

100% Money Back Guarantee

Vendor: Fortinet

Exam Code: Fortinet Certified Email Security Professional

Exam Name: FCESP

Version: Demo

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?

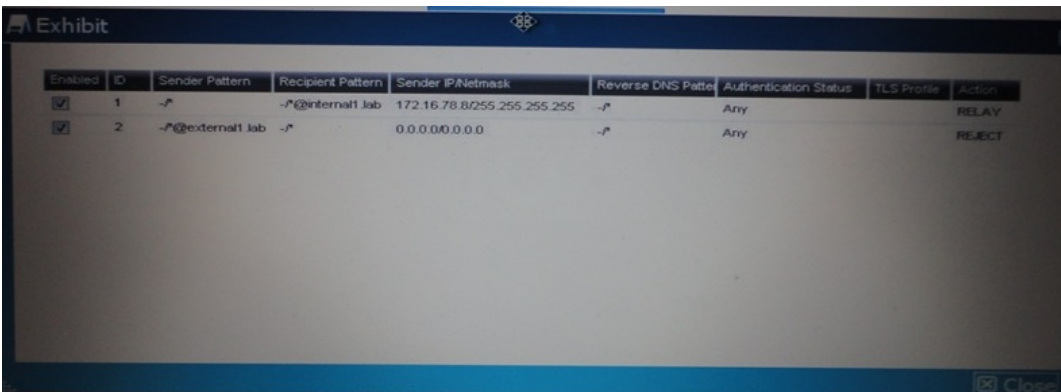
- A. Accept the email message but skip the MX record lookup. This mail message will be delivered using the configured relay server.
- B. Do not deliver the email message.
- C. Accept the email message and skip all message scanning, such as antispam and antivirus.
- D. Accept the email message and delete 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.



The screenshot shows a table of access control rules in a FortiMail configuration interface. The table has the following columns: Enabled, ID, Sender Pattern, Recipient Pattern, Sender IP/Netmask, Reverse DNS Pattern, Authentication Status, TLS Profile, and Action. Two rules are listed:

Enabled	ID	Sender Pattern	Recipient Pattern	Sender IP/Netmask	Reverse DNS Pattern	Authentication Status	TLS Profile	Action
<input checked="" type="checkbox"/>	1	~*	~*@internal1.lab	172.16.78.8/255.255.255.255	~*	Any		RELAY
<input checked="" type="checkbox"/>	2	~*@external1.lab	~*	0.0.0.0/0.0.0	~*	Any		REJECT

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

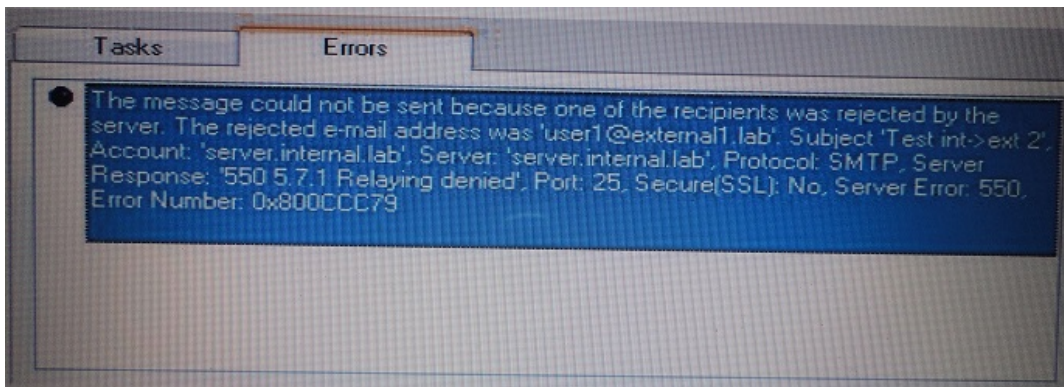
- A. Email messages from senders at external1.lab will be rejected.
- B. Email messages from external1.lab to internal1.lab from host IP 172.16.78.8 are relayed.
- C. Email messages from external1.lab to internal1.lab from any host IP address are relayed.
- D. Email messages from external1.lab to internal1.lab 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@training1.lab

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

by mail.training1.lab (Postfix) with ESMTP id A9160187073

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

Received: from mail.external.lab ([172.16.78.8])

by fm.sub.training1.lab with ESMTP id n3LEPHWu001093

for <user1@training1.lab>; Tue, 21 Apr 2009 10:25:17 -0400

Received: from 172.16.78.8 (localhost [127.0.0.1])

by mail.external.lab (Postfix) with ESMTP id 247D9BF893

for <user1@training1.lab>; Sat, 18 Apr 2009 15:53:06 +0200 (CEST)

Received: from 192.168.3.101

- A. DNSBL scan
- B. Dictionary scan
- C. Banned Word scan
- D. FortiGuard checksum

Answer: D

Explanation:

Question No : 16

Which of the following statements is true regarding Session-based antispam techniques?

- A. The entire mail content is inspected.
- B. They are enabled in the session profile only.
- C. SMTP commands, sender domain and IP address are checked.
- D. They are checked after application-based antispam techniques.

Answer: C

Explanation:

Question No : 17

Which of the following statements regarding the FortiMail unit's Greylisting feature is NOT correct?

- A. The FortiMail unit tracks the /32 bit host address of the sender.
- B. When an email is received from a new sender IP address, envelope sender and envelope recipient addresses, the FortiMail unit will initially send a temporary failure message.
- C. After the initial temporary fail message is sent, the message must be retransmitted between the Greylisting period expiry and initial expiry time periods.
- D. Pass-through is allowed until the configured TTL expires.
- E. An ACL with action Relay bypasses Greylisting.

Answer: A

Explanation:

Question No : 18

Which of the following is an advantage of using Banned Word scanning instead of Dictionary scanning?

- A. Mail Headers are inspected.
- B. It is easier to configure.
- C. Regular Expressions can be used.
- D. Non-ASCII characters are supported.

Answer: B

Explanation:

Question No : 19

Which operation is performed by the Forged IP scanning technique?

- A. DNS PTR record lookup on the sender's IP address then A record lookup on the canonical hostname
- B. DNS A record lookup on the sender's IP address then PTR record lookup
- C. DNS MX record lookup on the sender canonical hostname
- D. DNS TXT record lookup

Answer: A

Explanation:

Question No : 20

When using Sender Reputation on a FortiMail unit, which of the following actions can be taken against a source IP address generating spam or invalid email messages?

- A. Delay the email messages from that source IP address with a temporary fail.
- B. Reject the email messages from that source IP address with a permanent fail.
- C. Quarantine all the email messages from that source IP address.
- D. Limit the number of email messages allowed from that source IP address.

Answer: A,B,D

Explanation:

Question No : 21

Which of the following statements is true regarding oversized emails?

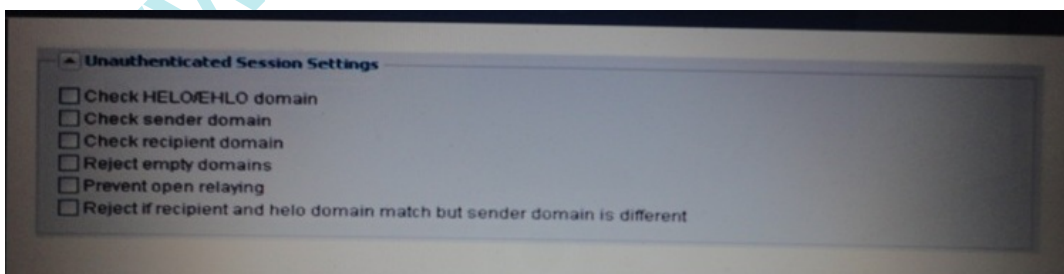
- A. The default maximum message size defined on the FortiMail unit is 10 MB.
- B. By default there is no maximum message size value defined on the FortiMail unit.
- C. The session profile parameter "Cap message size" can be used to increase the maximum message size.
- D. By default oversized emails are delivered at 0.00 local time.

Answer: A,C

Explanation:

Question No : 22

The option Prevent open relaying is shown in the exhibit. Which of the following statements is true regarding this option?



- A. Prevent open relaying is only available in Transparent mode.
- B. Prevent open relaying is only available in Server Mode.
- C. Prevent open relaying blocks all unauthenticated sessions.

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Trying our product !



- ★ **100%** Guaranteed Success
- ★ **100%** Money Back Guarantee
- ★ **365 Days** Free Update
- ★ **Instant Download** After Purchase
- ★ **24x7** Customer Support
- ★ Average **99.9%** Success Rate
- ★ More than **69,000** Satisfied Customers Worldwide
- ★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 One Year Free Update <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.