Fortinet

Exam Questions FCP_FMG_AD-7.6

FCP - FortiManager 7.6 Administrator

NEW QUESTION 1
An administrator has a FortiGate-HQ device with VDOMs—root, HR and Facilities, currently managed under the FortiManager ADOM—Site1. They try to move VDOM HR to the FortiManager ADOM—Site2, but it does not work.
Why is the administrator not able to move FortiGate-HQ VDOM HR to FortiManager ADOM—Site2?

A. The FortiGate-HQ must be managed under the FortiManager ADOM—root to allow moving its VDOMs to different ADOMs.
B. The administrator must have full access in the device layer of FortiGate-HQ VDOM-root before they can VDOMs to different ADOMs.
C. FortiManager must be in ADOM normal mode, which does not allow VDOMs to be managed separately.
D. The administrator must delete the FortiGate-HQ device from FortiManager and add it again using the Add Device wizard before moving the VDOM.

Answer: A

Explanation:
FortiGate devices must be managed under the FortiManager ADOM corresponding to the root VDOM to allow their individual VDOMs to be moved and managed in different ADOMs. Managing the root VDOM in a different ADOM prevents moving subordinate VDOMs across ADOMs.

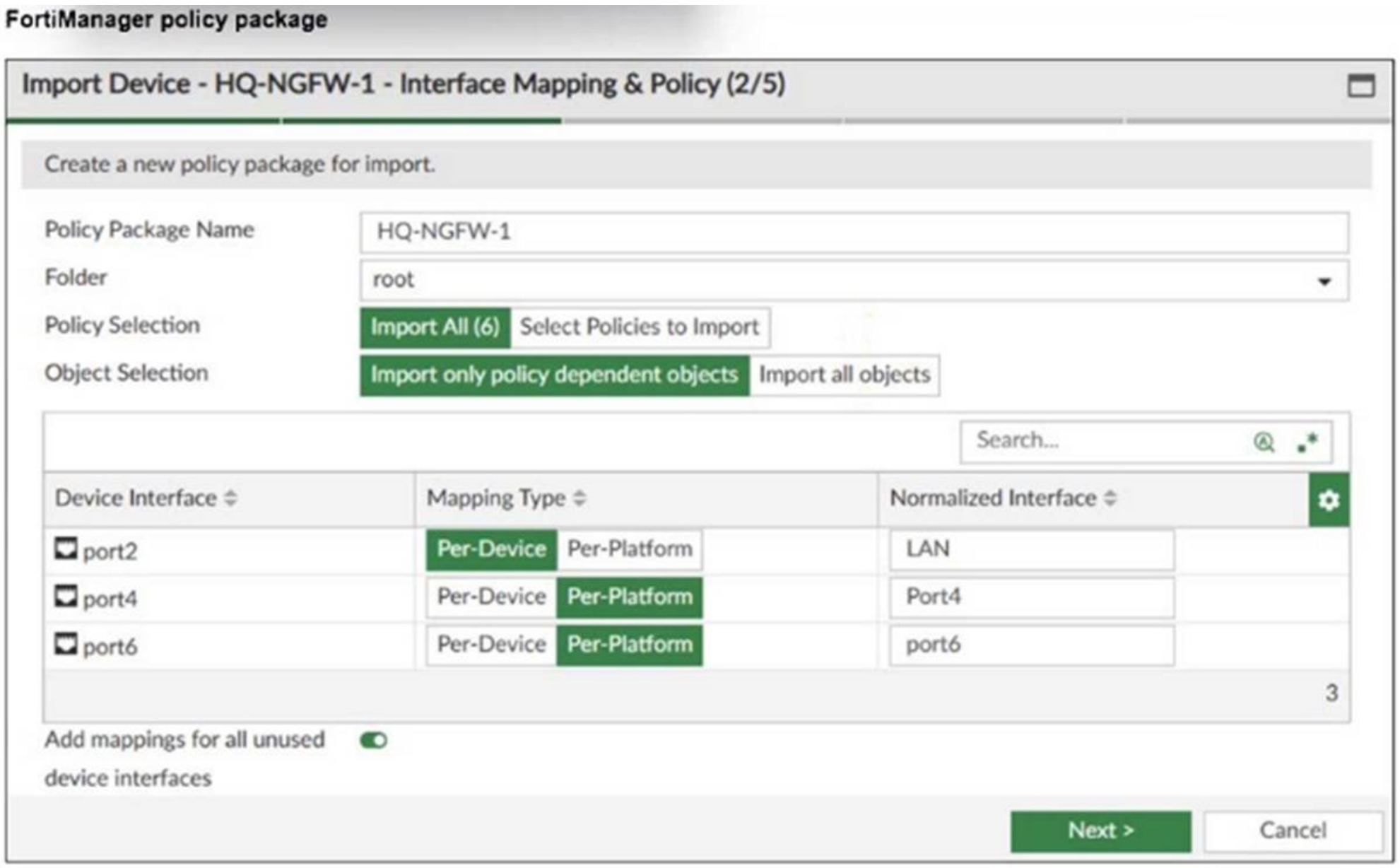
NEW QUESTION 2
Which is recommended when you are managing a high volume of logs in your network?

