

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 : FCNSP

Title : FortiOS 4.0 GA, FortiAnalyzer 4.0
GA(FCNSP v4.0)

Vendors : Fortinet

Version : DEMO

NO.1 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. Any other matched DLP rules are ignored.
- C. The traffic matching the DLP rule will bypass antivirus scanning.
- D. The client IP address will be added to a white list.

Answer: A

NO.2 Which of the following describes the best custom signature for detecting the use of the word "Fortinet" in chat applications.?

The sample packet trace illustrated in the exhibit provides details on the packet that requires detection.

- A. `F-SBID(--protocol tcp; --flow from_client; --pattern "X-MMS-IM-Format"; --pattern "fortinet"; --no_case;)`
- B. `F-SBID(--protocol tcp; --flow from_client; --pattern "fortinet"; --no_case;)`
- C. `F-SBID(--protocol tcp; --flow from_client; --pattern "X-MMS-IM-Format"; --pattern "fortinet"; --within 20; --no_case;)`
- D. `F-SBID(--protocol tcp; --flow from_client; --pattern "X-MMS-IM-Format"; --pattern "fortinet"; --within 20;)`

Answer:A

NO.3 When viewing the Banned User tab in User Monitor in Web Config, the administrator notes the entry

illustrated in the exhibit. Which of the following statements is correct regarding this entry?

- A. The entry displays a ban that has been added as a result of traffic triggering a configured DLP rule.
- B. The entry displays a ban that was triggered by HTTP traffic matching an IPS signature. This client is banned from receiving or sending any traffic through the FortiGate.
- C. The entry displays a quarantine, which could have been added by either IPS or DLP.
- D. This entry displays a ban entry that was added manually by the administrator on Dec 24th.

Answer: A

NO.4 Which of the following statements are correct regarding the antivirus scanning function on the FortiGate unit?

- A. Antivirus scanning can be configured to block certain file types and patterns.
- B. Antivirus scanning provides end-to-end virus protection for client workstations.
- C. Antivirus scanning provides virus protection for the HTTP, Telnet, SMTP, and FTP protocols.
- D. Antivirus scanning supports banned word checking.
- E. Antivirus scanning supports grayware protection.

Answer: AE

NO.5 Which of the following describes the difference between the ban and quarantine actions?

- A. A ban action prevents future transactions using the same protocol which triggered the ban. A quarantine action blocks all future transactions, regardless of the protocol.
- B. A ban action blocks the transaction. A quarantine action archives the data.
- C. A ban action has a finite duration. A quarantine action must be removed by an administrator.
- D. A ban action is used for known users. A quarantine action is used for unknown users.

Answer: A

NO.6 An administrator is examining the attack logs and notices the following entry:

```
attack_id=100663402 src=192.168.0.79 dst=64.64.64.64 src_port=57133 dst_port=80 interface=port3
```

```
src_int=n/a dst_int=n/a status=dropped proto=6 service=http msg="TCP session over limit
```

Based solely upon this log message, which of the following statements is correct?

- A. This attack was blocked by the HTTP protocol decoder.
- B. This attack was caught by the DoS sensor.
- C. This attack was launched against the FortiGate unit itself rather than a host behind the FortiGate unit.
- D. The number of concurrent connections to destination IP address 64.64.64.64 has exceeded the configured threshold.

Answer: B

NO.7 Based on the web filtering configuration illustrated in the exhibit, which one of the

following statements

is not a reasonable conclusion?

- A.Users can access both the www.google.com site and the www.fortinet.com site.
- B.When a user attempts to access the www.google.com site, the FortiGate unit will not perform web filtering on the content of that site.
- C.When a user attempts to access the www.fortinet.com site, any remaining web filtering will be bypassed.
- D.Downloaded content from www.google.com will be scanned for viruses if antivirus is enabled.

Answer: B

NO.8 Which of the following items are considered to be advantages of using the application control features on the FortiGate unit?

- A.Application control provides application detection regardless of the port used by the application.
- B.Application control allows session-ttl to be customized for specific application types.
- C.Application control allows custom application types to be added in a similar way to adding custom IPS signatures.
- D.Application control allows an administrator to check which applications are installed on workstations attempting to access the network.

Answer: AB

NO.9 The transfer of encrypted files or the use of encrypted protocols between users and servers on the

internet can frustrate the efforts of administrators attempting to monitor traffic passing through the

FortiGate unit and ensuring user compliance to corporate rules.

Which of the following items will allow the administrator to control the transfer of encrypted data through the FortiGate unit?

- A.Encrypted protocols can be scanned through the use of the SSL proxy.
- B.DLP rules can be used to block the transmission of encrypted files.
- C.Firewall authentication can be enabled in the firewall policy, preventing the use of

encrypted

communications channels.

D.Application control can be used to monitor the use of encrypted protocols; alerts can be sent to the administrator through email when the use of encrypted protocols is attempted.

Answer: AB

NO.10 Which part of an email message exchange is not inspected by the POP3 and IMAP proxies?

A.TCP connection

B.Protocol commands

C.Message headers

D.Message body

Answer: A