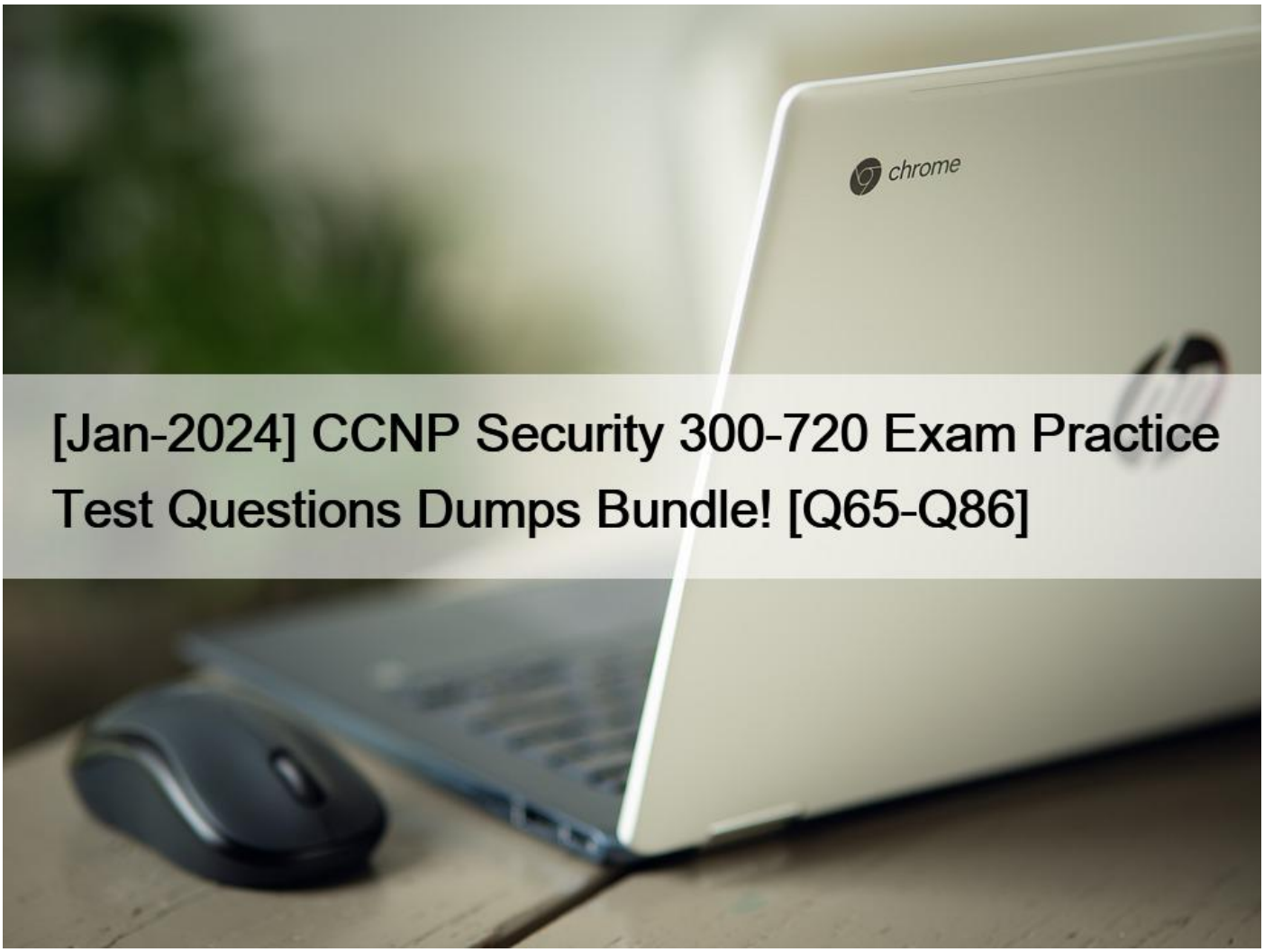
[Jan-2024 CCNP Security 300-720 Exam Practice Test Questions Dumps Bundle! [Q65-Q86



[Jan-2024] CCNP Security 300-720 Exam Practice Test Questions Dumps Bundle!
2024 Updated 300-720 PDF for the 300-720 Tests Free Updated Today!

