Free Questions for 300-720 by go4braindumps

Shared by Holloway on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Refer to the exhibit.

```
sample_filter:
if (mail-from == "test@cisco.com") AND (subject == "FW: Bounce Notification")
{
skip-viruscheck();
}
.
```

What results from this filter configuration?

Options:

A- Action is skipping all antivirus checks for the mail

B- Action is applied to all mail that has the subject 'FW: Bounce Notification.'

C- Action is applied to all mail from test@cisco.com.

D- Action is skipping all antispam checks for the mail.

Answer:

A

Question 2

Question Type: MultipleChoice

A Cisco Secure Email Gateway administrator must provide outbound email authenticity and configures a DKIM signing profile to handle this task. What is the next step to allow this organization to use DKIM for their outbound email?

Options:

A- Enable the DKIM service checker

B- Export the DNS TXT record to provide to the DNS registrar

C- Import the DNS record of the service provider into the Cisco Secure Email Gateway.

D- Configure the Trusted Sender Group message authenticity policy.

Answer:

B

Explanation:

To use DKIM for outbound email, the administrator must export the DNS TXT record from the Cisco Secure Email Gateway and provide it to the DNS registrar of the domain. This will allow the recipient servers to verify the DKIM signature of the email by querying the DNS record of the sender domain.Reference: [Cisco Secure Email Gateway Administrator Guide - Configuring DKIM Signing]

Question 3

Question Type: **MultipleChoice**

The CEO sent an email indicating that all emails containing a string of 123ABCDEFGHJ cannot be delivered and must be sent into quarantine for further inspection. Given the requirement, which regular expression should be used to match on that criteria?

Options:

A- \\D{3}[A-Z]{9}

B- \d{3}[A-Z]{9}

C- \W{3}[A-Z]{9}

D- {3}\d{9}[A-Z]

Answer:

B

Explanation:

A regular expression is a sequence of characters that defines a search pattern for text. To match a string of 123ABCDEFGHJ, you need to use the following regular expression: \d{3}[A-Z]{9}. This expression means that the string must start with three digits (\d{3}), followed by nine uppercase letters ([A-Z]{9}). This expression will match any string that has the same format as 123ABCDEFGHJ. Reference =User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Regular Expressions [Cisco Secure Email Gateway] - Cisco

Question 4

Question Type: **MultipleChoice**

A company has recently updated their security policy and now wants to drop all email messages larger than 100 MB coming from external sources. The Cisco Secure Email Gateway is LDAP integrated and all employee accounts are in the group "Employees". Which filter rule configuration provides the desired outcome?

Options:

A- if (mail-from-group == 'Employees') and (body-size > '100M') {drop()}

B- if (mail-from-group != 'Employees') and (body-size > 100M) {drop();}

C- if (mail-from-group == 'Employees') and (body-size > 100M) {bounce();}

D- if ('mail-from-group != Employees') and (body-size > 100M) {drop();}

Answer:

A

Question 5

The CEO added a sender to a safelist but does not receive an important message expected from the trusted sender. An engineer evaluates message tracking on the Cisco Secure Email Gateway appliance and determines that the message was dropped by the antivirus engine. What is the reason for this behavior?

Options:

A- The sender is included in an ISP blocklist

B- Administrative access is required to create a safelist.

C- The sender didn't mark the message as urgent

D- End-user safelists apply to antispam engines only.

Answer:

D

Explanation:

The reason why the CEO did not receive an important message expected from a trusted sender after adding them to a safelist is because end-user safelists apply to antispam engines only. End-user safelists are lists of sender addresses or domains that end users can create and manage through their quarantine accounts or email clients. End-user safelists allow end users to accept or exempt messages from certain senders or domains from being identified as spam by the antispam engines. However, end-user safelists do not affect other filtering engines such as antivirus, outbreak filters, or content filters. Reference =User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Safelists and Blocklists [Cisco Secure Email Gateway] - Cisco

Question 6

Question Type: **MultipleChoice**

An administrator manipulated the subnet mask but was still unable to access the user interface. How must the administrator access the Cisco Secure Email Gateway appliance to perform the initial configuration?

Options:

A- Use the serial or console port

B- Use the management port

C- Use the data 2 port

D- Use the data 1 port

Answer:

A

Explanation:

If you are unable to access the user interface of the Cisco Secure Email Gateway appliance after manipulating the subnet mask, you can use the serial or console port to perform the initial configuration.The serial or console port provides a command-line interface that allows you to configure basic network settings such as IP address, subnet mask, gateway, and hostname3. Reference =User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Configuring Network Settings [Cisco Secure Email Gateway] - Cisco

To Get Premium Files for 300-720 Visit

https://www.p2pexams.com/products/300-720

For More Free Questions Visit

https://www.p2pexams.com/cisco/pdf/300-720

20% DISCOUNT