A. Store logs on FortiManager and use FortiView.
B. Add and manage FortiAnalyzer from FortiManager.
C. Enable advanced ADOM mode on FortiManager.
D. Forward logs from FortiAnalyzer to FortiManager daily.

Answer: B

Explanation:
Adding and managing FortiAnalyzer from FortiManager is recommended for handling a high volume of logs, as FortiAnalyzer is designed specifically for centralized log management, analysis, and reporting, which offloads this workload from FortiManager.

NEW QUESTION 3
Refer to the exhibit.



An administrator added a FortiGate device to FortiManager with the default object settings at the ADOM layer.
What can you conclude from the import policy package process of the HQ-NGFW- 1 device?

A. The administrator must select Per Platform for all interfaces to correctly detect all interfaces from HQ- NGFW-1.
B. The administrator must manually create the port4 interface on the ADOM layer to avoid import policy errors.
C. FortiManager will create LAN, port4, and port6 as normalized interfaces at the ADOM layer.
D. FortiGate may not work as expected when the administrator does not import all objects.

Answer: C

Explanation:

The import process shows that FortiManager will create normalized interfaces named LAN, port4, and port6 at the ADOM layer, mapping them to the corresponding device interfaces based on the import settings.

NEW QUESTION 4
An administrator must create a policy and install it on a FortiGate device within an ADOM in backup mode. How can the administrator perform this task?

A. Use the Install Wizard located on the device manager.
B. Enable workflow mode to allow policy creation and approval.
C. Make sure the ADOM and FortiGate firmware versions match and use the ADOM policy package.
D. Use a FortiManager script to apply the configuration changes.

Answer: D

Explanation:
In backup mode, FortiManager does not directly manage policy installation via the usual ADOM policy packages; instead, administrators use FortiManager scripts to push configuration changes, including policies, to FortiGate devices.

NEW QUESTION 5
Refer to the exhibit.

An administrator assigned a new policy package to FortiGate HQ-NGFW-1. In the installation preview, they noticed some settings they did not modify and are unsure about the changes.
Based on the exhibit, which two things will happen if they continue with the installation? (Choose two.)

A. FortiGate HQ-NGFW-1 can use FortiManager firmware templates to upgrade firmware and ratings.
B. FortiGate HQ-NGFW-1 can contact the FortiManager acting as FortiGuard Distribution Server (FDS) to download FortiGuard updates.
C. FortiGate HQ-NGFW-1 will use the root_CA3 certificate in firewall address objects or policies.
D. FortiManager will install the CA certificate named root_CA3 to authenticate FortiGate-to-FortiManager communication protocol (FGFM) tunnel connections with FortiGate HQ- NGFW-1.

Answer: BD

Explanation:
The configuration includes a server-list with server-type set to "update rating," which enables FortiGate HQ- NGFW-1 to contact FortiManager as a FortiGuard Distribution Server (FDS) for FortiGuard updates.
The installation includes a root_CA3 certificate, which FortiManager will install on FortiGate HQ-NGFW-1 to authenticate FGFM tunnel connections between the

devices.

