

Exam	300-725
Title	Securing the Web with Cisco Web Security Appliance
Updated	Version 8.1
Product Type	60 Q&A With Explanation

QUESTION 1**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:

WPAD	Transparent Mode
WCCP	
PAC	Explicit Mode
PBR	

Section: (none) Explanation

Explanation/Reference:

Explanation:

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 2

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

A. when the passphrase contains only 5 characters

QUESTION 5**DRAG DROP**

Drag and drop the properties from the left onto the correct advanced web proxy setting descriptions on the right.
Select and Place:

Answer Area

In-Use Connection Timeout	maximum time (in seconds) that the web proxy keeps open a connection to a client or server after a transaction has been completed and no further activity is detected
Simultaneous Persistent Connections	maximum time (in seconds) that the web proxy waits for more data from an idle client or server when the current transaction has not yet been completed
Use Received Headers	maximum number of TCP sockets that the web proxy keeps open with servers
Persistent Connection Timeout	allows an upstream web proxy to identify clients by IP address

Correct Answer:

Answer Area

In-Use Connection Timeout	Persistent Connection Timeout
Simultaneous Persistent Connections	In-Use Connection Timeout
Use Received Headers	Simultaneous Persistent Connections
Persistent Connection Timeout	Use Received Headers

Section: (none) Explanation

Explanation/Reference:

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 6

Which two configuration options are available on a Cisco WSA within a decryption policy? (Choose two.)

- A. Pass Through
- B. Warn
- C. Decrypt
- D. Allow
- E. Block

Answer: A,C

Section: (none) Explanation

Explanation/Reference:

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_chapter_01011.html

QUESTION 7

Which information in the HTTP request is used to determine if it is subject to the referrer exceptions feature in the Cisco WSA?

- A. protocol
- B. version
- C. header
- D. payload

Answer: C

Section: (none) Explanation

Explanation/Reference:

Explanation:

Requests for embedded content usually include the address of the site from which the request originated (this is known as the "referrer" field in the request's HTTP header). This header information is used to determine categorization of the referred content.

Reference https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01100.html

QUESTION 8

What is used to configure WSA as an explicit proxy?

- A. IP Spoofing from router
- B. Network settings from user browser
- C. WCCP redirection from firewall
- D. Auto redirection using PBR from switch

Answer: B

Section: (none) Explanation

Explanation/Reference:

Reference: <https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.html>

QUESTION 9

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

Answer: A

Section: (none) Explanation

Explanation/Reference:

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 10

What is a benefit of integrating Cisco Cognitive Threat Analytics with a Cisco WSA?

- A. It adds additional information to the Cisco WSA reports
- B. It adds additional malware protection to the Cisco WSA
- C. It provides the ability to use artificial intelligence to block viruses
- D. It reduces time to identify threats in the network

Answer: B

Section: (none) Explanation

Explanation/Reference:

QUESTION 11

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

Answer: D

Section: (none) Explanation

Explanation/Reference:

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

QUESTION 12

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

- A. External DLP polices 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

Section: (none) Explanation

Explanation/Reference:

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 13

What are all of the available options for configuring an exception to blocking for referred content?

- A. all embedded/referred and all embedded/referred except
- B. selected embedded/referred except, all embedded/referred, and selected embedded/referred
- C. selected embedded/referred and all embedded/referred except
- D. all embedded/referred, selected embedded/referred, and all embedded/referred except

Answer: D

Section: (none) Explanation

Explanation/Reference:

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_chapter_01001.html (procedure)

QUESTION 14

Which statement about the SOCKS proxy is true?

- A. SOCKS is a general purpose proxy
- B. SOCKS operates on TCP port 80, 443, and 8334
- C. SOCKS is used only for traffic that is redirected through a firewall
- D. SOCKS is used for UDP traffic only

Answer: A

Section: (none) Explanation

Explanation/Reference:

Reference: <http://www.jguru.com/faq/view.jsp?EID=227532>

QUESTION 15

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

Section: (none) Explanation

Explanation/Reference:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-](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)

[7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_appendix_010111.html](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 16

What is a valid predefined time range when configuring a Web Tracking query?

- A. year
- B. minute
- C. hour
- D. month

Answer: B

Section: (none) Explanation

Explanation/Reference:

Explanation:

Web tracking query uses minute as a predefined time range to track web related queries.

QUESTION 17

When a Cisco WSA is installed with default settings, which port is assigned to the web proxy if the M1 port is used exclusively for management?

- A. T1
- B. P2
- C. T2
- D. P1

Answer: D

Section: (none) Explanation

Explanation/Reference:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-](https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-5/user_guide/b_WSA_UserGuide_11_5_1/b_WSA_UserGuide_11_5_1_chapter_01.html)

[5/user_guide/b_WSA_UserGuide_11_5_1/b_WSA_UserGuide_11_5_1_chapter_01.html](https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-5/user_guide/b_WSA_UserGuide_11_5_1/b_WSA_UserGuide_11_5_1_chapter_01.html)

QUESTION 18

Which configuration option is suitable for explicit mode deployment?

- A. PAC
- B. WCCP
- C. ITD
- D. PBR

Answer: A

Section: (none) Explanation

Explanation/Reference:
