DO NOT REPRINT
© FORTINET
Braindumps.com

FORTINET CERTIFIED PROFESSIONAL
Public Cloud Security

FortiMail Administrator Study Guide

FortiMail 7.4

FORTINET
Training Institute

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

FORTINET

4/25/2024

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

TABLE OF CONTENTS

01 Email Concepts 4
02 Basic Setup 42
03 Access Control and Policies 91
04 Authentication 129
05 Session Management 162
06 Antivirus and Antispam 197
07 Content Inspection 265
08 Securing Communications 311
09 High Availability 369
10 Server Mode 399
11 Transparent Mode 427
12 Maintenance 462
13 Troubleshooting 495

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FORTINET
Training Institute

FORTINET
CERTIFIED
PROFESSIONAL
Public Cloud
Security

FortiMail Administrator

Email Concepts

FortiMail 7.4

Last Modified: 25 April 2024

In this lesson, you will learn about basic email concepts and gain an understanding of SMTP and FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- SMTP and DNS Roles
- Mail Flow
- Email Transmission and Retrieval
- Operating Modes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 2

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

SMTP and DNS Roles

Objectives

- Identify SMTP roles
- Describe the importance of DNS in email exchanges

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 3

After completing this section, you should be able to achieve the objectives shown on this slide.

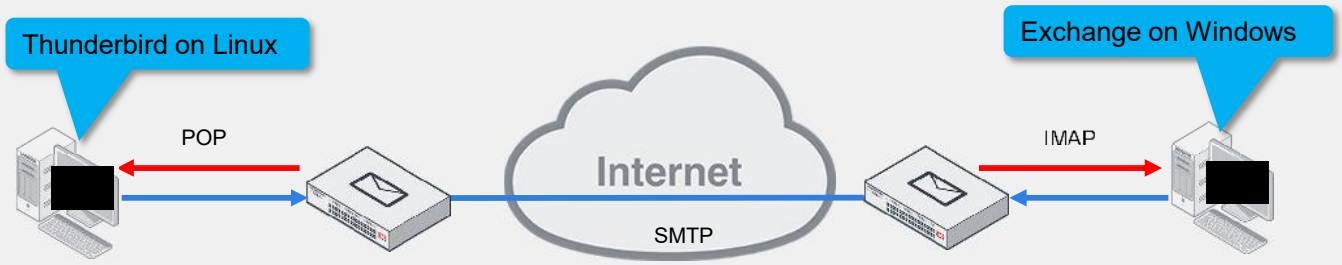
By demonstrating competence in SMTP and DNS roles, you will be able to identify SMTP device roles and understand the importance of DNS in email exchanges.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

What Is SMTP?

- Simple Mail Transport Protocol (SMTP)
  - Allows Mail Transfer Agents (MTA) to send email to each other
  - Platform-independent (Microsoft Exchange can SMTP email to a Lotus Domino server)
  - Separate protocol from delivery agents used by email clients to retrieve mail from mailboxes like Post Office Protocol (POP) or Internet Message Access Protocol (IMAP)



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

Mail servers use SMTP to deliver email between accounts in different domains. If a mail server wants to communicate a message to a separate mail server across the internet, it usually does so using SMTP. SMTP is distinct from mail delivery protocols in that it is universally used regardless of whatever endpoint client is being used.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SMTP Device Roles

- Mail user agent (MUA)
  - Microsoft Outlook, Mozilla Thunderbird, Apple Mail
  - SMTP for sending emails
  - POP3 or IMAP for retrieving emails from a mail server
- Mail transfer agent (MTA)
  - FortiMail, Postfix, Microsoft Exchange
  - Intermediate hop that processes email; also known as a mail relay
  - Open relays allow unvetted senders and are heavily exploited by spammers
- Mail server
  - Microsoft Exchange, FortiMail (server mode)
  - The final destination of an email
  - Contains user mailboxes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

End users interact with their email using a mail user agent (MUA), such as Microsoft Outlook, Mozilla Thunderbird, or Apple Mail, to compose and send email. MUAs facilitate email retrieval protocols such as POP or IMAP.

An SMTP server that handles email, but isn't the final destination server, is an MTA (also known as a mail relay). MTAs can exist internally, on an enterprise network, or on the internet, provided as a service by an ISP for its customers. FortiMail operating in gateway mode is an MTA. FortiMail in server mode is both an MTA and the destination mail server. Typically, MTAs implement a vetting mechanism to check if a sender is authorized to use the services of that MTA. This can be in the form of authentication or filtering rules, based on source IP addresses. MTAs that don’t implement these mechanisms are referred to as open relays. Open relays are widely exploited by spammers, to send unsolicited spam in bulk.

A mail server is the final destination of an email before the recipient retrieves it. A mail server might also support MTA functionality but also host user mailboxes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

DNS Role

- Mail exchanger (MX) record
  - A type of DNS record that specifies one or more MTAs for a domain
  - With multiple MTAs, priority values are used to indicate preference
    - Lower preference = higher priority

```
#nslookup -type=mx internal.lab
   Server: UnKnown
   Address: 10.0.1.10

   internal.lab MX preference = 20, mail exchanger = intsrv.internal.lab
   internal.lab MX preference = 10, mail exchanger = intgw.internal.lab
   intsrv.internal.lab  internet address = 10.0.1.99
   intgw.internal.lab  internet address = 10.0.1.11
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

DNS plays an important role in email delivery. When an MTA needs to verify where to send an email, it performs a lookup for a specific type of DNS record on the domain portion of the recipient's email address. This DNS record is known as the MX record. The MX record lookup can return one or more destination MTAs. To send the email, the sending MTA connects to the address indicated by the MX record.

When multiple MTA addresses exist, preference values are used to indicate priority. An MTA with the lowest preference always has the highest priority. If the MTA with the lowest preference doesn't respond to a TCP SYN request, then the next higher preference MTA is used. If the preference value is equal across multiple MX entries, then some form of load balancing may be used. The most common form of load balancing is DNS round robin. The DNS server randomizes the order of equally weighted DNS MX responses, where the senders therefore load distribute using whichever random server is at the top of the list.

Depending on the deployment mode of FortiMail, the public DNS records may indicate that FortiMail is the MX destination.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. What is an MUA?
   - ✓ A. Software that end users use to retrieve and send email messages
   - B. A protocol used to authenticate users for email retrieval

2. Which MX record does a remote MTA use to send emails to the `acmecorp.net` domain?

