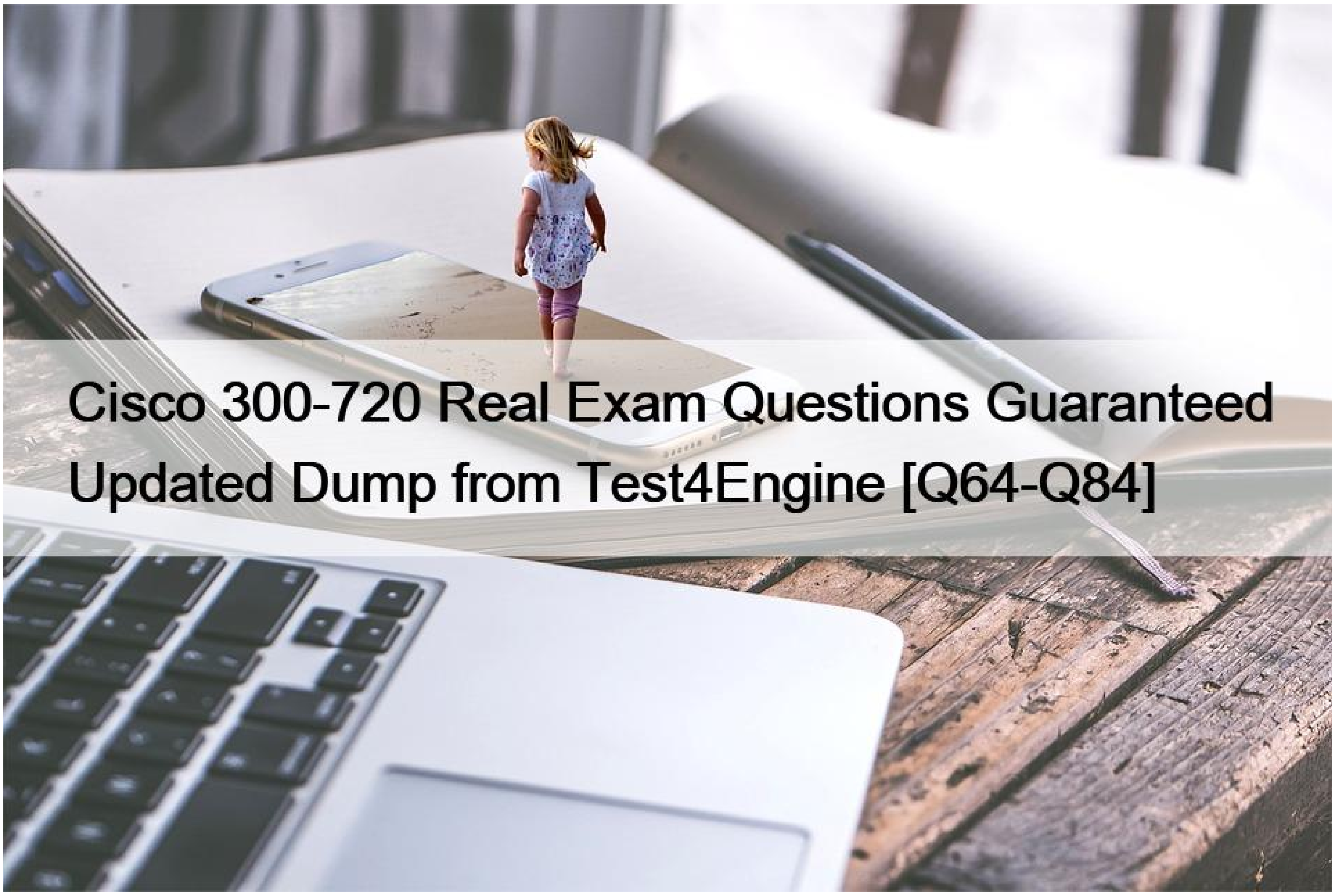
Cisco 300-720 Real Exam Questions Guaranteed Updated Dump from Test4Engine [Q64-Q84



Cisco 300-720 Real Exam Questions Guaranteed Updated Dump from Test4Engine
Verified Pass 300-720 Exam in First Attempt Guaranteed

QUESTION 64

What is the default method of remotely accessing a newly deployed Cisco Secure Email Virtual Gateway when a DHCP server is not available?
* Manual configuration of an IP address is required through the serial port before remote access
* DHCP is required for the initial IP address assignment
* Use the IP address of 192.168 42 42 via the Management port
* Manual configuration of an IP address is required through the hypervisor console before remote access
The default method of remotely accessing a newly deployed Cisco Secure Email Virtual Gateway when a DHCP server is not available is to use the IP address of 192.168.42.42 via the Management port. This IP address is assigned by default to the Management port of the virtual gateway and can be used to access the web user interface or the command-line interface of the appliance. Reference: [Cisco Secure Email Gateway Installation and Upgrade Guide &#8211; Configuring Network Settings]

QUESTION 65

To comply with a recent audit, an engineer must configure anti-virus message handling options on the incoming mail policies to attach warnings to the subject of an email.