NEW QUESTION 6
An administrator has assigned a global policy package to a new ADOM named ADOM1.
What will happen if the administrator tries to create a new policy package in ADOM1?

A. The administrator will be able to select the option to assign the global policy package to the new policy package.
B. FortiManager will automatically assign the global policy package to the new policy package.
C. FortiManager will automatically install policies on the policy package in ADOM1.
D. The administrator will have to assign the global policy package from the global ADOM.

Answer: A

Explanation:
When a global policy package is assigned to an ADOM, administrators creating new policy packages within that ADOM have the option to select and assign the global policy package to the new policy package if desired.

NEW QUESTION 7
What is the best explanation of how FortiManager helps with mass provisioning?

A. It upgrades the OS of each FortiGate device.
B. It provides local FortiGuard Distribution Server (FDS) services to the network.
C. It uses templates to configure the same settings on many devices simultaneously.
D. It sends email alerts when new devices connect.

Answer: C

Explanation:
FortiManager helps with mass provisioning by using templates that allow administrators to configure the same settings on multiple FortiGate devices simultaneously, streamlining deployment and management.

NEW QUESTION 8
Refer to the exhibit.

```
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)"
```

What can you conclude from the downloaded import report?

A. FortiManager does not support per-device mapping for firewall addresses.
B. The administrator will see a new policy package named Remote-FortiGate_root in the FortiManager ADOM database.
C. FortiManager will change the configuration of REMOTE_SUBNET to match the interface mapping coming in from Remote-FortiGate.
D. As a result of this policy import process, FortiManager will create a new firewall address called REMOTE_SUBNET in the ADOM database.

Answer: B

Explanation:
The import report shows that a new policy package named Remote-FortiGate_root will be created in the FortiManager ADOM database, but some firewall addresses and policies failed to import due to interface binding conflicts.

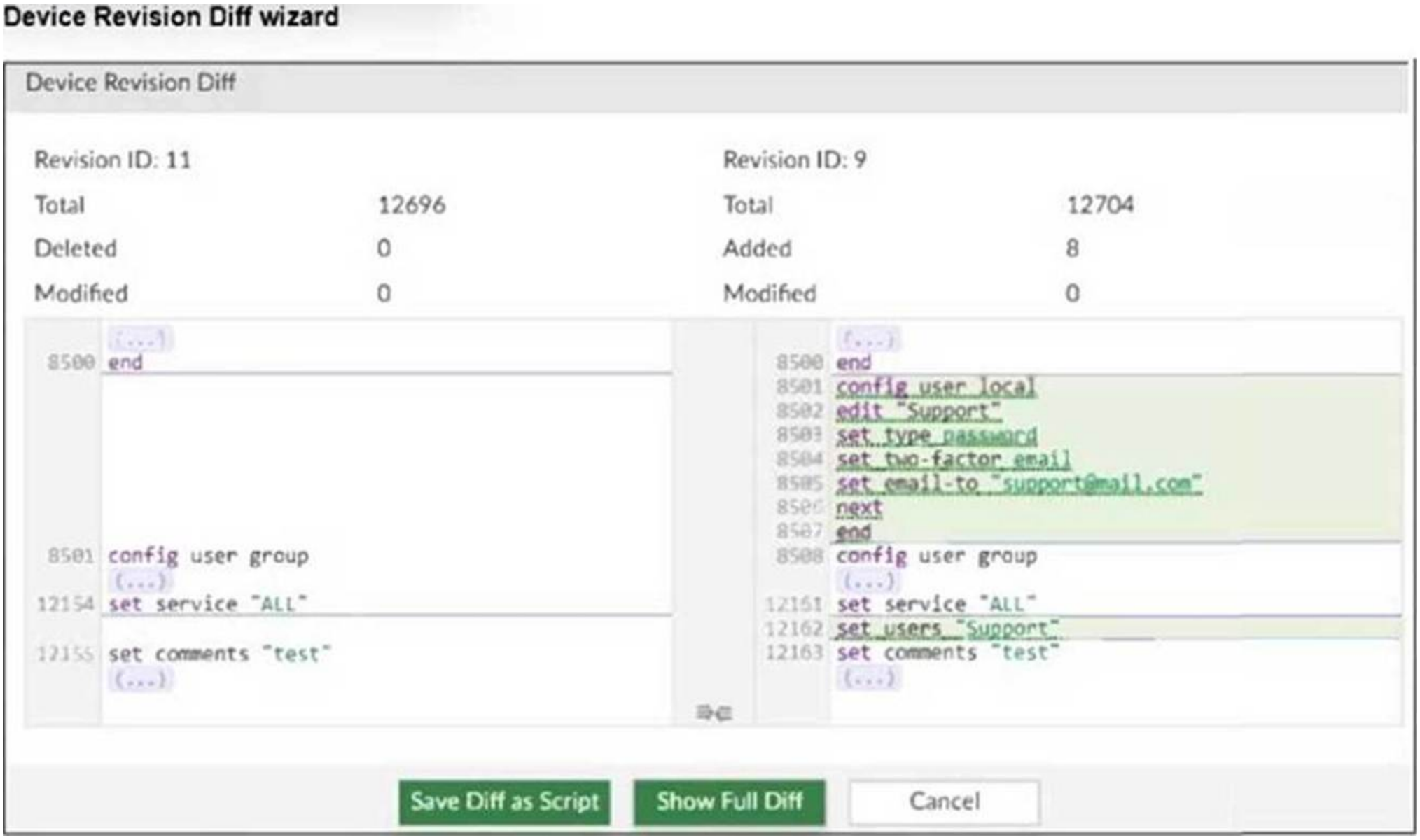
NEW QUESTION 9
What is the purpose of ADOM revisions?