```
nslookup -type=mx acmecorp.net

Non-authoritative answer:
acmecorp.net     MX preference = 5, mail exchanger = gw2.acmecorp.net
acmecorp.net     MX preference = 30, mail exchanger = gw1.acmecorp.net
```

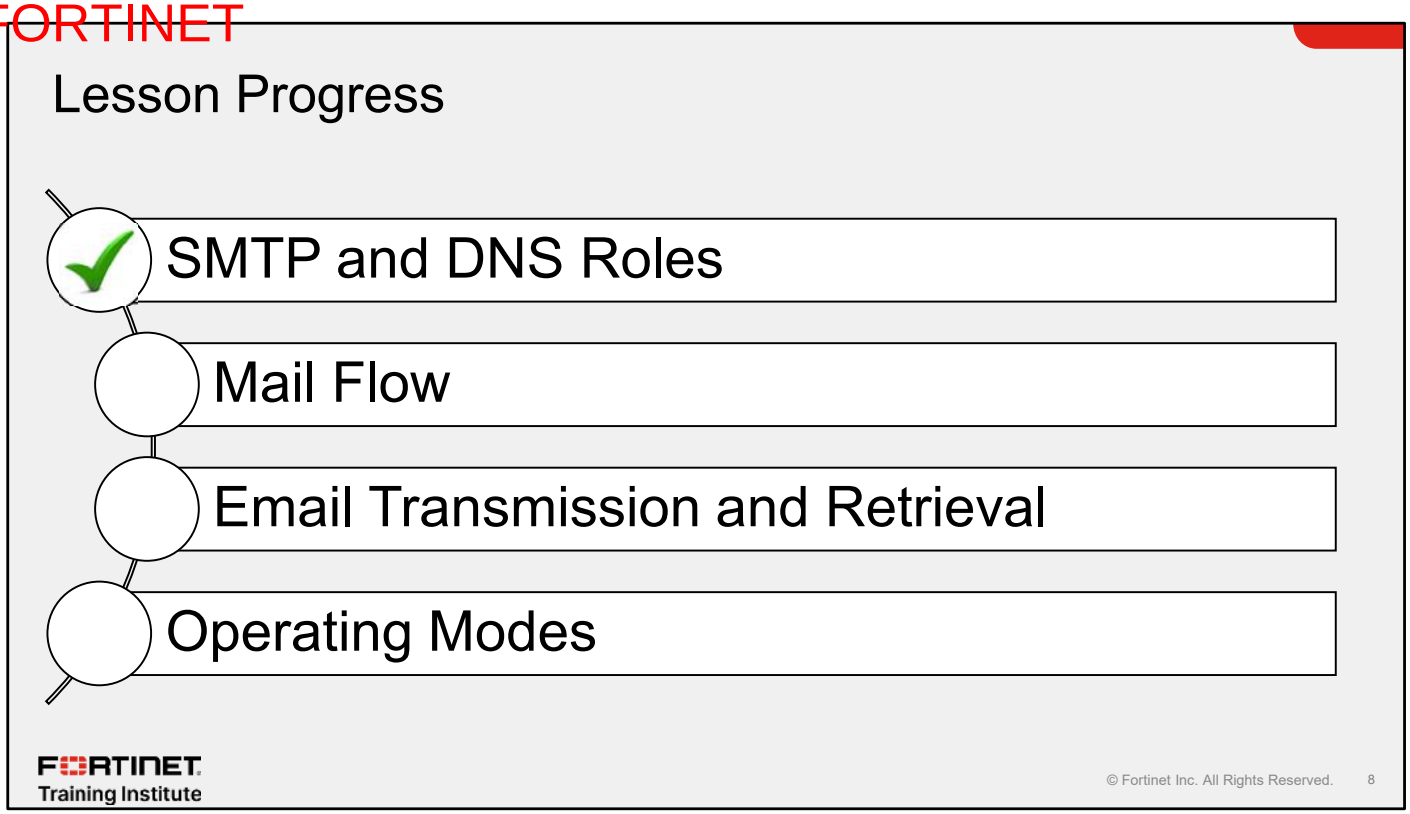
   - ✓ A. `gw2.acmecorp.net`
   - B. `gw1.acmecorp.net`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

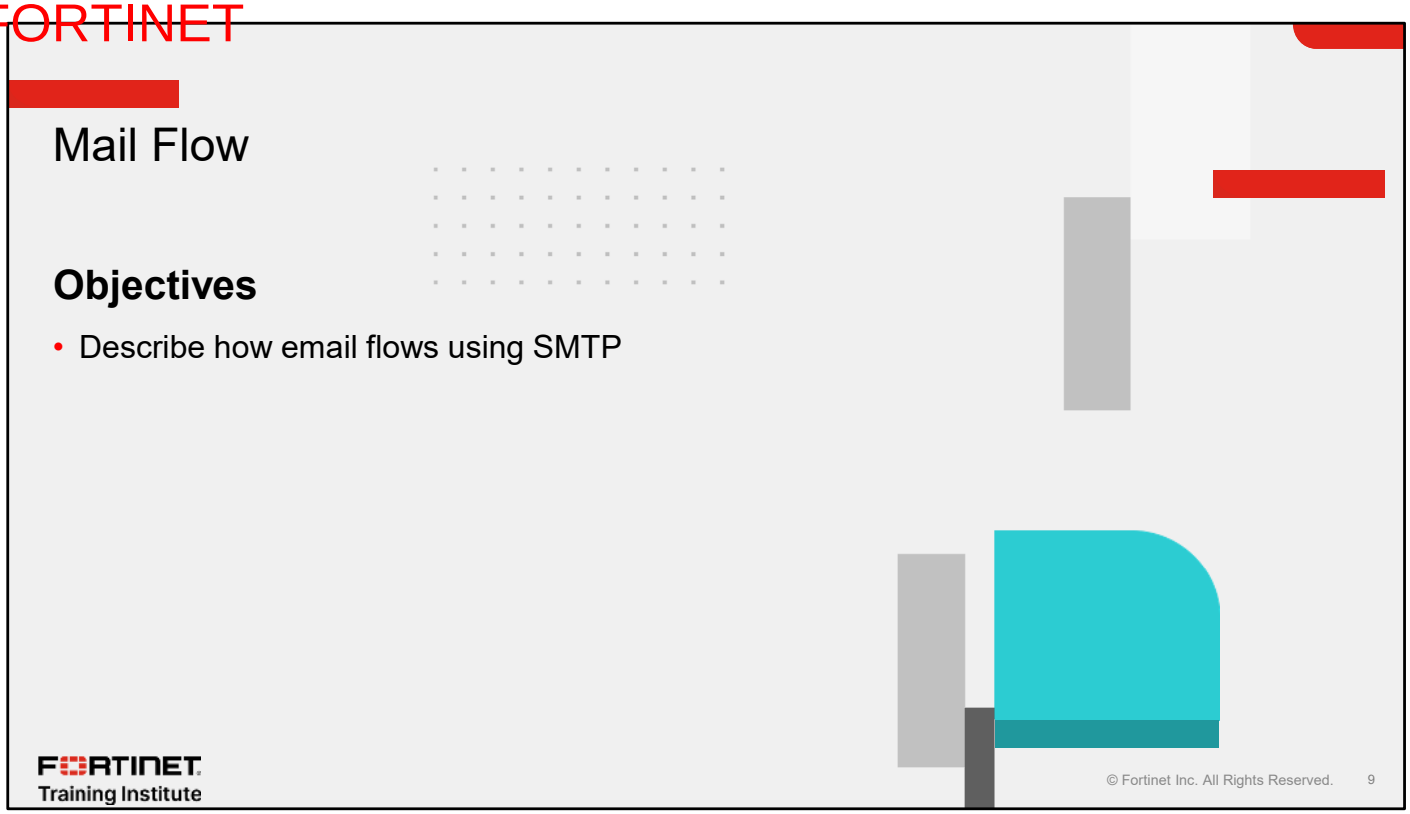


Good job! You now understand SMTP and DNS roles.

Now, you will learn about mail flow.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



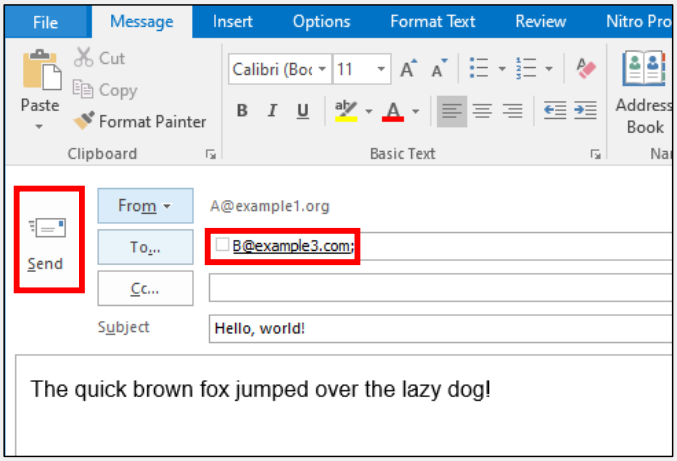
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in mail flow, you will be able to identify mail flows and how the SMTP protocol works.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Sending Email



1. The MUA connects to the local mail server (MTA)
2. The MTA performs a DNS MX record lookup on the domain portion of the recipient address: `example3.com`
3. The local MTA connects to the remote MTA and transmits the message
4. The remote MTA delivers the message to the user mailbox on the destination mail server

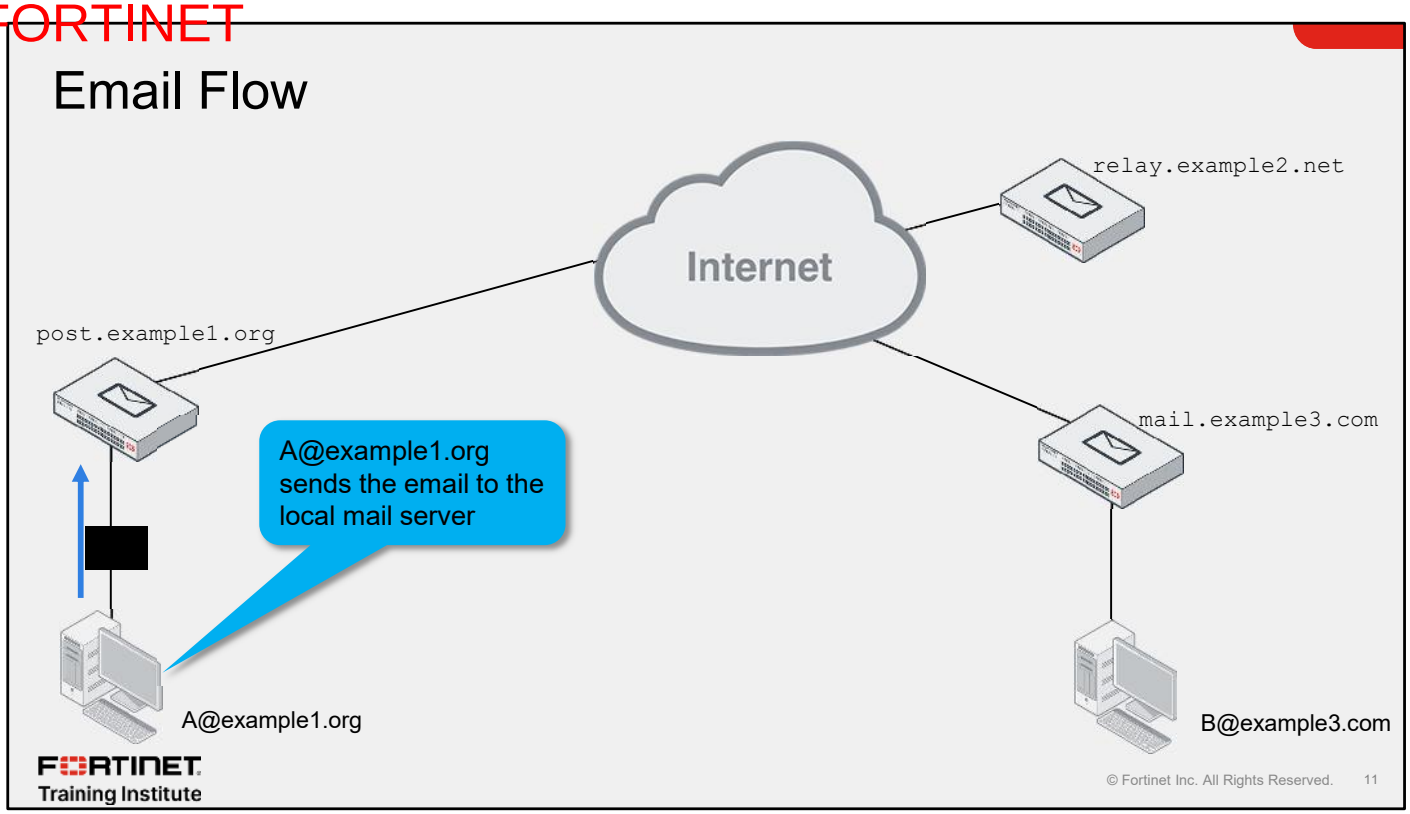
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

When a user composes an email message to a recipient in their email client software and clicks **Send**, the software connects to the mail relay. Usually, this is the corporate or ISP mail server. The mail relay performs a DNS lookup for the domain portion of the recipient's email address, requesting the MX record for that domain, and delivers the email to the listed next hop MTA. This process is repeated until the email reaches the destination mail server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

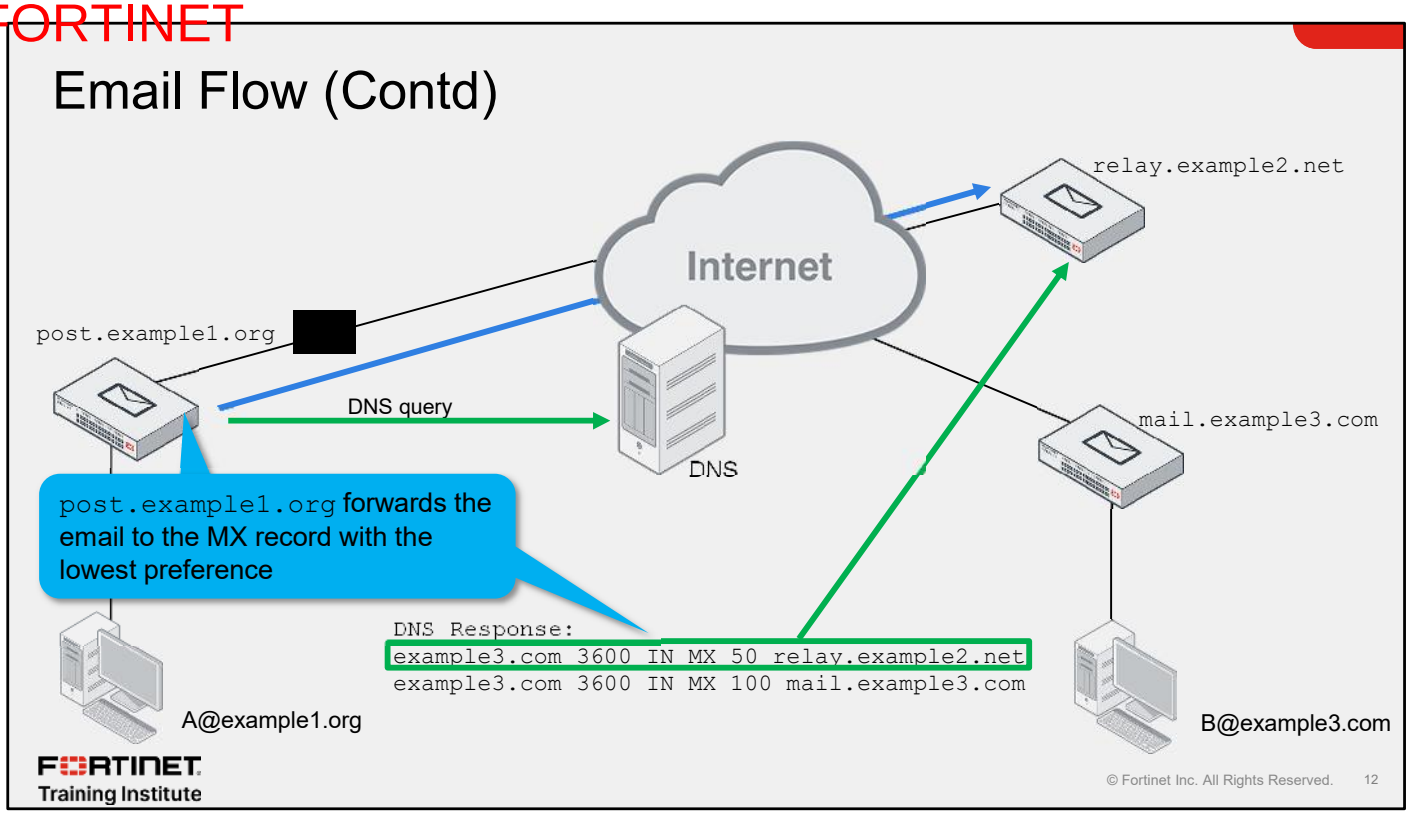


On the next few slides, you will learn about the process of sending an email.

This slide illustrates a scenario where user A@example1.org wants to send an email to B@example3.com. Since `post.example1.org` is the local mail server for the sender, the email will go through `post.example1.org`.

Vouchers & Dumps are Available | WhatsApp +201224560923

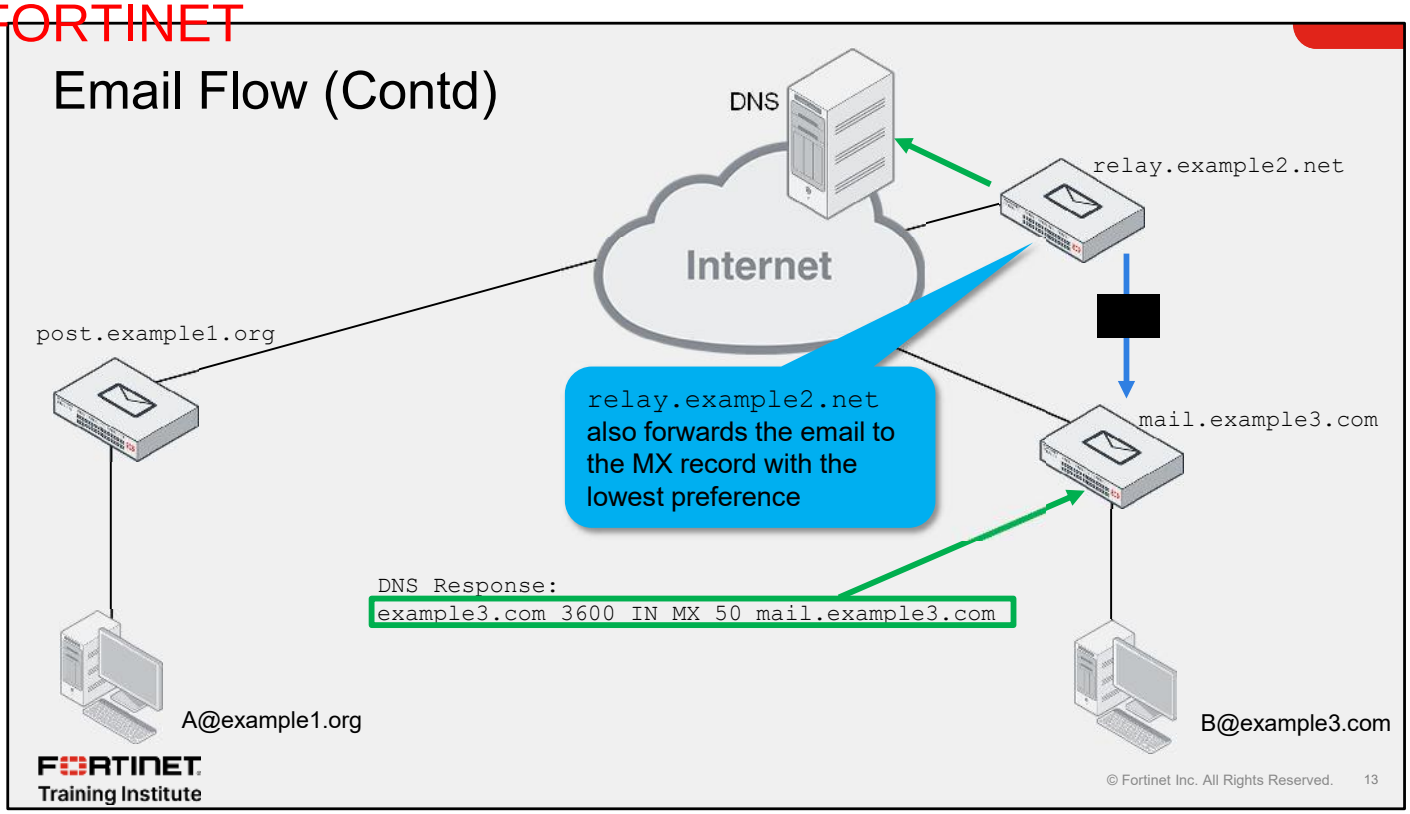
DO NOT REPRINT Brave-dumps.com
© FORTINET



To forward the email toward the destination, `post.example1.org` queries the public DNS server for the MX records of `example3.com`, and uses the entry with the lowest preference, which in this case is `relay.example2.net` with a preference value of `50`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

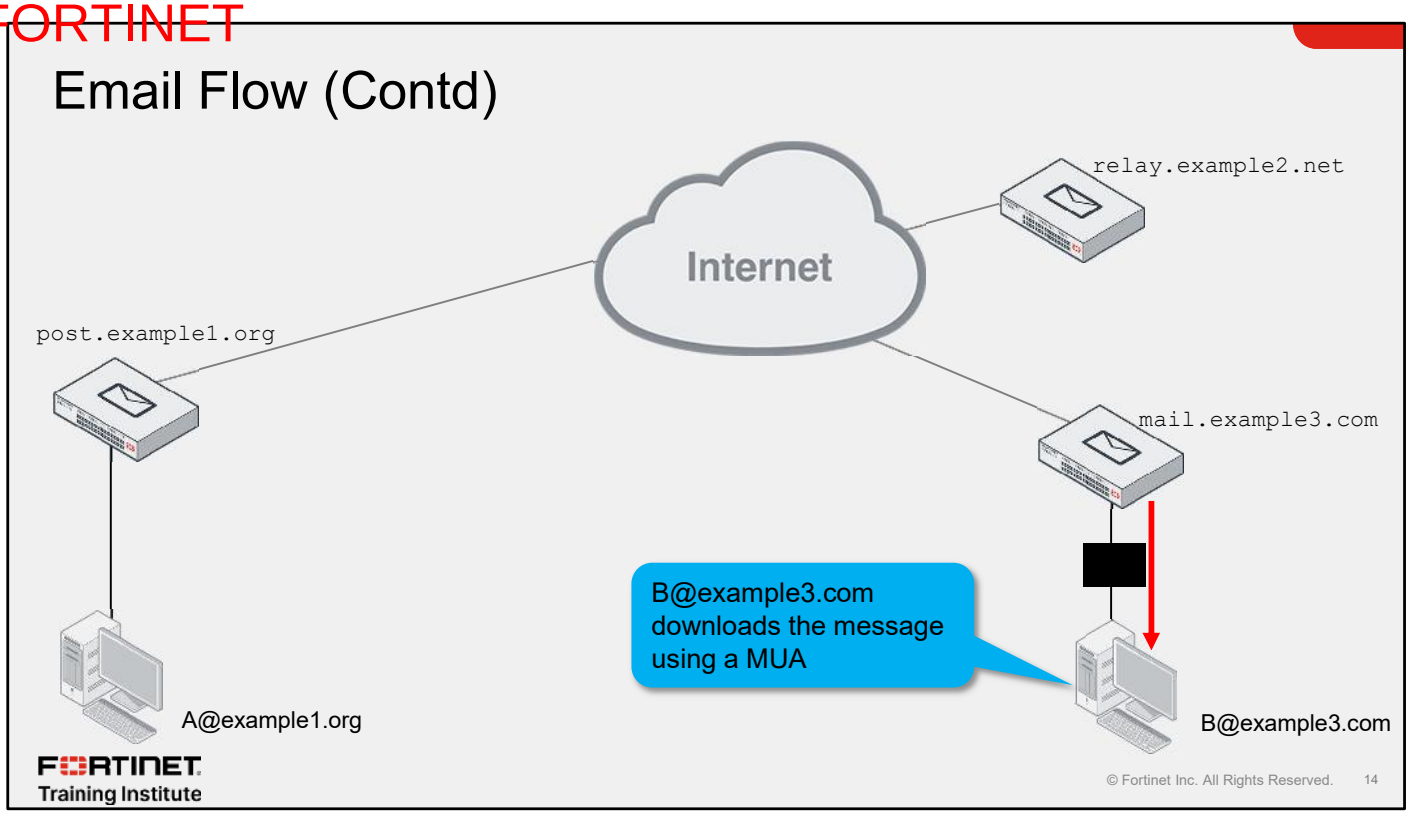


