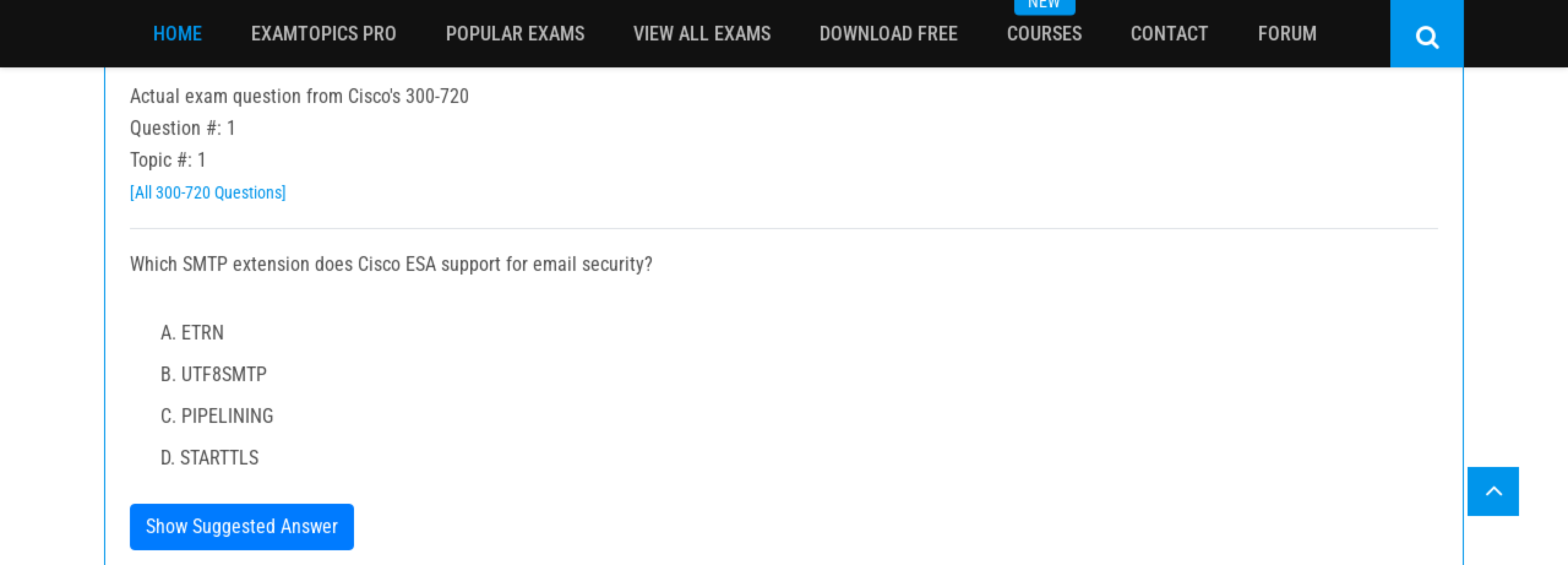


Actual exam question from Cisco's 300-720

Question #: 1

Topic #: 1

[All 300-720 Questions]

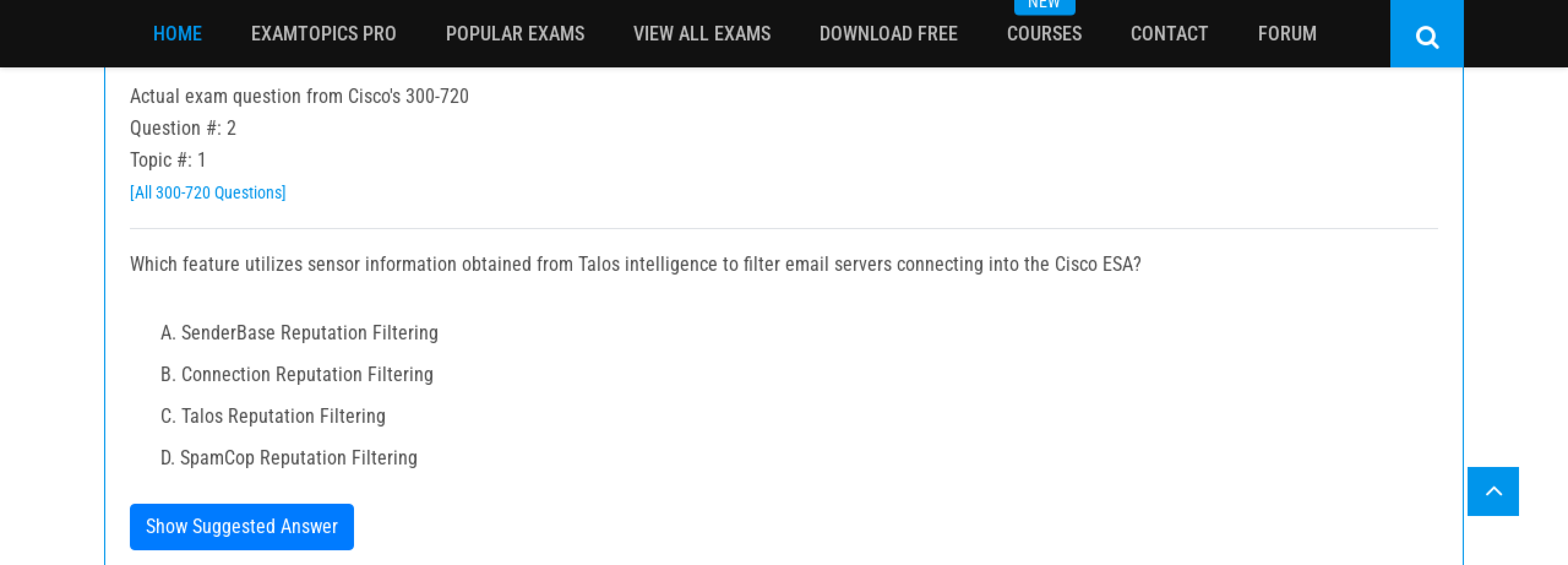
Which SMTP extension does Cisco ESA support for email security?

A. ETRN

B. UTF8SMTP

C. PIPELINING

D. STARTTLS



Actual exam question from Cisco's 300-720

Question #: 2

Topic #: 1

[All 300-720 Questions]

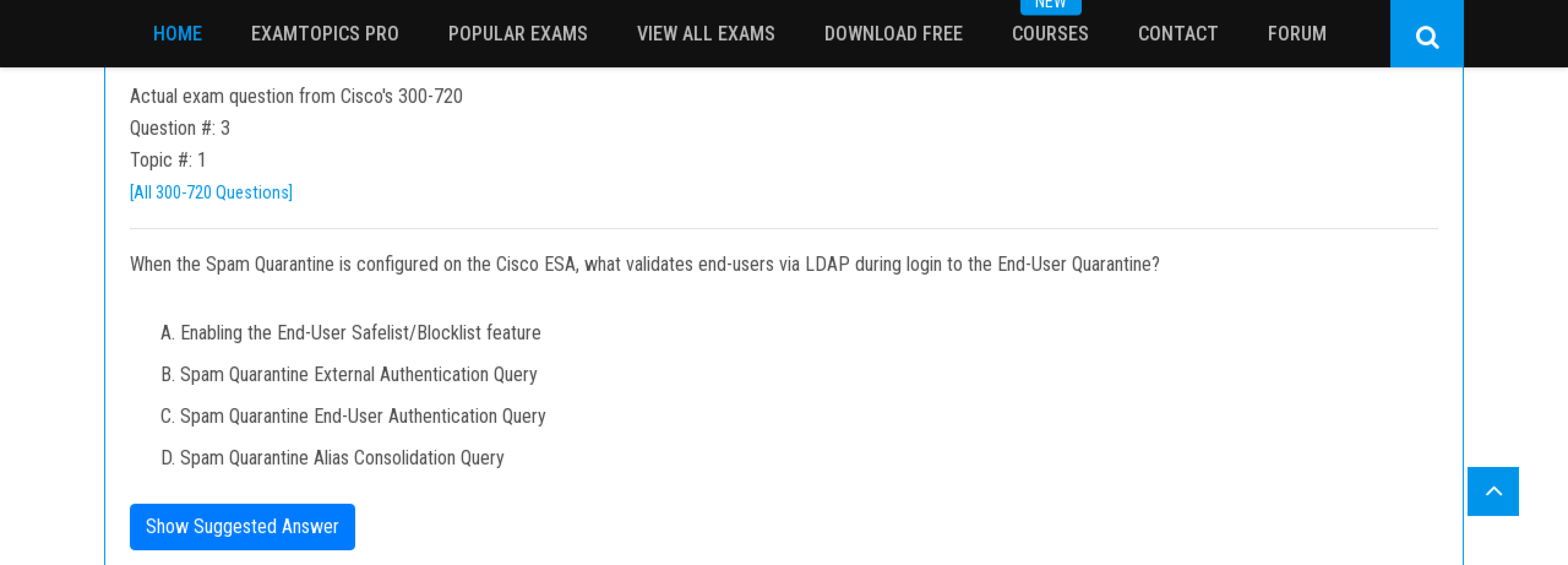
Which feature utilizes sensor information obtained from Talos intelligence to filter email servers connecting into the Cisco ESA?

A. SenderBase Reputation Filtering

B. Connection Reputation Filtering

C. Talos Reputation Filtering

D. SpamCop Reputation Filtering



Actual exam question from Cisco's 300-720

Question #: 3

Topic #: 1

[All 300-720 Questions]

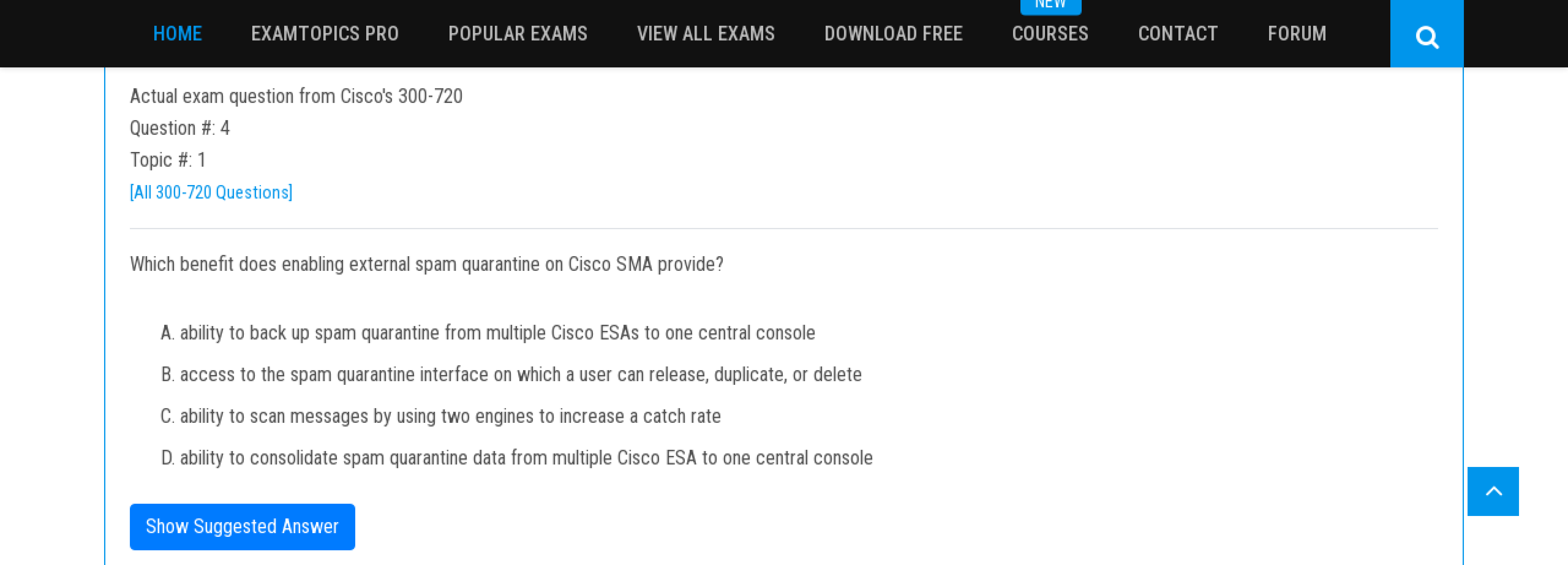
When the Spam Quarantine is configured on the Cisco ESA, what validates end-users via LDAP during login to the End-User Quarantine?

A. Enabling the End-User Safelist/Blocklist feature

B. Spam Quarantine External Authentication Query

C. Spam Quarantine End-User Authentication Query

D. Spam Quarantine Alias Consolidation Query



Actual exam question from Cisco's 300-720

Question #: 4

Topic #: 1

[All 300-720 Questions]

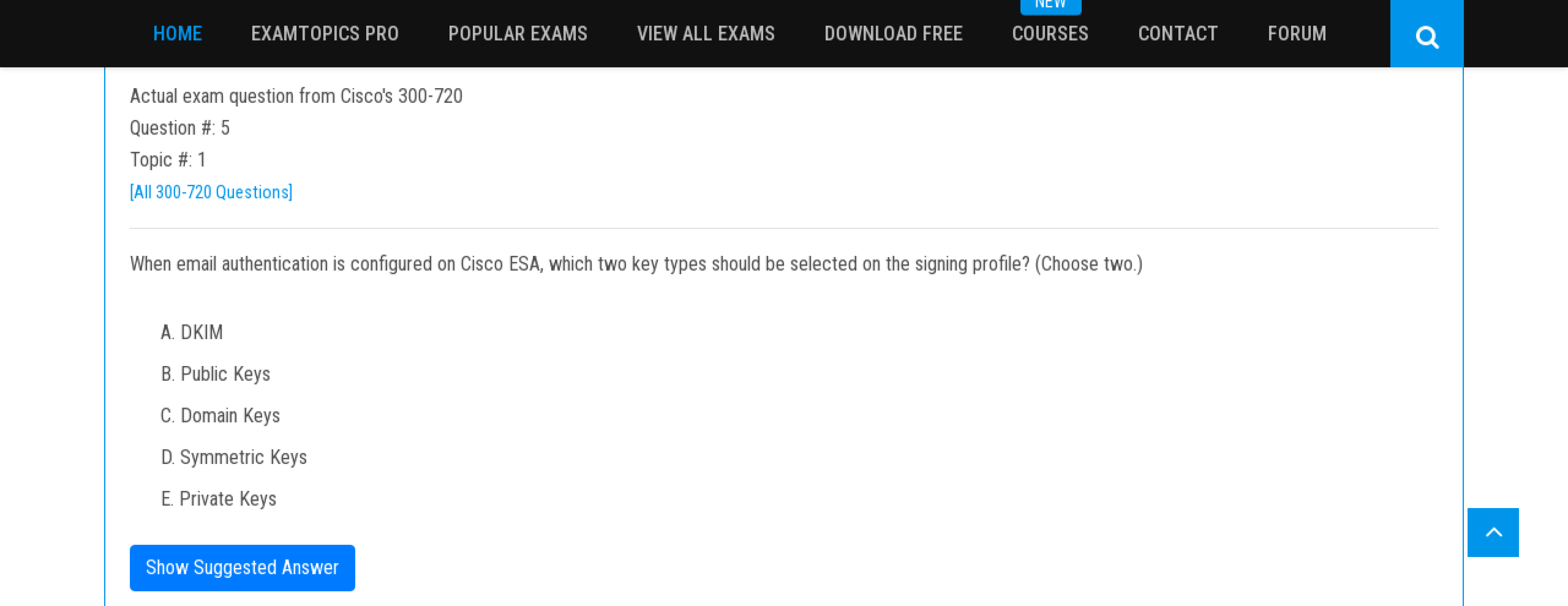
Which benefit does enabling external spam quarantine on Cisco SMA provide?

A. ability to back up spam quarantine from multiple Cisco ESAs to one central console

B. access to the spam quarantine interface on which a user can release, duplicate, or delete

C. ability to scan messages by using two engines to increase a catch rate

D. ability to consolidate spam quarantine data from multiple Cisco ESA to one central console



Actual exam question from Cisco's 300-720

Question #: 5

Topic #: 1

[All 300-720 Questions]

When email authentication is configured on Cisco ESA, which two key types should be selected on the signing profile? (Choose two.)

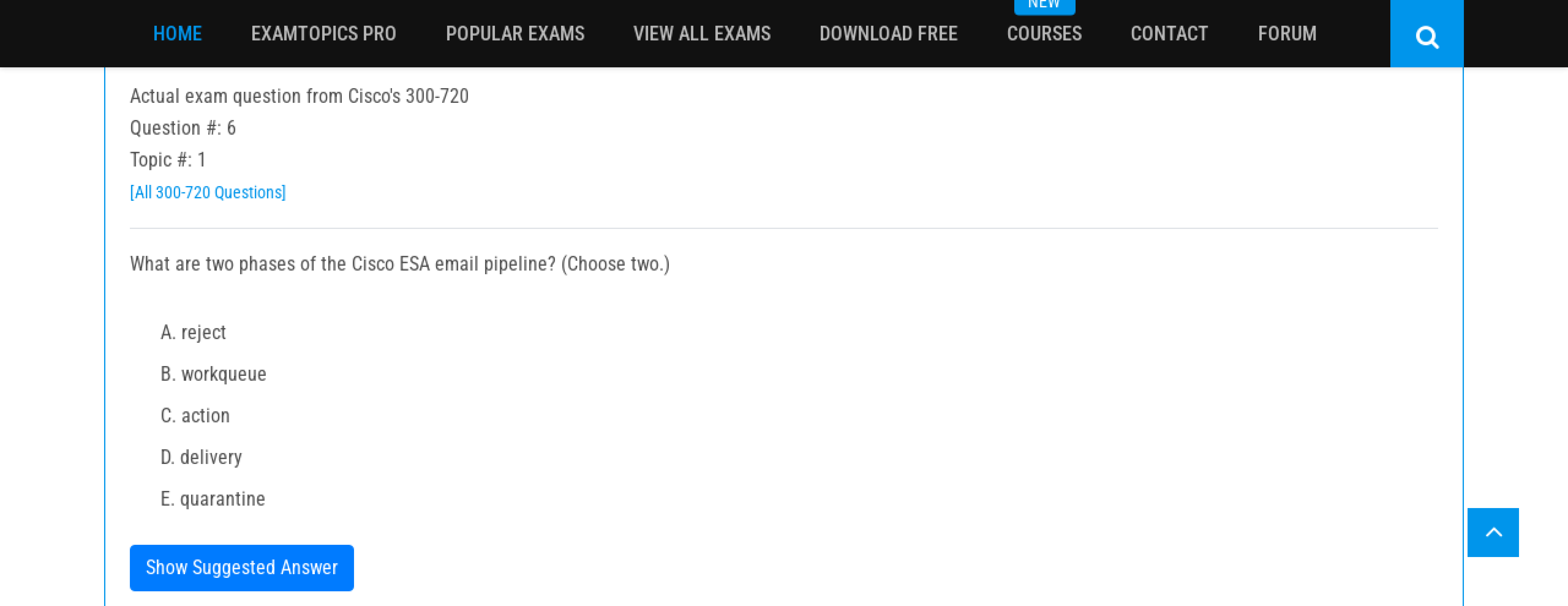
A. DKIM

B. Public Keys

C. Domain Keys

D. Symmetric Keys

E. Private Keys



Actual exam question from Cisco's 300-720

Question #: 6

Topic #: 1

[All 300-720 Questions]

What are two phases of the Cisco ESA email pipeline? (Choose two.)

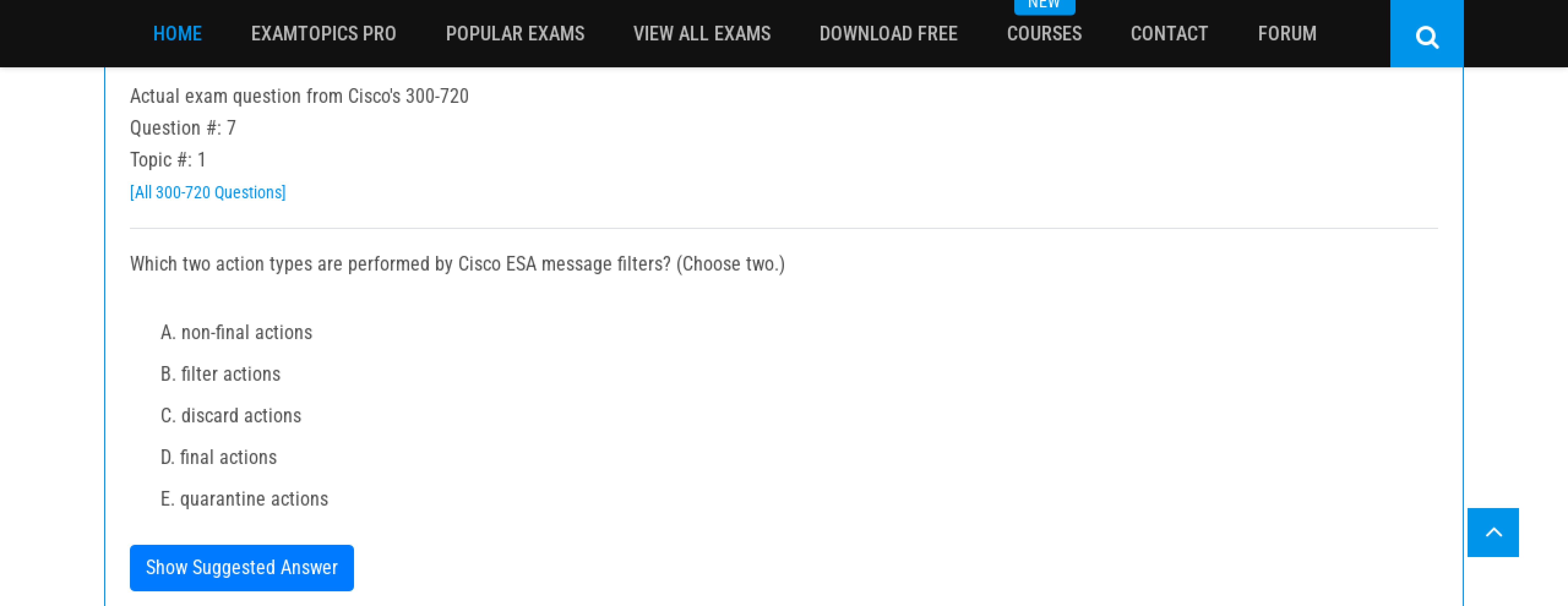
A. reject

B. workqueue

C. action

D. delivery

E. quarantine



Actual exam question from Cisco's 300-720

Question #: 7

Topic #: 1

[All 300-720 Questions]

Which two action types are performed by Cisco ESA message filters? (Choose two.)

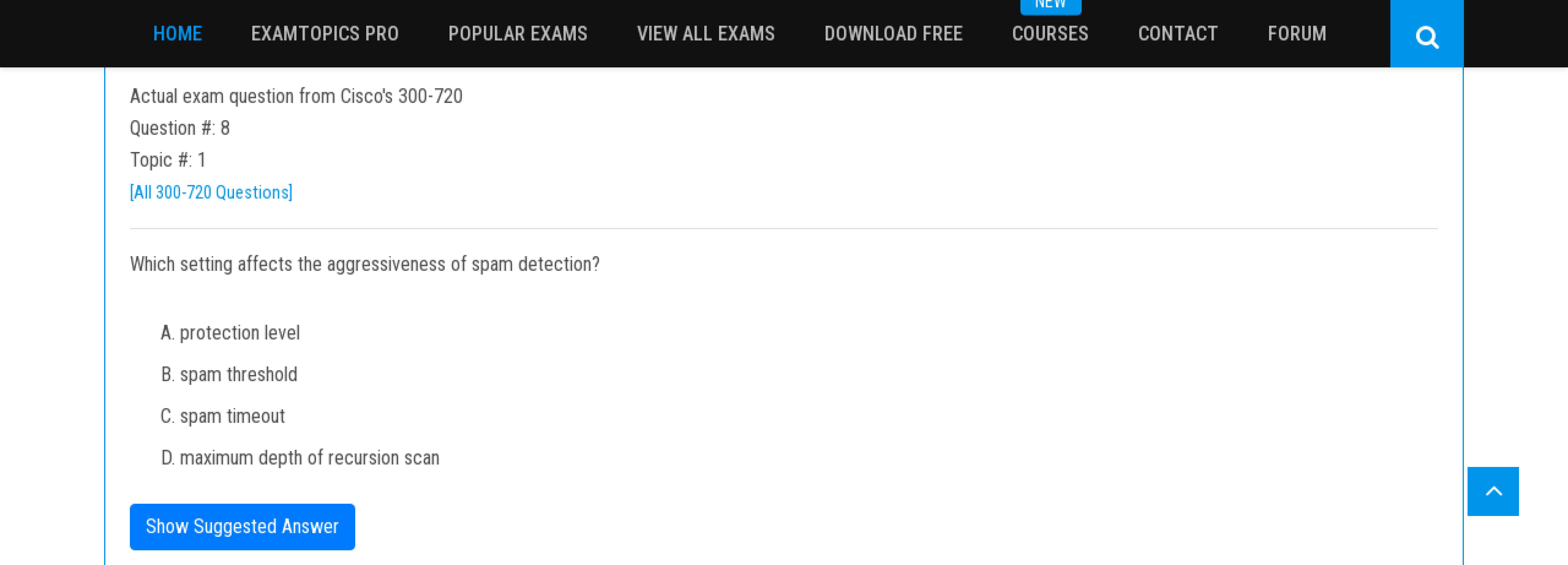
A. non-final actions

B. filter actions

C. discard actions

D. final actions

E. quarantine actions



Actual exam question from Cisco's 300-720

Question #: 8

Topic #: 1

[All 300-720 Questions]

Which setting affects the aggressiveness of spam detection?

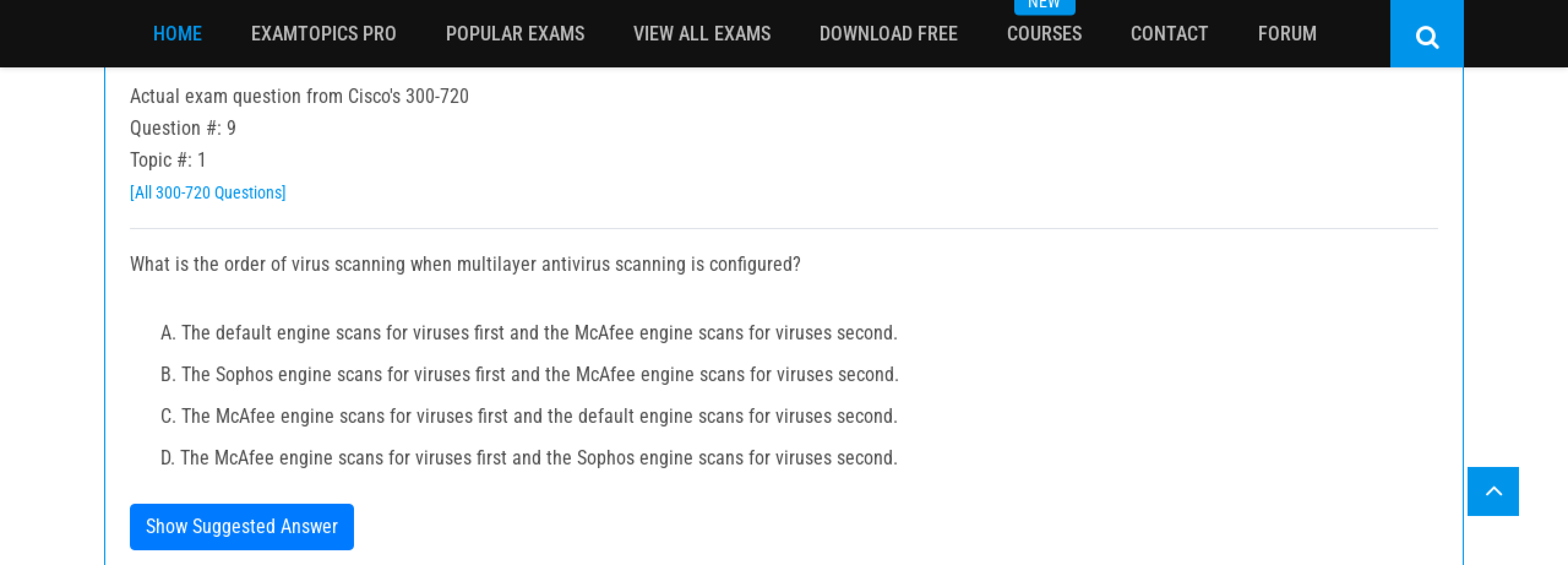
A. protection level

B. spam threshold

C. spam timeout

D. maximum depth of recursion scan

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 9

Topic #: 1

[All 300-720 Questions]

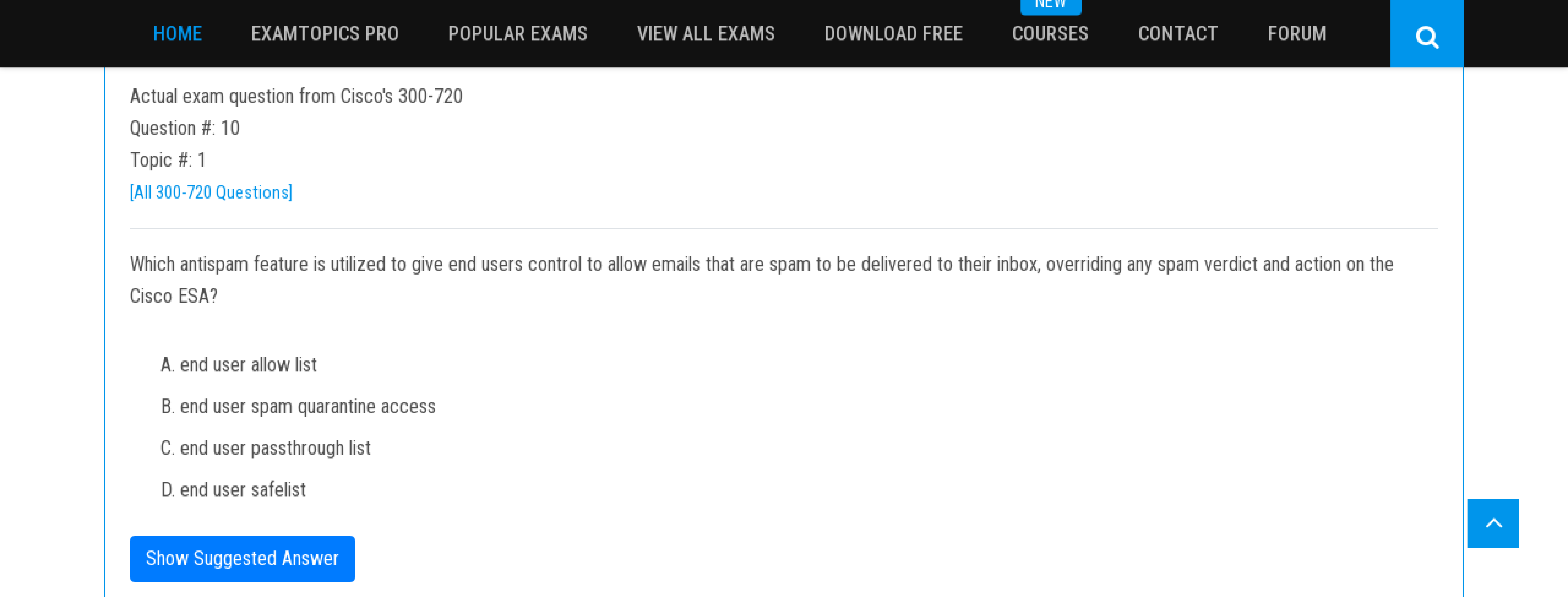
What is the order of virus scanning when multilayer antivirus scanning is configured?

A. The default engine scans for viruses first and the McAfee engine scans for viruses second.

B. The Sophos engine scans for viruses first and the McAfee engine scans for viruses second.

C. The McAfee engine scans for viruses first and the default engine scans for viruses second.

D. The McAfee engine scans for viruses first and the Sophos engine scans for viruses second.



Actual exam question from Cisco's 300-720

Question #: 10

Topic #: 1

[All 300-720 Questions]

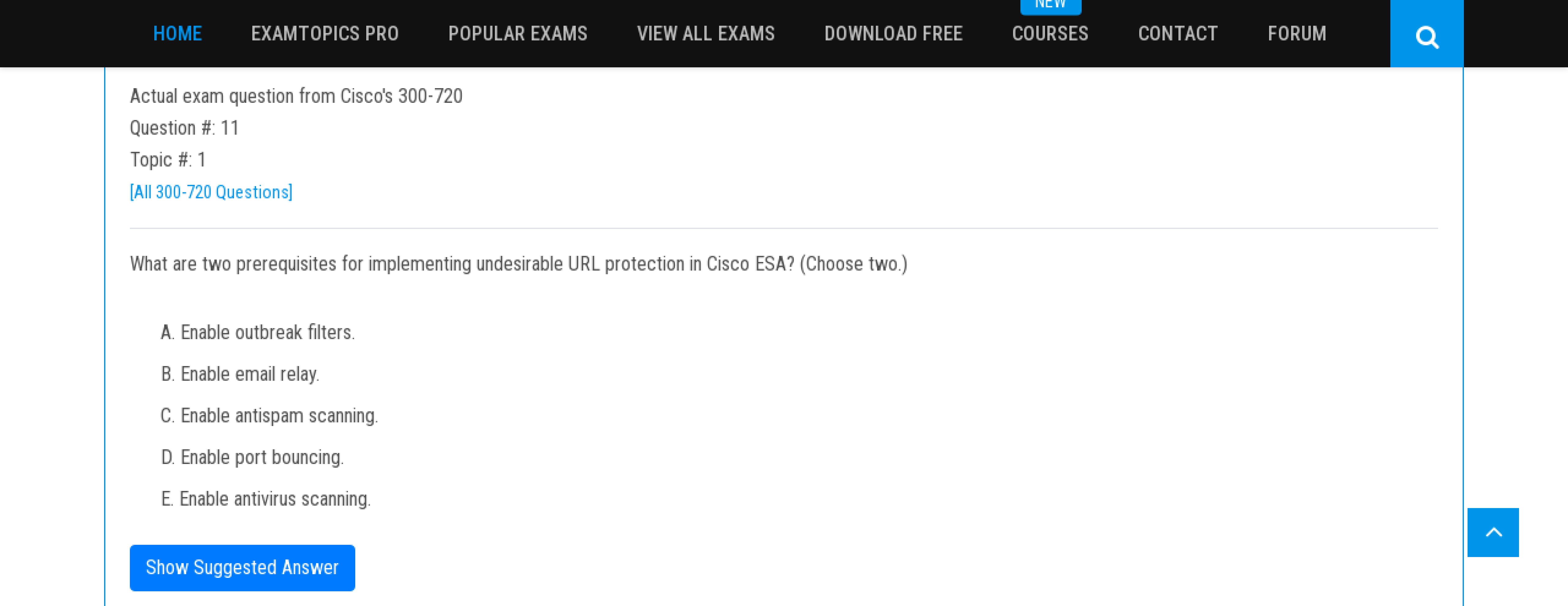
Which antispam feature is utilized to give end users control to allow emails that are spam to be delivered to their inbox, overriding any spam verdict and action on the Cisco ESA?

A. end user allow list

B. end user spam quarantine access

C. end user passthrough list

D. end user safelist



Actual exam question from Cisco's 300-720

Question #: 11

Topic #: 1

[All 300-720 Questions]

What are two prerequisites for implementing undesirable URL protection in Cisco ESA? (Choose two.)