A. ADOM revisions find unused, duplicate, and unnecessary firewall policies and objects.
B. ADOM revisions show specific changes in a policy package when it is installed.
C. ADOM revisions compare previous snapshots of the Policy Package and ADOM-level objects with the device-level database.
D. ADOM revisions save the current state of all policy packages and objects for an ADOM.

Answer: D

Explanation:
ADOM revisions save the current state of all policy packages and objects within an ADOM, allowing administrators to track changes over time and revert to previous configurations if needed.

NEW QUESTION 10
Refer to the exhibits.



An administrator needed to recover all the configurations related to the user, Support. The configurations were saved in configuration revision ID 9.
The administrator reverted the configuration using theConfiguration Revision Historywindow and received the CLI output shown in the exhibit.
What can you conclude from the CLI output?

A. The administrator set the flag to 0 to prevent configuration overrides.
B. The administrator reinstalled the policy package.
C. The administrator needs to retrieve the device to correctly detect the FortiGate firmware version.
D. The administrator installed only the device-level configuration.

Answer: C

Explanation:
The CLI output shows the status "dev-db: not modified; conf: in sync; cond: OK; dm: installed," but the firmware version for the device is listed as "[unknown]." This indicates that FortiManager has not properly detected the FortiGate firmware version, likely because the device needs to be retrieved to update its information.

NEW QUESTION 10
Which output is displayed right after moving the ISFW device from one ADOM to another?
A)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID   SN                HA      IP            NAME          ADOM     IPS                 FIRMWARE
fmgfaz-managed  325   FGVM010000077646  -       10.0.1.200    ISFW          ADOM76   7.00741 (regular)   7.0 MR6 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up
                |- vdom:[3]root flags:1 adom:ADOM76 pkg:[out-of-sync]ISFW
```

B)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID   SN                HA      IP            NAME          ADOM     IPS                 FIRMWARE
fmgfaz-managed  325   FGVM010000077646  -       10.0.1.200    ISFW          ADOM76   7.00741 (regular)   7.0 MR6 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                |- vdom:[3]root flags:0 adom:ADOM76 pkg:[imported]ISFW
```

