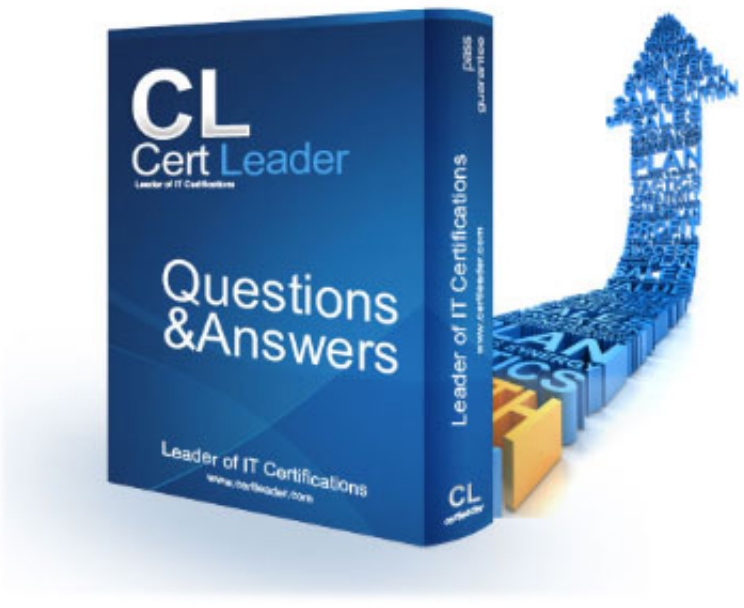
FCP_FMG_AD-7.6 Dumps

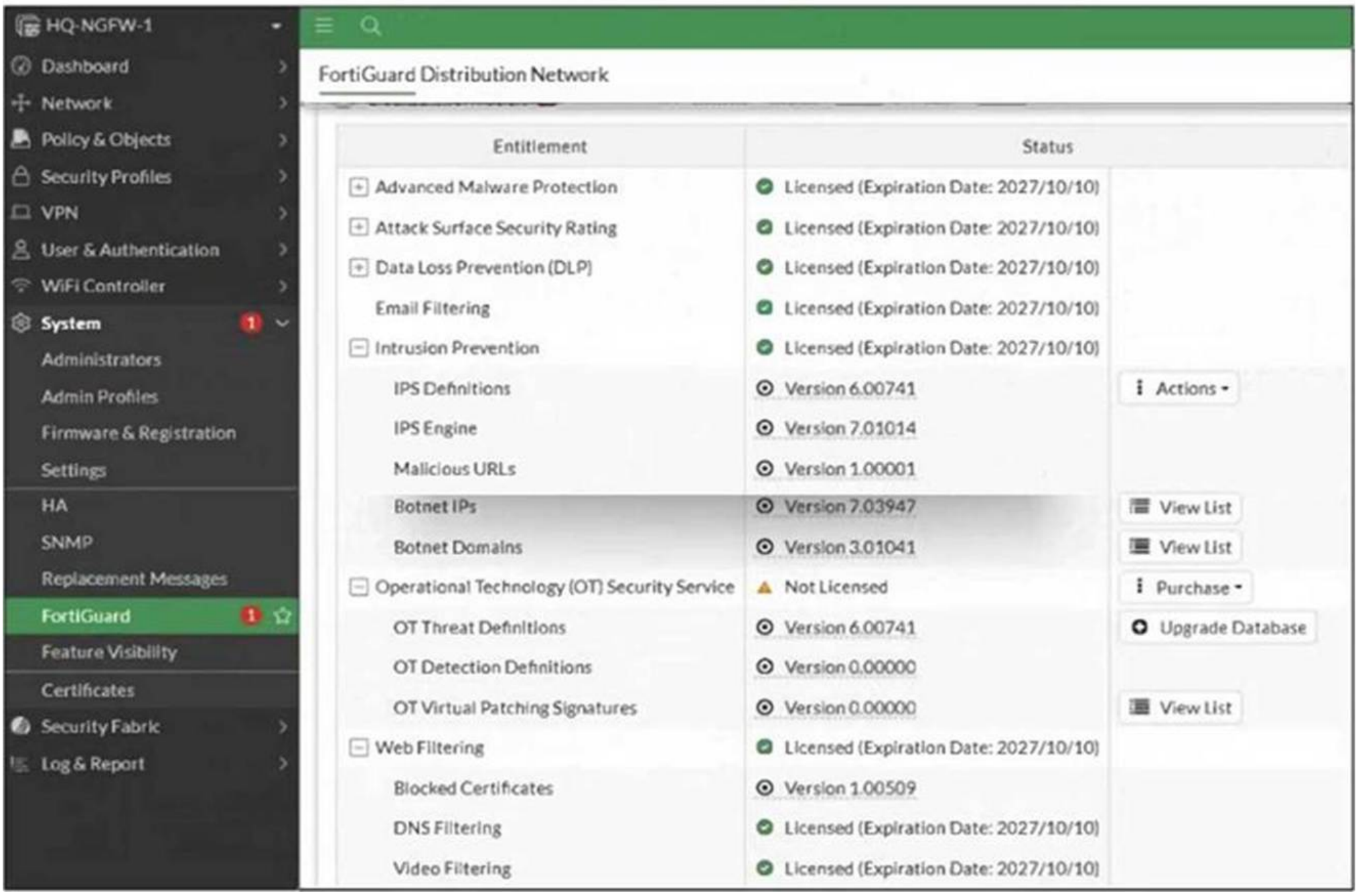
FCP - FortiManager 7.6 Administrator

https://www.certleader.com/FCP_FMG_AD-7.6-dumps.html

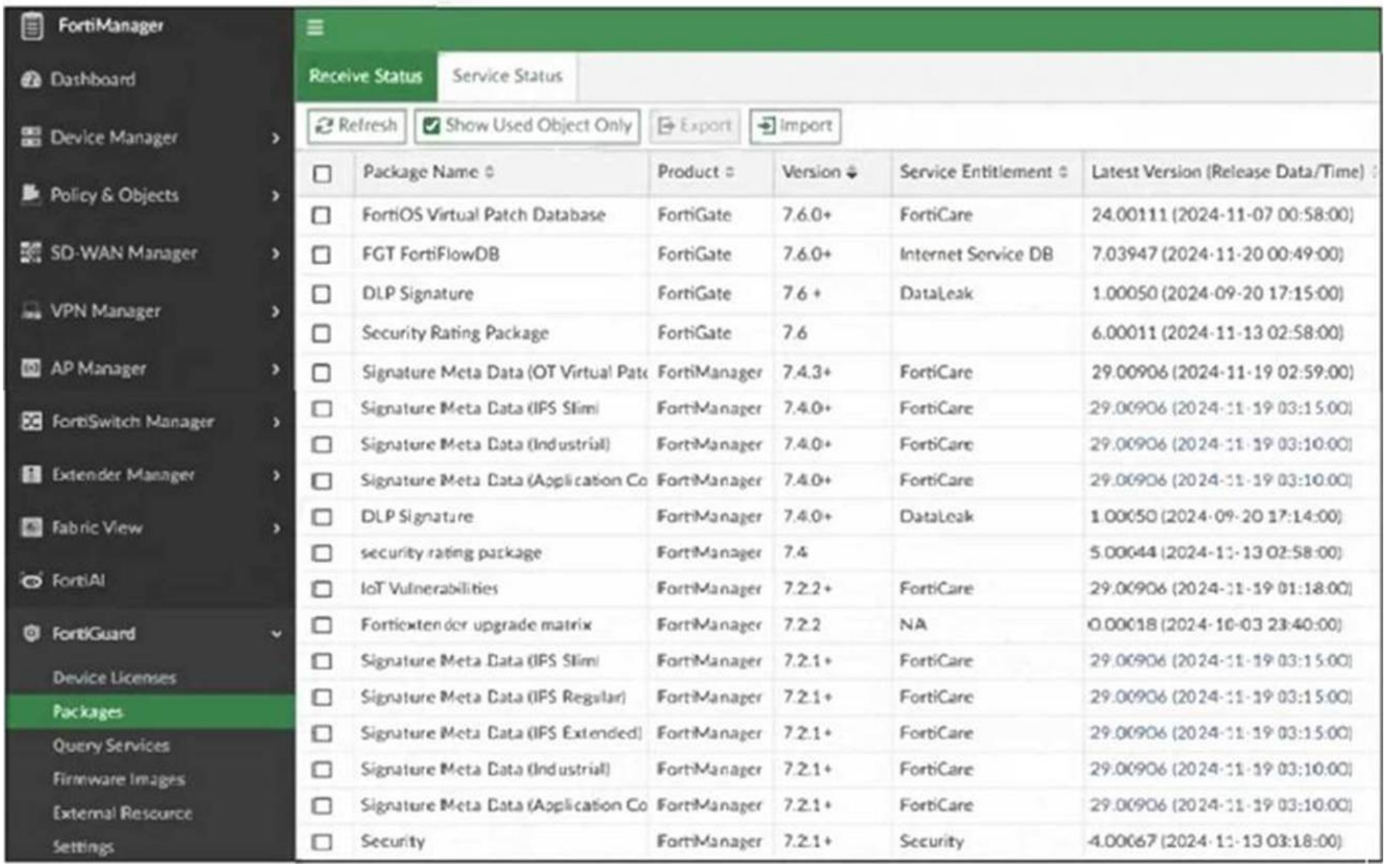


NEW QUESTION 1
Refer to the exhibits

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 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
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 4
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.