A. Enable outbreak filters.

B. Enable email relay.

C. Enable antispam scanning.

D. Enable port bouncing.

E. Enable antivirus scanning.

Show Suggested Answer

Actual exam question from Cisco's 300-720

Question #: 12

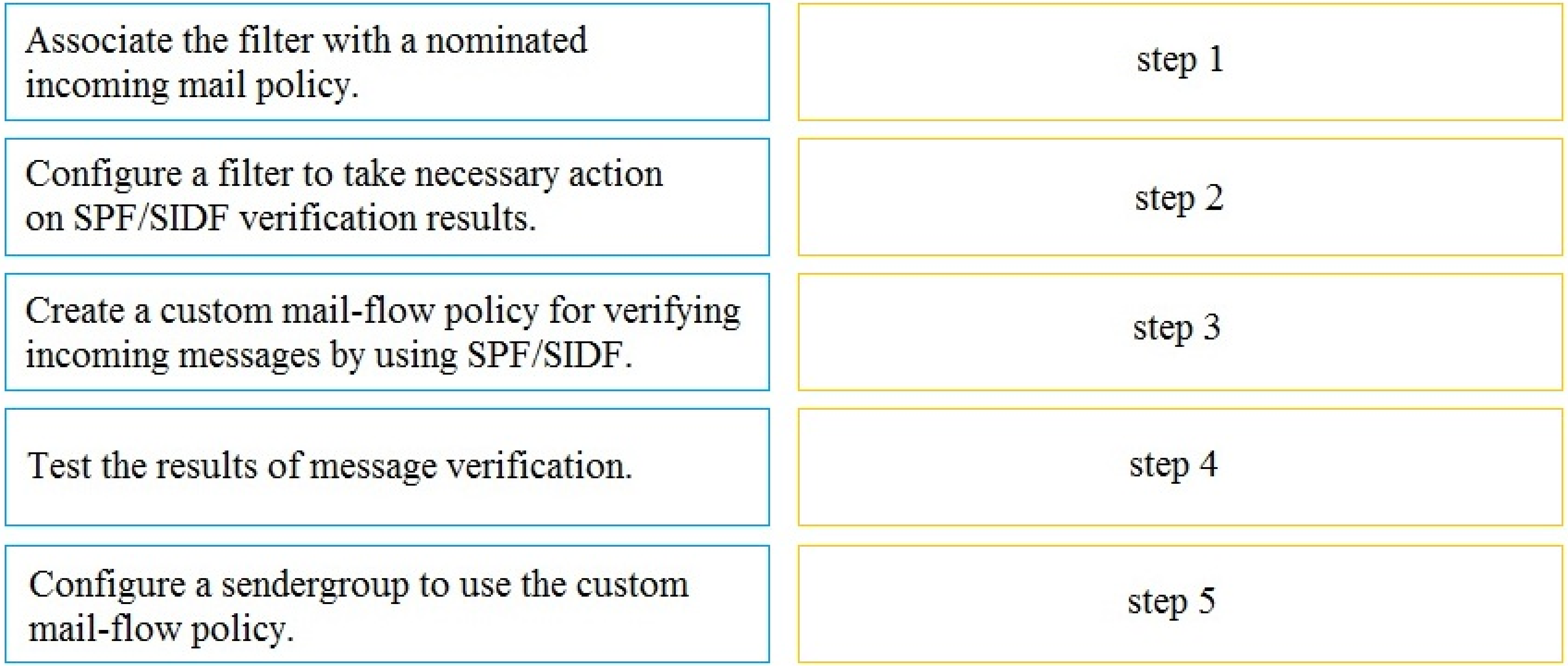
Topic #: 1

[All 300-720 Questions]

DRAG DROP -

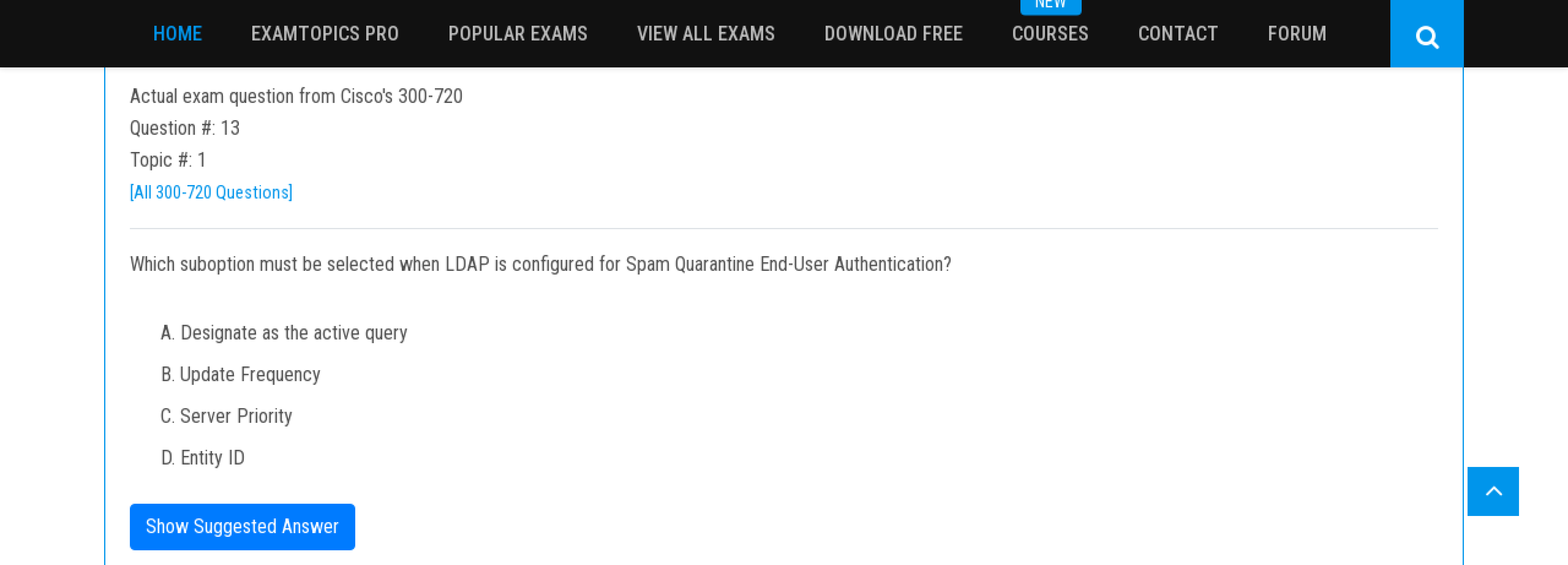
Drag and drop the steps to configure Cisco ESA to use SPF/SIDF verification from the left into the correct order on the right.

Select and Place:



Associate the filter with a nominated incoming mail policy.	step 1
Configure a filter to take necessary action on SPF/SIDF verification results.	step 2
Create a custom mail-flow policy for verifying incoming messages by using SPF/SIDF.	step 3
Test the results of message verification.	step 4
Configure a sendergroup to use the custom mail-flow policy.	step 5

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 13

Topic #: 1

[All 300-720 Questions]

Which suboption must be selected when LDAP is configured for Spam Quarantine End-User Authentication?

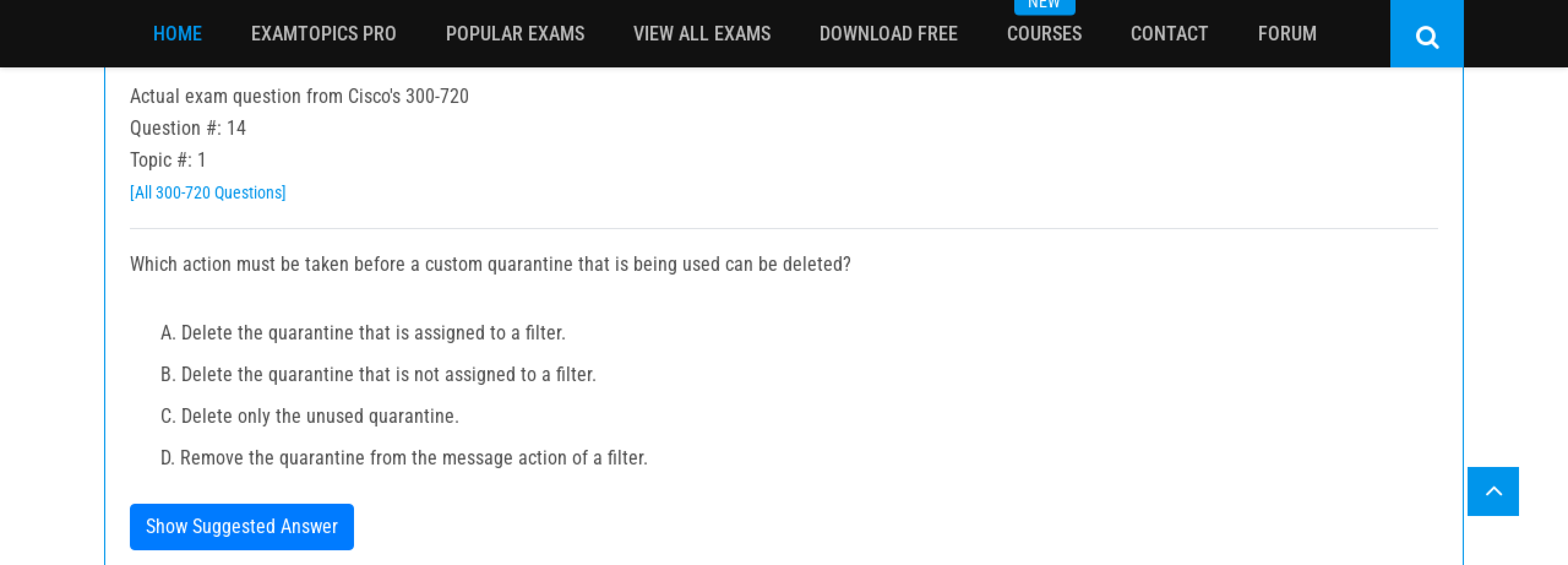
A. Designate as the active query

B. Update Frequency

C. Server Priority

D. Entity ID

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 14

Topic #: 1

[All 300-720 Questions]

Which action must be taken before a custom quarantine that is being used can be deleted?

A. Delete the quarantine that is assigned to a filter.

B. Delete the quarantine that is not assigned to a filter.

C. Delete only the unused quarantine.

D. Remove the quarantine from the message action of a filter.

Actual exam question from Cisco's 300-720

Question #: 15

Topic #: 1

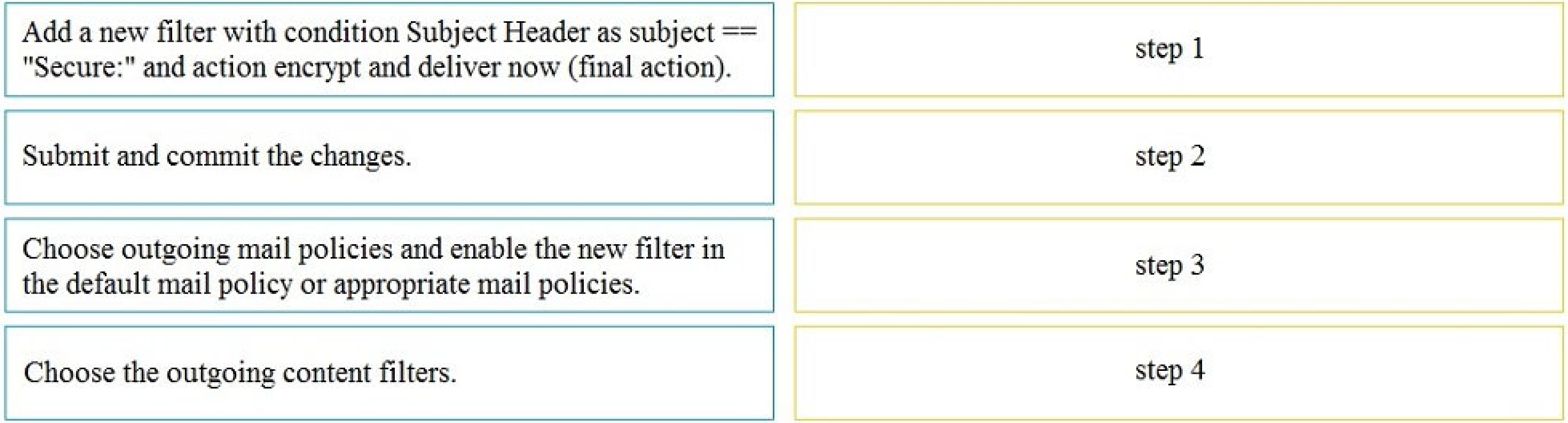
[All 300-720 Questions]

DRAG DROP -

An Encryption Profile has been set up on the Cisco ESA.

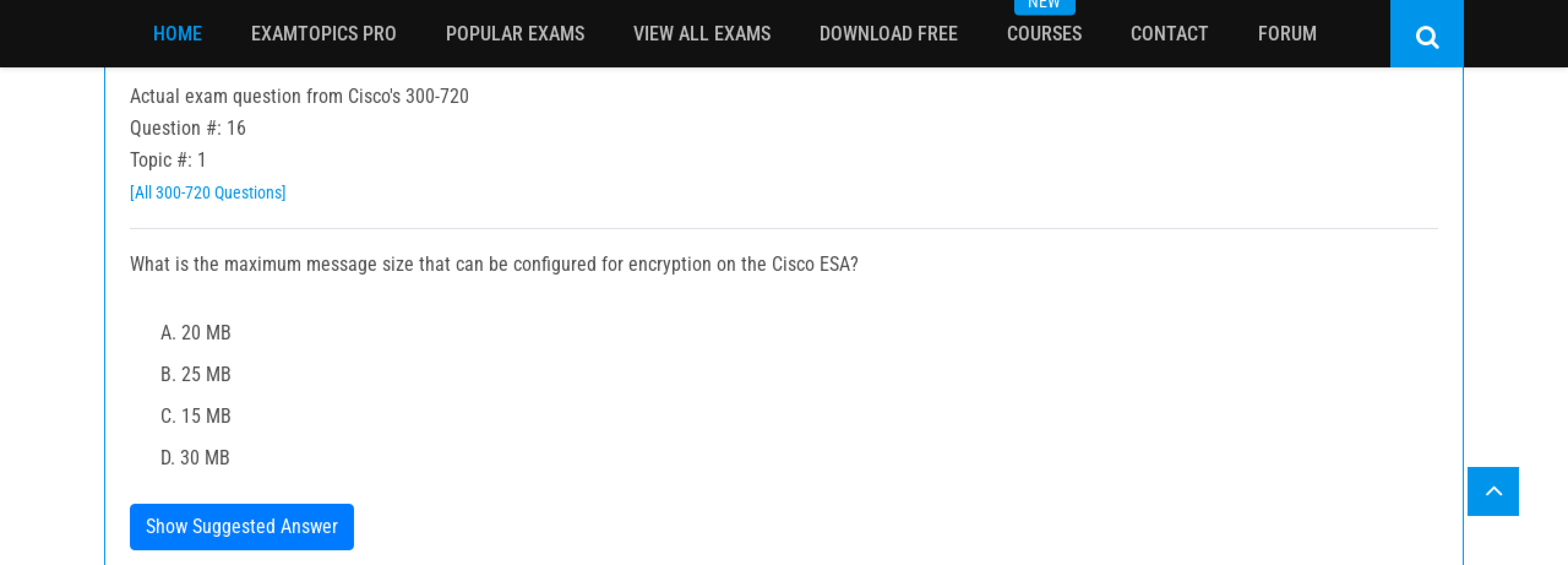
Drag and drop the steps from the left for creating an outgoing content filter to encrypt emails that contains the subject "Secure:" into the correct order on the right.

Select and Place:



Add a new filter with condition Subject Header as subject == "Secure:" and action encrypt and deliver now (final action).	step 1
Submit and commit the changes.	step 2
Choose outgoing mail policies and enable the new filter in the default mail policy or appropriate mail policies.	step 3
Choose the outgoing content filters.	step 4

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 16

Topic #: 1

[All 300-720 Questions]

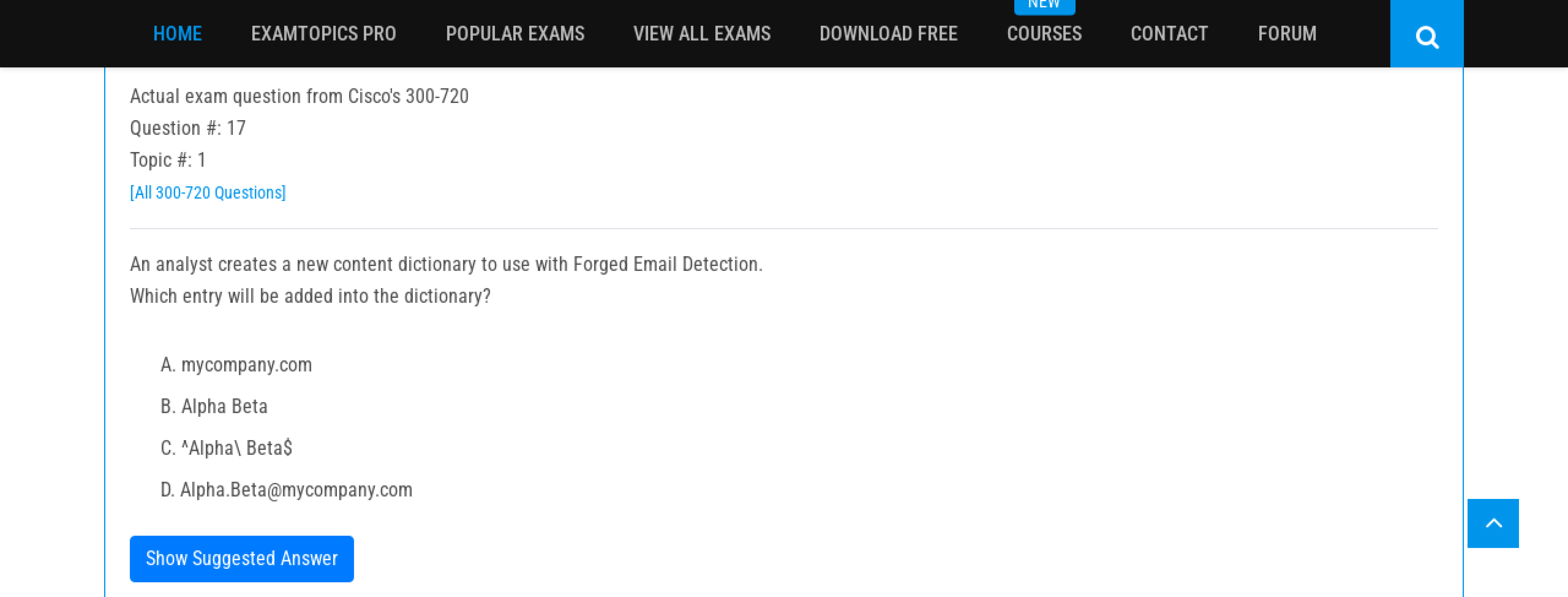
What is the maximum message size that can be configured for encryption on the Cisco ESA?

A. 20 MB

B. 25 MB

C. 15 MB

D. 30 MB



Actual exam question from Cisco's 300-720

Question #: 17

Topic #: 1

[All 300-720 Questions]

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

Which entry will be added into the dictionary?

A. mycompany.com

B. Alpha Beta

C. ^Alpha\ Beta$

D. Alpha.Beta@mycompany.com

Actual exam question from Cisco's 300-720

Question #: 18

Topic #: 1

[All 300-720 Questions]

Which process is skipped when an email is received from safedomain.com, which is on the safelist?

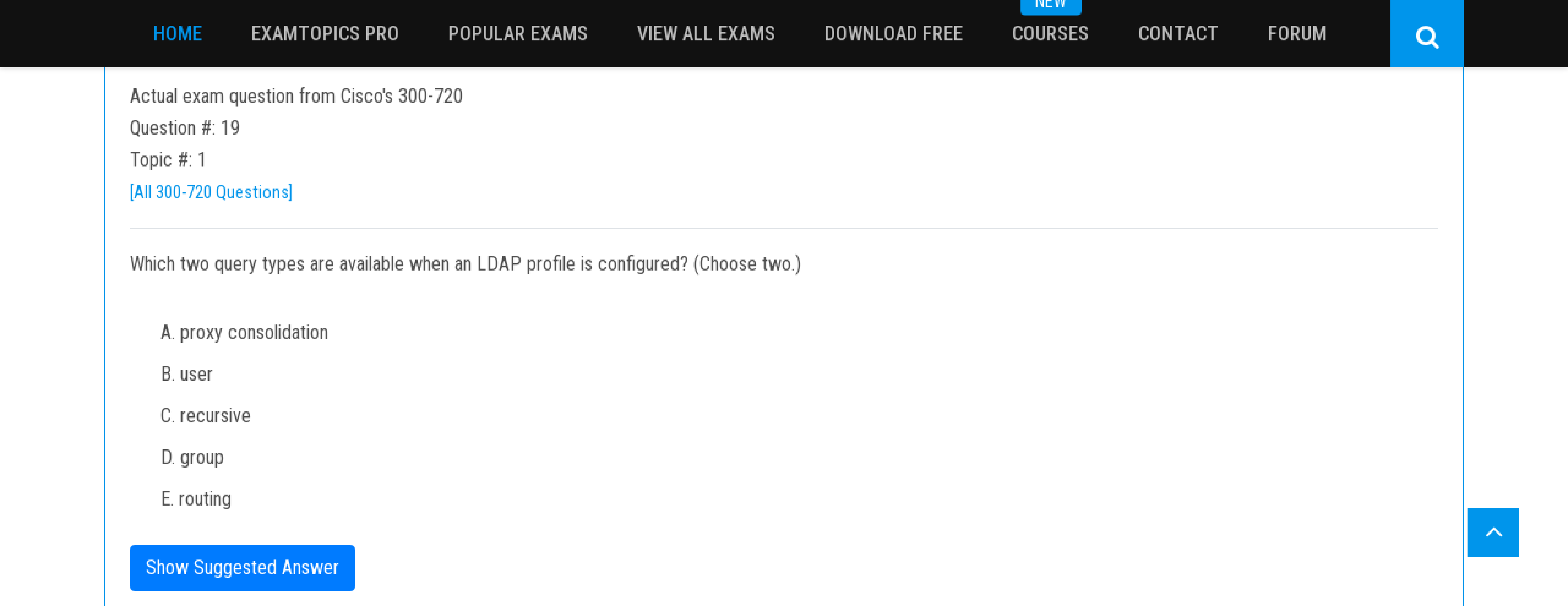
A. message filter

B. antivirus scanning

C. outbreak filter

D. antispam scanning

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 19

Topic #: 1

[All 300-720 Questions]

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

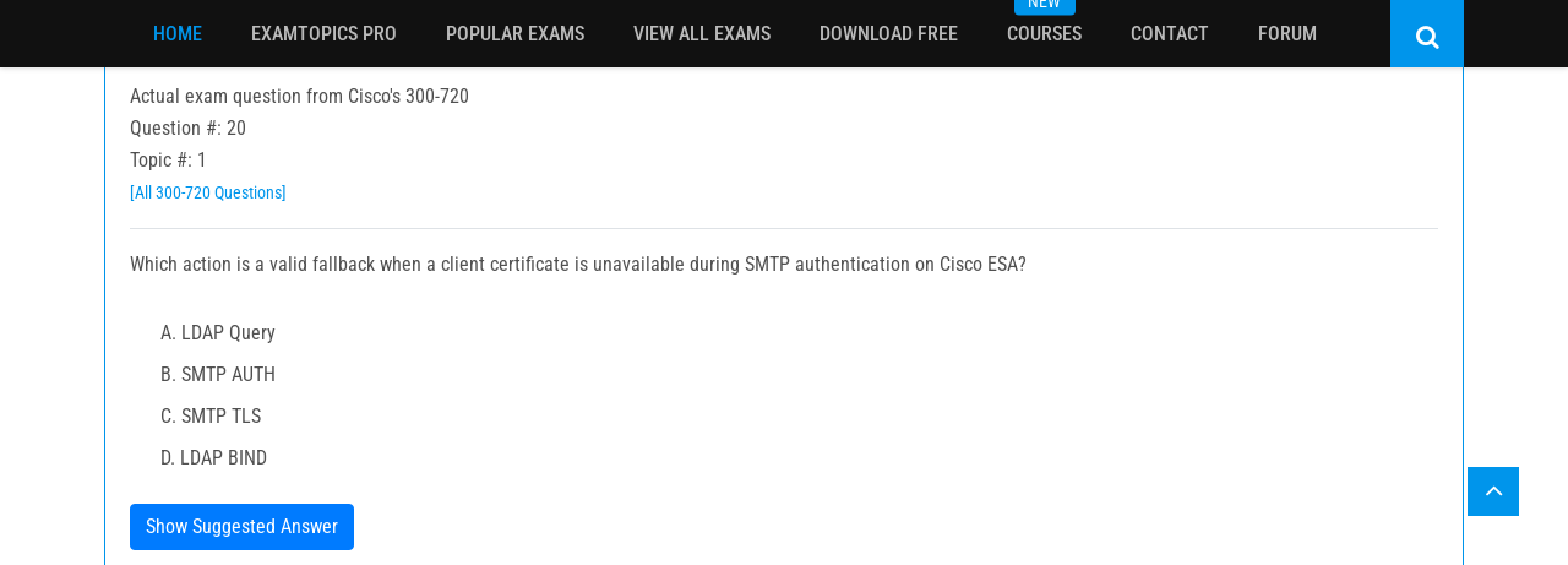
A. proxy consolidation

B. user

C. recursive

D. group

E. routing



Actual exam question from Cisco's 300-720

Question #: 20

Topic #: 1

[All 300-720 Questions]

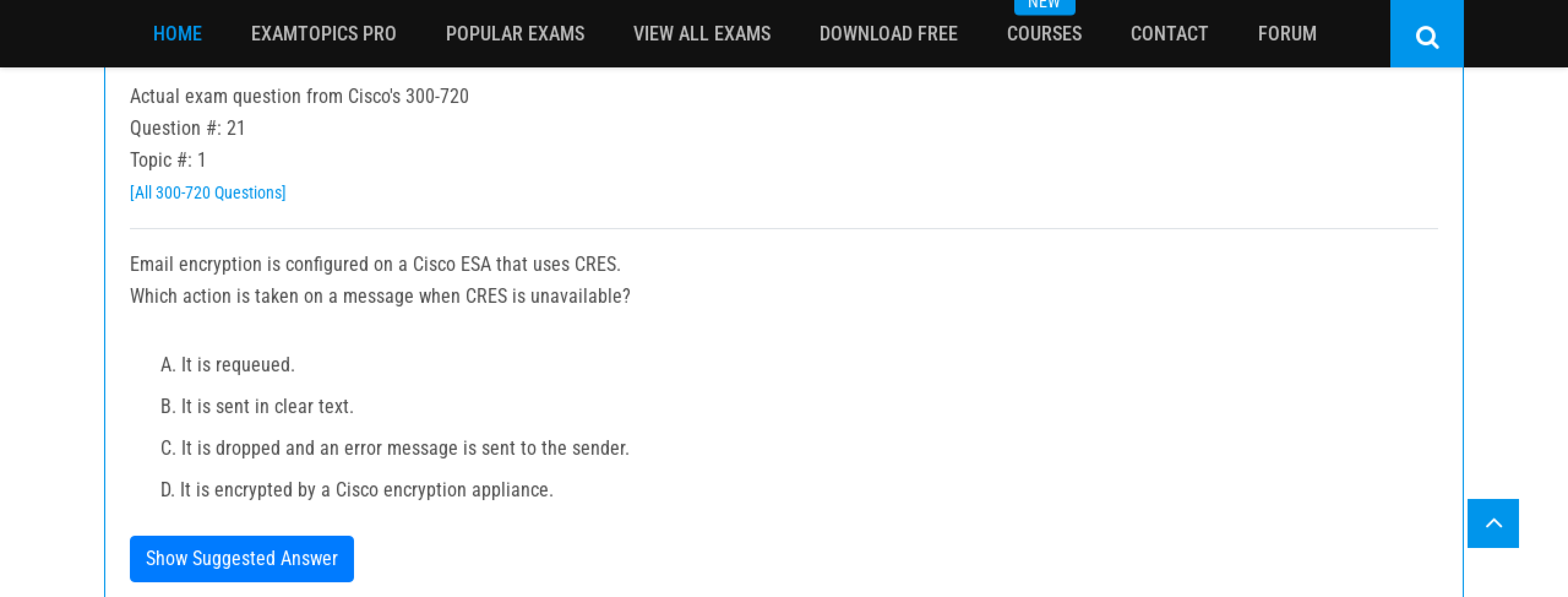
Which action is a valid fallback when a client certificate is unavailable during SMTP authentication on Cisco ESA?

A. LDAP Query

B. SMTP AUTH

C. SMTP TLS

D. LDAP BIND



Actual exam question from Cisco's 300-720

Question #: 21

Topic #: 1

[All 300-720 Questions]

Email encryption is configured on a Cisco ESA that uses CRES.

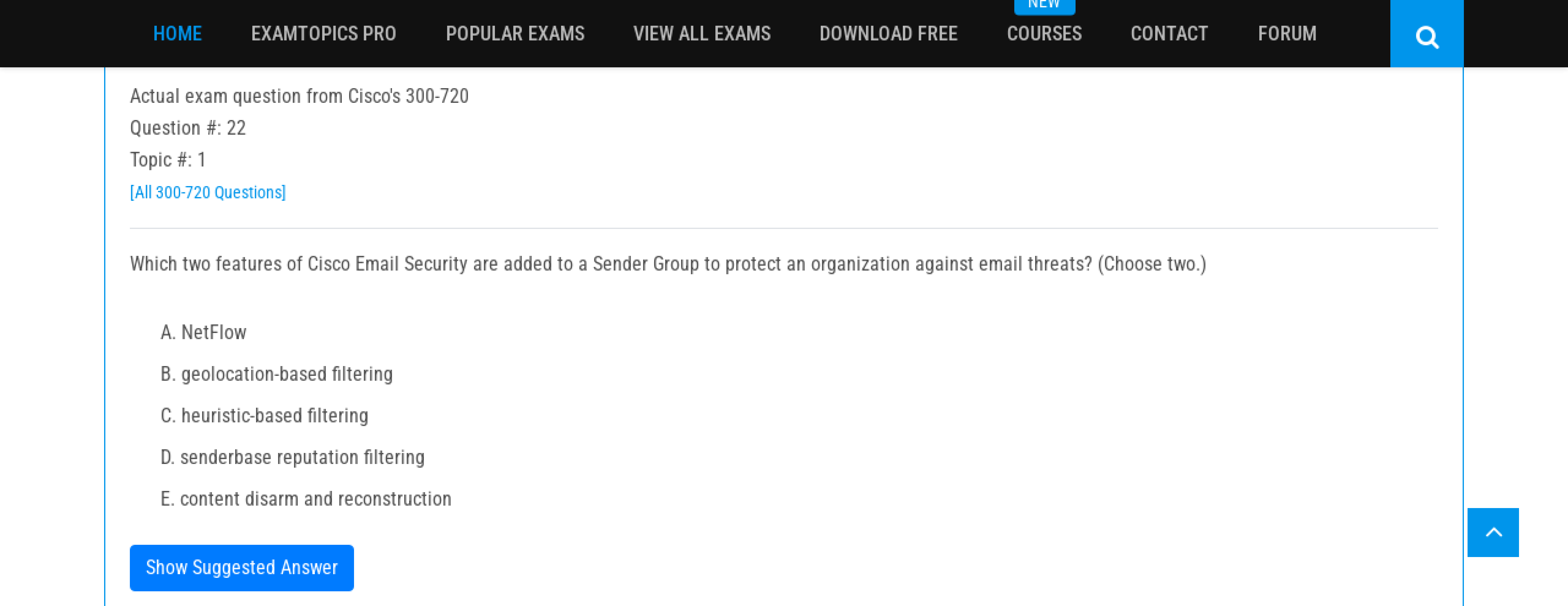
Which action is taken on a message when CRES is unavailable?

A. It is requeued.

B. It is sent in clear text.

C. It is dropped and an error message is sent to the sender.

D. It is encrypted by a Cisco encryption appliance.



Actual exam question from Cisco's 300-720

Question #: 22

Topic #: 1

[All 300-720 Questions]

Which two features of Cisco Email Security are added to a Sender Group to protect an organization against email threats? (Choose two.)

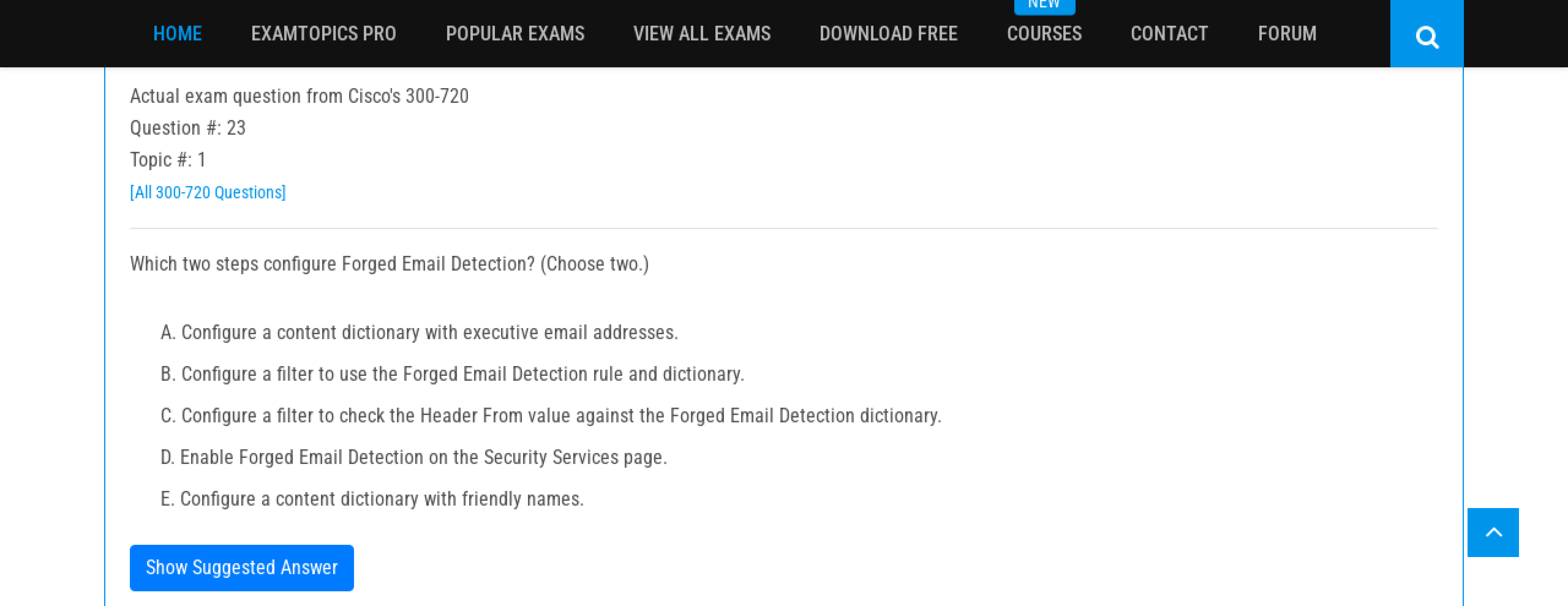
A. NetFlow

B. geolocation-based filtering

C. heuristic-based filtering

D. senderbase reputation filtering

E. content disarm and reconstruction



Actual exam question from Cisco's 300-720

Question #: 23

Topic #: 1

[All 300-720 Questions]

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

A. Configure a content dictionary with executive email addresses.

B. Configure a filter to use the Forged Email Detection rule and dictionary.

C. Configure a filter to check the Header From value against the Forged Email Detection dictionary.

D. Enable Forged Email Detection on the Security Services page.

E. Configure a content dictionary with friendly names.

Actual exam question from Cisco's 300-720

Question #: 24

Topic #: 1

[All 300-720 Questions]

What is the default behavior of any listener for TLS communication?

A. preferred-verify

B. off

C. preferred

D. required

Show Suggested Answer

Actual exam question from Cisco's 300-720

Question #: 25

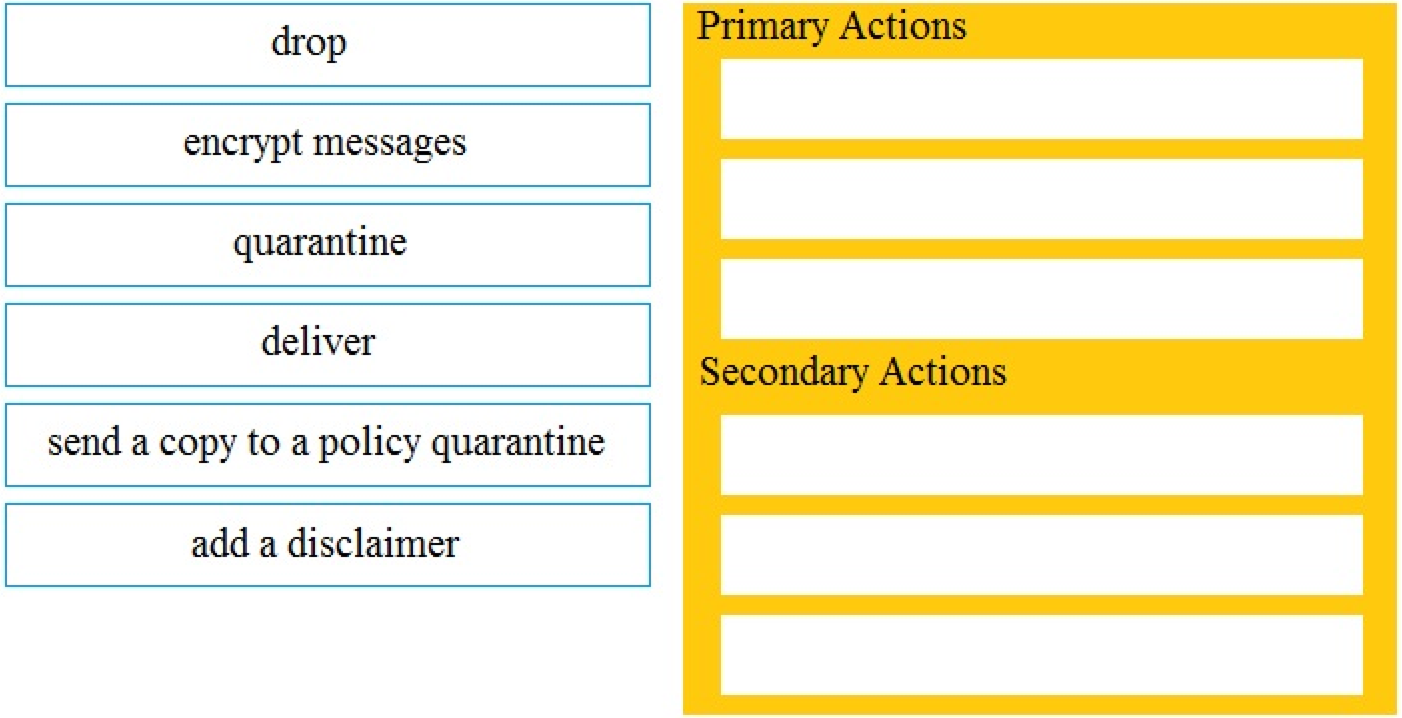
Topic #: 1

[All 300-720 Questions]

DRAG DROP -

Drag and drop the Cisco ESA reactions to a possible DLP from the left onto the correct action types on the right.

Select and Place:



drop

encrypt messages

quarantine

deliver

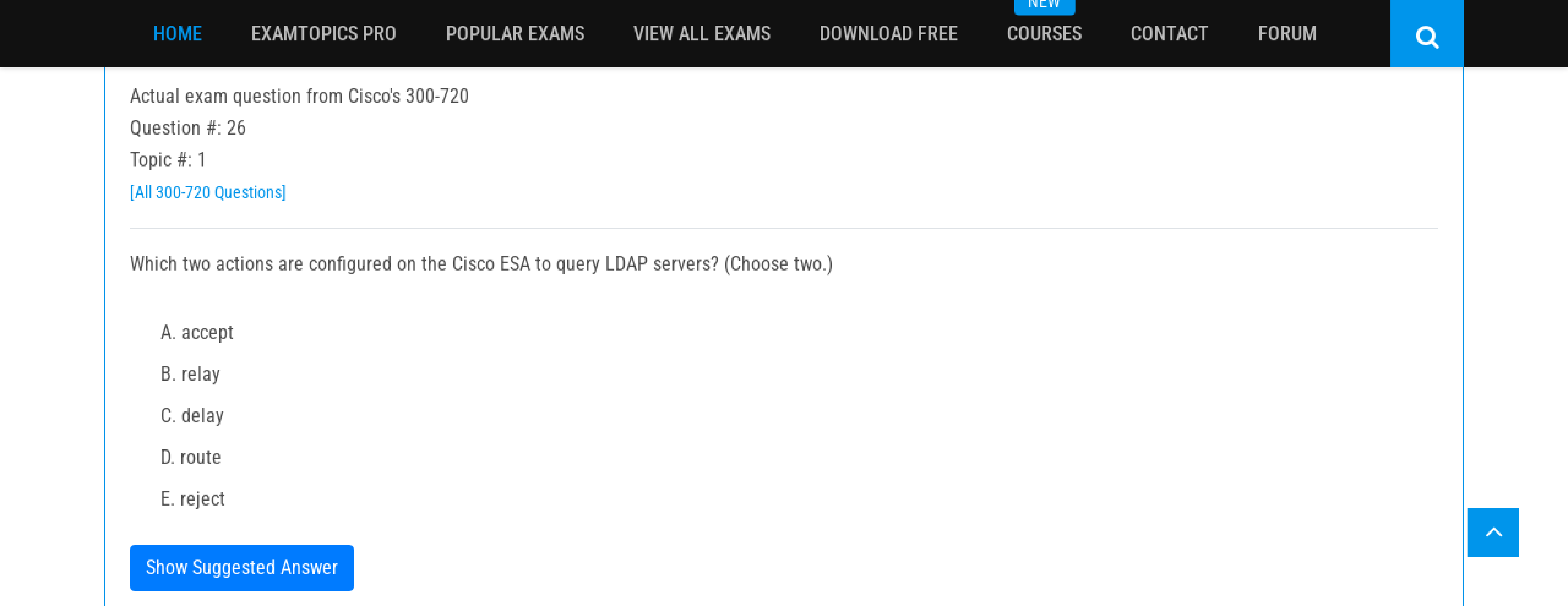
send a copy to a policy quarantine

add a disclaimer

Primary Actions

Secondary Actions

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 26

Topic #: 1

[All 300-720 Questions]

Which two actions are configured on the Cisco ESA to query LDAP servers? (Choose two.)

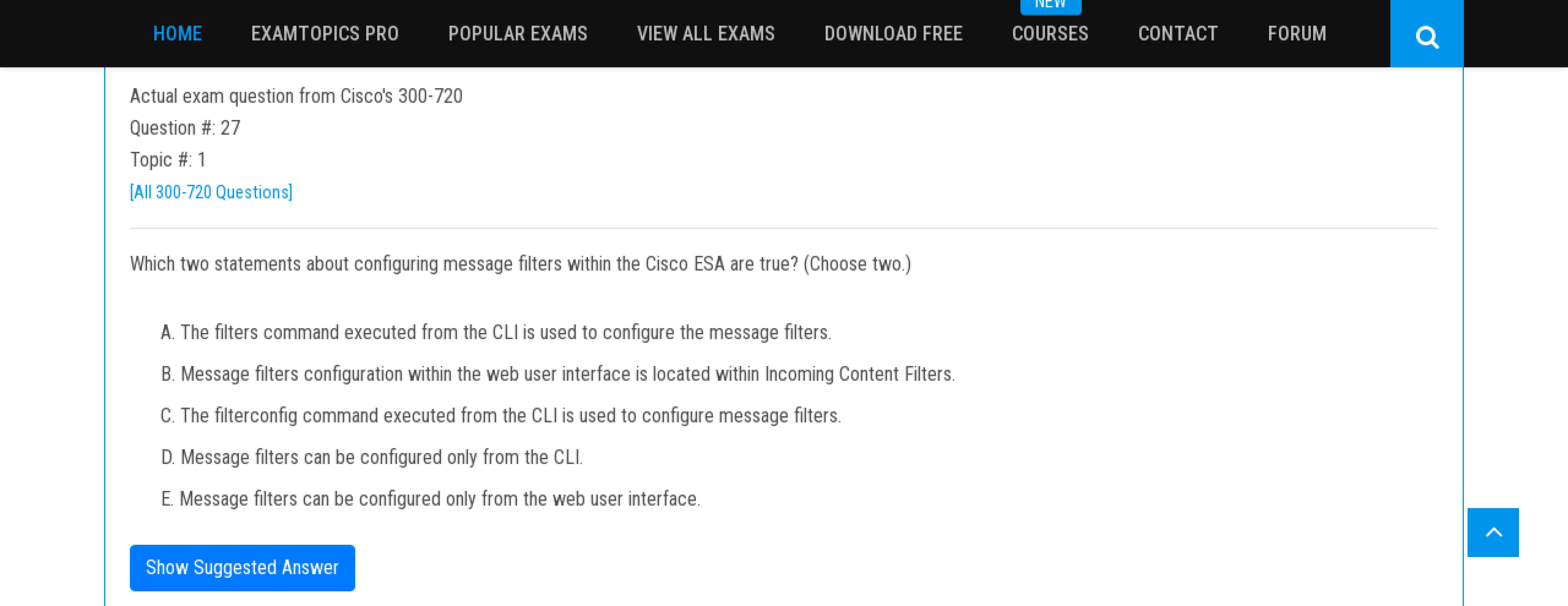
A. accept

B. relay

C. delay

D. route

E. reject



Actual exam question from Cisco's 300-720

Question #: 27

Topic #: 1

[All 300-720 Questions]

Which two statements about configuring message filters within the Cisco ESA are true? (Choose two.)

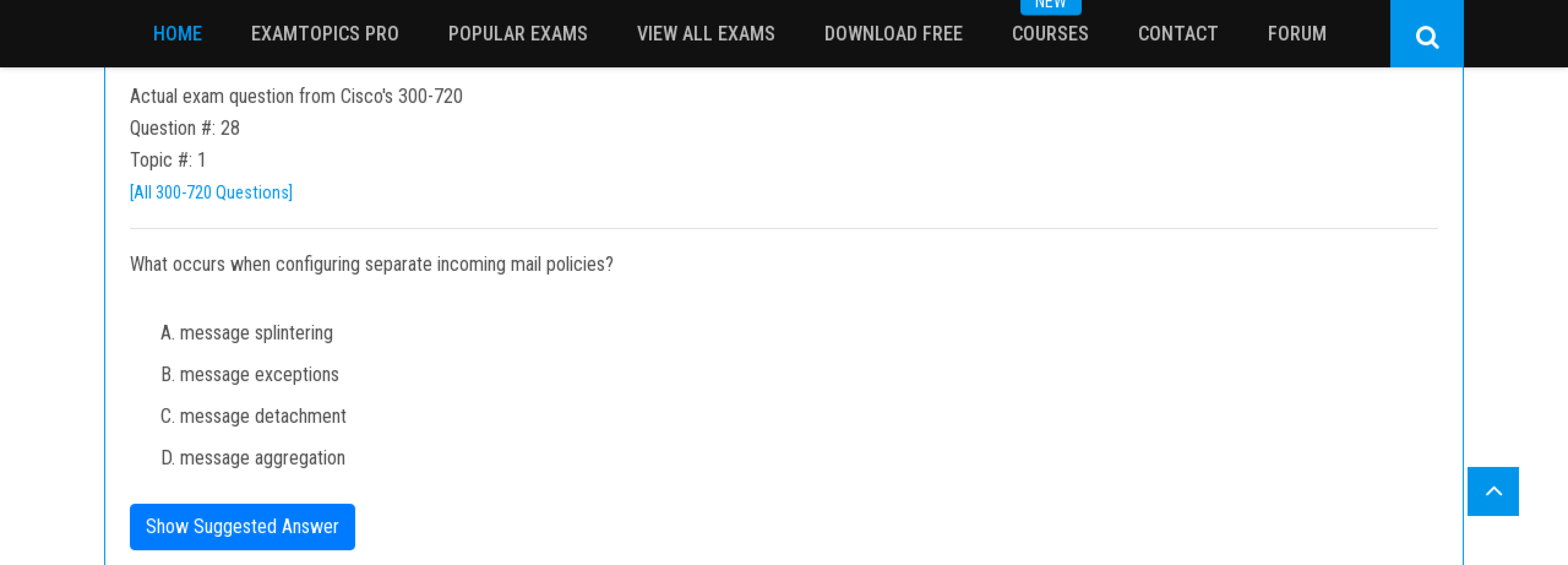
A. The filters command executed from the CLI is used to configure the message filters.

B. Message filters configuration within the web user interface is located within Incoming Content Filters.

C. The filterconfig command executed from the CLI is used to configure message filters.

D. Message filters can be configured only from the CLI.

E. Message filters can be configured only from the web user interface.



Actual exam question from Cisco's 300-720

Question #: 28

Topic #: 1

[All 300-720 Questions]

What occurs when configuring separate incoming mail policies?

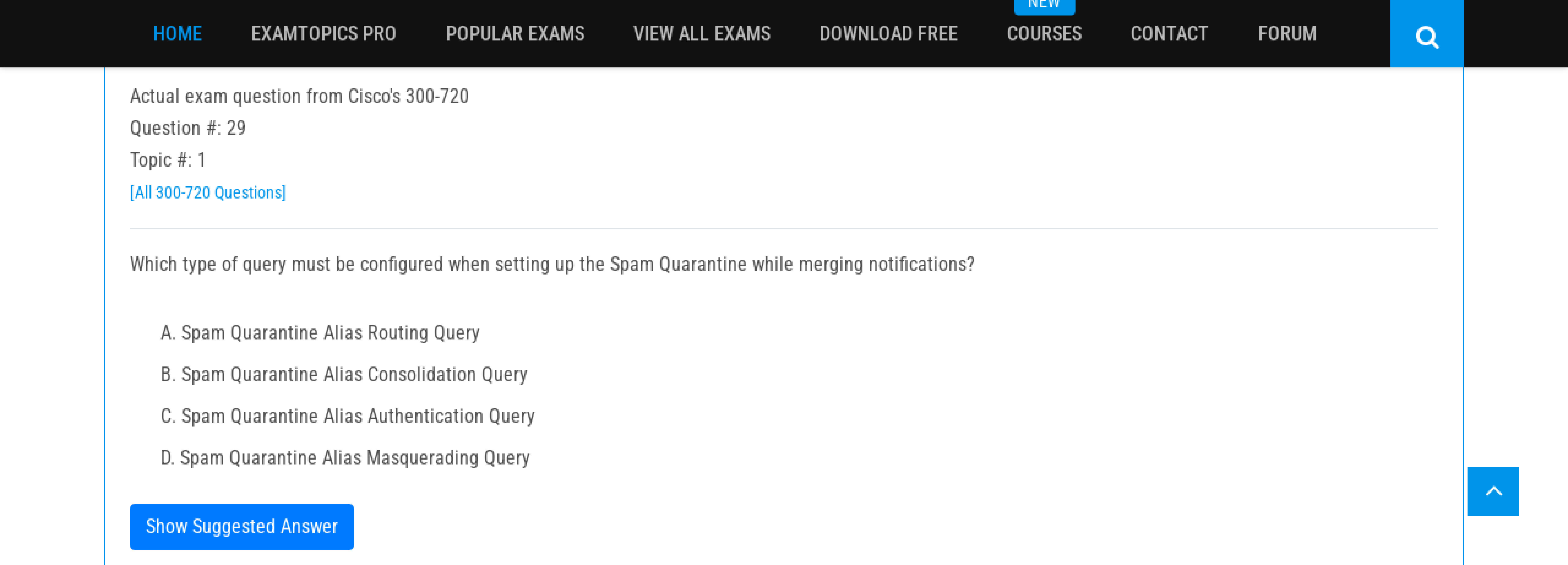
A. message splintering

B. message exceptions

C. message detachment

D. message aggregation

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 29

Topic #: 1

[All 300-720 Questions]

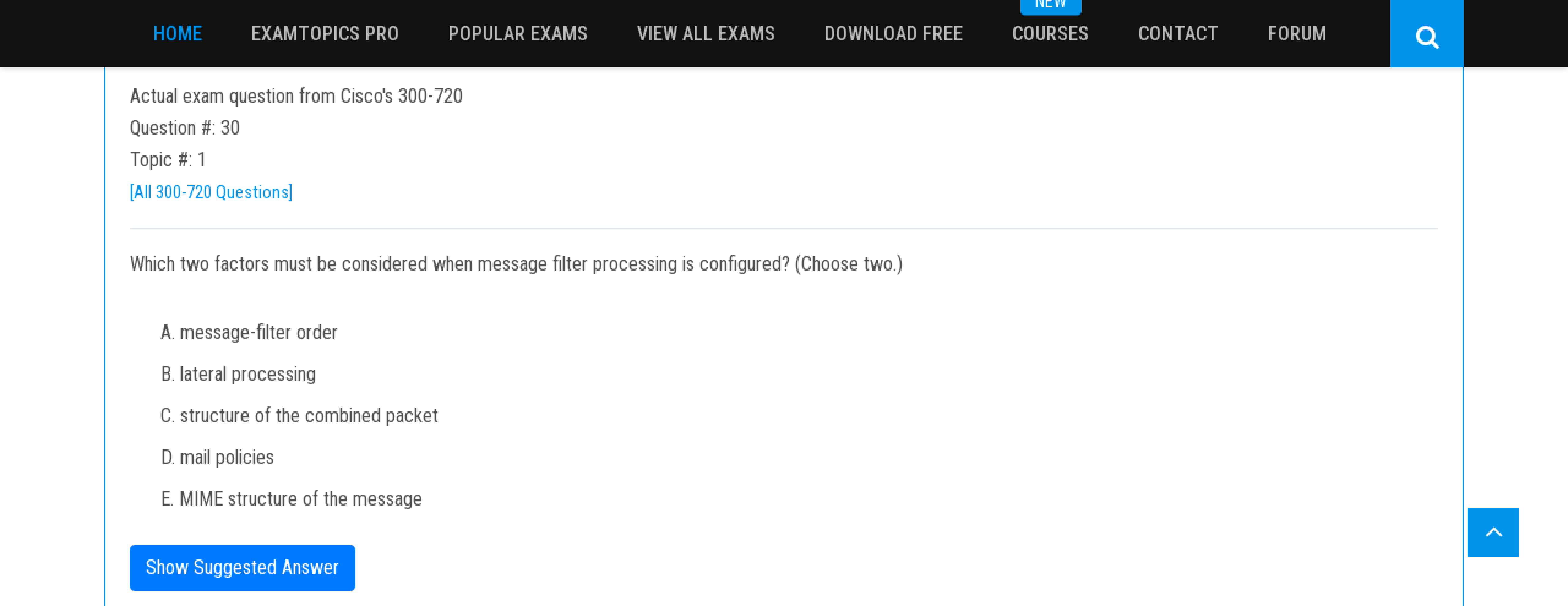
Which type of query must be configured when setting up the Spam Quarantine while merging notifications?

A. Spam Quarantine Alias Routing Query

B. Spam Quarantine Alias Consolidation Query

C. Spam Quarantine Alias Authentication Query

D. Spam Quarantine Alias Masquerading Query



Actual exam question from Cisco's 300-720

Question #: 30

Topic #: 1

[All 300-720 Questions]

Which two factors must be considered when message filter processing is configured? (Choose two.)

A. message-filter order

B. lateral processing

C. structure of the combined packet

D. mail policies

E. MIME structure of the message

Show Suggested Answer

Actual exam question from Cisco's 300-720

Question #: 31

Topic #: 1

[All 300-720 Questions]

How does the graymail safe unsubscribe feature function?

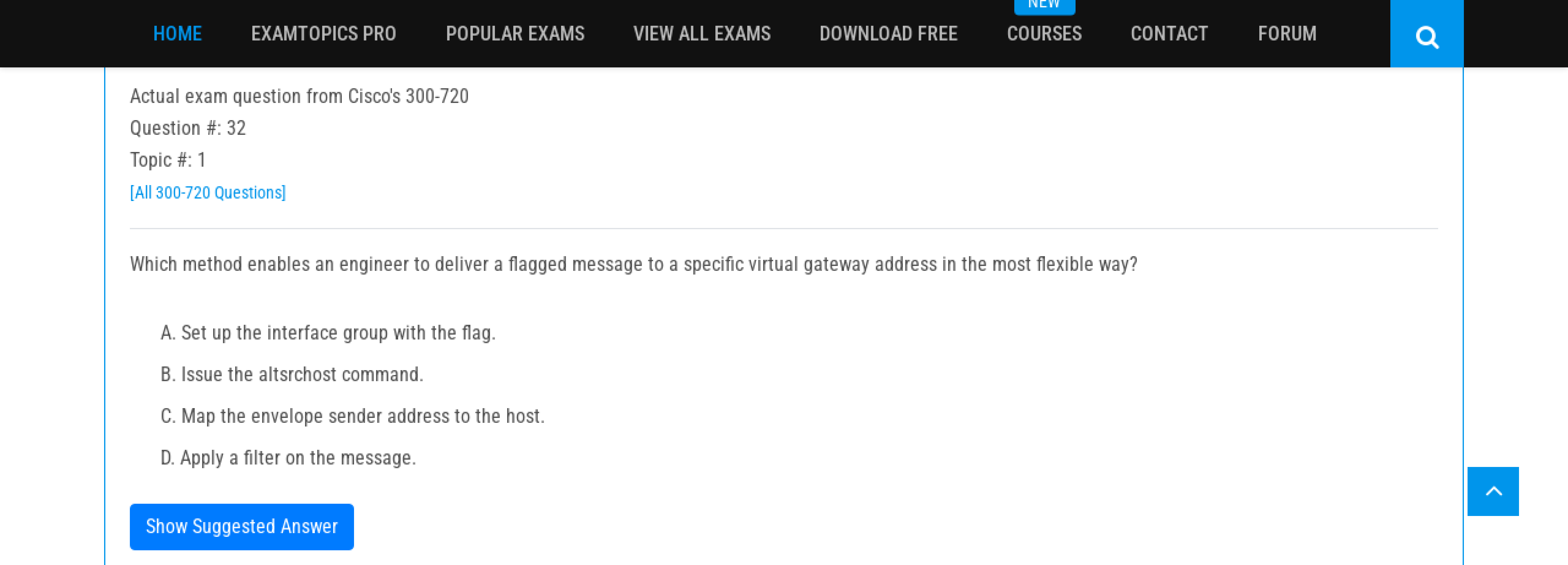
A. It strips the malicious content of the URI before unsubscribing.

B. It checks the URI reputation and category and allows the content filter to take an action on it.

C. It redirects the end user who clicks the unsubscribe button to a sandbox environment to allow a safe unsubscribe.

D. It checks the reputation of the URI and performs the unsubscribe process on behalf of the end user.

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 32

Topic #: 1

[All 300-720 Questions]

Which method enables an engineer to deliver a flagged message to a specific virtual gateway address in the most flexible way?

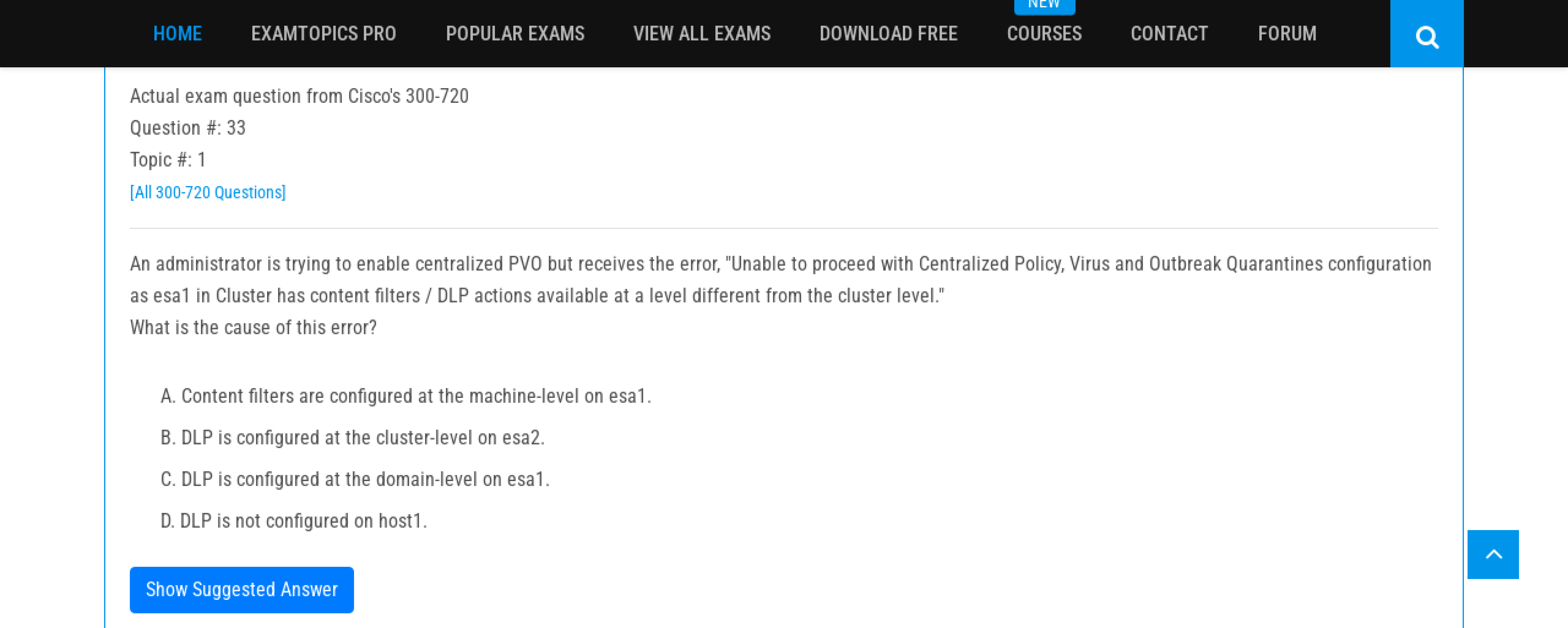
A. Set up the interface group with the flag.

B. Issue the altsrchost command.

C. Map the envelope sender address to the host.

D. Apply a filter on the message.

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 33

Topic #: 1

[All 300-720 Questions]

An administrator is trying to enable centralized PVO but receives the error, "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."

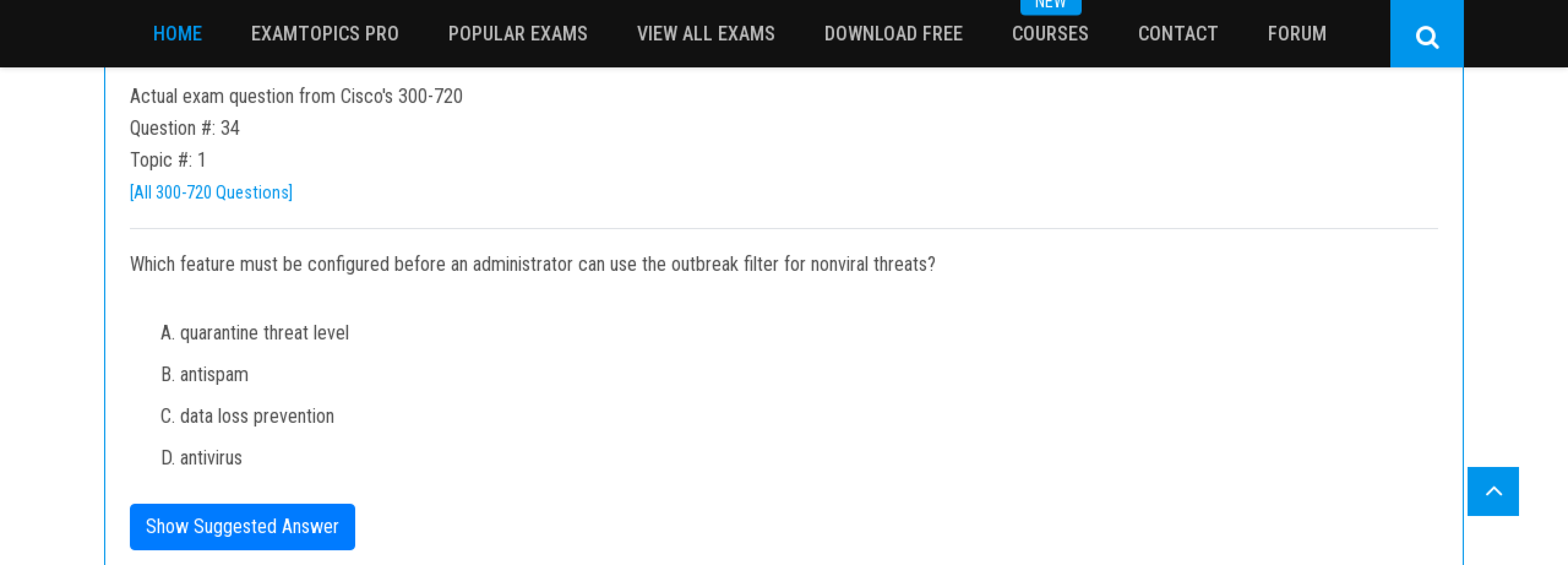
What is the cause of this error?

A. Content filters are configured at the machine-level on esa1.

B. DLP is configured at the cluster-level on esa2.

C. DLP is configured at the domain-level on esa1.

D. DLP is not configured on host1.



Actual exam question from Cisco's 300-720

Question #: 34

Topic #: 1

[All 300-720 Questions]

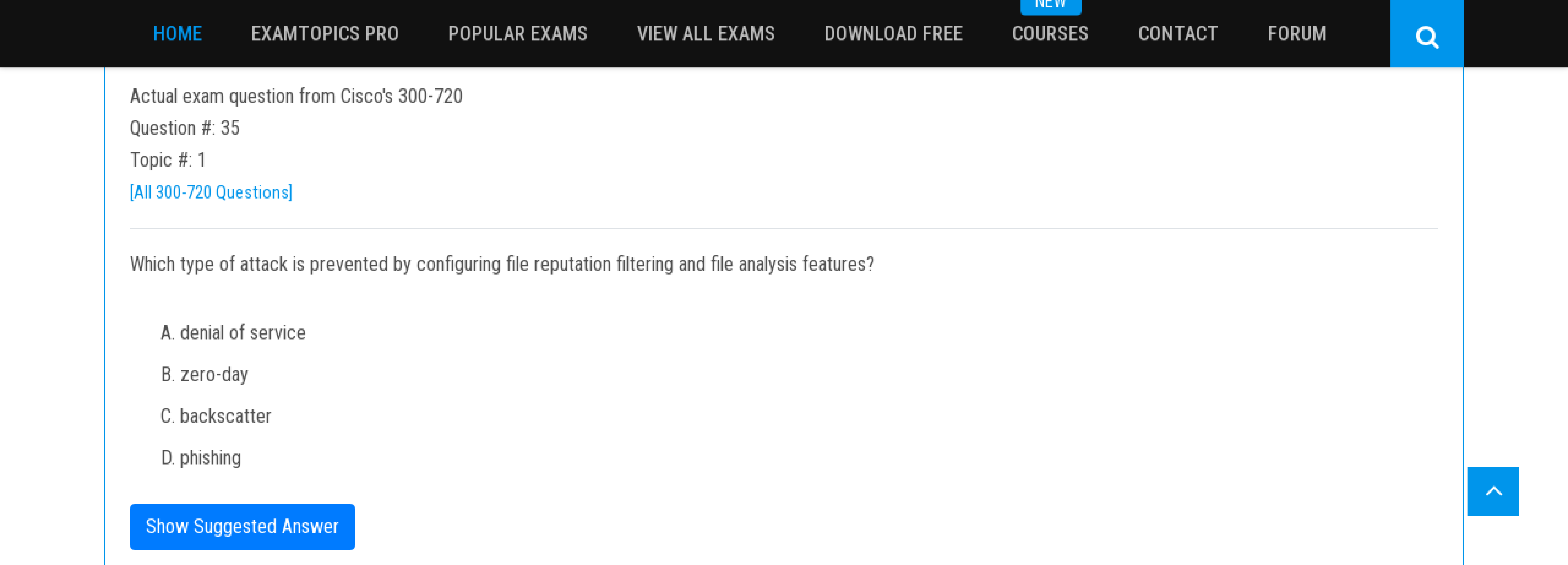
Which feature must be configured before an administrator can use the outbreak filter for nonviral threats?

A. quarantine threat level

B. antispam

C. data loss prevention

D. antivirus



Actual exam question from Cisco's 300-720

Question #: 35

Topic #: 1

[All 300-720 Questions]

Which type of attack is prevented by configuring file reputation filtering and file analysis features?

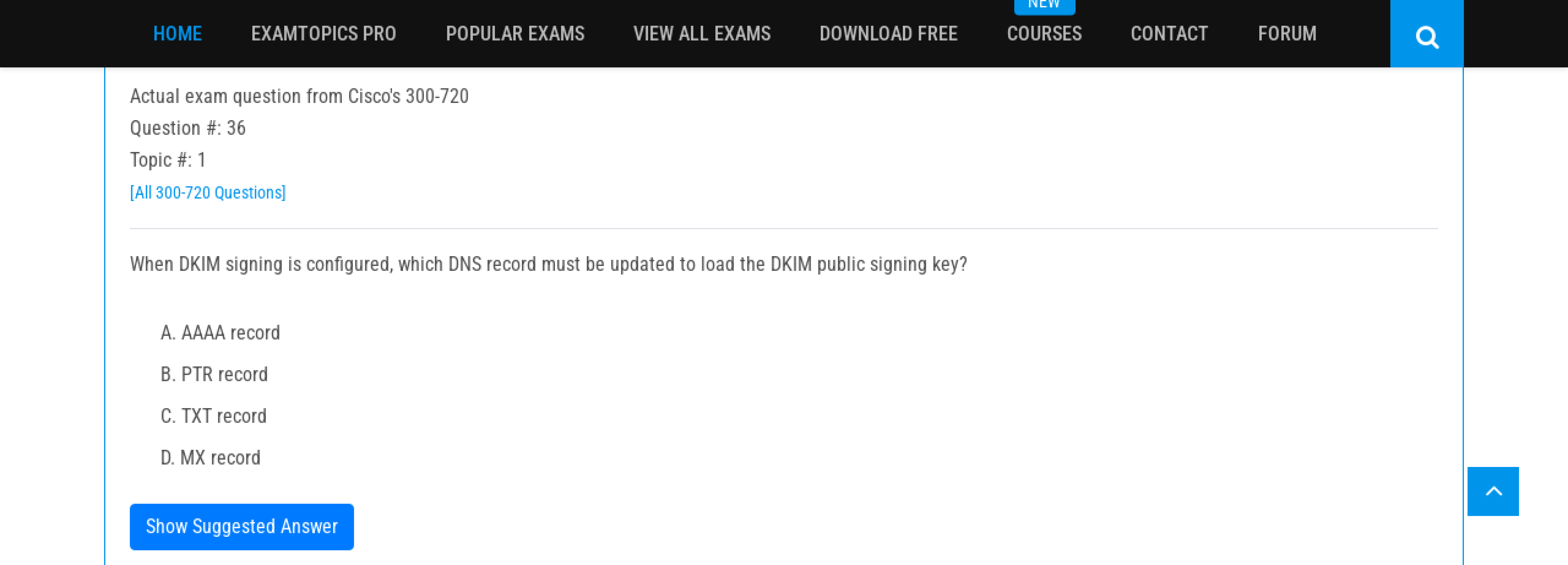
A. denial of service

B. zero-day

C. backscatter

D. phishing

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 36

Topic #: 1

[All 300-720 Questions]

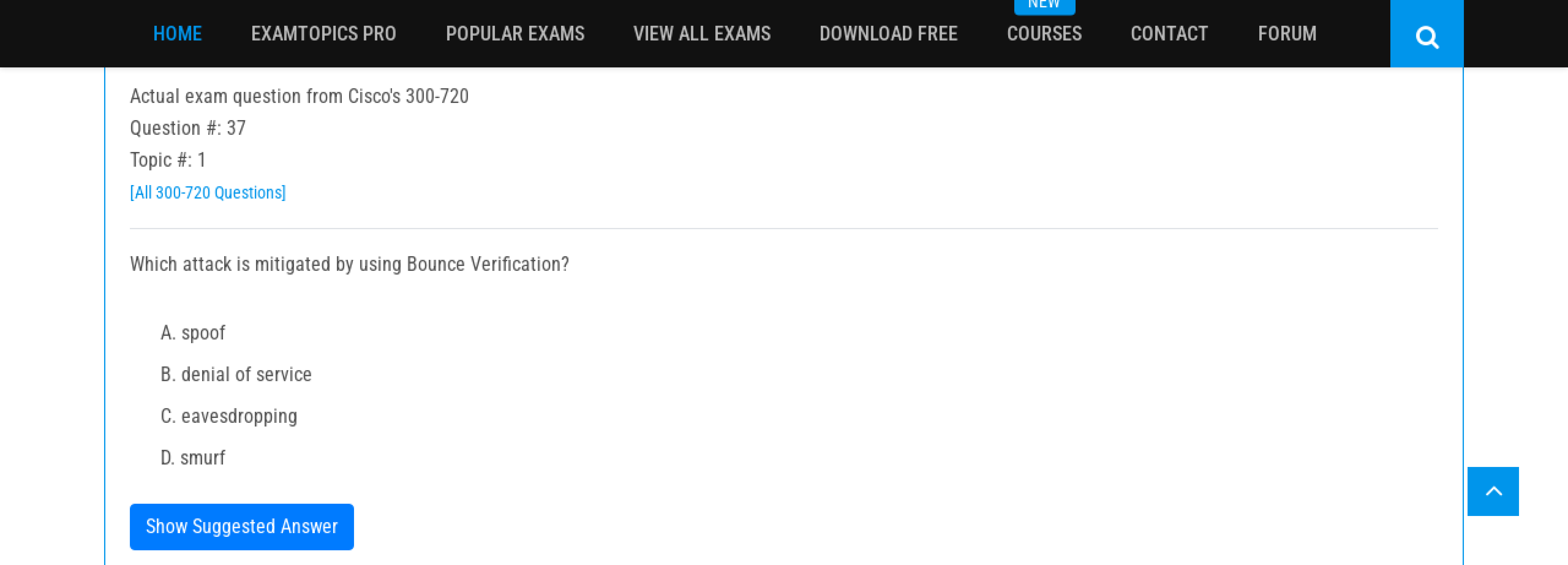
When DKIM signing is configured, which DNS record must be updated to load the DKIM public signing key?

A. AAAA record

B. PTR record

C. TXT record

D. MX record



Actual exam question from Cisco's 300-720

Question #: 37

Topic #: 1

[All 300-720 Questions]

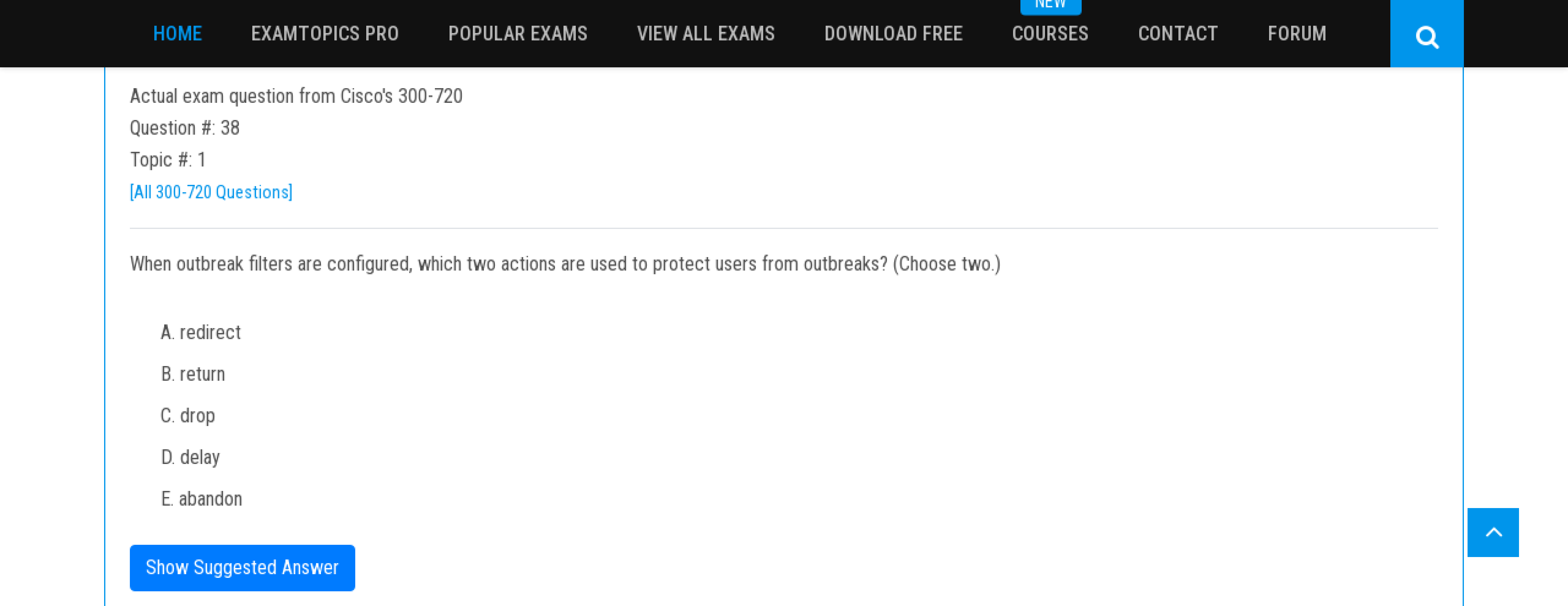
Which attack is mitigated by using Bounce Verification?

A. spoof

B. denial of service

C. eavesdropping

D. smurf



Actual exam question from Cisco's 300-720

Question #: 38

Topic #: 1

[All 300-720 Questions]

When outbreak filters are configured, which two actions are used to protect users from outbreaks? (Choose two.)

A. redirect

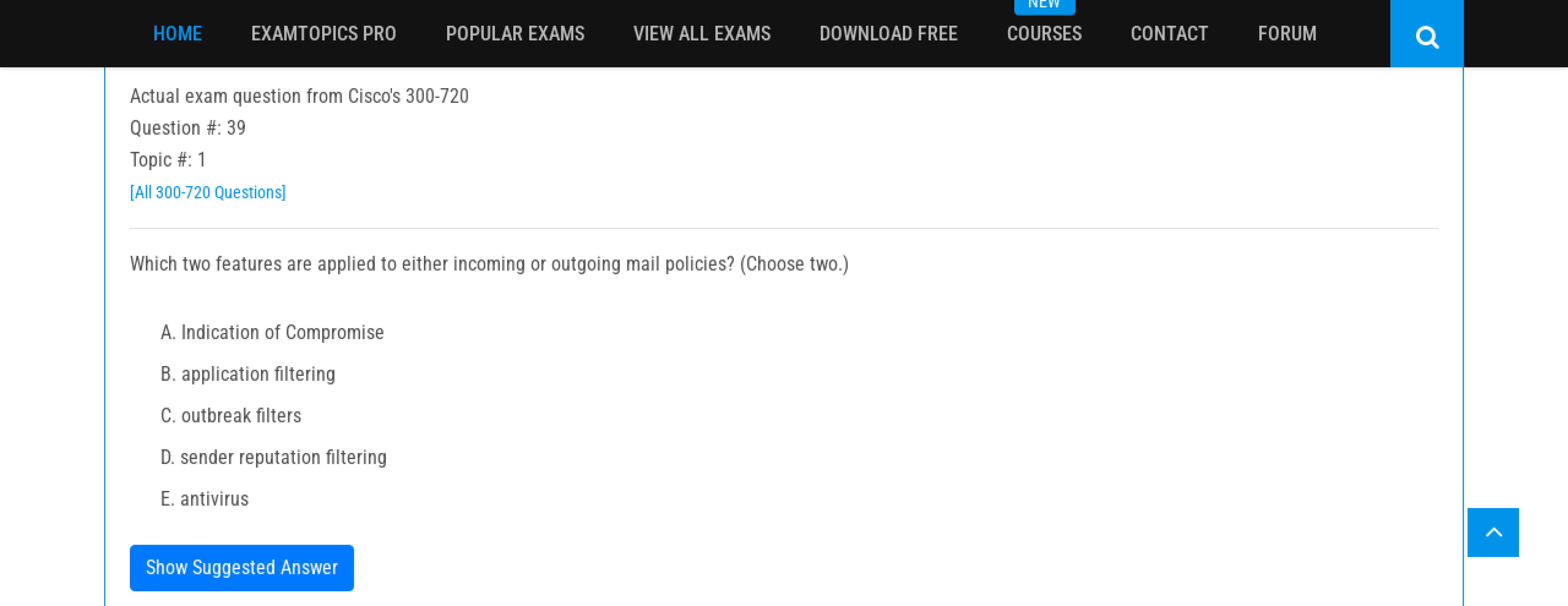
B. return

C. drop

D. delay

E. abandon

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 39

Topic #: 1

[All 300-720 Questions]

Which two features are applied to either incoming or outgoing mail policies? (Choose two.)

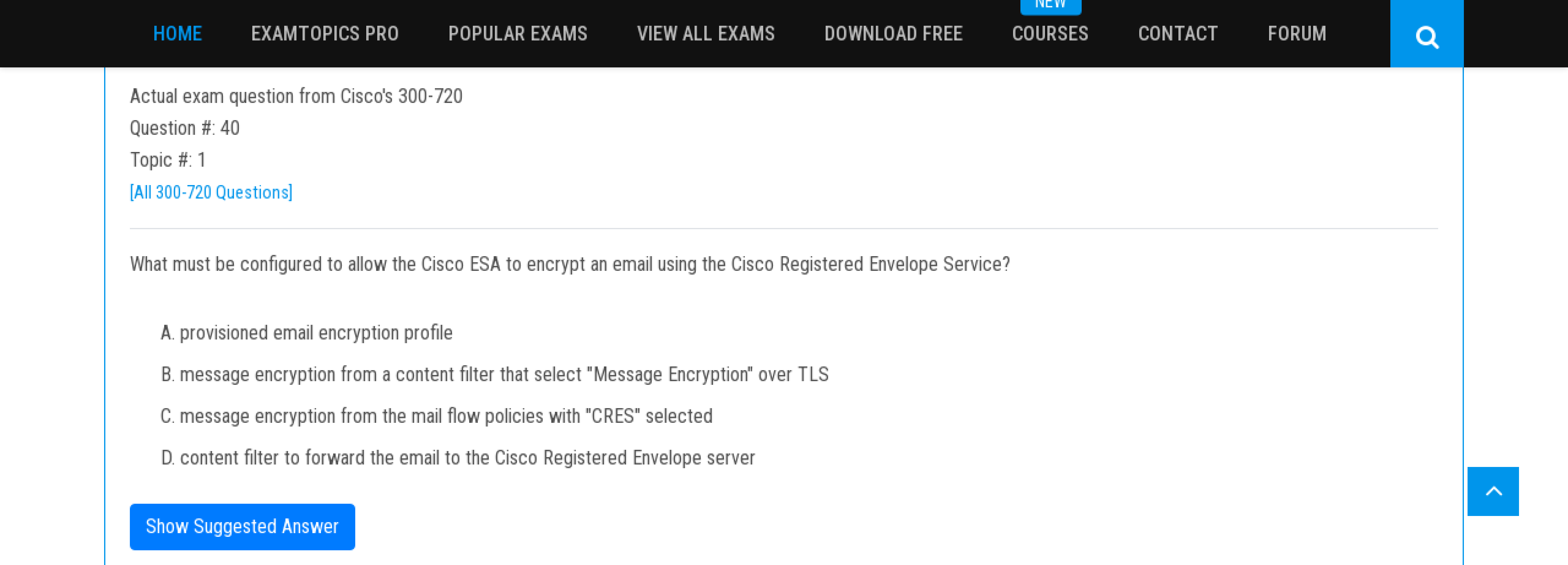
A. Indication of Compromise

B. application filtering

C. outbreak filters

D. sender reputation filtering

E. antivirus



Actual exam question from Cisco's 300-720

Question #: 40

Topic #: 1

[All 300-720 Questions]

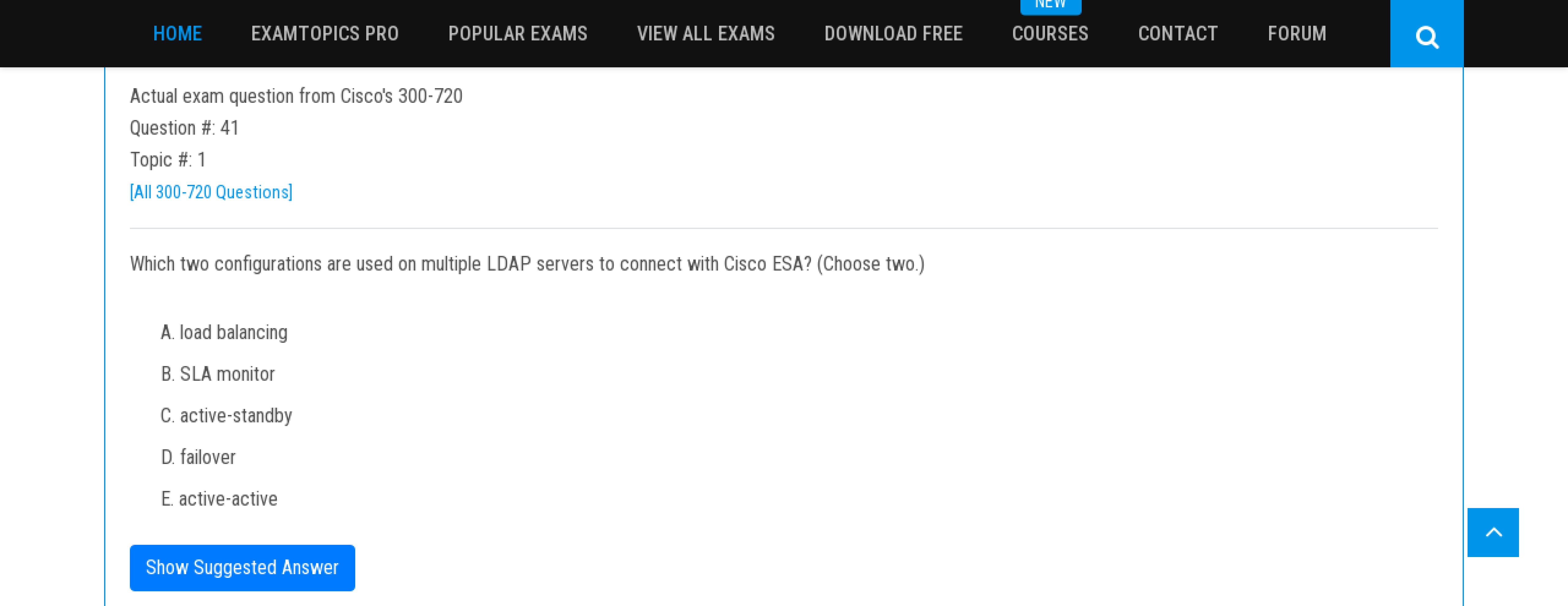
What must be configured to allow the Cisco ESA to encrypt an email using the Cisco Registered Envelope Service?

A. provisioned email encryption profile

B. message encryption from a content filter that select "Message Encryption" over TLS

C. message encryption from the mail flow policies with "CRES" selected

D. content filter to forward the email to the Cisco Registered Envelope server



Actual exam question from Cisco's 300-720

Question #: 41

Topic #: 1

[All 300-720 Questions]

Which two configurations are used on multiple LDAP servers to connect with Cisco ESA? (Choose two.)

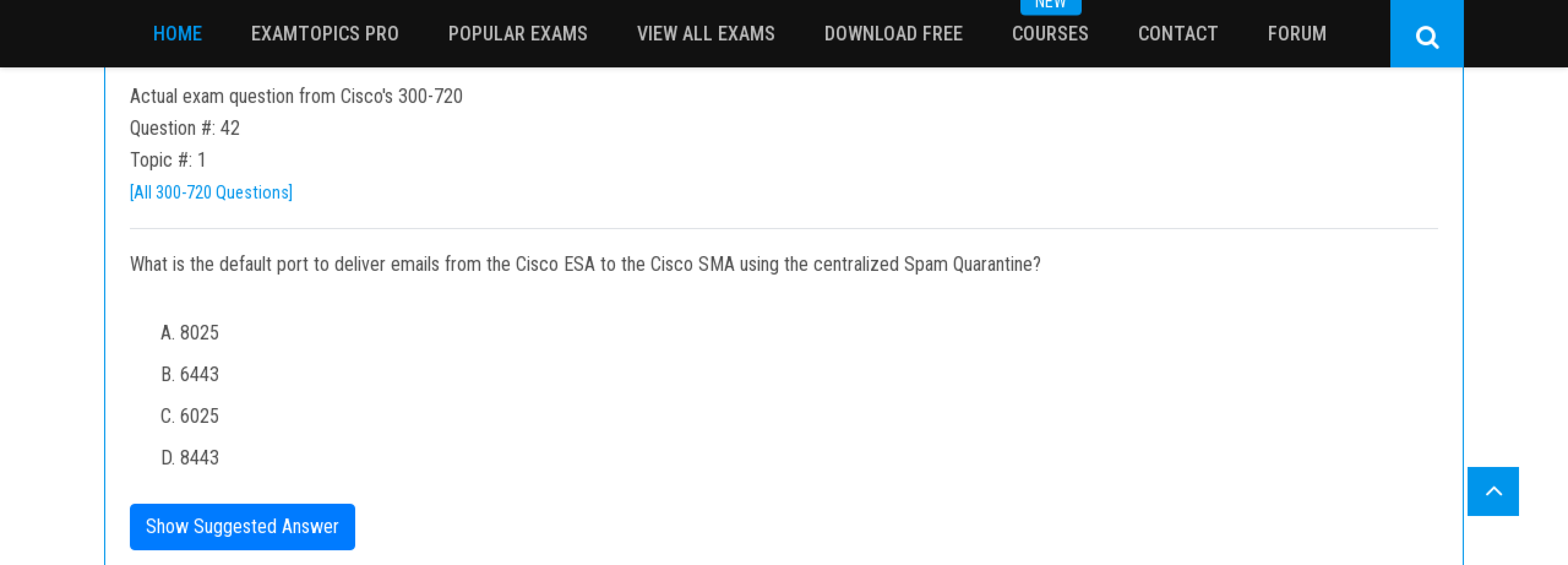
A. load balancing

B. SLA monitor

C. active-standby

D. failover

E. active-active



Actual exam question from Cisco's 300-720

Question #: 42

Topic #: 1

[All 300-720 Questions]

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

A. 8025

B. 6443

C. 6025

D. 8443

Actual exam question from Cisco's 300-720

Question #: 43

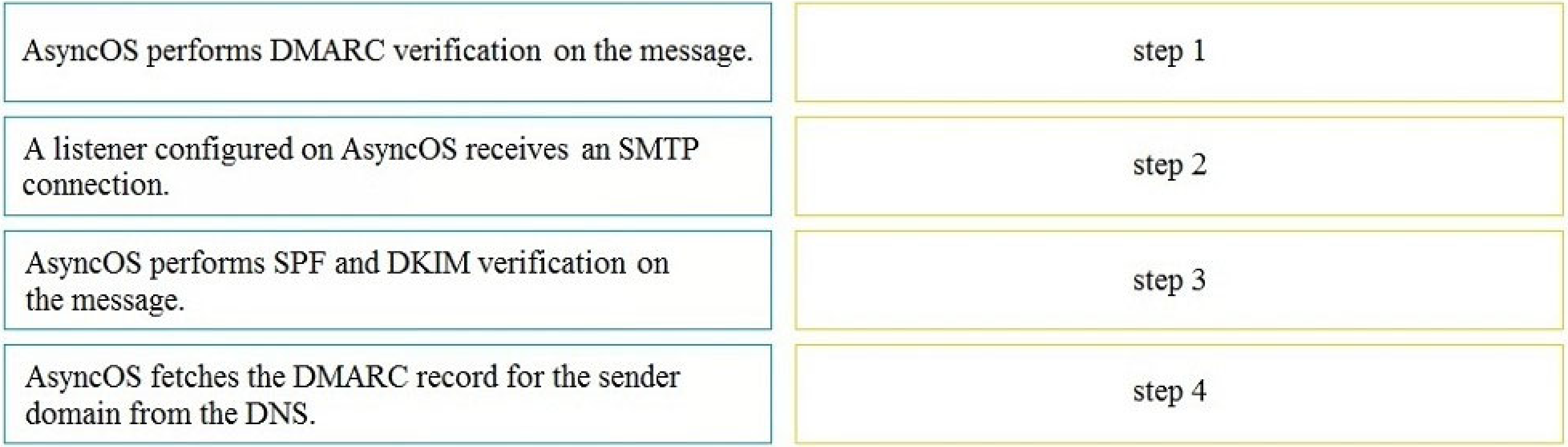
Topic #: 1

[All 300-720 Questions]

DRAG DROP -

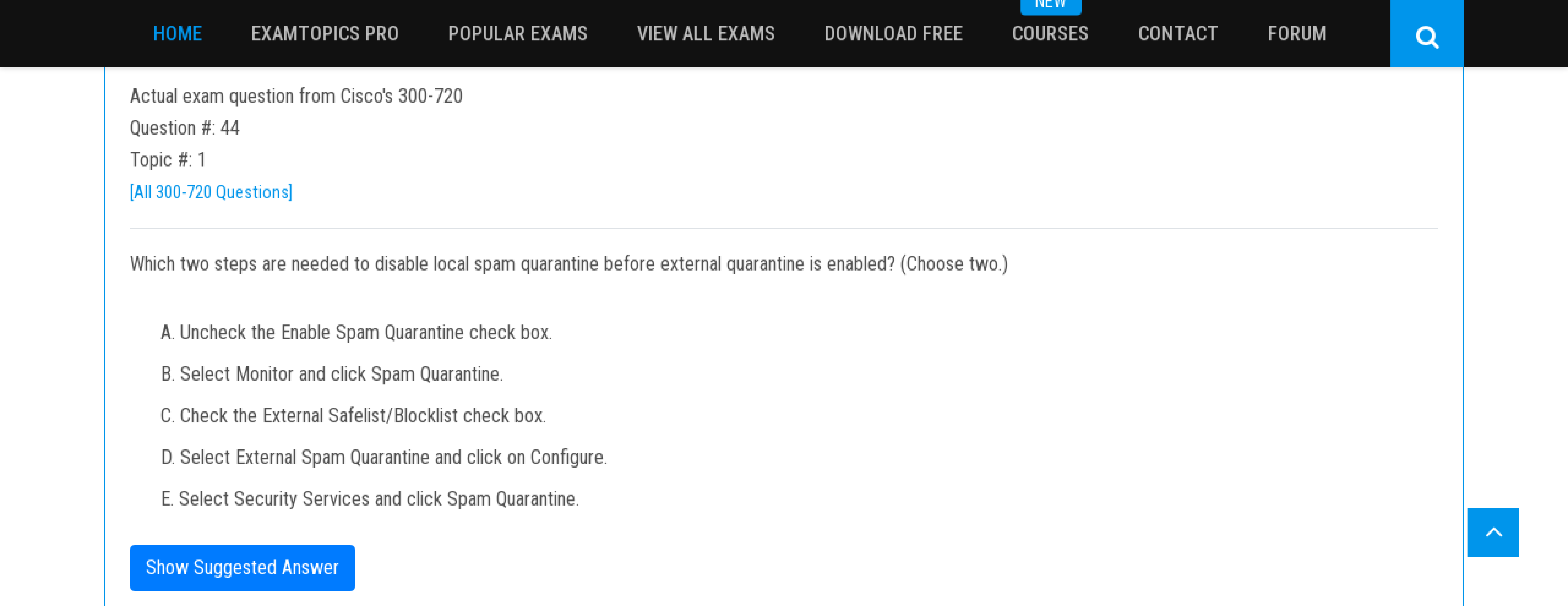
Drag and drop the AsyncOS methods for performing DMARC verification from the left into the correct order on the right.

Select and Place:



AsyncOS performs DMARC verification on the message.	step 1
A listener configured on AsyncOS receives an SMTP connection.	step 2
AsyncOS performs SPF and DKIM verification on the message.	step 3
AsyncOS fetches the DMARC record for the sender domain from the DNS.	step 4

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 44

Topic #: 1

[All 300-720 Questions]

Which two steps are needed to disable local spam quarantine before external quarantine is enabled? (Choose two.)

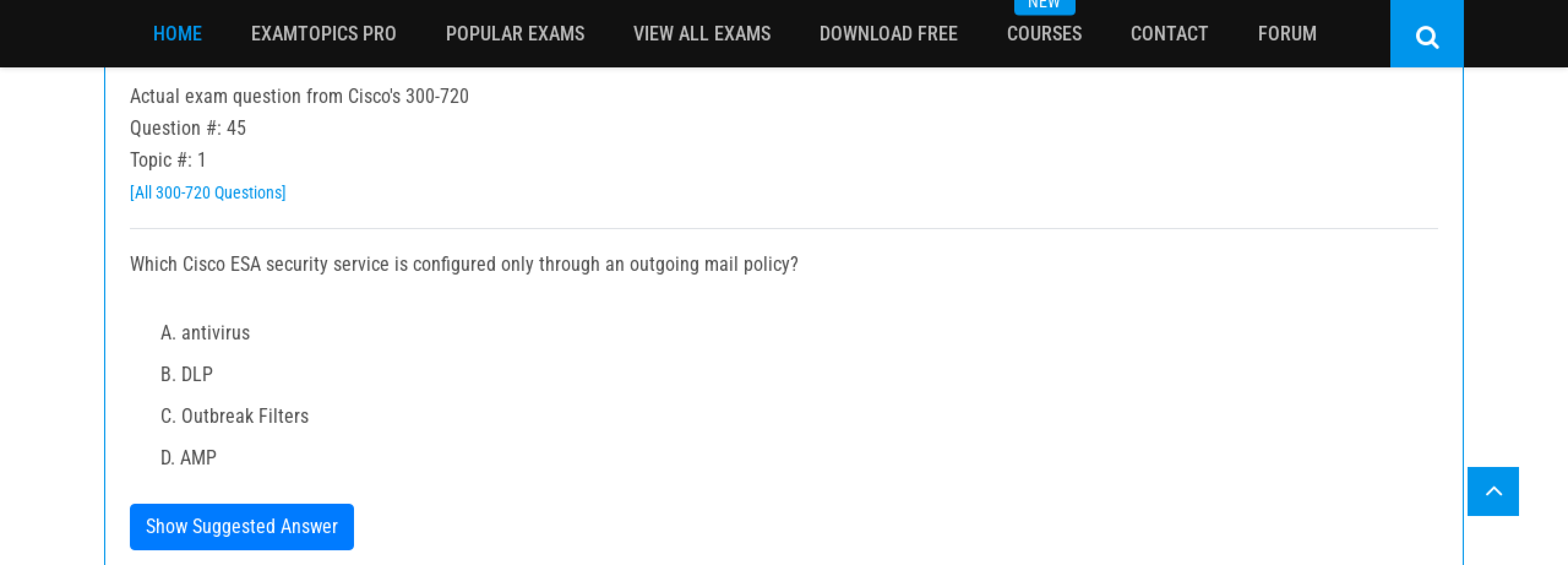
A. Uncheck the Enable Spam Quarantine check box.

B. Select Monitor and click Spam Quarantine.

C. Check the External Safelist/Blocklist check box.

D. Select External Spam Quarantine and click on Configure.

E. Select Security Services and click Spam Quarantine.



Actual exam question from Cisco's 300-720

Question #: 45

Topic #: 1

[All 300-720 Questions]

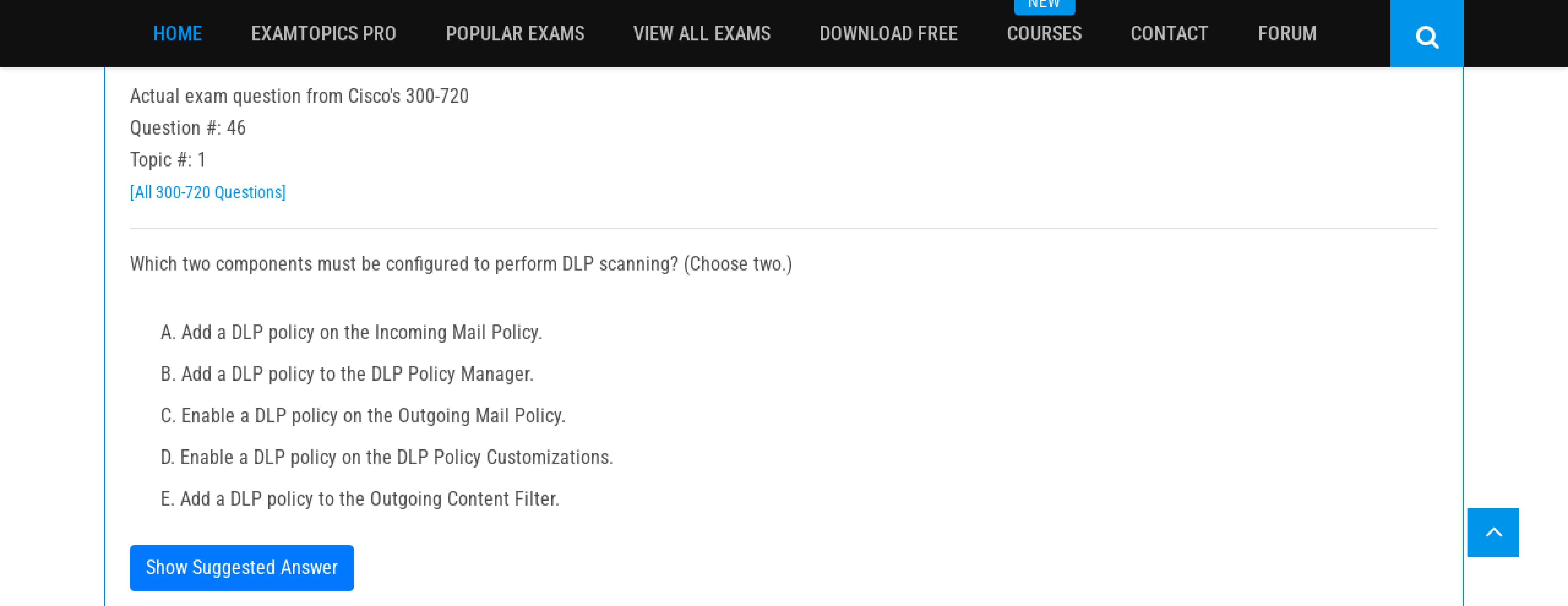
Which Cisco ESA security service is configured only through an outgoing mail policy?

A. antivirus

B. DLP

C. Outbreak Filters

D. AMP



Actual exam question from Cisco's 300-720

Question #: 46

Topic #: 1

[All 300-720 Questions]

Which two components must be configured to perform DLP scanning? (Choose two.)

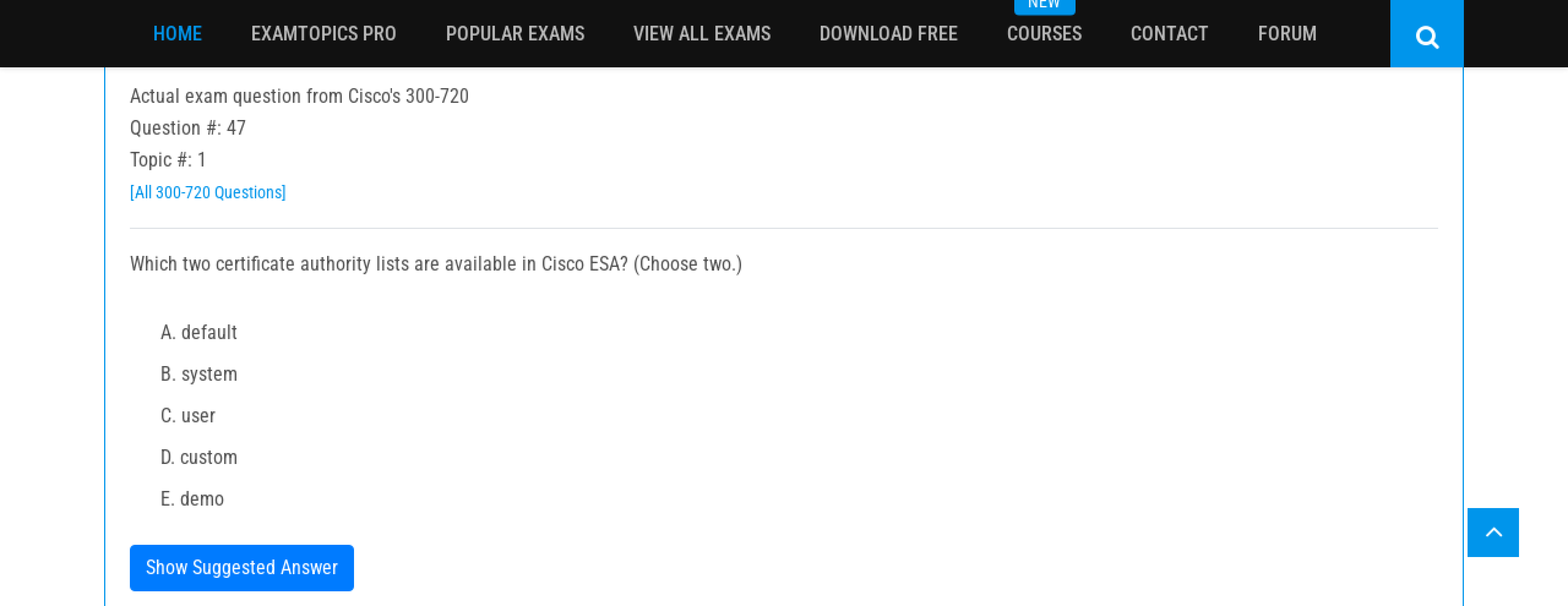
A. Add a DLP policy on the Incoming Mail Policy.

B. Add a DLP policy to the DLP Policy Manager.

C. Enable a DLP policy on the Outgoing Mail Policy.

D. Enable a DLP policy on the DLP Policy Customizations.

E. Add a DLP policy to the Outgoing Content Filter.



Actual exam question from Cisco's 300-720

Question #: 47

Topic #: 1

[All 300-720 Questions]

Which two certificate authority lists are available in Cisco ESA? (Choose two.)

A. default

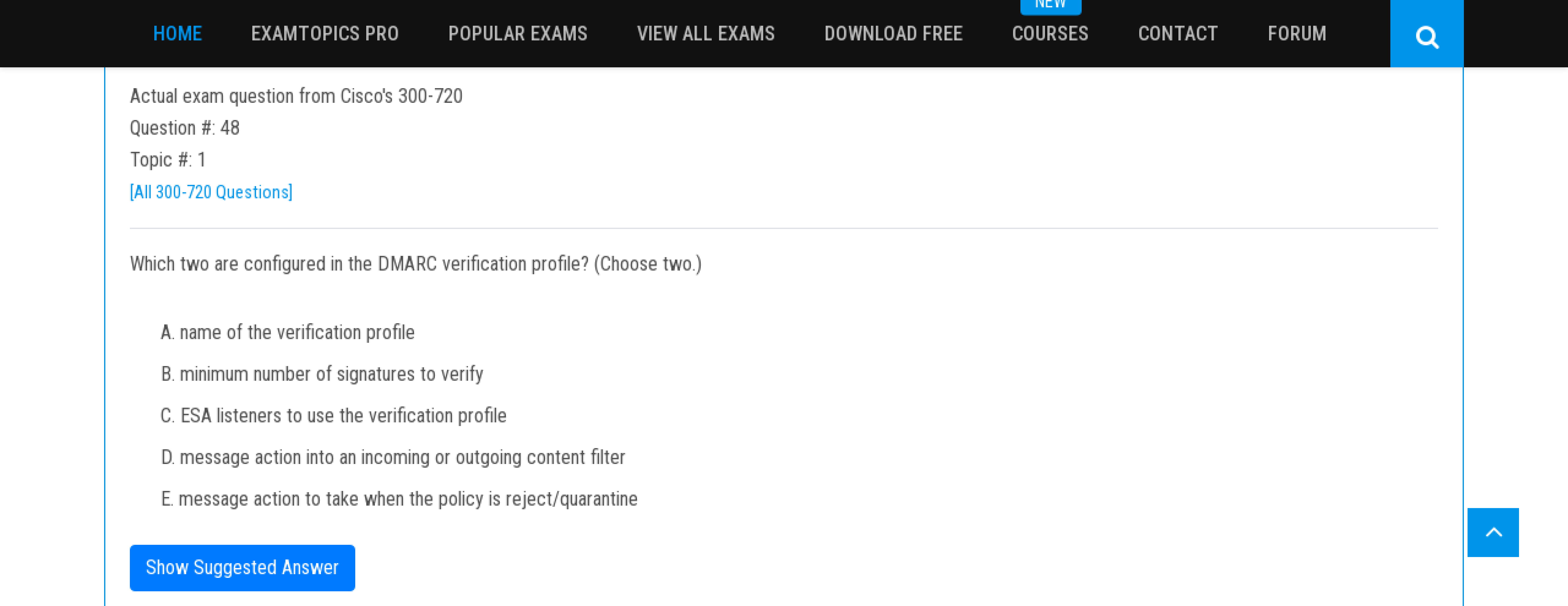
B. system

C. user

D. custom

E. demo

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 48

Topic #: 1

[All 300-720 Questions]

Which two are configured in the DMARC verification profile? (Choose two.)

A. name of the verification profile

B. minimum number of signatures to verify

C. ESA listeners to use the verification profile

D. message action into an incoming or outgoing content filter

E. message action to take when the policy is reject/quarantine

Show Suggested Answer

Actual exam question from Cisco's 300-720

Question #: 49

Topic #: 1

[All 300-720 Questions]

Which two components form the graymail management solution in Cisco ESA? (Choose two.)

A. cloud-based unsubscribe service

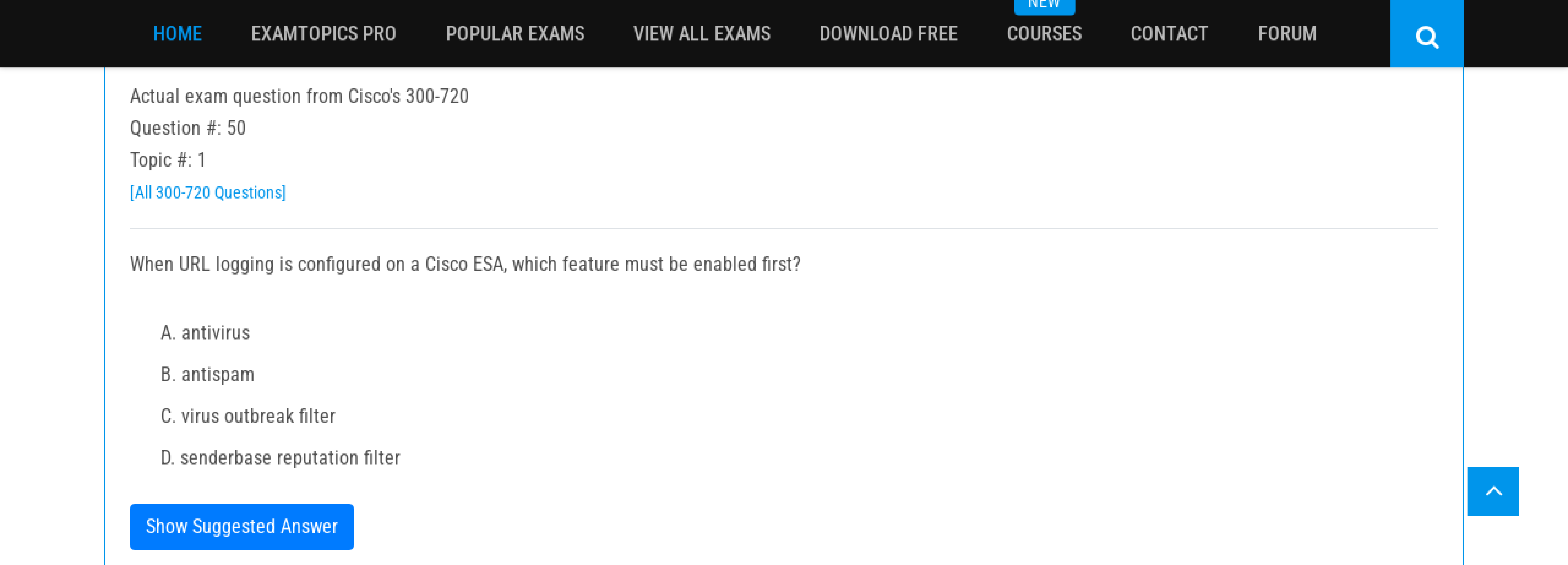
B. uniform unsubscription management interface for end users

C. secure subscribe option for end users

D. integrated graymail scanning engine

E. improved mail efficacy

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 50

Topic #: 1

[All 300-720 Questions]

When URL logging is configured on a Cisco ESA, which feature must be enabled first?

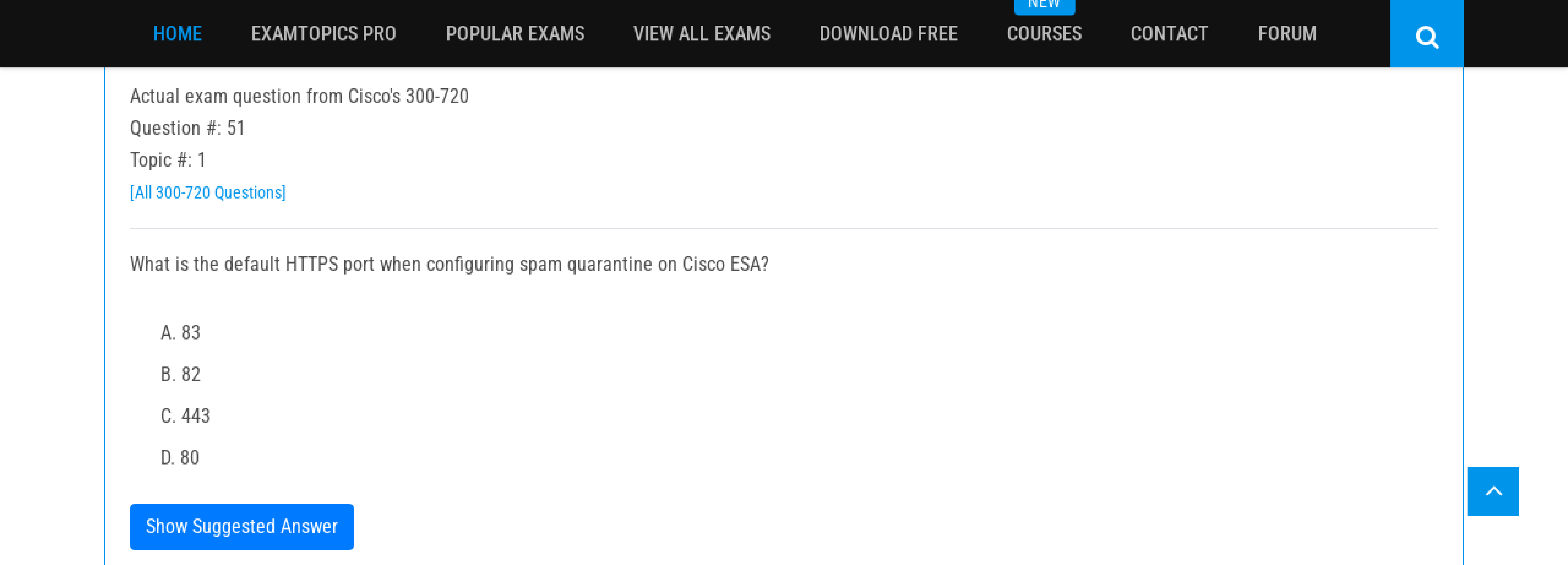
A. antivirus

B. antispam

C. virus outbreak filter

D. senderbase reputation filter

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 51

Topic #: 1

[All 300-720 Questions]

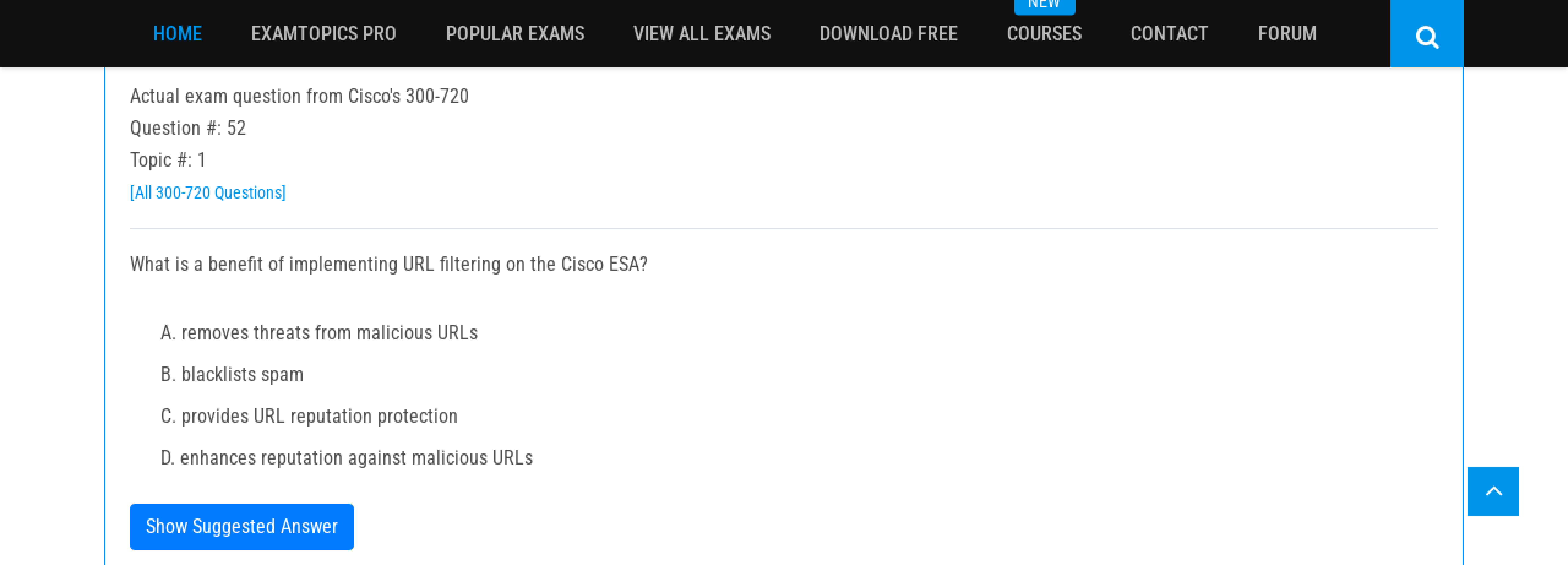
What is the default HTTPS port when configuring spam quarantine on Cisco ESA?