Since the `relay.example2.net` MTA is not the final destination for this email, it also queries the DNS server for the MX record for example3.com. This time, the smallest preference entry is `mail.example3.com`. So, `relay.example2.net` forwards the email to `mail.example3.com`.

Note that while the same DNS server providing different MX record responses is not a typical scenario, it is possible to achieve this using split-view DNS mechanisms. Split-view DNS is an implementation of DNS that provides different DNS responses based on the source IP of the DNS request. The network topology shown on this slide is using a split-view DNS mechanism to illustrate how email routing is achieved. This is very common in situations where separate filtering email devices are used but redundancy and continuity is important.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Finally, user B@example3.com uses their MUA to download the email from `mail.example3.com`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which type of DNS lookup does an MTA perform to verify where to send an email?
   A. CNAME record
   ✓ B. MX record

2. When an MX record lookup returns multiple FQDNs, which FQDN will FortiMail use to forward the email?
   A. The one with the highest preference value
   ✓ B. The one with the lowest preference value

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ SMTP and DNS Roles
- ✓ Mail Flow
- Email Transmission and Retrieval
- Operating Modes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

Good job! You now understand mail flow.

Now, you will learn about email transmission and retrieval.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Email Transmission and Retrieval

Objectives

- Describe SMTP messages and the message exchange process
- Differentiate between SMTPS and SMTP over TLS
- Differentiate between protocols used to send and receive email

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in email transmission and retrieval, you will be able to describe the message exchange process and differentiate between different protocols that are used to send and receive email.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SMTP Commands

- RFC 821 Original SMTP
  - `HELO`: Initiates an SMTP session
  - `MAIL FROM`: Sender email address
  - `RCPT TO`: Recipient email address
  - `DATA`: Email contents
  - `RSET`: Terminates an active session
  - `NOOP`: Keeps a session alive
  - `QUIT`: Ends a session gracefully
  - Three-digit server response codes: `2xx`, `3xx`, `4xx`, `5xx`
    - 2xx and 3xx: General status codes
    - 4xx: Temporary errors
    - 5xx: Permanent errors
- RFC 1869: Extended SMTP (ESMTP)