C)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID   SN                HA   IP            NAME   ADOM    IPS                FIRMWARE
fmgfaz-managed  325   FGVM010000077646  -    10.0.1.200    ISFW   ADOM76  7.00741 (regular)  7.0 MR6 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                |- vdom:[3]root flags:0 adom:ADOM76 pkg:[never-installed]
```

D)

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID   SN                HA   IP            NAME   ADOM    IPS                FIRMWARE
fmgfaz-managed  325   FGVM010000077646  -    10.0.1.200    ISFW   ADOM76  7.00741 (regular)  7.0 MR6 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
                |- vdom:[3]root flags:0 adom:ADOM76 pkg:[unknown]ISFW
```

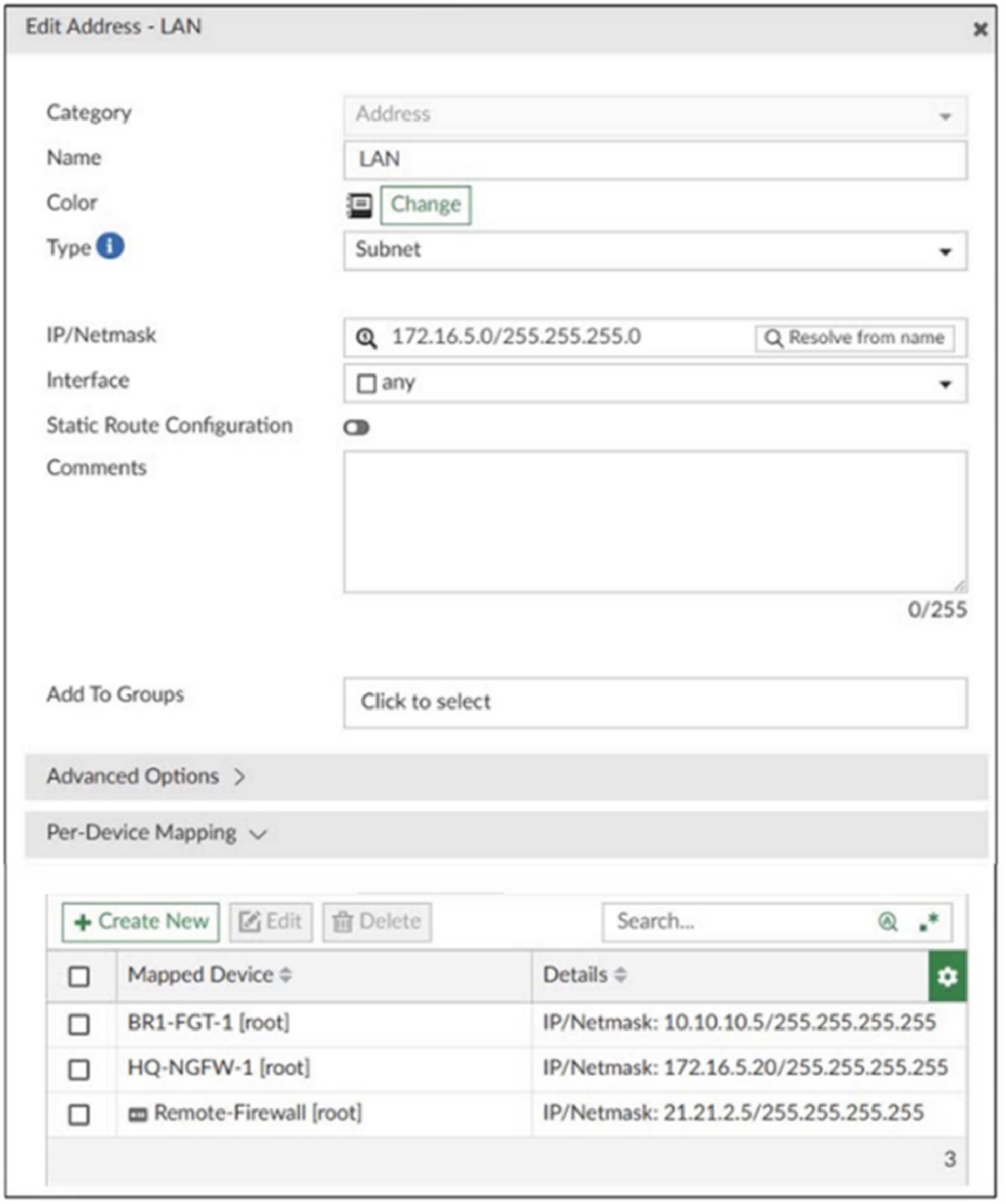
A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Explanation:
Right after moving the ISFW device to a new ADOM, the status typically shows the policy package as never-installed, indicating that the device has been assigned to the new ADOM but no policy package has yet been installed in that ADOM.

