

300-725^{Q&As}

Securing the Web with Cisco Web Security Appliance (SWSA)

Pass Cisco 300-725 Exam with 100% Guarantee

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

<https://www.leads4pass.com/300-725.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers



QUESTION 1

What is the primary benefit of using Cisco Advanced Web Security Reporting?

- A. ability to see the malicious activity of a user
- B. L4TM report with client-malware risk
- C. centralized and granular reporting
- D. access to a day report with historical data

Correct Answer: B

Reference: https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/datasheet_c78-729104.html

QUESTION 2

Which two log types does the Cisco WSA provide to troubleshoot Cisco data security and external data loss prevention policies? (Choose two.)

- A. upload data
- B. data security
- C. default proxy
- D. data access
- E. external data

Correct Answer: CE

Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010011.html

QUESTION 3

Which method is used by AMP against zero-day and targeted file-based attacks?

- A. analyzing behavior of all files that are not yet known to the reputation service
- B. periodically evaluating emerging threats as new information becomes available
- C. implementing security group tags
- D. obtaining the reputation of known files

Correct Answer: D

Reference: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html>

QUESTION 4

1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain DEFAULT_CASE_11-AnalyzeSuspectTraffic-Identity-OutboundMalwareScanningPolicy-DataSecurity Policy-ExternalDLPPolicy-Routing Policy
!IW_comp,6.9,-,"-, -, -, -, "-", "-","-", "IW_comp,-,"-, "-", "
["Unknown"], ["Unknown"], "-", " ", 198.34.0,-,[Local], "-", 37, "W32.CiscoTestVector", 33, 0,
"WSA-INFECTED-FILE.pdf"; "fd5ef49d4213e05f448f1ed9c98253d85829614fba368a421d14e64c426da5e"> -

Refer to the exhibit. Which statement about the transaction log is true?

- 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

Correct Answer: D

QUESTION 5

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

Correct Answer: C

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

QUESTION 6

What must be configured to require users to click through an acceptance page before they are allowed to go to the Internet through the Cisco WSA?

- A. Enable End-User Acknowledgement Page and set to Required in Identification Profiles
- B. Enable End -User URL Filtering Warning Page and set to Required in Identification Profiles
- C. Enable End-User Acknowledgement Page and set to Required in Access Policies

D. Enable End-User URL Filtering Warning Page and set to Required in Access Policies

Correct 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_010100.html

QUESTION 7

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

Correct Answer: AC

QUESTION 8

Which type of certificate must be installed on a Cisco WSA for HTTPS inspection?

- A. server
- B. client
- C. root
- D. wildcard

Correct Answer: C

Reference: <https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117792-technote-wsa-00.html>

QUESTION 9

Which two benefits does AMP provide compared to the other scanning engines on the Cisco WSA? (Choose two.)

- A. protection against malware
- B. protection against zero-day attacks
- C. protection against spam
- D. protection against viruses

E. protection against targeted file-based attacks

Correct Answer: AB

Reference: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html>

QUESTION 10

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

Correct 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 11

Which key is needed to pair a Cisco WSA and Cisco ScanCenter for CTA?

- A. public SSH key that the Cisco WSA generates
- B. public SSH key that Cisco ScanCenter generates
- C. private SSH key that Cisco ScanCenter generates
- D. private SSH key that the Cisco WSA generates

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010111.html

QUESTION 12

An administrator wants to restrict file uploads to Facebook using the AVC feature.

Under which two actions must the administrator apply this restriction to an access policy? (Choose two.)

- A. Monitor Facebook General
- B. Monitor Social Networking

C. Monitor Facebook Photos and Videos

D. Monitor Facebook Messages and Chat

E. Monitor Facebook Application

Correct Answer: AC

Reference: <https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/datasheet-c78-741272.html>

QUESTION 13

DRAG DROP

Drag and drop the Cisco WSA methods from the left onto the correct deployment modes on the right.

Select and Place:

WPAD	Transparent Mode
WCCP	
PAC	Explicit Mode
PBR	

Correct Answer:

	Transparent Mode
	Explicit Mode

	WCCP
	PBR
	PAC
	WPAD

You could use an explicit setting (browser config/PAC/WPAD) or transparent (WCCP/PBR) to point to the first proxy and then the first proxy will route based on category to one of the two upstream proxies based on your policy configuration. Reference: <https://community.cisco.com/t5/web-security/route-to-wsa-based-on-destination/td-p/2491179>

QUESTION 14

Which information within Cisco Advanced Web Security Reporting is used to generate a report that lists visited domains?

- A. URL categories
- B. web reputation
- C. websites
- D. application visibility

Correct Answer: A

Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/wsa/Advanced_Reporting/WSA_Advanced_Reporting_6/Advanced_Web_Security_Reporting_6_6.pdf (39)

QUESTION 15

Which two types of reports are scheduled on the Cisco WSA to analyze traffic? (Choose two.)

- A. Layer 3 traffic monitor
- B. URL categories
- C. host statistics
- D. application visibility
- E. system capacity

Correct Answer: AD

Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010101.pdf (8)

[Latest 300-725 Dumps](#)

[300-725 PDF Dumps](#)

[300-725 Braindumps](#)