Question #1 *Topic 1*

Which SMTP extension does Cisco ESA support for email security?

A. ETRN

B. UTF8SMTP

C. PIPELINING

D. STARTTLS

Suggested Answer: *D*
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_011000.html

Community vote distribution

D (100%)

XalaGyan 1 month, 2 weeks ago

Selected Answer: D

Correct Answer: STARTTLS

all other options are not related to security and some do not even exists

upvoted 1 times

Certife_dumps5 6 months, 4 weeks ago

Selected Answer: D

D is right answer.

upvoted 1 times

Jereban 11 months, 2 weeks ago

Selected Answer: D

Correct

upvoted 1 times

Jereban 11 months, 2 weeks ago

This dump is still valid ?

upvoted 1 times

GVKD 1 year, 9 months ago

Selected Answer: D

Correct.

AsyncOS supports the STARTTLS extension to SMTP (Secure SMTP over TLS), described in RFC 3207 (which obsoletes RFC 2487).

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_011000.html?bookSearch=true

upvoted 2 times

hakimbenda 1 year, 9 months ago

Correct

upvoted 1 times

Question #2 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

XalaGyan 1 month, 2 weeks ago

Selected Answer: A

Correct Answer: A

SenderBase is the correct feature name on Talos. the others are not features of Talos related to Emails.

upvoted 1 times

Certife_dumps5 6 months, 4 weeks ago

Selected Answer: A

A is correct answer.

upvoted 1 times

GVKD 1 year, 9 months ago

Selected Answer: A

Correct.

SenderBase Reputation Service

The Cisco SenderBase Reputation Service, using global data from the SenderBase Affiliate network, assigns a SenderBase Reputation Score to email senders

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_0101.html?bookSearch=true

upvoted 2 times

Question #3 *Topic 1*

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

Suggested Answer: *C*

Reference:

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

Community vote distribution

C (100%)

Certife_dumps5 6 months, 4 weeks ago

Selected Answer: C

C is correct.

upvoted 1 times

GVKD 1 year, 9 months ago

Selected Answer: C

Correct.

Spam Quarantine End-User Authentication. You can configure your appliance to validate users when they log in to the end-user quarantine.

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_011010.html?bookSearch=true

upvoted 2 times

Question #4 *Topic 1*

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

Suggested Answer: *D*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma11-0/user_guide/b_SMA_Admin_Guide/b_SMA_Admin_Guide_chapter_010101.html

Community vote distribution
D (100%)

XalaGyan 1 month, 2 weeks ago

Selected Answer: D

Correct Answer: D
Spam consolidation over backup. Why would you want to backup spam?
Correct is to consolidate the entire spam emails into one central location for scanning, deleting, treatment etc.
upvoted 1 times

Certife_dumps5 6 months, 4 weeks ago

Selected Answer: D

D is right.
upvoted 1 times

GVKD 1 year, 9 months ago

Selected Answer: D

Correct.

Centralized Policy, Virus, and Outbreak Quarantines
You can centralize policy, virus, and outbreak quarantines on a Security Management appliance. Messages are processed by Email Security appliances but are stored in quarantines on the Security Management appliance.

Centralizing policy, virus, and outbreak quarantines offers the following benefits:

Administrators can manage quarantined messages from multiple Email Security appliances in one location.
Quarantined messages are stored behind the firewall instead of in the DMZ, reducing security risk.
Centralized quarantines can be backed up using the standard backup functionality on the Security Management appliance.

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_0101010.html?bookSearch=true#con_1154400
upvoted 2 times

Question #5 *Topic 1*

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

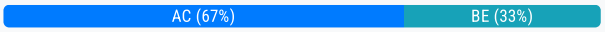
E. Private Keys

Suggested Answer: *AC*

Reference:

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

Community vote distribution



ahmirza 6 months, 4 weeks ago

Selected Answer: AC

The Question is about 'Key Types' and not the Keys Used so correct answer is DKIM and DomainKeys.

DomainKeys: This key type uses public key cryptography to sign emails, allowing the recipient to verify that the email was indeed sent by the domain it claims to be from.

DKIM: Similar to DomainKeys, DKIM also uses public key cryptography but includes additional features for better security and flexibility. It allows the sender to sign the email with a private key, and the recipient can verify the signature using the corresponding public key published in the DNS2.

These key types of help ensure the authenticity and integrity of the emails sent from your domain.

upvoted 1 times

adamx 1 year, 3 months ago

Selected Answer: AC

Correct

upvoted 1 times

ThePope 1 year, 8 months ago

When configuring the ESA under Mail Policy > Sending Profile, the two "Domain Key Type:" are DKIM and Domain Keys

upvoted 3 times

GVKD 1 year, 9 months ago

Selected Answer: BE

B & E are Correct.

With DomainKeys or DKIM email authentication, the sender signs the email using public key cryptography.

Configuring DomainKeys and DKIM Signing

A signing key is the private key stored on the appliance.

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_010101.html?bookSearch=true

upvoted 1 times

GVKD 1 year, 9 months ago

Private and Public keys

upvoted 1 times

iluxa 3 years, 11 months ago

it's DKIM/Domain Keys, asking about the signing profile here specifically.

upvoted 1 times

samismayilov 4 years ago

DomainKeys and DKIM signing works like this: a domain owner generates two keys — a public key stored in the public DNS (a DNS TXT record associated with that domain) and a private key that is stored on the appliance is used to sign mail that is sent (mail that originates) from that domain.

upvoted 1 times

samismayilov 4 years ago

asking which keys, for this needed private and public keys

upvoted 2 times

mkemm 4 years, 1 month ago

answer is correct, when adding domain signing profile options for Domain Key type is DKIM or Domain Keys

upvoted 1 times

geomix7 4 years, 2 months ago

Domain Key/DKIM is the same.

upvoted 2 times

Question #6 *Topic 1*

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

A. reject

B. workqueue

C. action

D. delivery

E. quarantine

Suggested Answer: *BD*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-1/user_guide/b_ESA_Admin_Guide_12_1/b_ESA_Admin_Guide_12_1_chapter_011.pdf
(p.1)

Community vote distribution

BD (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: BD

Correct.

The Email Pipeline is the flow of email as it is processed by the appliance . It has three phases:
• Receipt — Asthe appliance connectsto a remote host to receive incoming email, it adheresto configured limits and other receipt policies. For example, verifying that the host can send your users mail, enforcing incoming connection and message limits, and validating the message's recipient.
• Work Queue — The appliance processes incoming and outgoing mail, performing tasks such as filtering, safelist/blocklist scanning, anti-spam and anti-virus scanning, Outbreak Filters, and quarantining.
• Delivery — As the appliance connects to send outgoing email, it adheres to configured delivery limits and policies.For example, enforcing outbound connection limits and processing undeliverable messages as specified

https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-1/user_guide/b_ESA_Admin_Guide_12_1/b_ESA_Admin_Guide_12_1_chapter_011.pdf

upvoted 4 times

geomix7 3 years, 2 months ago

correct

upvoted 1 times

Question #7 *Topic 1*

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

Suggested Answer: *AD*
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

Community vote distribution

AD (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: AD

Correct.

The two types of actions are:

Final actions — such as deliver , drop , and bounce — end the processing of a message, and permit no further processing through subsequent filters.
Non-final actions perform an action which permits the message to be processed further.

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_1371434

upvoted 3 times

geomix7 3 years, 2 months ago

correct

upvoted 1 times

Question #8 *Topic 1*

Which setting affects the aggressiveness of spam detection?

A. protection level

B. spam threshold

C. spam timeout

D. maximum depth of recursion scan

Suggested Answer: *B*
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118220-technote-esa-00.html

Community vote distribution
B (100%)

hakimbenda 8 months, 3 weeks ago

Selected Answer: B

B - Correct

upvoted 1 times

GVKD 9 months, 2 weeks ago

Selected Answer: B

Correct.

Apply more aggressive spam thresholds if false-positives are less of a concern than missed spam:

Reduce the Positive Spam Threshold to 80 (default is 90) if false-positives are not a concern at the 'certain' threshold.

Reduce Suspected Spam Threshold to 40 (default is 50) if false-positives are not a concern at the 'suspect' threshold.

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118220-technote-esa-00.html

upvoted 2 times

Thusi26 1 year, 8 months ago

B

info

Apply more aggressive spam thresholds if false-positives are less of a concern than missed spam:

Reduce the Positive Spam Threshold to 80 (default is 90) if false-positives are not a concern at the 'certain' threshold.

Reduce Suspected Spam Threshold to 40 (default is 50) if false-positives are not a concern at the 'suspect' threshold.

upvoted 1 times

geomix7 3 years, 2 months ago

correct

upvoted 1 times

Question #9 *Topic 1*

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.

Suggested Answer: *D*

Community vote distribution

D (100%)

ahmirza 6 months, 4 weeks ago

Selected Answer: D

When multilayer antivirus scanning is configured on a Cisco Email Security Appliance (ESA), the order of virus scanning is as follows:

McAfee Engine: This engine scans the message first. If it detects a virus, the message is either dropped or repaired, depending on the configuration.
Sophos Engine: If the McAfee engine determines that the message is virus-free, the Sophos engine then scans the message, adding a second layer of protection.

This sequential scanning ensures that emails are thoroughly checked for viruses, enhancing the overall security of your email system.

upvoted 1 times

WARJ 1 year, 5 months ago

Sophos: The ESA first uses the Sophos antivirus engine. Sophos provides both signature-based and heuristic scanning to detect known and unknown malware.

McAfee: If you've also enabled the McAfee antivirus engine, the ESA will scan the email with McAfee after Sophos. Like Sophos, McAfee also employs signature-based and heuristic techniques to identify threats.

The answer is 'B'

upvoted 1 times

GVKD 1 year, 9 months ago

Selected Answer: D

Correct.

upvoted 2 times

Thusi26 2 years, 9 months ago

You cannot configure the order of virus scanning. When you enable multi-layer anti-virus scanning, the McAfee engine scans for viruses first, and the Sophos engine scans for viruses second.

upvoted 1 times

geomix7 4 years, 2 months ago

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_01011.html

upvoted 1 times

Question #10 *Topic 1*

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

Suggested Answer: *B*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_11-1/b_ESA_Admin_Guide_ces_11_1/b_ESA_Admin_Guide_chapter_011111.pdf

Community vote distribution

D (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: D

D is Correct.

You can allow end users (email users) to manage the safelist and blocklist for their own email accounts. For example, end users may find that emails from specific senders are sent to their spam quarantine when they do not want them to be treated as spam. To ensure that messages from these senders are not quarantined, they may want to add the senders to their safelists.

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_011111.html?bookSearch=true#task_1623646

upvoted 1 times

mkemm 3 years, 1 month ago

correct

upvoted 1 times

Question #11 *Topic 1*

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.

Suggested Answer: *AC*

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

Community vote distribution

AC (100%)

GVKD 8 months, 3 weeks ago

Selected Answer: AC

A and C are Correct.

upvoted 1 times

GVKD 9 months, 3 weeks ago

Correct

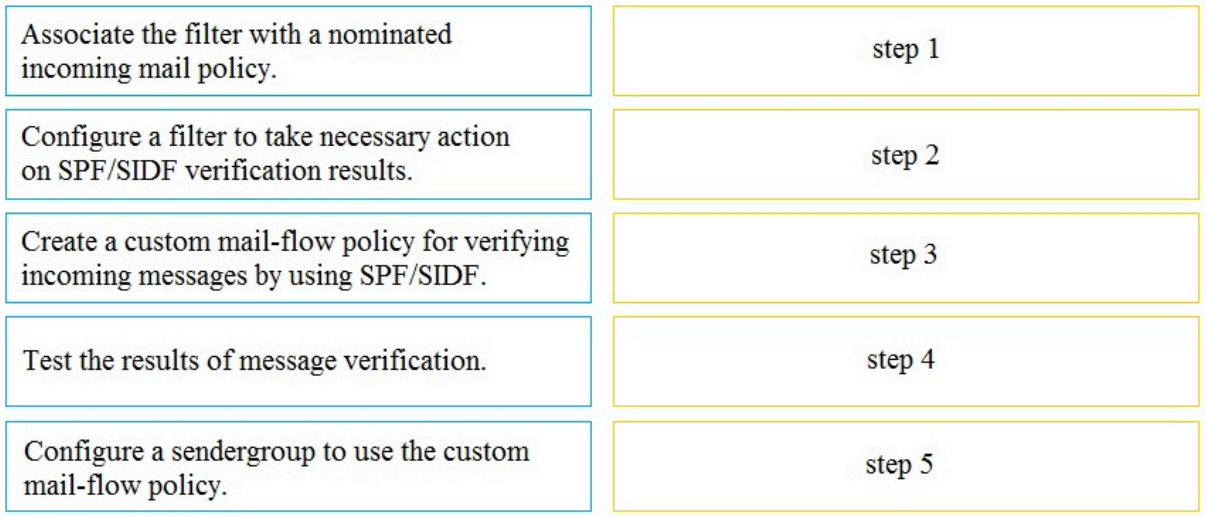
upvoted 1 times

Question #12 *Topic 1*

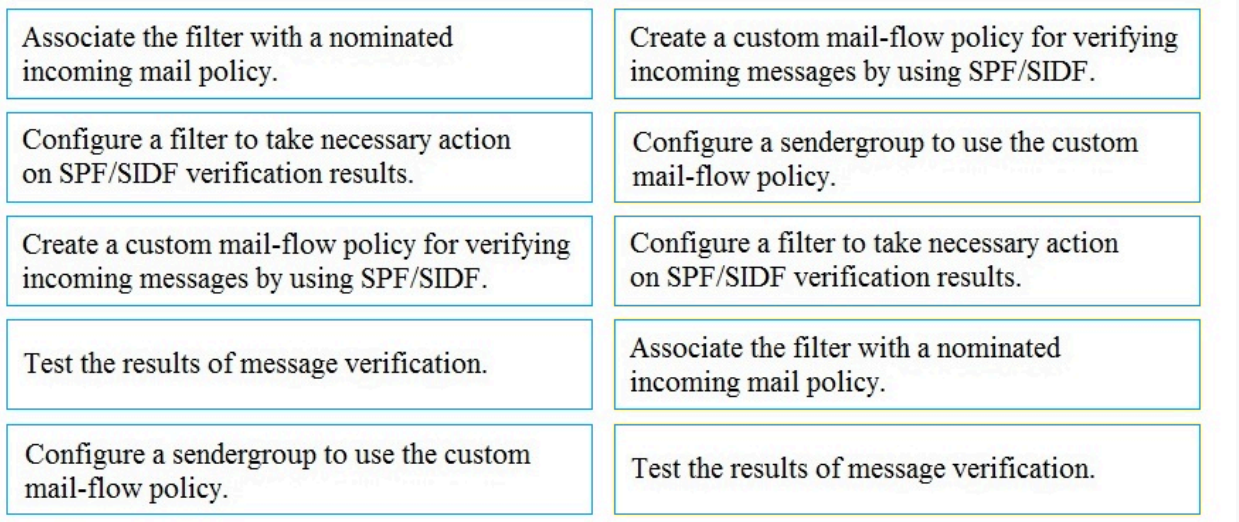
DRAG DROP -

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:



Suggested Answer:



GVKD 3 months, 3 weeks ago

This is correct.

"To enable the SPF for a certain domain, you might need to define a new sender group with a mail flow policy that has SPF enabled; then create filters as mentioned previously."

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117973-faq-esa-00.html

upvoted 1 times

shogun1204 3 months, 4 weeks ago

I dont think this one is right. I think Assoicate the filter and configure a sender group need to be flipped.

upvoted 1 times

Question #13 *Topic 1*

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

Suggested Answer: *A*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma11-5/user_guide/b_SMA_Admin_Guide_11_5/b_SMA_Admin_Guide_11_5_chapter_01010.html

Community vote distribution

A (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: A

Correct.

If you want the Spam Quarantine to use an LDAP query for end-user access, check the “Designate as the active query” check box. If there is an existing active query, it is disabled. When you open the System Administration > LDAP page, an asterisk (*) is displayed next to the active queries.

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_011010.html?bookSearch=true

upvoted 1 times

mkemm 3 years, 1 month ago

To have the quarantine use an LDAP query for end-user access or spam notifications, select the “Designate as the active query” check box. You can designate one end-user authentication query to control quarantine access and one alias consolidation query for spam notifications. Any existing active queries are disabled. On the Security Management appliance, choose Management Appliance > System Administration > LDAP page, an asterisk (*) is displayed next to the active queries.

upvoted 1 times

Question #14 *Topic 1*

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.

