



Cisco

CICSP

Cisco IronPort Certified Security Professional

QUESTION: 57

Which remark about the SSeries native FTP proxy is NOT true?

- A. Access policies may apply to native FTP traffic
- B. Data Loss Prevention policies may apply to native FTP traffic
- C. Authentication is supported in transparent mode
- D. Both active and passive mode FTP is supported
- E. By default, the FTP proxy uses port 8021

Answer: C

QUESTION: 58

The appearance of the string BLOCK_WBRS in the access log means

- A. The proxy blocked access to a site because of a suspicious server response.
- B. The proxy blocked access to a site with low reputation score.
- C. Your appliance or the WBRS key is out of support.
- D. The proxy blocked an outbound request because the client is infected with malware.

Answer: B

QUESTION: 59

Which of the following statements about the DVS engine is true?

- A. The DVS engine generates the WBRS.
- B. The DVS engine is only used for L4 Traffic Monitoring.
- C. The DVS engine can use Webroot and McAfee scanning in parallel.

Answer: C

QUESTION: 60

Which of the following is true about Outbound Malware Scanning?

- A. It has its own policy table.

- B. It is configured as part of IronPort Data Security.
- C. It is configured as part of Access Policies.
- D. It only has global configuration

Answer: C

QUESTION: 61

In the Setup Wizard, the default action taken when Malware is detected is _____.

Answer: monitor

QUESTION: 62

In access policies, object blocking is based only on MIME type.

- A. True
- B. False

Answer: B

QUESTION: 63

A single transaction can be scanned by Webroot, Sophos and McAfee in parallel.

- A. True
- B. False

Answer: A

QUESTION: 64

Which statement is true about WSA user authentication?

- A. WSA supports LDAP, but not NTLM.
- B. A single WSA can have multiple LDAP realms.
- C. WSA supports NTLM, but not LDAP.
- D. A single WSA can have up to two authentication realms: one for LDAP and one for NTLM.

Answer: B

QUESTION: 65

In the Setup Wizard, the default action to take when L4TM detects phone-home activity is _____.

Answer: block

QUESTION: 66

Which of the following is NOT provided by AVC?

- A. Deep IM control
- B. Safe Search
- C. Media bandwidth control
- D. Web usage quotas

Answer: D

Download Full Version From <https://www.certkillers.net>



DON'T KNOW
OR NO PREFERENCE

Pass your exam at First Attempt....Guaranteed!