Pass2Lead

https://Pass2Lead.com

NSE5^{Q&As}

Fortinet Network Security Expert 5 Written Exam (500)

Pass Fortinet NSE5 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/nse5.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

Which of the following statements describes the method of creating a policy to block access to an FTP site?

A. Enable Web Filter URL blocking and add the URL of the FTP site to the URL Block list.

B. Create a firewall policy with destination address set to the IP address of the FTP site, the Service set to FTP, and the Action set to Deny.

C. Create a firewall policy with a protection profile containing the Block FTP option enabled.

D. None of the above.

Correct Answer: B

QUESTION 2

Refer to the exhibit. What does the clock icon denote beside the Bandwidth and Applications Report?
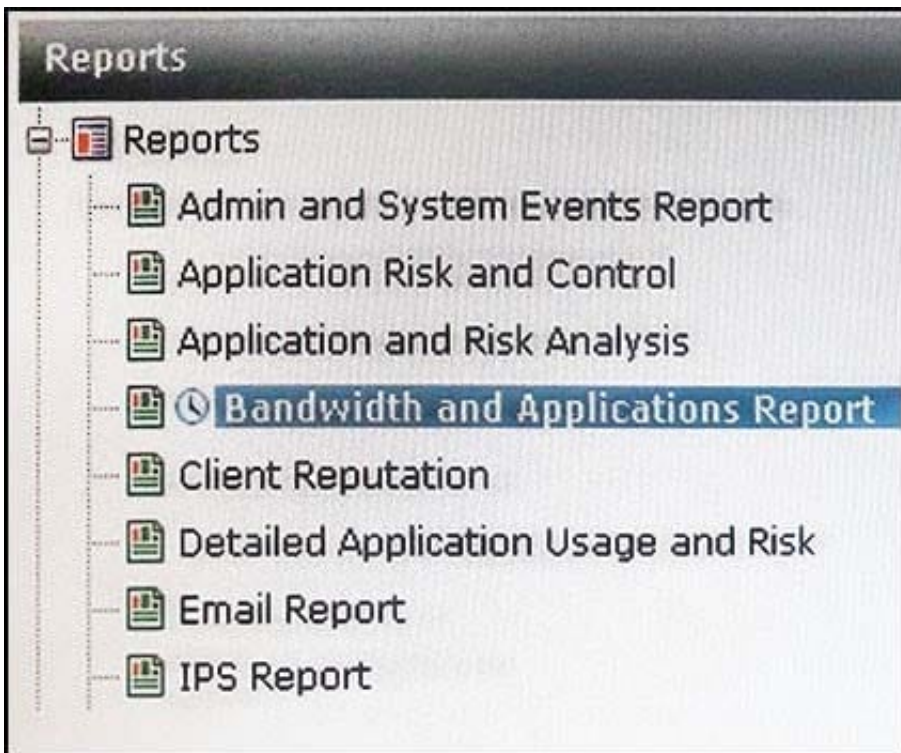
A. It is a custom report.

B. It is an imported report from either a different FortiAnalyzer device or a different (but supported) ADOM.

C. It is in the process of generating.

D. It is a scheduled report.

Correct Answer: D

QUESTION 3

You wish to create a firewall policy that applies only to traffic intended for your web server. The server has an IP address of 192.168.2.2 and belongs to a class C subnet.

When defining the firewall address for use in this policy, which one of the following addressing formats is correct?

A. 192.168.2.0 / 255.255.255.0

B. 192.168.2.2 / 255.255.255.0

C. 192.168.2.0 / 255.255.255.255

D. 192.168.2.2 / 255.255.255.255

Correct Answer: D

QUESTION 4

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

```
STUDENT # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

S    *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
     *>            [10/0] via 10.200.2.254, port2, [5/0]
C    *> 10.0.1.0/24 is directly connected, port3
S       10.0.2.0/24 [20/0] is directly connected, Remote 2
S    *> 10.0.2.0/24 [10/0] is directly connected, Remote_1
C    *> 10.200.1.0/24 is directly connected, port1
C    *> 10.200.2.0/24 is directly connected, port2
```

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

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

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

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

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

Correct Answer: AC

QUESTION 5

Review the static route configuration for IPsec shown in the Exhibit below; then answer the question following it.

