Vendor: Fortinet

Exam Code: NSE5_FMG-7.0

Exam Name: Fortinet NSE 5 - FortiManager 7.0

Version: DEMO

QUESTION 1
You are moving managed FortiGate devices from one ADOM to a new ADOM.
Which statement correctly describes the expected result?

A. Any pending device settings will be installed automatically
B. Any unused objects from a previous ADOM are moved to the new ADOM automatically
C. The shared policy package will not be moved to the new ADOM
D. Policy packages will be imported into the new ADOM automaticallyD

Answer: C
Explanation:
If you move a device from one ADOM to another, policies and objects are not imported into the ADOM database. You must run the Import Policy wizard to import policies and objects into the ADOM database.

QUESTION 2
In the event that one of the secondary FortiManager devices fails, which action must be performed to return the FortiManager HA to a working state?

A. Reconfigure the primary device to remove the peer IP of the failed device.
B. Reboot the failed device to remove its IP from the primary device.
C. Manually promote one of the working secondary devices to the primary role, and reboot the old primary device to remove the peer IP of the failed device.
D. The FortiManager HA state transition is transparent to administrators and does not require any reconfiguration.

Answer: A
Explanation:
If the primary unit fails, the backup units stop receiving HA heartbeat packets from the primary unit. If one of the backup units fails, the primary unit stops receiving HA heartbeat packets from the backup unit. In either case, the cluster is considered down until it is reconfigured.
Reconfigure the cluster by removing the failed unit from the cluster configuration. If the primary unit has failed, this means configuring one of the backup units to be the primary unit and adding peer IPs for all of the remaining backup units to the new primary unit configuration.
If a backup unit has failed, reconfigure the cluster by removing the peer IP of the failed backup unit from the primary unit configuration.
https://docs.fortinet.com/document/fortimanager/7.0.5/administration-guide/203784/if-the-primary-or-a-backup-unit-fails

QUESTION 3
Which two items does an FGFM keepalive message include? (Choose two.)

A. FortiGate uptime
B. FortiGate license information
C. FortiGate IPS version
D. FortiGate configuration checksum

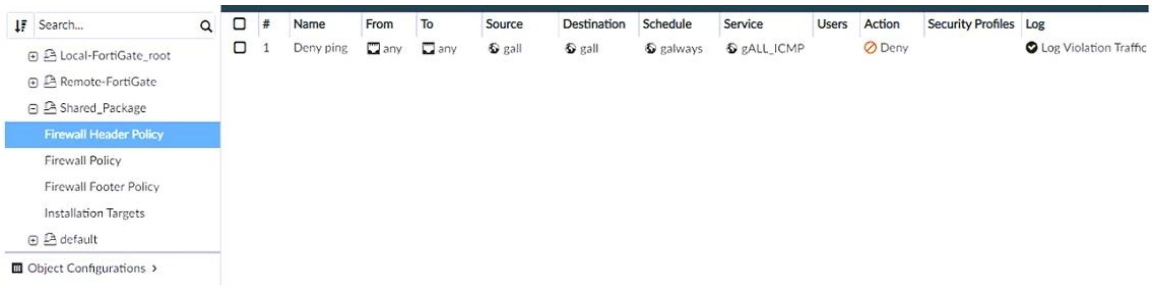
Answer: CD
Explanation:
Keepalive messages, including the configuration checksums, are sent from FortiGate at configurated intervals. The messages also show the intrusion prevention system (IPS) version of the FortiGate device.

QUESTION 4
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.

QUESTION 5
Refer to the exhibit. A service provider administrator has assigned a global policy package to a managed customer ADOM named My_ADOM, which has four policy packages. The customer administrator has access only to My_ADOM.
How can customer or service provider administrators remove both global header and footer policies from the policy package named Shared_Package?



A. The service provider administrator can unassign both global policies from My_ADOM.
B. The service provider administrator can unassign both policies from the global ADOM.
C. The customer administrator can unassign both global polices from My_ADOM.
D. The customer administrator can unassign both polices by locking My_ADOM.

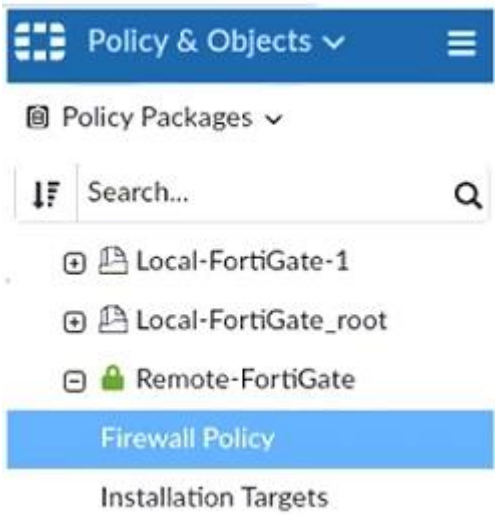
Answer: B
Explanation:
In the global ADOM layer, you create header and footer policy rules. You can assing these policy rules to multiple ADOMs.

