Exam Number/Code:700-281

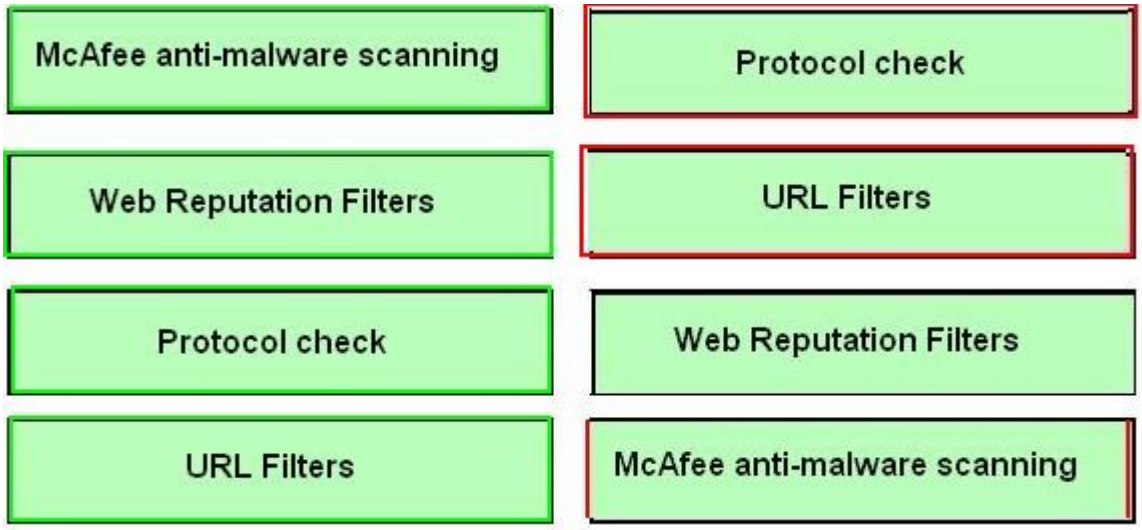
Exam Name: Web Security for Field Engineers

Version: Demo

QUESTION:1

Put the following features in the order they are applied.

Answer:



QUESTION: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: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: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: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.
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: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: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:8

What is "stream scanning"?

A. scanning streaming media for malware
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: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: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
Explanation:
http://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisc o_Content_Security_Virtual_Appliance_Install_Guide.pdf (Page no. 6)