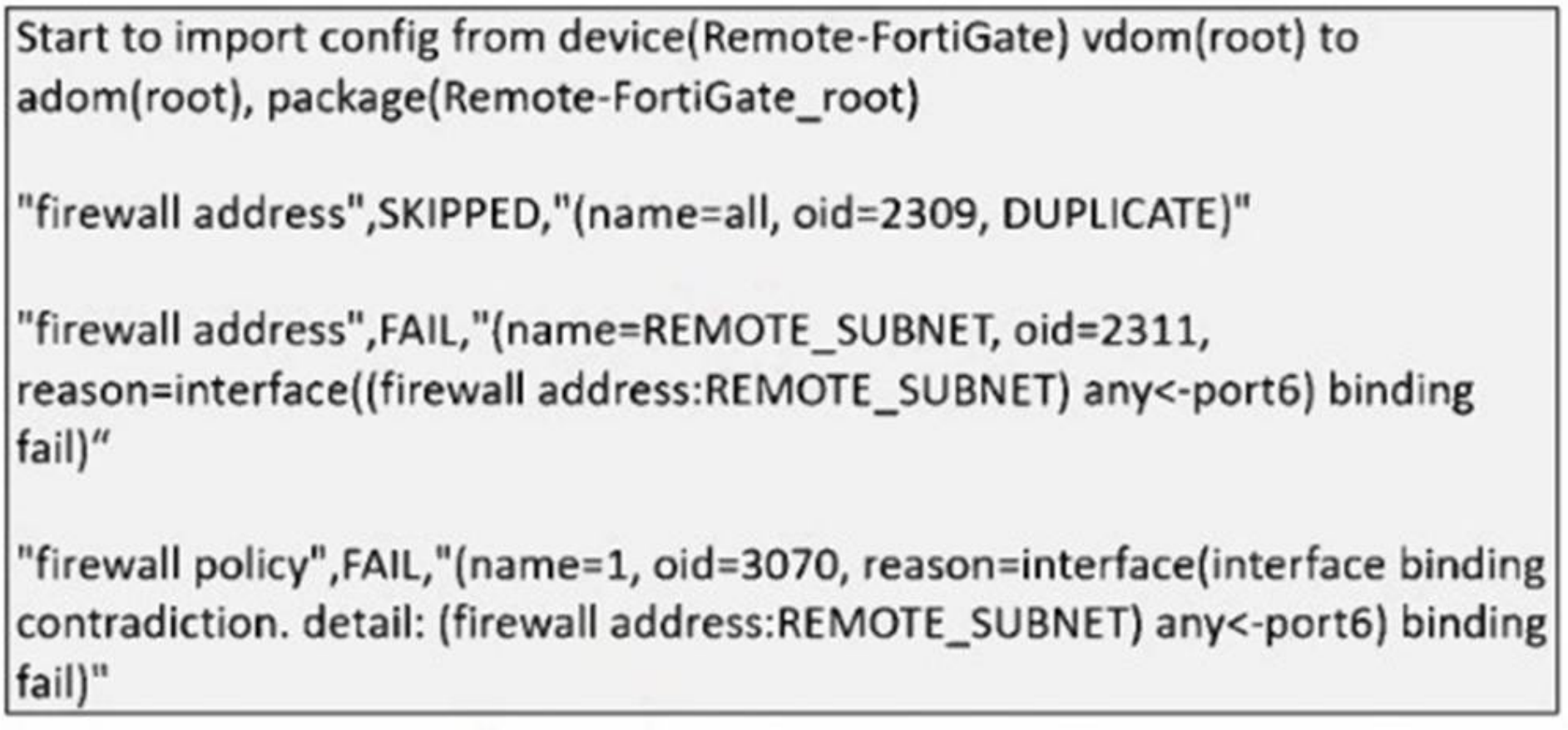
NEW QUESTION 5
You want to let multiple administrators work in the same ADOM without creating configuration conflicts.
What is the best and the most effective solution to apply?

A. Configure RADIUS authentication to assign ADOM roles to each user.
B. Enable workflow mode, which is the only way to prevent concurrent configuration conflicts.
C. Assign administrators with JSON API access to the FortiManager.
D. Activate workspace mode in the ADOM settings.