  - `EHLO` indicates extended features—`STARTTLS`, `AUTH`
- More SMTP commands (RFC 2554, 2920, 3207, and other RFCs) less common

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

Email on the internet follows a set of standards known as SMTP. The SMTP protocol was first submitted in 1982 under RFC 821. Although there have been many subsequent extensions, SMTP remains true to its name: it is a relatively *simple* protocol, with a limited number of commands and responses.

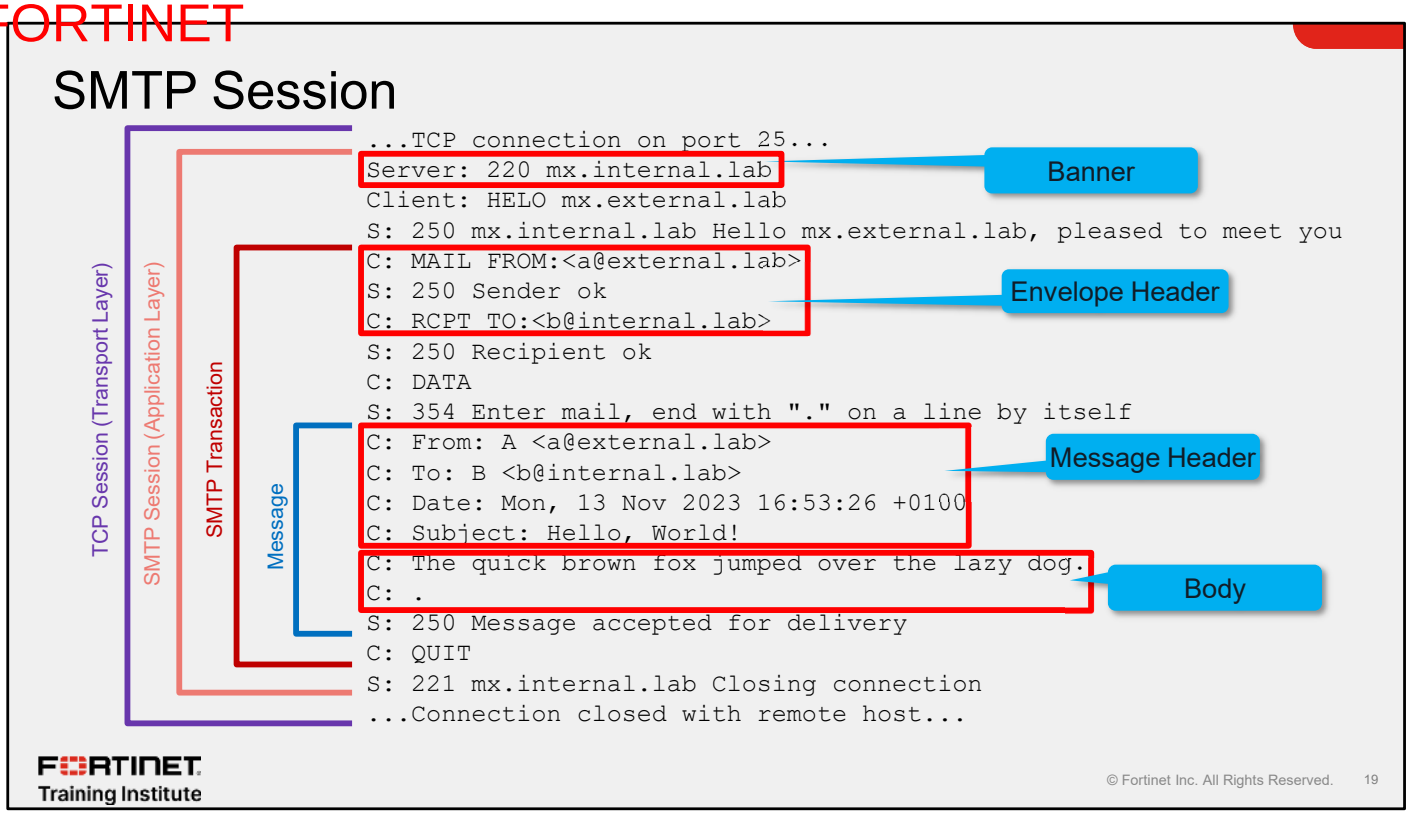
The SMTP commands shown on this slide show how the client—usually an MUA or an intermediary MTA—performs various tasks.

There are also three-digit server response codes that the receiving MTA can use to convey various status messages back to the sender.

Over the years, engineers have added features to SMTP that didn't exist in the original RFC. For example, servers that support ESMTP can be requested to use encryption of the email body using transport layer security (TLS).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide shows the commands that are typically used and seen by the client and server during an email exchange. It starts with the client—the sending MTA or MUA—initiating a TCP session on port 25 though keep in mind SMTP can be used over most TCP ports.

If the TCP session is established, the SMTP session starts when the receiving MTA presents the banner. The client then presents a `HELO` message, which the server acknowledges.

The client uses the `DATA` command to indicate the start of the actual email message, which includes the header and body. The message header can contain a lot more information than what is shown on this slide.

The client sends a single (.) to indicate the end of the message, and the server acknowledges the end of the SMTP transaction. If the client needs to send an additional email, the process starts again at the `MAIL FROM` step.

To end the SMTP session, the client sends the `QUIT` command, which is also acknowledged by the server. Then, the TCP session is torn down.

This type of message exchange occurs any time an SMTP device has to send an email. Whether it is an MUA-to-MTA or an MTA-to-MTA transmission, this kind of client-server interaction occurs. The only exception to this interaction is with Microsoft Outlook and Microsoft Exchange servers, which use a Microsoft proprietary protocol called Messaging Application Programming Interface (MAPI). MAPI is used for both email transmission and retrieval between Microsoft Outlook and Microsoft Exchange.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Message Header

```
...
Received: from relay.example2.net (relay.example2.net [4.3.2.1]) by mail.example3.com with ESMTP id 9876xyz;
  Mon, 13 Nov 2023 15:53:30 GMT

Received: from post.example1.org (1.2.3.4) by relay.example2.net (4.3.2.1) with SMTP id abcdef; Mon, 13 Nov
  2023 15:53:30 GMT

Received: from A (10.0.0.1) by post.example1.org with ESMTP id 123456; Mon, 13 Nov 2023 15:53:26 GMT

MIME-Version: 1.0
Subject: Hello, World!
Message-ID: <43849E86.29784.DF6209@localhost>
Priority: normal
X-mailer: Pegasus Mail for Windows (4.21c)
Content-type: text/plain; charset=US-ASCII
...
<email body>
...
```

First hop

Second hop

Third hop

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

A message header can contain a lot of useful information. Each email client has its own procedure for viewing the message header of a single email. Message headers are often used to gather information or troubleshoot email issues. The content of the message header remains intact when an email is forwarded as an attachment. Forwarding the email destroys the original message header because the MUA creates new headers from the new point of origin.

One of the most important parts of an email is the received header**.** Every time an email is generated by an MUA, or traverses an MTA, a received header is added. At a minimum, the received header contains the IP address of the sender, if it is the first hop, or the receiver, if it is an intermediary hop, as well as the date and time the email was processed by the hop. Depending on the vendor, MTAs sometimes add a session ID for the email, as well as the TLS version and cipher information (if applicable).

Received headers are added on top of one another. The bottom entry shows where the email started its journey, and the top entry shows where the email is currently located.

As well as the received headers, other information in the message header includes MIME headers, content headers, and the subject.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SMTP Authentication

- Security wasn't a consideration in the original RFC for SMTP
  - Standardized as ESMTP (extended SMTP) extensions
- `AUTH`
  - Provides authentication for SMTP clients
    - Uses Base64 for `AUTH PLAIN LOGIN`
  - Other older authentication algorithms can also be supported
    - For example, `CRAM-MD5`, `DIGEST-MD5`

```
S: 220 mx.internal.lab
C: EHLO external.lab
S: 250-AUTH PLAIN LOGIN
S: 250-STARTTLS
C: AUTH LOGIN
S: 334 VXNlcm5hbWU6
C: dXNlcm5hbWUuY29t
S: 334 UGFzc3dvcmQ6
C: bXlwYXNzd29yZA==
S: 235 ok, go ahead
```

Base64

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

The original RFC for SMTP did not include any requirements for security mechanisms. Email was transmitted in plaintext by unauthenticated users.

The `AUTH` extension was added later in the mid-1990s to verify sender identity. MTAs that support ESMTP can, and should, enforce authentication to ensure that only authorized users are allowed to send email. This verifies only the sender identity for outbound emails from a protected domain, but it does not prevent spoofing of inbound emails coming from external mail servers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SMTPS and STARTTLS

- To secure SMTP, SSL encryption was added as another layer using a separate TCP port
  - SMTP by default uses port 25, and SMTPS uses port 465 or 587
- STARTTLS was added as an extension
  - Functions on the same SMTP port
  - The client can upgrade a plaintext connection to be TLS-encrypted

```
S: 220 mx.internal.lab
C: EHLO external.lab
S: 250-AUTH PLAIN LOGIN
S: 250-STARTTLS
C: AUTH LOGIN
C: STARTTLS
S: 220 Ready to start TLS
...TLS handshake...
<encrypted data>
<encrypted data>
<encrypted data>
<encrypted data>
<encrypted data>
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

SMTPS implements a layer of security using TLS encryption, but it was never standardized. MTAs needed to maintain separate ports for encrypted and unencrypted sessions because SMTP by default uses port 25, and SMTPS uses port 465 or 587.

The current standard for secured email communication is SMTP over TLS. Connections are made using the standard SMTP port, and a TLS negotiation occurs after the SMTP session is established. If both sides agree, a secure connection is established and the remaining data is exchanged securely. Many ESMTP servers enforce the `STARTTLS` message for encryption. This means that the recipient MTA accepts only the envelope addresses (`MAIL FROM` and `RCPT TO`) after TLS is established.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SMTPS and STARTTLS (Contd)

SMTP over TLS (STARTTLS)

```
...TCP handshake on port 25...
S: 220 mx.internal.lab
C: EHLO external.lab
S: 250-AUTH PLAIN LOGIN
S: 250-STARTTLS
C: STARTTLS
S: 220 Ready to start TLS
...TLS handshake...
<encrypted data>
<encrypted data>
<encrypted data>
<encrypted data>
<encrypted data>
```

Sender chooses to use TLS encryption

STARTTLS encrypts the portion of the session most likely to contain sensitive data.

SMTPS

```
...TCP handshake on port 465...
...TLS Handshake...
<encrypted data>
<encrypted data>
<encrypted data>
<encrypted data>
<encrypted data>
<encrypted data>
<encrypted data>
<encrypted data>
<encrypted data>
<encrypted data>
```

SMTPS encrypts the entire session, including banner, HELO messages, and server extensions

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

In SMTP over TLS, the initial connection is made on the standard SMTP TCP port. The client, which can be an MUA or MTA, transmits its EHLO message and is presented with a list of extensions that represent the set of supported extensions on the server side of the connection. If STARTTLS is present in the list, and if the client wants a secure connection, then the client responds with STARTTLS. This initiates the TLS negotiation between the two endpoints. After the secure connection is established, the remaining SMTP traffic is encrypted on the network.

In SMTPS, the server and client start the SMTP session, which is fully encrypted in a TLS tunnel.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Retrieving Email—POP

- RFC 918 - Post Office Protocol (POP)
- Allows clients to download email from mailbox servers and save those messages to local storage
  - Usually deletes messages on the server after download
- RFC 1939 – Post Office Protocol - version 3 (POP3)
  - TCP/110 or TCP/995 (SSL/TLS)
    - SSL/TLS are commonly supported and used to encrypt entire session
    - If using port 110, username and password are sent in clear text

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

POP is used to download new messages and store them locally in the user's email client. Typically, the messages are deleted from the server after download. This works well, but there are some disadvantages. Since email messages are stored on the user's device after download, they are accessible only on that device. If the user accesses email from multiple devices, such as a smartphone and a laptop, it becomes challenging to keep track of which message is on which device.

It's important to use POP in a secure way. The original RFC for POP didn't implement any form of encryption, and passwords can be sent as clear text, unless the email server and client are configured to support the SSL/TLS extensions to POP3.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Retrieving Email—IMAP

- RFC 3501 - Internet Message Access Protocol - version 4 (IMAP4)
- Complete management of an email inbox
  - Messages usually kept on mail server until deletion
  - Allows multiple clients to manage the same mailbox
  - Manages folders within a mailbox
- TCP/143 (clear or STARTTLS) or TCP/993 (SSL/TLS)
  - SSL/TLS is the most common way to secure a connection

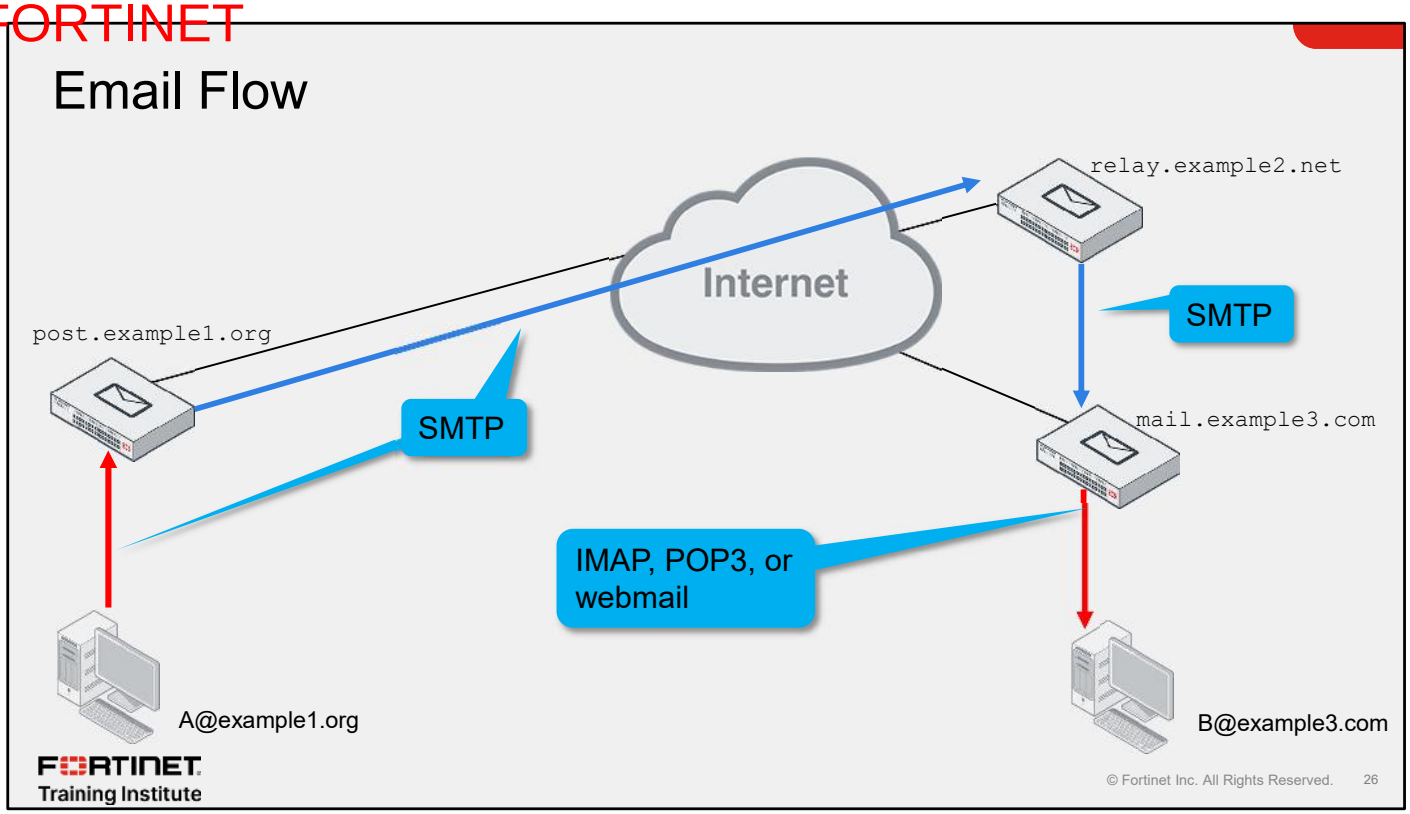
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

IMAP is another mail retrieval protocol that has multiple advantages over POP3. It provides more robust management of an email inbox, including message retention, allowing multiple managers of an inbox, folder management, and so on. IMAP is usually the go-to method for keeping multiple devices synchronized with the same inbox. Like POP3, IMAP functions on two separate ports. TCP port 143 can use a STARTTLS message to upgrade the connection to be TLS encrypted. Otherwise, IMAP will function in cleartext. TCP port 993 is used for complete end-to-end encryption using SSL.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Now, when you look at the mail flow example, you should be able to identify where SMTP transactions occur, and where IMAP, POP3, MAPI, and webmail transactions occur.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. SMTP STARTTLS is performed over which port?
   A. 465
   ✓ B. 25

2. Which protocol does a client use to retrieve emails from a mail server?
   ✓ A. IMAP
   B. SMTP

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ SMTP and DNS Roles
- ✓ Mail Flow
- ✓ Email Transmission and Retrieval
- Operating Modes

