Fortinet

Exam Questions FCP_FMG_AD-7.6

FCP - FortiManager 7.6 Administrator

NEW QUESTION 1
Company policy dictates that any time a change is made to a policy package on FortiManager an ADOM revision is created before the change installed, and that revision is held for a minimum of 90 days.
Over the past three months, each installed change has resulted in several unused policies and duplicate objects. The FortiManager administrator plans to upgrade the FortiGate devices and then upgrade the FortiManager ADOM from version 7.4 to 7.6.
Which action can the administrator take to avoid slow ADOM upgrades?

A. Check and repair the global configuration database before upgrading.
B. Export firewall policies to Excel, delete them on the ADO
C. then reimport them after upgradingthe ADOM.
D. Find unused firmware templates, then delete them before upgrading.
E. Limit ADOM revisions before upgrading.

Answer: D

Explanation:
Limiting ADOM revisions reduces the number of stored historical configurations, which helps avoid performance degradation and slow ADOM upgrades caused by a large volume of revisions.

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.

```
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.

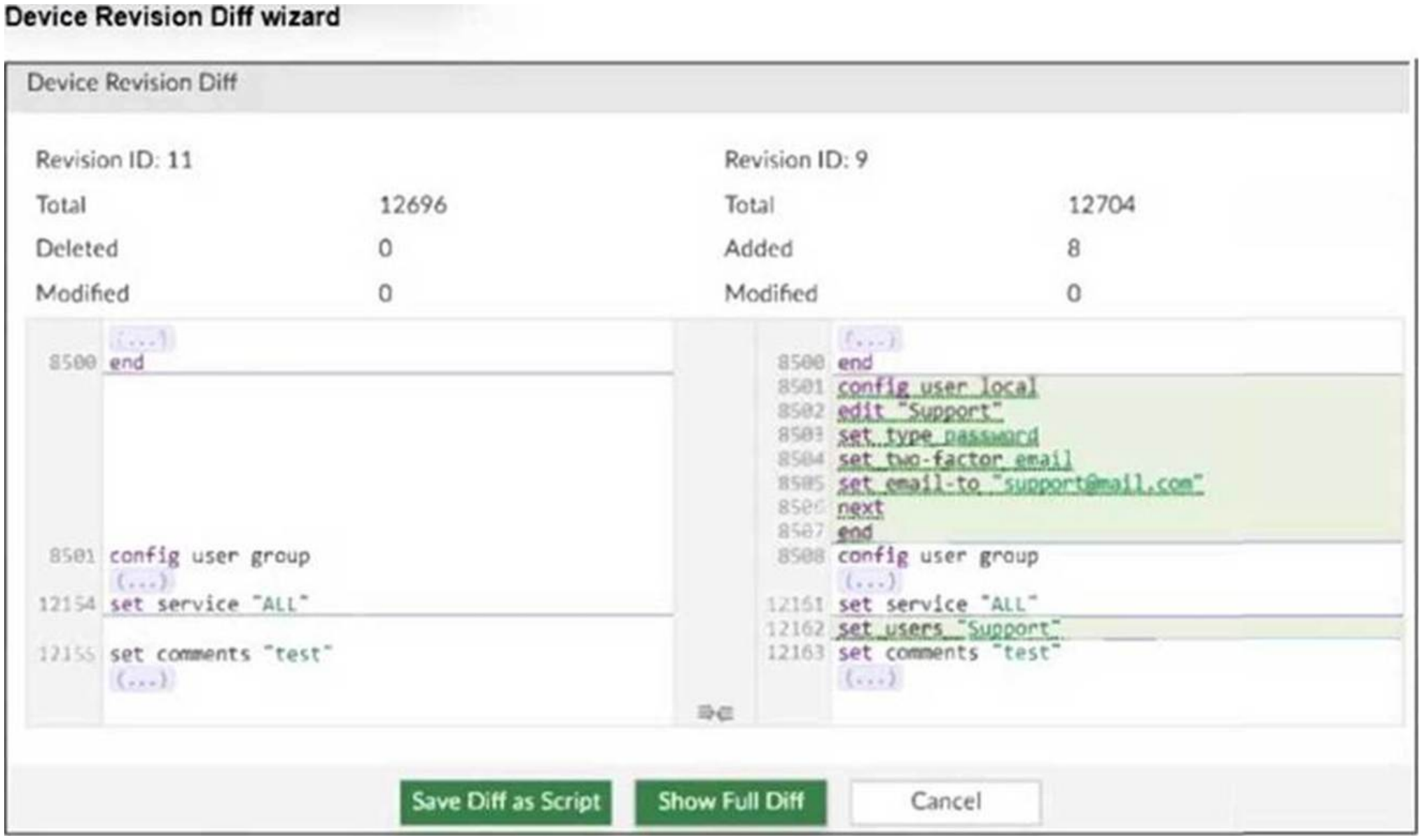
NEW QUESTION 4
What is the purpose of ADOM revisions?

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 5
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?

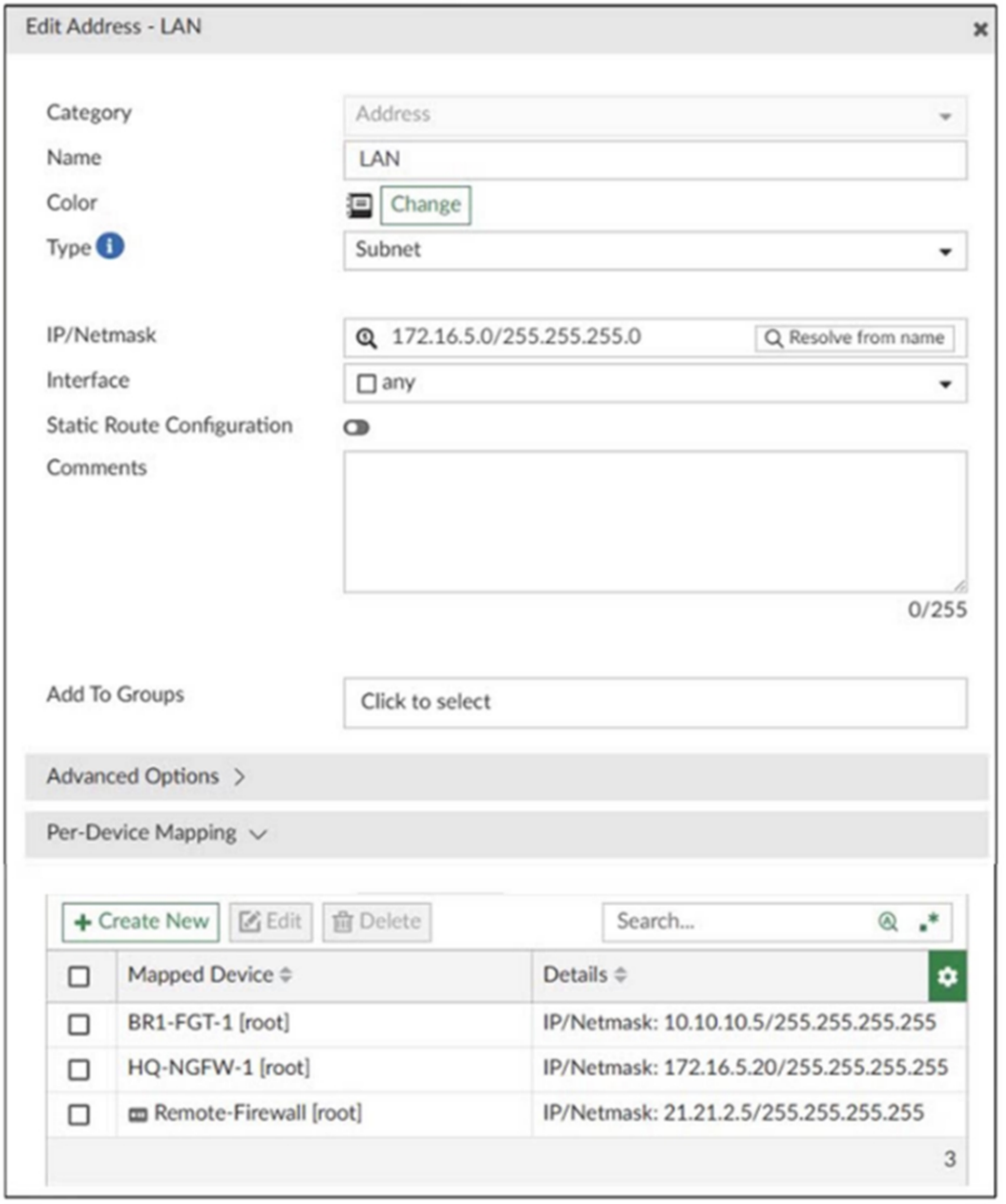
A. The administrator set the flag to 0 to prevent configuration overrides.
B. The administrator reinstalled the policy package.
