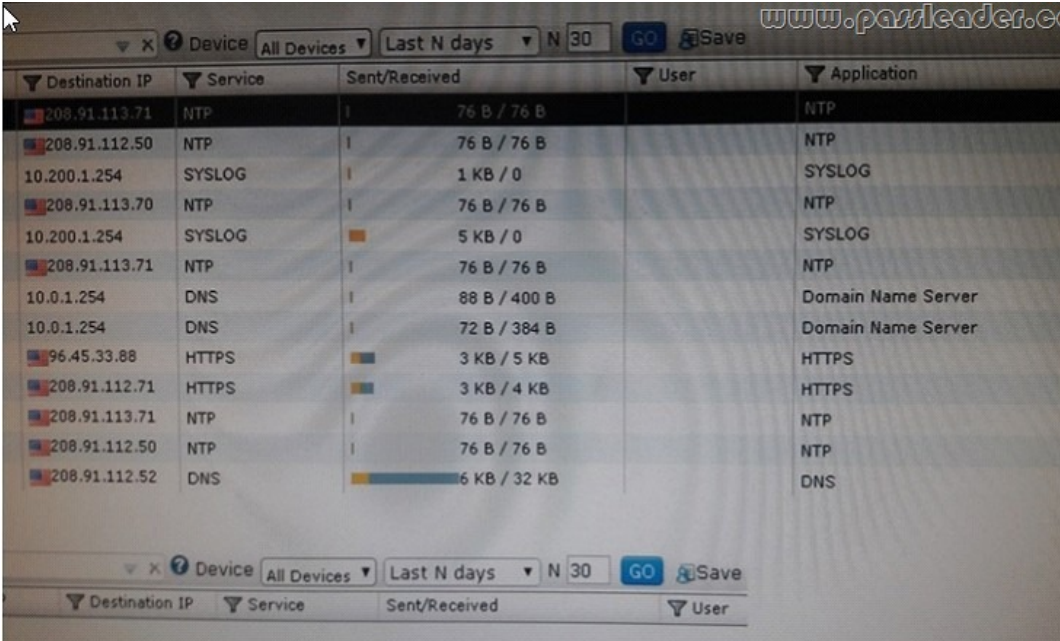


[Feb-2017 Dumps Free Share PassLeader NSE5 Exam Questions To Help You Pass Exam (Part B)

New Updated NSE5 Exam Questions from PassLeader NSE5 PDF dumps! Welcome to download the newest PassLeader NSE5 VCE dumps: <http://www.passleader.com/nse5.html> (293 Q&As) Keywords: NSE5 exam dumps, NSE5 exam questions, NSE5 VCE dumps, NSE5 PDF dumps, NSE5 practice tests, NSE5 study guide, NSE5 braindumps, NSE 5 - Fortinet Network Security Analyst Exam P.S. Free NSE5 dumps download from Google Drive:

https://drive.google.com/open?id=0B-ob6L_QjGLpU0FrbTh1X3JMSmM **NEW QUESTION 26** What is the problem with the following SQL SELECT statement? `SELECT dstip as "Destination IP", count(*) as session FROM $log-traffic GROUP BY dstip WHERE 5fileter and dstip is not null.`



Destination IP	Service	Sent/Received	User	Application
208.91.113.71	NTP	I 76 B / 76 B		NTP
208.91.112.50	NTP	I 76 B / 76 B		NTP
10.200.1.254	SYSLOG	I 1 KB / 0		SYSLOG
208.91.113.70	NTP	I 76 B / 76 B		NTP
10.200.1.254	SYSLOG	I 5 KB / 0		SYSLOG
208.91.113.71	NTP	I 76 B / 76 B		NTP
10.0.1.254	DNS	I 88 B / 400 B		Domain Name Server
10.0.1.254	DNS	I 72 B / 384 B		Domain Name Server
96.45.33.88	HTTPS	I 3 KB / 5 KB		HTTPS
208.91.112.71	HTTPS	I 3 KB / 4 KB		HTTPS
208.91.113.71	NTP	I 76 B / 76 B		NTP
208.91.112.50	NTP	I 76 B / 76 B		NTP
208.91.112.52	DNS	I 6 KB / 32 KB		DNS

A. The clauses are not coded in the right sequence. B. The clauses are not a log type. C. The FROM clause is not required. D. SQL queries are case-sensitive.

