which of the following DLP actions will always be performed if it is selected? A. Archive B. Quarantine Interface C. Ban Sender D. Block E. None F. Ban G. Quarantine IP Address Answer: A QUESTION 152 The following ban list entry is displayed through the CLI. get user ban list id cause src-ip-addr dst-ip-addr expires created 531 protect_client 10.177.0.21 207.1.17.1 indefinite Wed Dec 24 :21:33 2008 Based on this command output, which of the following statements is correct? A. The administrator has specified the Attack and Victim Address method for the quarantine. B. This diagnostic entry results from the administrator running the diag ips log test command. This command has no effect on traffic. C. A DLP rule has been matched. D. An attack has been repeated more than once during the holddown period; the expiry time has been reset to indefinite. Answer: A QUESTION 153 The Host Check feature can be enabled on the FortiGate unit for SSL VPN connections. When this feature is enabled, the FortiGate unit probes the remote host computer to verify that it is "safe" before access is granted. Which of the following items is NOT an option as part of the Host Check feature? A. FortiClient Antivirus software B. Microsoft Windows Firewall software C. FortiClient Firewall software D. Third-party Antivirus software Answer: B QUESTION 154 An administrator configures a VPN and

selects the Enable IPSec Interface Mode option in the phase 1 settings. Which of the following statements are correct regarding the IPSec VPN configuration? A. To complete the VPN configuration, the administrator must manually create a virtual IPSec interface in Web Config under System > Network. B. The virtual IPSec interface is automatically created after the phase1 configuration. C. The IPSec policies must be placed at the top of the list. D. This VPN cannot be used as part of a hub and spoke topology. E. Routes were automatically created based on the address objects in the firewall policies. Answer: B

QUESTION 155 A FortiClient fails to establish a VPN tunnel with a FortiGate unit. The following information is displayed in the FortiGate unit logs: msg="Initiator: sent 192.168.11.101 main mode message #1 (OK)" msg="Initiator: sent 192.168.11.101 main mode message #2 (OK)" msg="Initiator: sent 192.168.11.101 main mode message #3 (OK)" msg="Initiator: parsed 192.168.11.101 main mode message #3 (DONE)" msg="Initiator: sent 192.168.11.101 quick mode message #1 (OK)" msg="Initiator: tunnel 192.168.1.1/192.168.11.101 install ipsec sa" msg="Initiator: sent 192.168.11.101 quick mode message #2 (DONE)" msg="Initiator: tunnel 192.168.11.101, transform=ESP_3DES, HMAC_MD5" msg="Failed to acquire an IP address Which of the following statements is a possible cause for the failure to establish the VPN tunnel? A. An IPSec DHCP server is not enabled on the external interface of the FortiGate unit. B. There is no IPSec firewall policy configured for the policy-based VPN. C. There is a mismatch between the FortiGate unit and the FortiClient IP addresses in the phase 2 settings. D. The phase 1 configuration on the FortiGate unit uses Aggressive mode while FortiClient uses Main mode. Answer: A

QUESTION 156 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 is NOT required for this static default route to be displayed in the FortiGate unit's routing table? A. The Administrative Status of the wan1 interface is displayed as Up. B. The Link Status of the wan1 interface is displayed as Up. C. All other default routes should have an equal or higher distance. D. You must disable DHCP client on that interface. Answer: D

QUESTION 157 Which of the following methods does the FortiGate unit use to determine the availability of a web cache using Web Cache Communication Protocol (WCCP)? A. The FortiGate unit receives periodic "Here I am" messages from the web cache. B. The FortiGate unit polls all globally-defined web cache servers at a regular intervals. C. The FortiGate using uses the health check monitor to verify the availability of a web cache server. D. The web cache sends an "I see you" message which is captured by the FortiGate unit. Answer: C

QUESTION 158 Which of the following statements correctly describes the deepscan option for HTTPS? A. When deepscan is disabled, only the web server certificate is inspected; no decryption of content occurs. B. Enabling deepscan will perform further checks on the server certificate. C. Deepscan is only applicable to mail protocols, where all IP addresses in the header are checked. D. With deepscan enabled, archived files will be decompressed before scanning for a more comprehensive file inspection. Answer: A

QUESTION 159 When performing a log search on a FortiAnalyzer, it is generally recommended to use the Quick Search option. What is a valid reason for using the Full Search option, instead? A. The search items you are looking for are not contained in indexed log fields. B. A quick search only searches data received within the last 24 hours. C. You want the search to include the FortiAnalyzer's local logs. D. You want the search to include content archive data as well. Answer: A

QUESTION 160 Which spam filter is not available on a FortiGate device? A. Sender IP reputation database B. URLs included in the body of known SPAM messages C. Email addresses included in the body of known SPAM messages D. Spam object checksums E. Spam grey listing Answer: E

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!!!)