

- **Vendor: Fortinet**
- **Exam Code: NSE5_FMG-7.2**
- **Exam Name: Fortinet NSE 5 - FortiManager 7.2**
- **New Updated Questions from [Braindump2go](#) (Updated in [April/2024](#))**

[Visit Braindump2go and Download Full Version NSE5_FMG-7.2 Exam Dumps](#)

QUESTION 36

Refer to the exhibit. An administrator has created a firewall address object that is used in multiple policy packages for multiple FortiGate devices in an ADOM.8v

[NSE5_FMG-7.2 Exam Dumps](#) [NSE5_FMG-7.2 Exam Questions](#)

[NSE5_FMG-7.2 PDF Dumps](#) [NSE5_FMG-7.2 VCE Dumps](#)

<https://www.braindump2go.com/nse5-fmg-7-2.html>

Edit Firewall Address

Name	<input type="text" value="LAN"/>
Color	<input type="text" value="4"/>
Type	<input type="text" value="Subnet"/>
IP/Netmask	<input type="text" value="192.168.1.0/255.255.255.0"/>
Interface	<input checked="" type="checkbox"/> any
Static Route Configuration	<input type="checkbox"/>
Comments	<div style="border: 1px solid #ccc; height: 100px;"></div>
Add To Groups	<div style="border: 1px solid #ccc; padding: 5px;"> <input type="text" value=""/> Click to select </div>

Advanced Options >

Per-Device Mapping ▾

<input type="button" value="+ Create New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="text" value="Search..."/>		
<input type="checkbox"/>	Mapped Device	Details <input type="button" value="⚙"/>
<input type="checkbox"/>	Remote-FortiGate(root)	IP/Netmask: 10.0.5.0/255.255.255.0

After the installation operation is performed, which IP/netmask will be shown on FortiManager for this firewall address object without specify Per-Device Mapping?

- A. 0.0.0.0/0
- B. The FortiManager replaces the address object to none
- C. 192.168.1.0/24
- D. 10.0.5.0/24

Answer: C

Explanation:

Devices in the same ADOM for dynamic objects that were not specified for dynamic mapping will be assigned with an IP address from the Object's subnet.

QUESTION 37

Which two items does an FGFM keepalive message include? (Choose two.)

- A. FortiGate uptime

[NSE5_FMG-7.2 Exam Dumps](#) [NSE5_FMG-7.2 Exam Questions](#)

[NSE5_FMG-7.2 PDF Dumps](#) [NSE5_FMG-7.2 VCE Dumps](#)

<https://www.braindump2go.com/nse5-fmg-7-2.html>

- B. FortiGate license information
- C. FortiGate configuration checksum
- D. FortiGate IPS version