FORTINET Training Institute

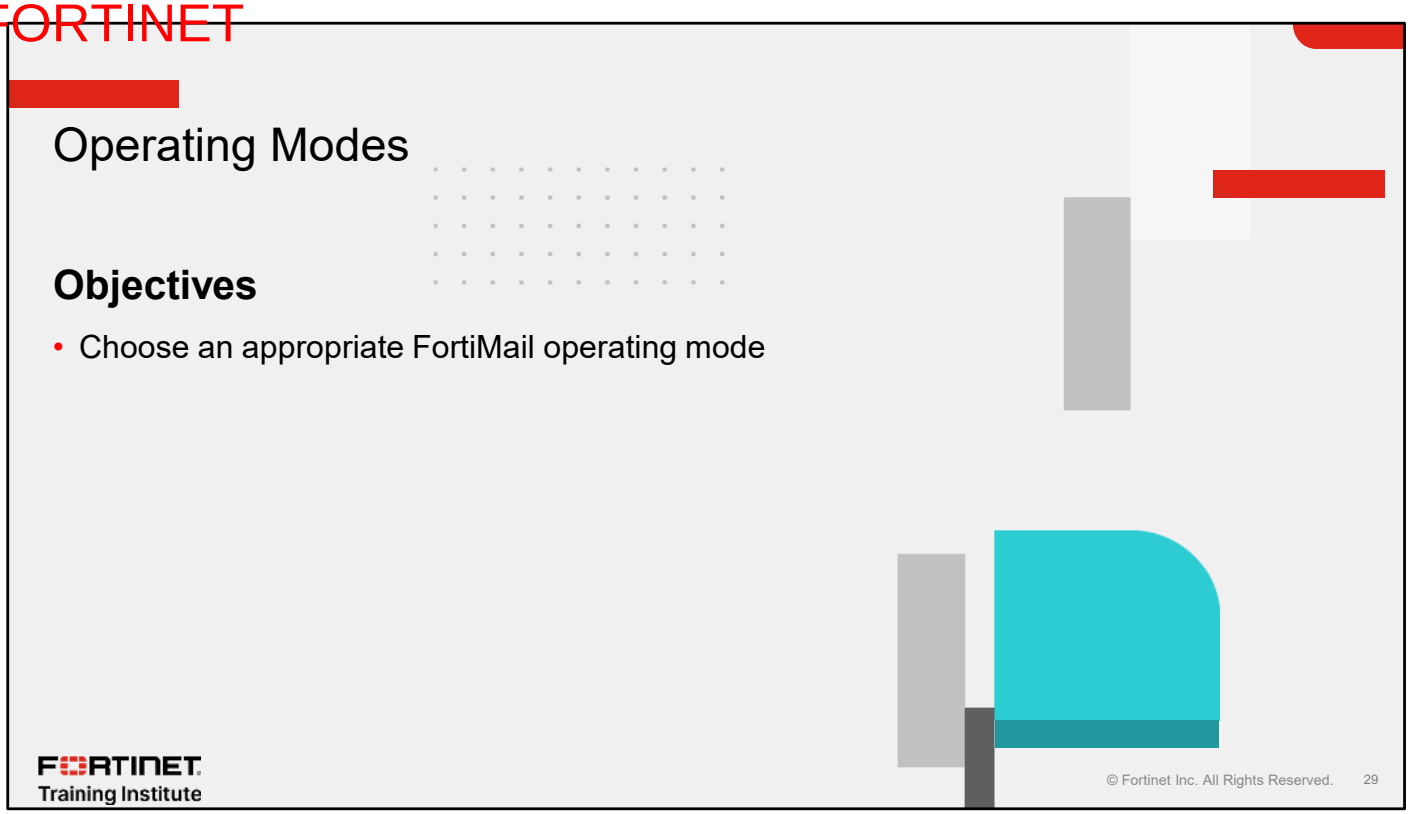
© Fortinet Inc. All Rights Reserved. 28

Good job! You now understand email transmission and retrieval.

Now, you will learn about operating modes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding FortiMail operating modes, you will be able to identify the appropriate operating mode for FortiMail, based on your network environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Gateway Mode

- Inbound and outbound MTA with application layer security
- Requires a DNS MX record change or a destination NAT rule change
  - All inbound email goes through FortiMail first, then is routed to a back-end mail server
- Default operation mode on FortiMail installation
- You must configure protected domains and associated mail servers

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

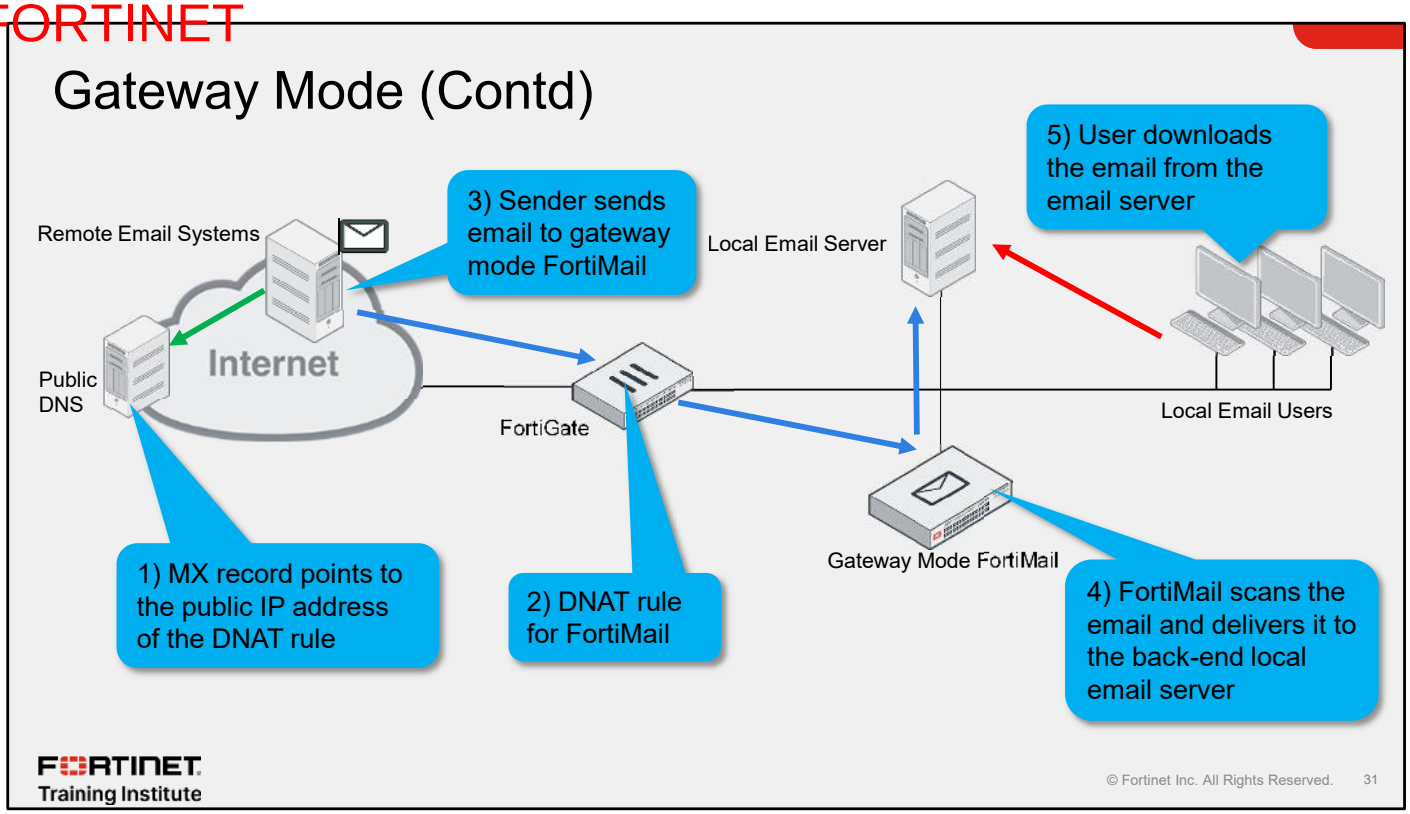
In gateway mode, FortiMail provides full MTA functionality. In the email path, FortiMail is situated in front of an existing email server and scans email. If FortiMail detects any spam emails, it discards them or stores them in the user quarantine mailboxes on the local FortiMail device. FortiMail delivers all clean emails to the back-end mail server.

Since incoming email needs to be directed to FortiMail, a DNS MX record change (or destination NAT rule change on the firewall) redirecting all inbound email traffic may be required. For complete protection, all outbound email should be routed through FortiMail for inspection.

Gateway mode deployments are excellent at extending existing email infrastructure scalability. FortiMail can offload all security-related and message-queuing tasks and reduce the overall performance requirements from back-end mail servers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In gateway mode DNS MX records usually point to an external firewall IP address that has a DNAT rule for the FortiMail device. After determining if the email is allowed, FortiMail scans and delivers the email to the corresponding local email server.

For outgoing email, FortiMail verifies if the sender of the email is valid and then performs its own DNS MX lookup for delivery unless email forwarding is configured.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Server Mode

- Full-featured mail server that has application layer security
- Receives, inspects, and delivers email to user mailboxes stored in a local database
- No separate email server required—all email is received and stored by FortiMail
- Ideal for small, drop-in, or new environments
  - Group calendars
  - Scheduling
  - Webmail

