

Exam Questions FCP_FMG_AD-7.6

FCP - FortiManager 7.6 Administrator

https://www.2passeasy.com/dumps/FCP_FMG_AD-7.6/



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

Refer to the exhibit.

FortiManager policy package

Import Device - HQ-NGFW-1 - Interface Mapping & Policy (2/5)

Create a new policy package for import.

Policy Package Name

HQ-NGFW-1

Folder

root

Policy Selection

Import All (6)

Select Policies to Import

Object Selection

Import only policy dependent objects

Import all objects

Search...

Device Interface	Mapping Type	Normalized Interface
☒ port2	Per-Device Per-Platform	LAN
☒ port4	Per-Device Per-Platform	Port4
☒ port6	Per-Device Per-Platform	port6

3

Add mappings for all unused device interfaces

Next >

Cancel

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 3

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

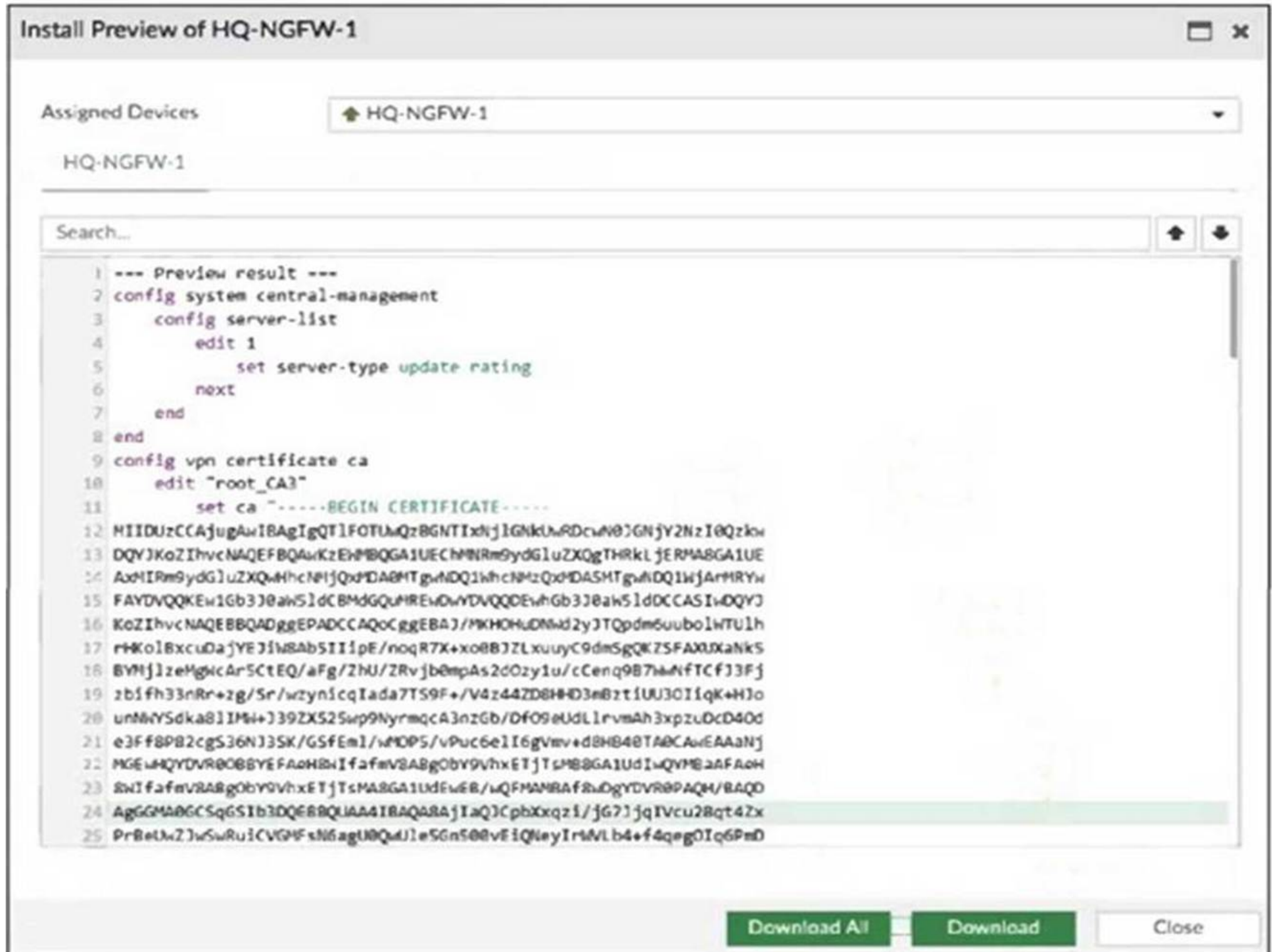
Explanation:

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 4

Refer to the exhibit.