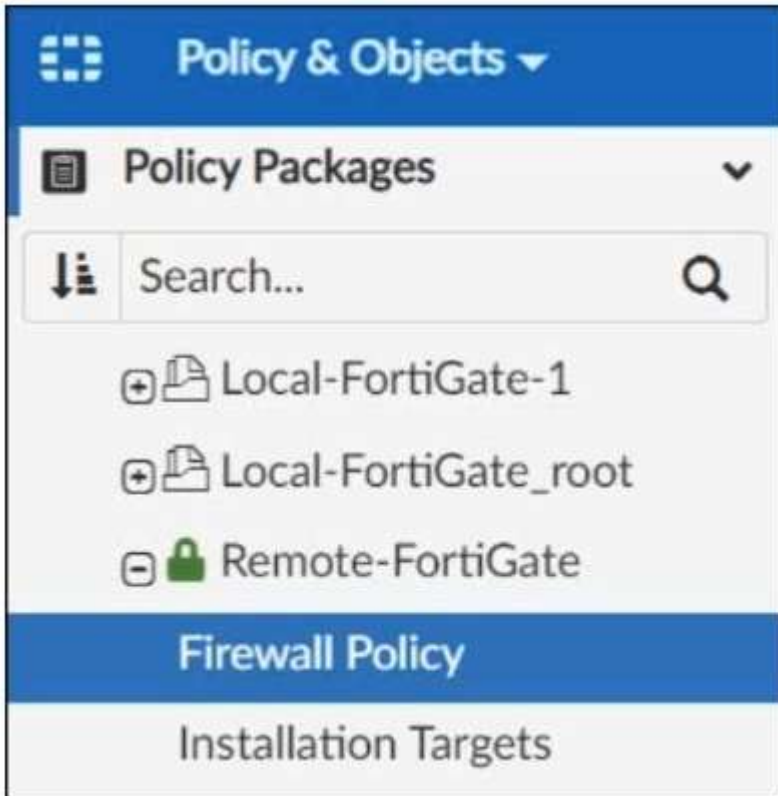
Answer: CD

Explanation:

Keepalive messages, including the configuration checksums, are sent from FortiGate at configured intervals. The messages also show the intrusion prevention system (IPS) version of the FortiGate device

QUESTION 38

Given the configuration shown in the exhibit, which two statements are true? (Choose two.)



- A. FortiManager is in workflow mode.
- B. An administrator can also lock the Local-FortiGate-1 policy package.
- C. The FortiManager ADOM workspace mode is set to Normal.
- D. The FortiManager ADOM is locked by the administrator.

Answer: BC

Explanation:

<https://docs.fortinet.com/document/fortimanager/7.2.4/administration-guide/397419/lock-an-individual-policy>

QUESTION 39

Refer to the exhibit. Which two statements about an ADOM set in Normal mode on FortiManager are true? (Choose two.)

[NSE5_FMG-7.2 Exam Dumps](#) [NSE5_FMG-7.2 Exam Questions](#)

[NSE5_FMG-7.2 PDF Dumps](#) [NSE5_FMG-7.2 VCE Dumps](#)

<https://www.braindump2go.com/nse5-fmg-7-2.html>

Create ADOM

Name:

Type: FortiGate 6.4 7.0 7.2

Description:

Devices

+ Select Device 🔍

<input type="checkbox"/>	Name	IP Address	⚙️
No record found.			

Mode: Normal Backup

Central Management: VPN FortiAP FortiSwitch

OK
Cancel

- A. It supports the FortiManager script feature.
- B. FortiManager automatically installs the configuration difference in revisions on the managed FortiGate.
- C. It allows making configuration changes for managed devices on FortiManager panes.
- D. You cannot assign the same ADOM to multiple administrators.

Answer: AC

QUESTION 40

What is the purpose of the Policy Check feature on FortiManager?

- A. It compares the policy packages with the revision history, and updates policy packages in the ADOM database.
- B. It provides recommendations for optimizing policies in a policy package.
- C. It merges and creates dynamic mappings for duplicate objects used in a policy package.
- D. It provides recommendations to combine similar policy packages within an ADOM into one single policy package.

Answer: B

Explanation:

https://training.fortinet.com/pluginfile.php/1793163/mod_resource/content/26/FortiManager_7.2_Study_Guide-Online.pdf?forcedownload=1