A. 83

B. 82

C. 443

D. 80



Actual exam question from Cisco's 300-720

Question #: 52

Topic #: 1

[All 300-720 Questions]

What is a benefit of implementing URL filtering on the Cisco ESA?

A. removes threats from malicious URLs

B. blacklists spam

C. provides URL reputation protection

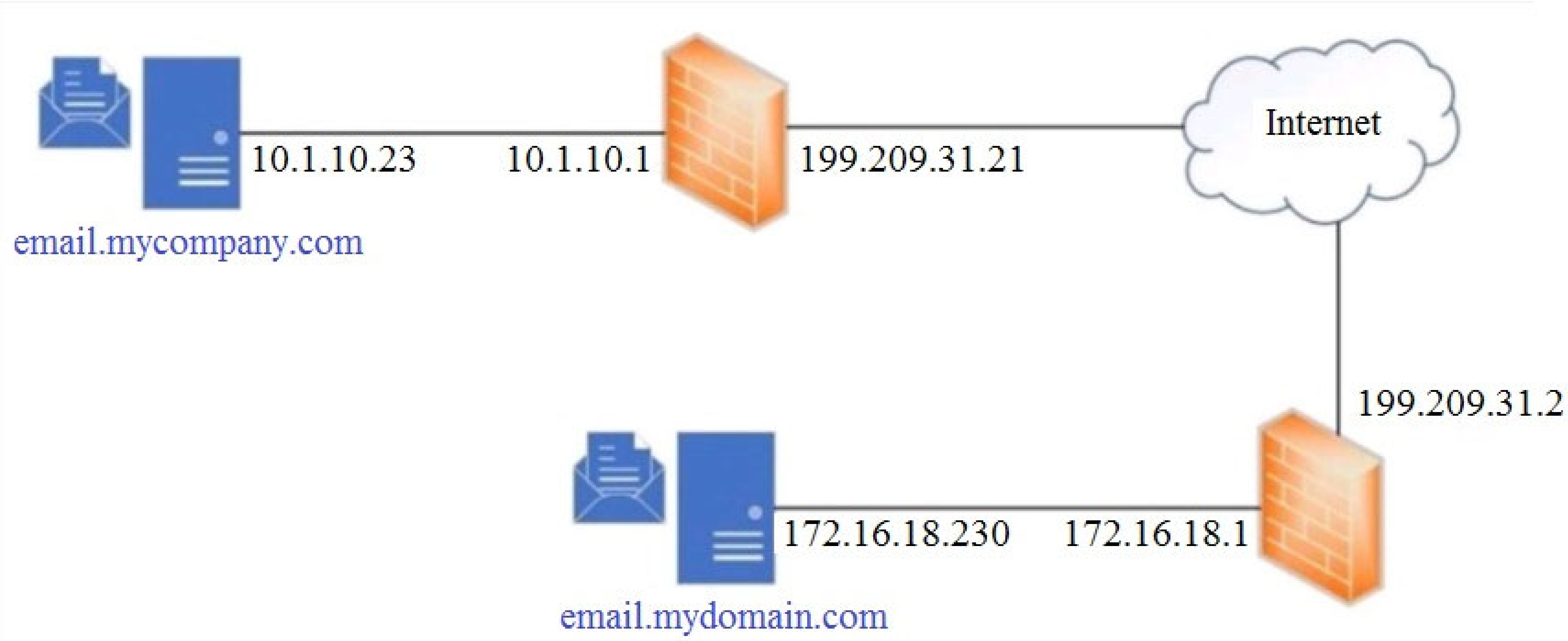
D. enhances reputation against malicious URLs

Actual exam question from Cisco's 300-720

Question #: 53

Topic #: 1

[All 300-720 Questions]



Refer to the exhibit. Which SPF record is valid for mycompany.com?

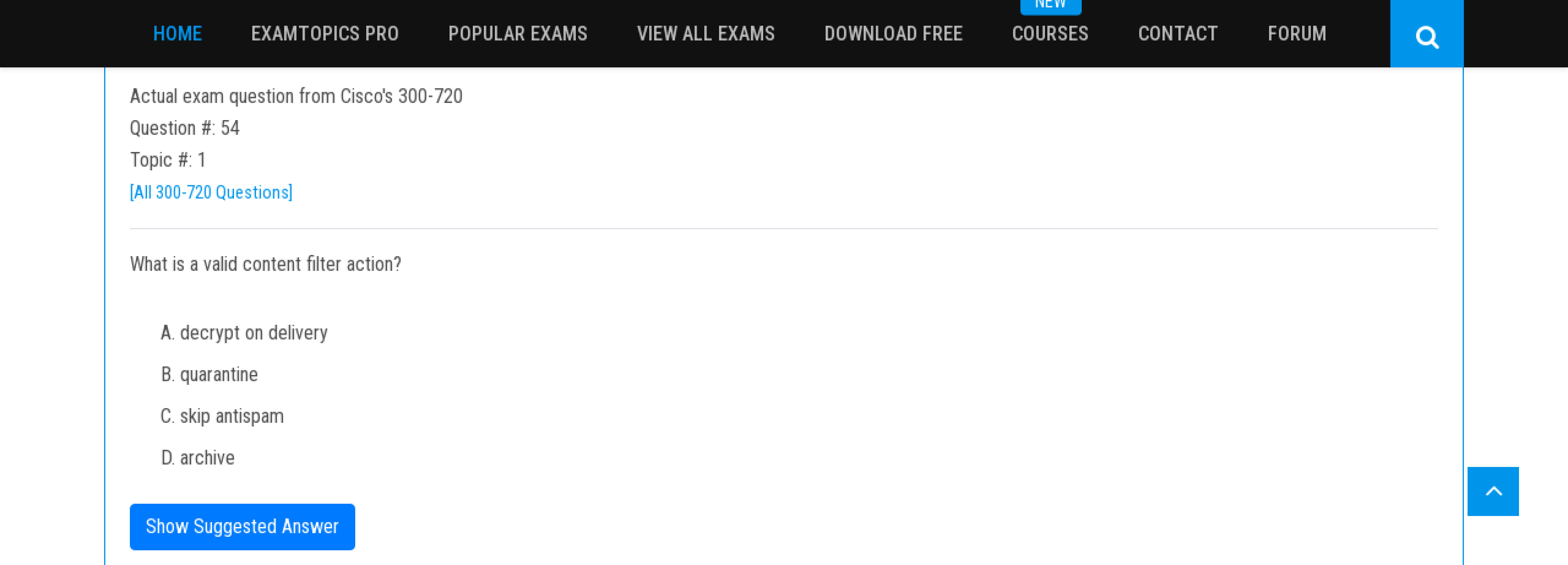
A. v=spf1 a mx ip4:199.209.31.2 -all

B. v=spf1 a mx ip4:10.1.10.23 -all

C. v=spf1 a mx ip4:199.209.31.21 -all

D. v=spf1 a mx ip4:172.16.18.230 -all

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 54

Topic #: 1

[All 300-720 Questions]

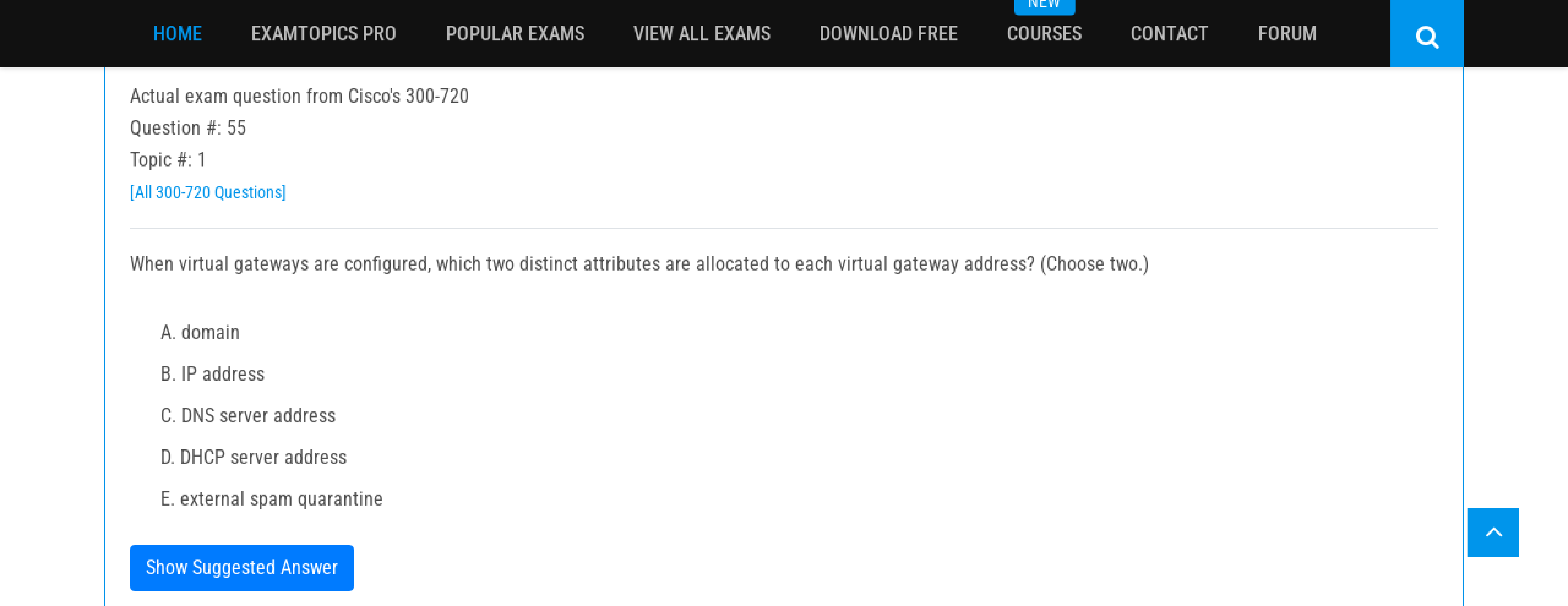
What is a valid content filter action?

A. decrypt on delivery

B. quarantine

C. skip antispam

D. archive



Actual exam question from Cisco's 300-720

Question #: 55

Topic #: 1

[All 300-720 Questions]

When virtual gateways are configured, which two distinct attributes are allocated to each virtual gateway address? (Choose two.)

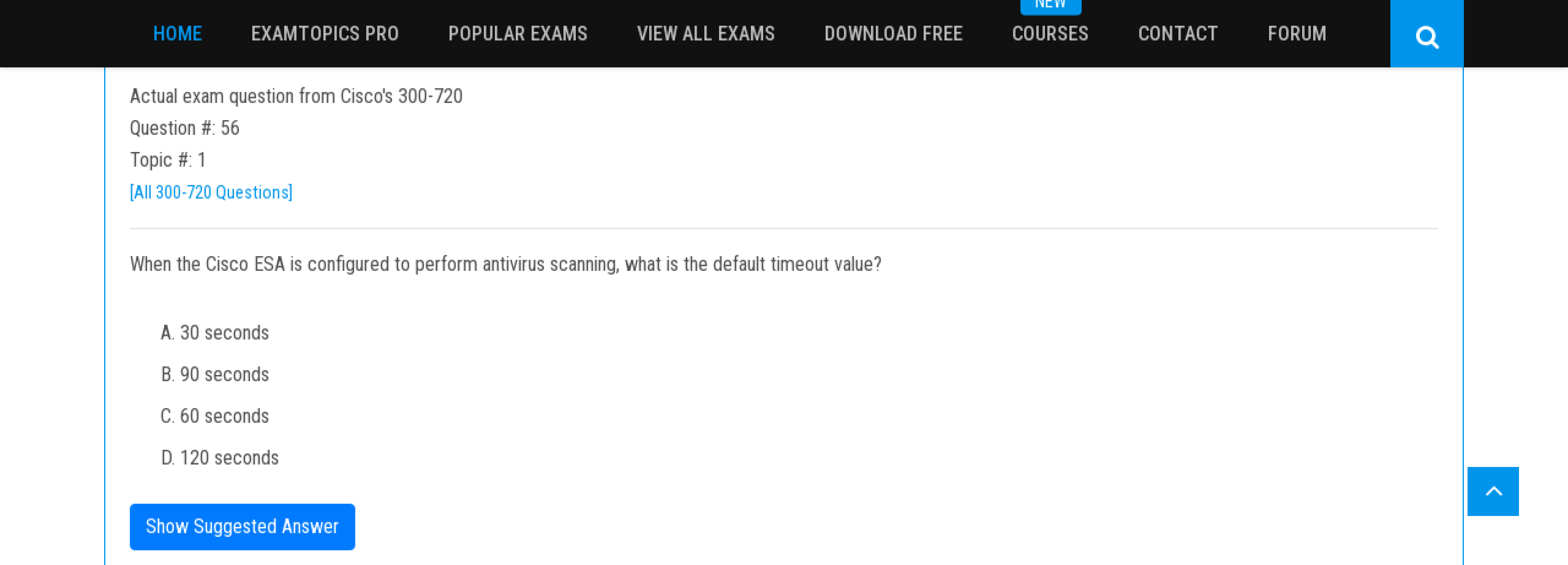
A. domain

B. IP address

C. DNS server address

D. DHCP server address

E. external spam quarantine



Actual exam question from Cisco's 300-720

Question #: 56

Topic #: 1

[All 300-720 Questions]

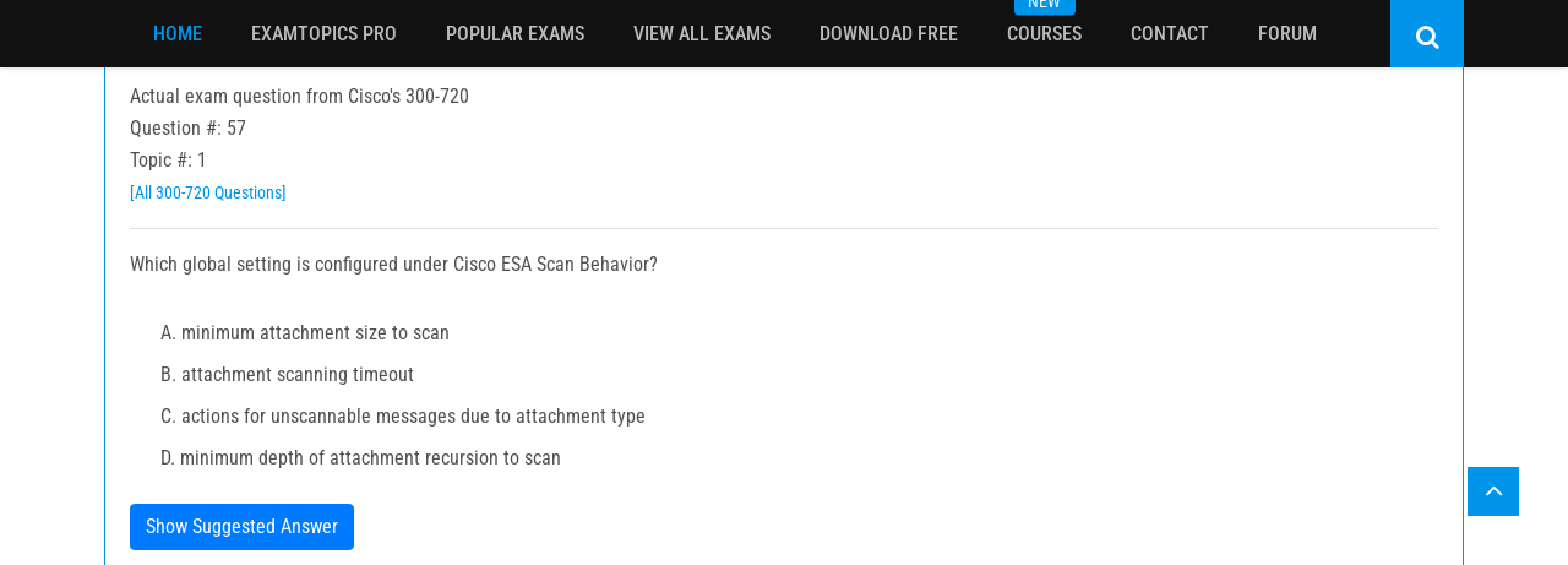
When the Cisco ESA is configured to perform antivirus scanning, what is the default timeout value?

A. 30 seconds

B. 90 seconds

C. 60 seconds

D. 120 seconds



Actual exam question from Cisco's 300-720

Question #: 57

Topic #: 1

[All 300-720 Questions]

Which global setting is configured under Cisco ESA Scan Behavior?

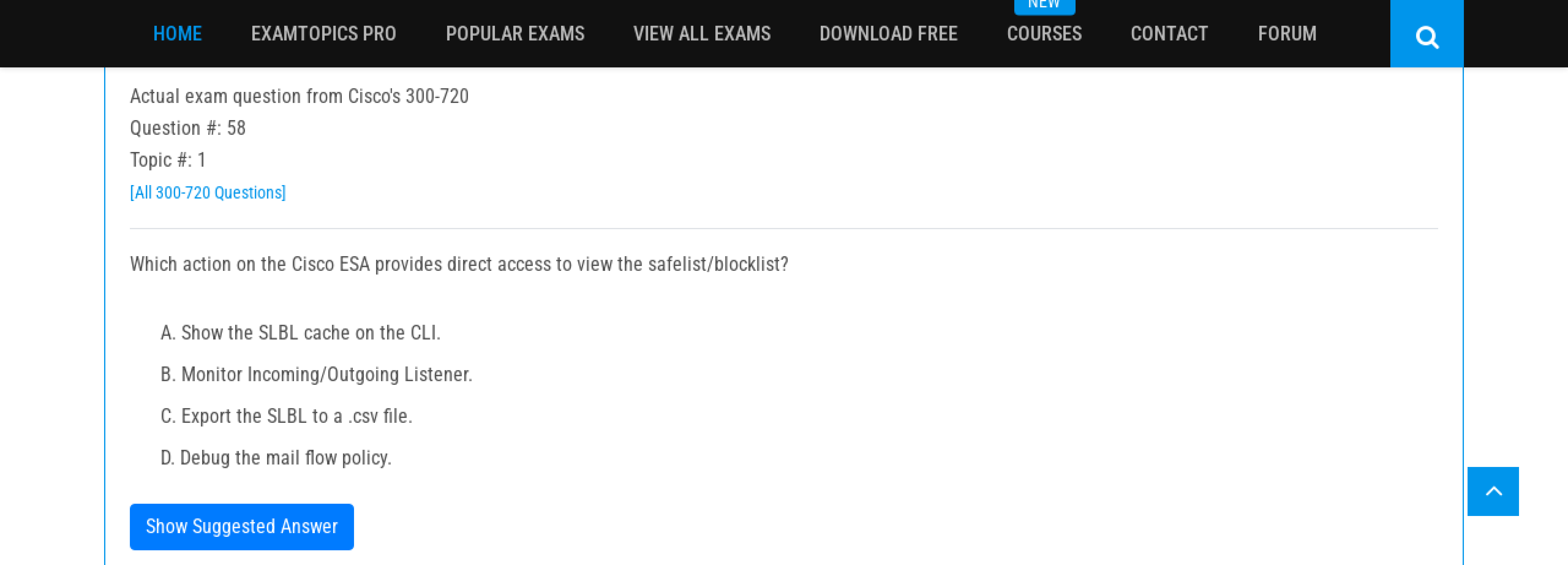
A. minimum attachment size to scan

B. attachment scanning timeout

C. actions for unscannable messages due to attachment type

D. minimum depth of attachment recursion to scan

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 58

Topic #: 1

[All 300-720 Questions]

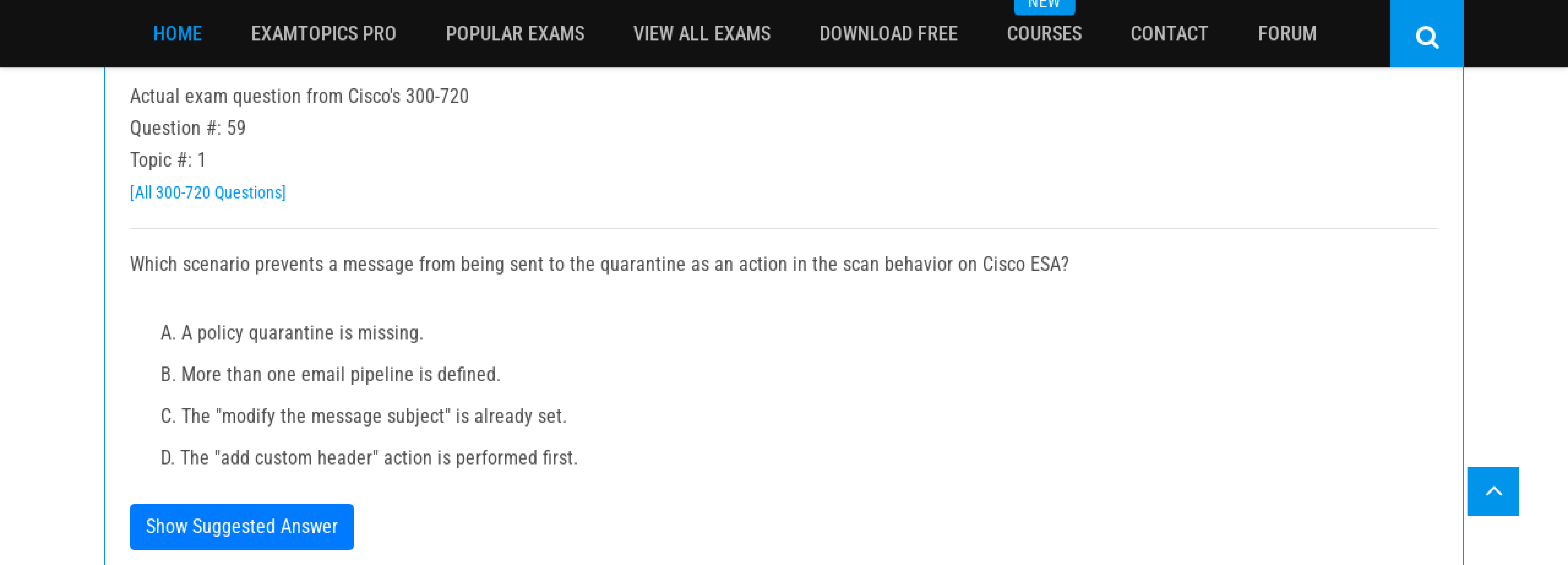
Which action on the Cisco ESA provides direct access to view the safelist/blocklist?

A. Show the SLBL cache on the CLI.

B. Monitor Incoming/Outgoing Listener.

C. Export the SLBL to a .csv file.

D. Debug the mail flow policy.



Actual exam question from Cisco's 300-720

Question #: 59

Topic #: 1

[All 300-720 Questions]

Which scenario prevents a message from being sent to the quarantine as an action in the scan behavior on Cisco ESA?

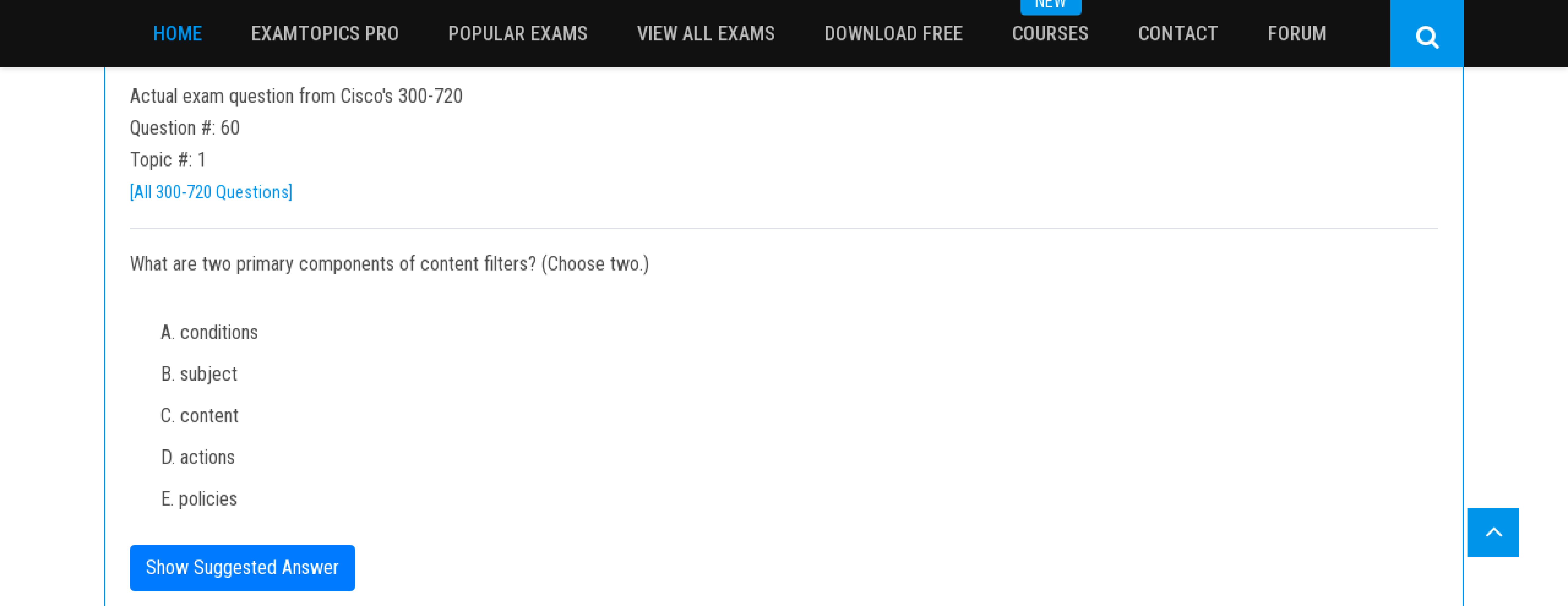
A. A policy quarantine is missing.

B. More than one email pipeline is defined.

C. The "modify the message subject" is already set.

D. The "add custom header" action is performed first.

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 60

Topic #: 1

[All 300-720 Questions]

What are two primary components of content filters? (Choose two.)

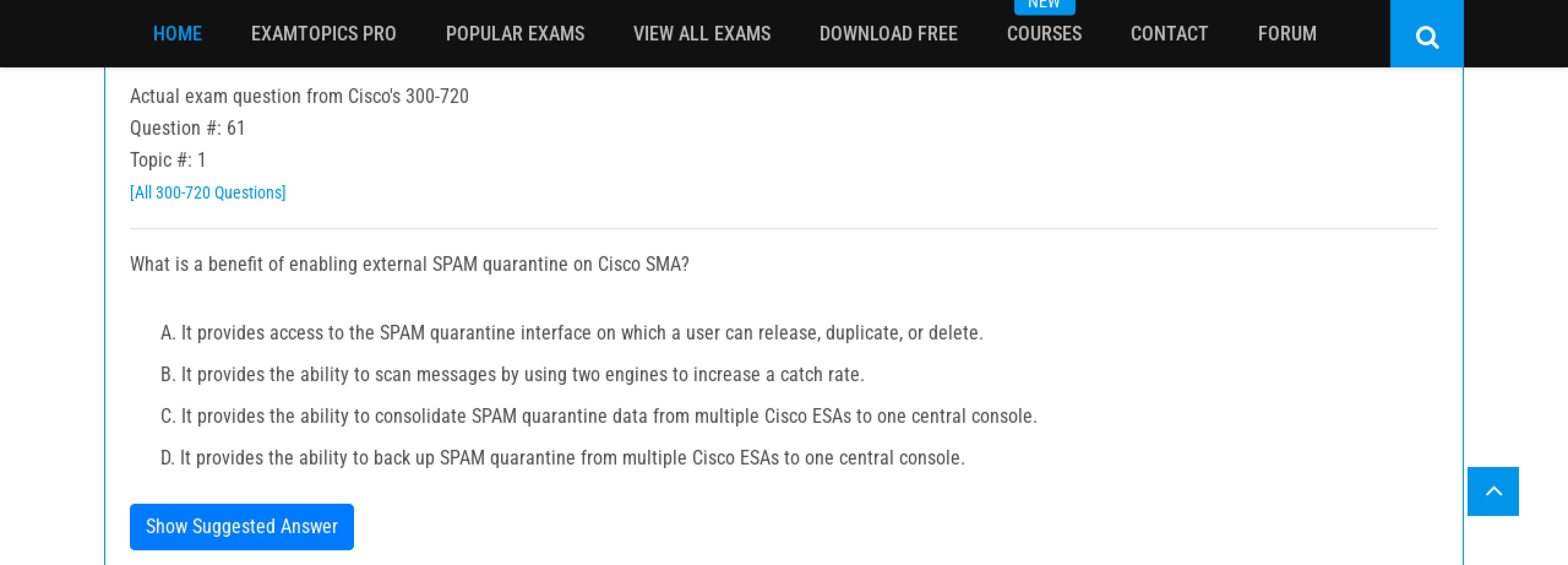
A. conditions

B. subject

C. content

D. actions

E. policies



Actual exam question from Cisco's 300-720

Question #: 61

Topic #: 1

[All 300-720 Questions]

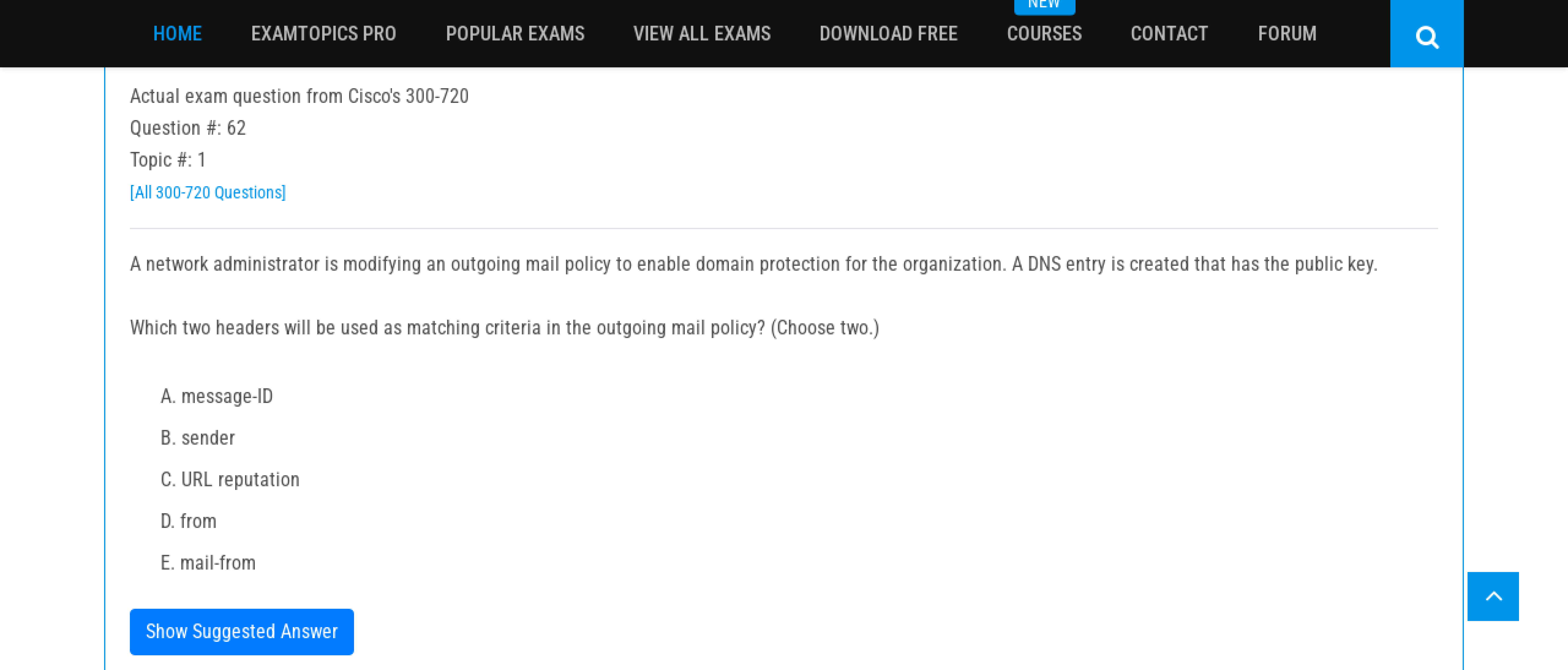
What is a benefit of enabling external SPAM quarantine on Cisco SMA?

A. It provides access to the SPAM quarantine interface on which a user can release, duplicate, or delete.

B. It provides the ability to scan messages by using two engines to increase a catch rate.

C. It provides the ability to consolidate SPAM quarantine data from multiple Cisco ESAs to one central console.

D. It provides the ability to back up SPAM quarantine from multiple Cisco ESAs to one central console.



Actual exam question from Cisco's 300-720

Question #: 62

Topic #: 1

[All 300-720 Questions]

A network administrator is modifying an outgoing mail policy to enable domain protection for the organization. A DNS entry is created that has the public key.

Which two headers will be used as matching criteria in the outgoing mail policy? (Choose two.)

A. message-ID

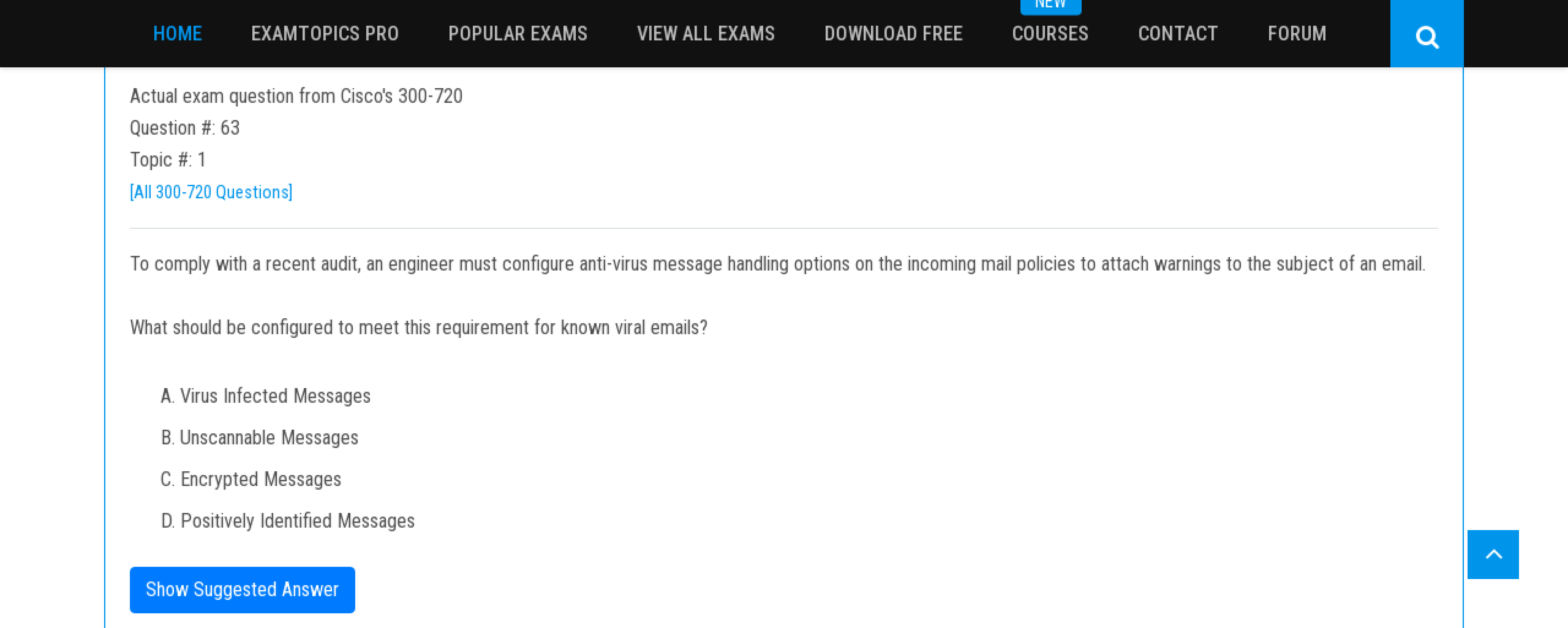
B. sender

C. URL reputation

D. from

E. mail-from

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 63

Topic #: 1

[All 300-720 Questions]

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.

