Fortinet Network Security Expert 4 Written Exam - FortiOS 5.4

1. Which of the following statements are correct regarding FortiGate virtual domains (VDOMs)? (Choose two)

A. Administrative users with a 'super_admin' profile can administrate only one VDOM.

B. Each VDOM can run different firmware versions.

C. VDOMs divide a single FortiGate unit into two or more independent firewall.

D. A management VDOM handles SNMP. logging, alert email and FortiGuard updates.

Answer(s): C,D

---

2. The exhibit shows the Disconnect Cluster Member command in a FortiGate unit that is part of a HA cluster with two HA members.

A. The system hostname is set to the unit serial number.

B. Port3 is configured with an IP address for management access.

C. The firewall rules are purged on the disconnected unit.

D. The HA mode changes to standalone.

Answer(s): B,D

---

3. Which firewall objects can be included in the Destination Address field of a firewall policy? (Choose three.)

A. MAC address

B. Virtual IP address.

C. IP address group.

D. IP address.

E. IP address pool.

Answer(s): B,C,D

---

4. Two FortiGate units with NP6 processors form an active-active cluster. The cluster is doing security profile (UTM) inspection over all the user traffic. What statements are true regarding the sessions that the master unit is offloading to the slave unit for inspection? (Choose two.)

A. They are accelerated by hardware in the master unit.

B. They are accelerated by hardware in the slave unit.

C. They are not accelerated by hardware in the slave unit.

D. They are not accelerated by hardware in the master unit.

Answer(s): A,C

---

5. What are required to be the same for two FortiGate units to form an HA cluster? (Choose two)

A. Model.

B. System time zone.

C. Hostname.

D. Firmware.

Answer(s): A,D

---

6. Which statements about application control are true? (Choose two.)

A. It can inspect encrypted traffic.

B. It can identify traffic from known applications, even when they are using non-standard TCP/UDP ports.

C. It cannot take an action on unknown applications.

D. Enabling application control profile in a security profile enables application control for all the traffic flowing through the FortiGate.

Answer(s): A,B

---

7. How do application control signatures update on a FortiGate device?

A. By running the Application Control auto-learning feature.

B. Upgrade the FortiOS firmware to a newer release.

C. Through FortiGuard updates.

D. Signatures are hard coded to the device and cannot be updated.

Answer(s): C

---

8. What is required in a FortiGate configuration to have more than one dialup IPsec VPN using aggressive mode?

A. All the aggressive mode dialup VPNs MUST accept connections from the same peer ID.

B. The peer ID setting must NOT be used.

C. Each peer ID MUST match the FQDN of each remote peer.

D. Each aggressive mode dialup MUST accept connections from different peer ID.

Answer(s): D

9. FSSO provides a single sign on solution to authenticate users transparently to a FortiGate unit using credentials stored in Windows active directory.

A. An FSSO domain controller agent must be installed on every domain controller.

B. An FSSO collector agent must be installed on every domain controller.

C. The FSSO domain controller agent will regularly update user logon information on the FortiGate unit.

D. The FSSO collector agent will receive user logon information from the domain controller agent and will send it to the FortiGate unit.

Answer(s): A,D

---

10. Which of the following spam filtering methods are supported on the FortiGate unit? (Select all that apply.)

A. Return Email DNS Check

B. Email Checksum Check

C. Black/White List

D. Open Relay Database List (ORDBL)

E. IP Address Check

Answer(s): A,B,C,D,E

---

11. When does a FortiGate load-share traffic between two static routes to the same destination subnet?

A. When they have the same distance and different priority.

B. When they have the same cost and distance.

C. When they have the same distance and the same weight.

D. When they have the same distance and same priority.

Answer(s): D

---

12. Which of the following statements are true about Man-in-the-middle SSL Content Inspection? (Choose three.)

A. The local service certificate of the web server must be installed in the FortiGate device

B. The FortiGate device acts as a sub-CA

C. The required SSL Proxy certificate must first be requested to a public certificate authority (CA).

D. The FortiGate device does man-in-the-middle inspection.

E. The FortiGate device "re-signs" all the certificates coming from the HTTPS servers

Answer(s): A,B,C

---

13. Which of the following statements is correct regarding the FortiGuard Services Web Filtering Override configuration as illustrated in the exhibit?

A. A client with an IP address of 10.10.10.12 is allowed access to any URL under the www.yahoo.com web site, including any subdirectory URLs, until August 7, 2009.

B. Any client on the same subnet as the authenticated user is allowed to access www.yahoo.com/images/ until August 7, 2009.

C. Any client on the same subnet as the authenticated user is allowed to accesswww.yahoo.com/images/.

D. A client with an IP of address 10.10.10.12 is allowed access to any subdirectory that is part of the www.yahoo.com web site.

E. A client with an IP address of 10.10.10.12 is allowed access to the www.yahoo.com/images/ web site and any of its offsite URLs.

Answer(s): E

---

14. Which of the following email spam filtering features is NOT supported on a FortiGate unit?

A. Greylisting

B. HELO DNS Lookup

C. Banned Word

D. Multipurpose Internet Mail Extensions (MIME) Header Check

Answer(s): A

---

15. A firewall policy has been configured such that traffic logging is disabled and a UTM function is enabled.

A. System

B. Traffic

C. None

D. UTM

Answer(s): B

---

16. Which statements are correct regarding virtual domains (VDOMs)? (Choose two.)

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

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

C. Different time zones can be configured in each VDOM.

D. VDOMs divide a single FortiGate unit into two or more virtual units that each have dedicated memory and CPUs.

Answer(s): A,B

---

17. What actions are possible with Application Control? (Choose three.)

A. Traffic Shaping

B. Block

C. Warn

D. Quarantine

E. Allow

Answer(s): A,B,E

---

18. An administrator has enabled proxy-based antivirus scanning and configured the following settings:

A. Files bigger than 10 MB are sent to the heuristics engine for scanning.

B. FortiGate scans the files in chunks of 10 MB.

C. Files bigger than 10 MB are not scanned for viruses and will be blocked.

D. FortiGate scans only the first 10 MB of any file.

Answer(s): C

---

19. In transparent mode, forward-domain is an CLI setting associate with ___________.

A. a firewall policy

B. static route

C. an interface

D. a virtual domain

Answer(s): C

---

20. In which order are firewall policies processed on a FortiGate unit?

A. Based on best match.

B. Based on the priority value.

C. From top to down, according with their policy ID number.

D. From top to down, according with their sequence number.

Answer(s): D