Suggested Answer: *D*
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_011111.html

Community vote distribution

D (100%)

GVKD 9 months ago

Selected Answer: D

Correct.
About Deleting Policy Quarantines:

• Before you delete a policy quarantine, see if it is associated with any active filters or message actions.
• You can delete a policy quarantine even if it is assigned to a filter or message action.
• If you delete a quarantine that is not empty, the default action defined in the quarantine will be applied to all messages.
• After you delete the quarantine associated with a filter or message action, any messages subsequently quarantined by that filter or message action will be sent to the Unclassified quarantine. You should customize the default settings of the Unclassified quarantine before you delete quarantines.
• You cannot delete the Unclassified quarantine.

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_011110.pdf

upvoted 1 times

Question #15 *Topic 1*

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

Suggested Answer:

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

Reference:

https://community.cisco.com/t5/email-security/keyword-in-subject-line-to-encrypt-message/td-p/2441383

GVKD 3 months, 3 weeks ago

Correct.

1) Under Mail Policies, Select Outgoing Content Filters

2) Click on Add Filter button. Add a new filter with condition as subject == "Secure:" and Action as Encrypt and Deliver. Click on Submit button.

3) Under Mail Policies, Select Outgoing Mail Policies, and enable this new filter in the default mail policy or appropriate mail policies.

4) Commit changes

https://community.cisco.com/t5/email-security/keyword-in-subject-line-to-encrypt-message/td-p/2441383

upvoted 1 times

Question #16 *Topic 1*

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

Suggested Answer: *A*
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117972-technote-esa-00.html

Community vote distribution
B (100%)

jolenzi Highly Voted 3 years, 2 months ago
Step 1
Click Security Services > Cisco IronPort Email Encryption.

Step 2
Click Enable.

Step 3
(Optional) Click Edit Settings to configure the following options:

The maximum message size to encrypt. Cisco's recommended message size is 10 MB. The maximum message size the appliance will encrypt is 25 MB.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5-1/user_guide/b_ESA_Admin_Guide_13-5-1/b_ESA_Admin_Guide_12_1_chapter_010011.html
upvoted 10 times

samismayilov Highly Voted 3 years ago
B. 25 MB
upvoted 7 times

GVKD Most Recent 9 months, 2 weeks ago
Selected Answer: B
B is Correct.

The maximum message size to encrypt. Cisco's recommended message size is 10 MB. The maximum message size the appliance will encrypt is 25 MB.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5-1/user_guide/b_ESA_Admin_Guide_13-5-1/b_ESA_Admin_Guide_12_1_chapter_010011.html
upvoted 2 times

a7mad150 1 year, 4 months ago
this is what ESA will show if you put more than 25 in Maximum Message Size to Encrypt:

"Value must be from 1 to 25M."
upvoted 2 times

jpapas 1 year, 5 months ago
B.25MB

Enabling Message Encryption on the Email Gateway

Procedure
Step 1

Click Security Services > Cisco IronPort Email Encryption.
Step 2

Click Enable.
Step 3

(Optional) Click Edit Settings to configure the following options:

The maximum message size to encrypt. Cisco's recommended message size is 10 MB. The maximum message size the email gateway will encrypt is 25 MB.

upvoted 2 times

ccnpsise 1 year, 8 months ago

25MB please corect it.

upvoted 2 times

mauritsbeu 2 years, 2 months ago

Selected Answer: B

see comments

upvoted 2 times

romke1981 2 years, 4 months ago

It is indeed 25 MB. Please correct your answer

upvoted 4 times

Question #17 *Topic 1*

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

Suggested Answer: *A*
Reference:
https://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/whitepaper_C11-737596.html

Community vote distribution
B (100%)

jolenzi Highly Voted 3 years, 2 months ago
B is correct.

While creating a content dictionary,

Enter the name of the user and not the email address. For example, enter " Olivia Smith " instead of " olivia.smith@example.com ."
Do not configure Advanced Matching and Smart Identifiers.
Do not choose weight for the terms used.
Do not use regular expressions.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5-1/user_guide/b_ESA_Admin_Guide_13-5-1/b_ESA_Admin_Guide_12_1_chapter_010110.html#con_1260492
upvoted 5 times

GVKD Most Recent 9 months, 2 weeks ago
Selected Answer: B
B is Correct.
Enter the name of the user and not the email address. For example, enter " Olivia Smith " instead of " olivia.smith@example.com ."

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5-1/user_guide/b_ESA_Admin_Guide_13-5-1/b_ESA_Admin_Guide_12_1_chapter_010110.html#con_1260492
upvoted 1 times

jpapas 1 year, 5 months ago
Selected Answer: B
https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5-1/user_guide/b_ESA_Admin_Guide_13-5-1/b_ESA_Admin_Guide_12_1_chapter_010110.html#con_1260492
upvoted 1 times

ccnpsise 1 year, 8 months ago
Why don't Exam topics update the answers? B is correct
upvoted 2 times

jaciro11 2 years, 2 months ago
Answer is B
upvoted 2 times

user636 3 years, 2 months ago
B is correct
upvoted 3 times

Question #18 *Topic 1*

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

Suggested Answer: *A*
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214269-filter-to-handle-messages-that-skipped-d.html

Community vote distribution
D (100%)

jolenzi Highly Voted 3 years, 2 months ago
D is correct, Antispam is disabled in Whitelist policy.
upvoted 6 times

GVKD Most Recent 9 months, 2 weeks ago
Selected Answer: D
D is Correct.
Administrators and end users can use safelists and blocklists to help determine which messages are spam. Safelists specify senders and domains that are never treated as spam. Blocklists specify senders and domains that are always treated as spam.

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_011111.html?bookSearch=true
upvoted 1 times

mipetric93 10 months, 4 weeks ago
D is correct
upvoted 1 times

jpapas 1 year, 5 months ago
Selected Answer: D
(spam) safelist if for antispam
upvoted 1 times

wernervv32 2 years ago
Selected Answer: D
D is the correct answer

https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_11-1/b_ESA_Admin_Guide_ces_11_1/b_ESA_Admin_Guide_chapter_011111.pdf

For example, a message is sent to both recipient A and recipient B.
Recipient A has safelisted the sender, whereas recipient B does not have an entry for the sender in the safelist or the blocklist. In this case, the message may be split into two messages with two message IDs. The message sent to recipient A is marked assafelisted with an X-SLBL-Result-Safelist header and skips anti-spam scanning, whereas the message bound for recipient B is scanned by the anti-spam scanning engine. Both messages then continue along the pipeline (through anti-virus scanning, content policies, and so on) and are subject to any configured settings.
upvoted 2 times

samismayilov 3 years ago
D. antispam scanning
upvoted 4 times

user636 3 years, 2 months ago
D is correct

upvoted 4 times

Question #19 *Topic 1*

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

Suggested Answer: *DE*

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

Community vote distribution

DE (100%)

Terry675 1 month, 1 week ago

Selected Answer: BD

User queries are used to check user credentials.

Group queries are used to check group memberships.

The other options (proxy consolidation, recursive, and routing) are not standard LDAP query types.

upvoted 1 times

GVKD 9 months, 2 weeks ago

Selected Answer: DE

Correct

upvoted 1 times

wernervv32 2 years ago

correct Answer

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118218-configure-esa-00.html

Second, you need to define the query to perform against the LDAP server you have just configured.

Choose the operation you want to perform:

- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure message routing. - MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.

upvoted 1 times

Question #20 *Topic 1*

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

Suggested Answer: *B*
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_011011.html

Community vote distribution

B (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: B

Correct

upvoted 1 times

wernervv32 2 years ago

B answer confirmed
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_011011.html

The certificate-based SMTP authentication profile allows the appliance to authenticate an SMTP connection over TLS using a client certificate. When creating the profile, you select the Certificate Authentication LDAP query to use for verifying the certificate. You can also specify whether the appliance falls back to the SMTP AUTH command to authenticate the user if a client certificate is not available.

upvoted 1 times

Question #21 *Topic 1*

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.

Suggested Answer: *B*
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117863-configure-esa-00.html

Community vote distribution
A (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: A

A is Correct.

If a temporary condition exists that prohibits the encryption of emails in the queue (i.e., temporary C-Series busyness or Cisco Secure Email Encryption Service unavailability), messages are re-queued and retried at a later time.

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_010010.html?bookSearch=true

upvoted 1 times

jpapas 1 year, 5 months ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5-1/user_guide/b_ESA_Admin_Guide_13-5-1/b_ESA_Admin_Guide_12_1_chapter_010011.html

upvoted 1 times

robcamac 2 years, 2 months ago

A is the right answer

upvoted 1 times

jolenzi 3 years, 2 months ago

A is correct.

"If a temporary condition exists that prohibits the encryption of emails in the queue (i.e., temporary C-Series busyness or CRES unavailability), messages are re-queued and retried at a later time."

