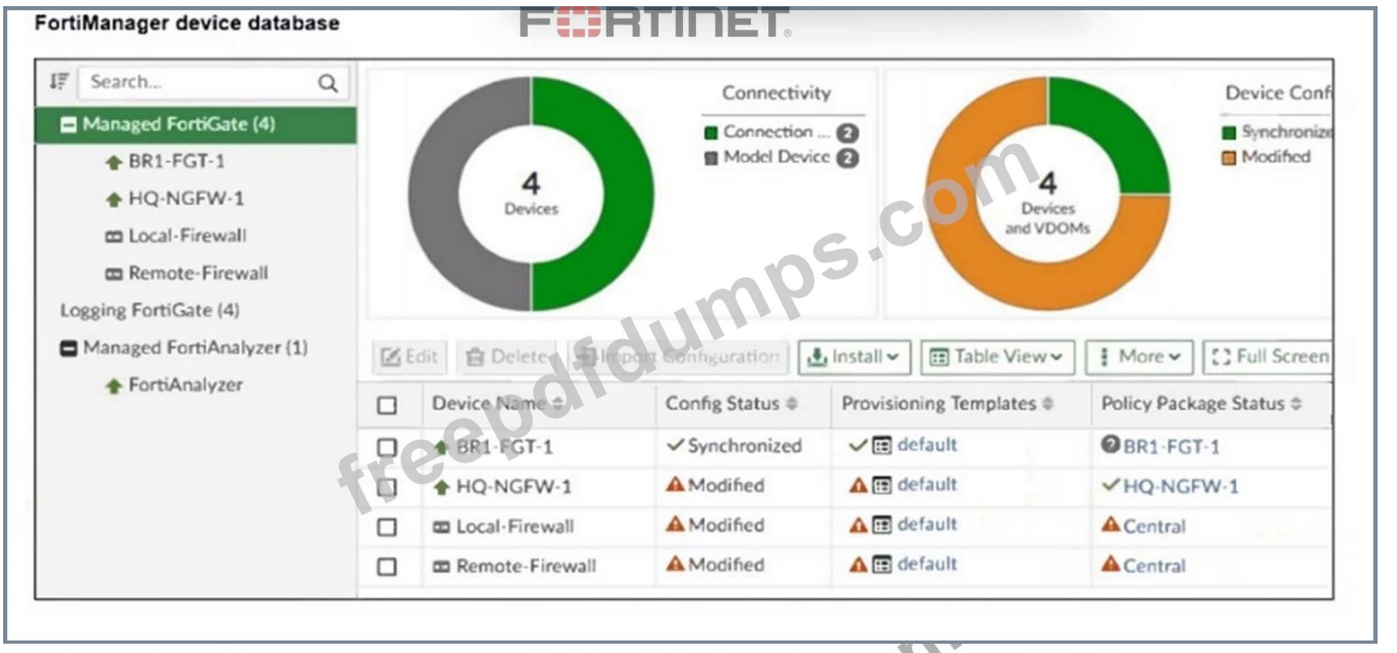
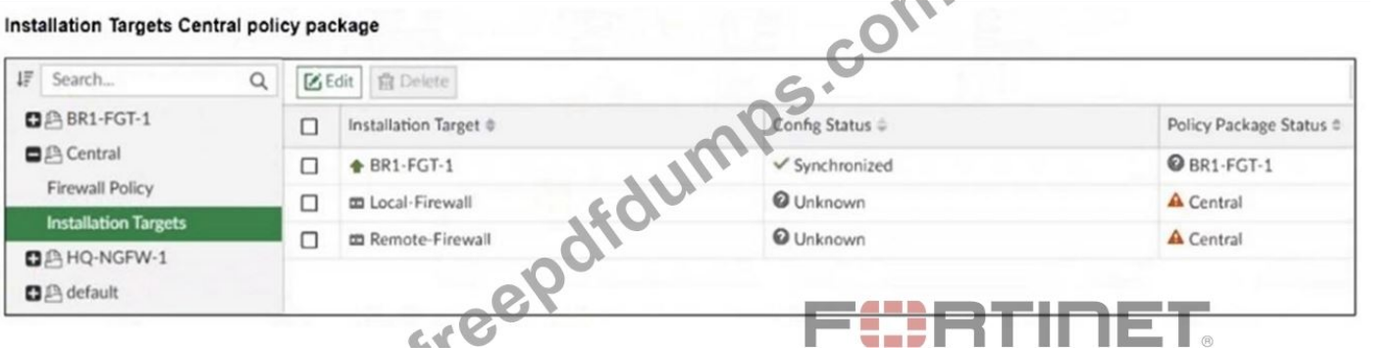
Fortinet.FCP_FMG_AD-7.6.v2026-04-01.q32

Exam Code:	FCP_FMG_AD-7.6
Exam Name:	FCP - FortiManager 7.6 Administrator
Certification Provider:	Fortinet
Free Question Number:	32
Version:	v2026-04-01
# of views:	140
# of Questions views:	320
https://www.freepdfdumps.com/Fortinet.FCP_FMG_AD-7.6.v2026-04-01.q32.html	

NEW QUESTION: 1
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: A,C (LEAVE A REPLY)
What if FortiManager is behind a NAT device?
If FortiManager is behind a NAT device, sending its IP address for push updates causes push updates to fail because this is a non-routable IP address from the FDN. You must configure the following:
* On FortiManager, configure the NAT device IP address and port used for push updates.
* On the NAT device, configure the virtual IP and port that forwards to FortiManager.device.

NEW QUESTION: 2
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: (SHOW ANSWER)

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: 3

Refer to the exhibit. How does FortiManager get antivirus and IPS updates?

```
FortiManager # diagnose fmupdate view-serverlist fds
Fortiguard Server Comm : Enabled
Server Override Mode   : Strict
FDS server list        :
Index   Address                     Port         TimeZone       Distance        Source
-------------------------------------------------------------------------------------
*0      10.0.1.50                   8890         -5             0               CLI
 1      96.45.33.89                 443          -5             0               FDNI
 2      96.45.32.81                 443          -5             0               FDNI
 ...
 9      fds1.fortinet.com           443          -5             0               DEFAULT
```


A. It uses all URLs in the list that contain the fds host name.

B. It gets updates from the server with IP address 10.0.1.50.

C. It connects to all servers marked as FortiGuard Distribution Network through Internet (FDNI) sources.

D. It connects to the public FortiGuard servers listed in the configuration.

Answer: B (LEAVE A REPLY)

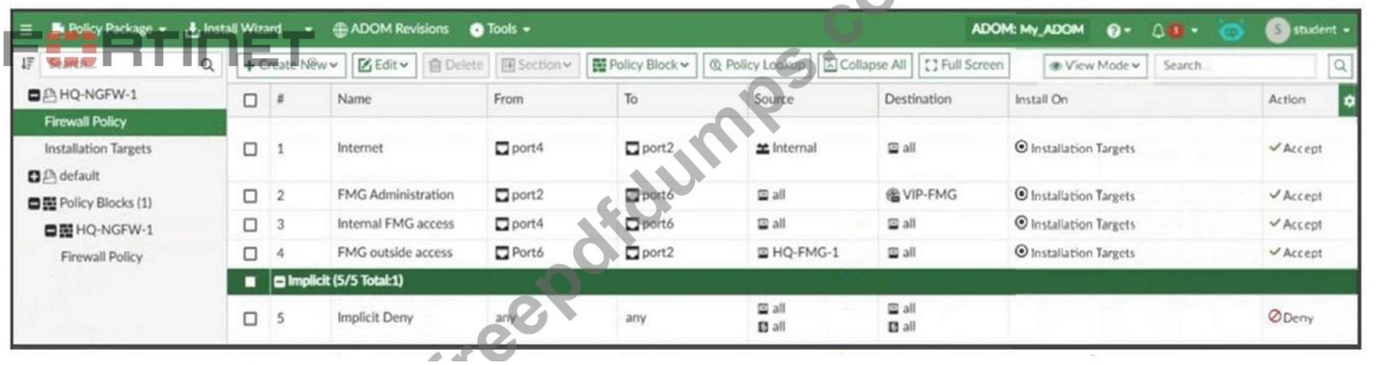
The output shows that Server Override Mode is set to Strict, and the server at index 0 (IP 10.0.1.50, port 8890) is marked with an asterisk *, indicating it is the active FortiGuard server. Since it was configured via CLI and is at the top of the list, FortiManager will exclusively use this server for antivirus and IPS updates.

NEW QUESTION: 4

Refer to the exhibits. An administrator ran the Install Wizard and selected to install both the policy package and device settings.

Why can the administrator not install the policy package on HQ-NGFW-1?

