Vendor: Cisco

Exam Code: 650-156

Exam Name: Cisco IronPort Security Professional - Email Security (ISPES)

Version: DEMO
1. What is the difference between the ACCEPT and RELAY action in the Mail Flow Policy?
   A. ACCEPT will allow the email in and handle it as an inbound message, RELAY won't accept the email unless configured in the RAT.
   B. ACCEPT will allow the email in and handle it as an inbound message, RELAY will accept the email but skip the RAT and handle it as an outbound message.
   C. ACCEPT will allow the email in and handle it as outbound and skip the RAT, RELAY will accept the email and handle it as inbound.
   D. ACCEPT will allow the email in and handle it as an outbound message, RELAY will accept the email and handle it as an inbound message.
   Answer: B

2. IPAS is enabled for all inbound mail but you want to bypass Spam checking for messages from lead2pass.com. Which three methods will do this.? (Choose three.)
   A. Add the IP addresses of the sending the sending mail servers of cisco.com to the White list.
   B. Create a message filter to bypass Spam checking for Cisco.com.
   C. Create a Mail Flow Policy for Sender Cisco.com and disable IPAS.
   D. Create an incoming mail policy to match on cisco.com and disable IPAS.
   E. Create a content filter to bypass Spam checking for Cisco.com.
   Answer: A,B,D

3. Which two connection behaviors, specified in each Mail Flow policy, will apply an Inbound Mail Policy? (Choose two.)
   A. CONTINUE
   B. ACCEPT
   C. REJECT
   D. RELAY
   Answer: B,C

4. What is the first CU command for entering a message filter?
   A. message
   B. filter
   C. message filter
   D. filters
   Answer: D

5. How should marketing messages that are missed by marketing mail detection is handled?
   A. Turn off this feature and report the issue to customer support for fine tuning of the filter.
   B. Send samples to spam@access.ironport.com
   C. Send samples to ham@access.ironport.com
   D. Send samples to ads@access.ironport.com.
   E. Access the Mail Policies: Anti-Spam menu and lower the marketing-mail threshold.
Answer: D

6. Which of the following reporting options will allow you to view aggregate traffic across a group of two email security appliances, separate from other appliance groups?
A. Sender Groups
B. Domain-Based Executive Summary
C. Email Flow Central
D. Email Reporting Groups
Answer: B

7. LDAP is enabled for all but one internal domain that is not represented in the LDAP directory, how would you configure the appliance to accept it?
A. Create a Domain Assignments profile pointing to DEV NULL.
B. Create a message filter to bypass_idapaccept for the domain.
C. Configure the LDAP accept on the listener with a 250 code.
D. Bypass LDAP accept in a RAT entry.
Answer: D

8. What is a base DN in the LDAP directory?
A. The fully qualified domain name.
B. A user's mail attribute
C. A user attribute used for location searches
D. A starting point with a LDAP schema for searches
Answer: D

9. What is the process of rewriting a private sender's address into a public sender's address called?
A. Forward address rewriting
B. LDAP Masquerading
C. Proxy address lookup
D. LDAP routing
Answer: B

10. You have finished installing a C-160 that is designed to relay incoming and outgoing mail for the mail server exchange.bravo.com. This is a one armed installation. The outgoing mail cannot be delivered. According to the mail log, what is the most likely problem?
A. An SMTP route needs to be configured for exchange.inside.com
B. The mail server needs to point to a private listener
C. Exchange.bravo.com needs to be configured on the RELAYUST
D. Exchange.bravo.com needs to be configured in the RAT
E. Exchange.bravo.com needs to be removed from the SUSPECTUST
Answer: C