Cisco

Exam 650-153

ESFE Cisco Email Security Field Engineer Specialist

Version: 8.2

[Total Questions: 111]

Question No : 1

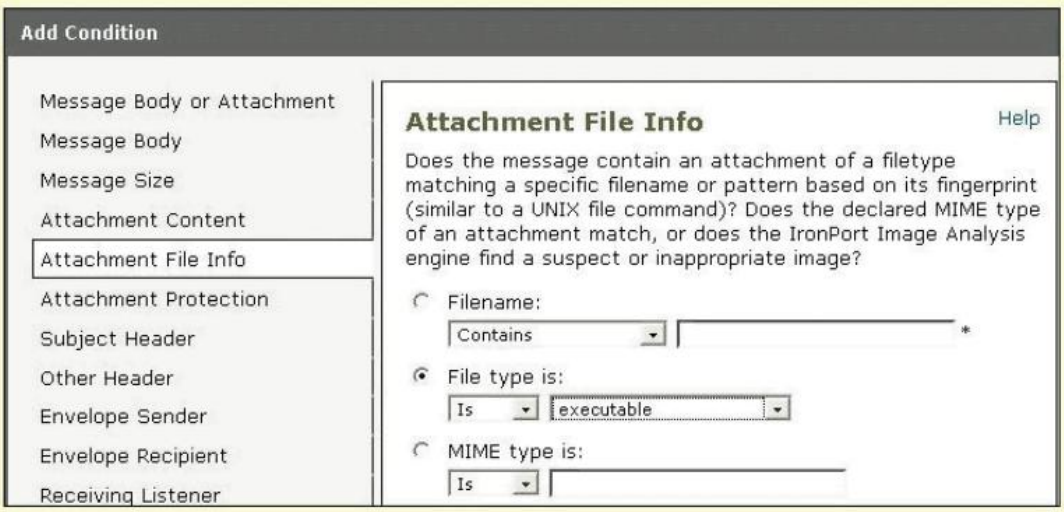
In the C-160's factory default configuration, which interface has ssh enabled by default on the 192.168.42.42 address?

A. Data 2
B. Data 1
C. None. SSH must be first enabled through the console.
D. Management

Answer: B

Question No : 2

Refer to the exhibit.



Based on the Add Condition menu which of listed file attachments will be matched? (Choose two.)

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

Answer: B,D

Question No : 3

How can C-Series archived reports be retrieved?

A. They cannot be retrieved, since the reporting information is deleted and data is collected for the next reporting period.
B. Archived reports are retrieved by going to ftp://mgmt.<C-Series host name>.com
C. Archived reports can be retrieved through the GUI by going to: Monitor > Archived Reports

Answer: C

Question No : 4

Which of the following choices shows the GUI menu path for importing a content dictionary to be used in an Incoming content filter?

A. Mail Policies > Dictionaries > Add Dictionary
B. System Administration > Configuration Directory > Import Dictionary
C. Mail Policies > Dictionaries > Import Dictionary
D. Mail Policies > Incoming Mail Policies > Dictionaries > Import Dictionary

Answer: C

Question No : 5

You have finished installing a C-160 that is designed to filter incoming and relay outgoing mail for the mail server exchange.bravo.com. This is a one armed installation. For some reason, outgoing mail cannot be delivered. According to the mail log, what is the most likely problem?

```
Fri Sep 25 17:07:46 2009 Info: New SMTP ICID 3451 interface Data 1 (192.168.10.102) addre
ss 172.20.0.10 reverse dns host exchange.inside.com verified yes
Fri Sep 25 17:07:46 2009 Info: ICID 3451 ACCEPT SG SUSPECTLIST match sbrs[-3.0:-1.0] SBRS
 -2.7
Fri Sep 25 17:07:46 2009 Info: Start MID 11938 ICID 3451
Fri Sep 25 17:07:46 2009 Info: MID 11938 ICID 3451 From: <ProprietaryToOutside@Outside.CO
M>
Fri Sep 25 17:07:46 2009 Info: MID 11938 ICID 3451 To: <brad@outside.com> Rejected by RAT
Fri Sep 25 17:07:46 2009 Info: ICID 3451 lost
Fri Sep 25 17:07:46 2009 Info: Message aborted MID 11938 Receiving aborted
Fri Sep 25 17:07:46 2009 Info: Message finished MID 11938 aborted
Fri Sep 25 17:07:46 2009 Info: ICID 3451 close
```

A. exchange.bravo.com needs to be configured in the RAT
B. exchange.bravo.com needs to be configured on the RELAYLIST
C. An SMTP route needs to be configured for exchange.inside.com
D. The mail server needs to point to a private listener.
E. exchange.bravo.com needs to be removed from the SUSPECTLIST

Answer: B

Question No : 6

Which of the following filters can only be applied to outbound messages?

A. Anti-Virus
B. DLP
C. Outbreak
D. Anti-Spam

Answer: B

Question No : 7

Which of the following parameters are used by the Anti-Spam engine? (Choose three.)