Cisco 300-720 exam is a certification exam designed for individuals who want to demonstrate their expertise in securing email with the Cisco Email Security Appliance. 300-720 exam is intended for professionals who have experience working with email security technologies and are looking to enhance their skills and knowledge in this area. The Cisco 300-720 exam is an advanced-level certification that validates the skills and knowledge required to configure, implement, and manage the Cisco Email Security Appliance.

Cisco Email Security Appliance is a powerful tool that helps organizations protect their email from spam, viruses, and other threats. It provides advanced threat protection, data loss prevention, and email encryption capabilities, making it an essential tool for organizations of all sizes. By earning the Cisco 300-720 certification, candidates can demonstrate their proficiency in using the

Cisco Email Security Appliance to secure their organization's email.

NEW QUESTION 65

An engineer is configuring a Cisco ESA for the first time and needs to ensure that any email traffic coming from the internal SMTP servers is relayed out through the Cisco ESA and is tied to the Outgoing Mail Policies.

Which Mail Flow Policy setting should be modified to accomplish this goal?
* Exception List
* Connection Behavior
* Bounce Detection Signing
* Reverse Connection Verification

NEW QUESTION 66

An administrator notices that the Cisco Secure Email Gateway delivery queue on an appliance is consistently full. After further investigation, it is determined that the IP addresses currently in use by appliance are being rate-limited by some destinations. The administrator creates a new interface with an additional IP address using virtual gateway technology, but the issue is not solved Which configuration change resolves the issue?
* Use the CLI command altsrchost to set the new interface as the source IP address for all mail.
* Use the CLI command loadbalance auto to enable mail delivery over all interfaces.
* Use the CLI command alt-src-host to set the new interface as a possible delivery candidate.
* Use the CLI command deliveryconfig to set the new interface as the primary interface for mail delivery

Determining Which Interface is Used for Mail Delivery Unless you specify the output interface via the deliveryconfig</code> command or via a message filter (alt-src-host), or through the use of a virtual gateway, the output interface is selected by the AsyncOS routing table.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_011001.html?bookSearch=true

NEW QUESTION 67

What are two prerequisites for implementing undesirable URL protection in Cisco ESA? (Choose two.)
* Enable outbreak filters.
* Enable email relay.
* Enable antispam scanning.
* Enable port bouncing.
* Enable antivirus scanning.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_01111.html

NEW QUESTION 68

An engineer wants to utilize a digital signature in outgoing emails to validate to others that the email they are receiving was indeed sent and authorized by the owner of that domain Which two components should be configured on the Cisco Secure Email Gateway appliance to achieve this? (Choose two.)
* DMARC verification profile
* SPF record

* Public/Private keypair
* Domain signing profile
* PKI certificate

Public/Private keypair. A public/private keypair is a pair of cryptographic keys that are used to generate and verify digital signatures. The private key is used to sign the email message, while the public key is used to verify the signature. The public key is published in a DNS record, while the private key is stored on the Cisco Secure Email Gateway appliance[1, p. 2].

Domain signing profile. A domain signing profile is a configuration that specifies the domain and selector to use for signing outgoing messages, as well as the signing algorithm, canonicalization method, and header fields to include in the signature. You can create multiple domain signing profiles for different domains or subdomains[1, p. 3].

The other options are not valid because:

A) DMARC verification profile is not a component for utilizing a digital signature in outgoing emails. It is a component for verifying the authenticity of incoming emails based on SPF and DKIM results[2, p. 1].

B) SPF record is not a component for utilizing a digital signature in outgoing emails. It is a component for validating the sender IP address of incoming emails based on a list of authorized IP addresses published in a DNS record[3, p. 1].

