Fortinet

Exam Questions FCP_FMG_AD-7.6

FCP - FortiManager 7.6 Administrator

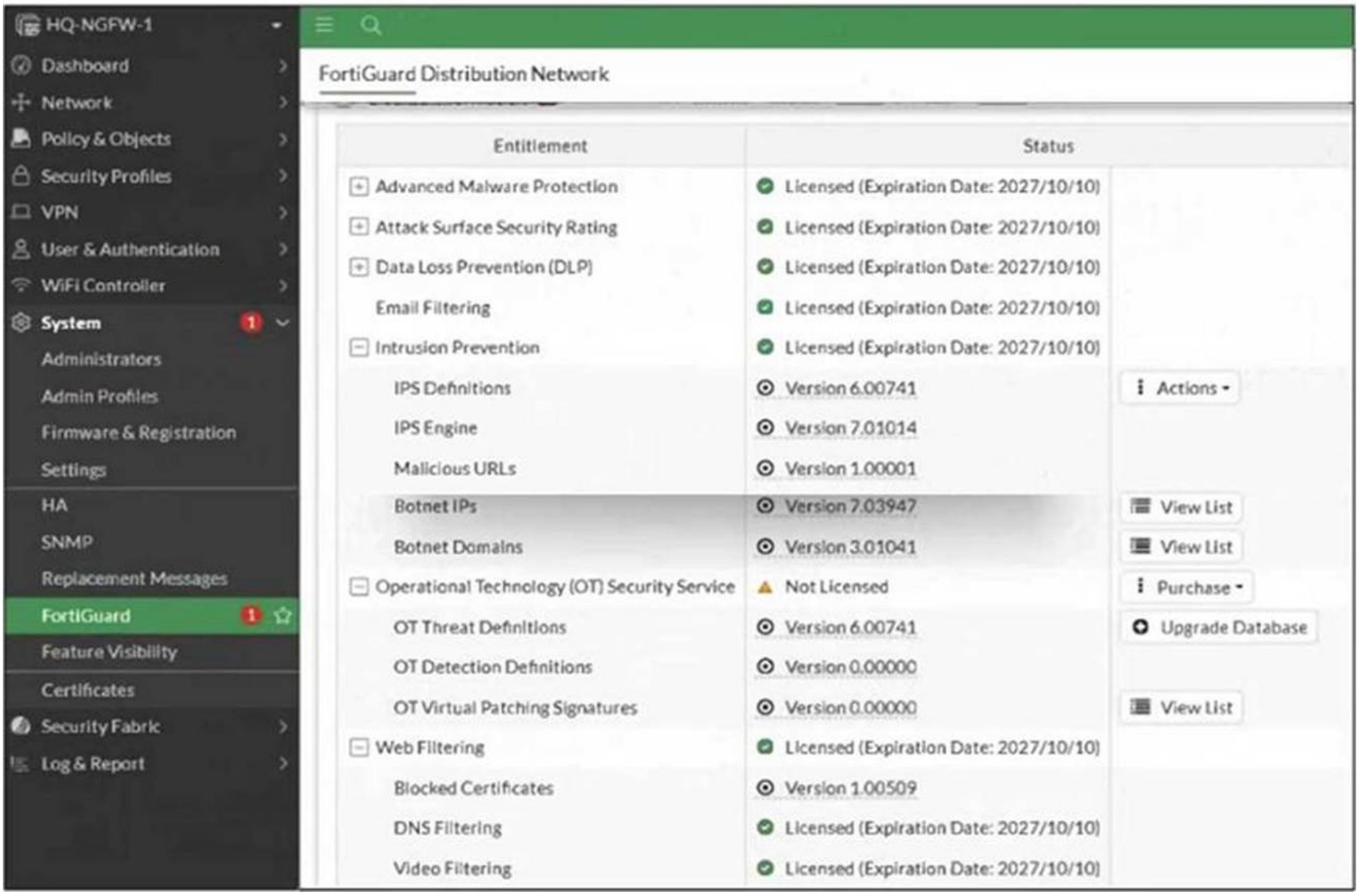
NEW QUESTION 1
The administrator uses FortiManager to push a CLI script using the Remote FortiGate Directly (via CLI) option to configure an IPsec VPN. However, when running the script, the administrator receives the following error:
config vpn ipsec phase2-interface [parameter(s) invalid. detail: object mismatch]
What must the administrator do to resolve the script error and successfully apply the IPsec configuration?