FortiManager—HQ-NGFW-1 install preview



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 5

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 6

While attempting to push a NetFlow configuration script through the FortiManager policy package: an administrator encounters an error stating that an object is unrecognized in line 4.

```
Starting log (Run on database)
config vdom
edit AGEUSR
[line 4] > config sys interface [parameter(s) invalid. detail: object unrecognized]
Failed to commit to DB, reason([line 4] > config sys interface [parameter(s) invalid. detail: object unrecognized])
```

Running script(NetFlow_Configuration) on DB failed

What must the administrator do to successfully apply the NetFlow configuration script and avoid the object unrecognized error?

- A. Make sure the user running the script has full access to the VDOM—AGEUSR.
- B. Run the script on the device database.
- C. Use metadata variables if they use VDOMs in the script.
- D. Create a normalized interface on the policy layer before running the script.

Answer: C

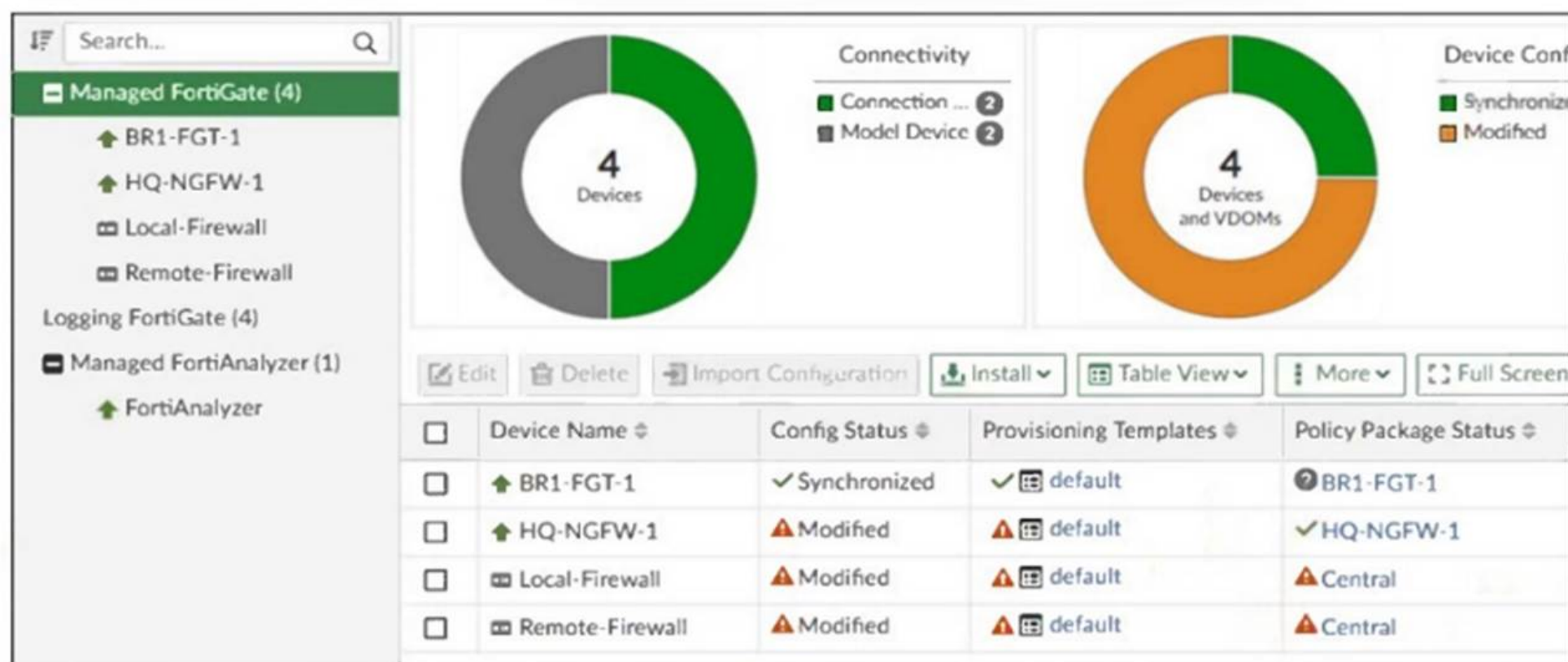
Explanation:

When using scripts that reference VDOM-specific objects, such as interfaces, in FortiManager, metadata variables must be used to correctly map those objects per VDOM. This prevents "object unrecognized" errors during script execution.

