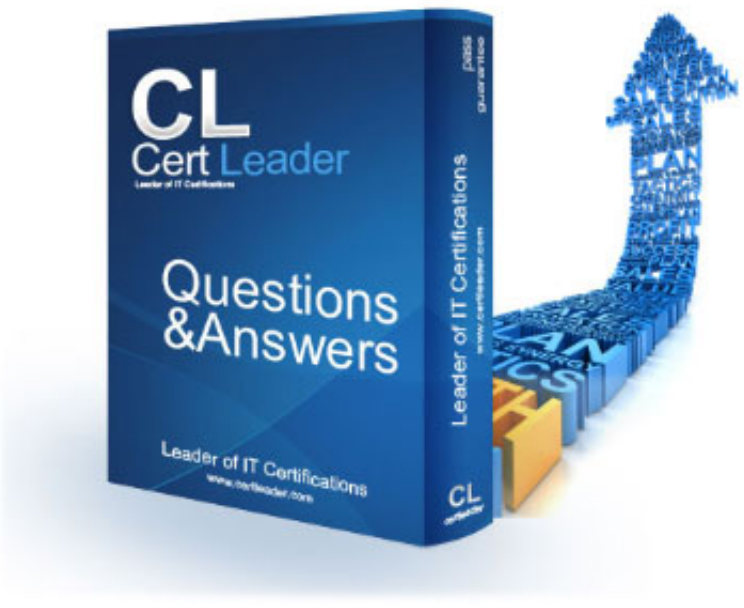
NSE5_FMG-7.0 Dumps

Fortinet NSE 5 - FortiManager 7.0

https://www.certleader.com/NSE5_FMG-7.0-dumps.html



NEW QUESTION 1
- (Exam Topic 1)
Which configuration setting for FortiGate is part of a device-level database on FortiManager?

A. VIP and IP Pools
B. Firewall policies
C. Security profiles
D. Routing

Answer: D

Explanation:
The FortiManager stores the FortiGate configuration details in two distinct databases. The device-level database includes configuration details related to device-level settings, such as interfaces, DNS, routing, and more. The ADOM-level database includes configuration details related to firewall policies, objects, and security profiles.

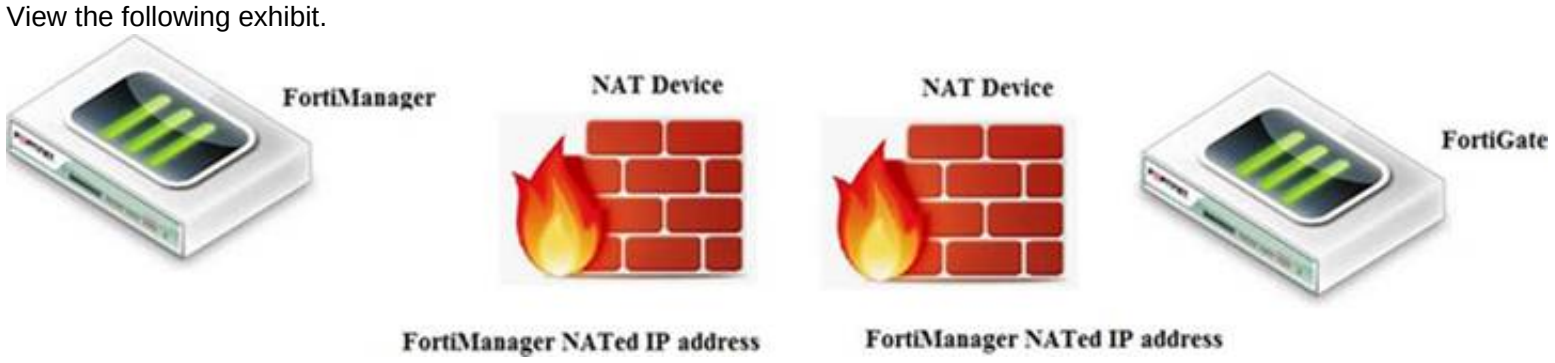
NEW QUESTION 2
- (Exam Topic 1)
Which two statements about the scheduled backup of FortiManager are true? (Choose two.)

A. It does not back up firmware images saved on FortiManager.
B. It can be configured using the CLI and GUI.
C. It backs up all devices and the FortiGuard database.
D. It supports FTP, SCP, and SFTP.

