# Fortinet

## Exam Questions FCP_FMG_AD-7.6

FCP - FortiManager 7.6 Administrator

**NEW QUESTION 1**
Refer to the exhibit.

```
FortiManager # diagnose dvm device list
--- There are currently 6 devices/vdoms managed ---
--- There are currently 6 devices/vdoms count for license ---

TYPE            OID    SN               HA      IP             NAME          ADOM     IPS                FIRMWARE        HW_GenX
fmgfaz-managed  188    FGVM02TM24013504 -       100.65.1.111   BR1-FGT-1     My_ADOM  7.0 MR6 (3401)  N/A
                |- STATUS: dev-db: not modified; conf: in sync; cond: pending; dm: installed; conn: up; template:[modified]default
                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[imported]BR1-FGT-1
```

Which two statements about the output are true? (Choose two.)

A. The latest revision history for the managed FortiGate does not match the device-level database.
B. Configuration changes have been installed on FortiGate, updating policy and device-level database.
C. The latest revision history for the managed FortiGate does match the FortiManager policy database.
D. The system template default will override device-level database configurations.

**Answer:** AD

**Explanation:**
The status "pending" indicates the latest revision history does not match the device-level database, meaning there are unapplied changes.
The template is marked as [modified], so the system template default will override device-level database configurations when installed.

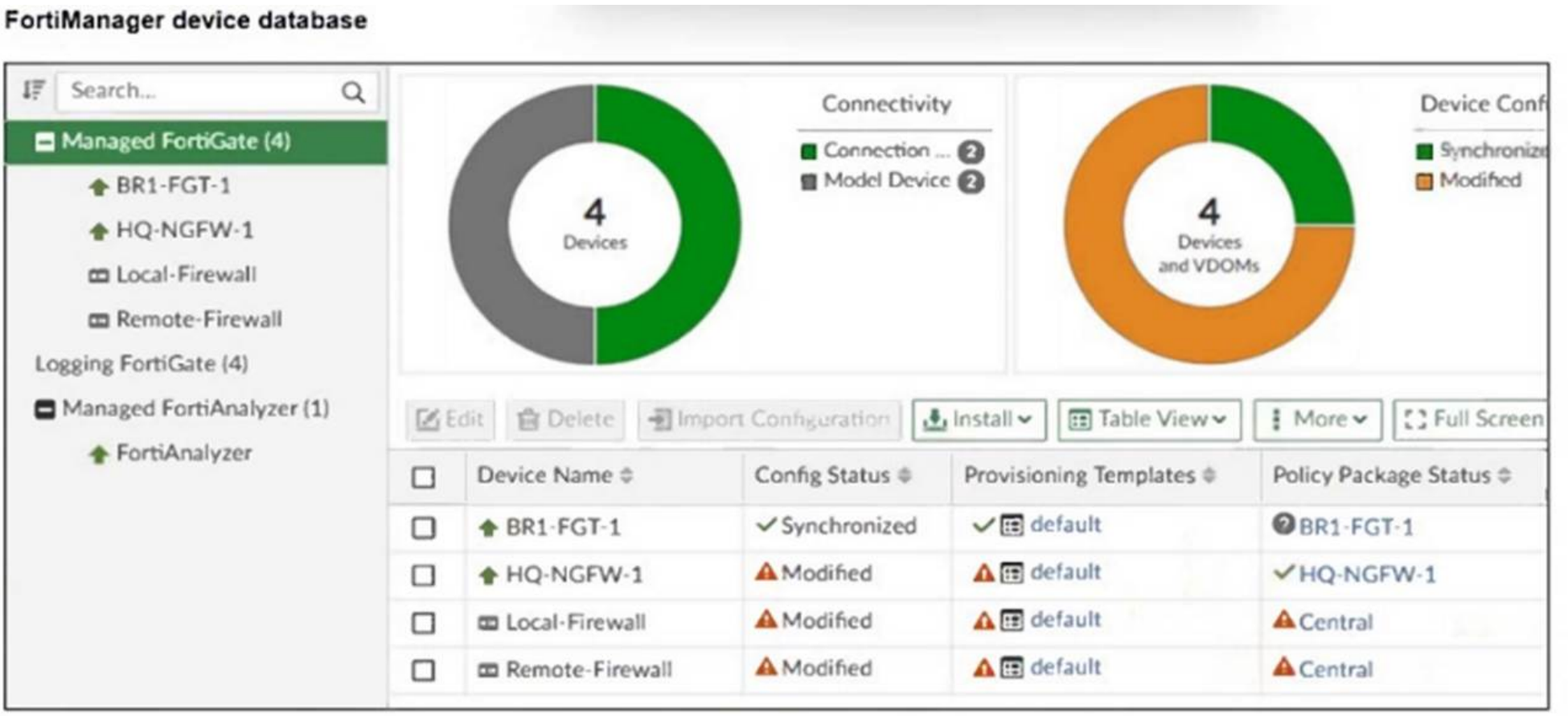
**NEW QUESTION 2**
An administrator must create a policy and install it on a FortiGate device within an ADOM in backup mode. How can the administrator perform this task?

