Fortinet Network Security Expert 5 Written Exam (500)

1. A FortiGate unit is configured with multiple VDOMs. An administrative account on the device has been assigned a Scope value of VDOM:root.

A. PPTP VPN configuration

B. Firewall addresses

C. FortiGuard Distribution Network configuration

D. DHCP servers

Answer(s): C

---

2. What two statements are correct regarding administrative users and accounts? (Choose two.)

A. Administrative user accounts can exist locally or remotely.

B. Administrative user login information is available to all administrators through the Web- based manager.

C. Administrative users must be assigned an administrative profile.

D. Administrative user access is restricted by administrative profiles only.

Answer(s): A,C

---

3. When configuring FortiGuard on FortiManager, which two statements are correct regarding Allow Push Update settings configured in the FortiGuard Antivirus and IPS Settings?

A. If an urgent or critical FortiGuard Antivirus and/or IPS update becomes available, the FortiManager built-in FDS will send push update notifications to each managed device.

B. FortiManager's built-in FDS service may not correctly receive push updates if the external facing IP address of any intermediary NAT device is dynamic.

C. FortiManager's built-in FDS service does not allow an administrator to override the default FortiManager IP address and port used by the FDN to send update messages.

D. If an urgent or critical FortiGuard Antivirus and/or IPS update becomes available, the FortiManager built-in FDS will receive push update notifications.

Answer(s): B,D

---

4. An administrator is examining the attack logs and notices the following entry:

A. This is an HTTP server attack.

B. The attack was against a FortiGate unit at the 192.168.1.100 IP address.

C. The attack was detected and blocked by the FortiGate unit.

D. The attack was detected and passed by the FortiGate unit.

Answer(s): B,D

---

5. Which of the following statements is correct about configuring web filtering overrides?

A. Admin overrides require an administrator to manually allow pending override requests which are listed in the Override Monitor.

B. Using Web Filtering Overrides requires the use of Firewall Policy Authentication.

C. The Override option for FortiGuard Web Filtering is available for any user group type.

D. The Override Scopes of User and User Group are only for use when Firewall Policy Authentication is also being used.

Answer(s): D

---

6. Which part of an email message exchange is NOT inspected by the POP3 and IMAP proxies?

A. TCP connection

B. File attachments

C. Message headers

D. Message body

Answer(s): A

---

7. Which of the following methods is best suited to changing device level settings on existing and future managed FortiGate devices?

A. Configure each managed FortiGate device and install.

B. Configure using CLI-only objects and install.

C. Configure using provisioning templates and install.

D. Configure a script for these settings and install.

Answer(s): C

---

8. Which of the following statements is not correct regarding virtual domains (VDOMs)?

A. VDOMs divide a single FortiGate unit into two or more virtual units that function as multiple, independent units.

B. VDOMs share firmware versions, as well as antivirus and IPS databases.

C. Only administrative users with a super_admin profile will be able to enter all VDOMs to make configuration changes.

D. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.

E. A backup management VDOM will synchronize the configuration from an active management VDOM.

Answer(s): E

---

9. Which two statements are correct regarding synchronization between primary and secondary devices in a FortiManager HA cluster? (Choose two.)

A. All device configurations including global databases are synchronized in the HA cluster.

B. FortiGuard databases are downloaded by the primary FortiManager device and then synchronized with all secondary devices.

C. Local logs and log configuration settings are synchronized in the HA cluster.

D. FortiGuard databases are downloaded separately by each cluster device.

Answer(s): A,D

---

10. Which two statements are correct for configuration changes made by FortiManager scripts?

A. When run on managed devices directly, you can install changes to the managed FortiGate devices using the installation wizard.

B. When run on the device database, you can install changes to the managed FortiGate devices using the installation wizard.

C. When run on the device database, changes are automatically installed to the managed FortiGate devices.

D. When run on managed devices directly, changes are automatically installed to the managed FortiGate devices.

Answer(s): C,D

---

11. Selecting Create New, as shown in the exhibit, will result in what?

A. A new policy package.

B. A new policy in the policy package.

C. A clone of the policy package.

D. A new policy folder.

Answer(s): B

---

12. What advantages are there in using a hub-and-spoke IPSec VPN configuration instead of a fully-meshed set of IPSec tunnels? (Select all that apply.)

A. Using a hub and spoke topology provides stronger encryption.

B. Using a hub and spoke topology simplifies configuration.

C. Using a hub and spoke topology is required to achieve full redundancy.

D. Using a hub and spoke topology reduces the number of tunnels.

Answer(s): B,D

---

13. What are the operating modes of FortiAnalyzer? (Choose two.)

A. Manager

B. Standalone

C. Analyzer

D. Collector

Answer(s): C,D

---

14. Which of the following is true regarding Switch Port Mode?

A. Provides separate routable interfaces for each internal port.

B. An administrator can select ports to be used as a switch.

C. Allows all internal ports to share the same subnet.

D. Configures ports to be part of the same broadcast domain.

Answer(s): C

---

15. An administrator is configuring a DLP rule for FTP traffic. When adding the rule to a DLP sensor, the administrator notes that the Ban Sender action is not available (greyed-out), as shown in the exhibit.

A. Firewall policy authentication is required before the Ban Sender action becomes available.

B. The Ban Sender action needs to be enabled globally for FTP traffic on the FortiGate unit before configuring the sensor.

C. The Ban Sender action is never available for FTP traffic.

D. The Ban Sender action is only available for known domains. No domains have yet been added to the domain list.

Answer(s): C

---

16. Review the output of the command get router info routing-table database shown in the Exhibit below; then answer the question following it.

A. There will be two default routes in the routing table.

B. There will be two routes for the 10.0.2.0/24 subnet in the routing table.

C. There will be six routes in the routing table.

D. There will be seven routes in the routing table.

Answer(s): A,C

---

17. An issue could potentially occur when clicking Connect to start tunnel mode SSL VPN. The tunnel will start up for a few seconds, then shut down.

A. This user does not have permission to enable tunnel mode. Make sure that the tunnel mode widget has been added to that user's web portal.

B. Make sure that only Internet Explorer is used. All other browsers are unsupported.

C. Check the SSL adaptor on the host machine. If necessary, uninstall and reinstall the adaptor from the tunnel mode portal.

D. This FortiGate unit may have multiple Internet connections. To avoid this problem, use the appropriate CLI command to bind the SSL VPN connection to the original incoming interface.

Answer(s): D

---

18. Which of the following items is NOT a packet characteristic matched by a firewall service object?

A. TCP/UDP source and destination ports

B. TCP sequence number

C. ICMP type and code

D. IP protocol number

Answer(s): B

---

19. If a FortiGate unit has a dmz interface IP address of 210.192.168.2 with a subnet mask of

A. 210.192.168.1 - 210.192.168.4

B. 210.192.168.3 - 210.192.168.10

C. 172.168.0.1 - 172.168.0.10

D. All of the above.

Answer(s): B

---

20. Workflow mode includes which new permissions for Super_Admin administrative users?

A. Approval, Self-approval, Change Notification

B. Change Notification, Self-disapproval, Submit

C. Self-disapproval, Approval, Accept

D. Self-approval, Approval, Reject

Answer(s): A