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5-1/user_guide/b_ESA_Admin_Guide_13-5-1/b_ESA_Admin_Guide_12_1_chapter_010011.html

upvoted 3 times

user636 3 years, 2 months ago

A is correct.

upvoted 2 times

Question #22 *Topic 1*

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

Suggested Answer: *CD*

Community vote distribution

BD (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: BD

B and D are Correct.

upvoted 3 times

a7mad150 1 year, 4 months ago

B and D , this is what can be done on HAT

upvoted 1 times

jpapas 1 year, 5 months ago

Selected Answer: BD

this is HAT senders : geoblocking and senderbase reputation score from talos IPs.

upvoted 2 times

user636 3 years, 2 months ago

B,D are correct answers.

upvoted 3 times

MarcioSantos51 2 years, 7 months ago

Yes, PAGE 3

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_00.pdf

upvoted 1 times

Question #23 *Topic 1*

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.

Suggested Answer: *AB*

Reference:

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

Community vote distribution

BE (100%)

user636 Highly Voted 3 years, 2 months ago

B,E are correct

upvoted 8 times

GVKD Most Recent 9 months, 2 weeks ago

Selected Answer: BE

B & E are Correct

upvoted 2 times

jpapas 1 year, 5 months ago

Selected Answer: BE

BE, Always friendly names not specific address

upvoted 1 times

robcamac 2 years, 2 months ago

B and E dudes

upvoted 3 times

samismayilov 3 years ago

B,E are correct

upvoted 4 times

iluxa 3 years ago

Just to clarify, in the forged email detection dictionary, we use names of executives and not email addresses correct? for example John Smith , and not JohnSmith@mycompany.com

upvoted 3 times

jolenzi 3 years, 2 months ago

B & E are correct.

upvoted 4 times

geomix7 3 years, 2 months ago

E because check for dispaly names and not for email addresses as answer A

upvoted 2 times

Question #24 *Topic 1*

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

A. preferred-verify

B. off

C. preferred

D. required

Suggested Answer: *B*

Reference:

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118954-config-esa-00.html

Community vote distribution

B (100%)

adamx 3 months, 3 weeks ago

Selected Answer: B

Correct

upvoted 1 times

freemen810 5 months, 1 week ago

c. preferred

upvoted 1 times

GVKD 9 months, 3 weeks ago

Correct

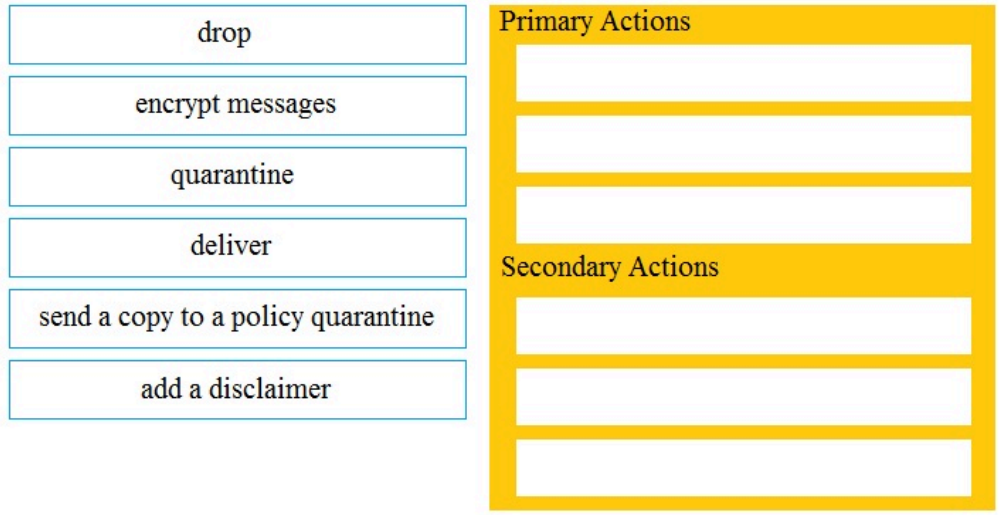
upvoted 1 times

Question #25 *Topic 1*

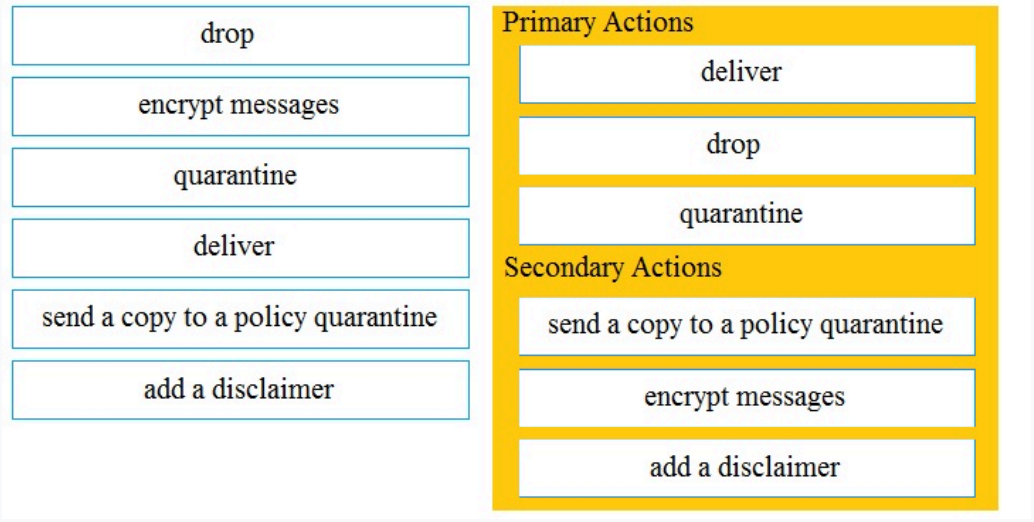
DRAG DROP -

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:



Suggested Answer:



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_010001.html
(message
actions)

GVKD 3 months, 3 weeks ago

Correct

upvoted 1 times

Question #26 *Topic 1*

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

Suggested Answer: *AD*
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

Community vote distribution

AD (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: AD

Correct.

If you store user information within LDAP directories in your network infrastructure you can configure the appliance to query your LDAP servers to accept, route, and authenticate messages.

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

upvoted 1 times

samismayilov 3 years ago

Correct.
When you configure your appliance to work with an LDAP directory, you must complete the following steps to configure your AsyncOS appliance for acceptance, routing, aliasing, and masquerading:

upvoted 1 times

Question #27 *Topic 1*

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.

Suggested Answer: *AD*

Reference:

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213940-esa-using-a-message-filter-to-take-act.html

Community vote distribution

AD (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: AD

Correct

upvoted 2 times

GVKD 9 months, 3 weeks ago

Correct.

Message filters can only be applied to the ESA via command line. So, you will need command line access to the ESA.

Log into the ESA via command line.
Run the following highlighted commands to apply the message filter to the ESA:
ironport.example.com> filters

Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> NEW

Enter filter script. Enter '.' on its own line to end.
large_spam_no_attachment:
if ((body-size > 2097152) AND NOT (attachment-size > 0)) {
quarantine("large_spam");
log-entry("*****This is a large message with no attachments*****");
}
.
1 filters added.

upvoted 1 times

Question #28 *Topic 1*

What occurs when configuring separate incoming mail policies?

A. message splintering

B. message exceptions

C. message detachment

D. message aggregation

Suggested Answer: *A*

Community vote distribution

A (100%)

GVKD 9 months ago

Selected Answer: A

Correct

upvoted 2 times

GVKD 9 months, 3 weeks ago

Correct

upvoted 1 times

Question #29 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

GVKD 9 months, 3 weeks ago

Selected Answer: B

Correct.

Spam Quarantine Alias Consolidation Queries
If you use spam notifications, the spam quarantine alias consolidation query consolidates the email aliases so that recipients do not receive quarantine alias.

https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide/b_ESA_Admin_Guide_ces_11_0/b_ESA_Admin_Guide_chapter_011010.htr

upvoted 2 times

Question #30 *Topic 1*

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

Suggested Answer: *AE*

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_01000.html

Community vote distribution

AE (100%)

GVKD 9 months, 3 weeks ago

Selected Answer: AE

Correct.

upvoted 3 times

Question #31 *Topic 1*

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.

Suggested Answer: *D*

Reference:

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

Community vote distribution

D (100%)

GVKD 9 months, 3 weeks ago

Selected Answer: D

Correct.