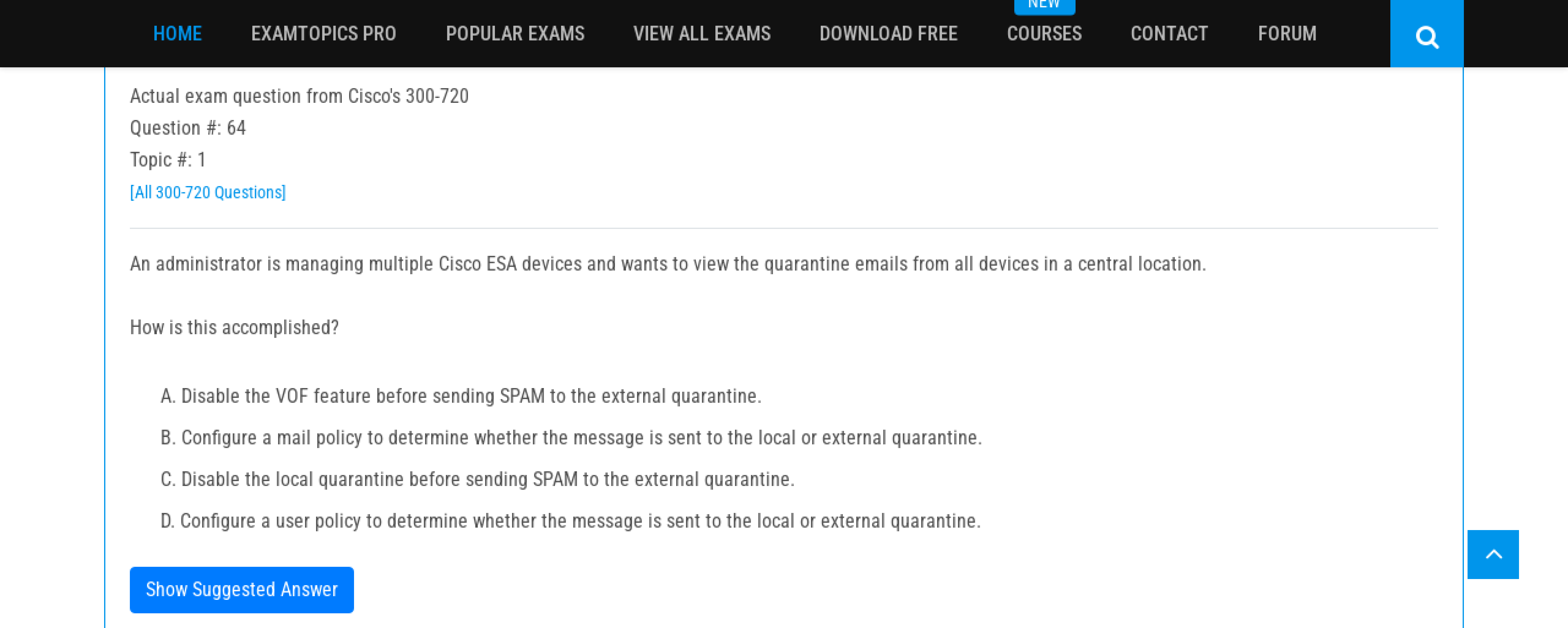
What should be configured to meet this requirement for known viral emails?

A. Virus Infected Messages

B. Unscannable Messages

C. Encrypted Messages

D. Positively Identified Messages



Actual exam question from Cisco's 300-720
Question #: 64
Topic #: 1
[All 300-720 Questions]

An administrator is managing multiple Cisco ESA devices and wants to view the quarantine emails from all devices in a central location.

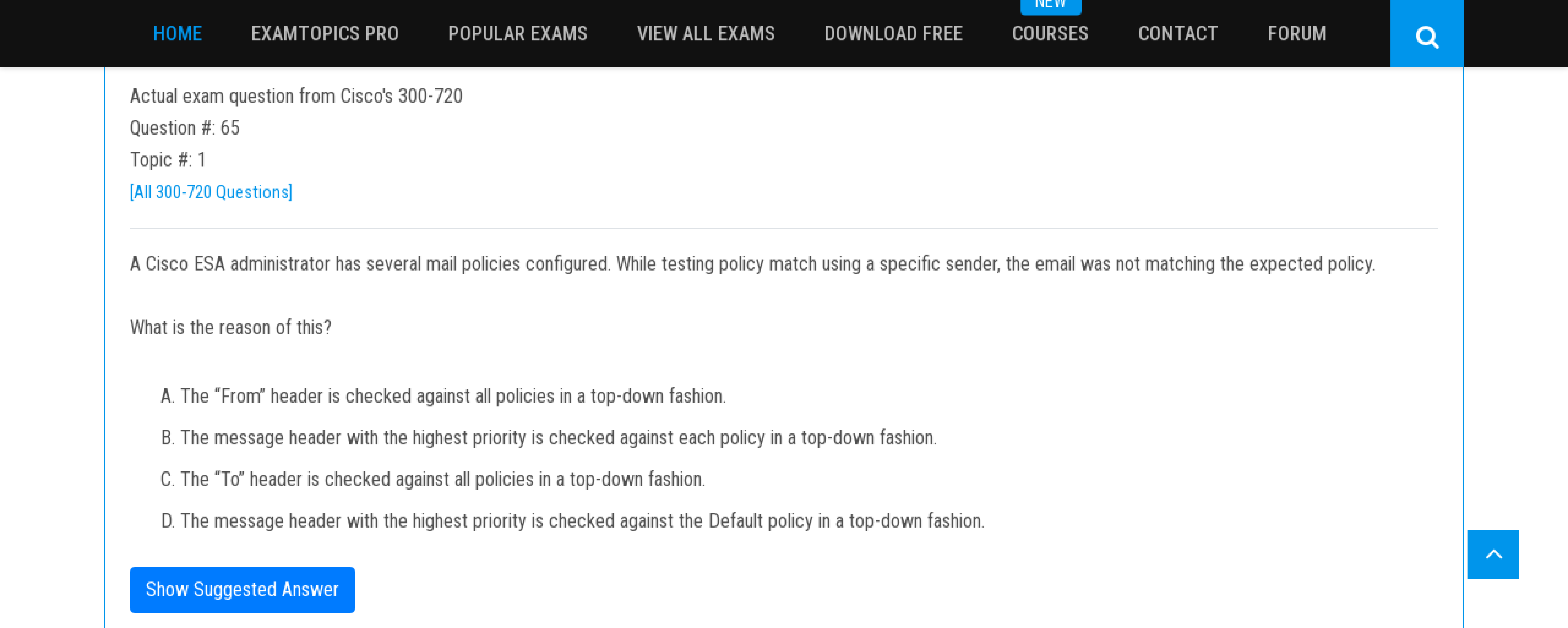
How is this accomplished?

A. Disable the VOF feature before sending SPAM to the external quarantine.

B. Configure a mail policy to determine whether the message is sent to the local or external quarantine.

C. Disable the local quarantine before sending SPAM to the external quarantine.

D. Configure a user policy to determine whether the message is sent to the local or external quarantine.



Actual exam question from Cisco's 300-720

Question #: 65

Topic #: 1

[All 300-720 Questions]

A Cisco ESA administrator has several mail policies configured. While testing policy match using a specific sender, the email was not matching the expected policy.

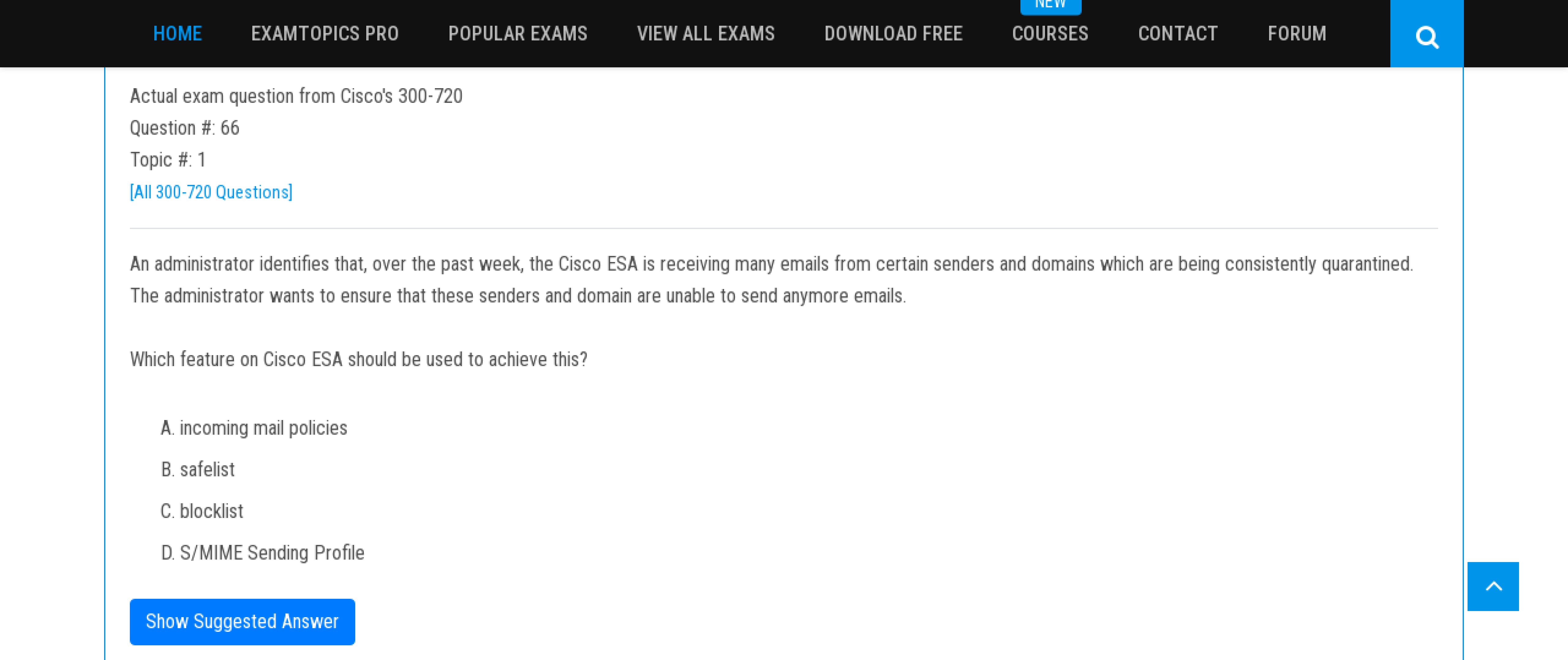
What is the reason of this?

A. The “From” header is checked against all policies in a top-down fashion.

B. The message header with the highest priority is checked against each policy in a top-down fashion.

C. The “To” header is checked against all policies in a top-down fashion.

D. The message header with the highest priority is checked against the Default policy in a top-down fashion.



Actual exam question from Cisco's 300-720

Question #: 66

Topic #: 1

[All 300-720 Questions]

An administrator identifies that, over the past week, the Cisco ESA is receiving many emails from certain senders and domains which are being consistently quarantined. The administrator wants to ensure that these senders and domain are unable to send anymore emails.

Which feature on Cisco ESA should be used to achieve this?

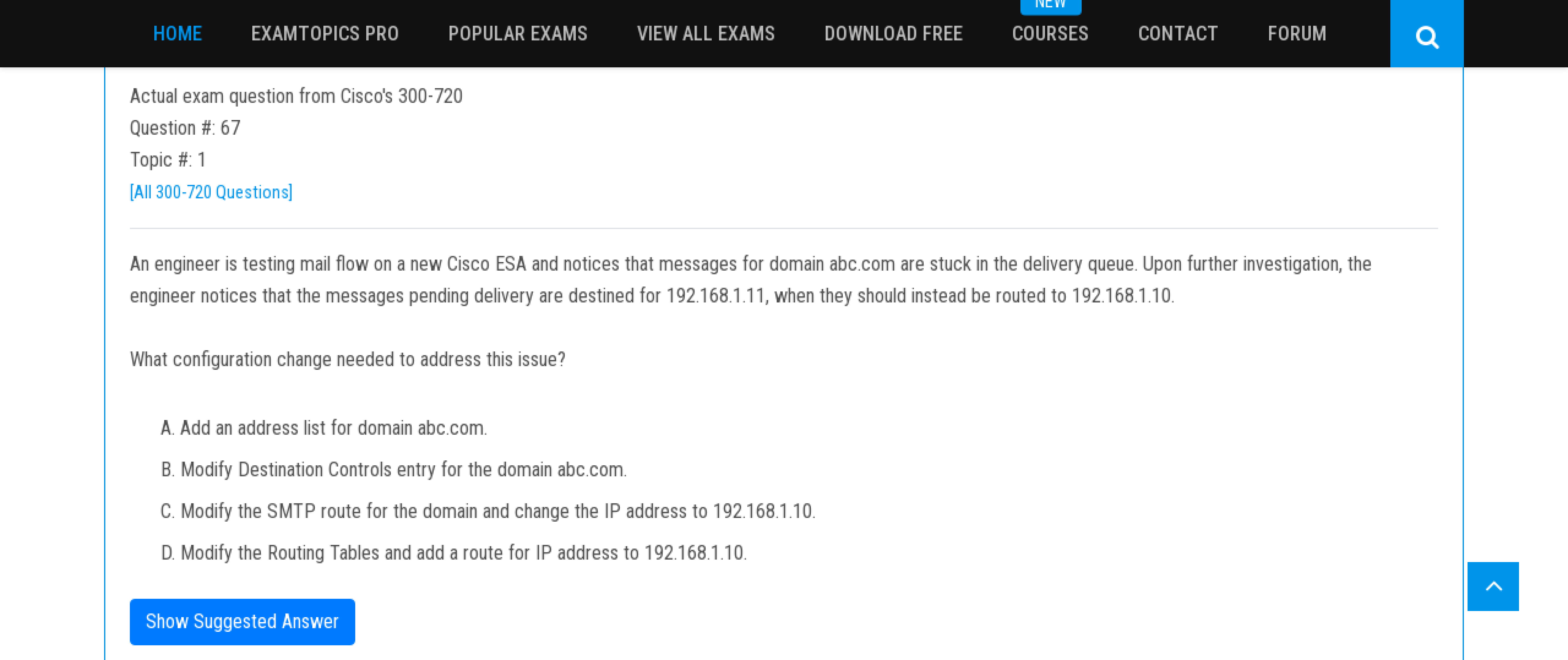
A. incoming mail policies

B. safelist

C. blocklist

D. S/MIME Sending Profile

Show Suggested Answer



Actual exam question from Cisco's 300-720
Question #: 67
Topic #: 1
[All 300-720 Questions]

An engineer is testing mail flow on a new Cisco ESA and notices that messages for domain abc.com are stuck in the delivery queue. Upon further investigation, the engineer notices that the messages pending delivery are destined for 192.168.1.11, when they should instead be routed to 192.168.1.10.

What configuration change needed to address this issue?

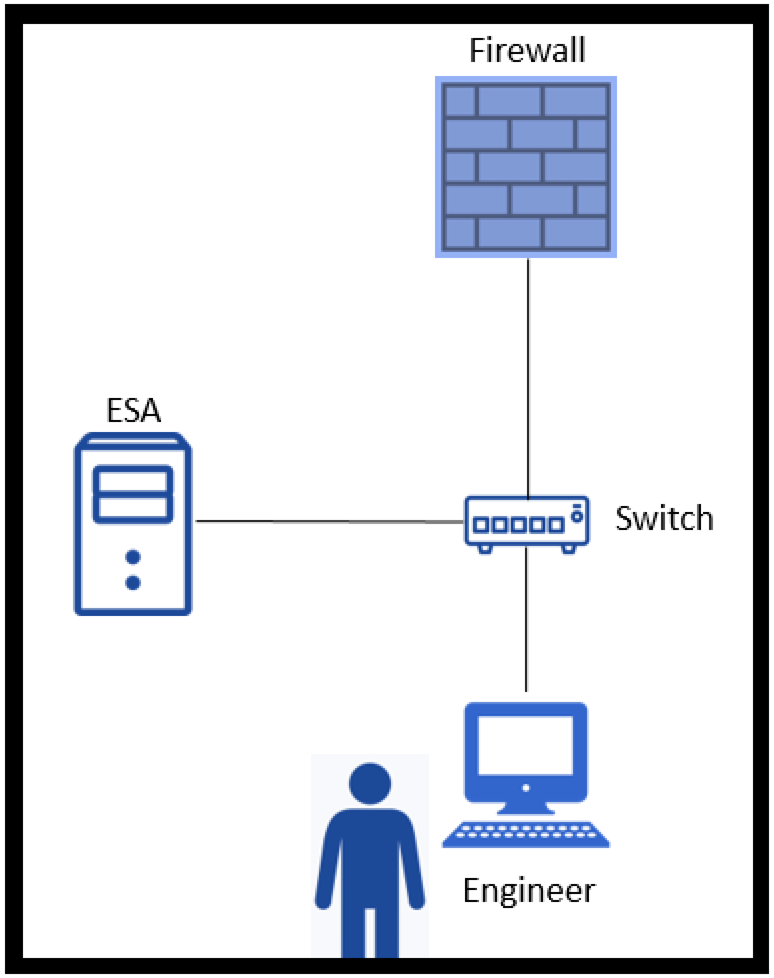
A. Add an address list for domain abc.com.

B. Modify Destination Controls entry for the domain abc.com.

C. Modify the SMTP route for the domain and change the IP address to 192.168.1.10.

D. Modify the Routing Tables and add a route for IP address to 192.168.1.10.

Actual exam question from Cisco's 300-720
Question #: 68
Topic #: 1
[All 300-720 Questions]



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?

A. Telnet

B. HTTPS

C. Ethernet

D. serial

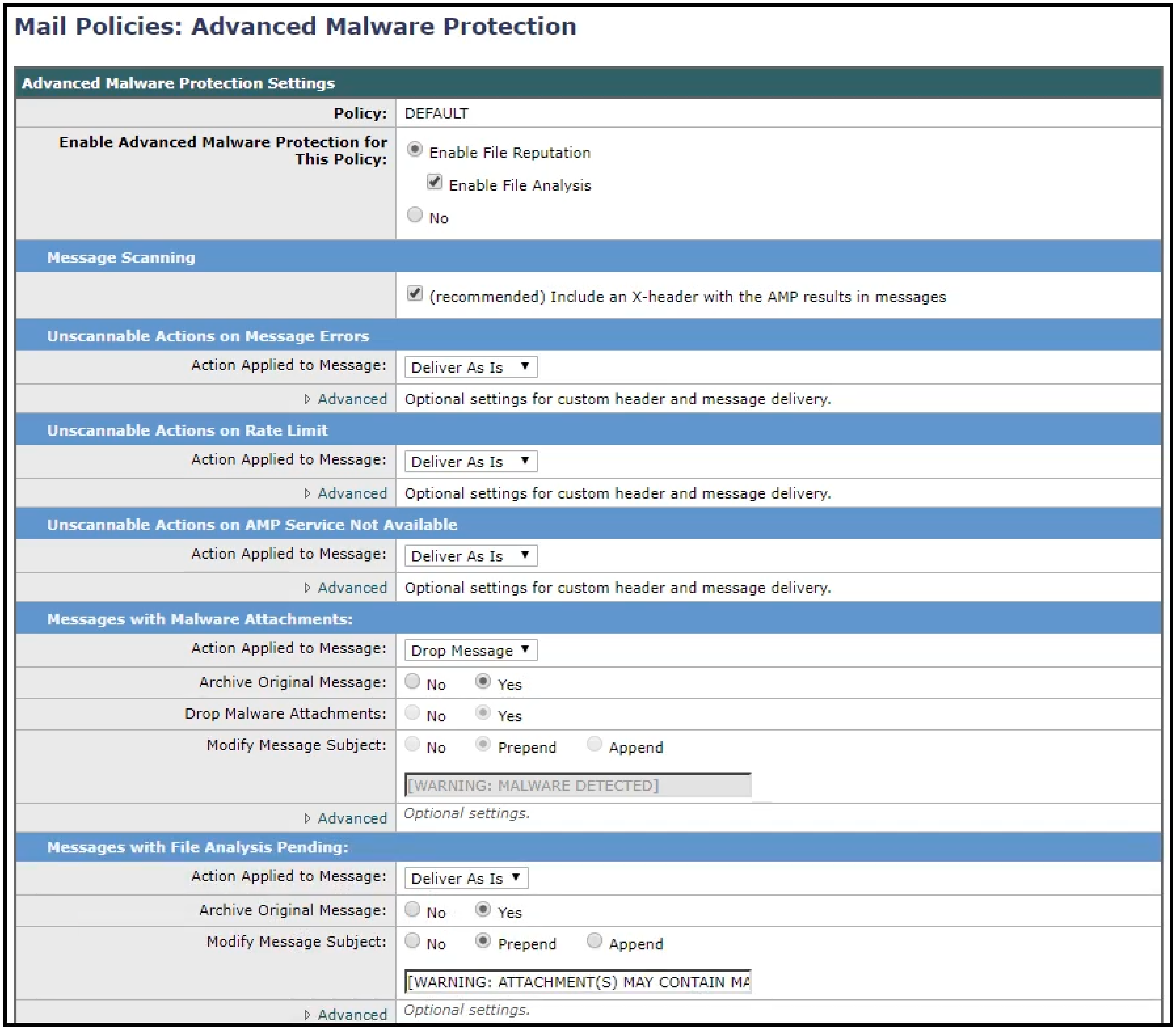
Show Suggested Answer

Actual exam question from Cisco's 300-720

Question #: 69

Topic #: 1

[All 300-720 Questions]



Mail Policies: Advanced Malware Protection

Advanced Malware Protection Settings	
Policy:	DEFAULT
Enable Advanced Malware Protection for This Policy:	● Enable File Reputation ☑ Enable File Analysis ○ No
Message Scanning	
	☑ (recommended) Include an X-header with the AMP results in messages
Unscannable Actions on Message Errors	
Action Applied to Message:	Deliver As Is ▼
▷ Advanced	Optional settings for custom header and message delivery.
Unscannable Actions on Rate Limit	
Action Applied to Message:	Deliver As Is ▼
▷ Advanced	Optional settings for custom header and message delivery.
Unscannable Actions on AMP Service Not Available	
Action Applied to Message:	Deliver As Is ▼
▷ Advanced	Optional settings for custom header and message delivery.
Messages with Malware Attachments:	
Action Applied to Message:	Drop Message ▼
Archive Original Message:	○ No ● Yes
Drop Malware Attachments:	○ No ● Yes
Modify Message Subject:	○ No ● Prepend ○ Append [WARNING: MALWARE DETECTED]
▷ Advanced	*Optional settings.*
Messages with File Analysis Pending:	
Action Applied to Message:	Deliver As Is ▼
Archive Original Message:	○ No ● Yes
Modify Message Subject:	○ No ● Prepend ○ Append [WARNING: ATTACHMENT(S) MAY CONTAIN MA
▷ Advanced	*Optional settings.*

Refer to the exhibit. How should this configuration be modified to stop delivering Zero Day malware attacks?

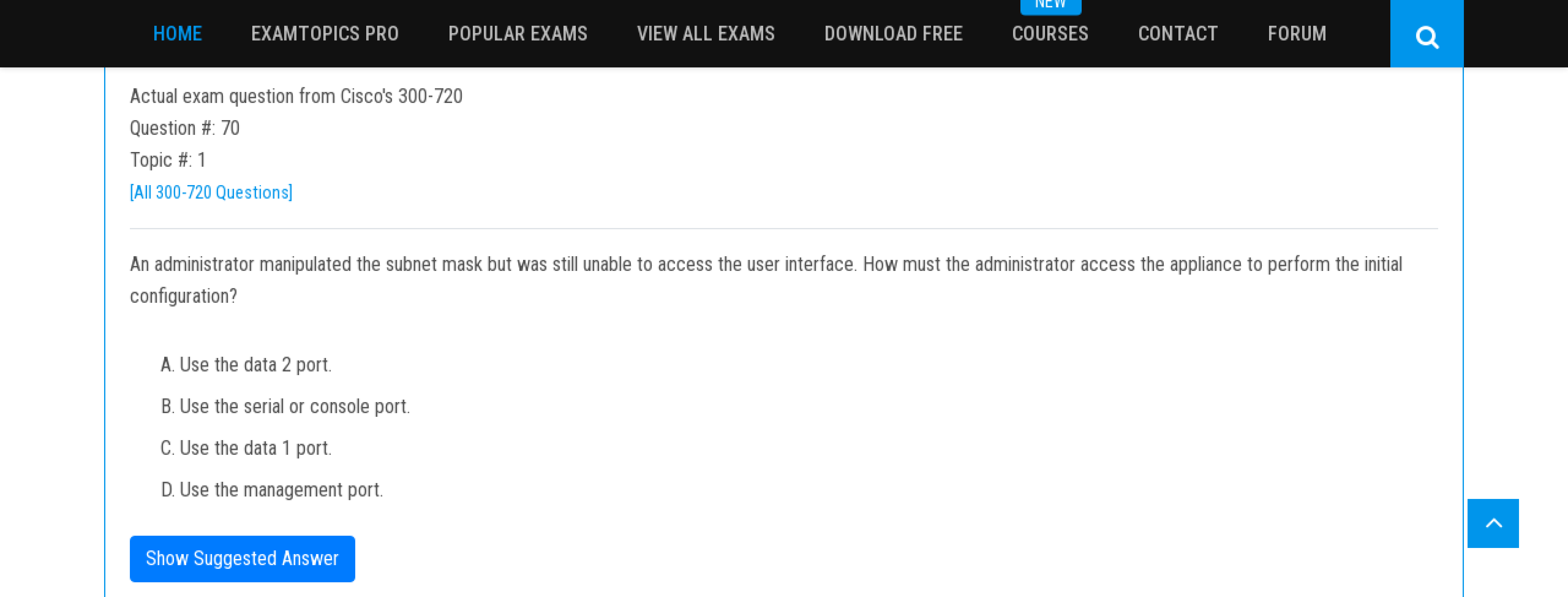
A. Change Unscannable Action from Deliver As Is to Quarantine.

B. Change File Analysis Pending action from Deliver As Is to Quarantine.

C. Configure mailbox auto-remediation.

D. Apply Prepend on Modify Message Subject under Malware Attachments.

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 70

Topic #: 1

[All 300-720 Questions]

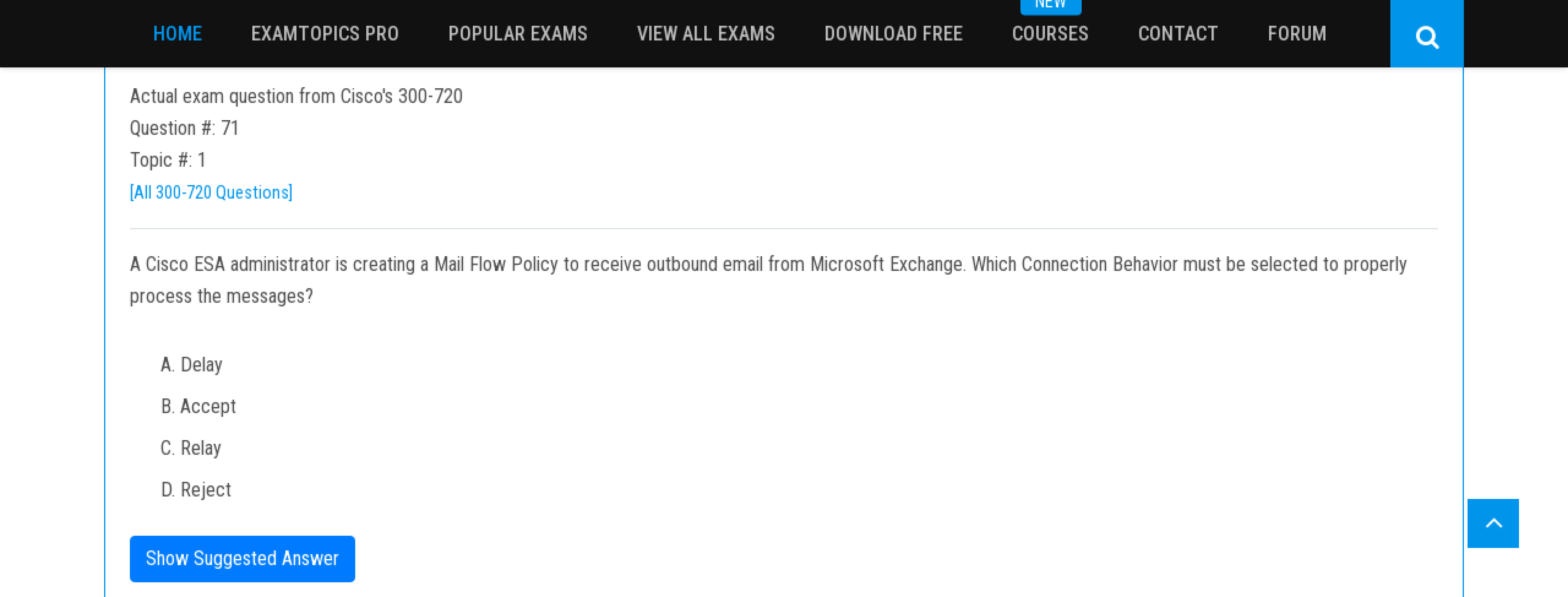
An administrator manipulated the subnet mask but was still unable to access the user interface. How must the administrator access the appliance to perform the initial configuration?

A. Use the data 2 port.

B. Use the serial or console port.

C. Use the data 1 port.

D. Use the management port.



Actual exam question from Cisco's 300-720

Question #: 71

Topic #: 1

[All 300-720 Questions]

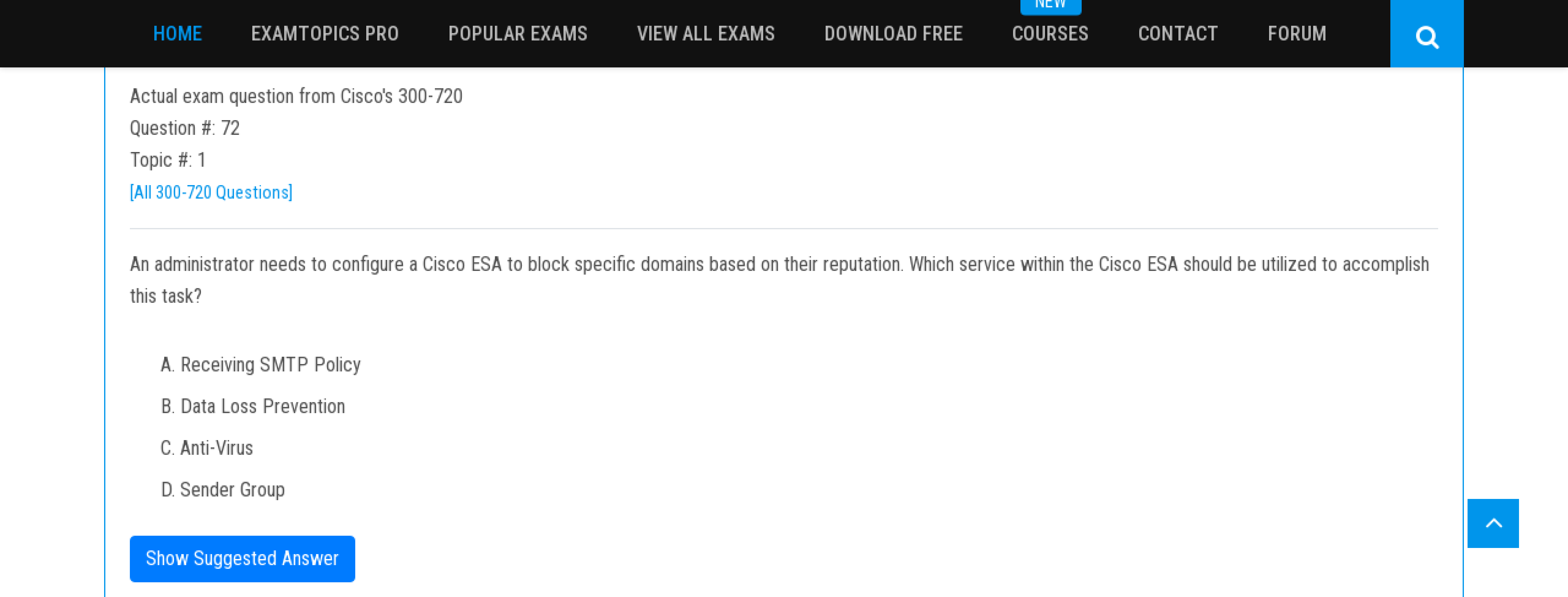
A Cisco ESA administrator is creating a Mail Flow Policy to receive outbound email from Microsoft Exchange. Which Connection Behavior must be selected to properly process the messages?

A. Delay

B. Accept

C. Relay

D. Reject



Actual exam question from Cisco's 300-720

Question #: 72

Topic #: 1

[All 300-720 Questions]

An administrator needs to configure a Cisco ESA to block specific domains based on their reputation. Which service within the Cisco ESA should be utilized to accomplish this task?

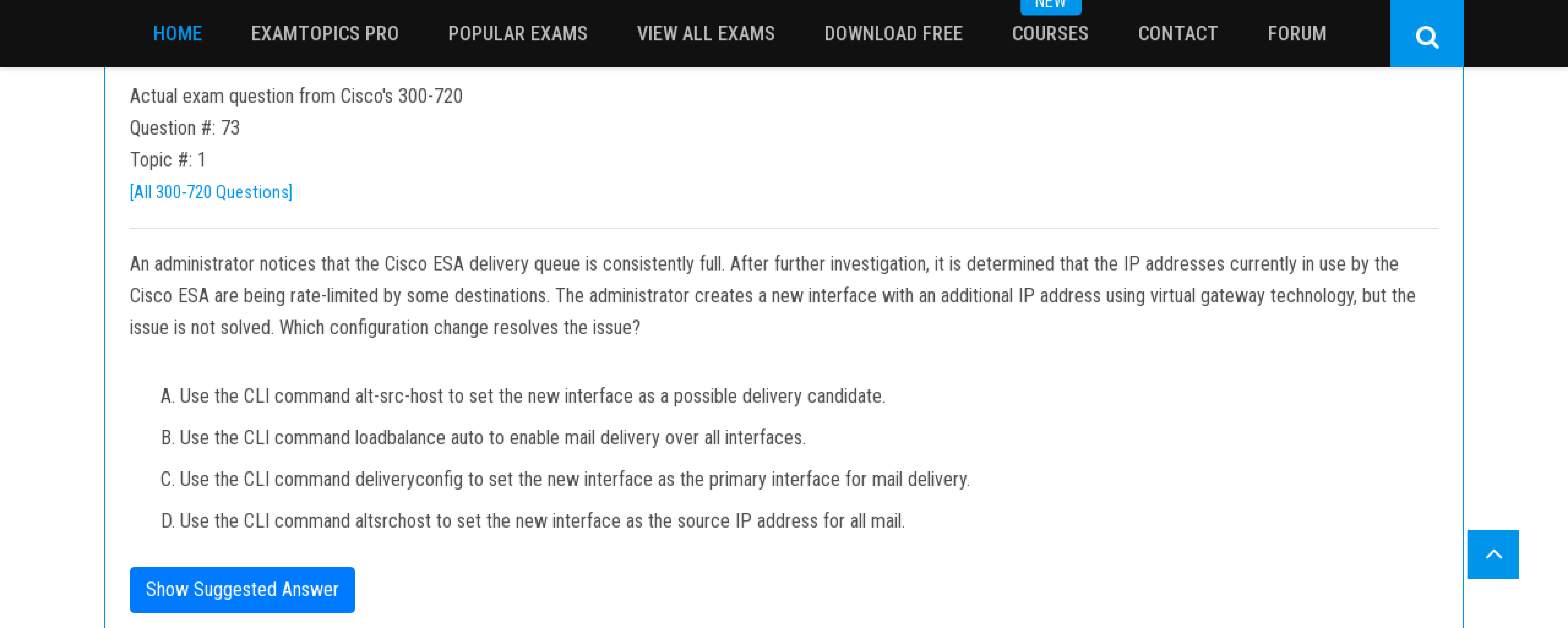
A. Receiving SMTP Policy

B. Data Loss Prevention

C. Anti-Virus

D. Sender Group

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 73

Topic #: 1

[All 300-720 Questions]

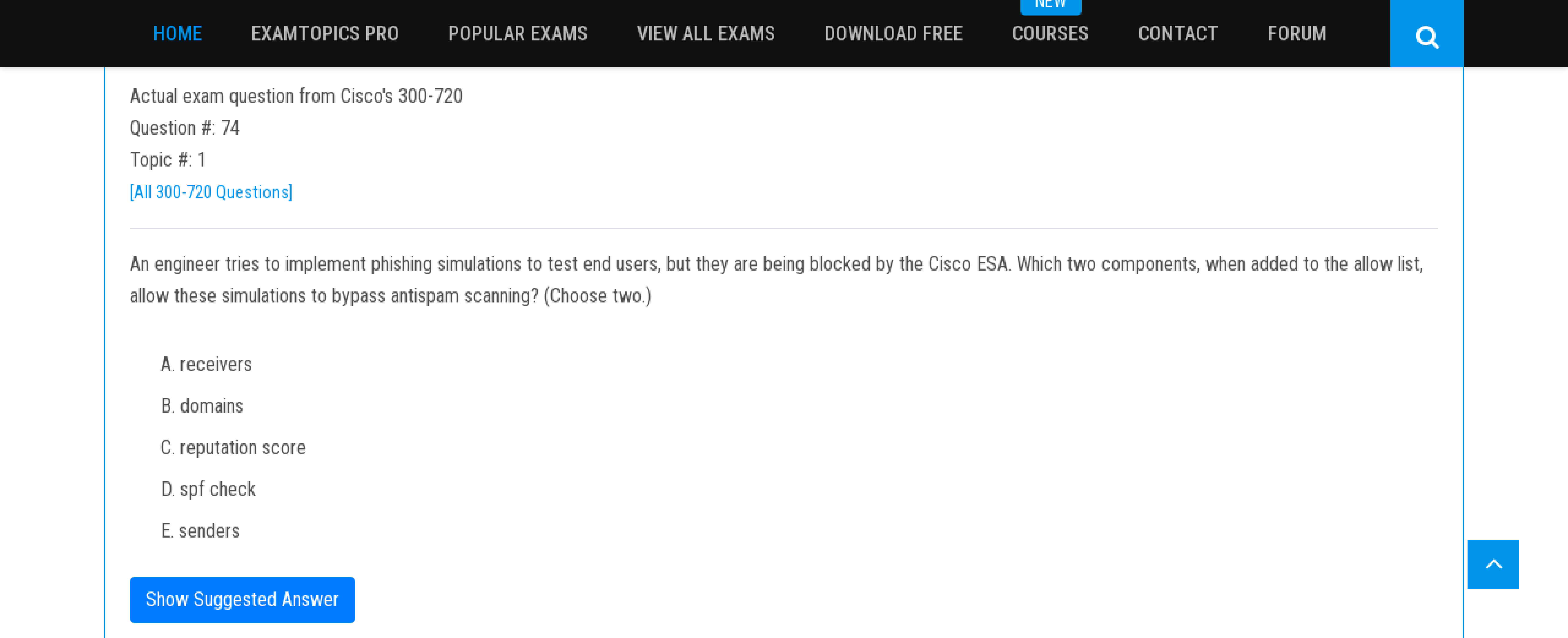
An administrator notices that the Cisco ESA delivery queue is consistently full. After further investigation, it is determined that the IP addresses currently in use by the Cisco ESA are being rate-limited by some destinations. The administrator creates a new interface with an additional IP address using virtual gateway technology, but the issue is not solved. Which configuration change resolves the issue?

