Cisco

Exam 700-281

Web Security for Field Engineers

Version: 6.2

[Total Questions: 50]

Question No : 1 DRAG DROP

Put the following features in the order they are applied.

McAfee anti-malware scanning	
Web Reputation Filters	
Protocol check	
URL Filters	

Answer:

McAfee anti-malware scanning	Protocol check
Web Reputation Filters	URL Filters
Protocol check	Web Reputation Filters
URL Filters	McAfee anti-malware scanning

Question No : 2

Why does L4TM require T1 to be in promiscuous mode?

A. To transmit TCP reset packets
B. To process traffic that is not intended for its MAC address
C. To receive Ethernet broadcasts
D. To bind with other promiscuous mode ports

Answer: B

Question No : 3

Which action does Dynamic Content Analysis enable the Web Security Appliance to do?

A. Reclassify miscategorized sites.
B. Determine the most likely category of the website delivering content.
C. Block web content based on the Web Reputation of the serving site.
D. Choose the best AV engine to scan content.
E. Redirect the user to a site that the security administrator chooses.

Answer: B

Explanation:

http://www.cisco.com/c/en/us/products/collateral/security/web-security-

appliance/datasheet_C78-718442.html

Question No : 4

In the access log, what does an ACL tag beginning with BLOCK_ADMIN indicate?

A. The transaction was blocked because of application or object properties.
B. The malware category is set to blocking mode.
C. The transaction was manually blocked by the administrative user.
D. The destination was manually added to the block list.

Answer: A

Question No : 5

You are helping the customer configure authentication. A new AsyncOS upgrade becomes
available; what should you do?