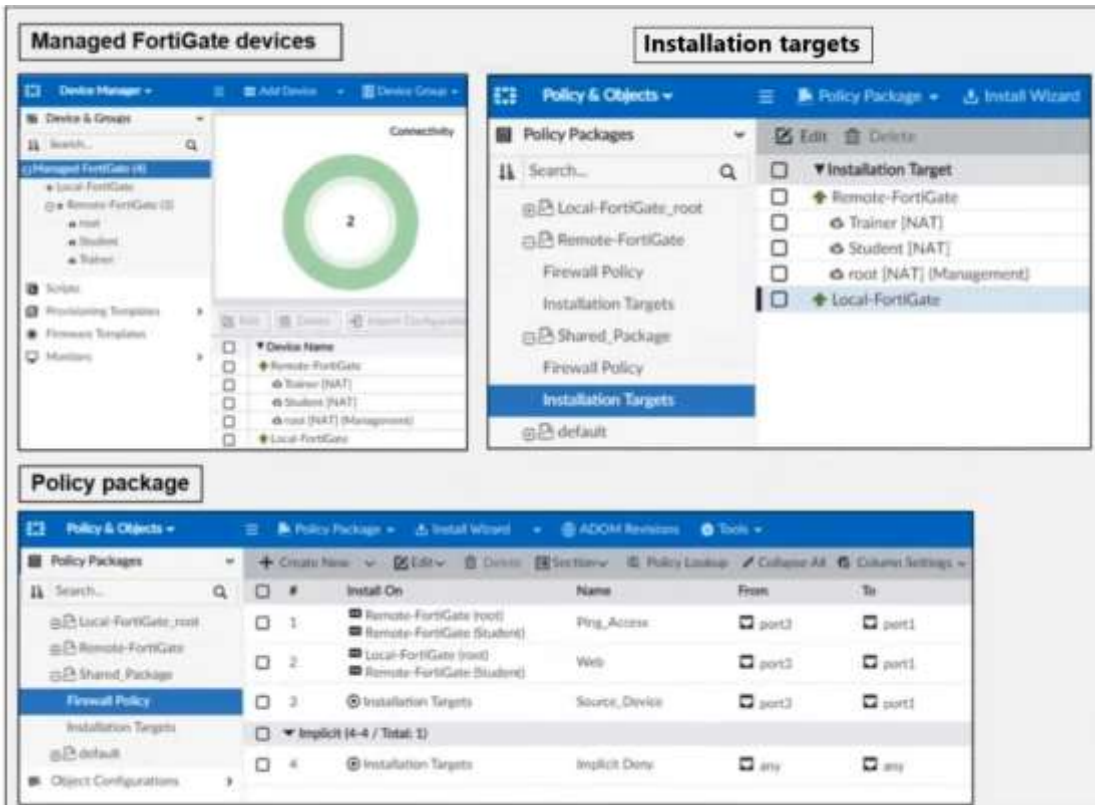
QUESTION 41

Refer to the exhibit. Given the configuration shown in the exhibit, what can you conclude from the installation targets in the Install On column? (Choose two.)

[NSE5_FMG-7.2 Exam Dumps](#) [NSE5_FMG-7.2 Exam Questions](#)

[NSE5_FMG-7.2 PDF Dumps](#) [NSE5_FMG-7.2 VCE Dumps](#)

<https://www.braindump2go.com/nse5-fmg-7-2.html>



The screenshot displays three panels from the FortiGate management console:

- Managed FortiGate devices:** Shows a connectivity chart with a green circle containing the number '2'. Below it, a list of devices is shown: Remote-FortiGate (root), Remote-FortiGate (Student), Local-FortiGate (root), and Local-FortiGate (Student).
- Installation targets:** Shows a list of installation targets under the 'Local-FortiGate' package: Remote-FortiGate, Trainer [NAT], Student [NAT], root [NAT] (Management), and Local-FortiGate.
- Policy package:** Shows a table of policy packages with columns for #, Install On, Name, From, and To.

#	Install On	Name	From	To
1	Remote-FortiGate (root) Remote-FortiGate (Student)	Ping_Access	port3	port1
2	Local-FortiGate (root) Remote-FortiGate (Student)	Web	port3	port1
3	Installation Targets	Source_Device	port3	port1
▼ Implicit (4-4 / Total: 1)				
4	Installation Targets	Implicit Deny	any	any

- A. Policy 3 will be installed on all FortiGate devices and vdom belongs to the ADOM.
- B. Policy seq.# 3 will be skipped because no installation targets are specified.
- C. Policy seq.# 3 will be installed on all managed devices and VDOMs that are listed under Installation Targets.
- D. Policy seq.# 2 will not be installed on the Local-FortiGate root VDOM because there is no root VDOM in the Installation Target.
- E. Policy seq # 1 will be installed on the Remote-FortiGate root[NAT] and Student[NAT] VDOMs only.