A. Add the end command after finishing the IPsec phase 1-interface configuration block.
B. Use IPsec templates to deploy provisioning templates.
C. Add a second config vpn ipsec phase2-interface block without linking it to phase1.
D. Run the script using the policy package or ADOM database method.

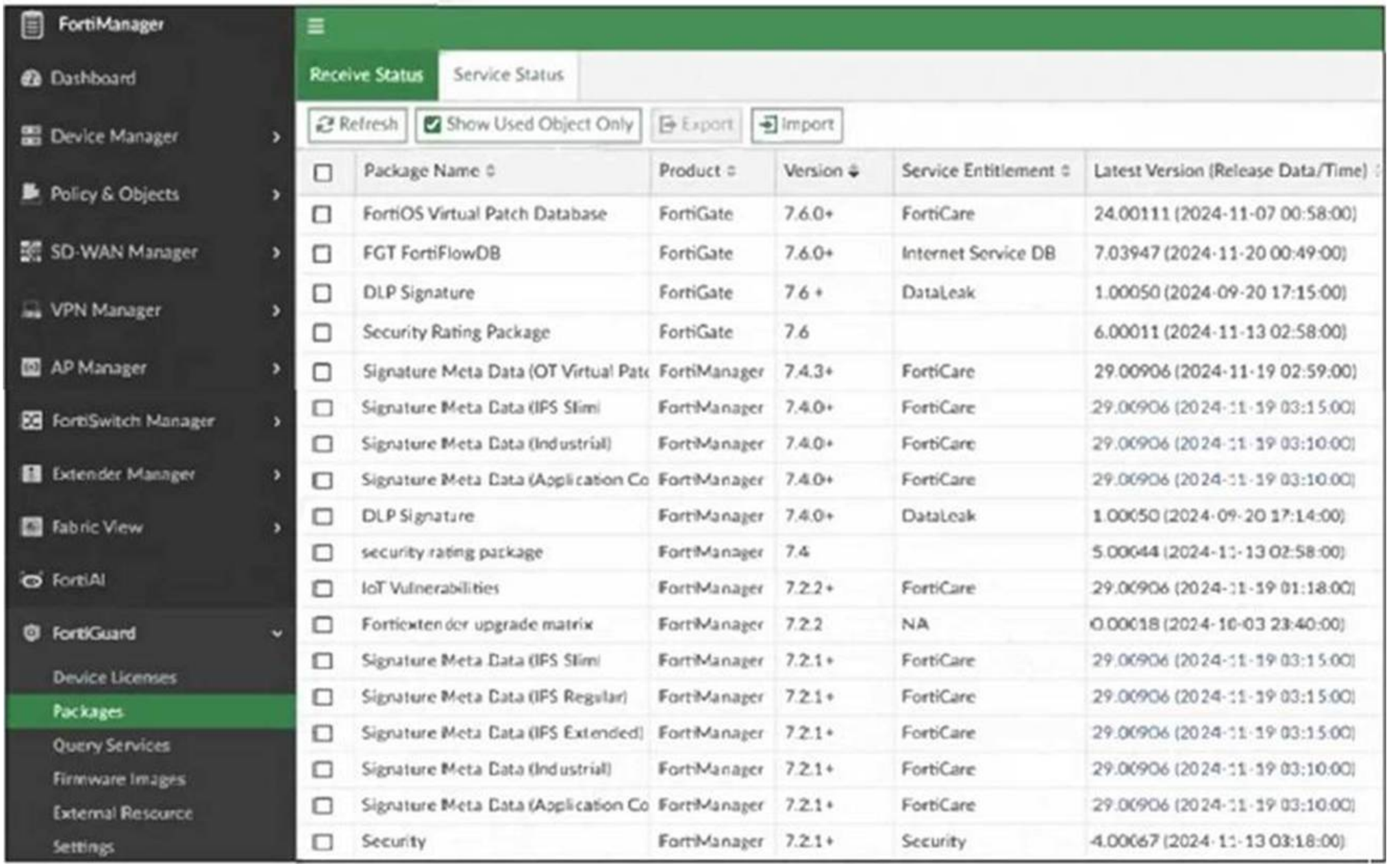
Answer: D

Explanation:
Running the script through the policy package or ADOM database method allows FortiManager to properly interpret object relationships and dependencies in the IPsec configuration, preventing object mismatch errors when pushing complex VPN settings directly via CLI.