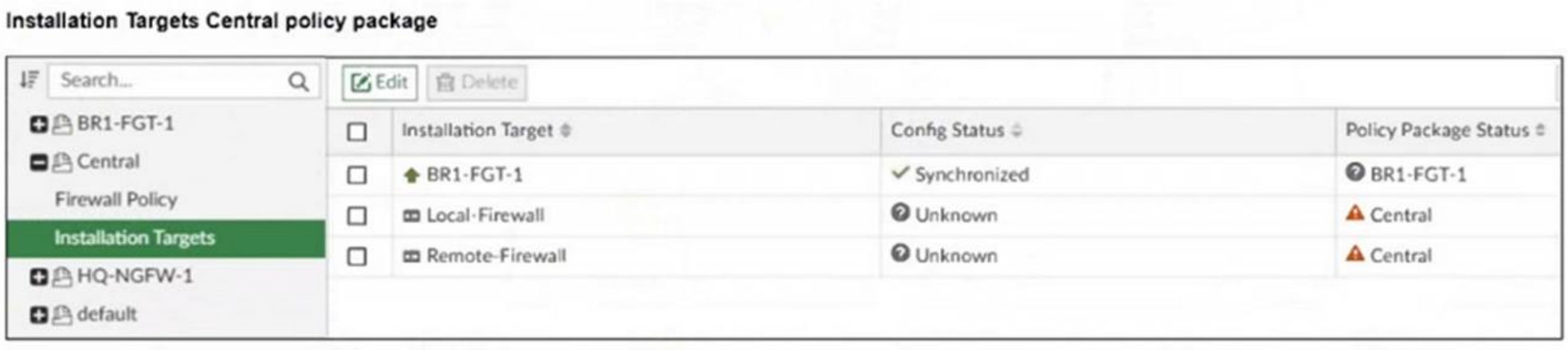
A. Use the Install Wizard located on the device manager.
B. Enable workflow mode to allow policy creation and approval.
C. Make sure the ADOM and FortiGate firmware versions match and use the ADOM policy package.
D. Use a FortiManager script to apply the configuration changes.