A. Use the CLI command alt-src-host to set the new interface as a possible delivery candidate.

B. Use the CLI command loadbalance auto to enable mail delivery over all interfaces.

C. Use the CLI command deliveryconfig to set the new interface as the primary interface for mail delivery.

D. Use the CLI command altsrchost to set the new interface as the source IP address for all mail.



Actual exam question from Cisco's 300-720

Question #: 74

Topic #: 1

[All 300-720 Questions]

An engineer tries to implement phishing simulations to test end users, but they are being blocked by the Cisco ESA. Which two components, when added to the allow list, allow these simulations to bypass antispam scanning? (Choose two.)

A. receivers

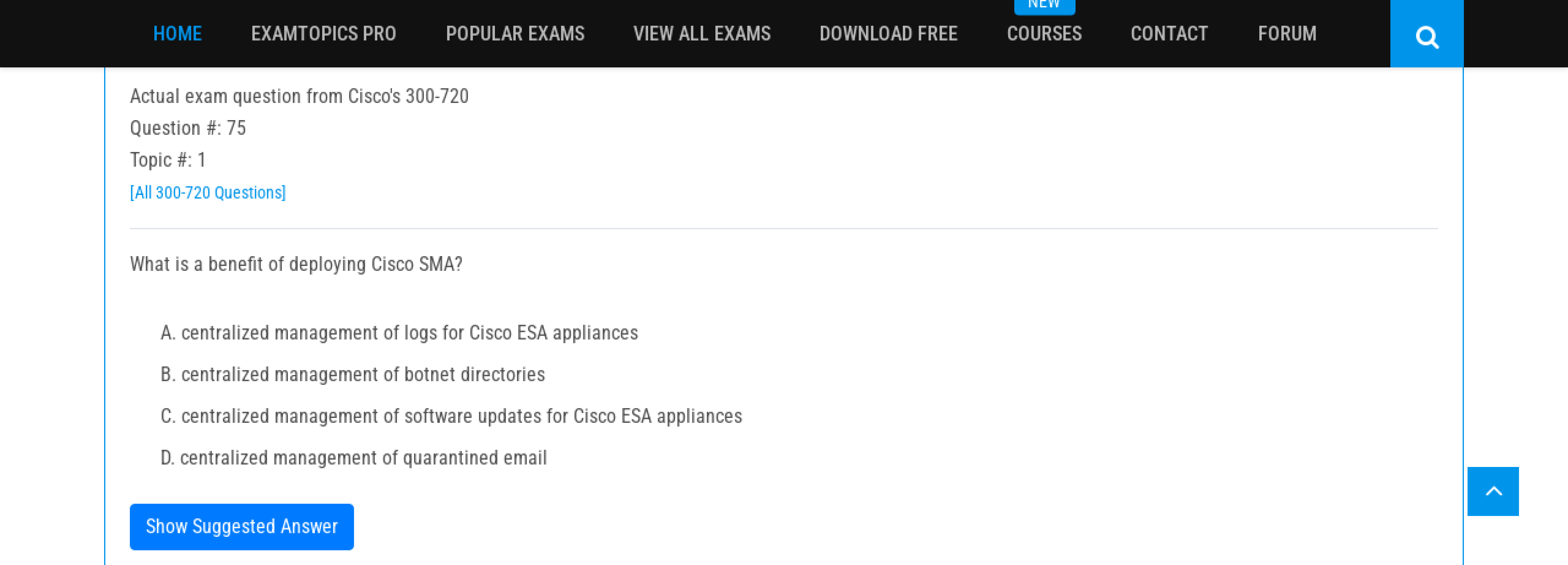
B. domains

C. reputation score

D. spf check

E. senders

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 75

Topic #: 1

[All 300-720 Questions]

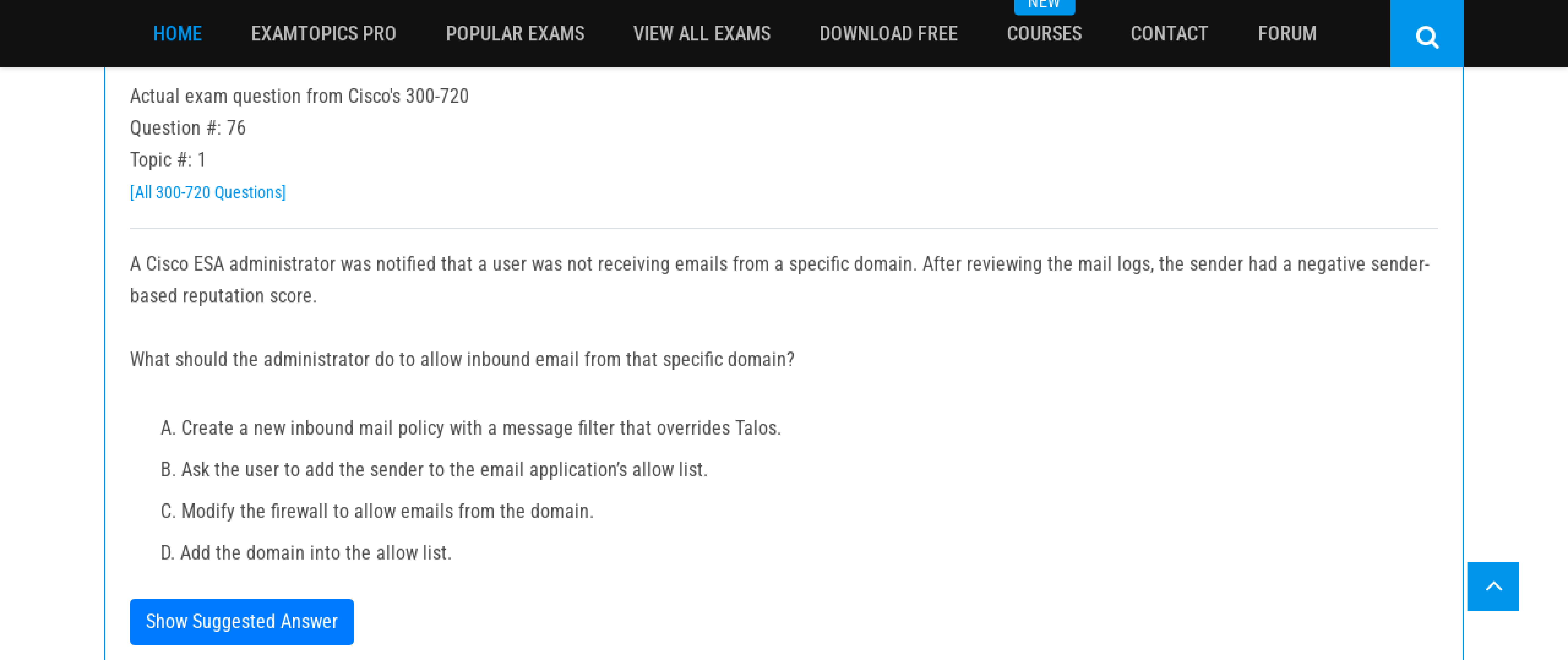
What is a benefit of deploying Cisco SMA?

A. centralized management of logs for Cisco ESA appliances

B. centralized management of botnet directories

C. centralized management of software updates for Cisco ESA appliances

D. centralized management of quarantined email



Actual exam question from Cisco's 300-720

Question #: 76

Topic #: 1

[All 300-720 Questions]

A Cisco ESA administrator was notified that a user was not receiving emails from a specific domain. After reviewing the mail logs, the sender had a negative sender-based reputation score.

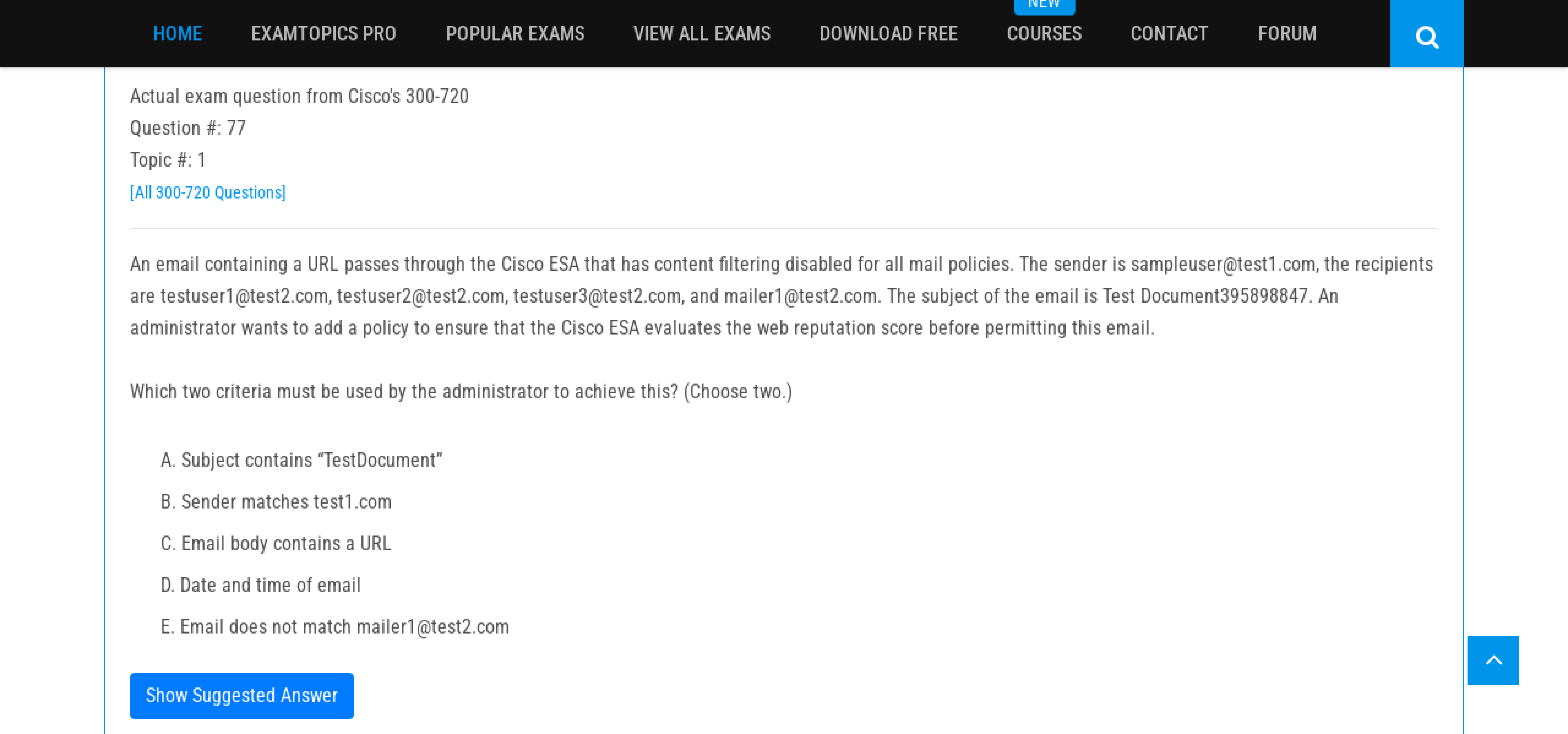
What should the administrator do to allow inbound email from that specific domain?

A. Create a new inbound mail policy with a message filter that overrides Talos.

B. Ask the user to add the sender to the email application's allow list.

C. Modify the firewall to allow emails from the domain.

D. Add the domain into the allow list.



Actual exam question from Cisco's 300-720

Question #: 77

Topic #: 1

[All 300-720 Questions]

An email containing a URL passes through the Cisco ESA that has content filtering disabled for all mail policies. The sender is sampleuser@test1.com, the recipients are testuser1@test2.com, testuser2@test2.com, testuser3@test2.com, and mailer1@test2.com. The subject of the email is Test Document395898847. An administrator wants to add a policy to ensure that the Cisco ESA evaluates the web reputation score before permitting this email.

Which two criteria must be used by the administrator to achieve this? (Choose two.)

A. Subject contains “TestDocument”

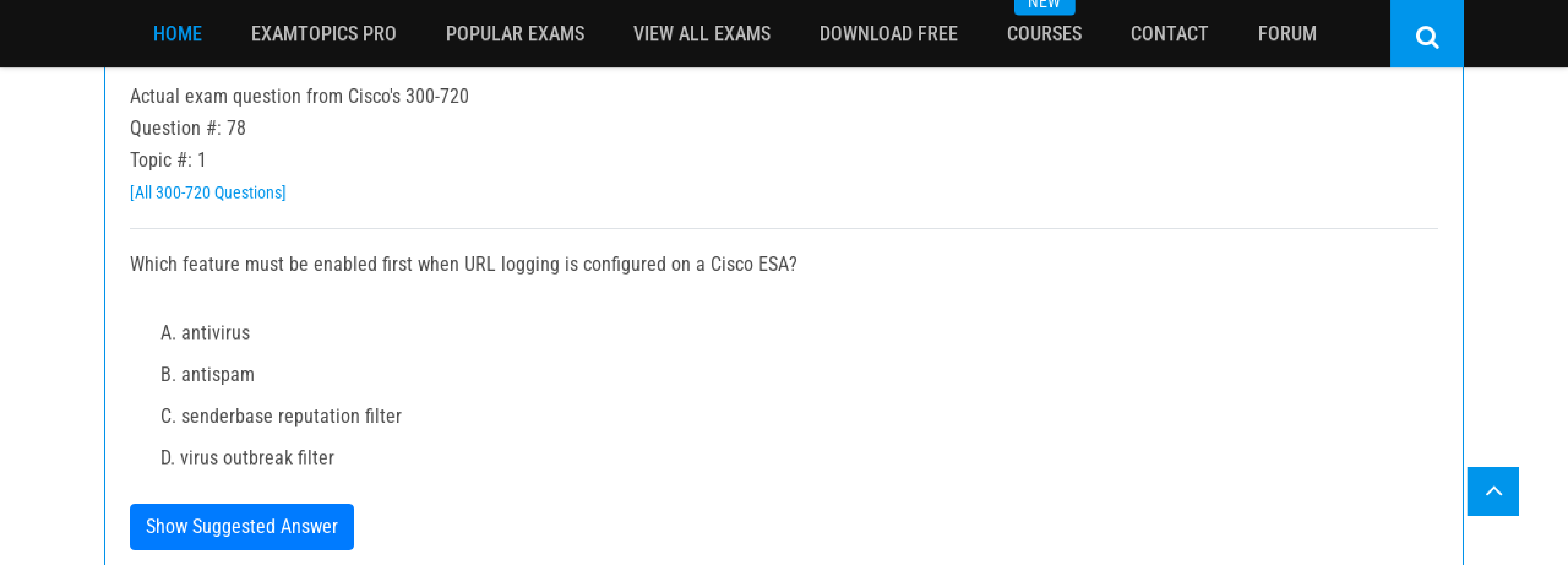
B. Sender matches test1.com

C. Email body contains a URL

D. Date and time of email

E. Email does not match mailer1@test2.com

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 78

Topic #: 1

[All 300-720 Questions]

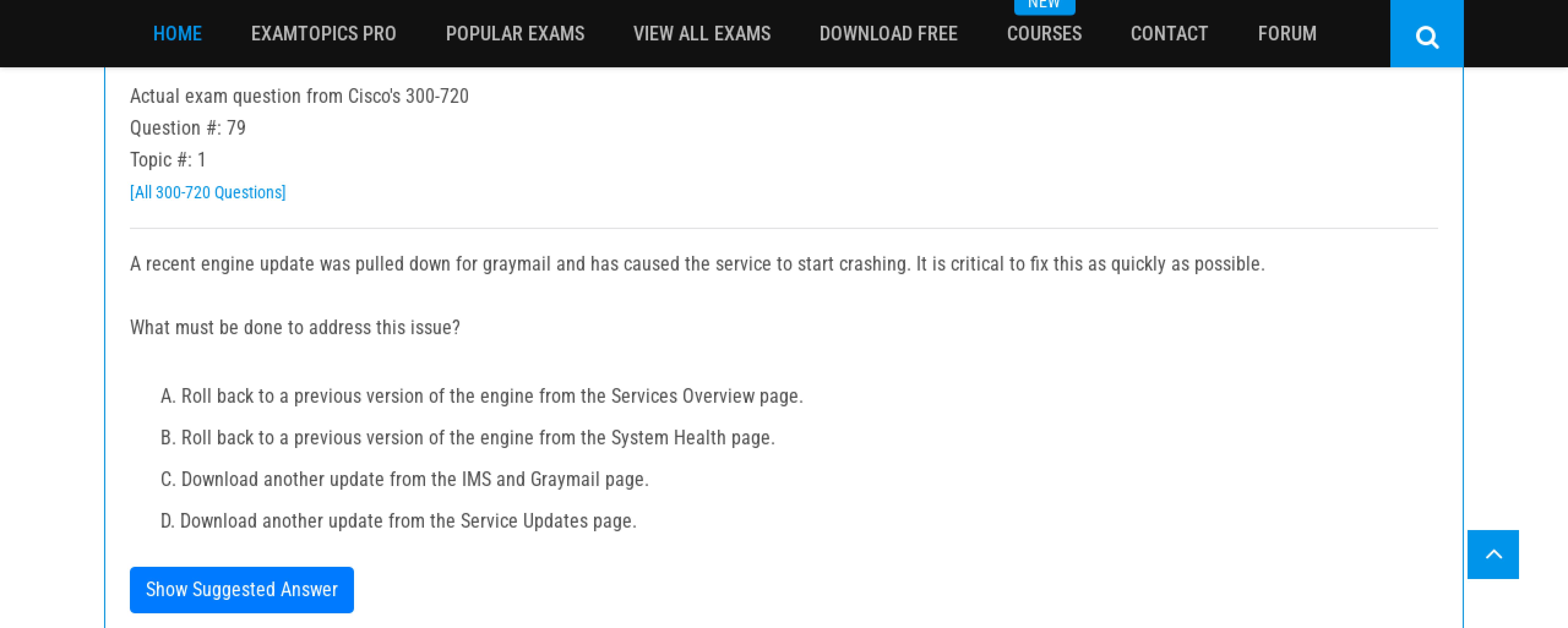
Which feature must be enabled first when URL logging is configured on a Cisco ESA?

A. antivirus

B. antispam

C. senderbase reputation filter

D. virus outbreak filter



Actual exam question from Cisco's 300-720

Question #: 79

Topic #: 1

[All 300-720 Questions]

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.

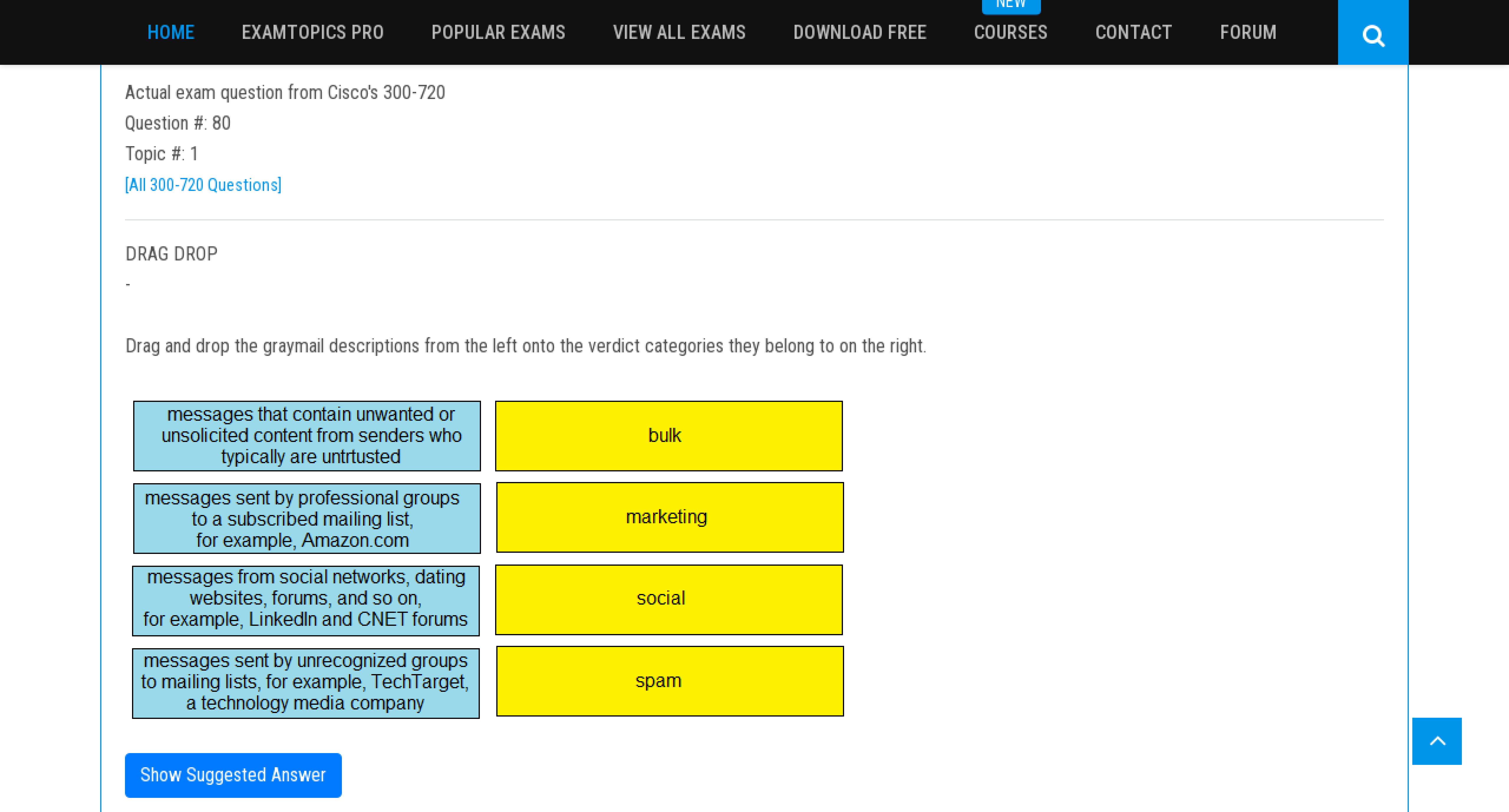
What must be done to address this issue?

A. Roll back to a previous version of the engine from the Services Overview page.

B. Roll back to a previous version of the engine from the System Health page.

C. Download another update from the IMS and Graymail page.

D. Download another update from the Service Updates page.



Actual exam question from Cisco's 300-720

Question #: 80

Topic #: 1

[All 300-720 Questions]

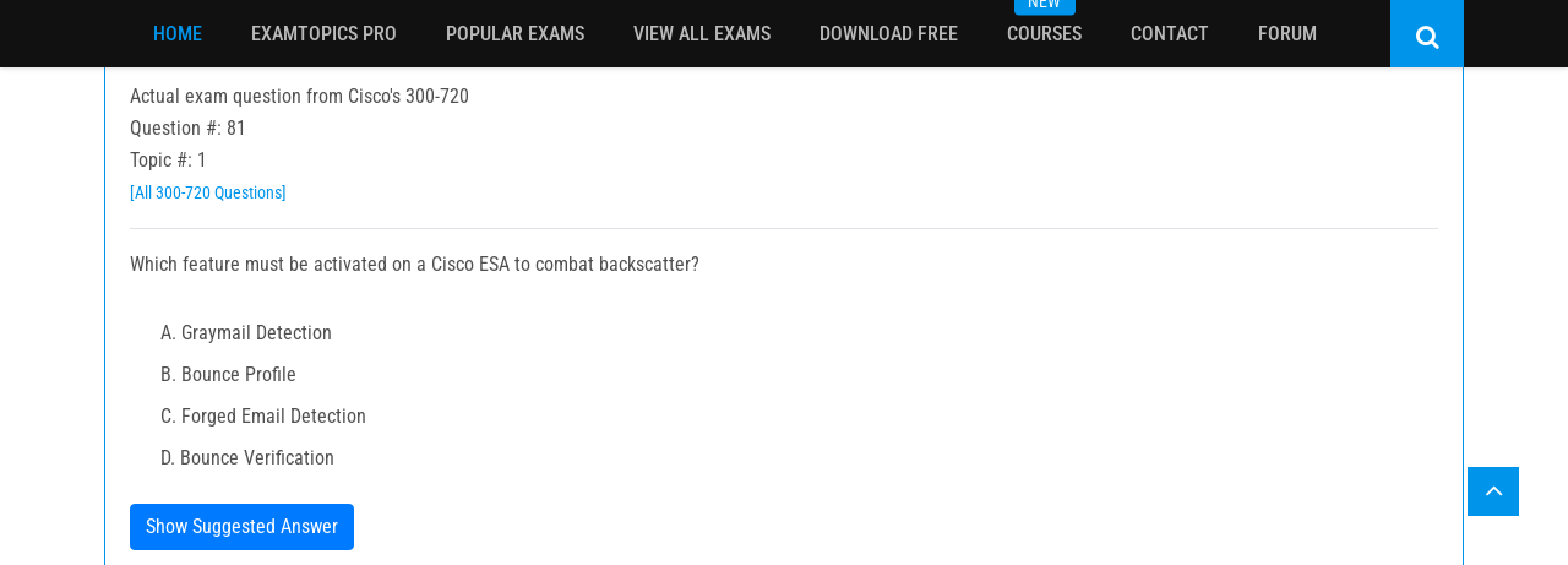
DRAG DROP

-

Drag and drop the graymail descriptions from the left onto the verdict categories they belong to on the right.

messages that contain unwanted or unsolicited content from senders who typically are untrtusted	bulk
messages sent by professional groups to a subscribed mailing list, for example, Amazon.com	marketing
messages from social networks, dating websites, forums, and so on, for example, LinkedIn and CNET forums	social
messages sent by unrecognized groups to mailing lists, for example, TechTarget, a technology media company	spam

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 81

Topic #: 1

[All 300-720 Questions]

Which feature must be activated on a Cisco ESA to combat backscatter?

A. Graymail Detection

B. Bounce Profile

C. Forged Email Detection

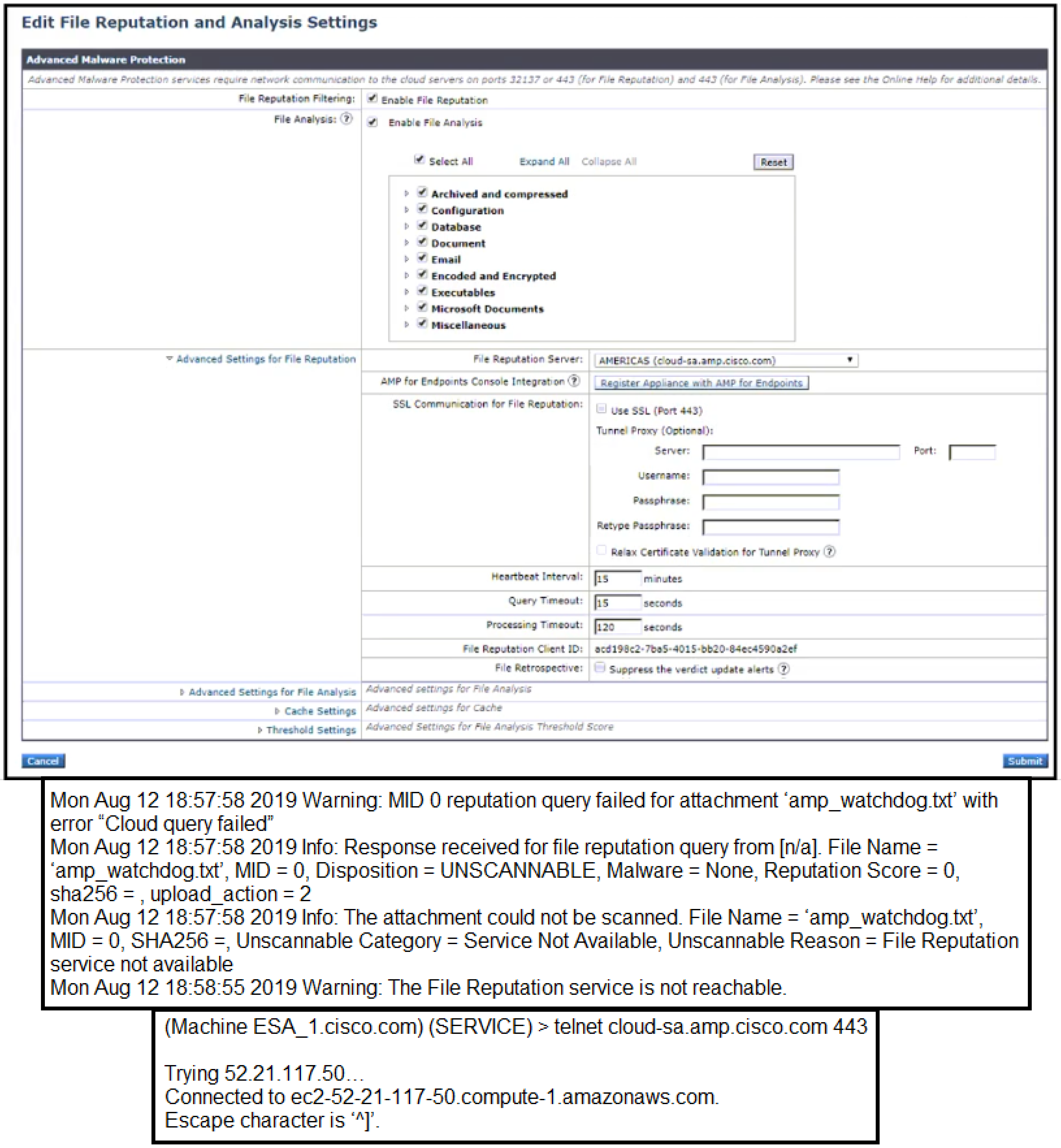
D. Bounce Verification

Actual exam question from Cisco's 300-720

Question #: 82

Topic #: 1

[All 300-720 Questions]



Edit File Reputation and Analysis Settings

Advanced Malware Protection

Advanced Malware Protection services require network communication to the cloud servers on ports 32137 or 443 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.

File Reputation Filtering: ☑ Enable File Reputation

File Analysis: ? ☑ Enable File Analysis

☑ Select All Expand All Collapse All Reset

- ☑ **Archived and compressed**
- ☑ **Configuration**
- ☑ **Database**
- ☑ **Document**
- ☑ **Email**
- ☑ **Encoded and Encrypted**
- ☑ **Executables**
- ☑ **Microsoft Documents**
- ☑ **Miscellaneous**

▿ Advanced Settings for File Reputation

File Reputation Server: AMERICAS (cloud-sa.amp.cisco.com) ▾

AMP for Endpoints Console Integration ? Register Appliance with AMP for Endpoints

SSL Communication for File Reputation: □ Use SSL (Port 443)

Tunnel Proxy (Optional):

Server: Port:

Username:

Passphrase:

Retype Passphrase:

□ Relax Certificate Validation for Tunnel Proxy ?

Heartbeat Interval: 15 minutes

Query Timeout: 15 seconds

Processing Timeout: 120 seconds

File Reputation Client ID: acd198c2-7ba5-4015-bb20-84ec4590a2ef

File Retrospective: □ Suppress the verdict update alerts ?

▹ Advanced Settings for File Analysis *Advanced settings for File Analysis*

▹ Cache Settings *Advanced settings for Cache*

▹ Threshold Settings *Advanced Settings for File Analysis Threshold Score*

Cancel Submit

```
Mon Aug 12 18:57:58 2019 Warning: MID 0 reputation query failed for attachment ‘amp_watchdog.txt’ with
error “Cloud query failed”
Mon Aug 12 18:57:58 2019 Info: Response received for file reputation query from [n/a]. File Name =
‘amp_watchdog.txt’, MID = 0, Disposition = UNSCANNABLE, Malware = None, Reputation Score = 0,
sha256 = , upload_action = 2
Mon Aug 12 18:57:58 2019 Info: The attachment could not be scanned. File Name = ‘amp_watchdog.txt’,
MID = 0, SHA256 =, Unscannable Category = Service Not Available, Unscannable Reason = File Reputation
service not available
Mon Aug 12 18:58:55 2019 Warning: The File Reputation service is not reachable.
```

```
(Machine ESA_1.cisco.com) (SERVICE) > telnet cloud-sa.amp.cisco.com 443

Trying 52.21.117.50…
Connected to ec2-52-21-117-50.compute-1.amazonaws.com.
Escape character is ‘^]’.
```

Refer to the exhibit. An administrator has configured File Reputation and File Analysis on the Cisco ESA; however, is does not function as expected. What must be configured on the Cisco ESA for this to function?

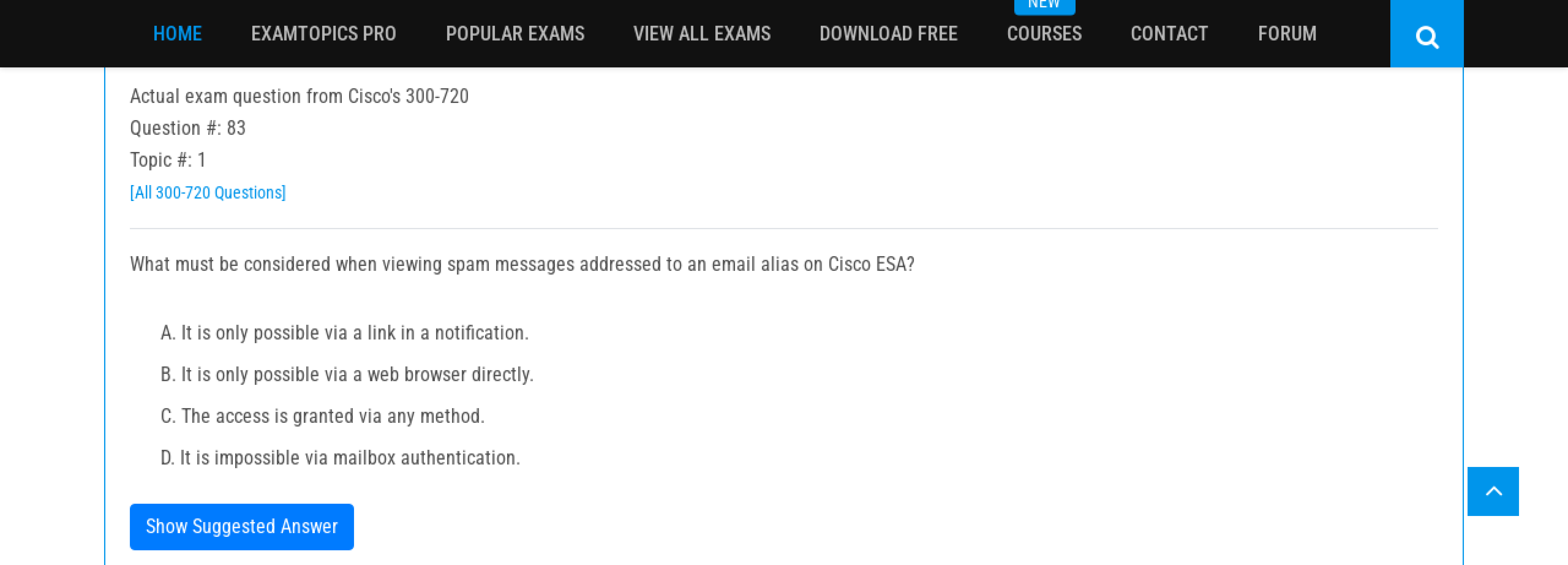
A. Upload the Root CA certificate for the File Reputation cloud to the Cisco ESA.

B. Open port 443 on the firewall for the Cisco ESA to connect to the File Reputation cloud.

C. Restart the File Reputation service to force the scanning engine to connect to the File Reputation cloud.

D. Configure the Cisco ESA to use SSL for the connection to the File Reputation server.

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 83

Topic #: 1

[All 300-720 Questions]

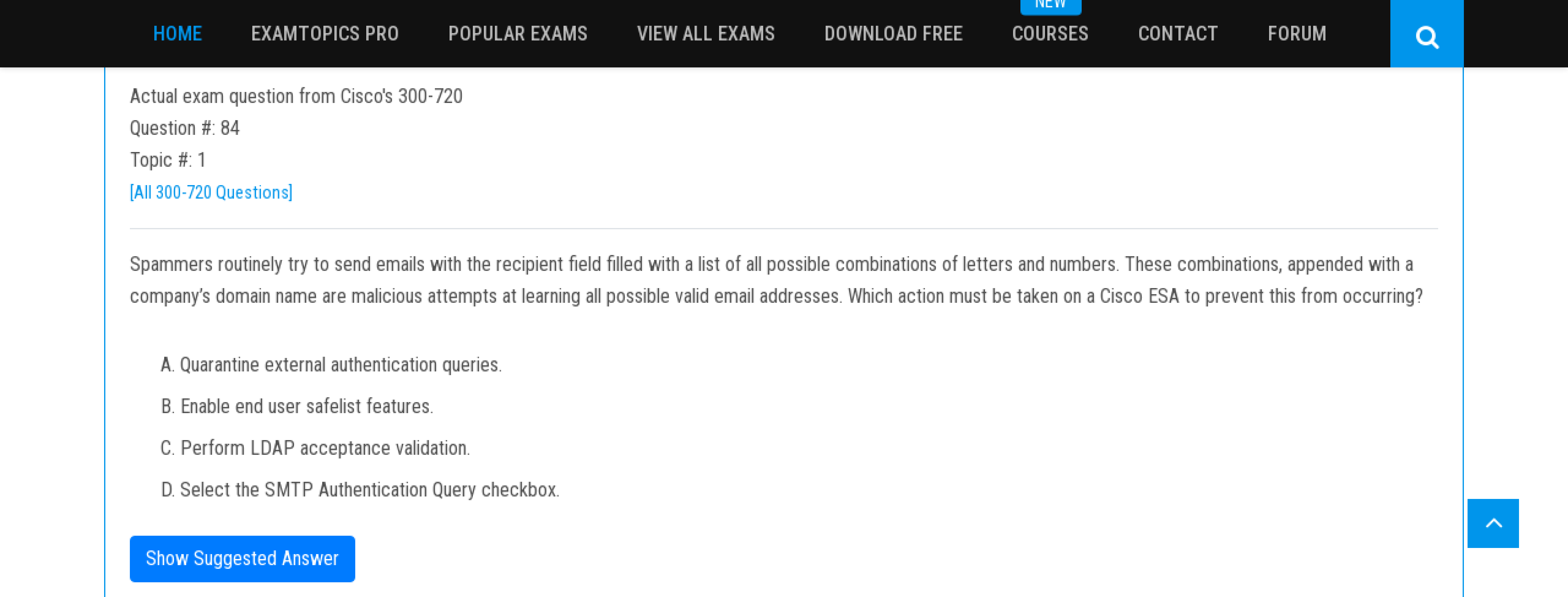
What must be considered when viewing spam messages addressed to an email alias on Cisco ESA?