Answer: AD

Explanation:
Reference: https://docs.ansible.com/ansible/latest/collections/fortinet/fortimanager/fmgr_system_backup_allsettings_modul

NEW QUESTION 3
- (Exam Topic 1)
View the following exhibit.



If both FortiManager and FortiGate are behind the NAT devices, what are the two expected results? (Choose two.)

A. FortiGate is discovered by FortiManager through the FortiGate NATed IP address.
B. FortiGate can announce itself to FortiManager only if the FortiManager IP address is configured on FortiGate under central management.
C. During discovery, the FortiManager NATed IP address is not set by default on FortiGate.
D. If the FCFM tunnel is torn down, FortiManager will try to re-establish the FGFM tunnel.

Answer: AC

Explanation:
Fortimanager can discover FortiGate through a NATed FortiGate IP address. If a FortiManager NATed IP address is configured on FortiGate, then FortiGate can announce itself to FortiManager. FortiManager will not attempt to re-establish the FGFM tunnel to the FortiGate NATed IP address, if the FGFM tunnel is interrupted. Just like it was in the NATed FortiManager scenario, the FortiManager NATed IP address in this scenario is not configured under FortiGate central management configuration.

NEW QUESTION 4
- (Exam Topic 1)
Refer to the exhibit.

```
FortiManager # diagnose dvm device list
--- There are currently 1 devices/vdoms managed ---

TYPE            OID    SN        HA    IP             NAME              ADOM       IPS                FIRMWARE
fmg/faz enabled 157    FGVM01..  -     10.200.1.1     Local-FortiGate   My_ADOM    14.00641 (regular) 6.0 MR2 (866)
                |- STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up

                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[imported]Local-FortiGate
```

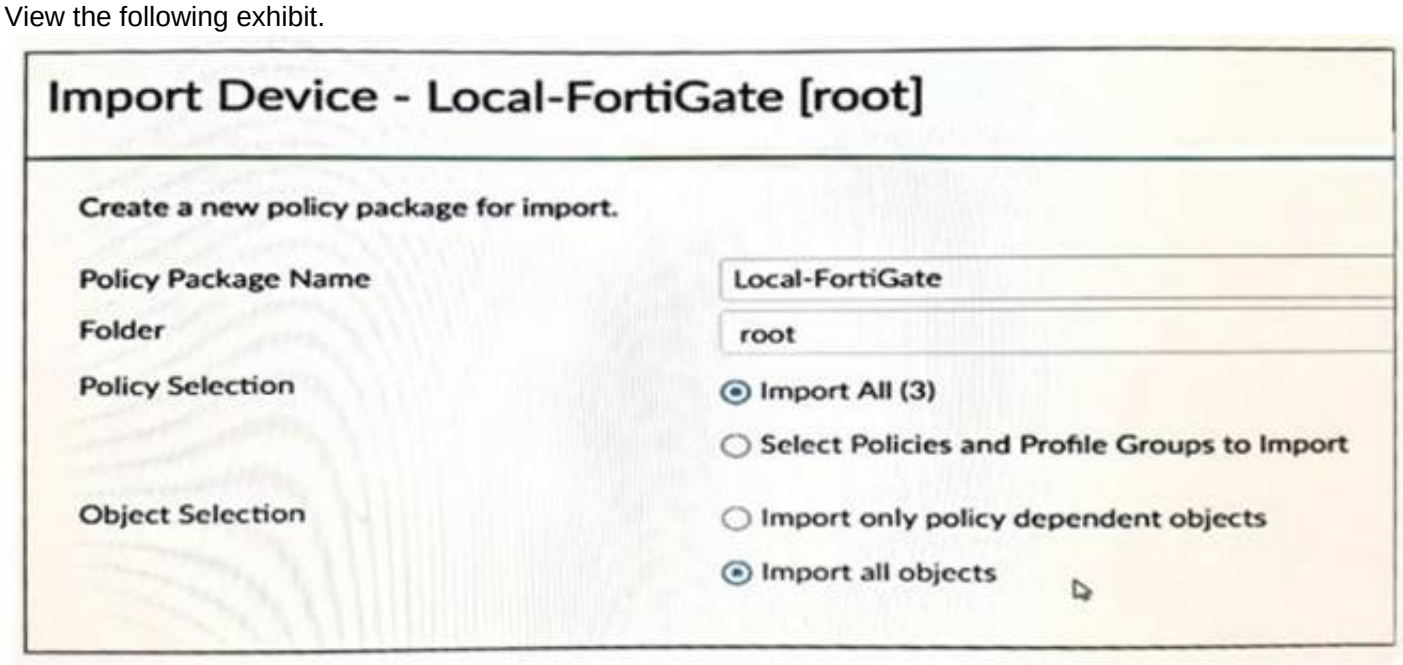
Which two statements about the output are true? (Choose two.)