NEW QUESTION 13
Refer to the exhibit.

FortiManager address object



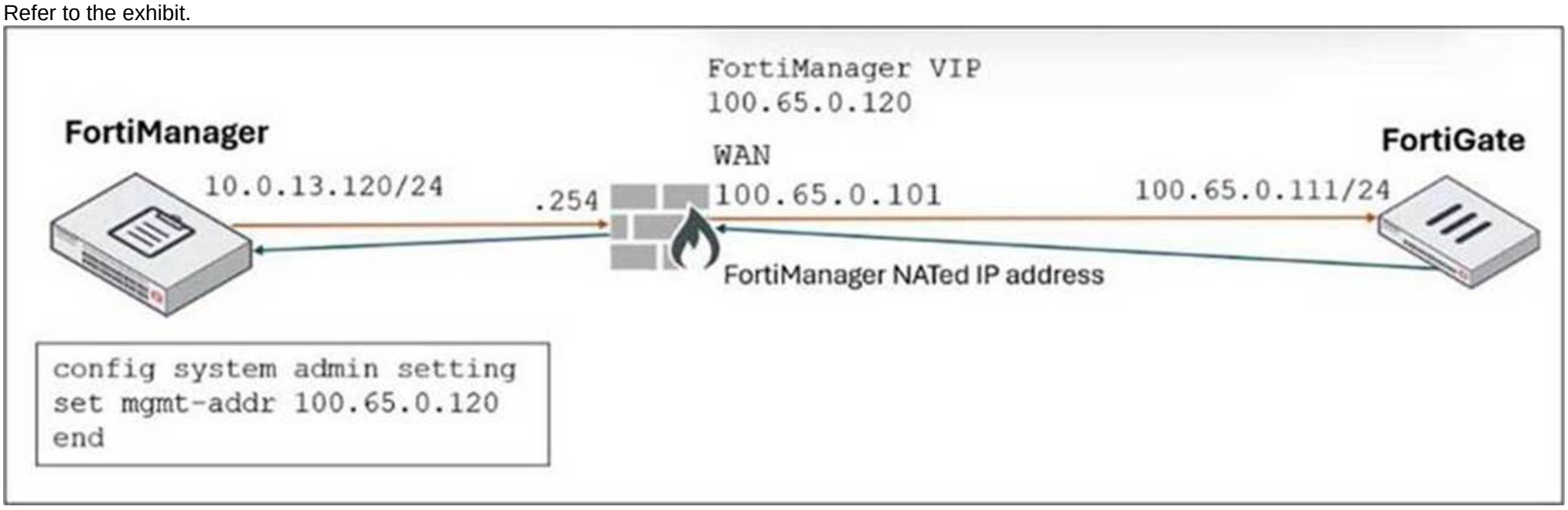
An administrator has created a firewall address object that is used in multiple policy packages for multiple FortiGate devices in an ADOM.
After the installation operation is performed, which IP/netmask will be installed on Remote-Firewall [VDOM1] for the LAN firewall address object?

A. 21.21.2.5/255.255.255.255
B. 172.16.5.20/255.255.255.255
C. 172.16.5.0/255.255.255.0
D. 10.10.10.5/255.255.255.255

Answer: A

Explanation:
The per-device mapping overrides the global IP/netmask setting for the firewall address object. For the device "Remote-Firewall," the mapped IP/netmask is 21.21.2.5/255.255.255.255, so this value will be installed on Remote-Firewall [VDOM1].