**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 3**
Refer to the exhibits.





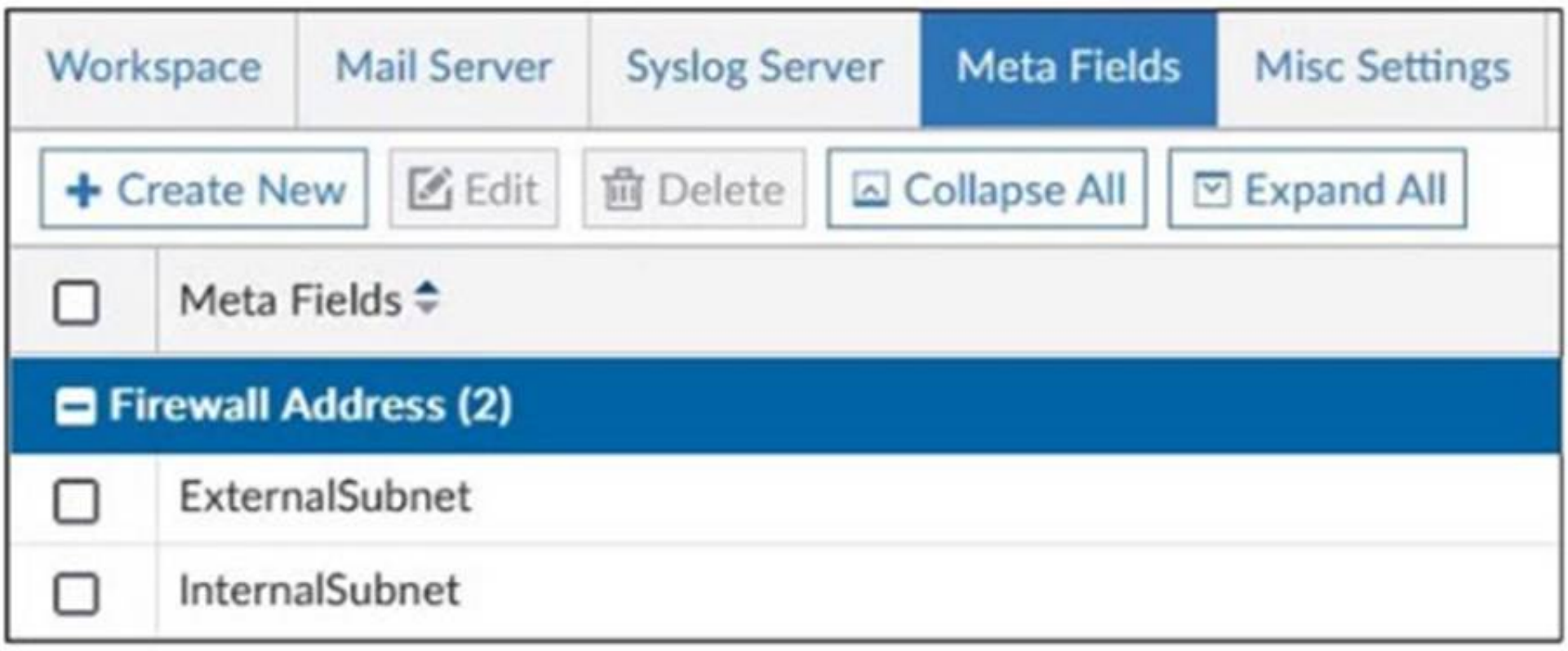

An administrator has been asked to install the same policies from a central policy package onto the BR1-FGT- 1 firewall.
The administrator added BR1-FGT-1 as a target in the central policy package installation.
What should the administrator do when reinstalling the central policy package on the BR1-FGT-1 firewall?

A. Assign only one policy package to the firewall because FortiManager does not allow more than one policy package assigned per device at the same time.
B. Import the policy package to change the unknown status and synchronize the policy package.
C. Use the install wizard to install the central policy package on the BR1-FGT-1 firewall.
D. First resolve the modified status in the configuration and provisioning templates to allow a smooth installation.

**Answer:** C

**Explanation:**
Using the Install Wizard is the recommended method to reinstall the central policy package on the BR1-FGT- 1 firewall, ensuring all settings, installation targets, and dependencies are correctly processed during installation.

**NEW QUESTION 4**
Refer to the exhibit.




An administrator created two new meta fields in FortiManager. Which operation can you perform with these parameters?

A. You can add them to objects as custom attributes.
B. You can export them to be used in other ADOMs.
C. You can use them as variables in scripts.
D. You can invoke them using the $ character.

**Answer:** A

**Explanation:**
Meta fields in FortiManager can be added to objects as custom attributes, allowing administrators to categorize and add additional information to firewall objects for easier management and identification.

**NEW QUESTION 5**
Which two conditions trigger FortiManager to create a new revision history? (Choose two.)

A. When FortiManager installs device-level changes on a managed device
B. When changes to the device-level database are made on FortiManager
C. When FortiManager is auto-updated with configuration changes made directly on a managed device
D. When a provisioning template is assigned to a managed device on the device-level database

**Answer:** BC

**Explanation:**
FortiManager creates a new revision history entry whenever changes are made to the device-level database on FortiManager.

FortiManager also creates a new revision when it auto-updates its database with configuration changes detected directly on a managed device.

**NEW QUESTION 6**
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
```

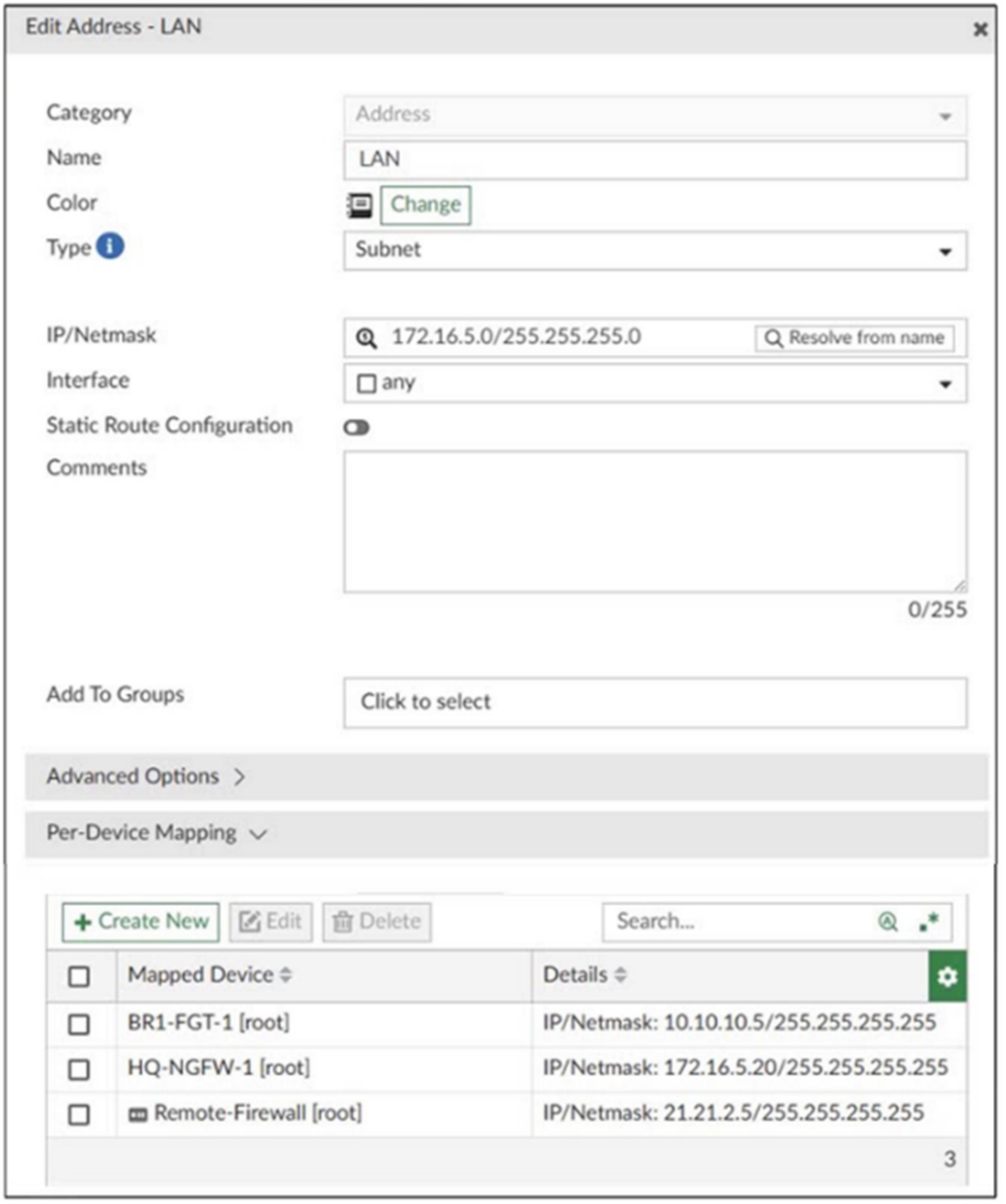
A. Option A
B. Option B
C. Option C
D. Option D

**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 7**
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].

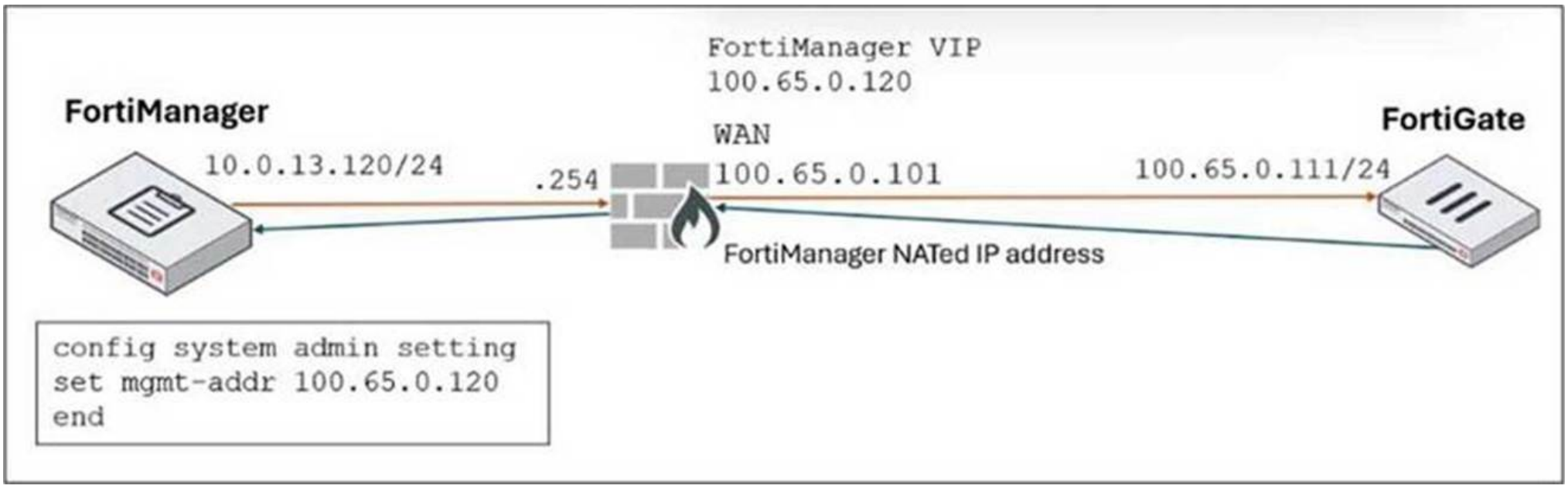
**NEW QUESTION 8**
A service provider administrator has assigned a global policy package to a managed customer ADOM named My_ADOM. The customer administrator has access only to My_ADOM.
How can the customer administrator edit the global header policy of the global policy package?

A. The customer administrator can edit the header policy by using workspace mode on the global ADOM.
B. The customer administrator can edit the header policy by using workflow mode on the global ADOM and My_ADOM.
C. The service provider administrator can unlock the global policy from the global ADOM to authorize changes to the customer administrator.