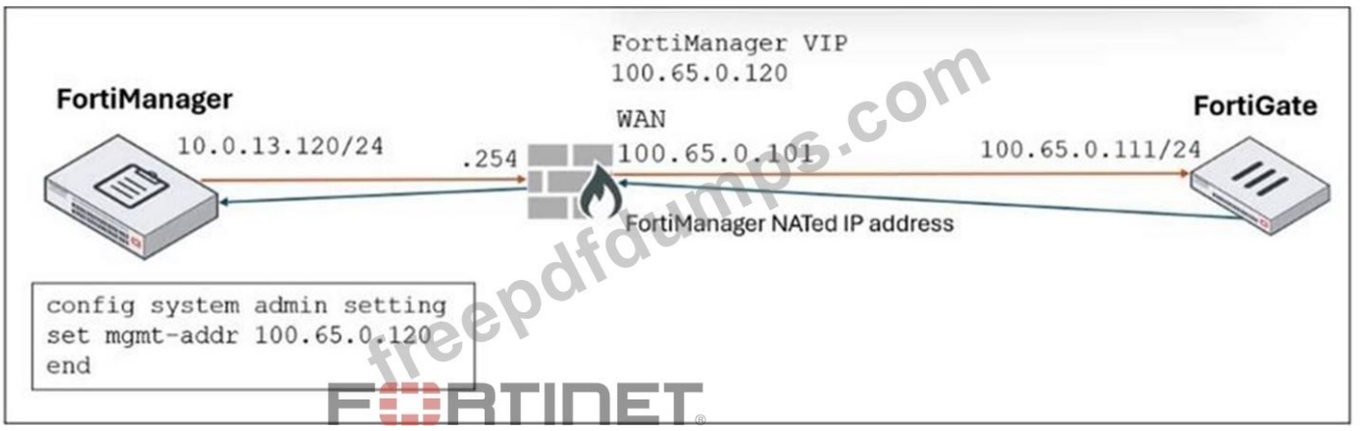
Firewall policy package



A. The administrator must change the Install on column from Installation Targets to HQ-NGFW-1.
B. The administrator must replace the interface Port6 with port6.
C. The administrator must use the admin user to install the policy package.
D. The administrator must remove the policy block assigned to HQ-NFFW-1.
Answer: (SHOW ANSWER)
Policy 4 has "Port6" in "From". The "P" in Port6 makes it a different interface. No the same than "port6" with "p".

NEW QUESTION: 5
What are two expected results when both FortiManager and FortiGate are behind network address translation (NAT) devices? (Choose two.)
A. During discovery, the FortiManager NATed IP address is not set by default on FortiGate.
B. FortiGate is discovered by FortiManager through the FortiGate NATed IP address.
C. If the FortiGate-FortiManager communication protocol (FGFM) tunnel is torn down, FortiManager will try to reestablish the FGFM tunnel.
D. FortiGate can announce itself to FortiManager only if the FortiManager non-NATed IP address is configured on FortiGate under central management.
Answer: (SHOW ANSWER)
When both FortiManager and FortiGate are behind NAT, the NATed IP address of FortiManager is not automatically set on the FortiGate during discovery. It must be configured manually if needed.
If the FGFM (FortiGate-FortiManager) tunnel is torn down due to network interruption or NAT timeout, FortiManager will attempt to reestablish the tunnel as part of its default behavior.

NEW QUESTION: 6
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: (SHOW ANSWER)

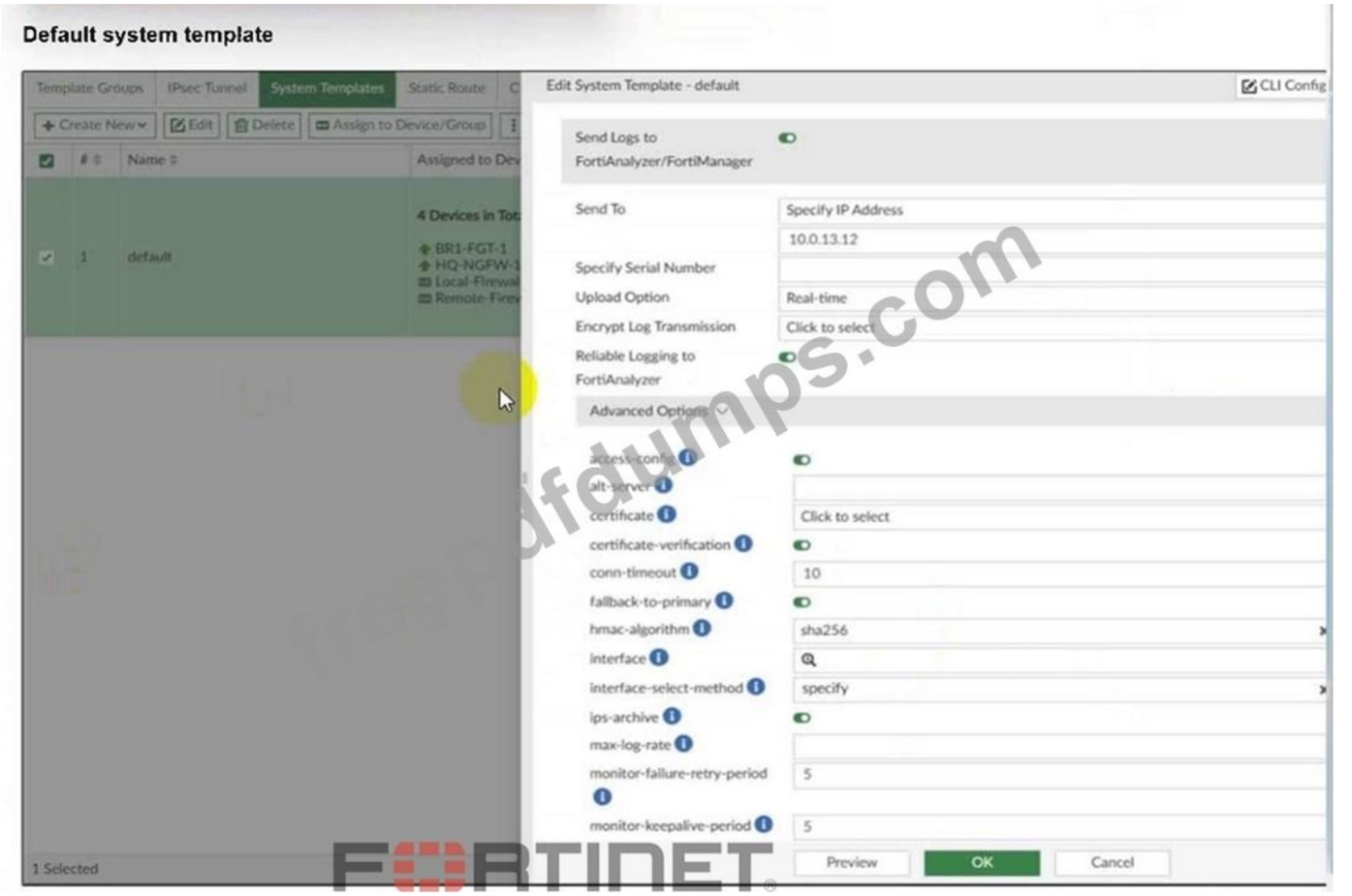
When FortiManager is behind a NAT device, setting the NATed IP address (100.65.0.120) in the system admin settings causes FortiManager to use that NATed IP address for communication and configuration with FortiGate during discovery and management operations.

NEW QUESTION: 7

Refer to the exhibit. An administrator has assigned the default system template to install all devices with the FortiAnalyzer IP address 10.0.13.12.

However, not all FortiGate devices can reach FortiAnalyzer using the default interface. Some devices may use the LAN interface, while others may use the WAN interface.

How can the administrator change the source interface for FortiGate devices using the default system template?



A. Use per-device dynamic object configurations at the ADOM level and apply them in the template.

B. Configure a metadata variable at the ADOM level and use it in the template.

C. Create a different system template for each FortiGate, if the configuration is different.

D. Create a meta field on FortiManager system settings of type Device and use it in the template.

Answer: B (LEAVE A REPLY)

Since the field "interface" has the magnifying glass icon, it means that you can use a metadata variable calling it the "$" symbol.

NEW QUESTION: 8

Refer to the exhibit. 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: (SHOW ANSWER)

If an administrator locks an ADOM (checks it out) and then closes their session ungracefully (e.g., browser crash, network disconnect) without explicitly checking the configuration back in, the ADOM remains in a locked state. FortiManager relies on the configured session timeout to automatically release the lock. This prevents other administrators from editing the configuration until the lock expires.

The lock is applied on a per-ADOM basis. A single administrator can log into FortiManager and check out (lock) multiple different ADOMs simultaneously, provided those ADOMs are not currently locked by another administrator.

NEW QUESTION: 9

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.

