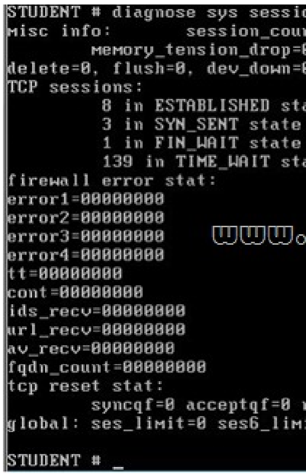
[2016-NEW! Free 240q NSE5 Exam Questions From PassLeader For Free Download (Question 101 – Question 120)

Passed NSE5 exam with the best PassLeader NSE5 exam dumps now! PassLeader are supplying the latest 240q NSE5 vce and pdf exam dumps covering all the new questions and answers, it is 100 percent pass ensure for NSE5 exam. PassLeader offer PDF and VCE format NSE5 exam dumps, and free version VCE player is also available. Visit passleader.com now and download the 100 percent passing guarantee 240q NSE5 braindumps to achieve your 70-331 certification exam easily! 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 101 Which of the following statements are correct regarding virtual domains (VDOMs)? (Select all that apply.) A.   VDOMs divide a single FortiGate unit into two or more virtual units that function as multiple, independent units. 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.   Only administrative users with a 'super_admin' profile will be able to enter multiple VDOMs to make configuration changes. Answer: ABC QUESTION 102 Two devices are in an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of 'diag sys session stat' for the STUDENT device. Exhibit B shows the command output of 'diag sys session stat' for the REMOTE device. Exhibit A:



```
STUDENT # diagnose sys sessi
misc info:       session_cou
        memory_tension_drop=
delete=0, flush=0, dev_down=
TCP sessions:
         8 in ESTABLISHED st
         3 in SYN_SENT state
         1 in FIN_WAIT state
         139 in TIME_WAIT st
firewall error stat:
error1=00000000
error2=00000000
error3=00000000     www.
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
global: ses_limit=0 ses6_lim

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     www.passleader.com
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? (Select all that apply.) A.   STUDENT is likely to be the master device. B.   Session-pickup is likely to be enabled. C.   The cluster mode is definitely Active-Passive. D.   There is not enough information to determine the cluster mode. Answer: AD QUESTION 103 Shown below is a section of output from the debug command diag ip arp list. index=2 ifname=port1 172.20.187.150 00:09:0f:69:03:7e state=00000004 use=4589 confirm=4589 update=2422 ref=1 In the output provided, which of the following best describes the IP address 172.20.187.150? A.   It is the primary IP address of the port1 interface. B.   It is one of the secondary IP addresses of the port1 interface. C.   It is the IP address of another network device located in the same LAN segment as the FortiGate unit's port1 interface. Answer: C QUESTION 104 In HA, the option Reserve Management Port for Cluster Member is selected as shown in the Exhibit below.