A. The number of recipients in the RCPT TO list.
B. Analysis of image content using optical character recognition
C. The characteristics of the message (random dots, multiple colors)
D. The reputation of URLs in the message
E. The sending mail domains reputation

Answer: C,D,E

Question No : 8

Which one of the following cannot be performed on the M-Series, when using it to support a C-Series?

A. Centralized message tracking
B. Centralized spam quarantining
C. Centralized Configuration Management
D. Centralized Reporting

Answer: A

Question No : 9

You have established connectivity to a factory default C-160 through the CLI, What command will allow you to change an interfaces speed and duplex?

A. ifconfig
B. interfaceconfig
C. etherconfig
D. mediaccnfig

Answer: C

Question No : 10

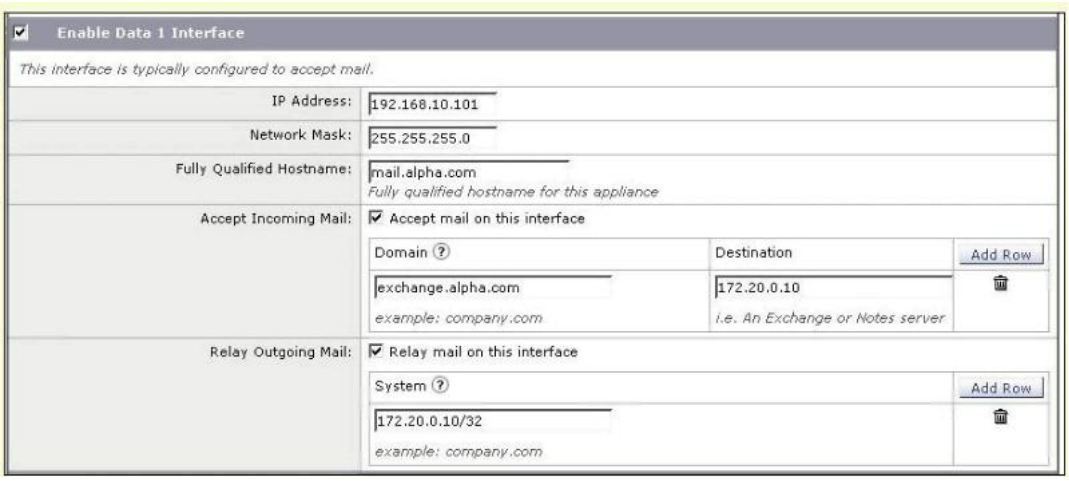
By default, the outgoing mail will be scanned by which one of the following?

A. Anti-Spam
B. Anti-Virus
C. Outbreak Filters
D. Reputation Filters

Answer: B

Question No : 11

Refer to the wizard screenshot.



In the system setup wizard, when configuring the Data 1 interface to accept mail from the internet, which of the following will be displayed in the SMTP banner?

A. Destination
B. Domain
C. Fully Qualified Hostname
D. IP address

Answer: C

Question No : 12

An organization has a single mail domain; exchange.bravo.com. Within this domain are several departments finance, accounting etc. Alan and Brian are in finance. Alice and Brenda are in accounting. You need to suggest a method for applying mail policies to members of finance that are different than members of accounting. What is the best solution?

A. On the C-Series, create individual mail policies for each department and enter their mailbox addresses into their corresponding department policy.
B. Move the members of accounting onto a different mail server; notes.bravo.com. and define its mail domain in the RAT and SMTP route table. Now Alice will have the mailbox alice@notes.bravo.com. Next create a mail policy for accounting that matches on this new domain and applies restrictions for accounting.
C. Define an employee's department membership in a group attribute of LDAP directory. On the C-Series, create individual mail policies for each department that reference group membership through an LDAP group query, and then apply that department's restrictions.
D. On the C-Series, create individual content filters for each department. Create a content dictionary for each department that contains their mailbox addresses. Reference these

dictionaries to determine a match on that department member and then apply the appropriate department restrictions in the action menu.

Answer: C

Question No : 13

When setting up a mail flow policy, two of the choices for connection behavior are "ACCEPT" and "RELAY". Select the following choice that describes the difference between these.

A. ACCEPT will check the "mail from" field against the HAT.
B. ACCEPT will check the "rcpt to" field against the HAT.
C. ACCEPT will check the "rcpt to" field against the RAT
D. ACCEPT will check the "mail from" field against the RAT.

Answer: C

Question No : 14

A large enterprise customer, whose domain name is csu.edu, needs to create a report on incoming and outgoing mail from either internal domains math.csu.edu or hum.csu.edu. How will you advise them?

A. Configure localized reporting and create scheduled domain reports.
B. Configure localized reporting and create scheduled outgoing senders: domains report.
C. Configure centralized reporting and create scheduled domain reports.
D. Configure localized reporting and create scheduled executive summary report.

Answer: C

Question No : 15

How does a customer report emails that are falsely classified as spam and quarantined by the C-Series appliance? (Choose two.)

A. Send the spam as an attachment in RFC 822 format to spam@access.ironport.com

B. Send the spam as an attachment in RFC 822 format to ham@access.ironport.com
C. Use the Submission plugin to submit this email back to IronPort.
D. Open a case for this problem and attach the spam to an RFC 822 format..