A. The latest revision history for the managed FortiGate does match with the FortiGate running configuration
B. Configuration changes have been installed to FortiGate and represents FortiGate configuration has been changed
C. The latest history for the managed FortiGate does not match with the device-level database
D. Configuration changes directly made on the FortiGate have been automatically updated to device-leveldatabase

Answer: AC

Explanation:
STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up– dev-db: modified –
This is the device setting status which indicates that configuration changes were made on FortiManager.
– conf: in sync – This is the sync status which shows that the latest revision history is in sync with Fortigate's configuration.– cond: pending – This is the configuration status which says that configuration changes need to be installed.
Most probably a retrieve was done in the past (dm: retrieved) updating the revision history DB (conf: in sync) and FortiManager device level DB, now there is a new modification on FortiManager device level DB (dev-db: modified) which wasn't installed to FortiGate (cond: pending), hence; revision history DB is not aware of that modification and doesn't match device DB.
Conclusion:– Revision DB does match FortiGate.– No changes were installed to FortiGate yet.– Device DB doesn't match Revision DB.– No changes were done on FortiGate (auto-update) but configuration was retrieved instead
After an Auto-Update or Retrieve:device database = latest revision = FGT
Then after a manual change on FMG end (but no install yet):latest revision = FGT (still) but now device database has been modified (is different).
After reverting to a previous revision in revision history:device database = reverted revision != FGT

NEW QUESTION 5
- (Exam Topic 1)
View the following exhibit.



An administrator is importing a new device to FortiManager and has selected the shown options. What will happen if the administrator makes the changes and installs the modified policy package on this managed FortiGate?

A. The unused objects that are not tied to the firewall policies will be installed on FortiGate
B. The unused objects that are not tied to the firewall policies will remain as read-only locally on FortiGate
C. The unused objects that are not tied to the firewall policies locally on FortiGate will be deleted
D. The unused objects that are not tied to the firewall policies in policy package will be deleted from the FortiManager database

Answer: C

Explanation:
Reference:
https://community.fortinet.com/t5/FortiManager/Import-all-objects-Versus-Import-only-policy-dependent-objec

NEW QUESTION 6
- (Exam Topic 1)
View the following exhibit:

```
#diagnose fmupdate view-serverlist fds
Fortiguard Server Comm: Enabled
Server Override Mode: Loose
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
....
38 fds1.fortinet.com     443     -5         0          DEFAULT
```

How will FortiManager try to get updates for antivirus and IPS?

A. From the list of configured override servers with ability to fall back to public FDN servers
B. From the configured override server list only
C. From the default server fdsl.fortinet.com
D. From public FDNI server with highest index number only

Answer: A

Explanation:
Reference:
https://community.fortinet.com/t5/Fortinet-Forum/Clarification-of-FortiManager-s-quot-Server-Override-Mode

NEW QUESTION 7
- (Exam Topic 1)
Refer to the following exhibit:

Which of the following statements are true based on this configuration? (Choose two.)

A. The same administrator can lock more than one ADOM at the same time
B. Ungraceful closed sessions will keep the ADOM in a locked state until the administrator session times out
C. Unlocking an ADOM will submit configuration changes automatically to the approval administrator
D. Unlocking an ADOM will install configuration automatically on managed devices

Answer: AB

Explanation:
Reference: http://help.fortinet.com/fmgr/cli/5-6-2/Document/0800_AD0Ms/200_Configuring+.htm

NEW QUESTION 8
- (Exam Topic 2)
An administrator is replacing a device on FortiManager by running the following command: execute device replace sn <devname> <serialnum>.
What device name and serial number must the administrator use?

A. Device name and serial number of the original device.
B. Device name and serial number of the replacement device.
C. Device name of the replacement device and serial number of the original device.
D. Device name of the original device and serial number of the replacement device.