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

A. Remote_1 is a Phase 1 object with interface mode enabled

B. The gateway address is not required because the interface is a point-to-point connection

C. The gateway address is not required because the default route is used

D. Remote_1 is a firewall zone

Correct Answer: AB

QUESTION 6

When backing up the configuration file on a FortiGate unit, the contents can be encrypted by enabling the encrypt option and supplying a password.

If the password is forgotten, the configuration file can still be restored using which of the following methods?

A. Selecting the recover password option during the restore process.

B. Having the password emailed to the administrative user by selecting the Forgot Password option.

C. Sending the configuration file to Fortinet Support for decryption.

D. If the password is forgotten, there is no way to use the file.

Correct Answer: D

QUESTION 7

By default, what happens when a log file reaches its maximum file size?

A. FortiAnalyzer overwrites the log files.

B. FortiAnalyzer stops logging.

C. FortiAnalyzer rolls the active log by renaming the file.

D. FortiAnalyzer forwards logs to syslog.

Correct Answer: C

QUESTION 8

Which of the following Regular Expression patterns will make the term "bad language" case insensitive?

A. [bad language]

B. /bad language/i

C. i/bad language/

D. "bad language"

E. /bad language/c

Correct Answer: B

QUESTION 9

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"

Correct Answer: BE

QUESTION 10

A DLP rule with an action of Exempt has been matched against traffic passing through the FortiGate unit.

Which of the following statements is correct regarding how this transaction will be handled by the FortiGate unit?

A. Any other matched DLP rules will be ignored with the exception of Archiving.

B. Future files whose characteristics match this file will bypass DLP scanning.

C. The traffic matching the DLP rule will bypass antivirus scanning.

D. The client IP address will be added to a white list.

Correct Answer: A

QUESTION 11

Setting workspace-mode to normal, as shown in the exhibit, allows what on FortiManager? (Choose two.) config system global set workspace-mode normal end

A. ADOM locking

B. VDOM locking

C. Unrestricted concurrent access

D. Restricted concurrent access

Correct Answer: AD

QUESTION 12

If a FortiGate unit has a dmz interface IP address of 210.192.168.2 with a subnet mask of 255.255.255.0, what is a valid dmz DHCP addressing range?

A. 172.168.0.1 - 172.168.0.10

B. 210.192.168.3 - 210.192.168.10

C. 210.192.168.1 - 210.192.168.4

D. All of the above.

Correct Answer: B

QUESTION 13

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

Correct Answer: A

![Pass2Lead](https://Pass2Lead.com)
QUESTION 14

Refer to the output below. Which statement is correct concerning the duplicate objects?

Start to import config from device (STUDENT-2) vdom (root) to adom (root), package (STUDENT-2)

"firewall service category", SUCCESS, "(name=General, oid=370, DUPLICATE)"

"firewall schedule recurring", SUCCESS, "(name=always, oid=466, DUPLICATE)"

"firewall address", SUCCESS, "(name=all, oid=358, DUPLICATE)"

"firewall service custom", SUCCESS, "(name=ALL, oid=419, DUPLICATE)"

"firewall vip", SUCCESS, "(name=FTP, oid=468, DUPLICATE)"

A. These duplicate objects exist on the same FortiGate device.

B. FortiManager does not import duplicate objects for entries already in the ADOM configuration database.

C. FortiManager is attempting to install these duplicate objects to the managed FortiGate device.

D. FortiManager creates the duplicate objects in the ADOM configuration database.

Correct Answer: B

QUESTION 15

What statements are true regarding disk log quota? (Choose two.)

A. The FortiAnalyzer stops logging once the disk log quota is met.

B. The FortiAnalyzer automatically sets the disk log quota based on the device.

C. The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.

D. The FortiAnalyzer disk quota is configurable, but has a minimum of 100MB and a maximum based on the reserved system space.

Correct Answer: CD

[Latest NSE5 Dumps](#)   [NSE5 Practice Test](#)   [NSE5 Study Guide](#)