Cisco

300-720 Exam

Cisco Securing Email with Cisco Email Security Appliance Exam

Questions & Answers
Demo

Version: 4.0

Question: 1

Which SMTP extension does Cisco ESA support for email security?

A. ETRN
B. UTF8SMTP
C. PIPELINING
D. STARTTLS

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

Question: 2

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

Answer: A

Question: 3

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

Answer: C

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

Question: 4

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.

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

Answer:

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

Question: 5

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

Answer: AC

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