Secure unsubscribe option for end users. Mimicking an unsubscribe option is a popular phishing technique. For this reason, the end users are generally wary of clicking unknown unsubscribe links. For such scenarios, the cloud-based Unsubscribe Service extracts the original unsubscribe URI, checks the reputation of the URI, and then performs the unsubscribe process on behalf of the end user. This protects end users from malicious threats masquerading as unsubscribe links.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-2-1/User_Guide/b_ESA_Admin_Guide_14-2-1/b_ESA_Admin_Guide_12_1_chapter_01110.html#id_101033

upvoted 2 times

Question #32 *Topic 1*

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.

Suggested Answer: *B*
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

Community vote distribution
D (100%)

GVKD 9 months, 3 weeks ago

Selected Answer: D

D is Correct:

Users requiring more power and flexibility in mapping messages to particular Virtual Gateways should investigate the use of message filters.

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_011001.html

upvoted 2 times

Dagio78 11 months ago

Answer B

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_011001.html

The altsrchost command provides the simplest and most straightforward method to segment each appliance into multiple IP interfaces (Virtual Gateway addresses) from which to deliver email. However, users requiring more power and flexibility in mapping messages to particular Virtual Gateways should investigate the use of message filters. See Using Message Filters to Enforce Email Policiesfor more information.

upvoted 1 times

Dagio78 11 months ago

Answer D not B

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_011001.html

The altsrchost command provides the simplest and most straightforward method to segment each appliance into multiple IP interfaces (Virtual Gateway addresses) from which to deliver email. However, users requiring more power and flexibility in mapping messages to particular Virtual Gateways should investigate the use of message filters. See Using Message Filters to Enforce Email Policiesfor more information.

upvoted 1 times

Dagio78 11 months ago

Delete this message please

upvoted 1 times

networkexpert 1 year, 10 months ago

D is correct answer:

Using message filters, you can set up specific filters to deliver flagged messages using a specific host IP interface (Virtual Gateway address) or interface group. See Alter Source Host (Virtual Gateway address) Action. (This method is more flexible and powerful than the one above.)

upvoted 1 times

robcamac 2 years, 2 months ago

Option D is correct. Check admin guide

upvoted 2 times

jolenzi 3 years, 2 months ago

Correct.

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118132-configure-esa-00.html

upvoted 2 times

Question #33 *Topic 1*

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.

Suggested Answer: *D*
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118026-technote-esa-00.html

Community vote distribution
D (100%)

GVKD 9 months, 3 weeks ago

Selected Answer: D

Correct

Scenario 5
The PVO cannot be enabled and shows this type of error message.

Unable to proceed with Centralized Policy, Virus and Outbreak Quarantines
configuration as host1 and host2 in Cluster have content filters / DLP actions
available at a level different from the cluster Level.
The error message can indicate that one of the hosts does not have a DLP feature key applied and DLP is disabled. The solution is to add the missing feature key and apply DLP settings identical as on the host that has the feature key applied. This feature key inconsistency might have the same effect with Outbreak Filters, Sophos Antivirus, and other feature keys.

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118026-technote-esa-00.html

upvoted 2 times

a7mad150 1 year, 4 months ago

A. %100

upvoted 1 times

samismayilov 3 years ago

D. DLP is not configured on host1.
Scenario 5
The PVO cannot be enabled and shows this type of error message.

Unable to proceed with Centralized Policy, Virus and Outbreak Quarantines
configuration as host1 and host2 in Cluster have content filters / DLP actions
available at a level different from the cluster Level.
The error message can indicate that one of the hosts does not have a DLP feature key applied and DLP is disabled. The solution is to add the missing feature key and apply DLP settings identical as on the host that has the feature key applied. This feature key inconsistency might have the same effect with Outbreak Filters, Sophos Antivirus, and other feature keys.
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118026-technote-esa-00.html

upvoted 1 times

geomix7 3 years, 2 months ago

A is correct

upvoted 1 times

Question #34 *Topic 1*

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

Suggested Answer: *B*
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_01110.html

Community vote distribution

B (100%)

GVKD 9 months, 3 weeks ago

Selected Answer: B

Correct

upvoted 2 times

samismayilov 3 years ago

Your appliance needs a feature key for Anti-Spam or Intelligent Multi-Scan in order for Outbreak Filters to scan for non-viral threats.

upvoted 1 times

jolenzi 3 years, 2 months ago

Correct.

"By default, the Outbreak Filters feature scans your incoming and outgoing messages for possible viruses during an outbreak. You can enable scanning for non-viral threats in addition to virus outbreaks if you enable anti-spam scanning on the appliance."

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_01110.html

upvoted 2 times

Question #35 *Topic 1*

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

Suggested Answer: *B*

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_010000.html#con_1809885

Community vote distribution

B (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: B

Correct.

upvoted 2 times

Question #36 *Topic 1*

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

Suggested Answer: *C*

Reference:

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

Community vote distribution

C (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: C

Correct.

upvoted 2 times

Question #37 *Topic 1*

Which attack is mitigated by using Bounce Verification?

A. spoof

B. denial of service

C. eavesdropping

D. smurf

Suggested Answer: *B*

Reference:

https://www.networkworld.com/article/2305394/ironport-adds-bounce-back-verification-for-e-mail.html

Community vote distribution

B (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: B

Correct.

upvoted 2 times

Question #38 *Topic 1*

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

Suggested Answer: *AD*
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_01110.html

Community vote distribution

AD (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: AD

Correct.

The Outbreak Filters feature uses three tactics to protect your users from outbreaks:
Delay.
Redirect.
Modify.

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_01110.html

upvoted 2 times

samismayilov 3 years ago

Correct

upvoted 1 times

mkemm 3 years, 1 month ago

The Outbreak Filters feature uses three tactics to protect your users from outbreaks:

Delay. Outbreak Filters quarantines messages that may be part of a virus outbreak or non-viral attack. While quarantined, the appliances receives updated outbreak information and rescans the message to confirm whether it's part of an attack.
Redirect. Outbreak Filters rewrites the URLs in non-viral attack messages to redirect the recipient through the Cisco web security proxy if they attempt to access any of the linked websites. The proxy displays a splash screen that warns the user that the website may contain malware, if the website is still operational, or displays an error message if the website has been taken offline. See Redirecting URLs for more information on redirecting URLs.
Modify. In addition to rewriting URLs in non-viral threat messages, Outbreak Filters can modify a message's subject and add a disclaimer above the message body to warn users about the message's content. See Modifying Messages for more information.

upvoted 1 times

Question #39 *Topic 1*

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

Suggested Answer: *CE*
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_01001.html

Community vote distribution

CE (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: CE

Correct.

Features that you want the appliance to use for incoming or outgoing messages.

Anti-Virus
File Reputation Filtering and File Analysis (incoming messages only)
Anti-Spam
Graymail Detection and Safe Unsubscribe
Outbreak Filters
Data Loss Prevention (outgoing messages only)
Content Filters

upvoted 2 times

Question #40 *Topic 1*

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

Suggested Answer: *B*
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_010010.html

Community vote distribution
A (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: A
A is the correct answer.

AsyncOS supports using encryption to secure inbound and outbound email. To use this feature, you create an encryption profile that specifies characteristics of the encrypted message and connectivity information for the key server.

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_010010.html
upvoted 2 times

mkemm 3 years ago
https://www.cisco.com/c/dam/en/us/products/collateral/security/esa-cres-encryption.pdf, so it is answer A
upvoted 2 times

user636 3 years, 2 months ago
A is correct
upvoted 3 times

Question #41 *Topic 1*

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

Suggested Answer: *AD*

You can enter multiple host names to configure the LDAP servers for failover or load-balancing. Separate multiple entries with commas.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/sma_user_guide/b_SMA_Admin_Guide_ces_11/b_SMA_Admin_Guide_chapter_01010.html

Community vote distribution

AD (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: AD

Correct.

You can use multiple LDAP servers to achieve the following results:

Failover. When you configure the LDAP profile for failover, the appliance fails over to the next LDAP server in the list if it cannot connect to the first LDAP server.

Load Balancing. When you configure the LDAP profile for load balancing, the appliance distributes connections across the list of LDAP servers when it performs LDAP queries.

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#con_1216413

upvoted 2 times

iluxa 3 years ago

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#con_1216413 , correct

upvoted 1 times

Question #42 *Topic 1*

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

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

Community vote distribution
C (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: C
Correct.

Point the ESA to the IP address of your SMA and specify the port you would like to use. The default is Port 6025.