NEW QUESTION 2
Refer to the exhibits
FortiGate GUI—FortiGuard



FortiManager GUI—FortiGuard



FortiGate CLI—Central management

```
HQ-NGFW-1 (central-management) # sh
config system central-management
    set type fortimanager
    set allow-push-firmware disable
    set allow-remote-firmware-upgrade disable
    set serial-number "FMG-VMTM24012945"
    set fmg "::ffff:10.0.13.120"
    config server-list
        edit 1
            set server-type update
            set server-address 192.168.1.120
        next
    end
    set include-default-servers disable
end
```

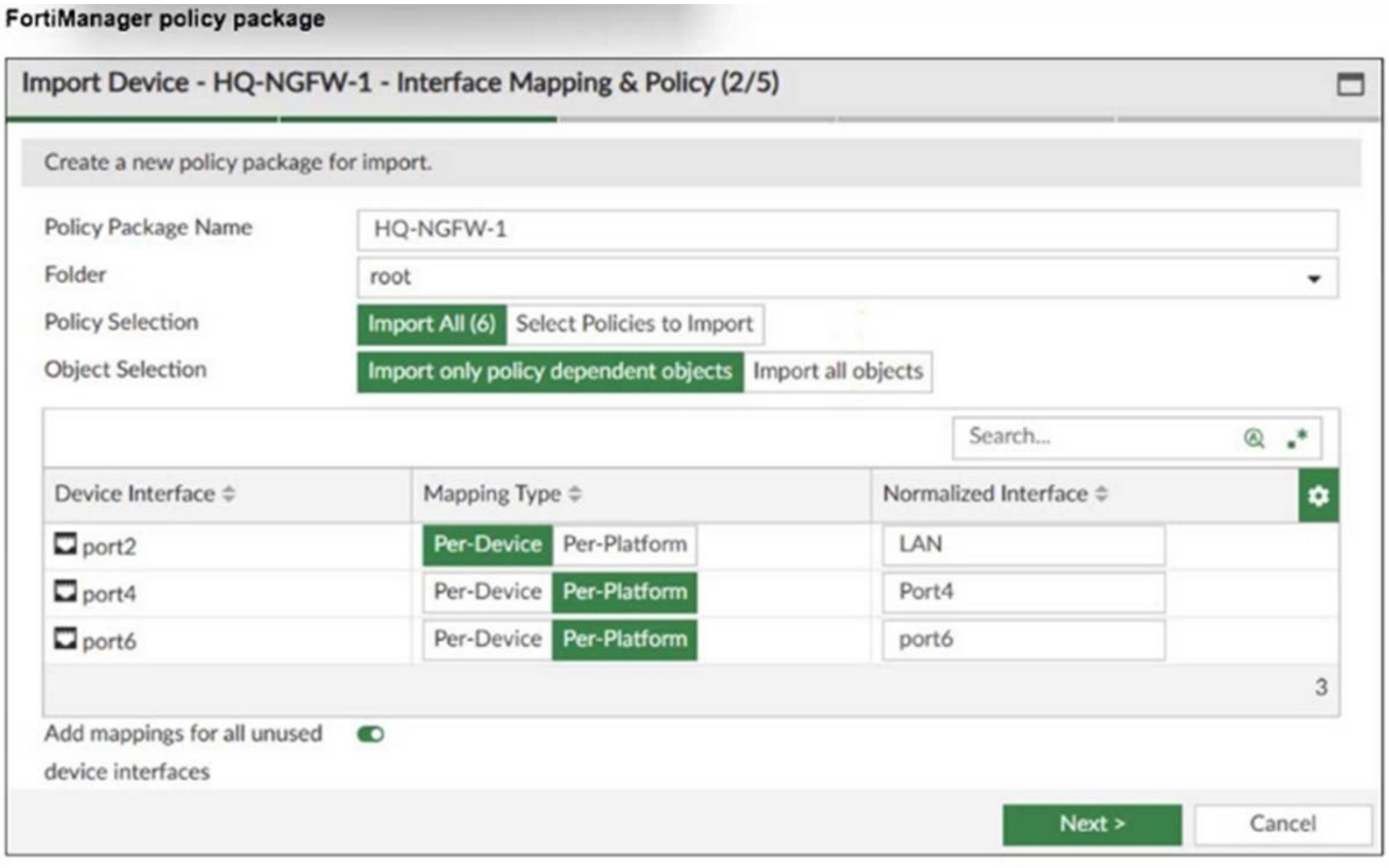
FortiGate HQ-NGFW-1 downloads and validates FortiGuard databases from FortiManager which acts as a local FortiGuard Distribution Server (FDS) in a closed network. An administrator pushes a new firewall policy with an intrusion prevention system (IPS) profile from FortiManager to FortiGate HQ- NGFW-1 However, FortiGate does not recognize the new IPS signature from FortiManager.
What is the most likely reason why FortiGate HQ-NGFW-1 does not recognize the new IPS signature?