Answer: A **NEW QUESTION 27** Which two statements are true regarding disk log quota? (Choose two.)

A. The FortiAnalyzer stops logging once the disk log quota is met. B. The FortiAnalyzer automatically sets the disk log quota based on the device. C. The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met. D. The FortiAnalyzer disk log quota is configurable, but has a minimum of 100mb and a maximum based on the reserved system space.

Answer: CD **NEW QUESTION 28**

Which statement is true regarding the import/export feature? A. This is only a feature for reports.

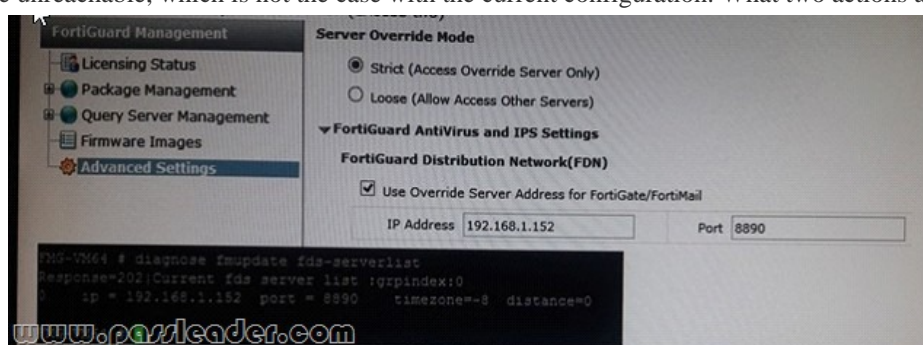
B. This feature is for reports and chart. C. This feature is for reports, charts, and datasets. D. This feature is for reports and datasets.

Answer: B **NEW QUESTION 29** Which two

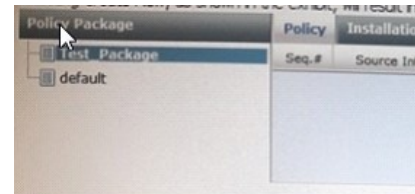
statements are true about Offline mode on the FortiManager? (Choose two.) A. Enabled by default.

B. Devices cannot be managed when Offline mode is enabled. C. Enabling Offline mode enables fgfm protocol (TCP 541). D. Offline mode is enabled by default when backup is restored on FortiManager.

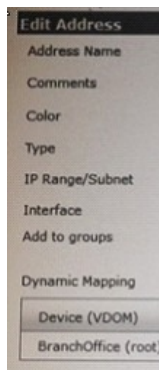
Answer: BD **NEW QUESTION 30** Given the Antivirus and IPS update service is enabled, and the FortiGuard settings as shown in the exhibit. The desired behavior is for managed devices to use public servers for these updates should FortiManager become unreachable, which is not the case with the current configuration. What two actions are necessary to correct this? (Choose two.)