Answer: CE

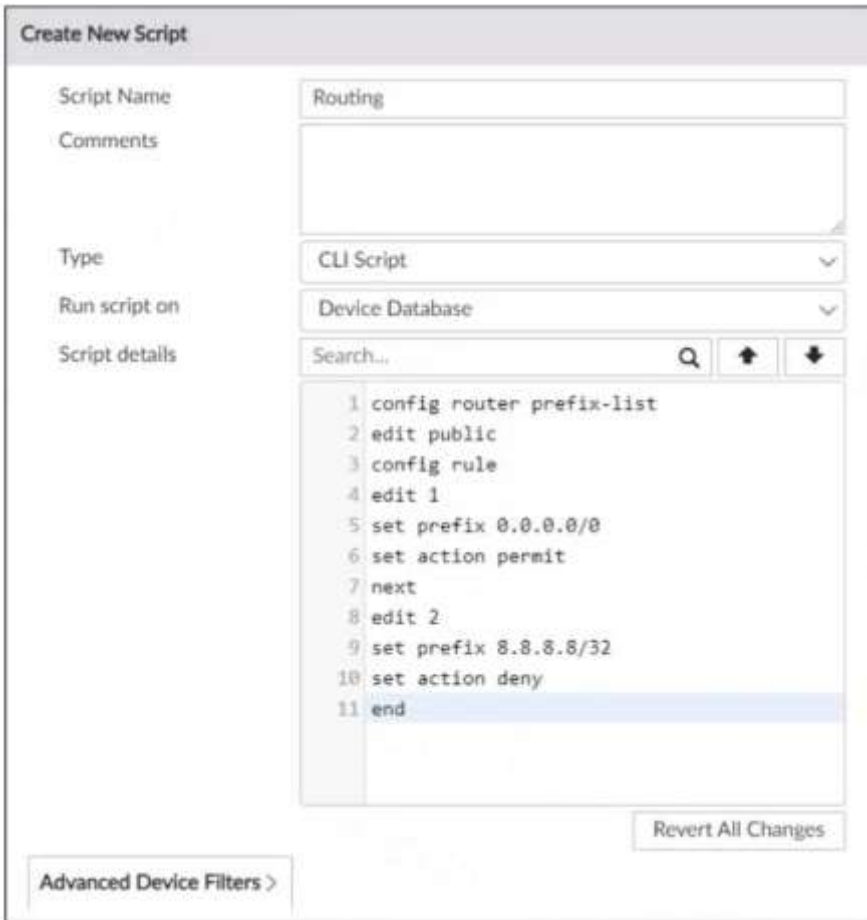
QUESTION 42

Refer to the exhibit. What will happen if the script is run using the Device Database option? (Choose two.)

[NSE5_FMG-7.2 Exam Dumps](#) [NSE5_FMG-7.2 Exam Questions](#)

[NSE5_FMG-7.2 PDF Dumps](#) [NSE5_FMG-7.2 VCE Dumps](#)

<https://www.braindump2go.com/nse5-fmg-7-2.html>



Create New Script

Script Name: Routing

Comments:

Type: CLI Script

Run script on: Device Database

Script details:

```
1 config router prefix-list
2 edit public
3 config rule
4 edit 1
5 set prefix 0.0.0.0/0
6 set action permit
7 next
8 edit 2
9 set prefix 8.8.8.8/32
10 set action deny
11 end
```

Revert All Changes

Advanced Device Filters >

- A. You must install these changes using the Install Wizard to a managed device.
- B. The script history will show successful installation of the script on the remote FortiGate.
- C. The successful execution of a script on the Device Database will create a new revision history.
- D. The Device Settings Status will be tagged as Modified.

Answer: AD

Explanation:

Once scripts are run on the device database, you can then install the changes on a managed device using the installation wizard.

