[Mar-2016 Update Valid 222q NSE4 Practice Test with Free PDF Study Guide Download (81-100)

100% Valid Dumps For NSE4 Exam Pass: PassLeader have been updated the 222q NSE4 exam dumps and added the new exam questions, in the latest version of NSE4 PDF dumps or VCE dumps, you will get all the new changed 222q NSE4 exam questions, which will help you 100% passing NSE4 exam, and you will get the free version of VCE Player together with your NSE4 VCE dumps. Welcome to visit our website -- passleader.com and get your NSE4 exam passed easily! 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 81   Regarding the header and body sections in raw log messages, which statement is correct? A.   The header and body section layouts change depending on the log type.   B.   The header section layout is always the same regardless of the log type. The body section layout changes depending on the log type.   C.   Some log types include multiple body sections.   D.   Some log types do not include a body section.   Answer: B QUESTION 82   In HA, the option Reserve Management Port for Cluster Member is selected as shown in the exhibit below.

Which statements are correct regarding this setting? (Choose two.) 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.   When connecting to port7 you always connect to the master device.   D.   A gateway address may be configured for port7. Answer: AD QUESTION 83 The exhibit shows the Disconnect Cluster Member command in a FortiGate unit that is part of a HA cluster with two HA members.

What is the effect of the Disconnect Cluster Member command as given in the exhibit. (Choose two.) A.   Port3 is configured with an IP address for management access.   B.   The firewall rules are purged on the disconnected unit.   C.   The HA mode changes to standalone.   D.   The system hostname is set to the unit serial number. Answer: AC QUESTION 84   Which firewall objects can be included in the Destination Address field of a firewall policy? (Choose three.) A.   IP address pool.   B.   Virtual IP address.   C.   IP address.   D.   IP address group.   E.   MAC address. Answer: BCD QUESTION 85   Which header field can be used in a firewall policy for traffic matching? A.   ICMP type and code.   B.   DSCP.   C.   TCP window size. D.   TCP sequence number. Answer: A QUESTION 86   The order of the firewall policies is important. Policies can be re-ordered from either the GUI or the CLI. Which CLI command is used to perform this function?

A.   set order   B.   edit policy   C.   reorder   D.   move Answer: D QUESTION 87   Examine the following CLI configuration: config system session-ttl   set default 1800   end   What statement is true about the effect of the above configuration line? A.   Sessions can be idle for no more than 1800 seconds.   B.   The maximum length of time a session can be open is 1800 seconds.   C.   After 1800 seconds, the end user must re-authenticate.   D.   After a session has been open for 1800 seconds, the FortiGate sends a keepalive packet to both client and server. Answer: A QUESTION 88   In which order are firewall policies processed on a FortiGate unit? A.   From top to down, according with their sequence number.   B.   From top to down, according with their policy ID number.   C.   Based on best match.   D.   Based on the priority value. Answer: A QUESTION 89   Which statements are true regarding local user authentication? (Choose two.) A.   Two-factor authentication can be enabled on a per user basis.   B.   Local users are for administration accounts only and cannot be used to authenticate network users.   C.   Administrators can create the user accounts is a remote server and store the user passwords locally in the FortiGate.   D.   Both the usernames and passwords can be stored locally on the FortiGate. Answer: AD QUESTION 90   Examine the following spanning tree configuration on a FortiGate in transparent mode: config system interface   edit <interface name>   set stp-forward enable   end   Which statement is correct for the above configuration? A.   The FortiGate participates in spanning tree.   B.   The FortiGate device forwards received spanning tree messages.   C.   Ethernet layer-2 loops are likely to occur.   D.   The FortiGate generates spanning tree BPDU frames. Answer: B