A. Change the server override mode from strict to loose. B. Change the port from 8890 to 443 in the Use Override Server Address for FortiGate/FortiMail settings. C. Uncheck the option Use Override Server Address for FortiGate/FortiMail. D. Change the IP address to a public FQDN server and port to 443 in the Use Override Server Address for FortiGate/FortiMail settings. **Answer: D NEW QUESTION 31** What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three.) A. RADIUS B. Local C. LDAP D. PKI E. TACACS+ **Answer: CDE NEW QUESTION 32** Which of the following methods is best suited to changing device level settings on existing and future managed FortiGate devices? A. Configure each managed FortiGate device and install. B. Configure using provisioning templates and install. C. Configure using CLI-only objects and install. D. Configure a script for these settings and install. **Answer: A NEW QUESTION 33** Which ports are commonly used by FortiManager? (Choose two.) A. TCP 541 for remote management of a FortiGate unit. B. TCP 5199 HA heartbeat or synchronization (FortiManager HA cluster). C. TCP 703 HA heartbeat or synchronization (FortiManager HA cluster). D. TCP 514 for remote management of a FortiGate unit. **Answer: CD NEW QUESTION 34** Which two statements are correct regarding FortiAnalyzer reports? (Choose two.) A. FortiAnalyzer provides the ability to create custom reports. B. FortiAnalyzer allows you to schedule reports to run. C. FortiAnalyzer includes pre-defined reports only. D. FortiAnalyzer allows reporting for FortiGate devices only. **Answer: AB NEW QUESTION 35** What are the operating modes of FortiAnalyzer? (Choose two.) A. Standalone B. Manager C. Analyzer D. Collector **Answer: AB NEW QUESTION 36** On the Device Managers tab, what does a red circle in the Logs field of a device indicate? A. A red circle indicates logs are being received. B. A red circle indicates the IPsec tunnel is down. C. A red circle indicates logs are not being received. D. A red circle indicates no recent logs have been received. **Answer: C NEW QUESTION 37** When statement correct compares FortiManager physical and virtual appliances? A. Physical and virtual FortiManager appliances may manage unlimited devices and have unrestricted storage. B. Physical and virtual FortiManager appliances use licenses to increase managed device and storage capacity limits. C. Physical and virtual FortiManager appliances have unrestricted daily logging rate. D. Physical and virtual FortiManager appliances use model types and licenses respectively, to differentiate managed device and storage capacity limits. **Answer: C NEW QUESTION 38** Select Create New, as shown in the exhibit, will result in what?



A. A new policy package. B. A new policy folder. C. A clone of the policy package. D. A new policy in the policy package. **Answer: B NEW QUESTION 39** What are the limitations when creating a chart using the Custom Chart wizard? (Choose two.) A. You cannot search multiple log types (for example, \$log-traffic, \$log-webfilter). B. You cannot select the format of the data. All charts are table charts by default. C. You can only create custom charts within the root ADOM only. D. You can only select from two variable charts. **Answer: AB NEW QUESTION 40** A user created firewall address object, as shown in exhibit. This object is used in multiple policy package for multiple FortiGate devices. When the install operation is performed, which two statements are correct for devices referencing this object? (Choose two.)



A. The object installed on the Branch Office FortiGate device will have a value of 10.0.1.0/24.
B. The object installed on the Branch Office FortiGate device will have a value of 192.168.1.0/24.
C. If no dynamic mapping is defined, the object installed will have a value of 192.168.1.0/24.

D. If no dynamic mapping is defined, the object will not be installed. **Answer: A** **NEW QUESTION 41**

Which two tabs are available on the FortiManager Web-based manager? (Choose two.) A. Device Manager

B. Policy & Objects C. FortiGate D. Database **Answer: CD**

NEW QUESTION 42 Workflow mode introduces which new permissions for Super_Admin administrative users?

A. Self-approval, Approval, Reject B. Self-disapproval, Approval, Accept

C. Approval, Self-approval, Change Notification D. Change Notification, Self-disapproval, Submit **Answer: C** **NEW QUESTION 43**

Which two statements are correct regarding FortiGate-FortiManager (FGFM) management protocol? (Choose two.)

A. A secure communication is established between FortiManager and the managed device on port TCP 514.

B. A secure communication is established between FortiManager and the managed device on port TCP 514.

C. The FGFM daemons run on both FortiGate (fgfmd) and FortiManager (fgfmsd).

D. Once the FortiGate is managed, the FGFM tunnel is authenticated and established using the IP address of FortiGate device. **Answer: CD** **NEW QUESTION 44**

Which two statements are correct regarding FortiGuard features on FortiManager? (Choose two.)

A. FortiManager can function as a local FortiGuard Distribution Server (FDS).

B. In FortiManager HA only master FortiManager can act as an FDS server.

C. When FortiManager is configured for closed network operation, it can connect to public FDS servers to obtain managed device information and sync packages.

D. FortiGuard information is not synchronized across a FortiManager cluster. **Answer: AC** **NEW QUESTION 45**

Which two statements are correct regarding header and footer policies? (Choose two.)

A. Header and footer policies can only be created in the root ADOM.

B. Header and footer policies can only be created in the global ADOM.

C. Header and footer policies are created in policy packages and assigned to ADOM policy packages.

D. Header and footer policies can be modified in the assigned ADOM policy package. **Answer: AD** **NEW QUESTION 46**

What is 'hot swapping'?