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118692-configure-esa-00.html
upvoted 1 times

Question #43 *Topic 1*

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

Suggested Answer:

AsyncOS performs DMARC verification on the message.	A listener configured on AsyncOS receives an SMTP connection.
A listener configured on AsyncOS receives an SMTP connection.	AsyncOS performs SPF and DKIM verification on the message.
AsyncOS performs SPF and DKIM verification on the message.	AsyncOS fetches the DMARC record for the sender domain from the DNS.
AsyncOS fetches the DMARC record for the sender domain from the DNS.	AsyncOS performs DMARC verification 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_11_1_chapter_010101.html

GVKD 9 months, 2 weeks ago

Correct.

The following describes how AsyncOS performs DMARC verification.

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

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_010101.html

upvoted 2 times

Question #44 *Topic 1*

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.

Suggested Answer: *AB*

Reference:

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118555-qa-esa-00.html

(configuration summary)

Community vote distribution

AB (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: AB

Correct.

Configuration Summary:

1) Enable centralized quarantine on the ESA appliance(s):GUI > Security Services > Spam Quarantine >Check Enable External Spam Quarantine

2) Disable the local quarantine(s):GUI > Monitor > Spam Quarantine> Uncheck Enable Spam Quarantine

3) Submit and Commit Changes.

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118555-qa-esa-00.html

upvoted 1 times

iluxa 3 years ago

Configuration Summary

Enable centralized quarantine on the ESA appliance(s):GUI > Security Services > Spam Quarantine >Check Enable External Spam Quarantine

Disable the local quarantine(s):GUI > Monitor > Spam Quarantine> Uncheck Enable Spam Quarantine

Submit and Commit Changes.

Optionally migrate quarantine messages from local to central quarantine via the process below.

upvoted 1 times

Question #45 *Topic 1*

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

A. antivirus

B. DLP

C. Outbreak Filters

D. AMP

Suggested Answer: *B*
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_01001.html

Community vote distribution

B (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: B

Correct.

Features that you want the appliance to use for incoming or outgoing messages.

Anti-Virus
File Reputation Filtering and File Analysis (incoming messages only)
Anti-Spam
Graymail Detection and Safe Unsubscribe
Outbreak Filters
Data Loss Prevention (outgoing messages only)
Content Filters

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_01001.html

upvoted 2 times

Question #46 *Topic 1*

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.

Suggested Answer: *BC*
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_010001.html

Community vote distribution

GVKD 9 months, 2 weeks ago

Selected Answer: BC

Correct.

Step 1
Enable the DLP feature.

Step 2
Define the possible actions that can be taken for messages in which violations are found or suspected.

Step 3
Create DLP policies.

Step 4
Set the order of the DLP policies.

Step 5
Ensure that you have created Outgoing Mail Policies for each group of senders and recipients whose messages will be scanned for DLP violations.

Step 6
Specify which DLP policies apply to which senders and recipients by assigning DLP policies to Outgoing Mail Policies.

Step 7
Configure settings for storage of and access to sensitive DLP information.

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_010001.html
upvoted 2 times

Question #47 *Topic 1*

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

A. default

B. system

C. user

D. custom

E. demo

Suggested Answer: *BD*
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

Community vote distribution
BD (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: BD

Correct.

Managing Lists of Certificate Authorities
The appliance uses stored trusted certificate authorities that it uses to verify a certificate from a remote domain to establish the domain's credentials. You can configure the appliance to use the following trusted certificate authorities:

Pre-installed list. The appliance has a pre-installed list of trusted certificate authorities. This is called the system list.
User-defined list. You can customize a list of trusted certificate authorities and then import the list onto the appliance.

You can use either the system list or the customized list, and you can also use both lists to verify certificate from a remote domain.

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_011000.html?bookSearch=true

upvoted 1 times

patataatomica 1 year, 4 months ago

Correct.

Networks> Certificates > Edit Certificate Authorities.

You chan choose between Custom List and System List.

upvoted 1 times

MarcioSantos51 2 years, 7 months ago

The appliance uses stored trusted certificate authorities that it uses to verify a certificate from a remote domain to establish the domain's credentials. You can configure the appliance to use the following trusted certificate authorities:

Pre-installed list. The appliance has a pre-installed list of trusted certificate authorities. This is called the system list.
User-defined list. You can customize a list of trusted certificate authorities and then import the list onto the appliance .

upvoted 2 times

Question #48 *Topic 1*

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

Suggested Answer: *AE*

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_010101.html#task_1231917

Community vote distribution

AE (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: AE

Correct.

upvoted 2 times

MarcioSantos51 2 years, 7 months ago

A DMARC verification profile consists of the following information:

A name for the verification profile.
Message action to take when the policy in the DMARC record is reject.
Message action to take when the policy in the DMARC record is quarantine.
Message action in case of a temporary failure.
Message action in case of a permanent failure.

correct

upvoted 2 times

Question #49 *Topic 1*

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

Suggested Answer: *AD*
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_01101.pdf
(p.2)

Community vote distribution

AD (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: AD

Correct.

upvoted 2 times

samismayilov 3 years ago

The graymail management solution in the appliance comprises of two components: an integrated graymail scanning engine and a cloud-based Unsubscribe Service.

upvoted 1 times

mkemm 3 years, 1 month ago

read carefully, but the answer is correct :)

upvoted 1 times

Question #50 *Topic 1*

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

Suggested Answer: *C*
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote-esa-00.html
(note under enable url filtering)

Community vote distribution

C (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: C

Correct.

Enabling Logging of URLs and Message Tracking Details for URLs
Logging of URL-related logs, and display of this information in Message Tracking details, is disabled by default. This includes the logs for the following events:

Category of any URL in the message matches the URL category filters
Reputation score of any URL in the message matches URL reputation filters
Outbreak Filter rewrites any URL in the message
To enable logging of these events, use the outbreakconfig command in the command-line interface (CLI).

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_01110.html?bookSearch=true

upvoted 2 times

Question #51 *Topic 1*

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

A. 83

B. 82

C. 443

D. 80

Suggested Answer: *A*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_11-1/b_ESA_Admin_Guide_ces_11_1/b_ESA_Admin_Guide_chapter_011111.pdf

Community vote distribution
A (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: A
Correct.

In the Spam Quarantine section, configure settings for access to the spam quarantine:

By default, HTTP uses port 82 and HTTPS uses port 83.

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_011111.html?bookSearch=true
upvoted 3 times

ccnpsise 1 year, 8 months ago
In the Spam Quarantine section, configure settings for access to the spam quarantine:

By default, HTTP uses port 82 and HTTPS uses port 83. Correct Answer is 83
upvoted 1 times

jaciro11 2 years, 2 months ago

Selected Answer: A
Its 83, 82 for http
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118692-configure-esa-00.pdf
upvoted 1 times

iluxa 3 years ago
A is correct : 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#task_1537411
upvoted 3 times

marionexpress 3 years, 1 month ago
Correct Answer is C
https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/hardware/x90_series/C690_QSG.pdf
upvoted 1 times

KoXiro 2 years, 4 months ago
It is 83
upvoted 1 times

Question #52 *Topic 1*

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

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

Community vote distribution

GVKD 9 months, 2 weeks ago

Selected Answer: C

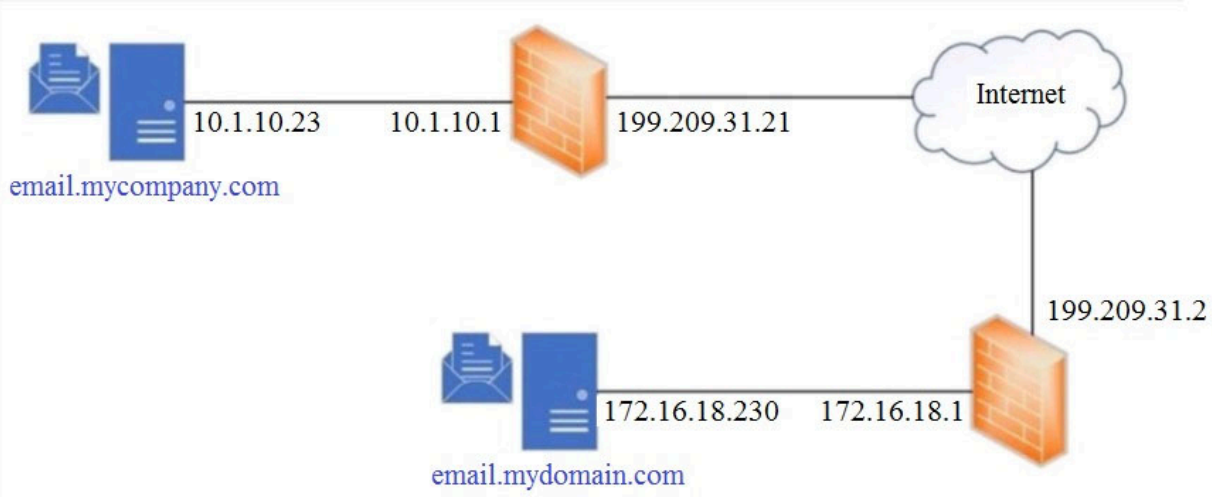
Correct.