Since the script changed the device settings in FortiManager, the Config Status shows "Modified" and needs to be installed with Installation Wizard.

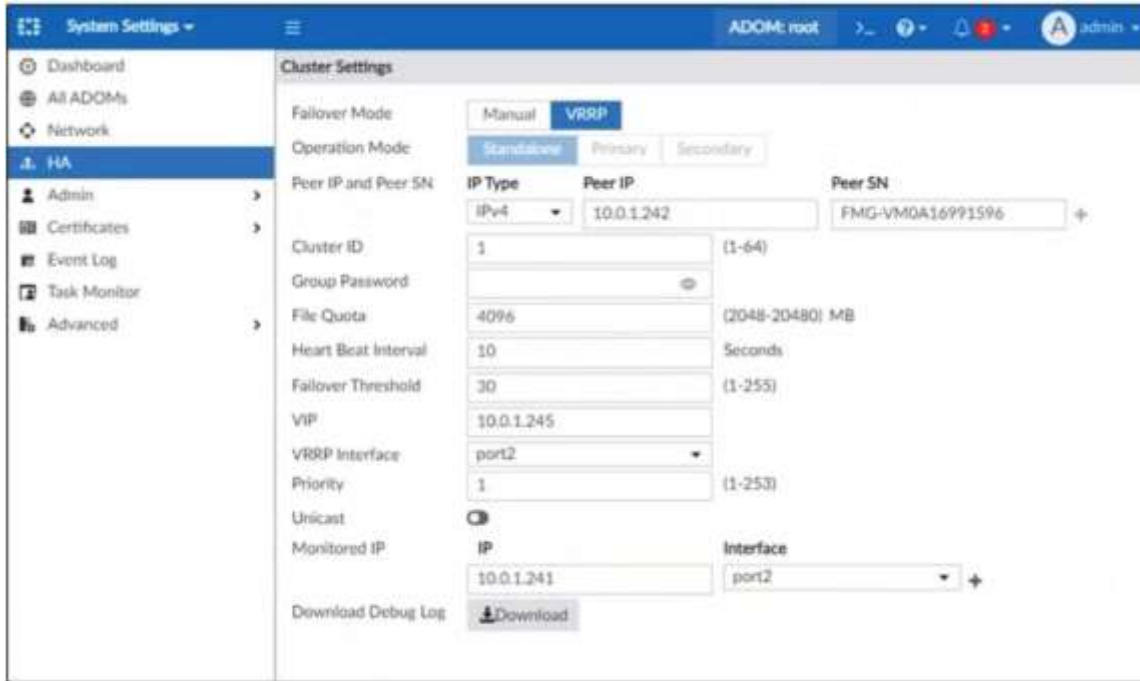
QUESTION 43

Refer to the exhibit. In the event that the monitored interface for the primary FortiManager device fails, which statement is true about FortiManager HA?

[NSE5_FMG-7.2 Exam Dumps](#) [NSE5_FMG-7.2 Exam Questions](#)

[NSE5_FMG-7.2 PDF Dumps](#) [NSE5_FMG-7.2 VCE Dumps](#)

<https://www.braindump2go.com/nse5-fmg-7-2.html>



- A. Reboot the failed device to remove its IP from the primary device.
- B. Manually promote one of the working secondary devices to the primary role, and reboot the old primary device to remove the peer IP of the failed device.
- C. Reconfigure the primary device to remove the peer IP of the failed device.
- D. The FortiManager HA failover is transparent to administrators and does not require any reconfiguration.

Answer: D

Explanation:

Select VRRP to configure automatic failover. When the monitored interface for the primary FortiManager is unreachable or down, HA automatic failover will occur, and the secondary FortiManager will automatically become the primary.

