Vendor: Cisco

Exam Code: 650-155

Exam Name: Cisco IronPort Security Instructor - Web Security (ISIWS)

Version: DEMO
1. Which of the following commands is used to view the cache hit rate? Select exactly 1 answer(s) from the following:
   A. proxystat
   B. proxyconfig
   C. advancedproxyconfig
   D. webcache
   **Answer:** A

2. DRAG DROP
   Match the HTTP response code with the meaning or use.?

   - 401: used when the WSA returns EUNs
   - 403: proxy authentication request
   - 404: web server authentication request
   - 407: page not found

   **Answer:**

   - Select
   - Deselect
3. Which of the following S-Series CLI commands can help troubleshoot WCCP?
   Select exactly 1 answer(s) from the following:
   A. weep debug enable
   B. tail proxylogs
   C. tail accesslogs
   D. show weep
   **Answer:** B

5. Which of the following is a drawback in using McAfee heuristic scanning?
   Select exactly 1 answer(s) from the following:
   A. Heuristic scanning increases the probability of false positives.
   B. Heuristic scanning increases the probability of false negatives.
   C. Heuristic scanning cannot detect new malware with unknown signature.
   D. Heuristic scanning requires a separate license key.
   **Answer:** A

6. For access policies, by default sites with Web reputation scores from what value through 10 are bypass malware scanning? Select exactly 1 answer(s) from the following:
   A. 0
   B. 3
   C. 6
   D. 9
   **Answer:** C

7. What is the S-Series Proxy Bypass List?
Select exactly 1 answer(s) from the following:
A. a list of proxy servers to be bypassed
B. a list of clients and destinations that will bypass the proxy in explicit forward mode
C. a list of user agents exempt from authentication
D. a list of clients and destinations that will bypass the proxy in transparent mode
Answer: D

8. What parameter used by the WSA to distinguish between WCCP services?
Select exactly 1 answer(s) from the following:
A. service ID
B. forwarding method
C. port number
D. return method
Answer: A

9. What WSA CLI command can be used to search for a string in a log?
Select exactly 1 answer(s) from the following:
A. find
B. logview
C. logsearch
D. grep
Answer: D

10. You see the code TCP_MISS in the access log. What does this mean?
Select exactly 1 answer(s) from the following:
A. The requested object was fetched from the WSA disk cache.
B. The requested object was fetched from the WSA memory cache.
C. The requested object was fetched from the remote server.
D. The requested object was fetched from the browser cache.
E. The requested object was not found on the remote server.
Answer: C

11. In the access log, you see an ACL tag beginning with BLOCK_ADMIN. What might be the cause?
Select exactly 1 answer(s) from the following:
A. The destination was manually added to the block list.
B. The transaction was manually blocked by the admin user.
C. The malware category is set to blocking mode.
D. The transaction was blocked because of object properties.
Answer: D

12. What are PAC files used for?
Select exactly 1 answer(s) from the following:
A. transparent mode proxy deployments
B. user-agent based policies  
C. L4TM  
D. explicit forward mode proxy deployments  
**Answer:** D

14. When can the user agent field be used to determine the decryption policy?  
Select exactly 1 answer(s) from the following:  
A. only in explicit forward proxy mode  
B. always  
C. never  
D. only in transparent proxy mode  
**Answer:** B

15. The appearance of the ACL tag BLOCK_WBRS in the access log means what?  
Select exactly 1 answer(s) from the following:  
A. The proxy blocked access to a site with low reputation score.  
B. Your appliance or the WBRS key is out of support.  
C. The proxy blocked an outbound request because the client is infected with malware.