Fortinet FCESP

Fortinet Certified Email Security Professional

Version: 5.0

QUESTION NO: 1

Which protection profile can be used to protect against Directory Harvest attacks?

A. antispam profile
B. session profile
C. content profile
D. antivirus profile

Answer: B
Explanation:

QUESTION NO: 2

What is one reason for deploying a FortiMail unit in Transparent Mode?

A. DNS records do not necessarily have to be modified.
B. Mail is not queued thereby expediting mail delivery.
C. Mail is not inspected unless a policy explicitly matches the traffic.
D. No user information needs to be stored on the FortiMail unit when operating in Transparent Mode.

Answer: A
Explanation:

QUESTION NO: 3

Which profile can be used to protect against Denial of Service attacks?

A. antispam profile
B. session profile
C. dos profile
D. security profile

Answer: B
Explanation:

QUESTION NO: 4

Which of the following parameters CANNOT be configured using the Quick Start Wizard?

A. protected domains
B. system time
C. operation mode
D. access control rules
E. antispam settings

Answer: C
Explanation:

QUESTION NO: 5

Which of the following DNS records resolves an IP address into a hostname?

A. MX record
B. PTR record
C. A record
D. NS record

Answer: B
Explanation:

QUESTION NO: 6

Which SMTP sessions are defined as incoming?

A. All SMTP sessions received by the FortiMail units
B. SMTP sessions for the protected domain
C. SMTP sessions received on the management interface
D. All sessions generated from the internal network

Answer: B
Explanation:

QUESTION NO: 7

Which back-end servers can be used to provide Recipient Verification?

A. LDAP servers
B. POP3 servers
C. RADIUS servers
D. SMTP servers

Answer: A,D
Explanation:

QUESTION NO: 8

Under which of the following conditions would an email be placed in the Dead Mail queue?

A. The recipient of the email is invalid.
B. The sender of the email is invalid.
C. The email is classified as spam.
D. The remote MTA is performing Greylisting.

Answer: A,B
Explanation:

QUESTION NO: 9

A System Administrator is concerned by the amount of disk space being used to store quarantine email messages for non-existent accounts. Which of the following techniques can be used on a FortiMail unit to PREVENT email messages from being quarantined for non-existent accounts?

A. Greylist Scanning
B. Recipient Address Verification
C. Sender Reputation
D. Automatic Removal of Invalid Quarantine Accounts

Answer: B
Explanation:

QUESTION NO: 10

Which of the following features can be used to expand a single recipient address into a group of one or many email addresses?

A. User Alias
B. Address Map
C. User Group
D. None of the above

Answer: A
Explanation:

QUESTION NO: 11

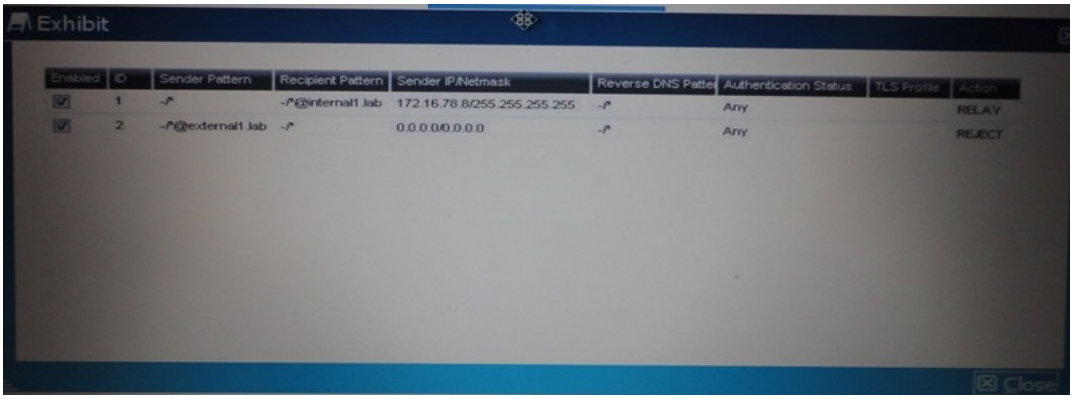
On a FortiMail unit, access control rules specify actions to be taken against matching email messages. Which of the following statements correctly describes the Bypass action?

A. Accept the email message but skip the MX record lookup. This mail message will be delivered using the configured relay server.
B. Do not deliver the email message.
C. Accept the email message and skip all message scanning, such as antispam and antivirus.
D. Accept the email message and delete it immediately without delivery.

Answer: C
Explanation:

QUESTION NO: 12

Two access control rules are configured on a FortiMail unit as illustrated in the exhibit.



Which of the following statements correctly describes the COMBINED action of these two access control rules?

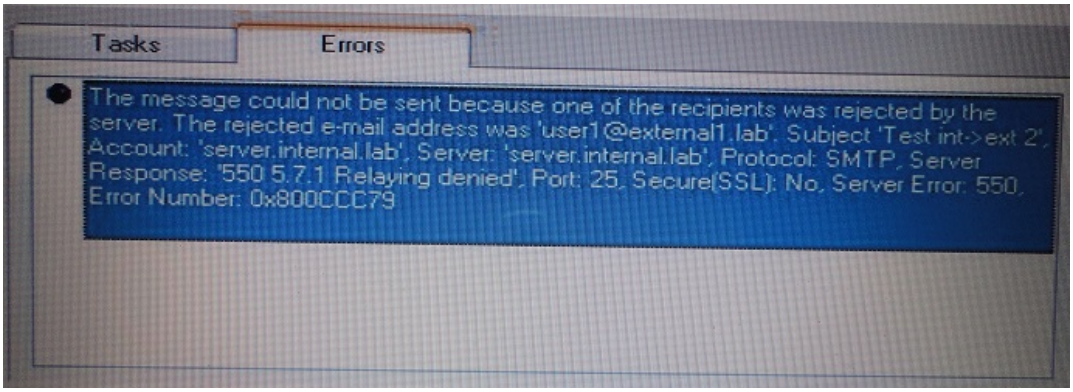
A. Email messages from senders at external1.lab will be rejected.
B. Email messages from external1.lab to internal1.lab from host IP 172.16.78.8 are relayed.
C. Email messages from external1.lab to internal1.lab from any host IP address are relayed.
D. Email messages from external1.lab to internal1.lab are restricted by the return DNS pattern.

Answer: B

Explanation:

QUESTION NO: 13

What is the best explanation for why a FortiMail unit would issue the error message indicated in the exhibit?



A. The recipient domain external1.lab is not defined.
B. This traffic comes from an authenticated sender.
C. Recipient verification is not working properly.
D. The session is matching an Access Control Rule with action "Reject".

Answer: A

Explanation:

QUESTION NO: 14

Which of the following FortiMail profile types apply to IP-based policies only?

A. Session profile
B. Content profile
C. IP pool
D. Antispam profile

Answer: A,C

Explanation:

QUESTION NO: 15

According to the Message Header printed below, which antispam technique detected this email as spam:

Return-Path: user1@external.lab

(SquirrelMail authenticated user user1)

by 172.16.78.8 with HTTP;

X-FEAS-HASH: 6ef419f0a0608b1655xxxxe68080df3cb12fc38f1118d2f085985eeb000274d7

Sat, 18 Apr 2009 15:53:06 +0200 (CEST)

Message-ID : <3029.192.168.3.101.1240062786.squirrel@172.16.78.8>

Date : Sat, 18 Apr 2009 15 :53 :06 +0200 (CEST)

Subject: [SPAM] Sales

From: user1@external.lab

To: user1@training1.lab

User-Agent: SquirrelMail/1.4.10a-1.fc6

MIME-Version : 1.0

Content-Type : text/plain ;charset=iso-8859-1

Content-Transfer-Encoding: 8bit

X-Priority: 3 (Normal)

Importance: Normal

X-Original-To: user1@training1.lab

Delivered-To: user1@training.lab

Received: from fm.sub.training1.lab (fm.sub.training1.lab [192.168.11.101])

by mail.training.lab (Postfix) with ESMTP id A9160187073

for <user1@training1.lab>; Sun, 19 Apr 2009 16:58:48 +0200 (CEST)