A. FortiGate must enable rating for the FortiManager IP address, 192.168.1.120, in server list 1.
B. FortiManager and FortiGate have different IPS database versions.
C. The administrator must enable IPv6 connections for FortiGuard services on FortiManager.
D. The administrator must enable the fortiguard-anycast option to correctly download all signatures from the local FDS.

Answer: B

Explanation:
The most likely reason FortiGate HQ-NGFW-1 does not recognize the new IPS signature is that FortiManager and FortiGate have different IPS database versions. The FortiManager may have pushed a signature update that FortiGate has not yet synchronized or validated locally, causing the signature to be unrecognized.

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.

```
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.

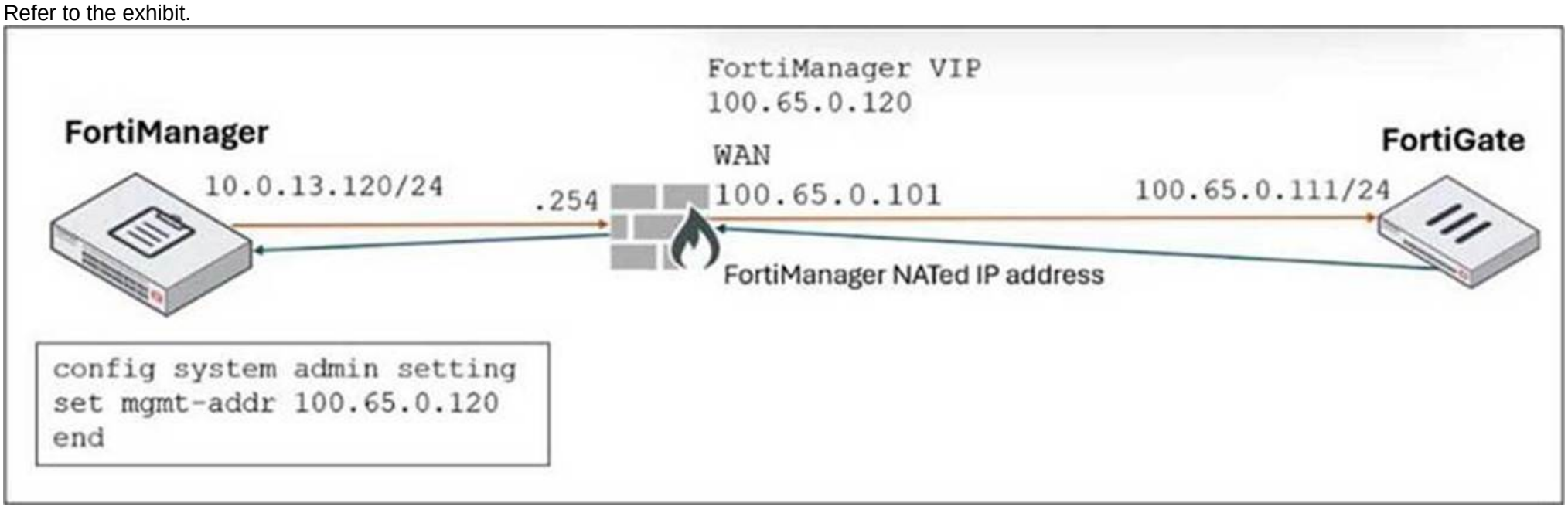
NEW QUESTION 6
An administrator is copying a system template profile between ADOMs by running the following command:
execute fmprofile export-profile ADOM 3547 /tmp/Backup_File
output dump to file: [/tmp/Backup_File]