E) PKI certificate is not a component for utilizing a digital signature in outgoing emails. It is a component for encrypting and decrypting email messages based on a certificate authority that issues and validates certificates[4, p. 1].

NEW QUESTION 69

Which two query types are available when an LDAP profile is configured? (Choose two.)

* proxy consolidation
* user
* recursive
* group
* routing

User and routing are two query types that are available when an LDAP profile is configured on Cisco ESA. User queries are used to validate end-user credentials, such as for Spam Quarantine End-User Authentication or SMTP Authentication. Routing queries are used to determine the destination mail server for a recipient, such as for Mail Flow Policies or Delivery Methods.

NEW QUESTION 70

What are organizations trying to address when implementing a SPAM quarantine?

* true positives
* false negatives
* false positives
* true negatives

https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0100000.html#c on_ 1482874

NEW QUESTION 71

Which two steps configure Forged Email Detection? (Choose two.)

* Configure a content dictionary with executive email addresses.
* Configure a filter to use the Forged Email Detection rule and dictionary.
* Configure a filter to check the Header From value against the Forged Email Detection dictionary.

* Enable Forged Email Detection on the Security Services page.
* Configure a content dictionary with friendly names.

Reference:

https://explore.cisco.com/esa-feature-enablement/user-guide-for-async-11

NEW QUESTION 72

Which two steps are needed to disable local spam quarantine before external quarantine is enabled? (Choose two.)
* Uncheck the Enable Spam Quarantine check box.
* Select Monitor and click Spam Quarantine.
* Check the External Safelist/Blocklist check box.
* Select External Spam Quarantine and click on Configure.
* Select Security Services and click Spam Quarantine.

To disable local spam quarantine before external quarantine is enabled on Cisco ESA, two steps are needed:

Select Security Services and click Spam Quarantine, which will open the Spam Quarantine settings page.

Uncheck the Enable Spam Quarantine check box, which will disable the local spam quarantine feature on Cisco ESA.

NEW QUESTION 73

A network administrator notices that there are a high number of queries to the LDAP server. The mail logs show an entry “550 Too many invalid recipients | Connection closed by foreign host.” Which feature must be used to address this?
* DHAP
* SBRS
* LDAP
* SMTP

Reference:

https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_011010.html DHAP (Directory Harvest Attack Prevention) is a feature that must be used to address this issue. DHAP is a mechanism that allows Cisco ESA to prevent directory harvest attacks, which are attempts by spammers or hackers to obtain valid email addresses from an LDAP server by sending messages with random or guessed recipients and checking for bounce messages.

To enable DHAP on Cisco ESA, the network administrator can follow these steps:

Select Network > Listeners and click Edit Settings for the listener that receives incoming messages.

Under SMTP Authentication Settings, select Enable Directory Harvest Attack Prevention.

Enter a value for Maximum Invalid Recipients per Hour, which is the number of invalid recipients that triggers DHAP.

Enter a value for Block Sender for (hours), which is the duration that Cisco ESA blocks messages from senders who exceed the maximum invalid recipients per hour.

Click Submit.

NEW QUESTION 74

Which two query types are available when an LDAP profile is configured? (Choose two.)
* proxy consolidation
* user
* recursive
* group
* routing

Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_011010.html

NEW QUESTION 75

When DKIM signing is configured, which DNS record must be updated to load the DKIM public signing key?
* AAAA record
* PTR record
* TXT record
* MX record

Reference:

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213939-esa- configure-dkim-signing.html

NEW QUESTION 76

Which method enables an engineer to deliver a flagged message to a specific virtual gateway address in the most flexible way?
* Set up the interface group with the flag.
* Issue the altsrchost command.
* Map the envelope sender address to the host.
* Apply a filter on the message.

Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_01000.html#con_1133810

NEW QUESTION 77

Which two service problems can the Cisco Email Security Appliance solve? (Choose two.)
* DLP
* IPS
* Antispam
* URL filtering

NEW QUESTION 78

Which action do Outbreak Filters take to stop small-scale and nonviral attacks, such as phishing scams and malware distribution sites?
* Rewrite URLs to redirect traffic to potentially harmful websites through a web security proxy
* Block all emails from email domains associated with potentially harmful websites.
* Strip all attachments from email domains associated with potentially harmful websites.
* Quarantine messages that contain links to potentially harmful websites until the site is taken offline

Outbreak Filters can take the action of rewriting URLs to redirect traffic to potentially harmful websites through a web security proxy. This allows the Cisco Secure Email Gateway to scan the content of the websites and block or warn the user if they are malicious or undesirable. This action can stop small-scale and nonviral attacks, such as phishing scams and malware distribution sites, that may not be detected by other filters. Reference: [Cisco Secure Email Gateway Administrator Guide – Configuring

Outbreak Filters]

NEW QUESTION 79

An engineer is configuring a Cisco ESA for the first time and needs to ensure that any email traffic coming from the internal SMTP servers is relayed out through the Cisco ESA and is tied to the Outgoing Mail Policies.

Which Mail Flow Policy setting should be modified to accomplish this goal?
* Exception List
* Connection Behavior
* Bounce Detection Signing
* Reverse Connection Verification
Reference:

Connection Behavior setting allows you to specify how the Cisco Email Security Appliance (ESA) handles incoming connections from different sender groups. You can choose from four different settings:

Accept: The ESA accepts all connections from the sender group and applies the mail flow policy settings to the messages.

Throttle: The ESA limits the number of concurrent connections and messages per connection from the sender group. This can help reduce the impact of spam or malicious traffic on the ESA’s performance.

Reject: The ESA rejects all connections from the sender group and returns a 5xx SMTP error code to the sender. This can help block unwanted or abusive senders from reaching your network.

Test: The ESA accepts connections from the sender group but does not deliver the messages to the recipients. Instead, it logs the messages and marks them as test messages. This can help you test the mail flow policy settings before applying them to real traffic.

To modify the Connection Behavior setting for a sender group, you need to do the following steps:

On the ESA, choose Mail Policies > HAT Overview.

Click Edit Settings for the sender group that you want to modify.

In the Mail Flow Policy Settings section, choose one of the options from the Connection Behavior drop-down list.

Click Submit and commit changes.

NEW QUESTION 80

Which two certificate authority lists are available in Cisco ESA? (Choose two.)
* default
* system
* user
* custom
* demo
Reference:

https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_11_1_chapter_011000.html#task_1194859

NEW QUESTION 81

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.)
* DSTP
* DKIM
* TLS
* PKI

NEW QUESTION 82

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?
* spam quarantine end-user authentication
* spam quarantine alias consolidation
* spam quarantine external authorization
* local mailbox (IMAP/POP) authentication

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.

NEW QUESTION 83

What is a benefit of implementing URL filtering on the Cisco ESA?
* removes threats from malicious URLs
* blacklists spam
* provides URL reputation protection
* enhances reputation against malicious URLs

Reference:

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote- esa-00.html

NEW QUESTION 84

Which process is skipped when an email is received from safedomain.com, which is on the safelist?
* message filter
* antivirus scanning
* outbreak filter
* antispam scanning

The safelist is a list of email addresses or domains that are considered legitimate and trustworthy by Cisco ESA. When an email is received from a sender on the safelist, Cisco ESA skips antispam scanning for that message and delivers it to the recipient without any spam filtering.

NEW QUESTION 85

Which feature utilizes sensor information obtained from Talos intelligence to filter email servers connecting into the Cisco ESA?
* SenderBase Reputation Filtering
* Connection Reputation Filtering
* Talos Reputation Filtering
* SpamCop Reputation Filtering

SenderBase Reputation Filtering is a feature that allows Cisco ESA to reject or throttle connections from email servers based on their reputation score, which is calculated by Talos using sensor information from various sources.

NEW QUESTION 86

Which two factors must be considered when message filter processing is configured? (Choose two.)
* message-filter order
* lateral processing
* structure of the combined packet
* mail policies
* MIME structure of the message