NEW QUESTION 15
Refer to the exhibit.



FortiManager is operating behind a network address translation (NAT) device, and the administrator configured the FortiManager NATed IP address under the FortiManager system administration settings.
What is the expected result during discovery?

A. FortiManager sets both the 100.65.0.120 IP address and 10.0.13.120 IP address on FortiGate.
B. FortiManager sets both the 100.65.0.120 IP address and 100.65.0.101 IP address on FortiGate.
C. FortiManager sets the 100.65.0.101 IP address on FortiGate.
D. FortiManager sets the 100.65.0.120 IP address on FortiGate.

Answer: D

Explanation:
When FortiManager is behind a NAT device, setting the NATed IP address (100.65.0.120) in the system admin settings causes FortiManager to use that NATed IP address for communication and configuration with FortiGate during discovery and management operations.

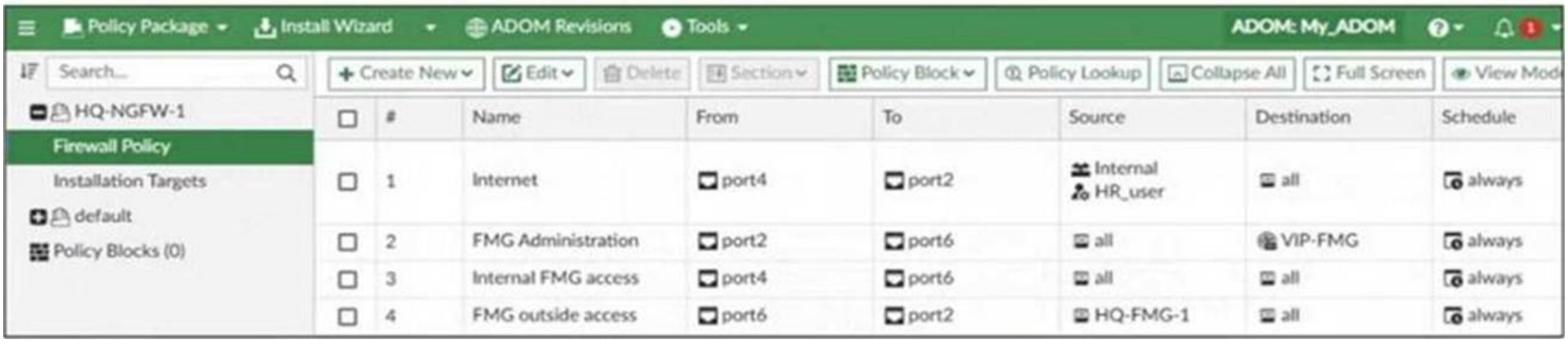
NEW QUESTION 16
An administrator configures a new BGP peer in the FortiManager device-level database of FortiGate. They reinstall the policy package to the managed FortiGate device without any errors. However, when the administrator logs in to FortiGate, they do not see the BGP configuration changes.
What is the most likely reason why FortiManager did not push the BGP peer changes to FortiGate?

A. The administrator must run a sanity check on FortiManager to make sure the database is not corrupted.
B. Fortigate has a BGP template assigned on the FortiManager database.
C. The administrator must use the Install Wizard and select Install device settings only to push BGP settings
D. The FortiGate firmware version is different from the FortiManager ADOM version.

