

# Fast2Test

## Pass Your Next Certification Exam Fast!

Everything you need to prepare, learn & pass your certification exam easily.

365 days free updates. First attempt guaranteed success.



### Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

### 365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.



### Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

### Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

We're not the only ones **happy** about Fast2test Practice Materials ...

**62316+** customers in 100+ countries use Fast2test Self Test Engine. Meet our customers.

<https://tw.fast2test.com>

高效的考試材料是最高通過率的考試題庫

**Exam** : **NSE5**

**Title** : Fortinet Network Security  
Expert 5 Written Exam (500)

**Vendor** : Fortinet

**Version** : DEMO

**NO.1** Given the Antivirus and IPS update service is enabled, and the FortiGuard settings as shown in the exhibit. The desired behavior is for managed devices to use public servers for these updates should FortiManager become unreachable, which is not the case with the current configuration. What two actions are necessary to correct this? (Choose two.)

The screenshot shows the FortiGuard Management interface. On the left, the 'Advanced Settings' menu is expanded. The main area displays 'Server Override Mode' with 'Strict (Access Override Server Only)' selected. Below it, 'FortiGuard AntiVirus and IPS Settings' is expanded, showing 'FortiGuard Distribution Network(FDN)' with 'Use Override Server Address for FortiGate/FortiMail' checked. The IP Address is 192.168.1.152 and Port is 8890. A terminal window at the bottom shows the command 'diagnose fupdate fds-serverlist' and its output: 'Response=202|Current fds server list :grpindex:0 0 ip = 192.168.1.152 port = 8890 timezone=-8 distance=0'.

- A. Change the server override mode from strict to loose.
- B. Change the port from 8890 to 443 in the Use Override Server Address for FortiGate/FortiMail settings.
- C. Uncheck the option Use Override Server Address for FortiGate/FortiMail.
- D. Change the IP address to a public FDS server and port to 443 in the Use Override Server Address for FortiGate/FortiMail settings.

**Answer:** A,C

**NO.2** Which of the following products is designed to manage multiple FortiGate devices?

- A. FortiGate device
- B. FortiAnalyzer device
- C. FortiClient device
- D. FortiManager device
- E. FortiMail device
- F. FortiBridge device

**Answer:** D

**NO.3** Examine the exhibit shown below then answer the question that follows it.

The screenshot shows the 'Edit UTM Proxy Options' configuration page. The 'SSL Inspection Options' section is visible, showing 'CA Certificate' set to 'Fortinet\_CA\_SSLProxy' and 'Inspect All Ports' unchecked. A table lists protocols and their inspection ports:

Enable	Protocol	Inspection Port(s)
<input checked="" type="checkbox"/>	HTTPS	443
<input type="checkbox"/>	SMTPS	465
<input type="checkbox"/>	POP3S	995
<input type="checkbox"/>	IMAPS	993
<input type="checkbox"/>	FTPS	990

Within the UTM Proxy Options, the CA certificate Fortinet\_CA\_SSLProxy defines which of the following:

- A. FortiGate unit's encryption certificate used by the SSL proxy.
- B. FortiGate unit's signing certificate used by the SSL proxy.
- C. FortiGuard's signing certificate used by the SSL proxy.
- D. FortiGuard's encryption certificate used by the SSL proxy.

**Answer:** A

**NO.4** Which statement is true regarding the import/export feature?

- A. This is only a feature for reports.
- B. This feature is for reports and charts.
- C. This feature is for reports, charts, and datasets.
- D. This feature is for reports and datasets.

