Free Questions for 300-720 by braindumpscollection

Shared by Robbins on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization wants to prevent proprietary patent documents from being shared externally via email. The network administrator reviewed the DLP policies on the Cisco Secure Email Gateway and could not find an existing policy with the appropriate matching patterns. Which type of DLP policy template must be used to create a policy that meets this requirement?

Options:

A- privacy protection

B- custom policy

C- regulatory compliance

D- acceptable use

Answer:

B

Explanation:

Custom policy is a type of DLP policy template that must be used to create a policy that meets this requirement. Custom policy allows the administrator to define their own criteria for detecting sensitive or confidential data in messages, such as keywords, regular expressions, file types, etc.

To create a custom DLP policy on Cisco ESA, the administrator can follow these steps:

Select Mail Policies > DLP Policy Manager and click Add Policy.

Enter a name and description for the DLP policy, such as Patent Protection.

Under Policy Template, select Custom Policy.

Click Submit.

Under Content Matching Criteria, click Add Criteria.

Choose a matching type, such as Keyword or Regular Expression, and enter a value that matches the proprietary patent documents, such as "patent number" or "\d{4}/\d{6}".

Click Submit.

The other options are not valid types of DLP policy templates to create a policy that meets this requirement, because they are predefined templates that do not match the proprietary patent documents.

Question 2

Question Type: MultipleChoice

A Cisco Secure Email Gateway administrator is creating a Mail Flow Policy to receive outbound email from Microsoft Exchange. Which Connection Behavior must be selected to properly process the messages?

Options:

A- Accept

B- Delay

C- Relay

D- Reject

Answer:

C

Explanation:

Relay is the connection behavior that must be selected to properly process the messages. Relay allows Cisco ESA to accept messages from the specified source and deliver them to the intended destination, without applying any content or reputation filters.

To configure a mail flow policy with relay connection behavior on Cisco ESA, the administrator can follow these steps:

Select Mail Policies > Mail Flow Policies and click Add Policy.

Enter a name and description for the mail flow policy, such as Exchange Outbound.

Under Connection Behavior, select Relay.

Click Submit.

The other options are not valid connection behaviors to properly process the messages, because they either reject, delay, or accept the messages with content or reputation filters applied.

Question 3

Question Type: MultipleChoice

What are the two different phases in the process of Cisco Secure Email Gateway performing S/MIME encryption? (Choose two.)

Options:

A- Attach the encrypted public key to the message

B- Encrypt the message body using the session key

C- Send the encrypted message to the sender

D- Attach the encrypted symmetric key to the message

E- Create a pseudo-random session key.

Answer:

D, E

Question 4

Question Type: MultipleChoice

Which of the following two steps are required to enable Cisco SecureX integration on a Cisco Secure Email Gateway appliance? (Choose two.)

Options:

A- Paste in the Registration Token generated from the Smart Licensing Account

B- Enable the Threat Response service under Network>Cloud Service Settings.

C- Select the correct Threat Response Server based on your region.

D- Paste in the Registration Token generated from the Security Services Exchange.

E- Enable the Security Services Exchange service under Network>Cloud Service Settings

Answer:

B, C

Explanation:

one of the methods to enable Cisco SecureX integration on a Cisco Secure Email Gateway appliance is to use the Threat Response service1.This service allows the appliance to send telemetry data to the SecureX cloud and provide visibility and response capabilities across multiple security products1.To use this service, the administrator needs to perform the following steps1:

Enable the Threat Response service: The administrator needs to go to Network > Cloud Service Settings and enable the Threat Response service.This will generate a registration token that can be used to register the appliance with SecureX1.

Select the correct Threat Response Server: The administrator needs to select the appropriate Threat Response server based on the region where the appliance is located.The available regions are North America, Europe, and Asia Pacific1.

Question 5

Question Type: MultipleChoice

An engineer is tasked with creating a content filter to catch attachments, including credit card numbers, and hold them for review until further action is taken. Which component on a Cisco Secure Email Gateway must be configured to meet this requirement?

Options:

A- Spam Quarantine

B- Policy Quarantine

C- Outbreak Filter

D- Content Filter

Answer:

D

Explanation:

Content filter is a component on a Cisco Secure Email Gateway that must be configured to catch attachments, including credit card numbers, and hold them for review until further action is taken. Content filter allows you to define rules based on message content and apply actions such as quarantine, encrypt, or modify. Reference = [User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Content Filters [Cisco Secure Email Gateway] - Cisco]

Question 6

Question Type: MultipleChoice

An administrator notices that incoming emails with certain attachments do not get delivered to all recipients when the emails have multiple recipients in different domains like cisco.com and test.com. The same emails when sent only to recipients in cisco.com are delivered properly. How must the Cisco Secure Email Gateway be configured to avoid this behavior?