NEW QUESTION 7

Refer to the exhibits.

FortiManager device database



Installation Targets Central policy package

Installation Target	Config Status	Policy Package Status
BR1-FGT-1	✓ Synchronized	BR1-FGT-1
Local-Firewall	⚠ Unknown	⚠ Central
Remote-Firewall	⚠ Unknown	⚠ Central

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 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.

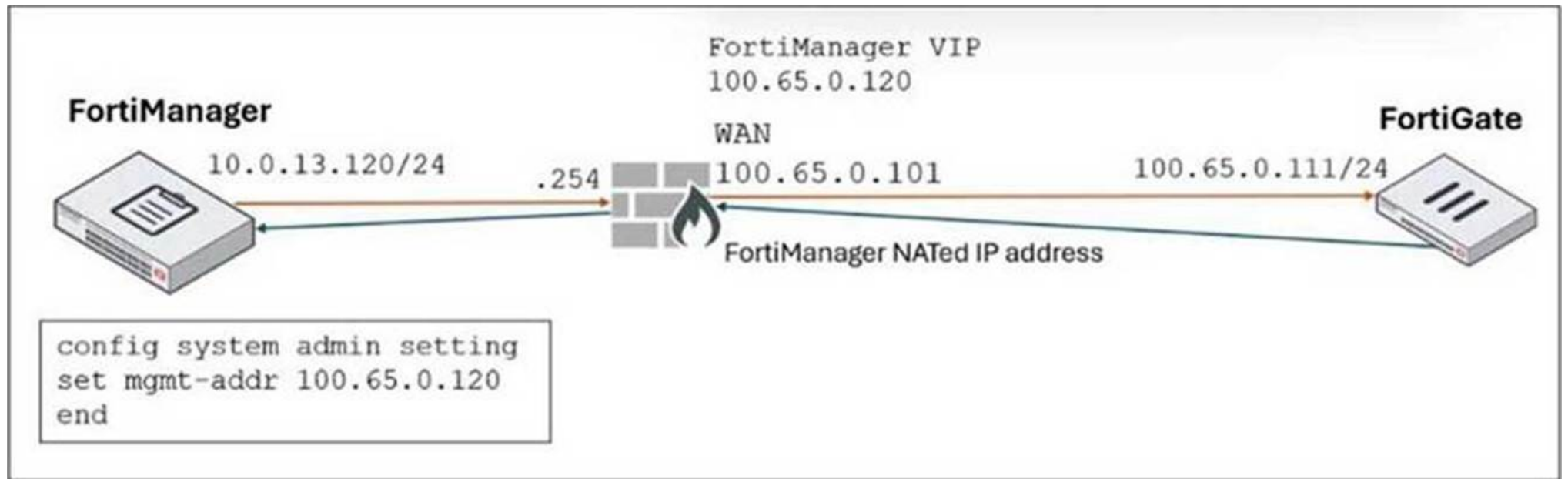
Answer: D

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

Refer to the exhibits.

Firewall policies

Policy Package

Install Wizard

ADOM Revisions

Tools

ADOM: My_ADOM

Search...

+ Create New

Edit

Delete

Section

Policy Block

Policy Lookup

Collapse All

Full Screen

View Mode

HQ-NGFW-1

Firewall Policy

Installation Targets

default

Policy Blocks (0)

	#	Name	From	To	Source	Destination	Schedule
☐	1	Internet	port4	port2	Internal HR_user	all	always
☐	2	FMG Administration	port2	port6	all	VIP-FMG	always
☐	3	Internal FMG access	port4	port6	all	all	always
☐	4	FMG outside access	port6	port2	HQ-FMG-1	all	always

Installation target

ADOM: My_ADOM			
Search...	Edit	Delete	Search...
HQ-NGFW-1	Installation Target	Config Status	Policy Package Status
Firewall Policy			
Installation Targets	HQ-NGFW-1	✓ Synchronized	⚠ HQ-NGFW-1

BR1-FGT-1 FortiTokens

BR1-FGT-1				
Dashboard	+ Create new Refresh Search			
Network				
Policy & Objects				
Security Profiles				
VPN				
User & Authentication				
User Definition				
	Type	Serial Number	Status	User
	Mobile Token	FTKMOB4A9AC5C56D	Available	*
	Mobile Token	FTKMOB4AE1B8B609	Available	*

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 (FTKMOB4A9AC5C56D) 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

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FMG_AD-7.6 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FMG_AD-7.6 Product From:

https://www.2passeasy.com/dumps/FCP_FMG_AD-7.6/

Money Back Guarantee

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