What should be configured to meet this requirement for known viral emails?
* Virus Infected Messages
* Unscannable Messages
* Encrypted Messages
* Positively Identified Messages

QUESTION 66

Which type of query must be configured when setting up the Spam Quarantine while merging notifications?
* Spam Quarantine Alias Routing Query
* Spam Quarantine Alias Consolidation Query
* Spam Quarantine Alias Authentication Query
* Spam Quarantine Alias Masquerading Query

QUESTION 67

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

QUESTION 68

Which two actions are configured on the Cisco ESA to query LDAP servers? (Choose two.)
* accept
* relay
* delay
* route
* reject
Reference:

https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_011010.html

QUESTION 69

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.
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

QUESTION 70

Which functionality is impacted if the assigned certificate under one of the IP interfaces is modified?
* traffic between the Cisco Secure Email Gateway and the LDAP server
* emails being delivered from the Cisco Secure Email Gateway
* HTTPS traffic when connecting to the web user interface of the Cisco Secure Email Gateway
* emails being received by the Cisco Secure Email Gateway
If the assigned certificate under one of the IP interfaces is modified, then the HTTPS traffic when connecting to the web user interface of the Cisco Secure Email Gateway will be impacted. The administrator must ensure that the certificate is valid and trusted by the browser or client that is used to access the web user interface. Otherwise, the connection may fail or generate a warning message. Reference: [Cisco Secure Email Gateway Administrator Guide &#8211; Configuring Certificates]

QUESTION 71

How does the graymail safe unsubscribe feature function?
* It strips the malicious content of the URI before unsubscribing.
* It checks the URI reputation and category and allows the content filter to take an action on it.
* It redirects the end user who clicks the unsubscribe button to a sandbox environment to allow a safe unsubscribe.
* It checks the reputation of the URI and performs the unsubscribe process on behalf of the end user.
Reference:

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200383-Graymail-Detection-and-Safe-Unsubscribin.html

QUESTION 72

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

QUESTION 73

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].

QUESTION 74

A Cisco ESA administrator has noticed that new messages being sent to the Centralized Policy Quarantine are being released after one hour. Previously, they were being held for a day before being released.

What was configured that caused this to occur?
* The retention period was changed to one hour.
* The threshold settings were set to override the clock settings.
* The retention period was set to default.
* The threshold settings were set to default.

You can configure Policy, Virus, and Outbreak Quarantines in any one of the following ways:

Choose Quarantine > Other Quarantine > View > +.

Choose Monitor > Policy, Virus, and Outbreak Quarantines and do one of the following.

Click Add Policy Quarantine.

Keep the following in mind, changing the retention time of the File Analysis quarantine from the default of one hour is not recommended.

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_011111.html?bookSearch=true

QUESTION 75

Which two components must be configured to perform DLP scanning? (Choose two.)
* Add a DLP policy on the Incoming Mail Policy.
* Add a DLP policy to the DLP Policy Manager.
* Enable a DLP policy on the Outgoing Mail Policy.
* Enable a DLP policy on the DLP Policy Customizations.
* Add a DLP policy to the Outgoing Content Filter.

QUESTION 76

A network engineer must tighten up the SPAM control policy of an organization due to a recent SPAM attack. In which scenario does enabling regional scanning improve security for this organization?
* when most of the received spam comes from a specific country
* when most of the received spam originates outside of the U.S.
* when most of the received email originates outside of the U.S.
* when most of the received email originates from a specific region
Enabling regional scanning improves security for this organization when most of the received email originates from a specific region. Regional scanning is a feature that allows Cisco ESA to apply different spam thresholds and actions based on the geographic region of the sender&#8217;s IP address, using a database of IP addresses and regions.

To enable regional scanning on Cisco ESA, the administrator can follow these steps:

Select Security Services > IronPort Anti-Spam and click Edit Settings.

Under Regional Scanning, select Enable Regional Scanning.

Click Submit.

Select Security Services > IronPort Anti-Spam > Regional Settings and click Add Region.

Choose a region from the drop-down menu, such as Asia Pacific.

Enter a spam threshold and an action for that region, such as 80 and Drop.

Click Submit.

QUESTION 77

An analyst creates a new content dictionary to use with Forged Email Detection.

Which entry will be added into the dictionary?
* mycompany.com
* Alpha Beta
* Alpha Beta$
* Alpha.Beta@mycompany.com
A content dictionary is a list of words or phrases that can be used to match against message content in Cisco ESA. For Forged Email Detection, a content dictionary can be used to specify the display names of internal senders that should not appear in the From header of external messages. The display name is usually the name of the sender as it appears in the email client, such as Alpha Beta. Therefore, the entry that will be added into the dictionary for this purpose is Alpha Beta.

QUESTION 78

Refer to the exhibit. An engineer needs to change the existing Forged Email Detection message filter so that it references a newly created dictionary named &#8216;Executives&#8217;.