Options:

A- Modify mail policies for cisco.com to ensure that emails are not dropped.

B- Modify mail policies so email recipients do not match multiple policies.

C- Modify DLP configuration to ensure that all attachments are permitted for test.com.

D- Modify DLP configuration to exempt DLP scanning for messages sent to test.com domain

Answer:

B

Explanation:

By modifying the mail policies, specifically the recipient matching criteria, you can ensure that email recipients do not match multiple policies simultaneously. When recipients in the email message belong to different domains (e.g., cisco.com and test.com), it can result in multiple policies being triggered simultaneously, leading to inconsistent delivery of emails with attachments.

DLP is for outgoing mail only and not relevant to incoming mail.

Question 7

Question Type: MultipleChoice

When the spam quarantine is configured on the Cisco Secure Email Gateway, which type of query is used to validate non administrative user access to the end-user quarantine via LDAP?

Options:

A- spam quarantine end-user authentication

B- spam quarantine alias consolidation

C- spam quarantine external authorization

D- local mailbox (IMAP/POP) authentication

Answer:

A

Explanation:

spam quarantine end-user authentication query is used to validate non administrative user access to the end-user quarantine via LDAP1.This query is configured in the System Administration > LDAP > LDAP Server Profile page and can be tested using the smtproutes command in the CLI1. The other queries are not related to this task.The spam quarantine alias consolidation query is used to consolidate multiple email addresses for a user into one login2.The spam quarantine external authorization query is used to authorize users to access an external spam quarantine on a separate Cisco Secure Email and Web Manager3.The local mailbox (IMAP/POP) authentication is an alternative method to authenticate users without using LDAP2.

Question 8

Question Type: MultipleChoice

An organization wants to designate help desk personnel to assist with tickets that request the release of messages from the spam quarantine because company policy does not permit direct end-user access to the quarantine. Which two roles must be used to allow help desk personnel to release messages while restricting their access to make configuration changes in the Cisco Secure Email Gateway? (Choose two.)

Options:

A- Administrator

B- Help Desk User

C- Read-Only Operator

D- Technician

E- Quarantine Administrator

Answer:

B, E

Explanation:

All users with administrator privileges can change spam quarantine settings and view and manage messages in the spam quarantine. You do not need to configure spam quarantine access for administrator users.

If you configure access to the spam quarantine for users with the following roles, they can view, release, and delete messages in the spam quarantine:

-Operator

-Read-only operator

-Help desk user

-Guest

-Custom user roles that have spam quarantine privileges

These users cannot access spam quarantine settings.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_14-0/b_ESA_Admin_Guide_12_1_chapter_0100000.html?bookSearch=true#con_1624156

Question 9

Question Type: MultipleChoice

What is the purpose of checking the CRL during SMTP authentication on a Cisco Secure Email Gateway?

Options:

A- Validate the date to check if the certificate is still valid

B- Check if the certificate is not revoked.

C- Confirm that corresponding CA is present

D- Verify the common name matches user ID

Answer:

B

Explanation:

The purpose of checking the Certificate Revocation List (CRL) during SMTP authentication on a Cisco Secure Email Gateway is to check if the certificate is not revoked by the issuing Certificate Authority (CA). A revoked certificate means that it is no longer valid and should not be trusted. Reference = [User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment) - Configuring SMTP Authentication [Cisco Secure Email Gateway] - Cisco]

Question 10

Question Type: MultipleChoice

An organization wants to use DMARC to improve its brand reputation by leveraging DNS records.

Which two email authentication mechanisms are utilized during this process? (Choose two.)

Options:

A- SPF

B- DSTP

C- DKIM

D- TLS

E- PKI

Answer:

A, C

Explanation:

https://www.cisco.com/c/en/us/products/security/what-is-dmarc.html

SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) are two email authentication mechanisms that are utilized during this process. SPF and DKIM allow the domain owner to publish DNS records that specify the authorized IP addresses or hosts for sending emails from that domain and sign the messages with a cryptographic key to prove their authenticity and integrity.

DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication standard that builds on SPF and DKIM and allows the domain owner to publish DNS records that specify how receivers should handle messages that fail SPF or DKIM verification, such as reject, quarantine, or none, and how to report back the results of DMARC validation.

The other options are not valid email authentication mechanisms that are utilized during this process, because they are not part of DMARC standard.