QUESTION 44

Refer to the exhibit showing a Download Import Report. Why is it failing to import firewall policy ID 1?

```
Start to import config from device(Remote-FortiGate) vdom(root) to
adom(root), package(Remote-FortiGate_root)

"firewall address",SKIPPED,"(name=all, oid=2309, DUPLICATE)"

"firewall address",FAIL,"(name=REMOTE_SUBNET, oid=2311,
reason=interface((firewall address:REMOTE_SUBNET) any<-port6) binding
fail)"

"firewall policy",FAIL,"(name=1, oid=3070, reason=interface(interface binding
contradiction. detail: (firewall address:REMOTE_SUBNET) any<-port6) binding
fail)"
```

[NSE5_FMG-7.2 Exam Dumps](#) [NSE5_FMG-7.2 Exam Questions](#)

[NSE5_FMG-7.2 PDF Dumps](#) [NSE5_FMG-7.2 VCE Dumps](#)

<https://www.braindump2go.com/nse5-fmg-7-2.html>

- A. Policy ID 1 for this managed FortiGate already exists on FortiManager in the policy package named Remote-FortiGate.
- B. The address object used in policy ID 1 already exists in the ADOM database with any as the interface association, and conflicts with the address object interface association locally on FortiGate.
- C. Policy ID 1 is configured from the interface any to port6. FortiManager rejects the request to import this policy because the any interface does not exist on FortiManager.
- D. Policy ID 1 does not have the ADOM Interface mapping configured on FortiManager.

Answer: B

QUESTION 45

What will be the result of reverting to a previous revision version in the revision history?

- A. It will generate a new version ID and remove all other revision history versions.
- B. It will install configuration changes to managed device automatically.
- C. It will tag the device settings status as Auto-Update.
- D. It will modify the device-level database.

Answer: D

QUESTION 46

Which two items are included in the FortiManager backup? (Choose two.)

- A. FortiGuard database
- B. Firmware images
- C. Flash configuration
- D. All devices

Answer: CD

Explanation:

<https://community.fortinet.com/t5/FortiManager/Technical-Tip-Items-included-in-the-backup-config-file/ta-p/275704>

QUESTION 47

An administrator's PC crashes before the administrator can submit a workflow session for approval. After the PC is restarted, the administrator notices that the ADOM was locked from the session before the crash. How can the administrator unlock the ADOM?

- A. Restore the configuration from a previous backup.
- B. Delete the previous admin session manually through the FortiManager GUI or CLI.
- C. Log in as Super_User in order to unlock the ADOM.
- D. Log in using the same administrator account to unlock the ADOM.

Answer: B

Explanation:

If a connection to FortiManager unexpectedly closes (PC crashed or browser closed) while an ADOM is locked, it will remain locked until the administrator session times out or the session is deleted. You can delete administrator sessions on the GUI or CLI. After the previous session is deleted, the ADOM will be unlocked immediately.

QUESTION 48

An administrator configures a new OSPF route on FortiManager and has not yet pushed the changes to the managed FortiGate device.

[NSE5_FMG-7.2 Exam Dumps](#) **[NSE5_FMG-7.2 Exam Questions](#)**

[NSE5_FMG-7.2 PDF Dumps](#) **[NSE5_FMG-7.2 VCE Dumps](#)**

<https://www.braindump2go.com/nse5-fmg-7-2.html>

In which database will the configuration be saved?

- A. Revision history database
- B. ADOM-level database
- C. Configuration-level database
- D. Device-level database

Answer: D

QUESTION 49

Refer to the exhibit. An administrator has configured the command shown in the exhibit on FortiManager. A configuration change has been installed from FortiManager to the managed FortiGate that causes the FGFM tunnel to go down for more than 15 minutes.

```
FortiManager # config system dm
(dm) # set rollback-allow-reboot enable
(dm) # end
FortiManager #
```

What is the purpose of this command?

- A. It allows FortiManager to unset the new configuration through CLI and reboot FortiGate.
- B. It allows FortiManager to revert and install a previous configuration revision on the managed FortiGate.
- C. It allows FortiGate to reboot and recover the previous configuration from its configuration file.
- D. It allows FortiGate to reboot and restore a previously working firmware image.