QUESTION 6
What is the advantage of using FortiManager to manage FortiAnalyzer?

A. It allows FortiManager to act as a collector and FortiAnalyzer device.
B. It allows FortiManager to manage all FortiGate devices.
C. It allows FortilManager to run reports based on FortiAnalyzer.
D. It allows FortiManager to store all managed FortiGate device logs.

Answer: C
Explanation:
When Fortimanager manages a FortiAnalyzer device, all configuration and data is ketp on FortiAnalyzer to support the following FortiAnalyzer features:
* FortiView
* Log View
* Incidents & Events
* Reports

QUESTION 7
Refer to the exhibit. Given the configuration shown in the exhibit, which two statements are true? (Choose two.)



A. An administrator can also lock the Local-FortiGate-1 policy package.
B. The FortiManager ADOM is locked by the administrator.
C. The FortiManager ADOM mode is set to Normal.
D. FortiManager is in workflow mode.

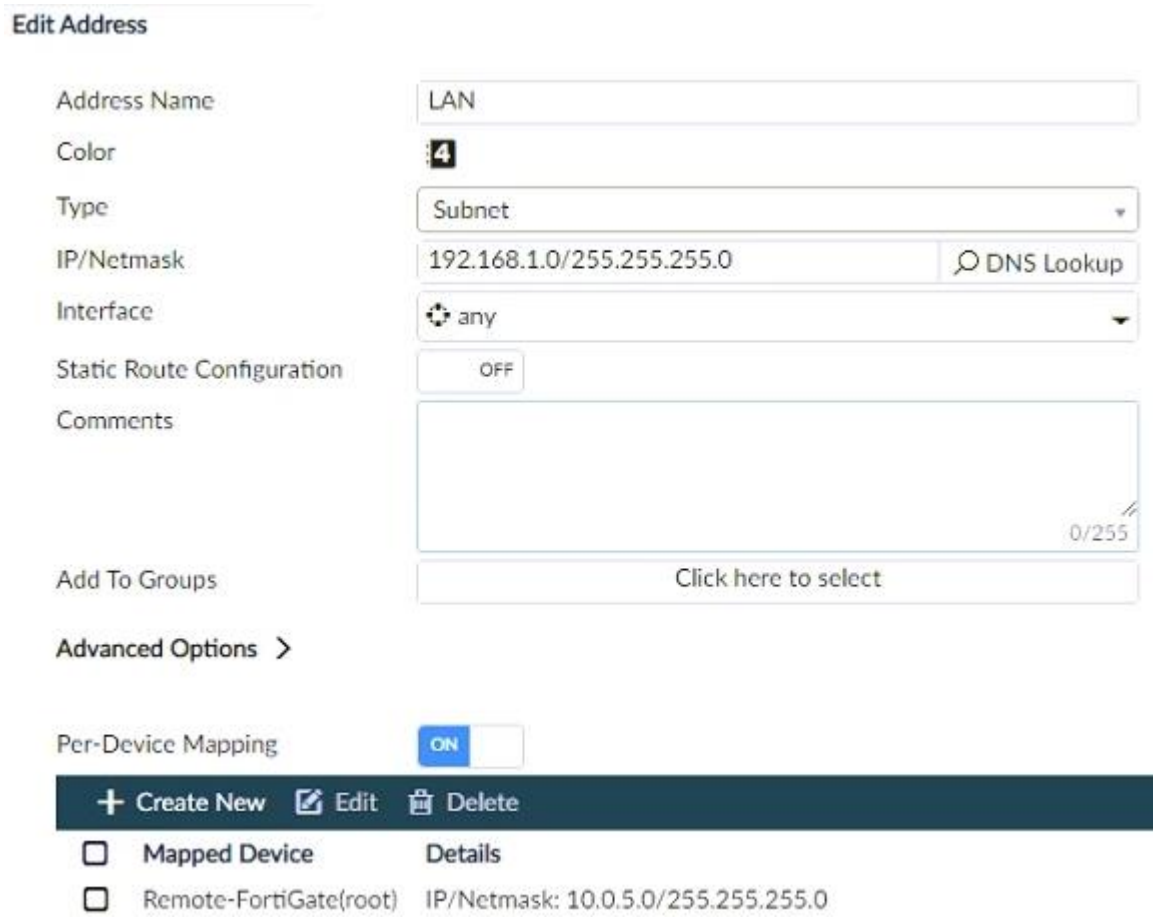
Answer: AD
Explanation:
Policy locking is available in workspace normal mode only. Policy locking allows administrators to work on, and lock, a single policy package instead of locking the whole ADOM.
Note that text in "D" option is wrong, since word "workflow" should be replaced by "workspace-mode normal":

(global)# set workspace-mode
disabled Workspace disabled.
normal Workspace lock mode.
per-adom Per-Adom workspace mode.
workflow Workspace workflow mode.