Answer: D

Explanation:
Activating workspace mode in the ADOM settings allows multiple administrators to work concurrently in the same ADOM by isolating their configuration changes in separate workspaces, preventing conflicts and enabling effective collaboration.

NEW QUESTION 6
Refer to the exhibit.



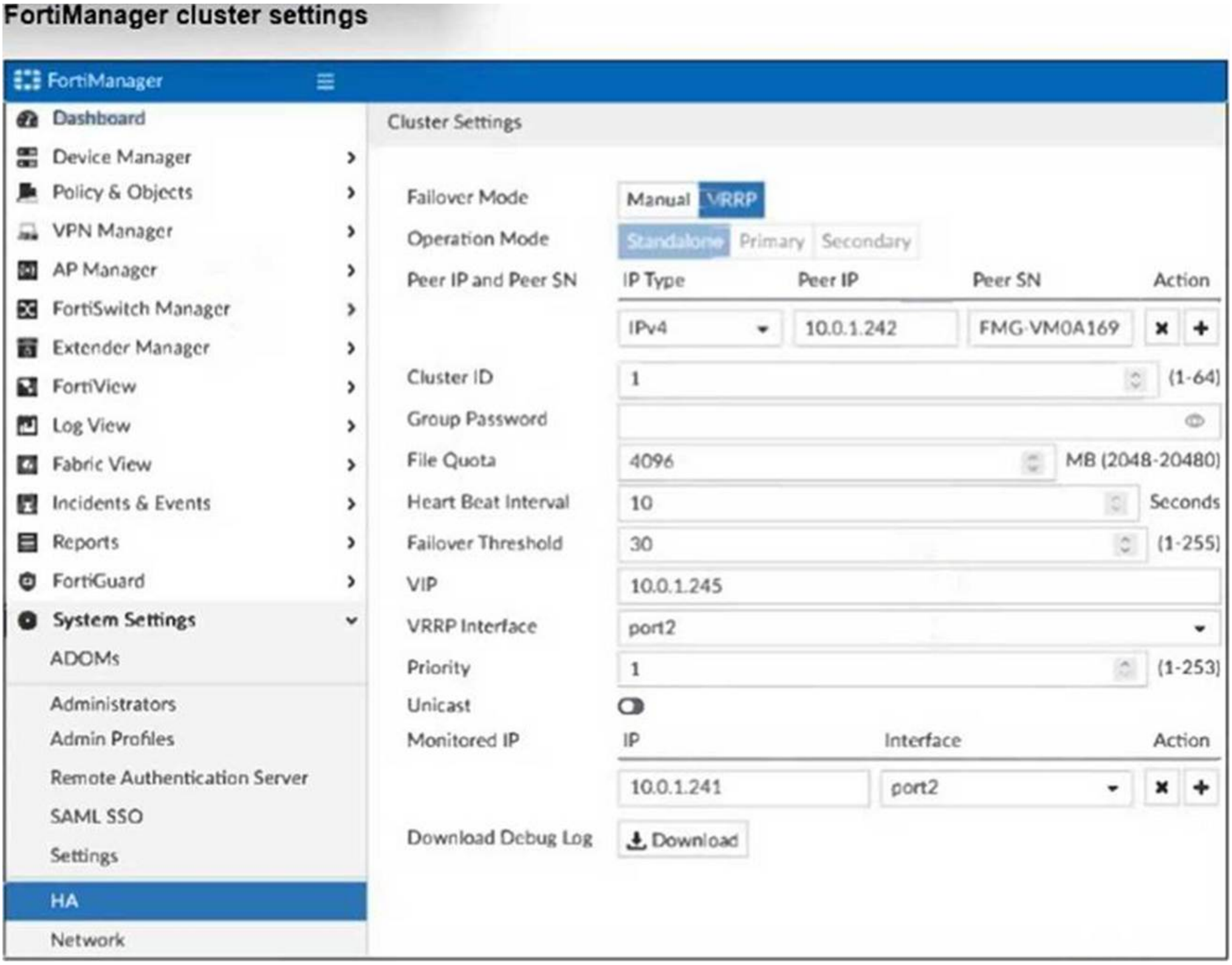
What can you conclude from the downloaded import report?

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 7
Refer to the exhibit.



If the monitored interface for the primary FortiManager device fails, what must you do to maintain high availability (HA)?

A. The FortiManager HAfailover is transparent to administrators and does not require any additional action.
B. Manually promote one of the working secondary devices to the primary role: and reboot the original primary device to remove the peer IP address of the failed device.
C. Reconfigure the primary device to remove the peer IP address of the failed device from its configuration.
D. Check the integrity database of the primary device to force a secondary device to become the new primary with all active interfaces.

