Cisco

Exam 700-280

Email Security for Field Engineers

Verson: Demo

[Total Questions: 10]

Question No : 1

Which option describes when a DLP incident occurs?

A. when potentially sensitive content appears in a message
B. when one or more users receive classified information via email
C. when a system administrator fails to enable the DLP feature key
D. if a message contains a number that looks like a credit card number

Answer: A

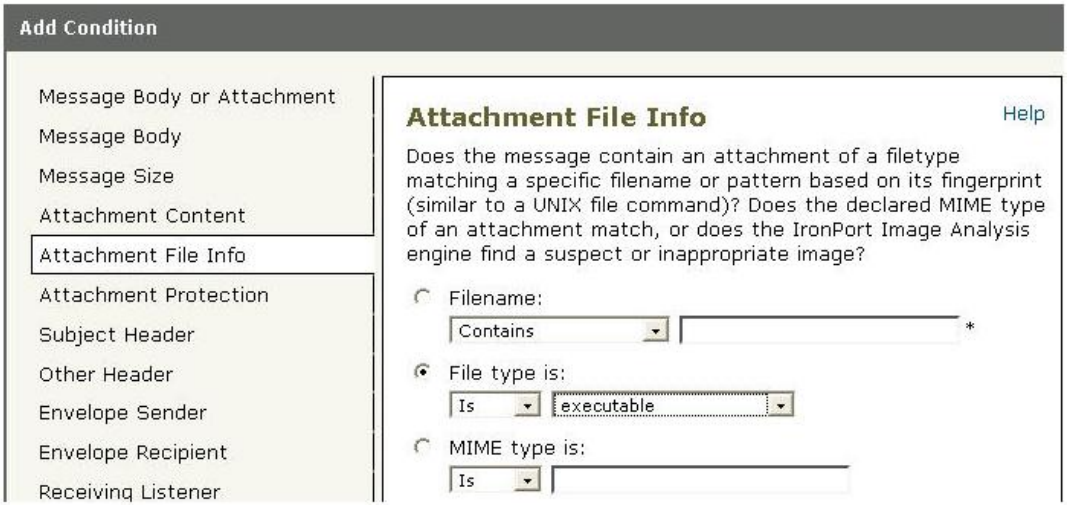
Question No : 2

Which option is the proper syntax of the nslookup command in the Cisco ESA CLIto list mail exchangers for domain "cisco.com"?

A. nslookup -d cisco.com -t mx
B. nslookup mx cisco.com
C. nslookup -type=mx cisco.com
D. nslookup cisco.com mx

Answer: B

Question No : 3



Refer to the exhibit. Based on the Add Condition menu which of listed file attachments will

be matched? (Choose two.)

A. A .msi attachment that has had its file extension changed to .pdf
B. A .pdf attachment that has had its file extension changed to .exe.
C. A.pdf attachment
D. A .exe attachment.

Answer: B,D

Question No : 4

Which content cannot be blocked by content filters?

A. RSADLP failure
B. DKIM failure
C. SPF failure
D. credit card numbers

Answer: A,B

Question No : 5

Your customer has the default spam settings on their appliance. They need an immediate reduction in missed spam, but without increasing their false positive rate. How should you advise them?

A. Enable Intelligent Multi-Scan
B. Enable Marketing Mail Detection.
C. In the HAT settings, increase the SBRS threshold for the BLACKLIST sender group.
D. Advise their end users to use the spam plugin or send false negatives samples to ham@access.ironport.com

Answer: A

Explanation:

IronPort Intelligent Multi-Scan incorporates multiple anti-spam scanning engines, including IronPort Anti-Spam, to provide an intelligent, multi-layer anti-spam solution. This method provides more accurate verdicts that increase the amount of spam that is caught but without increasing the false positives rate.
Reference:http://www.cisco.com/en/US/docs/security/esa/esa7.1/config_guide/ESA_7.1.1_

Configuration_Guide.pdf

Question No : 6

If the marketing message detection feature mislabels legitimate mail as marketing, which action corrects this error?

A. Turn off Marketing Message Detection.
B. Whitelistthe domains that send the mislabeled messages.
C. Send samples of mislabeled legitimate mail to ham@access.ironport.com.
D. Send samples of mislabeled legitimate mail to adds@access.ironport.com.

Answer: C

Question No : 7

Which statement describes how the Cisco Email Security Appliance connects to these hosts if multiple LDAP servers are specified for a single profile?

A. Load balancing or failover operation is configurable in the LDAP server profile.
B. It load balances or fails over depending on the LDAP server priority value.
C. It fails over in the order listed.
D. It load balances connections among all hosts listed.

Answer: D

Question No : 8

At what point in the SMTP conversation can the SMTP client send message headers?

A. Between RCPTTO and DATA
B. Between HELO and MAIL FROM
C. Between DATA and a period"." on a single line
D. Between MAIL FROM and RCPTTO

Answer: C

Question No : 9

In a "one armed installation" using a single listener, how would the system differentiate between incoming and outgoing email?

A. Mail flow direction is determined by the "Recipient to" field in the SMTP envelope.
B. Mail flow direction is determined by the type of listener, public verses private.
C. Mail flow direction is determined by using the source IP address.
D. Mail flow direction is determined by the "Mail From" field in the SMTP envelope.

Answer: C

Question No : 10

During which stage in a mail flow on a Cisco Email Security Appliance does content filtering occur?

A. Reputation filtering (SBRS) > message filters > antispam > antivirus > content filter > mail policies
B. Reputation filtering (SBRS) > message filters > mail policies > antispam > antivirus > content filter
C. Reputation filtering (SBRS) > message filters > content filter > mail policies > antispam > antivirus
D. Reputation filtering (SBRS) > mail policies > message filters > antispam > antivirus > content filter

Answer: D