



**Free Questions for 300-725 by ebraindumps**

**Shared by Mayo on 24-05-2024**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

---

**Question Type:** MultipleChoice

---

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

**Options:**

---

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

**Answer:**

---

C

**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](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 2

---

**Question Type:** MultipleChoice

---

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

### Options:

---

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

### Answer:

---

A, C

**Explanation:**

---

[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](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 3

---

**Question Type: DragDrop**

---

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

## Answer Area

<b>Answer:</b> 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
<b>Explanation:</b> Simultaneous Persistent Connections <a href="https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/wsa11-0-ug.html#chapter_0100">https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/wsa11-0-ug.html#chapter_0100</a>	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
<b>Question Type:</b> Multiple Choice Persistent Connection Timeout	allows an upstream web proxy to identify clients by IP address

## Question 4

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.)

### Options:

A- X-Forwarded-For

**B-** high availability

**C-** web cache

**D-** via

**E-** IP spoofing

**Answer:**

---

A, D

**Explanation:**

---

[https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user\\_guide/b\\_WSA\\_UserGuide/b\\_WSA\\_UserGuide\\_chapter\\_0100.html](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 5

---

**Question Type:** MultipleChoice

---

Refer to the exhibit.

```
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","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e"> -
```

Which statement about the transaction log is true?

**Options:**

---

- 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 6

---

**Question Type: MultipleChoice**

---

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

**Options:**

---

- 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

**Explanation:**

---

[https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user\\_guide/b\\_WSA\\_UserGuide/b\\_WSA\\_UserGuide\\_appendix\\_011001.html](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 7

---

Question Type: DragDrop

---

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

WPAD
WCCP
<b>Answer:</b>
PAC
<b>Explanation:</b>
PBR

Transparent Mode

Explicit Mode

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.

<https://community.cisco.com/t5/web-security/route-to-wsa-based-on-destination/td-p/2491179>

## Question 8

---

Question Type: MultipleChoice

---

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

**Options:**

---

- 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

**Explanation:**

---

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

## Question 9

---

**Question Type: MultipleChoice**

---

What is the purpose of using AMP file analysis on a Cisco WSA to continuously evaluate emerging threats?

**Options:**

---

- A-** to take appropriate action on new files that enter the network
- B-** to remove files from quarantine by stopping their retention period
- C-** to notify you of files that are determined to be threats after they have entered your network
- D-** to send all files downloaded through the Cisco WSA to the AMP cloud

**Answer:**

---

C

**Explanation:**

---

[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\\_01110.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_01110.html)

## Question 10

---

**Question Type: MultipleChoice**

---

What is a benefit of integrating Cisco WSA with TrustSec in ISE?

**Options:**

---

- A-** The policy trace tool can be used to match access policies using specific SGT
- B-** Traffic of authenticated users who use 802.1x can be tagged with SGT to identification profiles in a Cisco WSA
- C-** ISE can block authentication for users who generate multiple sessions using suspect TCP ports
- D-** Users in a specific SGT can be denied access to certain social websites.

**Answer:**

---

D

**Explanation:**

---

[https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/ISE-WSAIntegrationDoc/b\\_ISE-WSAIntegration.html](https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/ISE-WSAIntegrationDoc/b_ISE-WSAIntegration.html)

**Question 11**

---

**Question Type: MultipleChoice**

---

What is used to configure WSA as an explicit proxy?

**Options:**

---

- 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

**Explanation:**

---

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

**To Get Premium Files for 300-725 Visit**

**<https://www.p2pexams.com/products/300-725>**

**For More Free Questions Visit**

**<https://www.p2pexams.com/cisco/pdf/300-725>**