D. The customer administrator cannot edit the global header policy; only the service provider administrator can make changes from the global ADOM.

**Answer:** D

**Explanation:**
The global policy package is managed only from the global ADOM by the service provider administrator. Customer administrators with access solely to their ADOM (My_ADOM) cannot edit the global header policy; such changes must be made by the service provider administrator in the global ADOM.

**NEW QUESTION 9**
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 10**
After correcting a policy package configuration issue, you want to prevent administrators from repeating the mistake that caused the issue.
Which FortiManager approach best meets this need?

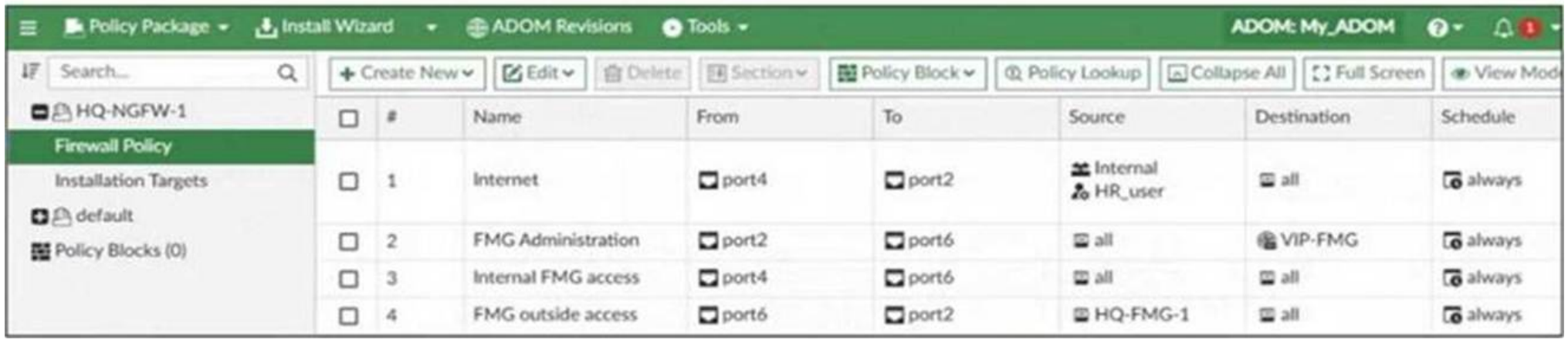
A. Configure an TCL script to run locally on FortiManager for each FortiGate.