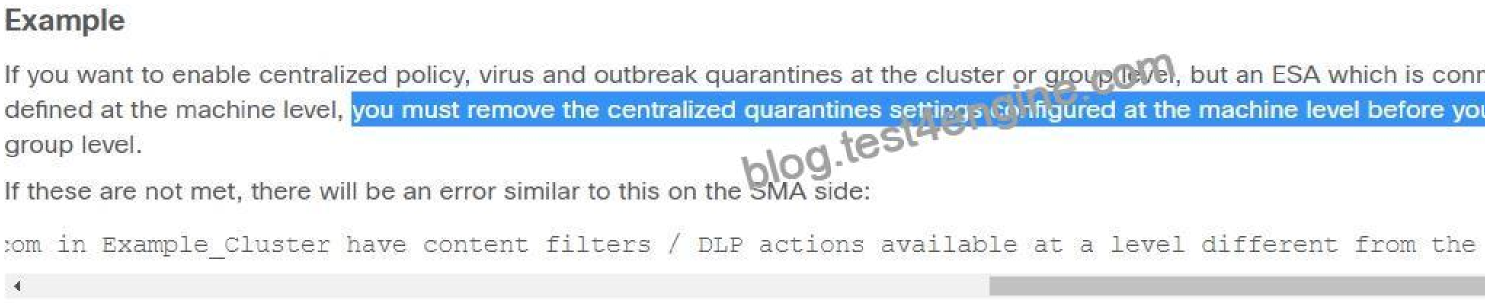
What should be done to accomplish this task?
* Change &#8220;from&#8221; to &#8220;Executives&#8221;.
* Change &#8220;TESF to &#8220;Executives&#8221;.
* Change fed&#8217; to &#8220;Executives&#8221;.
* Change &#8220;support&#8221; to &#8220;Executives&#8221;.

https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/BRKSEC-2240.pdf

QUESTION 79

An administrator is trying to enable centralized PVO but receives the error, &#8220;Unable to proceed with Centralized Policy, Virus and Outbreak Quarantines configuration as esa1 in Cluster has content filters / DLP actions available at a level different from the cluster level.&#8221; What is the cause of this error?

* Content filters are configured at the machine-level on esa1.
* DLP is configured at the cluster-level on esa2.
* DLP is configured at the domain-level on esa1.
* DLP is not configured on host1.



Example

If you want to enable centralized policy, virus and outbreak quarantines at the cluster or group level, but an ESA which is conn
defined at the machine level, you must remove the centralized quarantines settings configured at the machine level before yo
group level.

If these are not met, there will be an error similar to this on the SMA side:

```
:om in Example_Cluster have content filters / DLP actions available at a level different from the
```

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200083-Requirements-for-the-PVO-Migration-Wizar.html

QUESTION 80

Which three options are Cisco ESA facilities that can use LDAP group queries? (Choose three.)

* Anti-spam settings
* Sender groups
* Message filters
* RAT
* Incoming mail policies
* Content filters
* Destination controls
* SenderBase reputation filtering

QUESTION 81

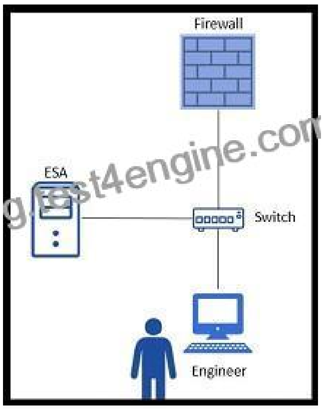
What is the default port to deliver emails from the Cisco ESA to the Cisco SMA using the centralized Spam Quarantine?

* 8025
* 6443
* 6025
* 8443

Explanation/Reference: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118692-configure-esa-00.html

QUESTION 82

Refer to the exhibit. An engineer is trying to connect to a Cisco ESA using SSH and has been unsuccessful. Upon further inspection, the engineer notices that there is a loss of connectivity to the neighboring switch.



Which connection method should be used to determine the configuration issue?
* Telnet
* HTTPS
* Ethernet
* serial

QUESTION 83

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 &#8220;Employees&#8221;. Which filter rule configuration provides the desired outcome?
* if (mail-from-group == &#8216;Employees&#8217;) and (body-size > &#8220;100M&#8221;) {drop()}
* if (mail-from-group != &#8216;Employees&#8217;) and (body-size > 100M) {drop();}
* if (mail-from-group == &#8216;Employees&#8217;) and (body-size > 100M) {bounce();}
* if (&#8216;mail-from-group != Employees&#8217;) and (body-size > 100M) {drop();}

QUESTION 84

A recent engine update was pulled down for graymail and has caused the service to start crashing. It is critical to fix this as quickly as possible.

What must be done to address this issue?
* Roll back to a previous version of the engine from the Services Overview page.
* Roll back to a previous version of the engine from the System Health page.
* Download another update from the IMS and Graymail page.
* Download another update from the Service Updates page.

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_0100010.html#task_9F07A032042F48C6AEDB69D325CD3C5F

Download Real Cisco 300-720 Exam Dumps Test Engine Exam Questions:
https://www.test4engine.com/300-720_exam-latest-braindumps.html]