The appliance uses the reputation and category of links in messages and other spam-identification algorithms to help identify spam. For example, if a link in a message belongs to a marketing website, the message is more likely to be a marketing message.

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

upvoted 2 times

Question #53 *Topic 1*



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

Suggested Answer: *C*

Community vote distribution

C (75%) B (25%)

GVKD 9 months, 2 weeks ago

Selected Answer: C

Correct.

upvoted 3 times

jaciro11 2 years, 2 months ago

Answer C

NAT in firewall internet interface.

upvoted 1 times

gospodinov 2 years, 4 months ago

Selected Answer: B

B is correct

upvoted 1 times

jaciro11 2 years, 2 months ago

Man this is an Ip behind the firewall tell me how the people will reach that IP from Internet...

So your answer is wrong.

Its needed to create a NAT from firewall IP nearly to internet.

Answer C

upvoted 1 times

Question #54 *Topic 1*

What is a valid content filter action?

A. decrypt on delivery

B. quarantine

C. skip antispam

D. archive

Suggested Answer: *B*
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_01010.html#con_1158022

Community vote distribution
B (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: B
Correct.

Content Filter Actions:

Quarantine
Encrypt on Delivery
Strip Attachment by Content
Strip Attachment by File Info
Strip Attachment with Macro
Drops all macro-enabled attachments of the specified file type.
URL Reputation
URL Category
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Bypass DKIM Signing
Send Copy (Bcc:)
Notify
Change Recipient to
Send to Alternate Destination Host
Strip Header
Add/Edit Header
Forged Email Detection
Add Message Tag
Add Log Entry
S/MIME Sign/Encrypt on Delivery
Encrypt and Deliver Now (Final Action)
S/MIME Sign/Encrypt (Final Action)
Bounce (Final Action)
Skip Remaining Content Filters (Final Action)
Drop (Final Action)

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_01010.html?bookSearch=true#con_1158022
upvoted 1 times

Question #55 *Topic 1*

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

Suggested Answer: *AB*

Reference:

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118542-qa-esa-00.html

Community vote distribution

AB (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: AB

Correct.

The Virtual Gateway technology enables users to separate the Cisco Email Security Appliance into multiple Virtual Gateway addresses, from which to send and receive emails. Each Virtual Gateway address is given a distinct IP address, hostname and domain, and email queue.

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118542-qa-esa-00.html

upvoted 2 times

Question #56 *Topic 1*

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

Suggested Answer: *C*
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_01011.html

Community vote distribution

C (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: C

Correct.

Configure a timeout value for the system to stop performing anti-virus scanning on a message. The default value is 60 seconds.

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_01011.html

upvoted 2 times

Question #57 *Topic 1*

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

Suggested Answer: *B*
Reference:
https://community.cisco.com/t5/email-security/cisco-ironport-esa-security-services-scan-behavior-impact-on-av/td-p/3923243

Community vote distribution
B (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: B

Correct.

1) Click Security Services > Scan Behavior.

2) Define the attachment type mapping.

3) Configure the global settings.

4) Edit the required fields:

Action for attachments with MIME types
Maximum depth of attachment recursion to scan
Maximum attachment size to scan
Attachment Metadata scan
Attachment scanning timeout
etc...

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?bookSearch=true

upvoted 2 times

Question #58 *Topic 1*

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.

Suggested Answer: *C*
Reference:
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117922-technote-esa-00.html

Community vote distribution
C (100%)

GVKD 9 months ago

Selected Answer: C
C is Correct.

In order to see or modify the SLBL, and administrator would need to do one of the following:

1) log into the EUQ using their admin account and password
-Choose Safelist or Blocklist from the Options drop-down menu in the upper right
-Find and modify the Senders/Senders List for the Recipient Address, as needed
2) export the SLBL to a .csv file
-System Administration > Configuration File and choose Backup/Backup Now
-The file is saved on the appliance and will need exported via FTP, or other file retrieval method from the appliance.
-The file is saved to the configuration directory, and indicated by the file name saved as. i.e., slbl-564D6C9B806B5719XXXX-57284F5DYYYY-20160203T141646.csv
-Looking at the SLBL .csv file.

https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200343-How-to-modify-the-End-User-Safelist-Bloc.html
upvoted 2 times

Question #59 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

A (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: A

A is Correct.

Sending Message to Policy Quarantine:

When flagged for quarantine, the message that is not scanned by the Content Scanner continues through the rest of the email pipeline. When the message reaches the end of the pipeline, if the message has been flagged for one or more quarantines then it enters those queues. Note that if the message does not reach the end of the pipeline, it is not placed in a quarantine.

For example, a content filter can cause a message to be dropped or bounced, in which case the message will not be quarantined.

Note:
If a policy quarantine is not defined in your appliance , you cannot sent the message to the quarantine.

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_01000.html?bookSearch=true#con_1371434

upvoted 2 times

pepgua 2 years, 5 months ago

A seems correct to me..
Note under - Sending Message to Policy Quarantine
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_01000.html?bookSearch=true

upvoted 1 times

geomix7 3 years, 2 months ago

any reference?

upvoted 1 times

Question #60 *Topic 1*

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

A. conditions

B. subject

C. content

D. actions

E. policies

Suggested Answer: *AD*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_11-1/b_ESA_Admin_Guide_ces_11_1/b_ESA_Admin_Guide_chapter_01010.pdf

Community vote distribution
AD (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: AD
Correct.

Content filters have the following components:
• conditions that determine when the appliance uses a content filter to scan a message (optional)
• actions that the appliance takes on a message (required)
• action variables that the appliance can add to a message when modifying it (optional)

https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_11-1/b_ESA_Admin_Guide_ces_11_1/b_ESA_Admin_Guide_chapter_01010.pdf
upvoted 2 times

ccnpsise 1 year, 8 months ago

there is a new Q i am not sure about how the Q was constructed but it is something about a company employs a user help desk to assist in message quaratine and which right should be given to him to fulfil this task. options are Administrator,User help desk, Technician, Quarantine Administrator.

10% of the questions here came out in my exam today
upvoted 2 times

stealthscout 1 year, 4 months ago

This question appeared in my exam, thank you.
upvoted 1 times

iluxa 3 years ago

Correct.
upvoted 2 times

Question #61 *Topic 1*

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.

Suggested Answer: *C*

Community vote distribution

C (100%)

mikeXTR 9 months, 1 week ago

Correct.

upvoted 1 times

hakimbenda 1 year, 2 months ago

Selected Answer: C

Correct

upvoted 1 times

GVKD 1 year, 3 months ago

Selected Answer: C

Correct.

The Security Management appliance includes the following features:

External spam quarantine. Holds spam and suspected spam messages for end users, and allow end users and administrators to review messages that are flagged as spam before making a final determination.
Centralized policy, virus, and outbreak quarantines. Provide a single location behind the firewall to store and manage messages quarantined by anti-virus scanning, outbreak filters, and policies.
Centralized reporting. Run reports on aggregated data from multiple Email Security appliances.
Centralized tracking. Track email messages that traverse multiple Email Security appliances.

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_0101010.html?bookSearch=true

upvoted 2 times

Question #62 *Topic 1*

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

Suggested Answer: *BD*

Community vote distribution

BD (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: BD

Correct.

DomainKeys and DKIM Authentication

With DomainKeys or DKIM email authentication, the sender signs the email using public key cryptography. The verified domain can then be used to detect forgeries by comparing it with the domain in the From: (or Sender:) header of the email.

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_010101.html?bookSearch=true

upvoted 1 times

Question #63 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

A (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: A

A is Correct.

Message Handling Settings:

Repaired Message Handling
Messages are considered repaired if the message was completely scanned and all viruses have been repaired or removed. These messages will be delivered as is.

Encrypted Message Handling
Messages are considered encrypted if the engine is unable to finish the scan due to an encrypted or protected field in the message. Messages that are marked encrypted may also be repaired.

Unscannable Message Handling
Messages are considered unscannable if a scanning timeout value has been reached, or the engine becomes unavailable due to an internal error. Messages that are marked unscannable may also be repaired.