Answer: C

Explanation:

If the connection fails to reestablish, FortiGate applies the unset command after 15 minutes (not configurable and not based on sock timeout values). If the connection remains down, and rollback-allow-reboot is enabled on FortiManager, FortiGate reboots to recover the previous configuration from its configuration file.

QUESTION 50

What is the purpose of ADOM revisions?

- A. To save the FortiManager configuration in the System Checkpoints
- B. To revert individual policy packages and device-level settings for a managed FortiGate
- C. To save the current state of the whole ADOM
- D. To save the current state of all policy packages and objects for an ADOM

Answer: D

QUESTION 51

Refer to the exhibit. Given the configuration shown in the exhibit, what are two results from this configuration? (Choose two.)

[NSE5_FMG-7.2 Exam Dumps](#) [NSE5_FMG-7.2 Exam Questions](#)

[NSE5_FMG-7.2 PDF Dumps](#) [NSE5_FMG-7.2 VCE Dumps](#)

<https://www.braindump2go.com/nse5-fmg-7-2.html>

```
FortiManager # config system global
(global)# set workspace-mode normal
(global)# end
FortiManager #
```

- A. Two or more administrators can make configuration changes at the same time, in the same ADOM.
- B. The same administrator can lock more than one ADOM at the same time.
- C. Concurrent read-write access to an ADOM is disabled.
- D. You can validate administrator login attempts through external servers.

Answer: BC

QUESTION 52

Refer to the exhibit. An administrator is about to add the FortiGate device to FortiManager using the discovery process. FortiManager is operating behind a NAT device, and the administrator configured the FortiManager NATed IP address under the FortiManager system administration settings.



What is the expected result?

- A. During discovery, FortiManager uses only the FortiGate serial number to establish the connection.
- B. During discovery, FortiManager sets the FortiManager NATed IP address on FortiGate.
- C. During discovery, FortiManager sets the NATed device IP address on FortiGate.
- D. During discovery, FortiManager sets both the FortiManager NATed IP address and NAT device IP address on FortiGate.

Answer: B

Explanation:

You can configure the FortiManager NATed IP address on FortiGate under the central management configuration. This allows FortiGate to announce itself to FortiManager and try to re-establish the FGFM tunnel, if it is torn down. Configuring the FortiManager NATed IP address on FortiGate allows both FortiManager and FortiGate to re-establish the FGFM tunnel. Also, if you configure the FortiManager NATed IP address under the FortiManager system administrator settings, FortiManager sets this address on FortiGate during the discovery process.

QUESTION 53

An administrator has enabled Service Access on FortiManager. What is the purpose of Service Access on the FortiManager interface?

- A. It allows FortiManager to determine the connection status of managed devices.
- B. It allows administrative access to FortiManager.

[NSE5_FMG-7.2 Exam Dumps](#) [NSE5_FMG-7.2 Exam Questions](#)

[NSE5_FMG-7.2 PDF Dumps](#) [NSE5_FMG-7.2 VCE Dumps](#)

<https://www.braindump2go.com/nse5-fmg-7-2.html>

- C. It allows third-party applications to gain read/write access to FortiManager.
- D. It allows FortiManager to respond to requests for FortiGuard services from FortiGate devices.

Answer: D

Explanation:

Select the Fortinet services that are allowed access on this interface. These include FortiGate Updates and Web Filtering. Service access is not enabled on any port by default.

<https://docs.fortinet.com/document/fortimanager/7.2.4/administration-guide/578841/configuring-network-interfaces>

[NSE5_FMG-7.2 Exam Dumps](#) [NSE5_FMG-7.2 Exam Questions](#)

[NSE5_FMG-7.2 PDF Dumps](#) [NSE5_FMG-7.2 VCE Dumps](#)

<https://www.braindump2go.com/nse5-fmg-7-2.html>