Workflow mode allows blocking the whole ADOM.

QUESTION 8
Refer to the exhibit. 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 shown on FortiManager for this firewall address object?



A. The FortiManager replaces the address object to none.
B. 192.168.1.0/24
C. 0.0.0.0/0
D. 10.0.5.0/24

Answer: B
Explanation:
In the example shown on this slide, the dynamic address object LocalLan refers to the internal network address of the managed firewalls. The object has a default value of 192.168.1.0/24. The mapping rules are defined per device. For Remote-FortiGate, the address object LocalLan refers to 10.10.11.0/24, whereas for Local-FortiGate the same object refers to 10.10.10.0/24. The devices in the ADOM that do not have dynamic mapping for LocalLan have a default value of 192.168.1.0/24.
In the exibit, the address objetc LAN has a default IP/mask 192.168.1.0/24. So, that's de value it will show bu default.
Option D is wrong because 10.0.5.0/24 is the custom network address configured in "Remote-Fortigate" and it's imported as a dynamic mapping.

QUESTION 9

Refer to the exhibit. An administrator is about to add the FortiGate device to FortiManager using the discovery process. FortiManager is operating behind a NAT device, and the administrator configured the FortiManager NATed IP address under the FortiManager system administration settings.
What is the expected result?


```
config system admin setting
set mgmt-addr <FMG_NATed IP address>
```

A. During discovery, FortiManager sets both the FortiManager NATed IP address and NAT device IP address on FortiGate.
B. During discovery, FortiManager uses only the FortiGate serial number to establish the connection.
C. During discovery, FortiManager sets the FortiManager NATed IP address on FortiGate.
D. During discovery, FortiManager sets the NATed device IP address on FortiGate.

Answer: C
Explanation:
You can configure the FortiManager NATed IP address on FortiGate under the central management configuration.

QUESTION 10
An administrator is tasked with troubleshooting an issue with push updates failing on a FortiManager device that is located behind a NAT device.
Which two settings should the administrator check? (Choose two.)

A. That the virtual IP address and correct ports are set on the NAT device
B. That the NAT device IP address and correct ports are configured on FortiManager
C. That the external IP address on the NAT device is set to DHCP and configured with the virtual IP
D. That the override server IP address is set on FortiManager and the NAT device

Answer: AB
Explanation:
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. By default, the port for push updates is UDP 9443, but you can configure a different port number.
- On the NAT device, configure the virtual IP and port that forwards to FortiManager.
FortiManager may not receive push updates if the external IP address of the NAT device changes.

QUESTION 11
Refer to the exhibit.Review the Download Import Report.
Why is it failing to import firewall policy ID 1?

Start to import config from device(Remote-FortiGate) vdom(root) to adom(root), package(Remote-FortiGate_root)

"firewall address",SKIPPED,"(name=all, oid=2309, DUPLICATE)"

"firewall address",FAIL,"(name=REMOTE_SUBNET, oid=2311, reason=interface((firewall address:REMOTE_SUBNET) any<-port6) binding fail)"

"firewall policy",FAIL,"(name=1, oid=3070, reason=interface(interface binding contradiction. detail: (firewall address:REMOTE_SUBNET) any<-port6) binding fail)"

A. Policy ID 1 for this managed FortiGate already exists on FortiManager in the policy package named Remote-FortiGate.
B. Policy ID 1 is configured from the interface any to port6. FortiManager rejects the request to import this policy because the any interface does not exist on FortiManager.
C. Policy ID 1 does not have the ADOM Interface mapping configured on FortiManager.
D. The address object used in policy ID 1 already exists in the ADOM database with any as the interface association, and conflicts with the address object interface association locally on FortiGate.

Answer: D
Explanation:
FortiManager can create a dynamic mapping for an address object, if the address object name is the same, but contains a different value locally. However, there is one restriction: the associated interface cannot be different. This is because, at the ADOM level, this address object might be used by other policy packages, which might not have the same interfaces.

QUESTION 12
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
Explanation:
For example, if there are two FortiGate devices in an HA cluster (active-active or active-pasive), both FortiGate devices have the same configuration and are counted as one device. However, enabling a VDOM increases the size of the configuration, because each VDOM is logically a separare firewall.

LEAD2PASS
First Test, First Pass!

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

CISCO Microsoft CompTIA ORACLE

(ISC)² CITRIX hp JUNIPER NETWORKS

CEH Certified Ethical Hacker EXIN EMC² where information lives

10% Discount Coupon Code: ASTR14