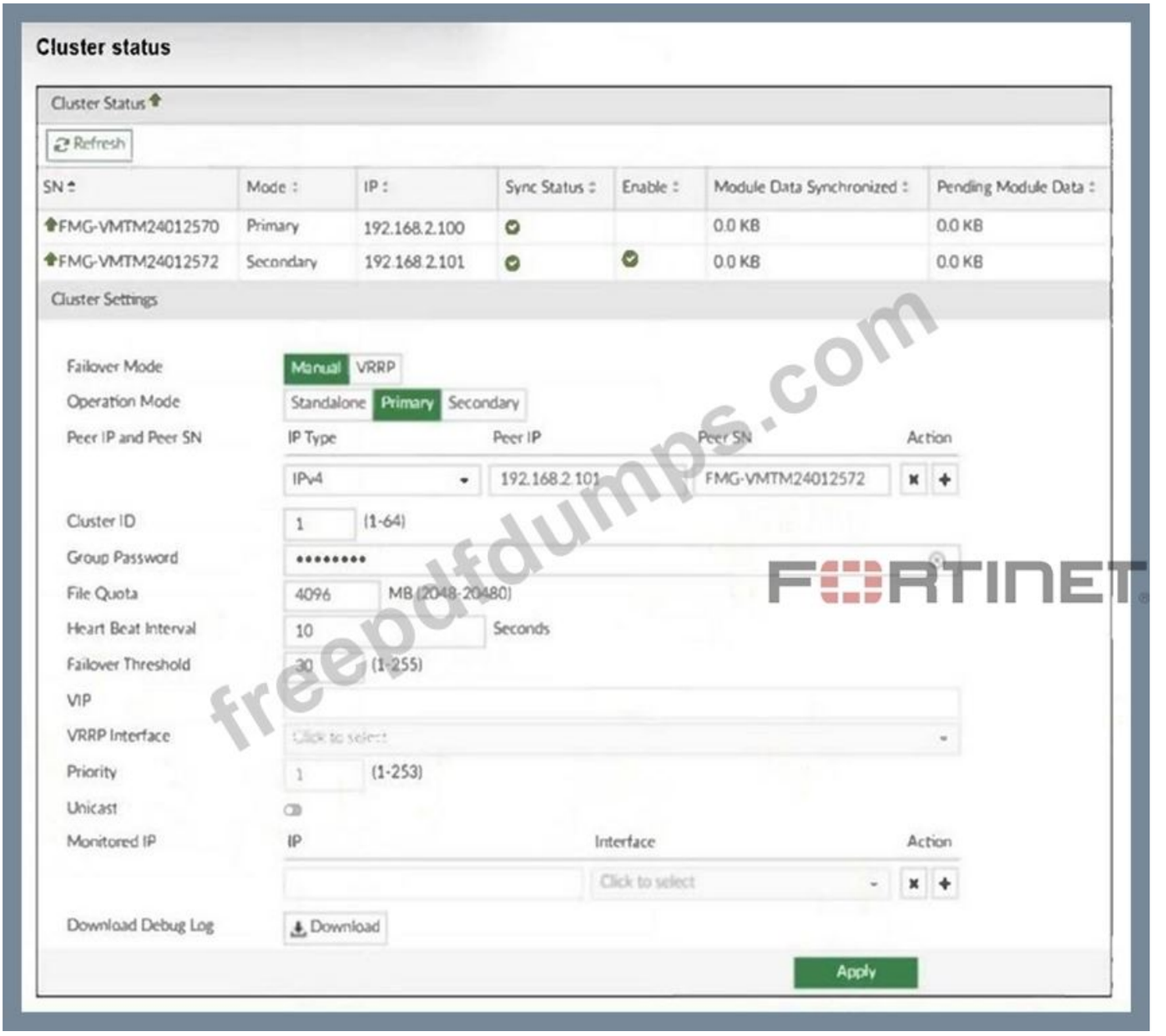
D. Use a FortiManager script to apply the configuration changes.

Answer: (SHOW ANSWER)

To make configuration changes from FortiManager to managed devices while in backup mode, you must use the script feature..

NEW QUESTION: 10

Refer to the exhibit. Which statement about the environment shown in the exhibit is true?



A. You must restart the secondary device if you promote it to primary.

B. No FortiGuard packages have been synchronized between the cluster member.

C. A failover will take place after five minutes without receiving heartbeat packets.

D. FortiAnalyzer features are not enabled on this FortiManager device.

Answer: D (LEAVE A REPLY)

HA is not supported if you have the FortiAnalyzer features enabled on FortiManager.

NEW QUESTION: 11

What allows FortiManager to run CLI scripts on FortiGate devices without prompting for SSH authentication each time?

A. FortiGate devices using the legacy login method.

B. The secure management tunnel between FortiManager and FortiGate devices.

C. The script using the Remote FortiGate Directly (via CLI) option.

D. The script on the FortiManager device database.

Answer: B (LEAVE A REPLY)

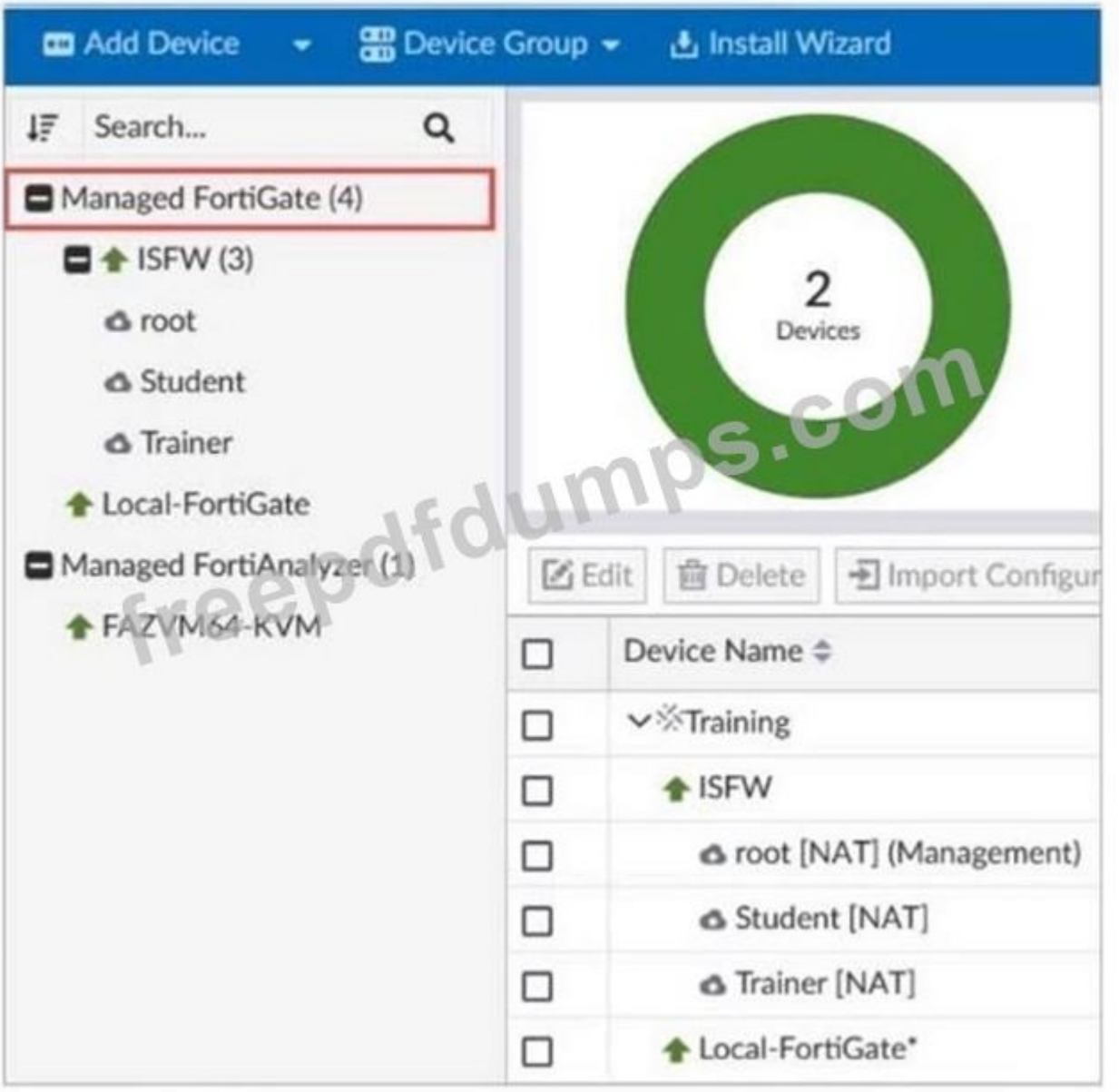
FortiManager uses a secure management tunnel (TCP port 541) to communicate with managed FortiGate devices. This tunnel allows FortiManager to run CLI scripts, push configuration changes, and retrieve information without prompting for SSH authentication each time, as trust is already established through device authorization and certificate exchange.

NEW QUESTION: 12
Refer to the exhibit. Which two statements about the configuration shown in the exhibit are true? (Choose two.)

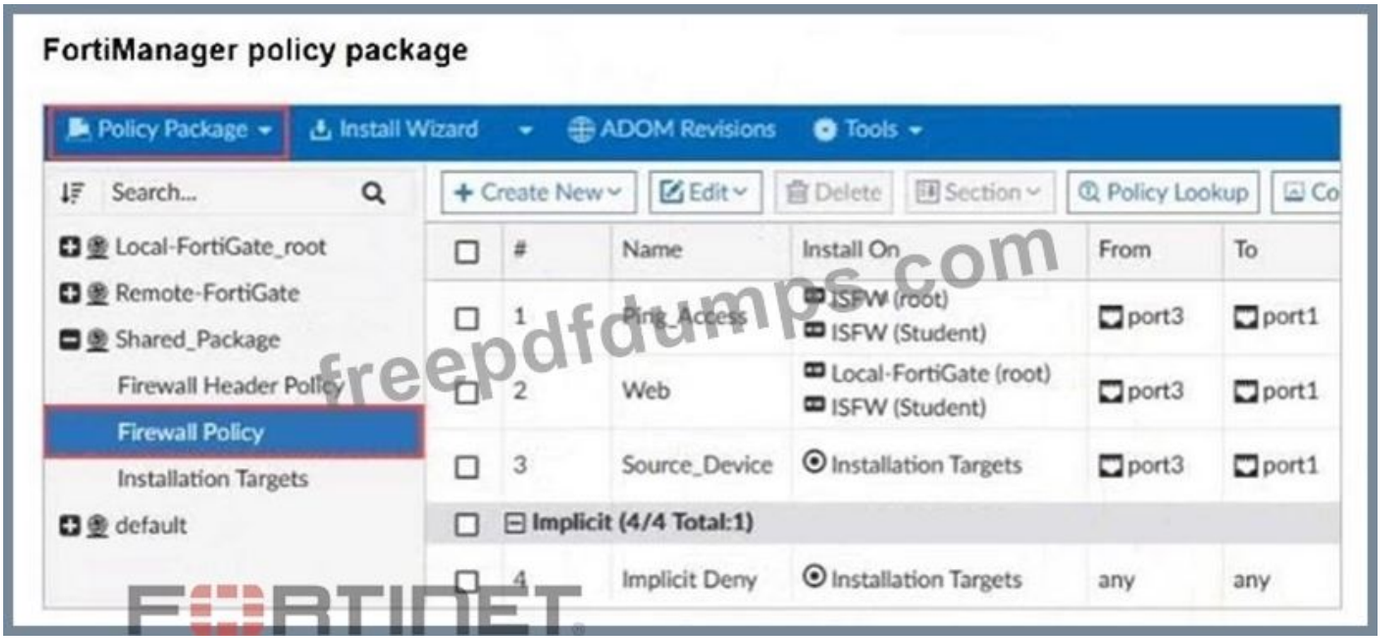
A. An administrator can lock the Local-FortiGate_root policy package.
B. The administrator created a snapshot of the Remote-FortiGate policy package.
C. The FortiManager ADOM workspace mode is set to normal.
D. The FortiManager is in workflow mode.
Answer: A,C (LEAVE A REPLY)
The lock icon next to the Remote-FortiGate policy package indicates it is currently locked by an administrator. This confirms that policy packages like Local-FortiGate_root can also be locked, meaning an administrator can lock them.
The presence of individual locks and the lack of workflow-specific icons or steps indicate that FortiManager is operating in Normal Mode, not Workflow Mode.

NEW QUESTION: 13
Refer to the exhibits. What can you conclude, based on the configuration shown in the exhibit?

Managed FortiGate devices



FortiManager policy package



A. Policy sequence #1 will be installed on the internal segmentation firewall (ISFW) device root [NAT] and Trainer [NAT] VDOMs.

B. Policy sequence #3 must have devices or VDOMs listed in the Install On column; otherwise, it will cause errors.

C. The global policy package will be added to the top of the ISFW policy package.

D. The administrator needs to retrieve the Local-FortiGate configuration to sync with the Security Fabric group, Training.

Answer: C (LEAVE A REPLY)

In FortiManager, when a global policy package is assigned to a local ADOM policy package, it is typically inserted at the top of the local policy sequence. This allows global rules (such as compliance or baseline security policies) to be enforced before local rules.

So, if the exhibit shows that a global policy is linked to the ISFW policy package, it will be added to the top of that package during installation.

NEW QUESTION: 14

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 (LEAVE A REPLY)

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: 15
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 (LEAVE A REPLY)
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: 16
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: C (LEAVE A REPLY)
An ADOM can work in device moces: Normal, which is the default mode, and Advanced.

In Normal mode, you cannot assign diferent FortiGate virtual domains (VDOMs) to different Fortitvlanager ADOMs.
In Advanced mode, you can assign different VDOMs from the sarne FortjGate device to diferent ADOMs. The system applies this setting globally to all ADOMs. This resutts in more complex management scenarios, and it is recommended for advanced users only.

NEW QUESTION: 17
Refer to the exhibit. What percent of the available RAM is being used by the process in charge of downloading the web and email filter databases from the public FortiGuard servers?

FortiManager CLI output

```
FortiManager # execute top
top - 13:08:23 up 1 day,  1:01,  0 users,  load average: 2.40, 3.19, 3.34

Tasks: 188 total,   2 running, 186 sleeping,   0 stopped,   0 zombie

%Cpu(s): 15.4 us,  7.7 sy,  0.0 ni, 76.9 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st

MiB Mem : 7955.5 total,   2235.6 free,  2895.6 used,  2824.1 buff/cache

MiB Swap: 2048.0 total,   2048.0 free,     0.0 used.  4011.0 avail Mem

  PID USER      PR  NI    VIRT    RES  %CPU  %MEM     TIME+ S COMMAND
 1163 root      20   0   17.6m   2.1m   7.1   0.1   0:00.05 R top
    1 root      20   0  602.2m  14.9m   0.0   0.7   0:11.67 S /bin/initXXXXXXXXXX
    2 root      20   0    0.0m   0.0m   0.0   0.0   0:00.00 S [kthreadd]
 1462 root      20   0  303.2m 248.0m   0.0   3.1   0:14.72 S fwmsvrd
 1463 root      20   0  288.2m 232.3m   0.0   2.9   0:16.47 S fgdlinkd
 1465 root      20   0  383.7m 328.0m   0.0   4.1   0:15.26 S fgdsvr
 1467 root      20   0   84.0m  23.6m   0.0   0.3   0:00.06 S /bin/fgdhttpd
 1468 root      20   0   63.9m  13.1m   0.0   0.2   0:13.00 S fgdupd
 1469 root      20   0   63.5m  12.6m   0.0   0.2   0:00.07 S fmtr_svrd
 1470 root      20   0    6.3m   3.5m   0.0   0.0   0:00.09 S /bin/webconsoled
 1471 root      20   0  996.4m 850.6m   0.0  10.7   0:00.01 S srchd
 1475 root      20   0  996.4m 120.6m   0.0   1.5   0:00.00 S fclinkd
```


A. 2.9
B. 3.1
C. 1.5
D. 4.1

Answer: (SHOW ANSWER)

The fgdlinkd process on FortiManager is responsible for downloading web-filter and email-filter databases from public FortiGuard servers, providing up-to-date security threat protection.

NEW QUESTION: 18

An administrator upgrades FortiManager with workspace mode (per ADOM) enabled to the latest version but notices that the ADOM versions did not change.

Why were the ADOMs not upgraded?

A. The administrator did not run the database integrity check before performing the upgrade.

B. FortiManager does not automatically upgrade ADOMs after a firmware upgrade.

C. A FortiManager process task is stuck and blocking the ADOM upgrade, so the administrator must fix it.

D. A user had all ADOMs locked before the upgrade, which stopped them from being upgraded.

Answer: (SHOW ANSWER)

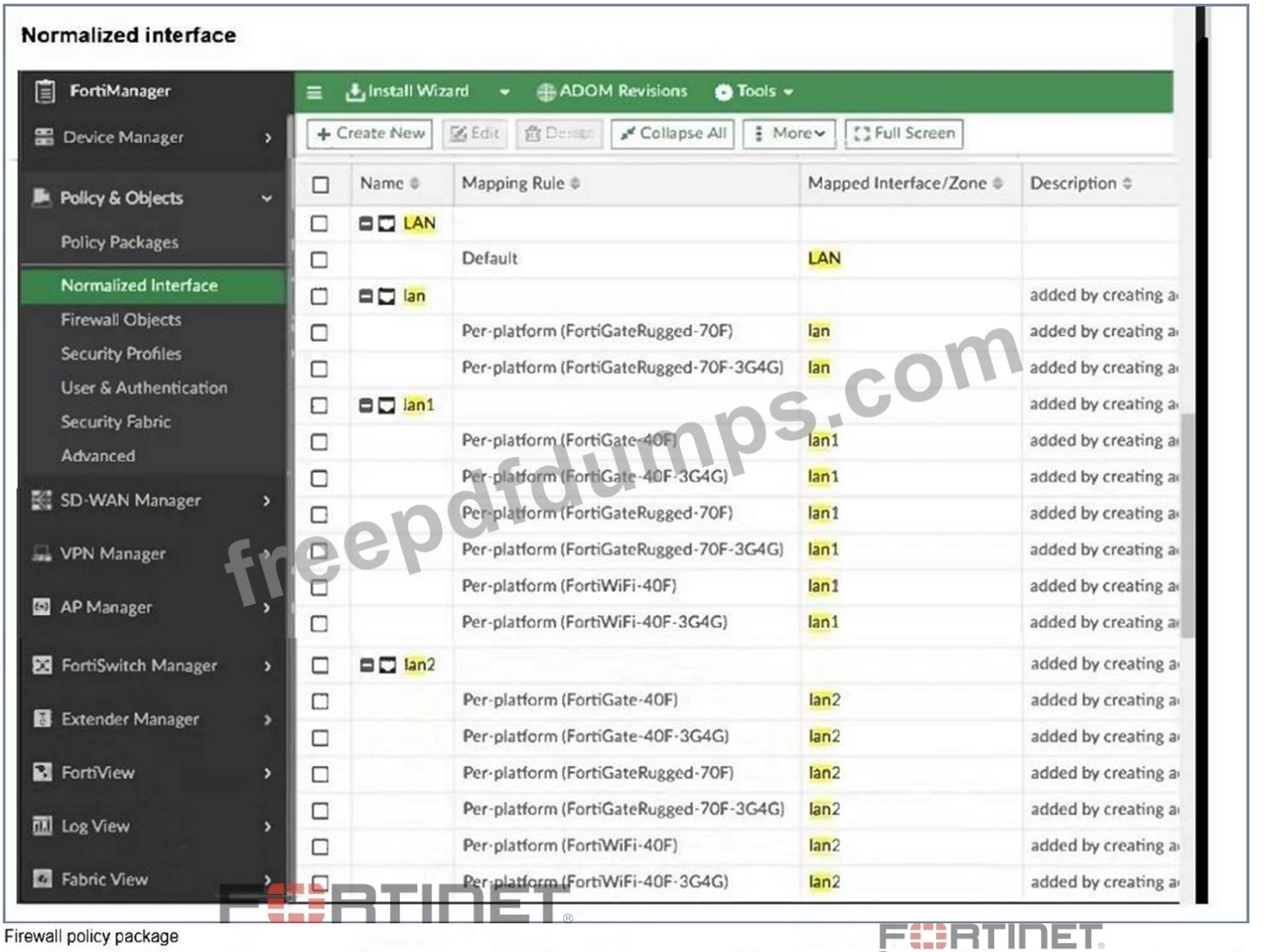
After a FortiManager firmware upgrade, ADOM versions are not automatically upgraded. This is by design, allowing administrators to manually control when to upgrade each ADOM, ensuring compatibility with the FortiGate firmware versions managed within those ADOMs.

NEW QUESTION: 19

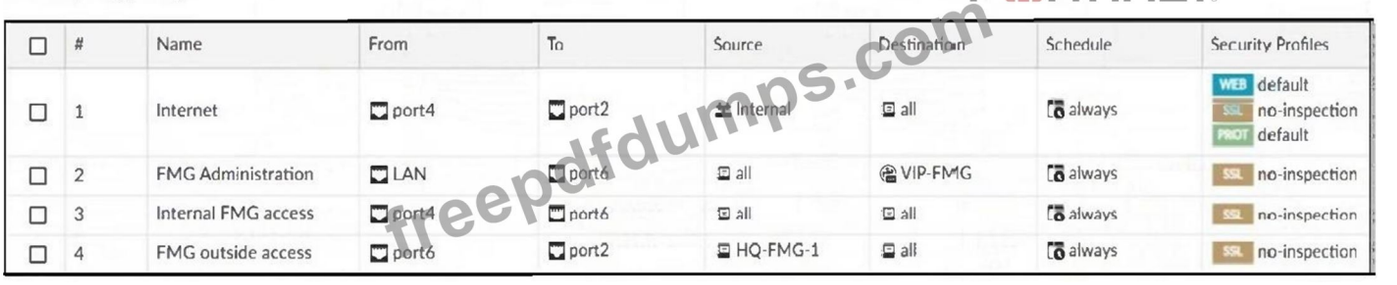
Refer to the exhibits. An administrator must replace the source LAN interface in policy ID 2 on their FortiGateRugged-70F.

However, when they try to install the policy package, they receive the error shown in the exhibit.

What should the administrator do to resolve the error?



Firewall policy package



#	Name	From	To	Source	Destination	Schedule	Security Profiles
1	Internet	port4	port2	Internal	all	always	WEB default SSL no-inspection PROT default
2	FMG Administration	LAN	port6	all	VIP-FMG	always	SSL no-inspection
3	Internal FMG access	port4	port6	all	all	always	SSL no-inspection
4	FMG outside access	port6	port2	HQ-FMG-1	all	always	SSL no-inspection

A. Use the API to assign a system template interface forFortiGateRugged-70F model.

B. Use a metadata variable to dynamically assign an interface when this error occurs.

C. Create a per0device mapping for the LAN interface.

D. Replace LAN with lan1, which is supported by FortiGateRugged-70F models.

Answer: C (LEAVE A REPLY)

The installation error clearly states that the dynamic interface mapping for "LAN" is undefined for device HQ-NGFW-1 (a FortiGateRugged-70F). In the "Normalized Interface" view, "LAN" is a normalized name, but FortiGateRugged-70F uses "lan1" as the actual interface. To resolve the conflict, the administrator must create a per-device mapping linking the normalized interface "LAN" to "lan1" for the FortiGateRugged-70F device. This allows FortiManager to properly translate the interface name during policy installation.

NEW QUESTION: 20

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.

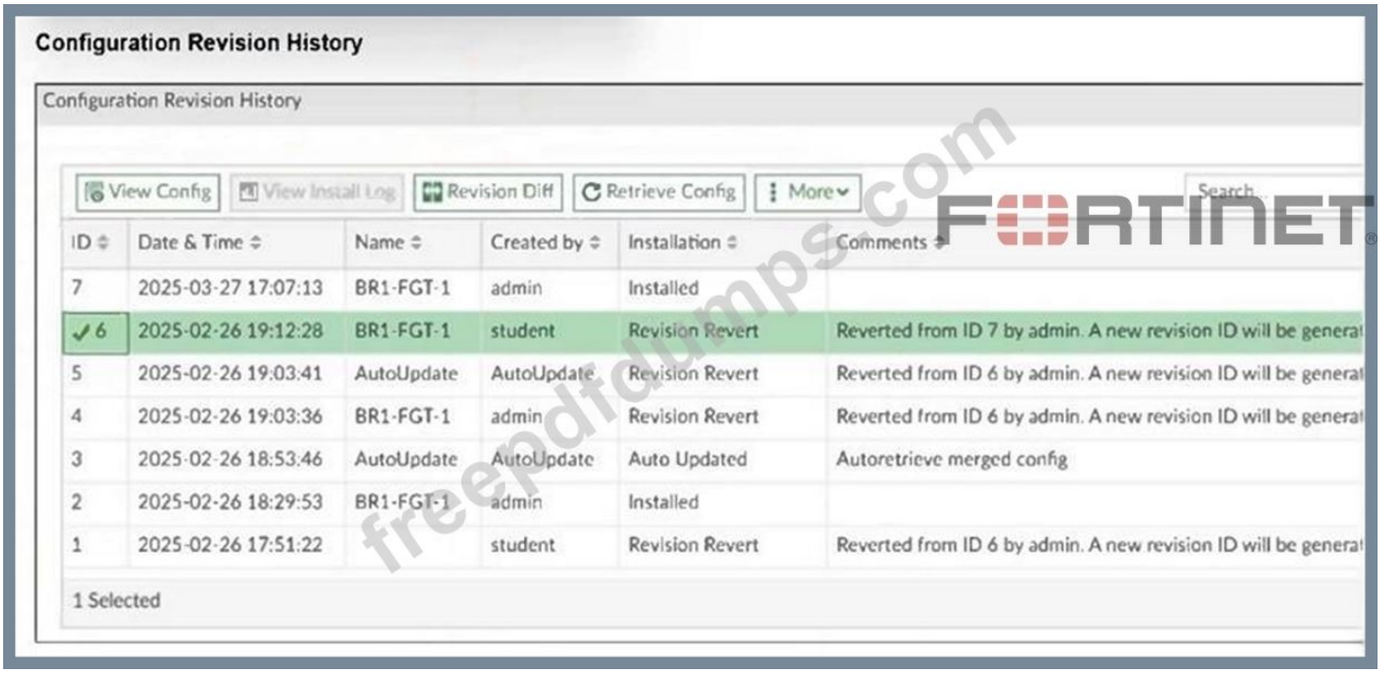
Answer: D (LEAVE A REPLY)

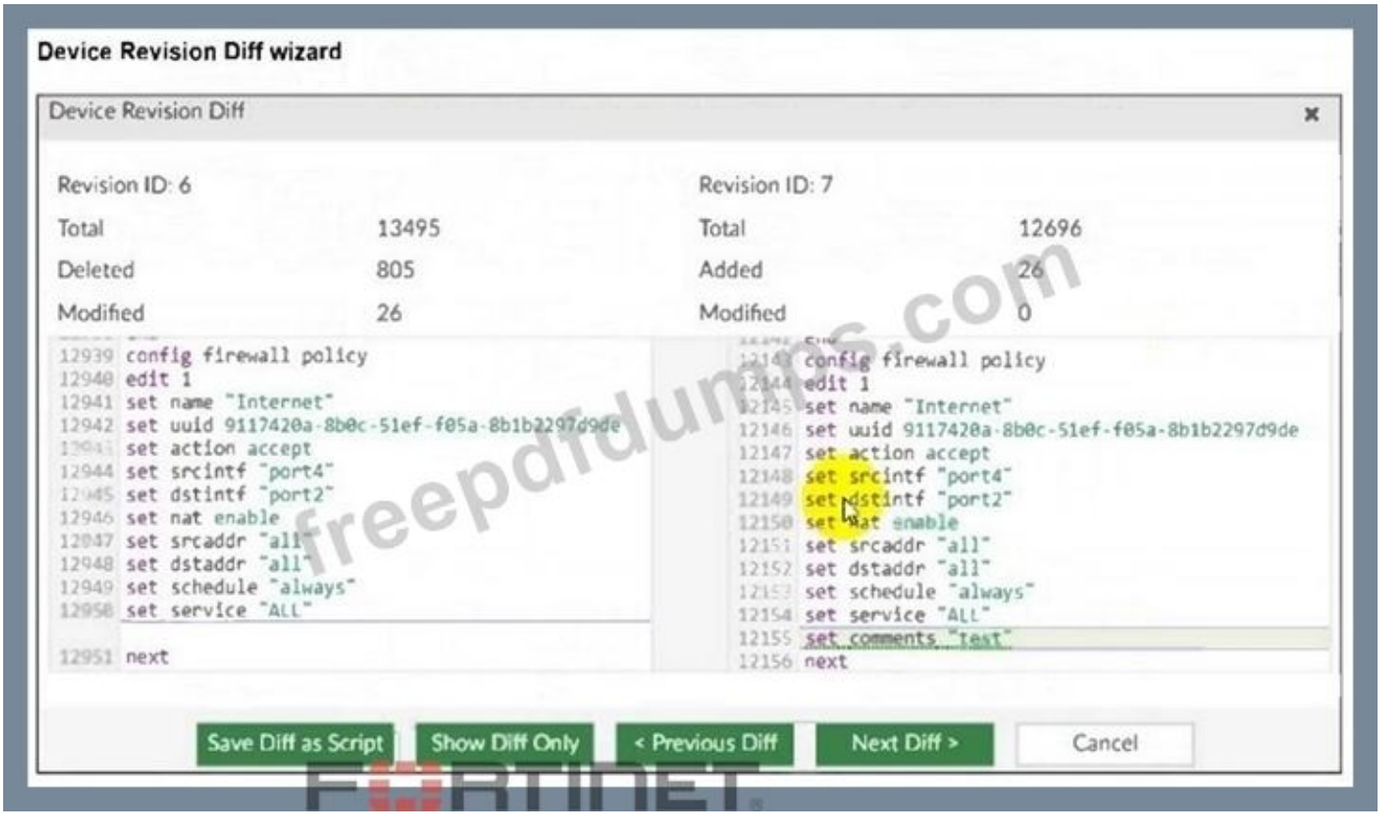
The global policy package is managed only from the global ADOM by the service provider administrator. Customer administrators with access solely to their ADOM (My_ADOM) cannot edit the global header policy; such changes must be made by the service provider administrator in the global ADOM.

NEW QUESTION: 21

Refer to the exhibits. An administrator admin used the Configuration Revision History window to revert the FortiGate device configuration to revision ID 6. After running the reinstall policy package, the administrator noticed problems with the firewall policy- they could not see the unset comment on policy ID 1.

Why did FortiManager not remove the comment from policy ID 1 when the administrator ran reinstall policy package?





A. Because the administrator student must install the configuration changes to correctly see the expected results.

B. Because the administrator must import the firewall policies to update the firewall policy package.

C. Because every time the administrator uses the revert configfile, they must use the Install Wizard instead of running the reinstall policy package.

D. Because the administrator used the Revision Diff view, which shows what changed, not what will be installed.

Answer: B (LEAVE A REPLY)

Reverting the configuration on the FortiGate directly does not update FortiManager's internal policy package.

FortiManager does not automatically sync with what's on the FortiGate device after a manual configuration revert or change directly on the FortiGate.

NEW QUESTION: 22

A FortiManager administrator opens the revision history and choose to revert to a previous version.

What will this action do to the current device configuration?

A. It will trigger an unknown device-level database status, and the administrator will have to import a policy package to sync.

B. It will trigger a conflict status if it is using any provisioning template, and the administrator will have to install changes.

C. It will revert both configurations: device-level database and policy layer database.

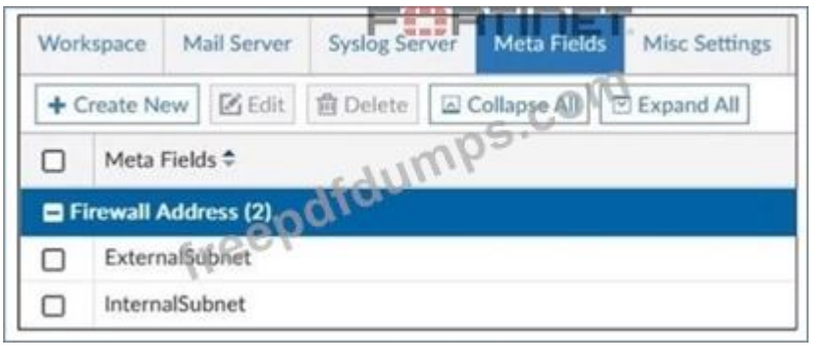
D. It will modify the device-level database.

Answer: D (LEAVE A REPLY)
When you revert to a previous ADOM revision in FortiManager, the device-level database (which contains configuration settings specific to the managed device) will be modified to match the version you reverted to. This action restores the device configuration from that revision, effectively undoing any changes made since that point in time.

NEW QUESTION: 23
What are two outcomes of ADOM revisions? (Choose two.)
A. ADOM revisions can save the current state of the entire ADOM.
B. ADOM revisions do not increase the size of configuration backups.
C. ADOM revisions can save the current state of all policy packages and objects for an ADOM.
D. ADOM revisions appear in the Install Policy & Package Settings section of the install wizard.
Answer: (SHOW ANSWER)
Note that an ADOM revision is a snapshot of the entire ADOM and not the changes specific to this policy package.
Warning: Keep in mind that ADOM revisions can significantly increase the size of the configuration backup.

NEW QUESTION: 24
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: C (LEAVE A REPLY)
If you change BGP in FortiManager and only reinstall the policy package, the change will NOT reach FortiGate because BGP is a device setting. You must install device settings.

NEW QUESTION: 25
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: (SHOW ANSWER)

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: 26

An administrator assigned the Training global policy package to the Branches policy package in ADOM1. Later, the administrator created a new policy package named Remotes on ADOM1. What should the administrator do to sync the Training global policy package with the Remotes policy package in ADOM1?

A. Manually add and assign the Remotes policy package to the Training global policy package

B. Use the automatically install policies to ADOM devices method to sync from the Training global policy package to the Remotes policy package

C. Assign the Training global policy package to the Remotes policy package

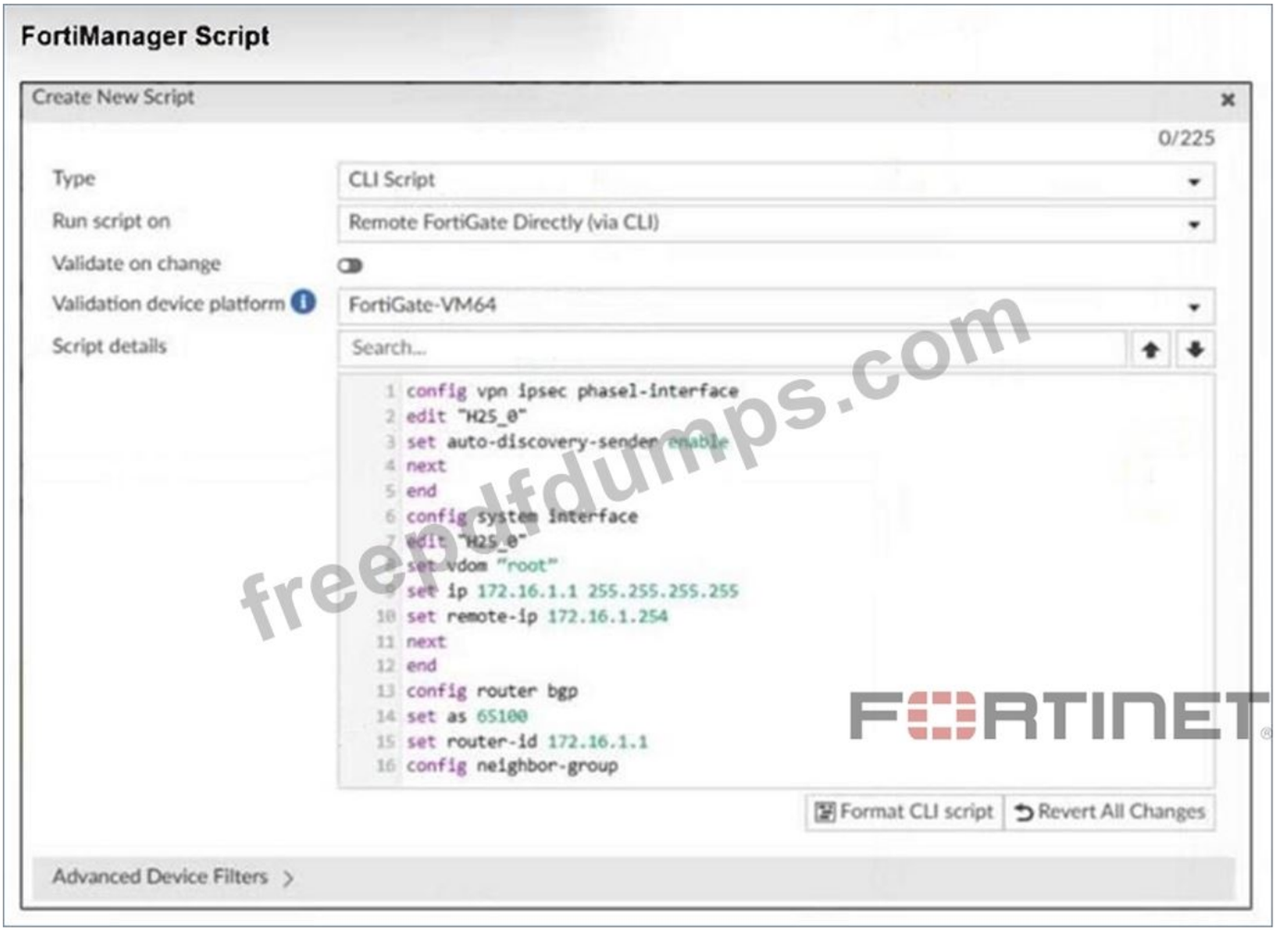
D. Unassign the Training policy package and reassign it to all policy packages within ADOM1

Answer: (SHOW ANSWER)

In FortiManager, global policy packages are not automatically assigned to new policy packages created in an ADOM. To apply a global policy (like "Training") to a new policy package (like "Remotes"), the administrator must manually assign the global policy to that policy package. Therefore, the correct step is to assign the Training global policy package to the Remotes policy package.

NEW QUESTION: 27

Refer to the exhibit. Which two actions will occur if you run the script using the Remote FortiGate Directly (via CLI) option? (Choose two.)



A. FortiManager will provide a preview of CLI commands before executing this script on a managed FortiGate.

B. FortiManager will create a new revision history.

C. FortiGate will auto-updated the FortiManager device-level database.

D. You will have to install these changes using the Install Wizard.

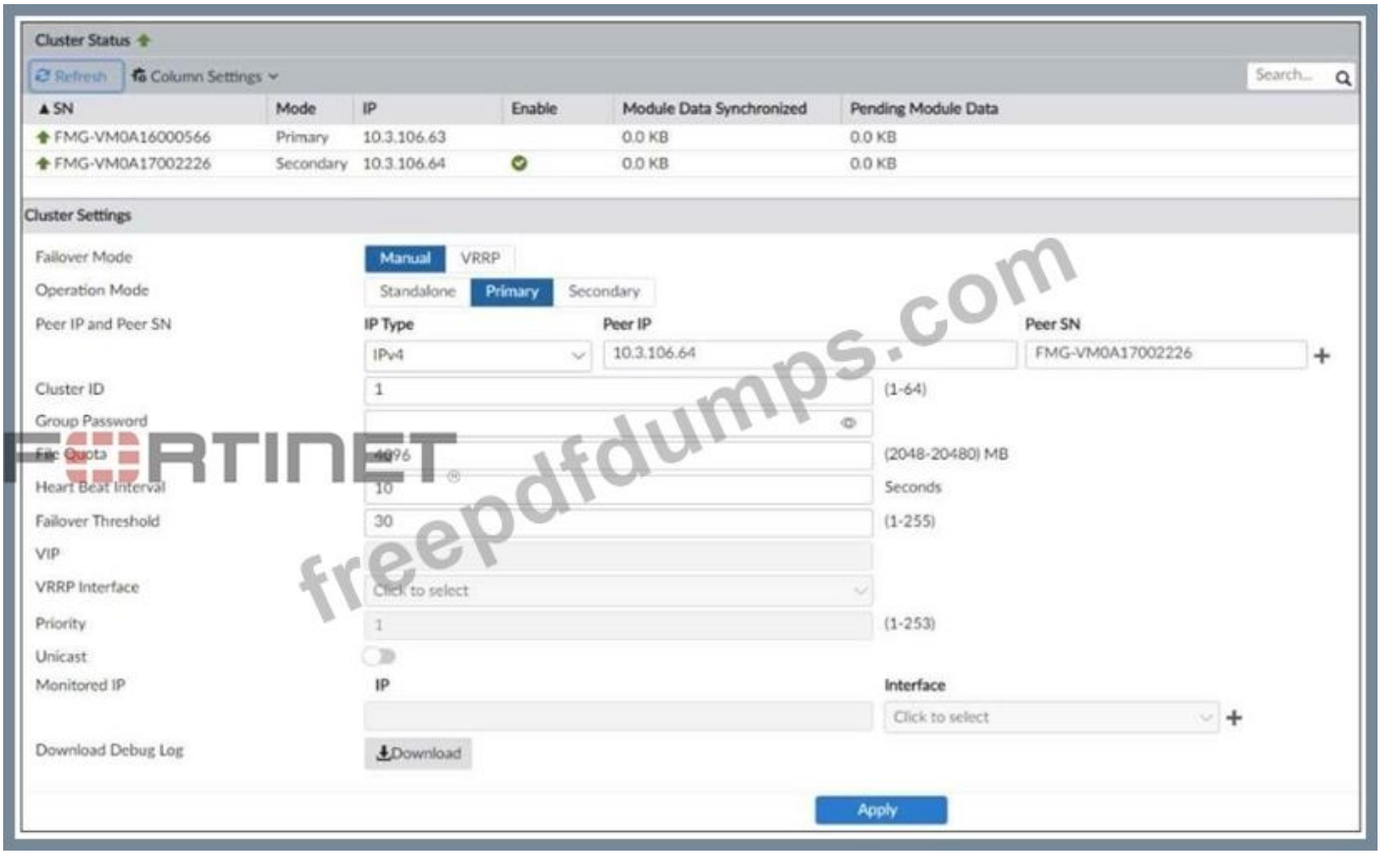
Answer: B,C (LEAVE A REPLY)

When you run a script using "Remote FortiGate Directly (via CLI)", FortiManager logs the configuration changes and creates a new revision history for the device.

Since the script is executed directly on the FortiGate, the FortiGate device automatically updates FortiManager's device-level database after the script is successfully applied.

NEW QUESTION: 28

Refer to the exhibit. Which statement about the environment shown in the exhibit is correct?



A. You must restart the secondary unit if you promote it to become the primary.

B. A failover will take place after five minutes without receiving heartbeat packets.

C. FortiAnalyzer features are not enabled on this FortiManager device.

D. No FortiGuard packages have been synchronized between the cluster members yet.

Answer: C (LEAVE A REPLY)

If FortiAnalyzer features are enabled, you cannot add FortiAnalyzer to FortiManager. You will also not be able to configure FortiManager high availability (HA).

NEW QUESTION: 29

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 (LEAVE A REPLY)

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: 30

An administrator created a new ADOM named Training for FortiGate devices only. Then, the administrator added the root FortiGate device of a Security Fabric group to the Training ADOM. Which statement correctly describes the expected result for the downstream devices in the Security Fabric, given the actions taken by the administrator?