Answer: D

NEW QUESTION 9
- (Exam Topic 2)
Which two statements regarding device management on FortiManager are true? (Choose two.)

A. FortiGate devices in HA cluster devices are counted as a single device.
B. FortiGate in transparent mode configurations are not counted toward the device count on FortiManager.
C. FortiGate devices in an HA cluster that has five VDOMs are counted as five separate devices.
D. The maximum number of managed devices for each ADOM is 500.

Answer: AC

NEW QUESTION 10
- (Exam Topic 2)
Which two statements about Security Fabric integration with FortiManager are true? (Choose two.)

A. The Security Fabric license, group name and password are required for the FortiManager Security Fabric integration
B. The Fabric View module enables you to generate the Security Fabric ratings for Security Fabric devices
C. The Security Fabric settings are part of the device level settings
D. The Fabric View module enables you to view the Security Fabric ratings for Security Fabric devices

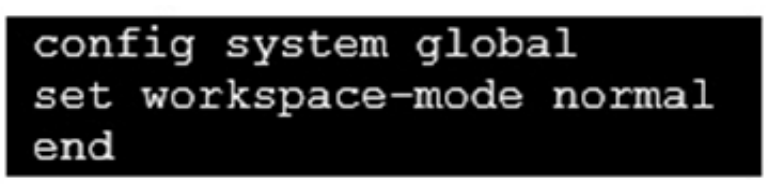
Answer: CD

NEW QUESTION 10
- (Exam Topic 2)
What does a policy package status of Conflict indicate?

A. The policy package reports inconsistencies and conflicts during a Policy Consistency Check.
B. The policy package does not have a FortiGate as the installation target.
C. The policy package configuration has been changed on both FortiManager and the managed device independently.
D. The policy configuration has never been imported after a device was registered on FortiManager.

Answer: C

NEW QUESTION 14
- (Exam Topic 2)
Refer to the exhibit.



Given the configuration shown in the exhibit, which two statements are true? (Choose two.)

A. It allows two or more administrators to make configuration changes at the same time, in the same ADOM.
B. It disables concurrent read-write access to an ADOM.
C. It allows the same administrator to lock more than one ADOM at the same time.
D. It is used to validate administrator login attempts through external servers.

Answer: BC

Explanation:
Reference:
https://docs.fortinet.com/document/fortimanager/6.0.4/administration-guide/86456/concurrentadom-access

NEW QUESTION 19
- (Exam Topic 2)
An administrator has assigned a global policy package to custom ADOM1. Then the administrator creates a new policy package, Fortinet, in the custom ADOM1.
Which statement about the global policy package assignment to the newly-created policy package Fortinet is true?

A. When a new policy package is created, it automatically assigns the global policies to the new package.
B. When a new policy package is created, you need to assign the global policy package from the global ADOM.
C. When a new policy package is created, you need to reapply the global policy package to the ADOM.
D. When a new policy package is created, you can select the option to assign the global policies to the new package.

Answer: A

Explanation:
Global Policy Package is applied at the ADOM level and you have the option to choose which ADOM policy packages you want to exclude (there is no option to choose Policy Packages to include).

NEW QUESTION 23
- (Exam Topic 2)
Refer to the exhibit.

An administrator logs into the FortiManager GUI and sees the panes shown in the exhibit.
Which two reasons can explain why the FortiAnalyzer feature panes do not appear? (Choose two.)

A. The administrator logged in using the unsecure protocol HTTP, so the view is restricted.
B. The administrator profile does not have full access privileges like the Super_User profile.
C. The administrator IP address is not a part of the trusted hosts configured on FortiManager interfaces.
D. FortiAnalyzer features are not enabled on FortiManager.

Answer: BD

NEW QUESTION 24
- (Exam Topic 2)
An administrator's PC crashes before the administrator can submit a workflow session for approval. After the PC is restarted, the administrator notices that the ADOM was locked from the session before the crash.
How can the administrator unlock the ADOM?

A. Restore the configuration from a previous backup.
B. Log in as Super_User in order to unlock the ADOM.
C. Log in using the same administrator account to unlock the ADOM.
D. Delete the previous admin session manually through the FortiManager GUI or CLI.