Where does this command export the system template profile from?

A. FortiManager /tmp/Backup_File folder
B. FortiManager ADOM policy database
C. ADOM device database
D. FortiManager configuration backup file

Answer: B

Explanation:
The command exports the system template profile from the FortiManager ADOM policy database, which stores the configuration templates for devices within that ADOM.

NEW QUESTION 7
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 8
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.

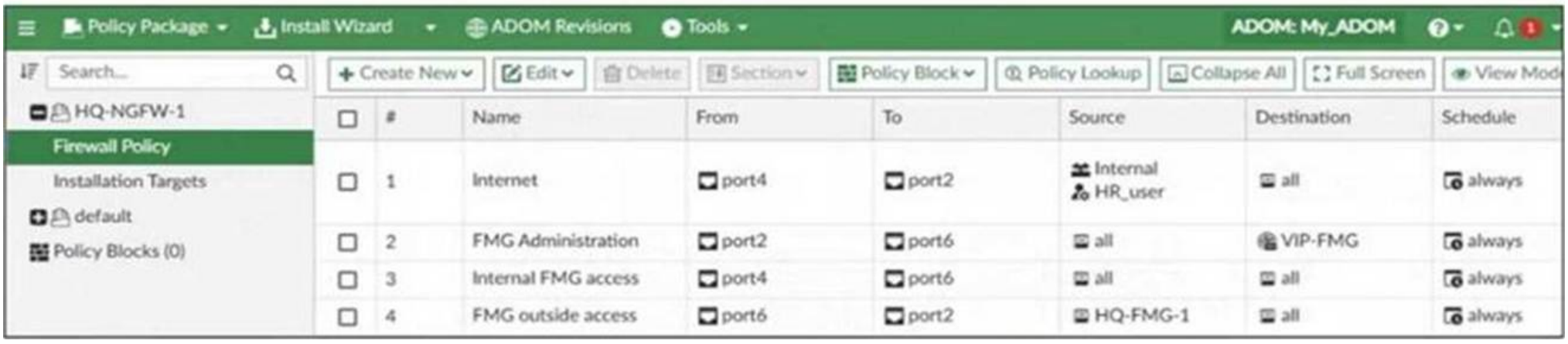
NEW QUESTION 9
After correcting a policy package configuration issue, you want to prevent administrators from repeating the mistake that caused the issue.
Which FortiManager approach best meets this need?

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.

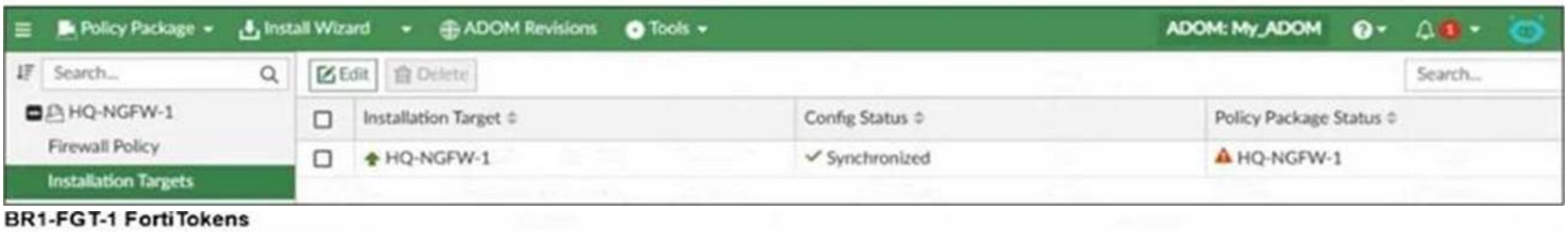
Answer: D

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.

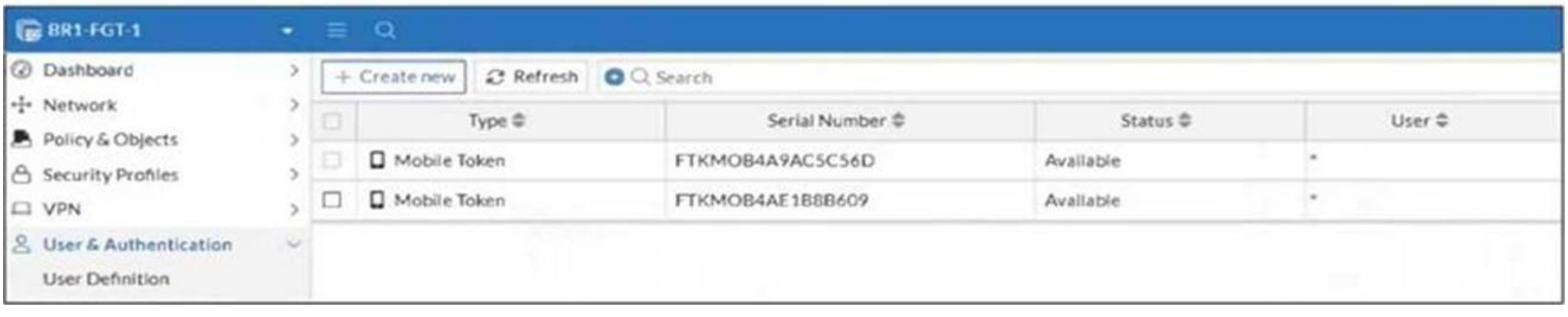
NEW QUESTION 10
Refer to the exhibits.
Firewall policies



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 10
.....

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