A. Hot swapping means administrators can confine FortiAnalyzer to write to all hard device in order to make the array fault tolerant.

B. Hot swapping means administrators can replace a failed disk on devices that support software RAID while the device is still running.

C. Hot swapping means administrators can ensure the parity data of a redundant drive is valid while the device is still running.

D. Hot swapping means administrators can replace a failed disk on devices that support hardware RAID while the device is still running. **Answer: D**

NEW QUESTION 47 What is the purpose of locking an ADOM revision?

A. To prevent further changes from Device Manager.

B. To disable revision history.

C. To prevent auto deletion.

D. To lock the Policy and Objects tab. **Answer: A** **NEW QUESTION 48**

Which two statements are correct regarding synchronization between primary and secondary devices in a FortiManager HA cluster? (Choose two.)

A. All device configurations including global databases are synchronized in the HA cluster.

B. FortiGuard databases are downloaded separately by each cluster device.

C. FortiGuard databases are downloaded by the primary FortiManager device and then synchronized with all secondary devices.

D. Local logs and log configuration settings are synchronized in the HA cluster. **Answer: AB** **NEW**

QUESTION 49 Refer to the exhibits.

Refer to the exhibits. Examine the logs from the FortiView > Log View page:

Example: srcip=172.16.86.11 service=HTTP

#	Date/Time	Device ID	Action	Source IP	Destination IP	Service	Sent/Received
1	02-24 04:59	FGVM010000032664	accept	10.200.3.1	208.91.113.71	NTP	76 B / 76 B
2	02-24 04:59	FGVM010000032664	accept	10.200.3.1	208.91.112.50	NTP	76 B / 76 B
3	02-24 04:59	FGVM010000032374	accept	10.200.1.1	10.200.1.254	SYSLOG	1 KB / 0
4	02-24 04:54	FGVM010000032374	accept	10.200.1.1	208.91.113.70	NTP	76 B / 76 B
5	02-24 04:54	FGVM010000032374	accept	10.200.1.1	10.200.1.254	SYSLOG	5 KB / 0
6	02-24 04:50	FGVM010000032374	accept	10.200.1.1	208.91.113.71	NTP	76 B / 76 B
7	02-24 04:49	FGVM010000032374	accept	10.0.1.10	10.0.1.254	DNS	88 B / 400 B
8	02-24 04:49	FGVM010000032374	accept	10.0.1.10	10.0.1.254	DNS	72 B / 384 B
9	02-24 04:48	FGVM010000032374	close	10.200.1.1	96.45.33.88	HTTPS	3 KB / 5 KB
10	02-24 04:48	FGVM010000032374	close	10.200.1.1	208.91.112.71	HTTPS	3 KB / 4 KB
11	02-24 04:47	FGVM010000032664	accept	10.200.3.1	208.91.113.71	NTP	76 B / 76 B
12	02-24 04:47	FGVM010000032664	accept	10.200.3.1	208.91.112.50	NTP	76 B / 76 B
13	02-24 04:43	FGVM010000032374	accept	10.200.1.1	208.91.112.52	DNS	6 KB / 32 KB

What is one possible reason this search result yields no results?

service=https

#	Date/Time	Device ID	Action	Source IP	Destination IP	Service	Sent/Received
No records found.							

A. You cannot use SQL syntax in the Search field of the FortiView > Log View page.
B. Case Sensitive Search is enabled. C. There are no logs that include https as a service. D. You cannot search for logs from the FortiView > Log View page. **Answer: C NEW**
QUESTION 50 Which tabs do not appear when FortiAnalyzer is operating in Collector mode? A. FortiView B. Event Management C. Device Manager D. Reporting **Answer: A NEW**
QUESTION 51 ?? Download the newest PassLeader NSE5 dumps from passleader.com now! 100% Pass Guarantee! NSE5 PDF dumps & NSE5 VCE dumps: <http://www.passleader.com/nse5.html> (293 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. Free NSE5 Exam Dumps Collection On Google Drive: https://drive.google.com/open?id=0B-ob6L_QjGLpU0FrBTh1X3JMSmM