Answer: D

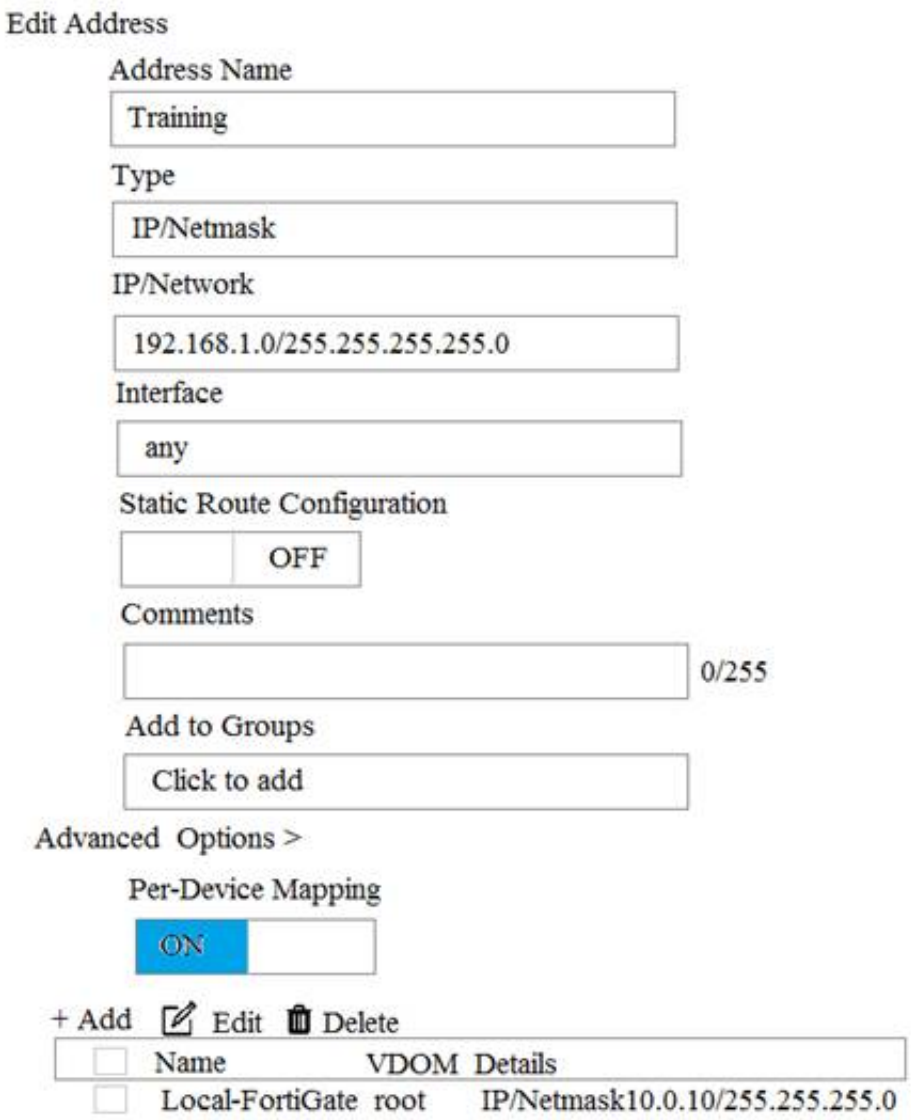
NEW QUESTION 26
- (Exam Topic 3)
Which of the following statements are true regarding VPN Gateway configuration in VPN Manager? (Choose two.)

A. Managed gateways are devices managed by FortiManager in the same ADOM
B. External gateways are third-party VPN gateway devices only
C. Protected subnets are the subnets behind the device that you don't want to allow access to over the IPsec VPN
D. Managed devices in other ADOMs must be treated as external gateways

Answer: AD

Explanation:
Reference: http://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/1300_VPN_Manager/0800_IPsec_VPN_Gateway/0400_Create_mngd_gateway.htm

NEW QUESTION 31
- (Exam Topic 3)
View the following exhibit.



An administrator has created a firewall address object, Training, which is used in the Local-FortiGate policy package. When the install operation is performed, which IP Netmask will be installed on the Local-FortiGate, for the Training firewall address object?