A. The downstream devices are automatically authorized.

B. The downstream devices will appear in the Managed FortiGate section of the rootADOM.

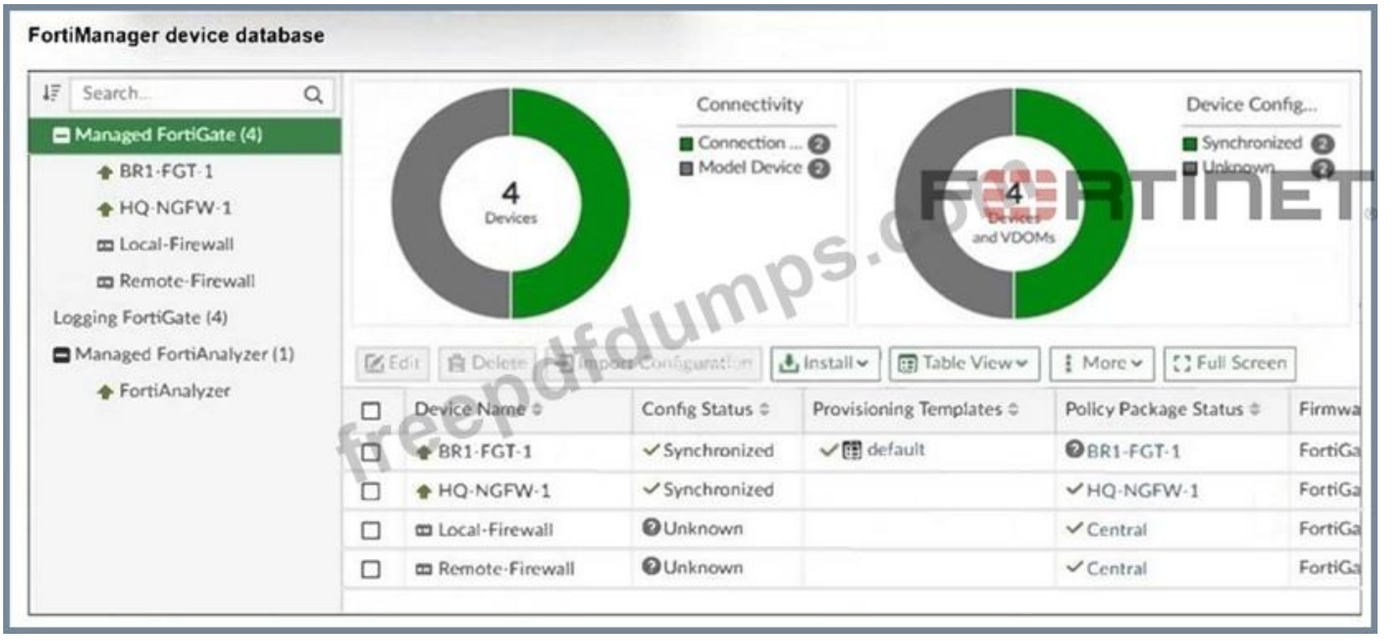
C. The downstream devices show as unauthorized in the root ADOM.

D. The downstream devices must be added using the Add Device wizard.

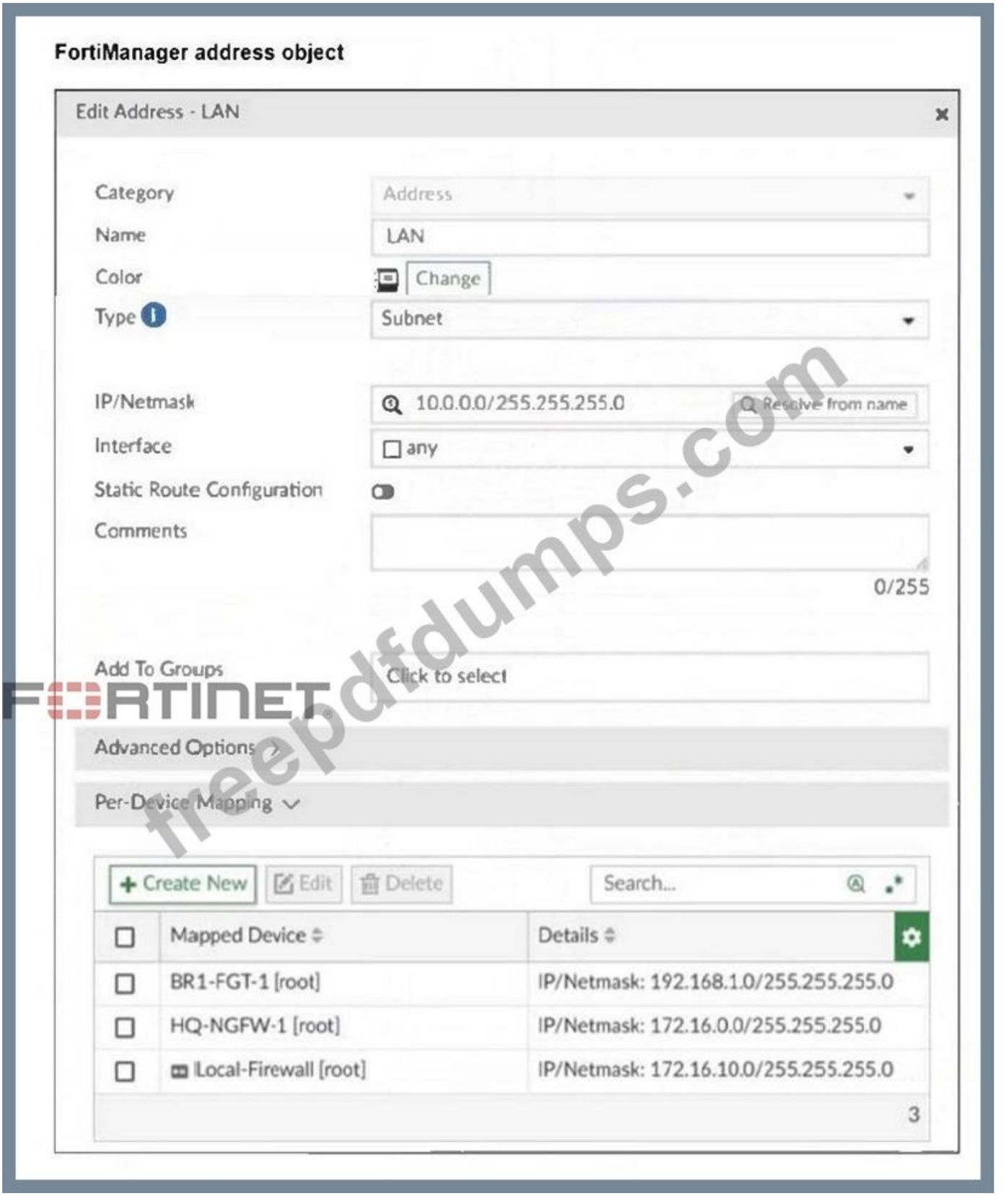
Answer: C (LEAVE A REPLY)

When you add the root FortiGate device of a Security Fabric group to an ADOM (in this case, Training), FortiManager:
- Automatically detects the downstream FortiGate devices in the Security Fabric.
- However, those downstream devices are not automatically added or authorized.
- They will appear as unauthorized devices under the root FortiGate in the Training ADOM, not in the root ADOM.
You must manually authorize each downstream device if you want FortiManager to manage them.

NEW QUESTION: 31
Refer to the exhibits. Which IP/netmask will be present in the LAN firewall address object on the Remote-Firewall?



FortiManager address object



A. 172.16.0.0/255.255.255.0

B. 10.0.0.0/255.255.255.0

C. 192.168.1.0/255.255.255.0

D. 172.16.10.0/255.255.255.0

Answer: (SHOW ANSWER)

In FortiManager, the "Per-Device Mapping" section allows for overriding the default object value for specific devices. The Remote-Firewall is not listed in the Per-Device Mapping table. Therefore, it will use the default value defined in the top portion of the address object, which is 10.0.0.0/255.255.255.0.

NEW QUESTION: 32
An administrator wants to configure and manage multiple objects in the FortiManager database and give access to other users who work in the same database. To stay in control of the changes made to firewall policies by other team members, the administrator needs a setup where all modifications go through a central check before they can be installed.
How can the administrator create this setup?
A. Enable the prompt asking the administrator to accept firewall policies changes before saving.
B. Enable the workspace (for all ADOMs) to control all changes made by any administrator.
C. Enable device lock and the advanced mode feature in the ADOM.
D. Enable workflow mode and the ADOM lock feature.
Answer: (SHOW ANSWER)
Enabling workflow mode along with the ADOM lock feature ensures that all configuration changes go through a centralized review and approval process before installation, allowing controlled and coordinated management of firewall policies by multiple administrators.

Valid FCP_FMG_AD-7.6 Dumps shared by Actual4test.com for Helping Passing FCP_FMG_AD-7.6 Exam! Actual4test.com now offer the **newest FCP_FMG_AD-7.6 exam dumps**, the Actual4test.com FCP_FMG_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com FCP_FMG_AD-7.6 dumps with Test Engine here: https://www.actual4test.com/FCP_FMG_AD-7.6_examcollection.html (**75** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)