A. It is only possible via a link in a notification.

B. It is only possible via a web browser directly.

C. The access is granted via any method.

D. It is impossible via mailbox authentication.



Actual exam question from Cisco's 300-720

Question #: 84

Topic #: 1

[All 300-720 Questions]

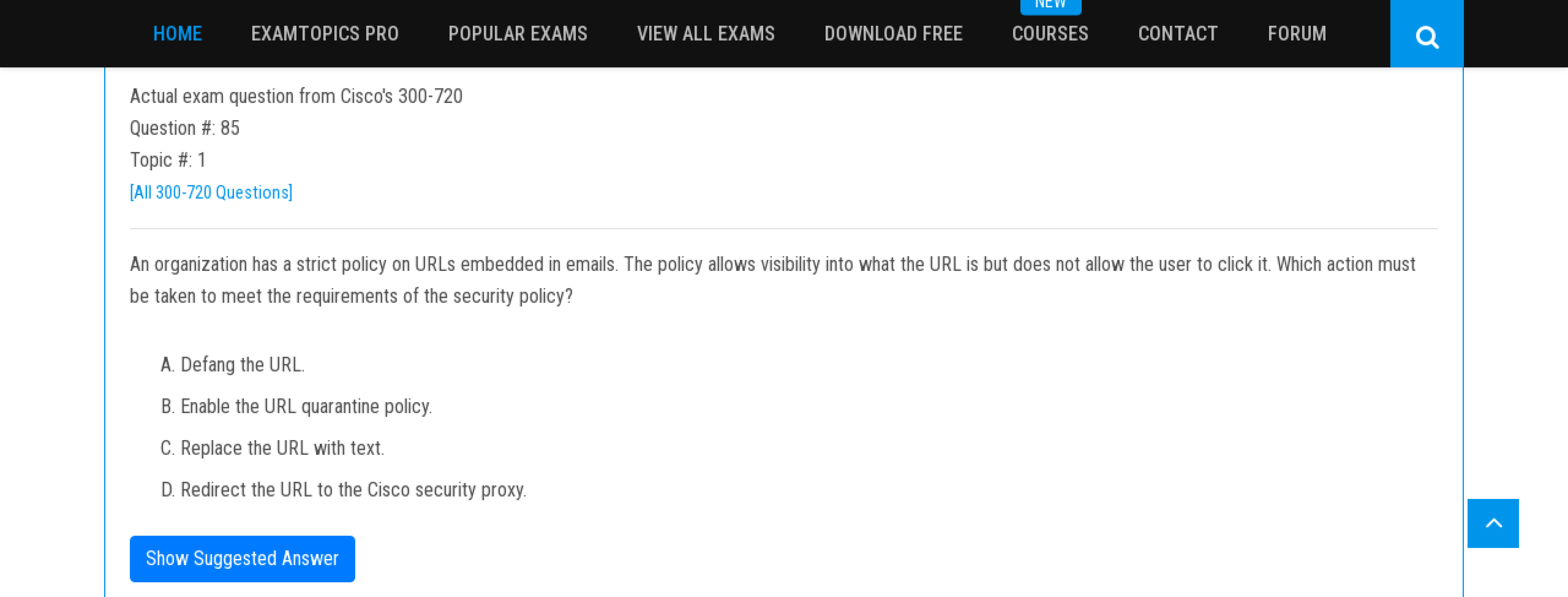
Spammers routinely try to send emails with the recipient field filled with a list of all possible combinations of letters and numbers. These combinations, appended with a company's domain name are malicious attempts at learning all possible valid email addresses. Which action must be taken on a Cisco ESA to prevent this from occurring?

A. Quarantine external authentication queries.

B. Enable end user safelist features.

C. Perform LDAP acceptance validation.

D. Select the SMTP Authentication Query checkbox.



Actual exam question from Cisco's 300-720

Question #: 85

Topic #: 1

[All 300-720 Questions]

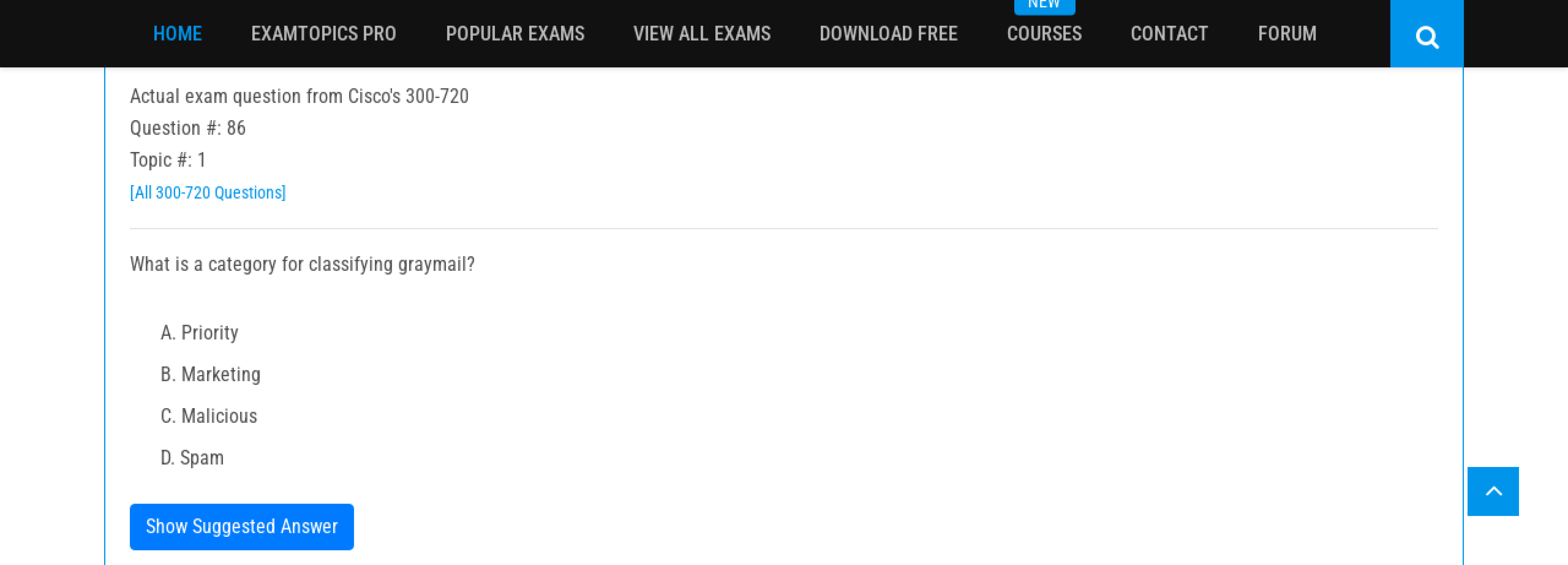
An organization has a strict policy on URLs embedded in emails. The policy allows visibility into what the URL is but does not allow the user to click it. Which action must be taken to meet the requirements of the security policy?

A. Defang the URL.

B. Enable the URL quarantine policy.

C. Replace the URL with text.

D. Redirect the URL to the Cisco security proxy.



Actual exam question from Cisco's 300-720

Question #: 86

Topic #: 1

[All 300-720 Questions]

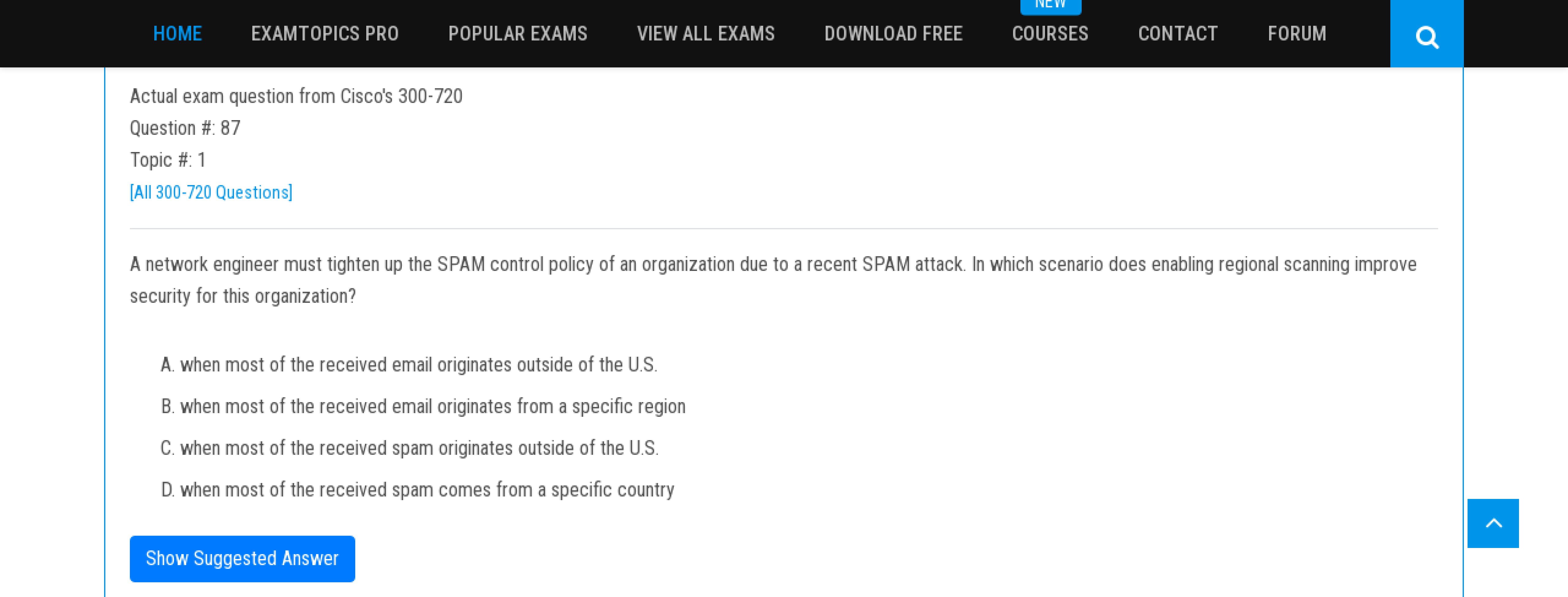
What is a category for classifying graymail?

A. Priority

B. Marketing

C. Malicious

D. Spam



Actual exam question from Cisco's 300-720

Question #: 87

Topic #: 1

[All 300-720 Questions]

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?

A. when most of the received email originates outside of the U.S.

B. when most of the received email originates from a specific region

C. when most of the received spam originates outside of the U.S.

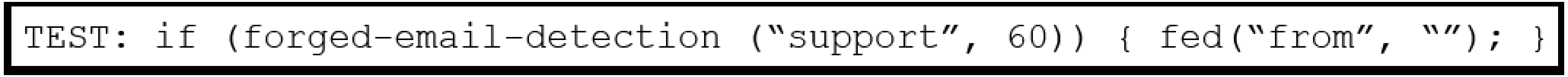
D. when most of the received spam comes from a specific country

Actual exam question from Cisco's 300-720

Question #: 88

Topic #: 1

[All 300-720 Questions]



```
TEST: if (forged-email-detection (“support”, 60)) { fed(“from”, “”); }
```

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 ‘Executives’.

What should be done to accomplish this task?

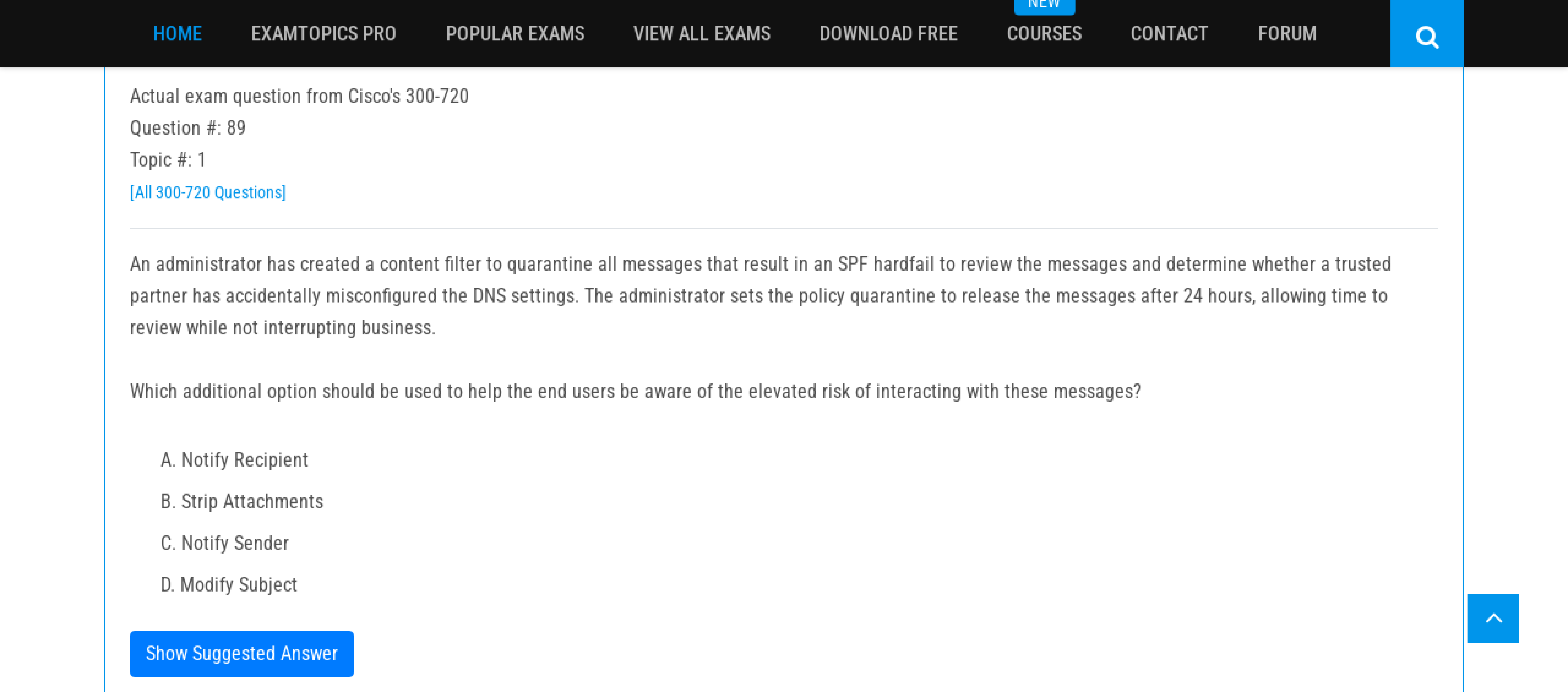
A. Change “from” to “Executives”.

B. Change “TEST” to “Executives”.

C. Change “fed” to “Executives”.

D. Change “support” to “Executives”.

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 89

Topic #: 1

[All 300-720 Questions]

An administrator has created a content filter to quarantine all messages that result in an SPF hardfail to review the messages and determine whether a trusted partner has accidentally misconfigured the DNS settings. The administrator sets the policy quarantine to release the messages after 24 hours, allowing time to review while not interrupting business.

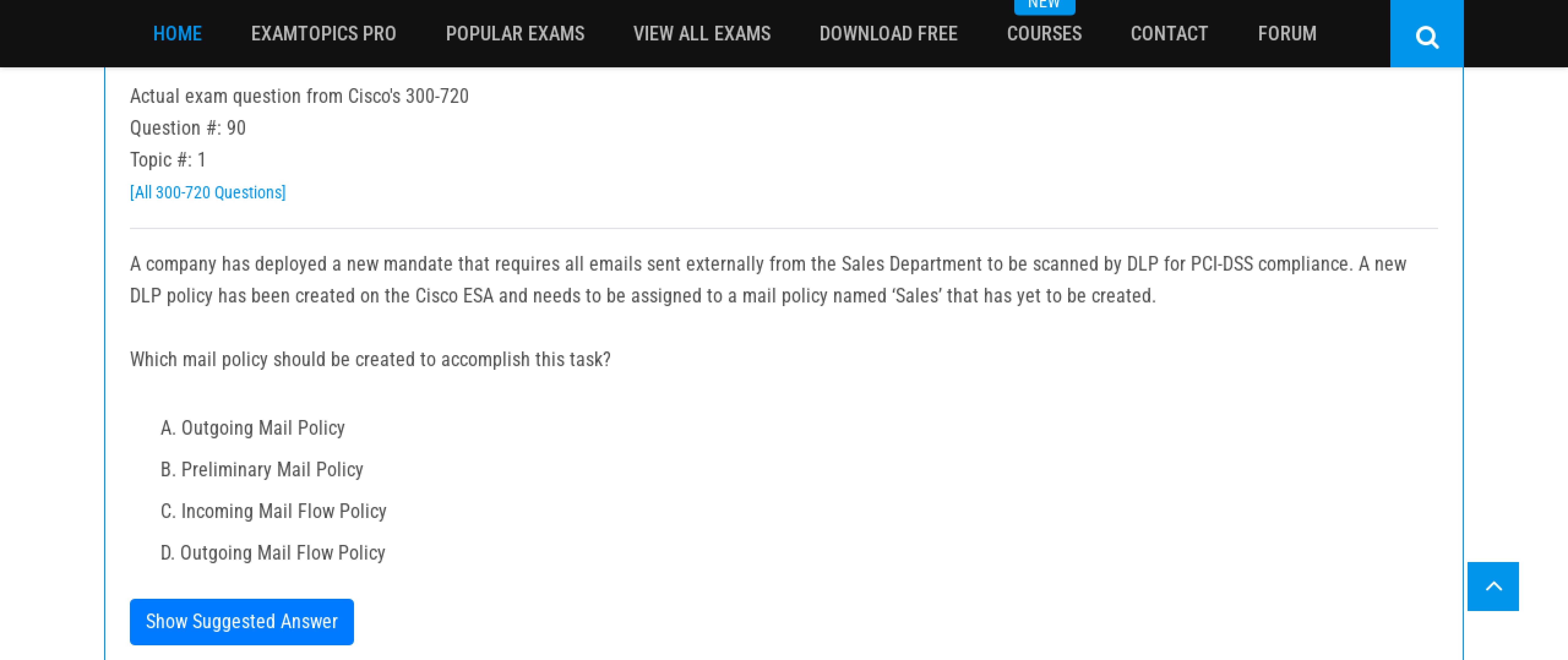
Which additional option should be used to help the end users be aware of the elevated risk of interacting with these messages?

A. Notify Recipient

B. Strip Attachments

C. Notify Sender

D. Modify Subject



Actual exam question from Cisco's 300-720

Question #: 90

Topic #: 1

[All 300-720 Questions]

A company has deployed a new mandate that requires all emails sent externally from the Sales Department to be scanned by DLP for PCI-DSS compliance. A new DLP policy has been created on the Cisco ESA and needs to be assigned to a mail policy named ‘Sales’ that has yet to be created.

Which mail policy should be created to accomplish this task?

A. Outgoing Mail Policy

B. Preliminary Mail Policy

C. Incoming Mail Flow Policy

D. Outgoing Mail Flow Policy

Actual exam question from Cisco's 300-720

Question #: 91

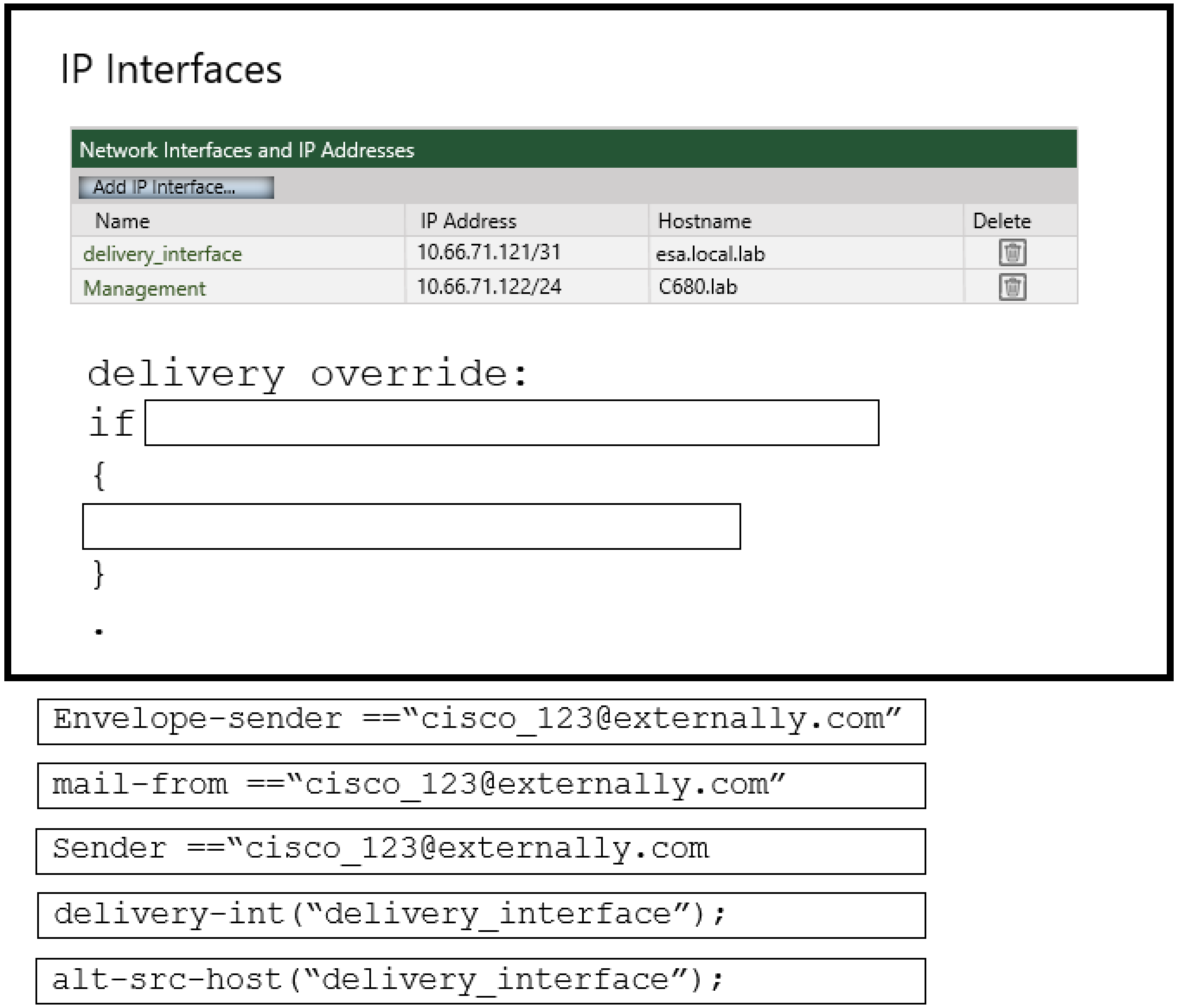
Topic #: 1

[All 300-720 Questions]

DRAG DROP

-

An administrator must ensure that emails sent from cisco_123@externally.com are routed through an alternate virtual gateway. Drag and drop the snippet from the bottom onto the blank in the graphic to finish the message filter syntax. Not all snippets are used.



IP Interfaces

Network Interfaces and IP Addresses

Add IP Interface...

Name	IP Address	Hostname	Delete
delivery_interface	10.66.71.121/31	esa.local.lab	🗑
Management	10.66.71.122/24	C680.lab	🗑

```
delivery override:
 if [                    ]
 {
[                    ]
 }
 .
```

```
Envelope-sender ==“cisco_123@externally.com”
```

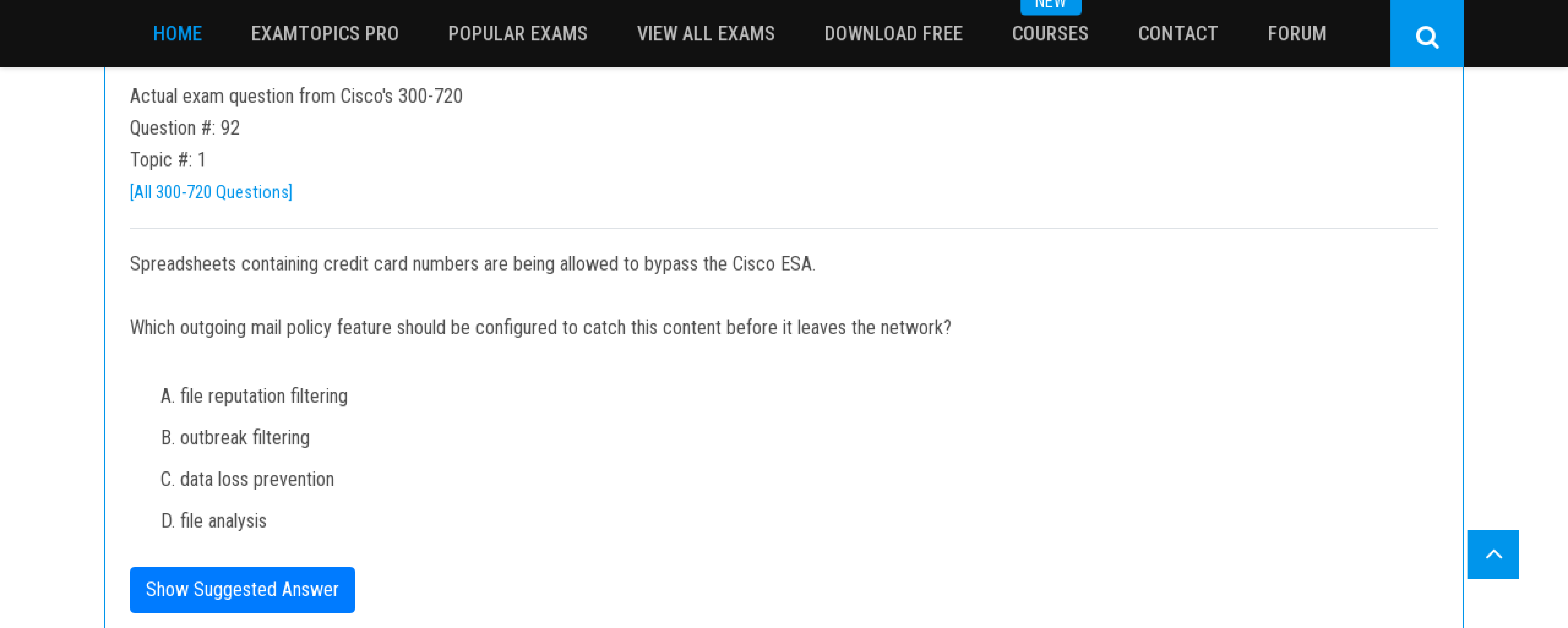
```
mail-from ==“cisco_123@externally.com”
```

```
Sender ==“cisco_123@externally.com
```

```
delivery-int(“delivery_interface”);
```

```
alt-src-host(“delivery_interface”);
```

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 92

Topic #: 1

[All 300-720 Questions]

Spreadsheets containing credit card numbers are being allowed to bypass the Cisco ESA.

Which outgoing mail policy feature should be configured to catch this content before it leaves the network?

A. file reputation filtering

B. outbreak filtering

C. data loss prevention

D. file analysis

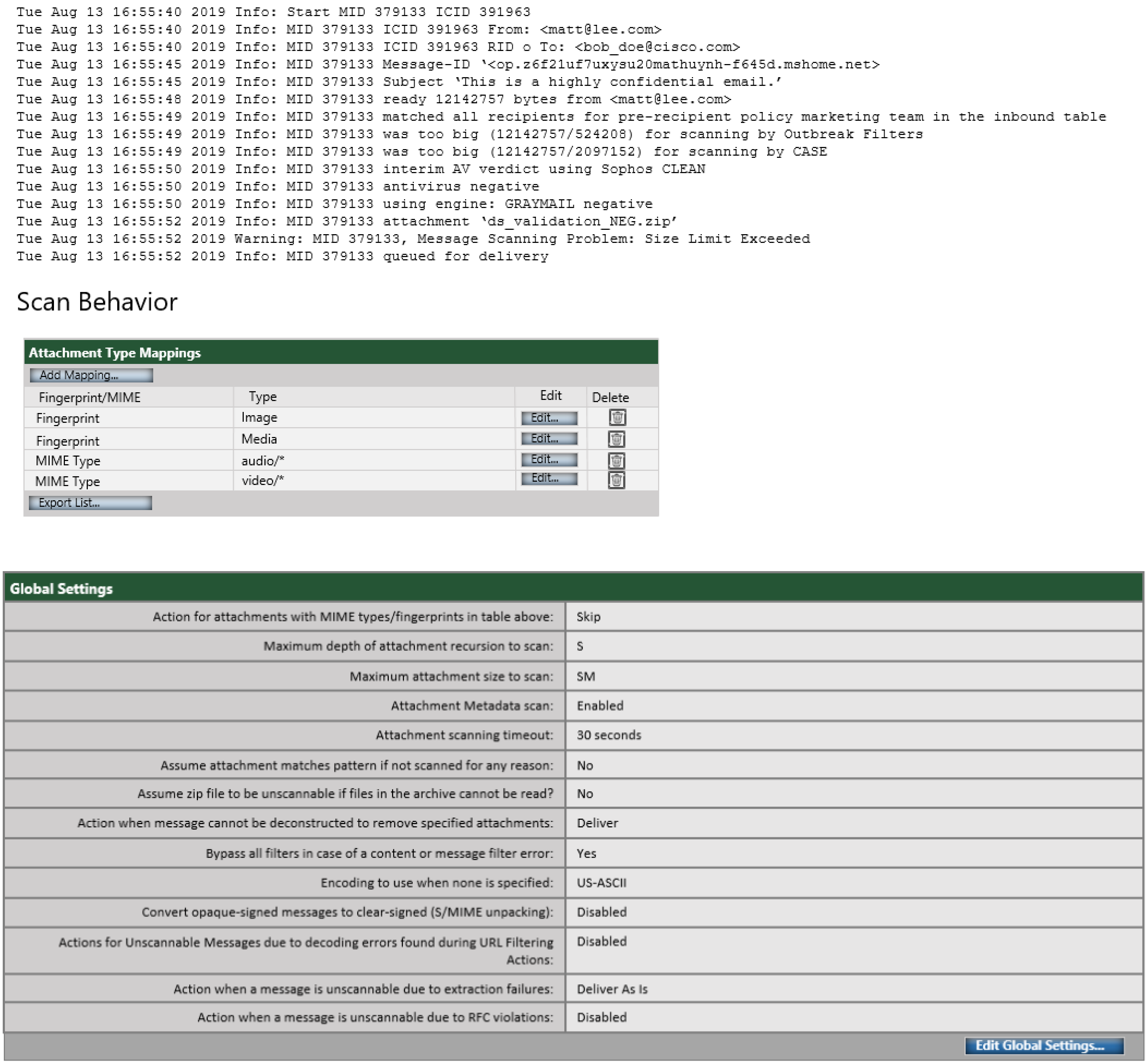
Show Suggested Answer

Actual exam question from Cisco's 300-720

Question #: 93

Topic #: 1

[All 300-720 Questions]



```
Tue Aug 13 16:55:40 2019 Info: Start MID 379133 ICID 391963
Tue Aug 13 16:55:40 2019 Info: MID 379133 ICID 391963 From: <matt@lee.com>
Tue Aug 13 16:55:40 2019 Info: MID 379133 ICID 391963 RID o To: <bob_doe@cisco.com>
Tue Aug 13 16:55:45 2019 Info: MID 379133 Message-ID ‘<op.z6f21uf7uxysu20mathuynh-f645d.mshome.net>
Tue Aug 13 16:55:45 2019 Info: MID 379133 Subject ‘This is a highly confidential email.’
Tue Aug 13 16:55:48 2019 Info: MID 379133 ready 12142757 bytes from <matt@lee.com>
Tue Aug 13 16:55:49 2019 Info: MID 379133 matched all recipients for pre-recipient policy marketing team in the inbound table
Tue Aug 13 16:55:49 2019 Info: MID 379133 was too big (12142757/524208) for scanning by Outbreak Filters
Tue Aug 13 16:55:49 2019 Info: MID 379133 was too big (12142757/2097152) for scanning by CASE
Tue Aug 13 16:55:50 2019 Info: MID 379133 interim AV verdict using Sophos CLEAN
Tue Aug 13 16:55:50 2019 Info: MID 379133 antivirus negative
Tue Aug 13 16:55:50 2019 Info: MID 379133 using engine: GRAYMAIL negative
Tue Aug 13 16:55:52 2019 Info: MID 379133 attachment ‘ds_validation_NEG.zip’
Tue Aug 13 16:55:52 2019 Warning: MID 379133, Message Scanning Problem: Size Limit Exceeded
Tue Aug 13 16:55:52 2019 Info: MID 379133 queued for delivery
```

Scan Behavior

Attachment Type Mappings

Fingerprint/MIME	Type	Edit	Delete
Fingerprint	Image	Edit...	🗑
Fingerprint	Media	Edit...	🗑
MIME Type	audio/*	Edit...	🗑
MIME Type	video/*	Edit...	🗑

Global Settings

Action for attachments with MIME types/fingerprints in table above:	Skip
Maximum depth of attachment recursion to scan:	S
Maximum attachment size to scan:	SM
Attachment Metadata scan:	Enabled
Attachment scanning timeout:	30 seconds
Assume attachment matches pattern if not scanned for any reason:	No
Assume zip file to be unscannable if files in the archive cannot be read?	No
Action when message cannot be deconstructed to remove specified attachments:	Deliver
Bypass all filters in case of a content or message filter error:	Yes
Encoding to use when none is specified:	US-ASCII
Convert opaque-signed messages to clear-signed (S/MIME unpacking):	Disabled
Actions for Unscannable Messages due to decoding errors found during URL Filtering Actions:	Disabled
Action when a message is unscannable due to extraction failures:	Deliver As Is
Action when a message is unscannable due to RFC violations:	Disabled

Refer to the exhibit. Which configuration on the scan behavior must be updated to allow the attachment to be scanned on the Cisco ESA?

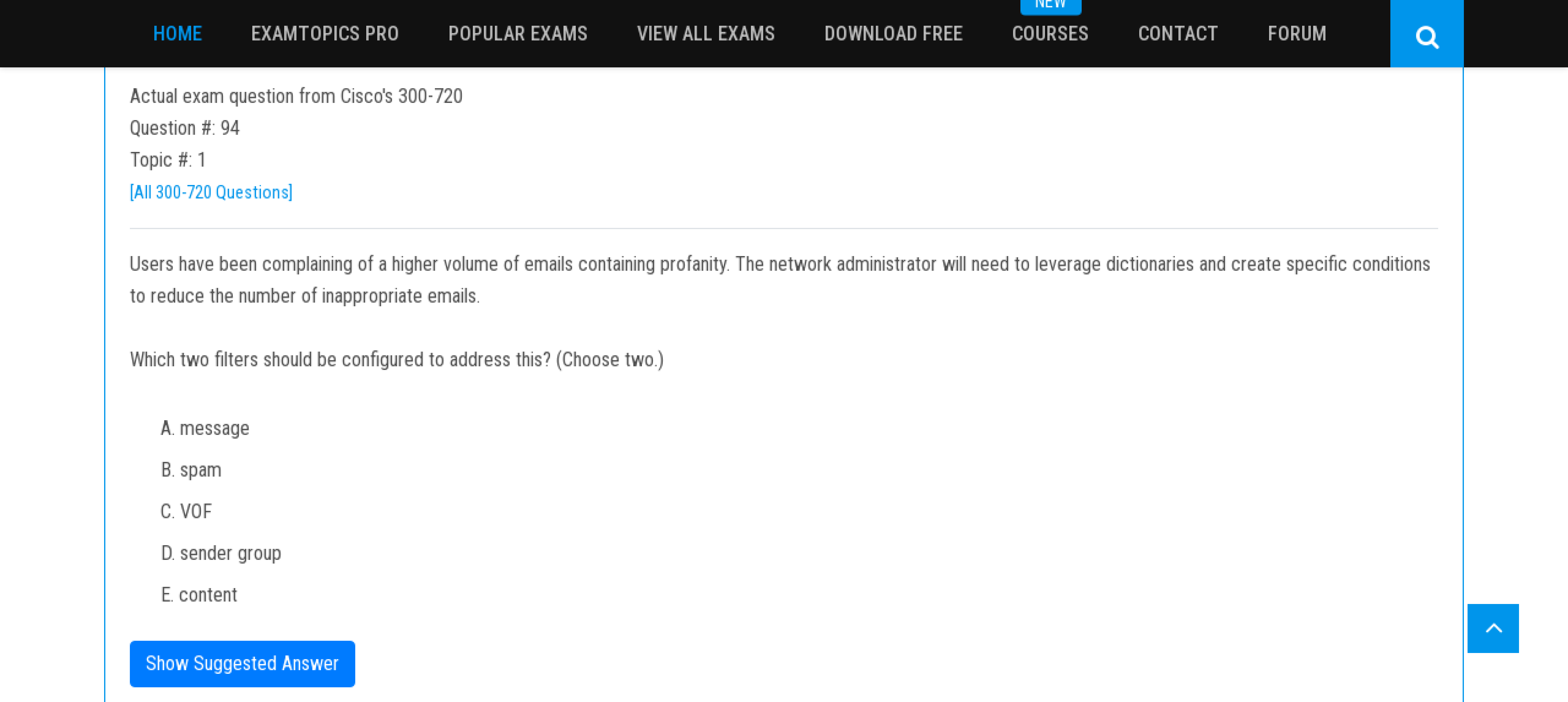
A. Add an additional mapping for attachment type for zip files.

B. Enable assume match pattern if the email was not scanned for any reason.

C. Increase the maximum recursion depth from 5 to a larger value.

D. Increase the maximum attachment size to scan to a larger value.

Show Suggested Answer



Actual exam question from Cisco's 300-720

Question #: 94

Topic #: 1

[All 300-720 Questions]

Users have been complaining of a higher volume of emails containing profanity. The network administrator will need to leverage dictionaries and create specific conditions to reduce the number of inappropriate emails.

Which two filters should be configured to address this? (Choose two.)

A. message

B. spam

C. VOF

D. sender group

E. content