

Cisco 700-281 Exam

Volume: 50 Questions

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

Cisco 700-281 Exam

- 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

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: C

Question No: 5

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

- A. Avoid mentioning the upgrade to the customer.

Cisco 700-281 Exam

- B. Immediately show the customer how to run the CLI command upgrade.
- C. Contact customer support and ask them to run the upgrade for you.
- D. Schedule a convenient time to upgrade again, backing up the configuration before and after the upgrade.

Answer: D

Question No: 6

Which of these cannot be used in defining policies?

- A. User agent
- B. Proxy port
- C. Usage quotas
- D. Time of day

Answer: C

Question No: 7

If authentication is enabled, which statement is true?

- A. Client reports will display both the username and IP address of the clients
- B. Client reports will display the IP address of the authentication server.
- C. Client reports are not affected by authentication.
- D. Client reports will display authenticated usernames.

Answer: D

Question No: 8

What is "stream scanning"?

- A. scanning streaming media for malware

Cisco 700-281 Exam

- B. passing pieces of a download to the client while the download is being scanned
- C. scanning multiple downloads at the same time
- D. passing scanned pieces of the file between two different malware-scanning engines

Answer: B

Question No: 9

Which of these is not used as a monitoring tool?

- A. CLI commands
- B. email alerts
- C. SNMP traps
- D. policy trace

Answer: D

Question No: 10

Which option describes how a user enables licensed features on the virtual WSA?

- A. from the CLI using the featurekey command
- B. from the CLI using the loadlicense command
- C. from the CLI using the update command
- D. from the GUI using the System Administration/Feature Keys menu page
- E. from the GUI using the System Administration/Feature Key Settings menu page

Answer: B

Question No: 11

Which option describes the Cisco best practice for configuration of the Web Usage Control feature?

- A. To configure the Global Policy as the most restrictive

Cisco 700-281 Exam

- B. To configure the Global Policy as the least restrictive
- C. To configure every access policy using the inherited attributes from the Global Policy
- D. To leave all actions in the Global Policy set to Monitor

Answer: C

Question No: 12

What does the appearance of the ACL tag BLOCK_WBRS in the access log mean?

- A. Your appliance or the WBRS key is out of support.
- B. The proxy blocked an outbound request because the client is infected with malware
- C. The proxy blocked access to a site because of a suspicious server response.
- D. The proxy blocked access to a site with a low reputation score.

Answer: D

Question No: 13

Which option describes the Cisco best practice for using authentication-based access policies?

- A. It should be used as the Global Policy.
- B. It should be used above nonauthenticating access policies in the Web Security Manager/Access Policies menu page
- C. It should be used below nonauthenticating access policies in the Web Security Manager/Access Policies menu page.
- D. It should be used as the only policy.

Answer: B

Question No: 14

If you want to create a ScanSafe filter that will block any shopping or gambling website, what should you add to the filter?