Answer: A

Explanation:
In a FortiManager HA cluster configured with VRRP failover, the failover process is automatic and transparent to administrators. If the monitored interface on the primary device fails, the secondary device takes over without requiring manual intervention to maintain HA.

NEW QUESTION 8
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 9
Push updates are failing on a FortiGate device located behind a network address translation (NAT) device? Which two settings should the administrator check to correct this problem? (Choose two.)

A. Make sure the NAT device IP address and the correct ports are configured on FortiManager.
B. Make sure FortiGuard updates and web service are enabled on the FortiGuard service interface.
C. Make sure the virtual IP address and the correct ports are configured on the NAT device.

D. Make sure the Bind to IP address option on the FortiGuard service interface is set to the virtual IP address from the NAT device.

Answer: AC

Explanation:
FortiManager must have the NAT device's IP address and correct ports configured to communicate properly with the FortiGate behind NAT.
The NAT device must have the correct virtual IP address and ports configured to allow push updates to reach the FortiGate device.

NEW QUESTION 10
Refer to the exhibit.

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

What are two results from the configuration shown in the exhibit? (Choose two.)

A. Ungraceful closed sessions will keep the ADOM in a locked state until the administrator session times out.
B. The administrator can lock policy blocks and FortiManager global ADOM.
C. The same administrator can lock more than one ADOM at the same time.
D. The administrator must have access to the ADOM to approve changes.

Answer: AB

Explanation:
In normal workspace mode, ungraceful session closures will keep the ADOM locked until the session times out, preventing other administrators from editing.
Normal workspace mode allows administrators to lock policy blocks and the global ADOM, providing granular locking control.

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
```

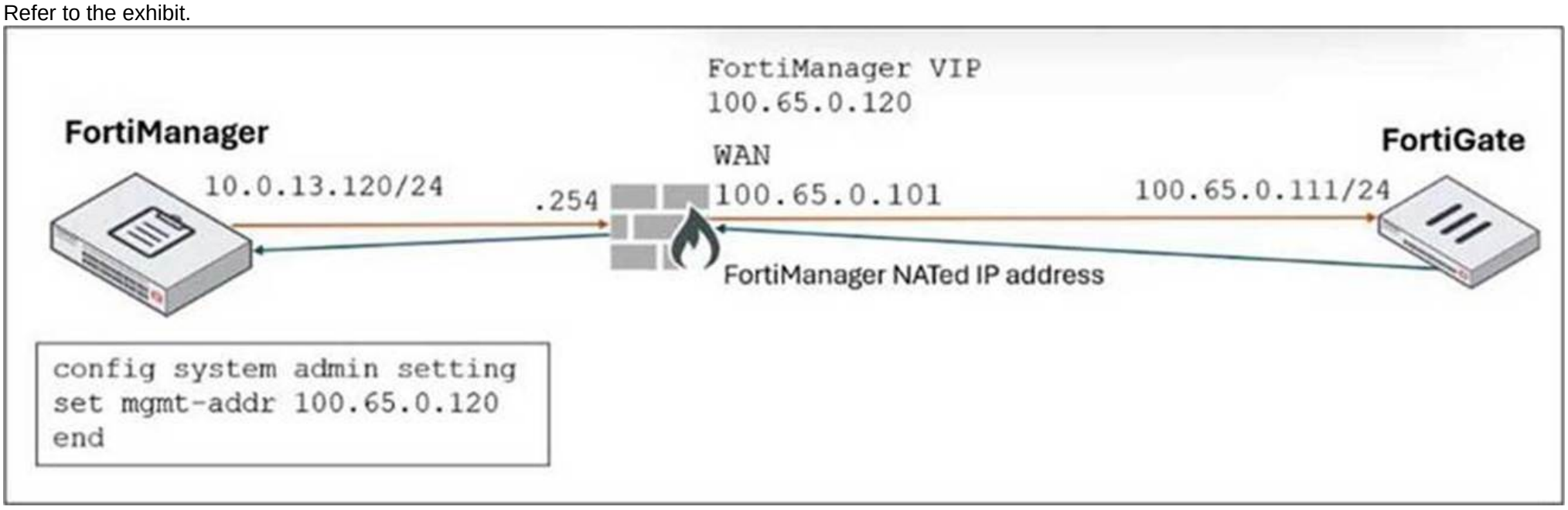
A. Option A

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 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
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 20
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCP_FMG_AD-7.6 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FMG_AD-7.6-dumps.html