C. The administrator needs to retrieve the device to correctly detect the FortiGate firmware version.
D. The administrator installed only the device-level configuration.

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 6
Refer to the exhibit.

FortiManager address object



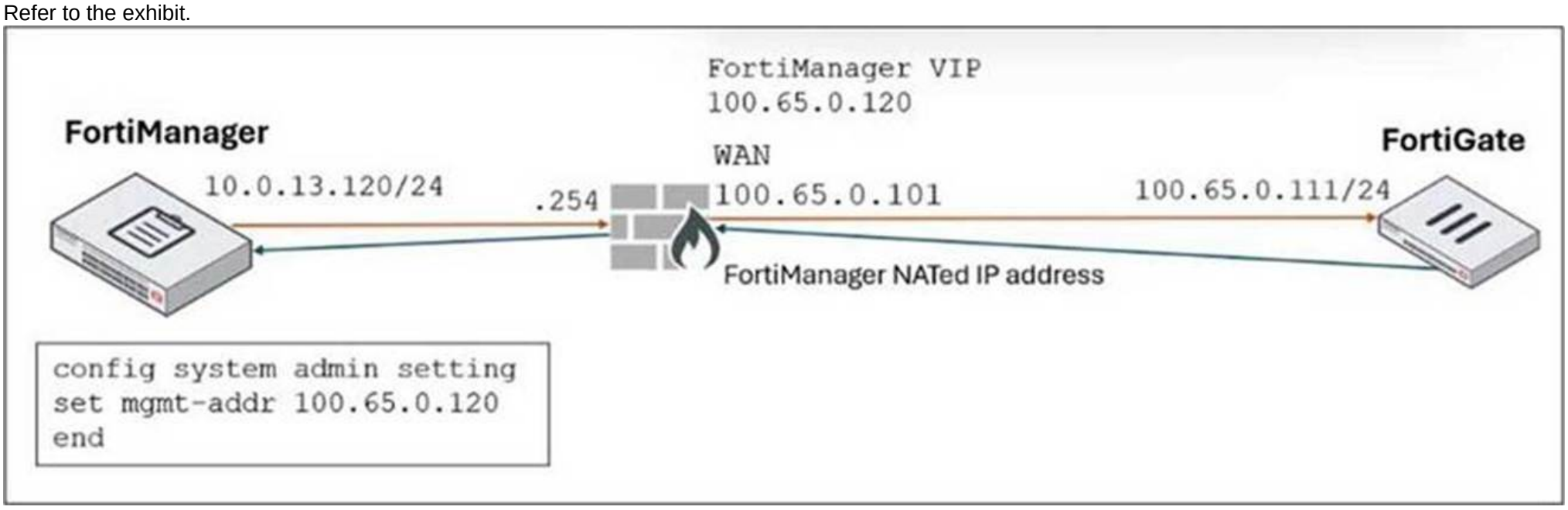
An administrator has created a firewall address object that is used in multiple policy packages for multiple FortiGate devices in an ADOM.
After the installation operation is performed, which IP/netmask will be installed on Remote-Firewall [VDOM1] for the LAN firewall address object?

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 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 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