

EXAMUNION

Certified IT Exam Material Authority



Accurate study guides, High passing rate!
We offer free update service for one year!

<http://www.examunion.com>

Exam : **650-153**

Title : ESFE Cisco Email Security
Field Engineer Specialist

Version : Demo

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

2. Refer to the exhibit.

Add Condition

- Message Body or Attachment
- Message Body
- Message Size
- Attachment Content
- Attachment File Info**
- Attachment Protection
- Subject Header
- Other Header
- Envelope Sender
- Envelope Recipient
- Receiving Listener

Attachment File Info Help

Does the message contain an attachment of a filetype matching a specific filename or pattern based on its fingerprint (similar to a UNIX file command)? Does the declared MIME type of an attachment match, or does the IronPort Image Analysis engine find a suspect or inappropriate image?

Filename:
Contains [] *

File type is:
Is [] executable []

MIME type is:
Is []

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

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

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

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) address 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.COM>
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

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

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

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

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

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

11.Refer to the wizard screenshot.

<input checked="" type="checkbox"/> Enable Data 1 Interface		
<i>This interface is typically configured to accept mail.</i>		
IP Address:	<input type="text" value="192.168.10.101"/>	
Network Mask:	<input type="text" value="255.255.255.0"/>	
Fully Qualified Hostname:	<input type="text" value="mail.alpha.com"/> <i>Fully qualified hostname for this appliance</i>	
Accept Incoming Mail:	<input checked="" type="checkbox"/> Accept mail on this interface	
	Domain ?	Destination <input type="button" value="Add Row"/>
	<input type="text" value="exchange.alpha.com"/> <i>example: company.com</i>	<input type="text" value="172.20.0.10"/> <i>i.e. An Exchange or Notes server</i> <input type="button" value=""/>
Relay Outgoing Mail:	<input checked="" type="checkbox"/> Relay mail on this interface	
	System ?	<input type="button" value="Add Row"/>
	<input type="text" value="172.20.0.10/32"/> <i>example: company.com</i>	<input type="button" value=""/>

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

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

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

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

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