Virus Infected Message Handling
The system may be unable to drop the attachment or completely repair a message. In these cases, you can configure how the system handles messages that could still contain viruses.

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_01011.html#con_1132282

upvoted 2 times

Question #64 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

C (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: C

Ci is Correct.

Disabling the Local Spam Quarantine to Activate the External Quarantine
If you were using a local spam quarantine before enabling an external spam quarantine, you must disable the local quarantine in order to send messages to the external quarantine.

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_0101010.html?bookSearch=true#con_1172419

upvoted 3 times

Question #65 *Topic 1*

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.

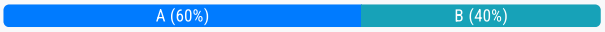
B. The message header with the highest priority is checked against each policy in a top-down fashion.

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.

Suggested Answer: *D*

Community vote distribution



GVKD 9 months ago

Selected Answer: B

B might be more correct.

The envelope sender and the envelope recipeint have a higher priority over the sender header when you match a message to a mail policy. If you configure a mail policy to match a specific user, the messages are automatically classified into the mail policy based on the envelope sender and the envelope recipient.

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_01001.html

upvoted 2 times

GVKD 9 months, 2 weeks ago

Selected Answer: A

A is Correct.

First Match Wins
Each user (sender or recipient) is evaluated for each mail policy defined the appropriate mail policy table in a top-down fashion.

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_01001.html?bookSearch=true

upvoted 3 times

Question #66 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: A

Correct.

The appliance enforces your organization's policies for messages sent to and from your users through the use of mail policies. These are sets of rules that specify the types of suspect, sensitive, or malicious content that your organization may not want entering or leaving your network. This content may include:

-spam
-legitimate marketing messages
-graymail
-viruses
-phishing and other targeted mail attacks
-confidential corporate data
-personally identifiable information

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_01001.html?bookSearch=true

upvoted 1 times

Question #67 *Topic 1*

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.

Suggested Answer: *C*

Community vote distribution

C (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: C

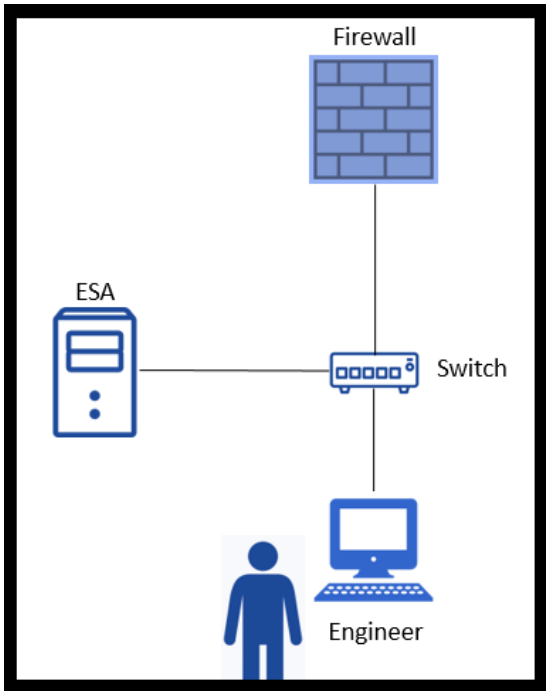
Correct.

SMTP Routes allow you to redirect all email for a particular domain to a different mail exchange (MX) host.

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

upvoted 1 times

Question #68 *Topic 1*



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

Suggested Answer: *D*

Community vote distribution

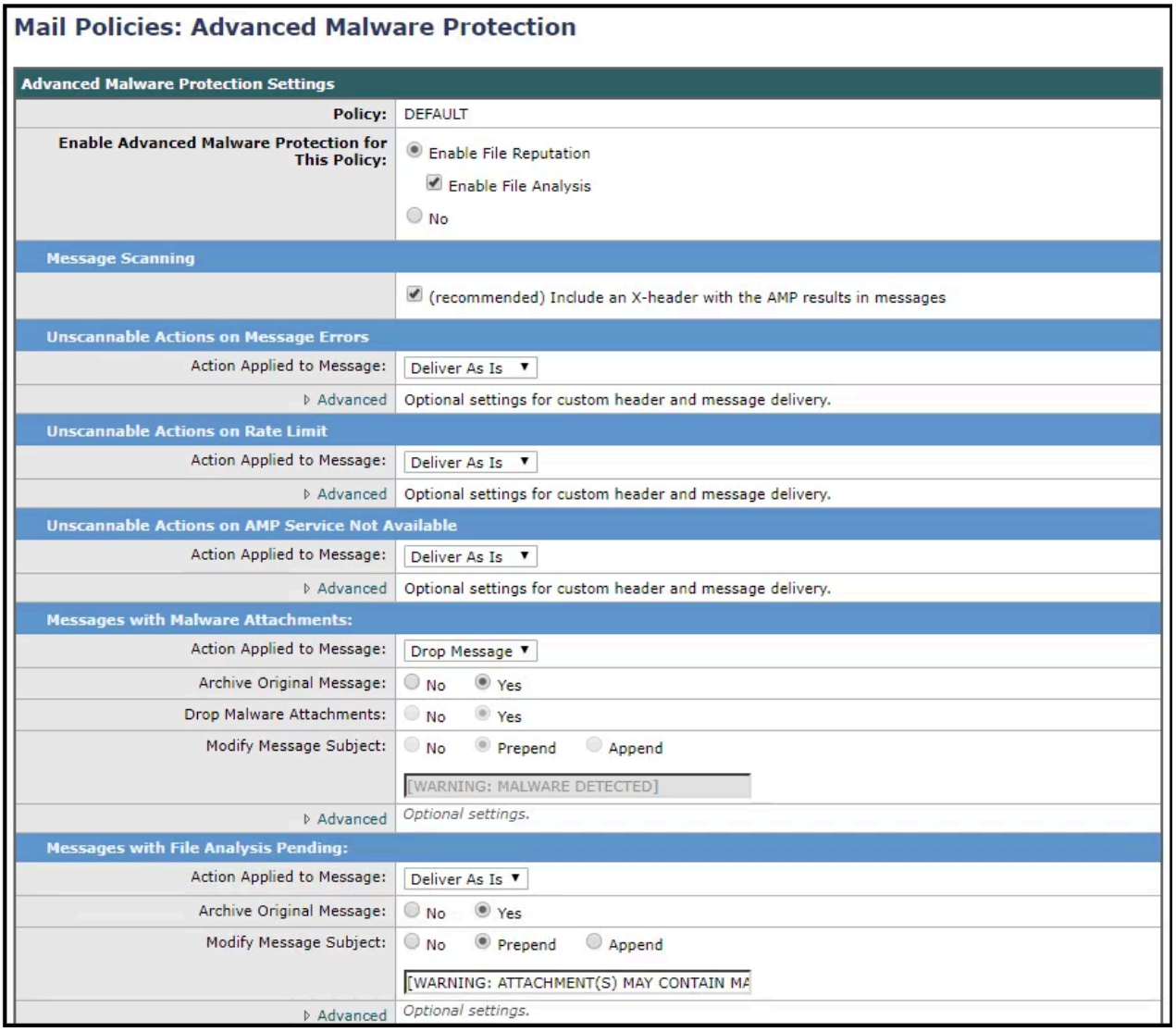
D (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: D

Correct.

upvoted 1 times



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.

Suggested Answer: *C*

Community vote distribution

B (100%)

GVKD Highly Voted 9 months, 2 weeks ago

Selected Answer: B

B is Correct.

Overview of File Reputation Filtering and File Analysis:

Advanced Malware Protection protects against zero-day and targeted file-based threats in email attachments by:

-Obtaining the reputation of known files.
-Analyzing behavior of certain files that are not yet known to the reputation service.
-Continuously evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats

after they have entered your network.
-This feature is available for incoming messages and outgoing messages.

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_010000.html?bookSearch=true

upvoted 6 times

adamx Most Recent 3 months, 3 weeks ago

Selected Answer: B

Cannot be C as mailbox auto remediation is for emails already delivered

upvoted 2 times

Question #70 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

B (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: B

Correct.

upvoted 2 times

Question #71 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

C (100%)

GVKD 9 months, 2 weeks ago

Selected Answer: C

Correct.

Default HAT Entries
By default, the HAT is defined to take different actions depending on the listener type:

Public listeners. The HAT is set to accept email from all hosts.
Private listeners. The HAT is set up to relay email from the host(s) you specify, and reject all other hosts.

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_0110.html?bookSearch=true

upvoted 2 times