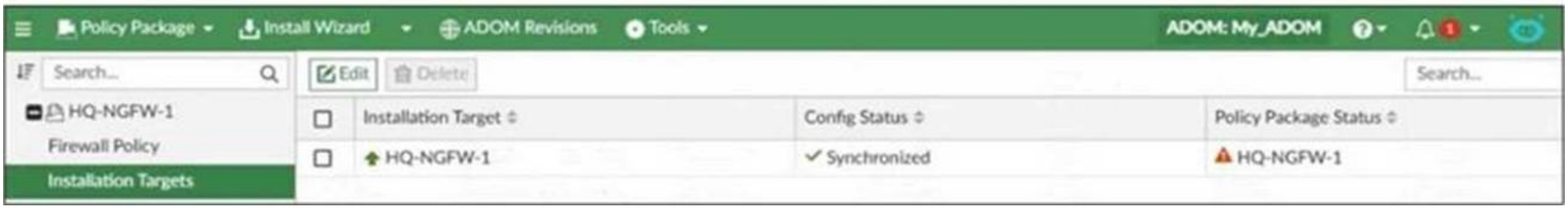
Answer: B

Explanation:
If a BGP template is assigned to the FortiGate device on FortiManager, device-level BGP configurations made directly in the device-level database are overridden by the template settings, so the changes do not get pushed to the device.

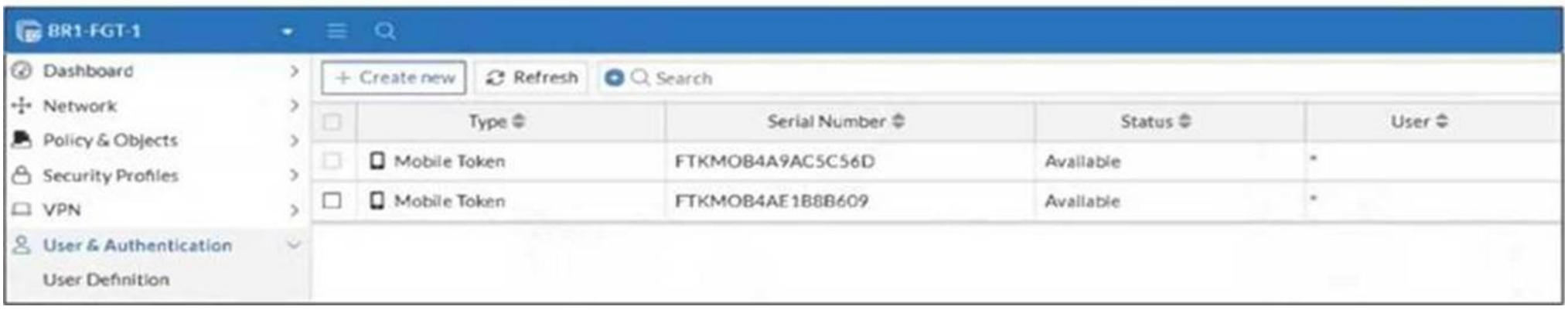
NEW QUESTION 19
Refer to the exhibits.
Firewall policies



Installation target



BR1-FGT-1 FortiTokens



An administrator needs to push a FortiToken Mobile to assign it to HR_user in the HQ-NGFW-1.
However, when installing the policy package, they receive the following error message:

```
Copy device global objects

Vdom copy failed:
error -999 -

Copy objects for vdom root
"firewall policy", "1", id=5532, COMMIT FAIL - invalid value - prop[user fortitoken]:
Mobile FortiToken FTKMOB4A9AC5C56D used by user local HR_user could not be found at
device
"user local", "FTKMOB4A9AC5C56D", id=5586, COMMIT FAIL - invalid value - prop[user
fortitoken]: Mobile FortiToken FTKMOB4A9AC5C56D used by user local HR_user could not
be found at device
```

Why is the administrator not able to install the FortiToken on the HQ-NGFW-1 firewall?

A. The administrator must use a user local meta field to assign FortiToken.
B. The administrator must use a valid FortiToken that exists on HQ-NGFW-1.
C. The administrator must use a metadata variable to assign the same FortiToken to multiple users in FortiManager.
D. The administrator must use per-device mapping to assign the FortiToken to HQ-NGFW-1.

Answer: B

Explanation:
The error occurs because the FortiToken used (FTKM0B4A9AC5C56D) must already exist and be registered on the FortiGate device HQ-NGFW-1. FortiManager cannot push or create new FortiTokens on the device; the token must be valid and present on the FortiGate before it can be assigned to a user.

NEW QUESTION 22
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FMG_AD-7.6 Practice Exam Features:

* FCP_FMG_AD-7.6 Questions and Answers Updated Frequently

* FCP_FMG_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FMG_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FMG_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year