High Availability

Mode: Active-Passive

Device Priority: 200

☑ Reserve Management Port for Cluster Member: port7

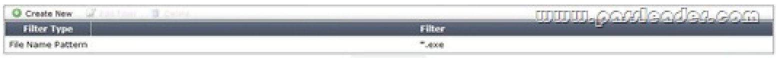
Which of the following statements are correct regarding this setting? (Select all that apply.) A.   Interface settings on port7 will not be synchronized with other cluster members. B.   The IP address assigned to this interface must not overlap with the IP address subnet assigned to another interface. C.   Port7 appears in the routing table. D.   A gateway address may be configured for port7. E.   When connecting to port7 you always connect to the master device. Answer: AD QUESTION 105 Which of the following represents the correct order of criteria used for the selection of a Master unit within a FortiGate High Availability (HA) cluster when master 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 106 Examine the Exhibits shown below, then answer the question that follows. Review the following DLP Sensor (Exhibit 1):

Seq #	Type	Action	Services	Archive
1	File Type	Log Only	SMTP, POP3, IMAP, HTTP, NNTP	Disable
2	File Type	Quarantine Interface	SMTP, POP3, IMAP, HTTP, NNTP	Disable
3	File Type	Block	SMTP, POP3, IMAP, HTTP, NNTP	Disable

Review the following File Filter list for rule #1 (Exhibit 2):

Filter Type	Filter
File Type	Audio (mp3)
File Type	Audio (wma)
File Type	Audio (wav)

Review the following File Filter list for rule #2 (Exhibit 3):



Filter Type	Filter
File Name Pattern	*.exe

Review the following

F

l

e

F

l

t

e

r

l

S

t

f

o

r

r

u

e

E

x

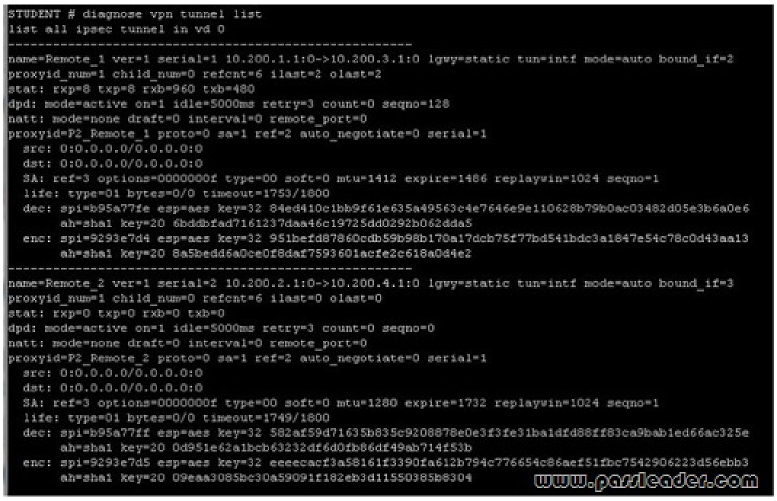
h

b

t

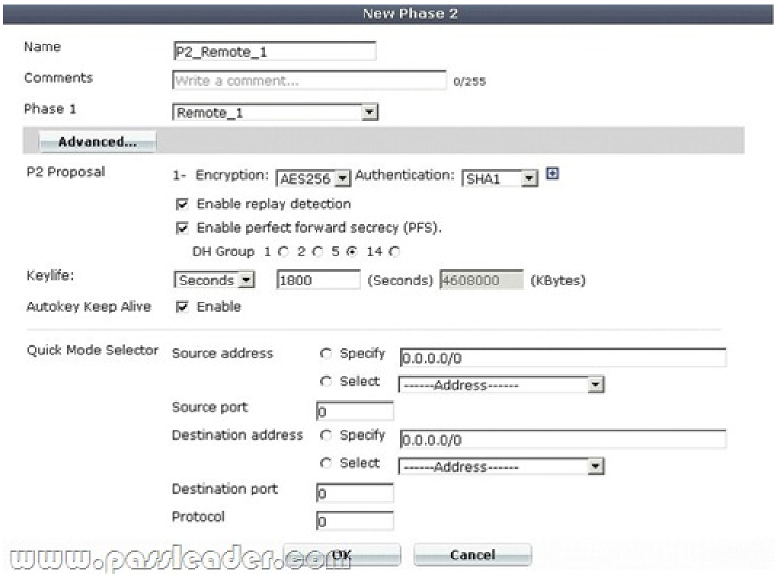
Filter Type	Filter
File Type	Archive (arj)
File Type	Archive (bzip)
File Type	Archive (cab)
File Type	Archive (zip)

An MP3 file is renamed to `workbook.exe' and put into a ZIP archive. It is then sent through the FortiGate device over HTTP. It is intercepted and processed by the configuration shown in the above Exhibits 1-4. Assuming the file is not too large for the File scanning threshold, what action will the FortiGate unit take? A.   The file will be detected by rule #1 as an `Audio (mp3)', a log entry will be created and it will be allowed to pass through.   B.   The file will be detected by rule #2 as a "*.exe", a log entry will be created and the interface that received the traffic will be brought down.   C.   The file will be detected by rule #3 as an Archive(zip), blocked, and a log entry will be created.   D.   Nothing, the file will go undetected. Answer: A QUESTION 107   Review the CLI configuration below for an IPS sensor and identify the correct statements regarding this configuration from the choices below. (Select all that apply.)   config ips sensor   edit "LINUX_SERVER"   set comment "   set replacemsg-group "   set log enable   config entries   edit 1   set action default   set application all   set location server   set log enable   set log-packet enable   set os Linux   set protocol all   set quarantine none   set severity all   set status default   next   end   next   end A.   The sensor will log all server attacks for all operating systems.   B.   The sensor will include a PCAP file with a trace of the matching packets in the log message of any matched signature.   C.   The sensor will match all traffic from the address object `LINUX_SERVER'.   D.   The sensor will reset all connections that match these signatures.   E.   The sensor only filters which IPS signatures to apply to the selected firewall policy. Answer: BE QUESTION 108   Which of the following statements are correct regarding Application Control? A.   Application Control is based on the IPS engine.   B.   Application Control is based on the AV engine.   C.   Application Control can be applied to SSL encrypted traffic.   D.   Application Control cannot be applied to SSL encrypted traffic. Answer: AC QUESTION 109   Review the IPsec diagnostics output of the command diag vpn tunnel list shown in the Exhibit.



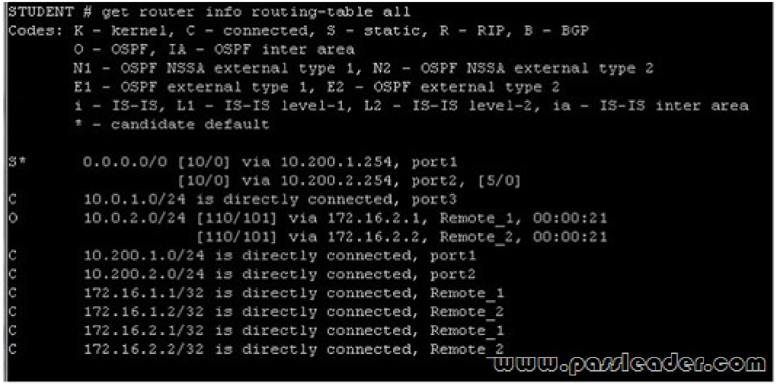
```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=Remote_1 ver=1 serial=1 10.200.1.1:0->10.200.3.1:0 lgwy=static tun=intf mode=auto bound_if=2
proxyid_num=1 child_num=0 refcnt=6 ilast=2 olast=2
stat: rxp=8 txp=8 rxb=960 txb=480
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 8a5bedd6a0ce0f8daf7593601acfe2c618a0d4e2
------------------------------------------------------
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 582af59d71635b835c9208878e0e3f3fe31ba1dfd88ff83ca9bab1ed66ac325e
       ah=sha1 key=20 0d951e62a1bcb63232df6d0fb86df49ab714f53b
  enc: spi=9293e7d5 esp=aes key=32 eeeecacf3a58161f3390fa612b794c776654c86aef51fbc7542906223d56ebb3
       ah=sha1 key=20 09eaa3085bc30a59091f182eb3d11550385b8304
```

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 110   Select the answer that describes what the CLI command diag 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 111   Review the IPsec Phase2 configuration shown in the Exhibit; then answer the question following it.



Name: P2_Remote_1
Comments: Write a comment... 0/255
Phase 1: Remote_1
P2 Proposal: 1- Encryption: AES256 Authentication: SHA1
☑ Enable replay detection
☑ Enable perfect forward secrecy (PFS).
DH Group 1 ○ 2 ○ 5 ● 14 ○
Keylife: Seconds 1800 (Seconds) 4608000 (KBytes)
Autokey Keep Alive: ☑ Enable
Quick Mode Selector
Source address ○ Specify 0.0.0.0/0
○ Select ------Address------
Source port 0
Destination address ○ Specify 0.0.0.0/0
○ Select ------Address------
Destination port 0
Protocol 0

Which of the following statements are correct regarding this configuration? (Select all that apply). 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 112 Identify the correct properties of a partial mesh VPN deployment: 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 113 In the case of TCP traffic, which of the following correctly describes the routing table lookups performed by a FortiGate unit when searching for a suitable gateway? A.   A look-up is done only when the first packet coming from the client (SYN) arrives. B.   A look-up is done when the first packet coming from the client (SYN) arrives, and a second is performed when the first packet coming from the server (SYNC/ACK) arrives. C.   A look-up is done only during the TCP 3-way handshake (SYNC, SYNC/ACK, ACK). D.   A look-up is always done each time a packet arrives, from either the server or the client side. Answer: B QUESTION 114 Review the output of the command get router info routing-table all shown in the Exhibit below; then answer the question following it.



```
STUDENT # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

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
O       10.0.2.0/24 [110/101] via 172.16.2.1, Remote_1, 00:00:21
                    [110/101] via 172.16.2.2, Remote_2, 00:00:21
C       10.200.1.0/24 is directly connected, port1
C       10.200.2.0/24 is directly connected, port2
C       172.16.1.1/32 is directly connected, Remote_1
C       172.16.1.2/32 is directly connected, Remote_2
C       172.16.2.1/32 is directly connected, Remote_1
C       172.16.2.2/32 is directly connected, Remote_2
```

Which one of the following statements correctly describes this output? A.   The two routes to the 10.0.2.0/24 subnet are ECMP routes and traffic will be load balanced based on the configured ECMP settings. B.   The route to the 10.0.2.0/24 subnet via interface Remote_1 is the active and the route via Remote_2 is the backup. C.   OSPF does not support ECMP therefore only the first route to subnet 10.0.1.0/24 is used. D.   172.16.2.1 is the preferred gateway for subnet 10.0.2.0/24. Answer: A QUESTION 115 What are the requirements for a cluster to maintain TCP connections after device or link failover? (Select all that apply.) A.   Enable session pick-up. B.   Only applies to connections handled by a proxy. C.   Only applies to UDP and ICMP connections. D.   Connections must not be handled by a proxy. Answer: AD QUESTION 116 With 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 the Secondary Domain Controller running only the Domain Controller Agent, which of the following statements are correct? (Select all that apply.) A.   The login event is sent to the Collector Agent. B.   The FortiGate unit receives the user information from the Domain Controller Agent of the Secondary Controller. C.   The Collector Agent performs the DNS lookup for the authenticated client's IP address. D.   The user cannot be authenticated with the FortiGate device in this manner because each Domain Controller Agent requires a dedicated Collector Agent. Answer: AC QUESTION 117 Which of the following statements are TRUE for Port Pairing and Forwarding Domains? (Select all that apply.) A.   They both create separate broadcast domains. B.   Port Pairing works only for physical interfaces. C.   Forwarding Domains only apply to virtual interfaces. D.   They may contain physical and/or virtual interfaces. E.   They are only available in high-end models. Answer: AD QUESTION 118 For Data Leak Prevention, which of the following 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 QUESTION 119 What advantages are there in using a hub-and-spoke IPSec VPN configuration instead of a fully-meshed set of IPSec tunnels? (Select all that apply.) A.   Using a hub and spoke topology is required to achieve full redundancy. B.   Using a hub and spoke topology simplifies configuration because fewer tunnels are required. C.   Using a hub and spoke topology provides stronger encryption. D.   The routing at a spoke is simpler, compared to a meshed node. Answer: BD QUESTION 120 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 NTLM and Polling Mode are not used? (Select all that apply.) 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 retrieve user information from the Domain Controller Agent and will send the user logon information to the FortiGate unit. E.   For non-domain computers, the only way to allow FSSO authentication is to install an FSSO client. Answer: BD 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!!!)