



Securing the Web with Cisco Web Security Appliance (SWSA)



EXAMKILLER

Help Pass Your Exam At First Try



Exam 300-725

Securing the Web with Cisco Web Security Appliance (300-725 SWSA)

Version: 3.0

[Total Questions: 60]

Question No : 2

Question No : 3

- A. The log does not have a date and time
- B. The proxy had the content and did not contact other servers
- C. The transaction used TCP destination port 8187
- D. The AnalyzeSuspectTraffic policy group was applied to the transaction

Answer: D

Question No : 4

Which two parameters are mandatory to control access to websites with proxy authentication on a Cisco WSA? (Choose two.)

- A. External Authentication
- B. Identity Enabled Authentication
- C. Transparent User Identification
- D. Credential Encryption
- E. Authentication Realm

Answer: D,E

Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_appendix_010111.html

Question No : 5

Which action is a valid default for the Global Access Policy in the Application Visibility Control engine on the Cisco WSA?

- A. bandwidth limit
- B. permit
- C. restrict
- D. monitor

Answer: D

Reference: <https://hrouhani.org/cisco-web-security-appliance-ironport/>

Question No : 6

Which type of FTP proxy does the Cisco WSA support?

- A. non-native FTP
- B. FTP over UDP tunneling
- C. FTP over HTTP
- D. hybrid FTP

Answer: C

Reference: <https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117984-qanda-wsa-00.html>

Question No : 7

What causes authentication failures on a Cisco WSA when LDAP is used for authentication?

- A. when the passphrase contains only 5 characters
- B. when the passphrase contains characters that are not 7-bit ASCII
- C. when the passphrase contains one of following characters '@ # \$ % ^'
- D. when the passphrase contains 50 characters

Answer: B

Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_appendix_011001.html

Question No : 8

What is the function of a PAC file on a Cisco WSA?

- A. The file allows redirection of web traffic to a specific proxy server
- B. The file is mandatory for a transparent proxy to redirect user traffic
- C. The file provides instructions about which URL categories are permitted
- D. The file is mandatory for an explicit proxy to forward user traffic

Answer: A

Reference: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/116052-config-webauth-proxy-00.html>

Question No : 9

Which two features can be used with an upstream and downstream Cisco WSA web proxy to have the upstream WSA identify users by their client IP address? (Choose two.)

- A. X-Forwarded-For
- B. high availability
- C. web cache
- D. via
- E. IP spoofing

Answer: A,D

Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_0100.html

Question No : 10

Which two sources provide data to Cisco Advanced Web Security Reporting to create dashboards? (Choose

two.)

- A. Cisco WSA devices
- B. Cisco ISE
- C. Cisco ASA
- D. Cisco Security MARS
- E. Cisco Cloud Web Security gateways

Answer: A,E

Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/wsa/Advanced_Reporting/WSA_Advanced_Reporting_6/Advanced_Web_Security_Reporting_6_1.pdf

Question No : 11

Which statement about configuring an identification profile for machine authentication is true?

- A. Cloud Web Security Connector mode with an active directory enabled supports machine authentication
- B. Identification profile machine ID is supported locally, but the Cisco WSA does not support machine ID authentication
- C. Cloud Web Security with Kerberos enabled supports machine authentication
- D. If an Active Directory realm is used, identification can be performed for an authenticated user or IP address but not for a machine ID

Answer: C

Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01001.html

Question No : 12 DRAG DROP

Drag and drop the Cisco WSA access policy elements from the left into the order in which they are processed on the right.

Answer Area

custom URL category	action 1
malware scanning	action 2
MIME type filter	action 3
application filter	action 4
URL category	action 5

Answer:

Answer Area

custom URL category	application filter
malware scanning	MIME type filter
MIME type filter	malware scanning
application filter	URL category
URL category	custom URL category

Question No : 13 CORRECT TEXT

Which port is configured in a browser to use the Cisco WSA web proxy with default settings?

- B.8443
- C.8021
- D.3128

Answer: D

Question No : 14

Which behavior is seen while the policy trace tool is used to troubleshoot a Cisco WSA?

- A. External DLP policies are evaluated by the tool
- B. A real client request is processed and an EUN page is displayed
- C. SOCKS policies are evaluated by the tool
- D. The web proxy does not record the policy trace test requests in the access log when the tool is in use

Answer: D

Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_appendix_011001.html#con_1415277

Question No : 15

What is required on the Cisco WSA when an AMP file reputation server private cloud is configured?

- A. private key from the server to encrypt messages
- B. private key to decrypt messages
- C. public and private keys from the server
- D. public key from the server

Answer: D

Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010001.html

Question No : 16

By default, which two pieces of information does the Cisco WSA access log contain? (Choose two.)

- A. HTTP Request Code
- B. Content Type
- C. Client IP Address
- D. User Agent
- E. Transaction ID

Answer: A,C

Question No : 17

Which two caches must be cleared on a Cisco WSA to resolve an issue in processing requests? (Choose two.)

- A. authentication cache
- B. application cache
- C. logging cache
- D. DNS cache
- E. HTTP cache

Answer: A,D

Reference: <https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118259-technote-wsa-00.html>

Question No : 18

Which statement about Cisco Advanced Web Security Reporting integration is true?

- A. AWSR uses IP addresses to differentiate Cisco WSA deployments
- B. AWSR does not require a license to index data
- C. AWSR can remove log files after they are indexed
- D. AWSR installation is CLI-based on Windows and Red Hat Linux systems

Answer: D

Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/wsa/Advanced_Reporting/WSA_Advanced_Reporting_7/Advanced_Web_Security_Reporting_7_0.pdf

Question No : 19

A user browses to a company website that is categorized as “Business and Industry” and contains a Facebook post. The user cannot see the Facebook post because the category “Social Networking” is blocked.

Which configuration allows the user to see the Facebook post?

- A)