Answer: B,D

Question No : 16

Which of the following CLI commands will configure the default route?

A. setgateway
B. setdefaultroute
C. ip route 0.0.0.0 0.0.0.0

Answer: A

Question No : 17

Which of the following RAT entries will accept mail for example.com and all of its sub-domains? Select two.

A. example.com
B. .example.com
C. *©example.com
D. *©*.example.com

Answer: A,B

Question No : 18

One of the items on the Pre-Install Worksheet is "Create DNS records for default the hostname". Which of the following sections in the work sheet contains this item?

A. Action Items
B. Contact Information
C. Current Email Topology
D. Functionality Desired

Answer: A

Question No : 19

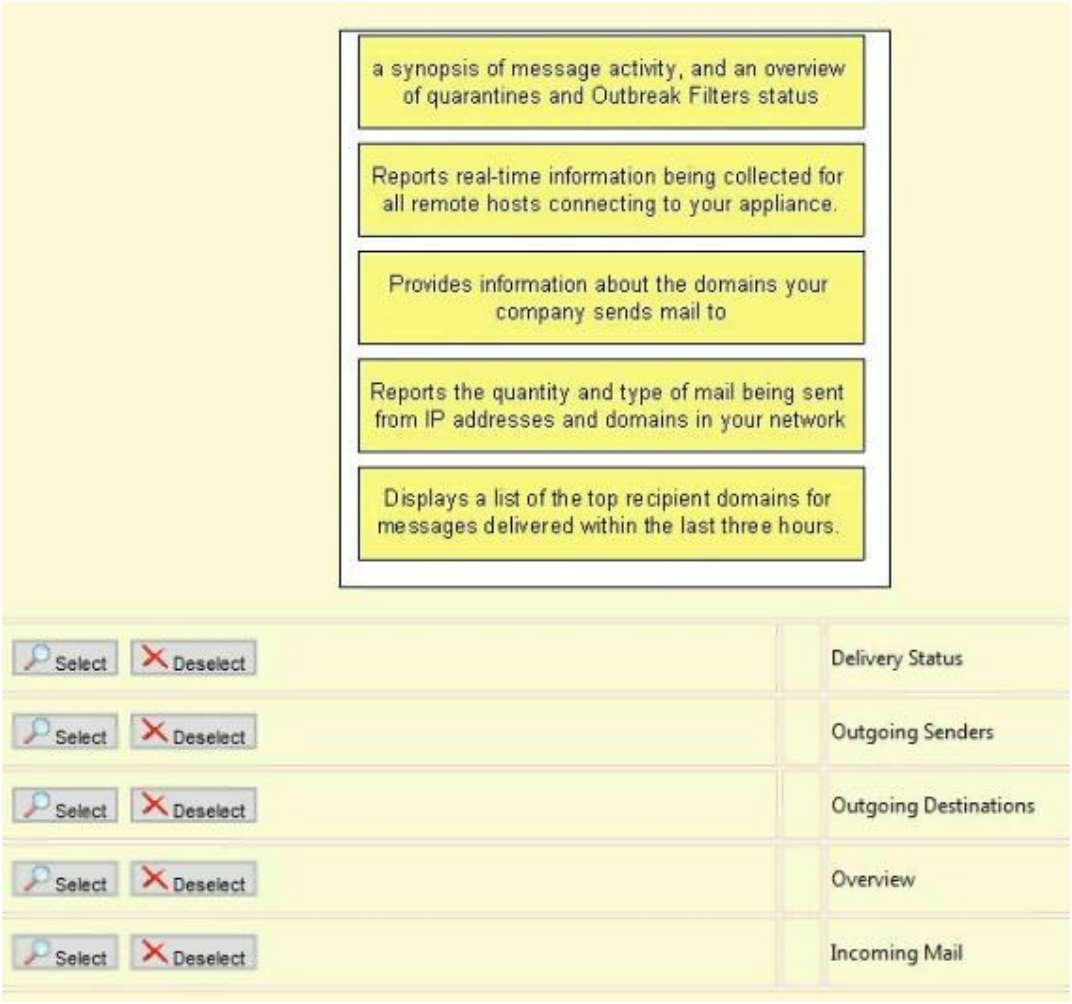
In the IronPort C-Series, which of the following control the SMTP conversation? (Choose two.)

A. Message Filters
B. Outbreak Filters
C. Anti-Virus
D. Content Filters
E. Host Access Table
F. Recipient Access Table
G. IronPort Anti-Spam

Answer: E,F

Question No : 20 DRAG DROP

Match the following report types with their definition.


a synopsis of message activity, and an overview of quarantines and Outbreak Filters status
Reports real-time information being collected for all remote hosts connecting to your appliance.
Provides information about the domains your company sends mail to
Reports the quantity and type of mail being sent from IP addresses and domains in your network
Displays a list of the top recipient domains for messages delivered within the last three hours.
Select
Deselect
Delivery Status
Select
Deselect
Outgoing Senders
Select
Deselect
Outgoing Destinations
Select
Deselect
Overview
Select
Deselect
Incoming Mail

Answer: