

[Free-Dumps Quality Free PassLeader 650-153 Study Guide With Free VCE and PDF Download (Question 11 – Question 40)]

New Updated 650-153 Exam Questions from PassLeader 650-153 PDF dumps! Welcome to download the newest PassLeader 650-153 VCE dumps: <http://www.passleader.com/650-153.html> (113 Q&As) Keywords: 650-153 exam dumps, 650-153 exam questions, 650-153 VCE dumps, 650-153 PDF dumps, 650-153 practice tests, 650-153 study guide, 650-153 braindumps, Cisco Email Security Field Engineer Specialist (ESFE) Exam p.s. Free 650-153 dumps download from Google Drive: https://drive.google.com/open?id=0B-ob6L_QjGLpQUt3UnhsblFiUW8

QUESTION 11 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 using the source IP address. B. Mail flow direction is determined by the type of listener, public verses private. C. Mail flow direction is determined by the "Recipient to" field in the SMTP envelope. D. Mail flow direction is determined by the "Mail From" field in the SMTP envelope. Answer: A

QUESTION 12 You are performing a test of the IronPort Anti-Spam engine. In order to trigger the anti-spam engine for suspect spam, what is the value of the x-advertisement header needs to be added to the message? Enter the string in lowercase _____. Answer: spam

QUESTION 13 One of the items on the Pre-Install Worksheet is "Base DN". Which of the following sections in the work sheet contains this item? A. Network Settings B. Firewall Rules C. Mail Information D. Authentication Answer: D

QUESTION 14 A new C-160 has been delivered and needs to be configured. What subnet and C-Series interface does your laptop need to be configured on? A. Data 2 192.168.10.0/24 B. Data 1 192.168.42.0/24 C. Data 2 192.168.42.0/24 D. Data 1 192.168.10.0/24 Answer: B

QUESTION 15 Your customer has several DLP policies enabled such that policy order effects the operation. In which menu is the order of the DLP policies changed? A. Mail Policies > DLP Policy Manager, edit policy order B. Security Settings > RSA DLP > edit policy order C. Mail Policies > Outgoing Mail Policies > DLP, edit order D. Mail Policies > Mailflow policies, edit policy order Answer: A

QUESTION 16 Drag and Drop question Match only the following default sender groups with their default senderbase reputation scores.



Answer:



QUESTION 17 At what point in the SMTP conversation can the SMTP client send message headers? A. Between MAIL FROM and RCPT TO B. Between RCPT TO and DATA C. Between DATA and a period "." on a single line D. Between HELO and MAIL FROM Answer: C

QUESTION 18 In the default settings, which of the following sender groups will match on a reputation

score of +2? A. SUSPECTLISTB. BLACKLISTC. RELAYUSTD. UNKNOWNUSTE. WHITEUST Answer: D
QUESTION 19Which of the following types of DNS records deals with mail delivery for a specific domain? A. TXTB. MXC.
PTRD. A Answer: B QUESTION 20By default, how do Outbreak filters avoid quarantining false positives? A. All false
positives must be quarantined until a Virus signature is received so that they can be checked.B. False positives are released as
updates provide a better description of suspected attachment.C. Positive matches are not quarantined. They are dropped.D. False
positives do not occur as the Anti-Virus engine will check the signature against the incoming mail.Only positive matches against the
signature are quarantined for checking later on. Answer: B QUESTION 21Drag and Drop questionOrder the following (applicable)
steps so that McAfee is enabled as the second of two anti-virus engines. Assume that this follows the system setup wizard.



Answer:



QUESTION 22How does a customer report spam that gets through the C-Series appliance? (Choose two.) A. Send the spam as
an attachment in RFC 822 format to spam@access.ironport.comB. Use the Submission plugin to submit this email back to
IronPortC. Open a case for this problem and attach the spam to an RFC 822 formatD. Send the spam as an attachment in RFC
822 format to ham@access.ironport.com Answer: AB QUESTION 23During system setup, how are scheduled reports handled? A.
By default scheduled reports are sent to the alert recipient specified in the system setup.B. Scheduled reports are only configured
after system setup.C. The recipient for scheduled reports can be different than the alert recipient and scheduled reports can be
configured during system setup or afterwards. Answer: B QUESTION 24When saving a configuration file that will be reloaded into
the appliance, which one of the following must be changed before saving? A. Unmask the password stringsB. Shut down the
mail listenersC. Clustered systems must be un-clusteredD. Feature key strings must be recorded Answer: A QUESTION 25Drag
and Drop questionThe following ate steps for registering a Recipient with CRES. Place them in the correct order.



Answer:

QUESTION 26 By default a domain that falls into either of two sender groups, in the following list, will have its messages tagged for both Anti-spam and Anti-virus scanning. Which two sender groups are these? (Choose two.) A. Unknown List B. White List C. Black List D. Suspect List E. Relay List Answer: AD

QUESTION 27 Which one of the following will allow an administrator to view sensitive compliance information, such as a credit card number, that has triggered a DLP filter? A. mail logs B. Scheduled DLP Reports C. Message Tracking D. Policy Quarantine Answer: B

QUESTION 28 Drag and Drop question
 Instructions: Click the button labeled Select, it will change color to light green. Next, click on the area of the picture which corresponds to the selected answer, the button will change back to white and a small check-mark will appear next to the answer indicating that you have selected. You wish to change your selection for one of the areas, click the button labeled Deselect, this will remove the area that you previously selected.

Answer:

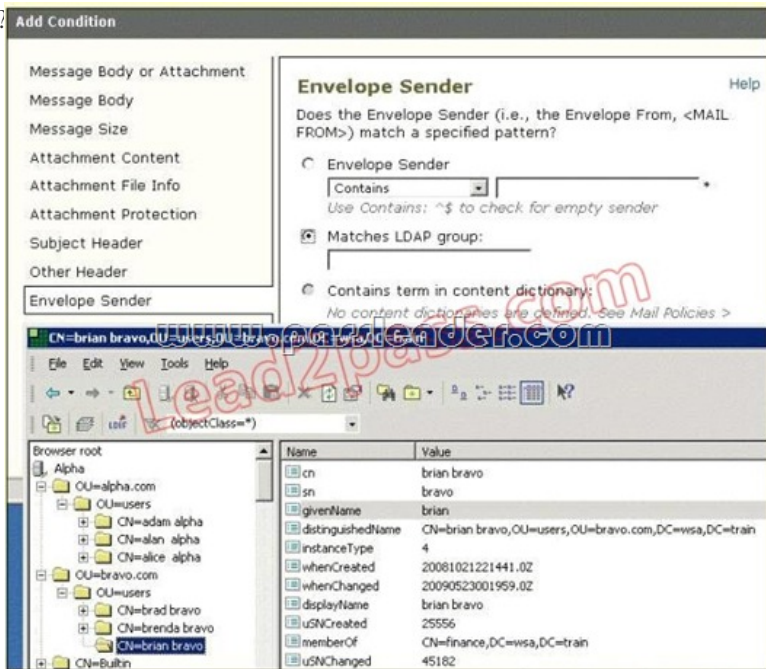
QUESTION 29 Drag and Drop question
 Instructions: Click the button labeled Select, it will change color to light green. Next, click on the area of the picture which corresponds to the selected answer, the button will change back to white and a small check-mark will appear next to the answer indicating that you have selected.



Answer:



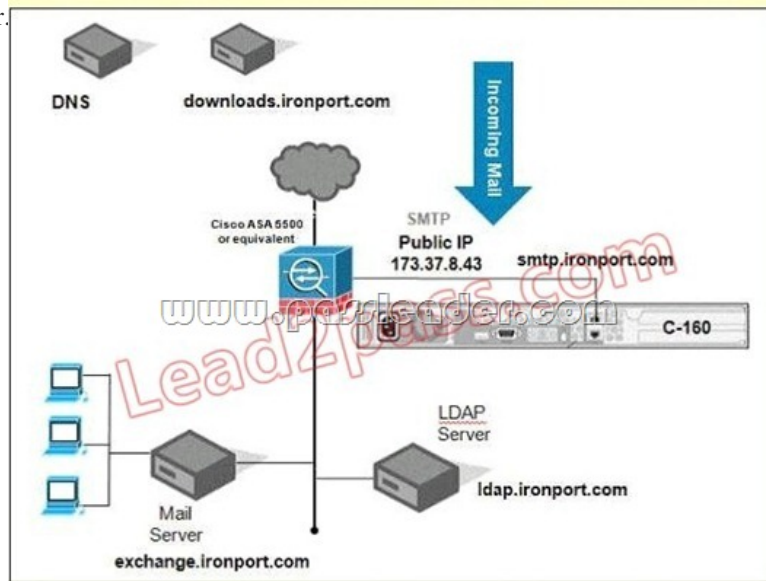
QUESTION 30 You need to create an outgoing content filter to perform footer stamping for members of the finance group. The picture shows the Add Condition menu and the LDAP directory. What attribute value needs to be ENTERED in the Add Condition menu?



Answer: Please use the following link to get the answer of this task.

- http://www.cisco.com/en/US/docs/security/esa/esa7.0/getting_started/ESA_7.0.1_GA_Getting_Started_Guide.pdf (Page 51)
- http://www.cisco.com/en/US/docs/security/esa/esa7.1/config_guide/ESA_7.1.1_Configuration_Guide.pdf (Page 416, Page 455-663)
- <https://supportforums.cisco.com/thread/1000592> QUESTION 31 You need to verify SMTP access to a newly installed C-160. Perform telnet to the appliance from a Linux shell outside of the enterprise. Enter the command string, as you would in this Linux

shell. Include the appropriate port number.



Answer: Please use the following link to get the answer of this task.

http://www.cisco.com/en/US/docs/security/esa/esa7.1/cli_guide/ESA_7.1_FCS_CLI_Reference_Guide.pdf (Page 32) QUESTION 32 Where we usually find the 3xx message? A. EHLOB. Mail FromC. Rcpt toD. Data Answer: D QUESTION 33 After LDAP accept is enabled, what is the best solution to prevent directory harvest attacks? A. Specify all of the legitimate mailbox addresses in the RAT.B. Modify the default mail flow policy.C. Create an access list as a content dictionary and match this resource, with a content filter, against incoming emails.D. Create an access list as a content dictionary and match this resource, with a message filter, against incoming emails. Answer: B QUESTION 34 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. In the HAT settings, increase the SBRS threshold for the BLACKLIST sender group.B. Advise their end users to use the spam plugin or send false negatives samples to ham@access.ironport.com.C. Enable Marketing Mail Detection.D. Enable Intelligent Multi-Scan Answer: D QUESTION 35 Which of the following are best practice techniques when deploying content filters? (Choose two.) A. Use the trace tool whenever possible.B. Apply the filter in a test mail policy that contains one mailbox sender or recipient.C. Run the 'filter test menu' before applying it to any mail policy.D. Add an action to bcc all matches to your admin account. Answer: BC QUESTION 36 Which of the following security features are enabled for incoming mail by default? (Choose three.) A. bounce verificationB. IronPort Anti-SpamC. Sophos Anti-VirusD. McAfee Anti-VirusE. Outbreak filters Answer: E QUESTION 37 Of the following which one is enabled by default on the C-Series? A. Local ReportingB. Local Message trackingC. EncryptionD. Bounce Verification Answer: D QUESTION 38 In the C-160's factory default configuration, which interface has ssh enabled by default on the 192.168.42.42 address? A. Data 2B. Data 1C. None. SSH must be first enabled through the consoleD. Management Answer: B QUESTION 39 Refer to the exhibit. Based on the Add Condition menu which of listed file attachments will be matched? (Choose two.)



A. A.pdf attachmentB. A. msi attachment that has had its file extension changed to .pdfC. A. pdf attachment that has had its file extension changed to .exeD. A. exe attachment Answer: BD QUESTION 40 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
Download the newest PassLeader 650-153 dumps from passleader.com now! 100% Pass Guarantee! 650-153 PDF dumps & 650-153 VCE dumps: <http://www.passleader.com/650-153.html> (113 Q&As)
(New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) p.s. Free 650-153 dumps download from Google Drive: https://drive.google.com/open?id=0B-ob6L_QjGLpQUt3UnhsbFiUW8