http://www.passleader.com/nse4.html QUESTION 91   Two devices are in an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of diagnose sys session stat for the STUDENT device. Exhibit B shows the command output of diagnose sys session stat for the REMOTE device.   Exhibit A:

```
STUDENT # diagnose sys session stat
Misc info:        session_count=166 setup_rate=68 exp_co
          memory_tension_drop=0 ephemeral=0/57344 removea
delete=0, flush=0, dev_down=0/0
TCP sessions:
        8 in ESTABLISHED state
        3 in SYN_SENT state
        1 in FIN_WAIT state
        139 in TIME_WAIT 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=2 data=0 ses=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

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? (Choose two.) A.   STUDENT is likely to be the master device.   B.   Session-pickup is likely to be enabled.   C.   The cluster mode is active-passive.   D.   There is not enough information to determine the cluster mode. Answer: AD QUESTION 92   An administrator has formed a high availability cluster involving two FortiGate 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.   Increase the number of FortiGate units in the cluster and configure HA in active-active mode.   B.   Enable monitoring of all active interfaces.   C.   Set up a full-mesh design which uses redundant interfaces.   D.   Configure the HA ping server feature to allow for HA failover in the event that a path is disrupted. Answer: C QUESTION 93   In 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 slave unit? A.   Request: internal host; slave FortiGate; master FortiGate; Internet; web server.   B.   Request: internal host; slave FortiGate; Internet; web server.   C.   Request: internal host; slave FortiGate; master FortiGate; Internet; web server.   D.   Request: internal host; master FortiGate; slave FortiGate; Internet; web server. Answer: D QUESTION 94   Two 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
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 #                        www.passleade
STUDENT #
STUDENT # show system ha
config system ha
    set mode a-p
    set password ENC 9FHCYwOJXK9z8w6QkUnUsREWBr
McEECpiT3Z/3dCmIuYIDgW2sE+1A1kHfADOV/r5DkaqGnbj
    set hbdev "port2" 50
    set override disable
    set priority 200
end

STUDENT # _
```

Exhibit B
```
Log hard disk: Available
Hostname: REMOTE
Operation Mode: NAT
Current virtual domain: root
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-a, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:41:46 2013

REMOTE # show system ha
config system ha
    set mode a-a
    set password ENC 9FHCYwOJXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4ds7YGvl2Cir+8
B6Mf/rGXhOu5lygP+yPgI5SDnSMEz4J1Nv4E09skIO0mBQbcgxhSE
    set hbdev "port2" 50
    set session-pickup enable
    set override disable
    set priority 100
end

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 95   Which IPsec configuration mode can be used for implementing GRE-over-IPsec VPNs?. A.   Policy-based only.   B.   Route-based only.   C.   Either policy-based or route-based VPN.   D.   GRE-based only. Answer: B QUESTION 96   You are the administrator in charge of a FortiGate acting as an IPsec VPN gateway using route-based mode. Users from either side must be able to initiate new sessions. There is only 1 subnet at either end and the FortiGate already has a default route. Which two configuration steps are required to achieve these objectives? (Choose two.) A.   Create one firewall policy.   B.   Create two firewall

policies.   C.   Add a route to the remote subnet.   D.   Add two IPsec phases 2. Answer: BC QUESTION 97   An administrator wants to create an IPsec VPN tunnel between two FortiGate devices. Which three configuration steps must be performed on both units to support this scenario? (Choose three.) A.   Create firewall policies to allow and control traffic between the source and destination IP addresses.   B.   Configure the appropriate user groups to allow users access to the tunnel.   C.   Set the operating mode to IPsec VPN mode.   D.   Define the phase 2 parameters.   E.   Define the Phase 1 parameters. Answer: ADE QUESTION 98   What is IPsec Perfect Forwarding Secrecy (PFS)?. A.   A phase-1 setting that allows the use of symmetric encryption.   B.   A phase-2 setting that allows the recalculation of a new common secret key each time the session key expires.   C.   A `key-agreement' protocol.   D.    A `security-association-agreement' protocol. Answer: B QUESTION 99   An administrator has configured a route-based site-to-site IPsec VPN. Which statement is correct regarding this IPsec VPN configuration? A.   The IPsec firewall policies must be placed at the top of the list.   B.   This VPN cannot be used as part of a hub and spoke topology.   C.   Routes are automatically created based on the quick mode selectors.   D.   A virtual IPsec interface is automatically created after the Phase 1 configuration is completed. Answer: D QUESTION 100   A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, updates are not being received. Which are two reasons for this problem? (Choose two.) A.   The FortiGate is connected to multiple ISPs.   B.   There is a NAT device between the FortiGate and the FortiGuard Distribution Network.   C.   The FortiGate is in Transparent mode.   D.   The external facing interface of the FortiGate is configured to get the IP address from a DHCP server. Answer: BD

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