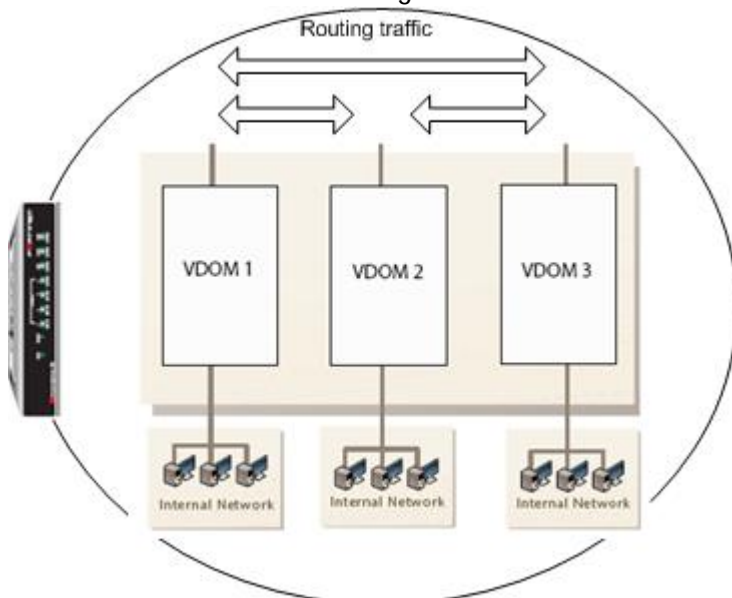
**Answer:** B

**NO.5** Which of the following are valid components of the Fortinet Server Authentication Extensions (FSAE)? (Select all that apply.)

- A. Domain Local Security Agent.
- B. Collector Agent.
- C. Active Directory Agent.
- D. User Authentication Agent.
- E. Domain Controller Agent.

**Answer:** B,E

**NO.6** A FortiGate unit is configured with three Virtual Domains (VDOMs) as illustrated in the exhibit.



Which of the following statements are true if the network administrator wants to route traffic between all the VDOMs? (Select all that apply.)

- A. The administrator should configure inter-VDOM links to avoid using external interfaces and routers.

- B. As with all FortiGate unit interfaces, firewall policies must be in place for traffic to be allowed to pass through any interface, including inter-VDOM links. This provides the same level of security internally as externally.
- C. This configuration requires the use of an external router.
- D. Inter-VDOM routing is automatically provided if all the subnets that need to be routed are locally attached.
- E. As each VDOM has an independent routing table, routing rules need to be set (for example, static routing, OSPF) in each VDOM to route traffic between VDOMs.

**Answer:** A,B,E

**NO.7** When a FortiManager HA primary device fails, which two statements are correct for promoting a secondary device to the primary role? (Choose two.)

- A. Must manually reconfigure one of the secondary devices to become the master device.
- B. Reboot is required when promoting from secondary to primary.
- C. All other secondary devices must be reconfigured to point to new primary device.
- D. The FortiManager HA supports IP takeover where an HA state transition does not require manual intervention.

**Answer:** A,C

**NO.8** Which of the following is true regarding Switch Port Mode?

- A. Allows all internal ports to share the same subnet.
- B. Provides separate routable interfaces for each internal port.
- C. An administrator can select ports to be used as a switch.
- D. Configures ports to be part of the same broadcast domain.

**Answer:** A

**NO.9** In which order are firewall policies processed on the FortiGate unit?

- A. They are processed from the top down as they appear in Web Config.
- B. They are processed based on the policy ID number shown in the left hand column of the policy window.
- C. They are processed using a policy hierarchy scheme that allows for multiple decision branching.
- D. They are processed based on a priority value assigned through the priority column in the policy window.


**Answer:** A

**NO.10** The Idle Timeout setting on a FortiGate unit applies to which of the following?

- A. Web browsing
- B. FTP connections
- C. User authentication
- D. Administrator access
- E. Web filtering overrides.

**Answer:** D

**NO.11** In HA, the option Reserve Management Port for Cluster Member is selected as shown in the Exhibit below.



High Availability

Mode: Active-Passive

Device Priority: 200

Reserve Management Port for Cluster Member: port7

Which of the following statements are correct regarding this setting? (Select all that apply.)

- A. Interface settings on port7 will not be synchronized with other cluster members.
- B. The IP address assigned to this interface must not overlap with the IP address subnet assigned to another interface.
- C. Port7 appears in the routing table.
- D. A gateway address may be configured for port7.
- E. When connecting to port7 you always connect to the master device.

**Answer:** A,D

**NO.12** Which of the following statements is correct about how the FortiGate unit verifies username and password during user authentication?

- A. If a remote server is included in a user group, it will be checked before local accounts.
- B. An administrator can define a local account for which the password must be verified by querying a remote server.
- C. If authentication fails with a local password, the FortiGate unit will query the authentication server if the local user is configured with both a local password and an authentication server.
- D. The FortiGate unit will only attempt to authenticate against Active Directory if Fortinet Server Authentication Extensions are installed and configured.

**Answer:** B

**NO.13** A FortiGate unit is configured to receive push updates from the FortiGuard Distribution Network, however, updates are not being received.

Which of the following statements are possible reasons for this? (Select all that apply.)

- A. The external facing interface of the FortiGate unit is configured to use DHCP.
- B. The FortiGate unit has not been registered.
- C. There is a NAT device between the FortiGate unit and the FortiGuard Distribution Network and no override push IP is configured.
- D. The FortiGate unit is in Transparent mode which does not support push updates.

**Answer:** A,B,C

**NO.14** How can DLP file filters be configured to detect Office 2010 files? (Select all that apply.)

- A. File Type. Microsoft Office(msoffice)
- B. File Type. Archive(zip)
- C. File Type. Unknown Filetype(unknown)
- D. File Name. "\*.ppt", "\*.doc", "\*.xls"

E. File Name. "\*.pptx", "\*.docx", "\*.xlsx"

**Answer:** B,E

**NO.15** What are the main management wizards used in Device Manager?

A. Add Device, Provisioning Templates, and View Installation

B. Add Device, Install Wizard, and Import Policy

C. Script, Configuring CLI-Objects, and Re-install Policy

D. View Installation, Import Policy, and Script

**Answer:** B

**NO.16** In HA, what is the effect of the Disconnect Cluster Member command as given in the Exhibit.



A. The HA mode changes to standalone.

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

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

D. All other interface IP settings are maintained.

**Answer:** A,B

**NO.17** Which of the following network protocols are supported for administrative access to a FortiGate unit?

A. HTTPS, HTTP, SSH, TELNET, PING, SNMP

B. FTP, HTTPS, NNTP, TCP, WINS

C. HTTP, NNTP, SMTP, DHCP

D. Telnet, FTP, RLOGIN, HTTP, HTTPS, DDNS

E. Telnet, UDP, NNTP, SMTP

**Answer:** A

**NO.18** What effect do administrative domains (ADOM) have on report settings? (Choose two.)

A. None. ADOMs cannot be used with reports.

B. Reports must be configured within their own ADOM.

C. Chart Library, Macro Library, Dataset Library, and Output Profile become ADOM- specific.

D. Dataset Library becomes global for all ADOMs.

**Answer:** B,C

**NO.19** If Open Shortest Path First (OSPF) has already been configured on a FortiGate unit, which of the following statements is correct if the routes learned through OSPF need to be announced by Border Gateway Protocol (BGP)?

- A.** The FortiGate unit will automatically announce all routes learned through OSPF to its BGP peers if the FortiGate unit is configured as an OSPF Autonomous System Boundary Router (ASBR).
- B.** The FortiGate unit will automatically announce all routes learned through OSPF to its BGP peers if the FortiGate unit is configured as an OSPF Area Border Router (ABR).
- C.** At a minimum, the network administrator needs to enable Redistribute OSPF in the BGP settings.
- D.** The BGP local AS number must be the same as the OSPF area number of the routes learned that need to be redistributed into BGP.
- E.** By design, BGP cannot redistribute routes learned through OSPF.

**Answer:** C

**NO.20** Which of the following products provides dedicated hardware to analyze log data from multiple FortiGate devices?

- A.** FortiGate device
- B.** FortiAnalyzer device
- C.** FortiClient device
- D.** FortiManager device
- E.** FortiMail device
- F.** FortiBridge device

**Answer:** B