A. 10.0.1.0/24
B. It will create firewall address group on Local-FortiGate with 192.168.0.1/24 and 10.0.1.0/24 object values
C. 192.168.0.1/24
D. Local-FortiGate will automatically choose an IP Network based on its network interface settings.

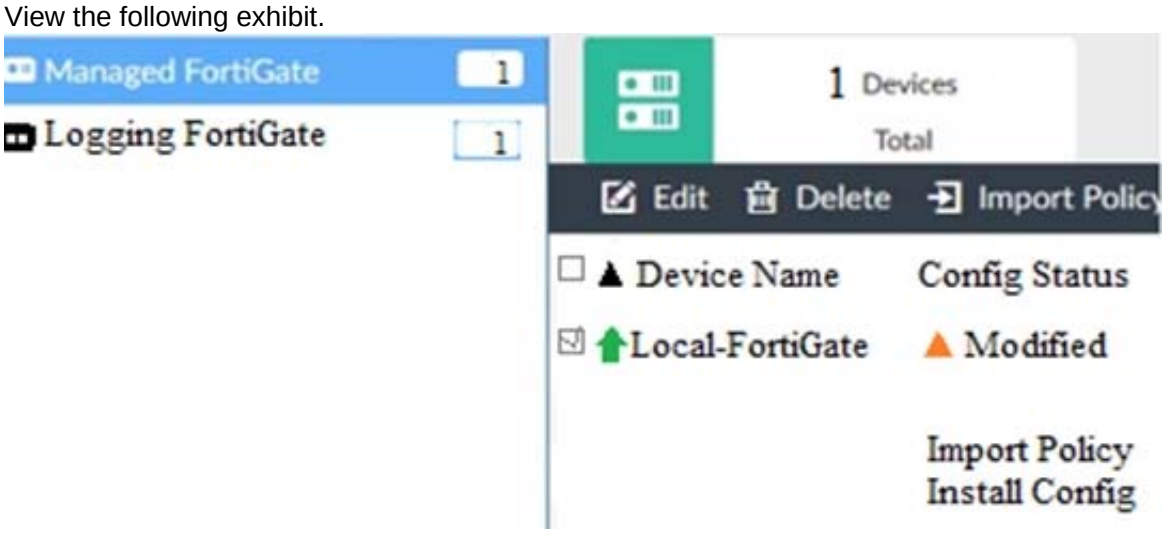
Answer: A

NEW QUESTION 36
- (Exam Topic 3)
An administrator would like to authorize a newly-installed AP using AP Manager. What steps does the administrator need to perform to authorize an AP?

A. Authorize the new AP using AP Manager and wait until the change is updated on the FortiA
B. Changes to the AP's state do not require installation.
C. Changes to the AP's state must be performed directly on the managed FortiGate.
D. Authorize the new AP using AP Manager and install the policy package changes on the managed FortiGate.
E. Authorize the new AP using AP Manager and install the device level settings on the managed FortiGate.

Answer: D

NEW QUESTION 39
- (Exam Topic 3)
View the following exhibit.



When using Install Config option to install configuration changes to managed FortiGate, which of the following statements are true? (Choose two.)

A. Once initiated, the install process cannot be canceled and changes will be installed on the managed device
B. Will not create new revision in the revision history
C. Installs device-level changes to FortiGate without launching the Install Wizard
D. Provides the option to preview configuration changes prior to installing them

Answer: AC

NEW QUESTION 43
- (Exam Topic 3)
View the following exhibit.

```
Start to import config from device(Local-FortiGate) vdom(root) to adom(My_ADOM), package(Local-Fortigate_root)

"firewall service category",SKIPPED,"(name=General,oid=697, DUPLICATE)"

"firewall address", SUCCESS,"(name=LOCAL_SUBNET,oid=684,new object)"

"firewall service custom",SUCCESS,"(name=ALL,oid=863,update previous object)"

"firewall policy",SUCCESS,"(name=1,oid-1090, new object)"
```

Which one of the following statements is true regarding the object named ALL?

A. FortiManager updated the object ALL using FortiGate's value in its database
B. FortiManager updated the object ALL using FortiManager's value in its database
C. FortiManager created the object ALL as a unique entity in its database, which can be only used by this managed FortiGate.
D. FortiManager installed the object ALL with the updated value.

Answer: A

NEW QUESTION 44
.....

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 NSE5_FMG-7.0 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE5_FMG-7.0-dumps.html