B. Restrict administrators with an administration profile from viewing the revision history to limit who can make changes.
C. Enable the change note to require administrators to add a note whenever they change object configurations.
D. Enable a workflow requiring approval before installing policy packages on any FortiGate.

**Answer:** D

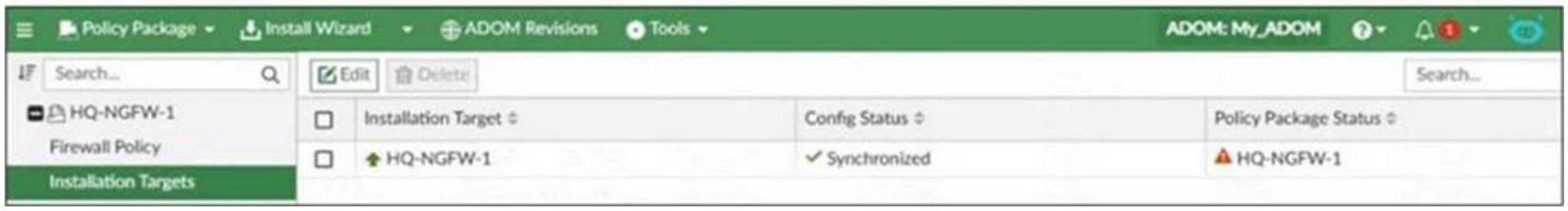
**Explanation:**
Enabling a workflow with approval ensures that any policy package changes must be reviewed and approved before installation, preventing administrators from repeating configuration mistakes and enforcing change control.

**NEW QUESTION 10**
Refer to the exhibits.

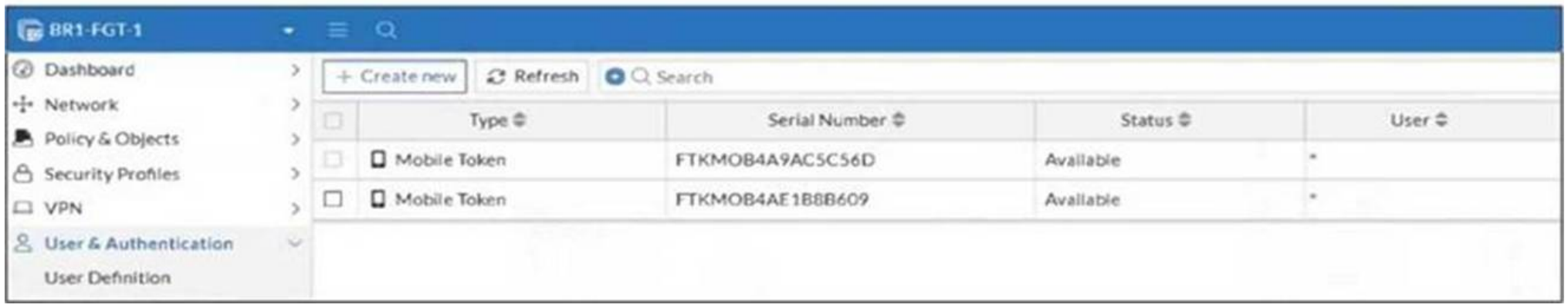
**Firewall policies**




**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 15**
.....

# 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