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

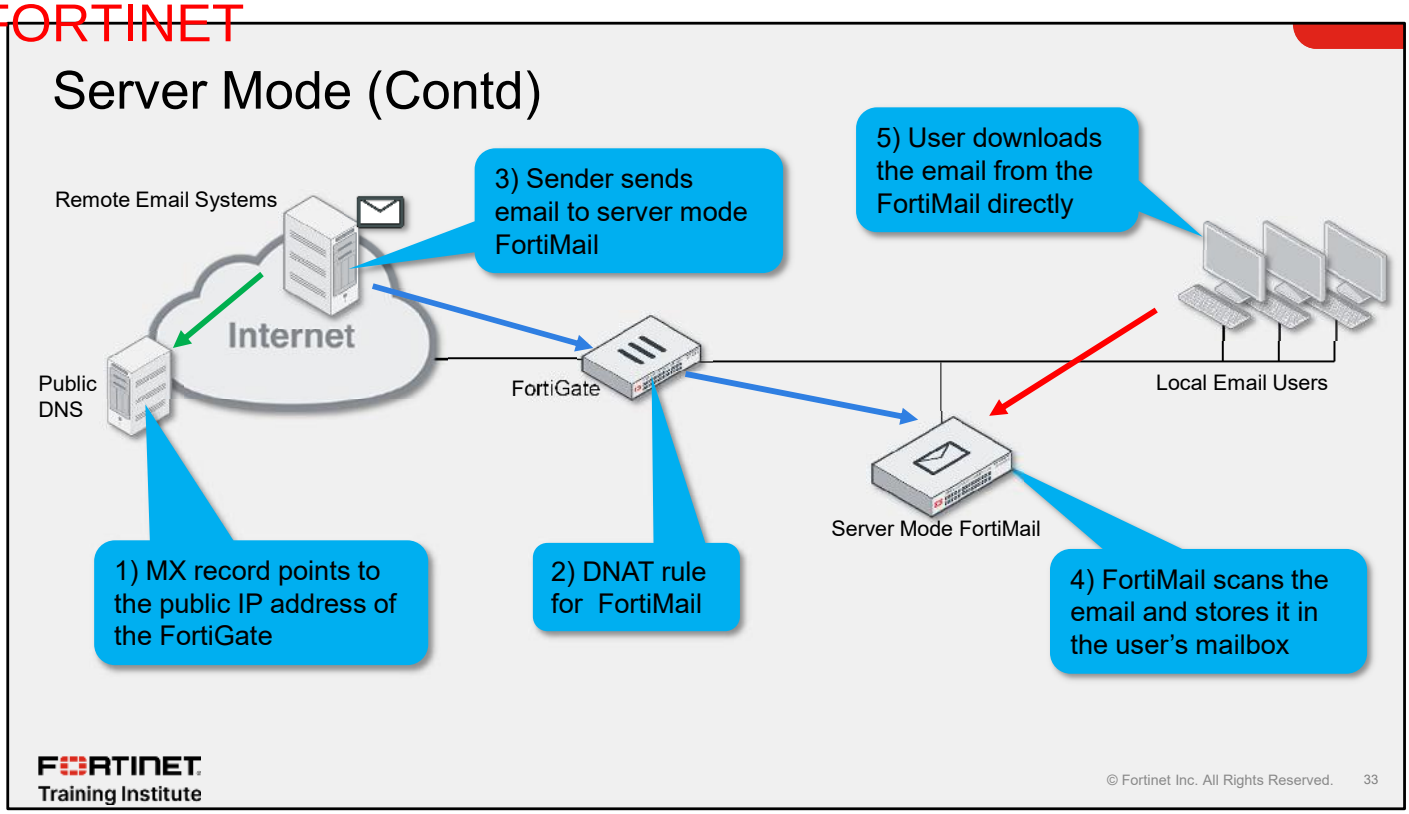
In server mode, FortiMail provides all of the typical functions of an email server, as well as security scans. You can use FortiMail operating in server mode as a drop-in replacement for retiring email servers. It is also an excellent choice for environments deploying internal email servers for the first time.

The same DNS MX record change or destination NAT rule change on the firewall is needed to redirect all inbound email traffic to FortiMail for inspection. After inspection, FortiMail delivers the clean emails to the end-user mailboxes stored locally on FortiMail. End users use IMAP, POP3, or webmail to access their inboxes.

Along with storing user mailboxes, FortiMail running in server mode provides a complete group calendar, resource scheduling, webmail, and other advanced features.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can set up server mode FortiMail by setting a MX record to point to an external IP address that has a DNAT rule pointing to FortiMail. If FortiMail receives an email for a protected domain and configured email box, it scans and stores the email until the user connects with webmail, POP3, or IMAP to retrieve the email from FortiMail.

To handle outgoing email, configure the local email user clients to use FortiMail as their outbound SMTP server. FortiMail can then authenticate outgoing email.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Transparent Mode

- Physically located on the SMTP path
- Intercepts email, even though destination IP address is not FortiMail
- DNS MX record or DNAT rules are not required to point to FortiMail
- Very little additional configuration needed on the network
  - FortiMail scans mail as it is passes through
  - No additional network configuration necessary
  - Easy to configure and scan email for multiple domains

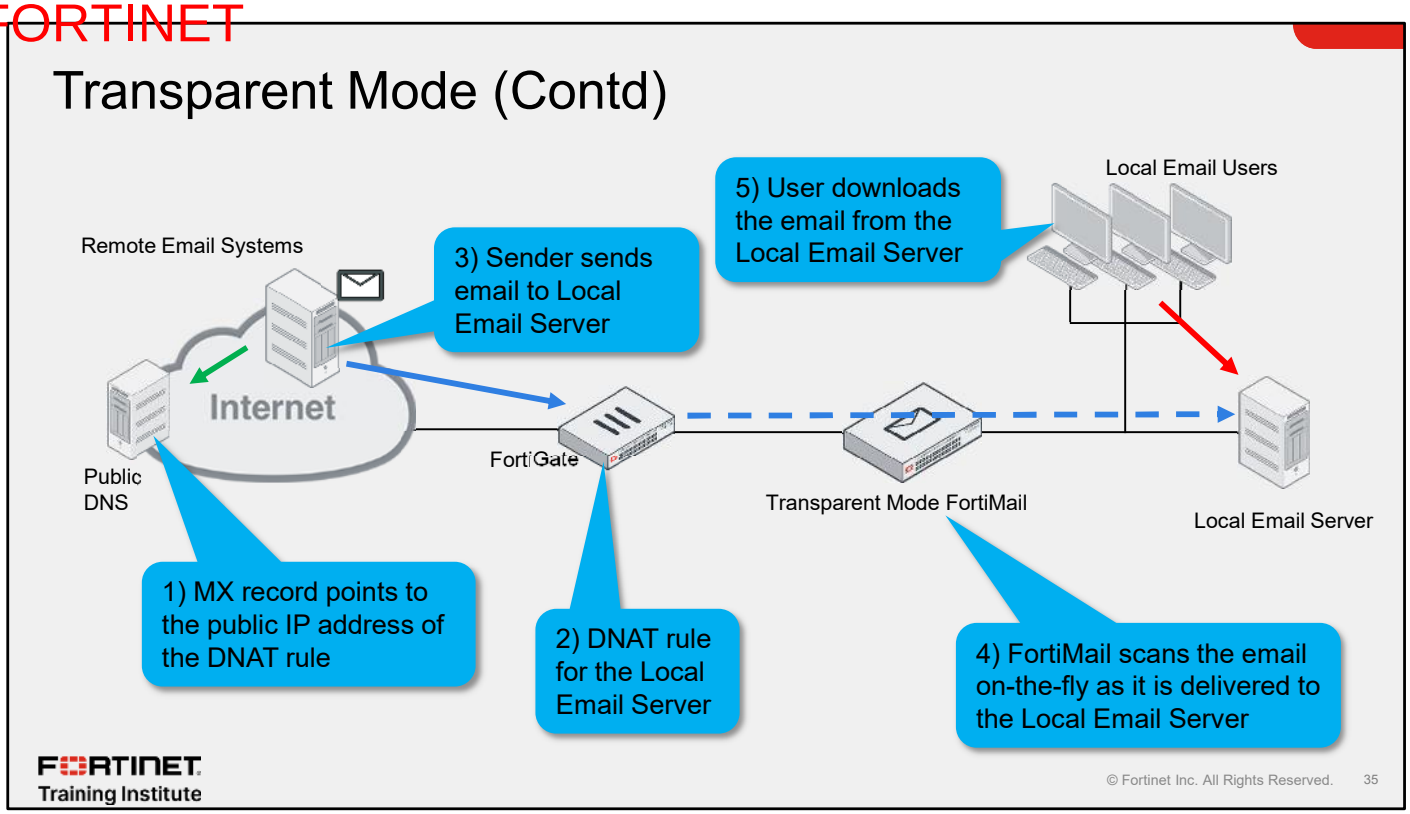
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 34

In transparent mode, FortiMail is physically located on the email path to intercept email traffic transparently for inspection. When operating in transparent mode, FortiMail isn't the intended IP destination of the email; and therefore, no DNS MX record or DNAT rule change is required. This allows you to deploy FortiMail in environments where you don’t want to or cannot change IP address and DNS MX records. Transparent mode is often used in large MSSPs or carrier environments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



As long as the email traffic is routed through the FortiMail device, it is able to scan and filter email as it is delivered and sent from local email servers. FortiMail does not need additional DNS MX records and it can protect multiple email domains.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which three modes are FortiMail operating modes? (Choose three.)
   - ✓ A. Server mode
   - ✓ B. Transparent mode
   - C. NAT/Route mode
   - ✓ D. Gateway mode
   - E. Proxy mode

2. Which type of environments often use FortiMail running in transparent mode?
   - A. Small-to-medium businesses (SMBs)
   - ✓ B. Internet service providers (ISPs)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 36

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- SMTP and DNS Roles
- Mail Flow
- Email Transmission and Retrieval
- Operating Modes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 37

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Review

- ✓ Identify SMTP roles
- ✓ Describe the importance of DNS in email exchanges
- ✓ Describe how email flows using SMTP
- ✓ Describe SMTP messages and the message exchange process
- ✓ Differentiate between SMTPS and SMTP over TLS
- ✓ Differentiate between protocols used to send and receive email
- ✓ Choose an appropriate FortiMail operating mode

FORTINET Training Institute

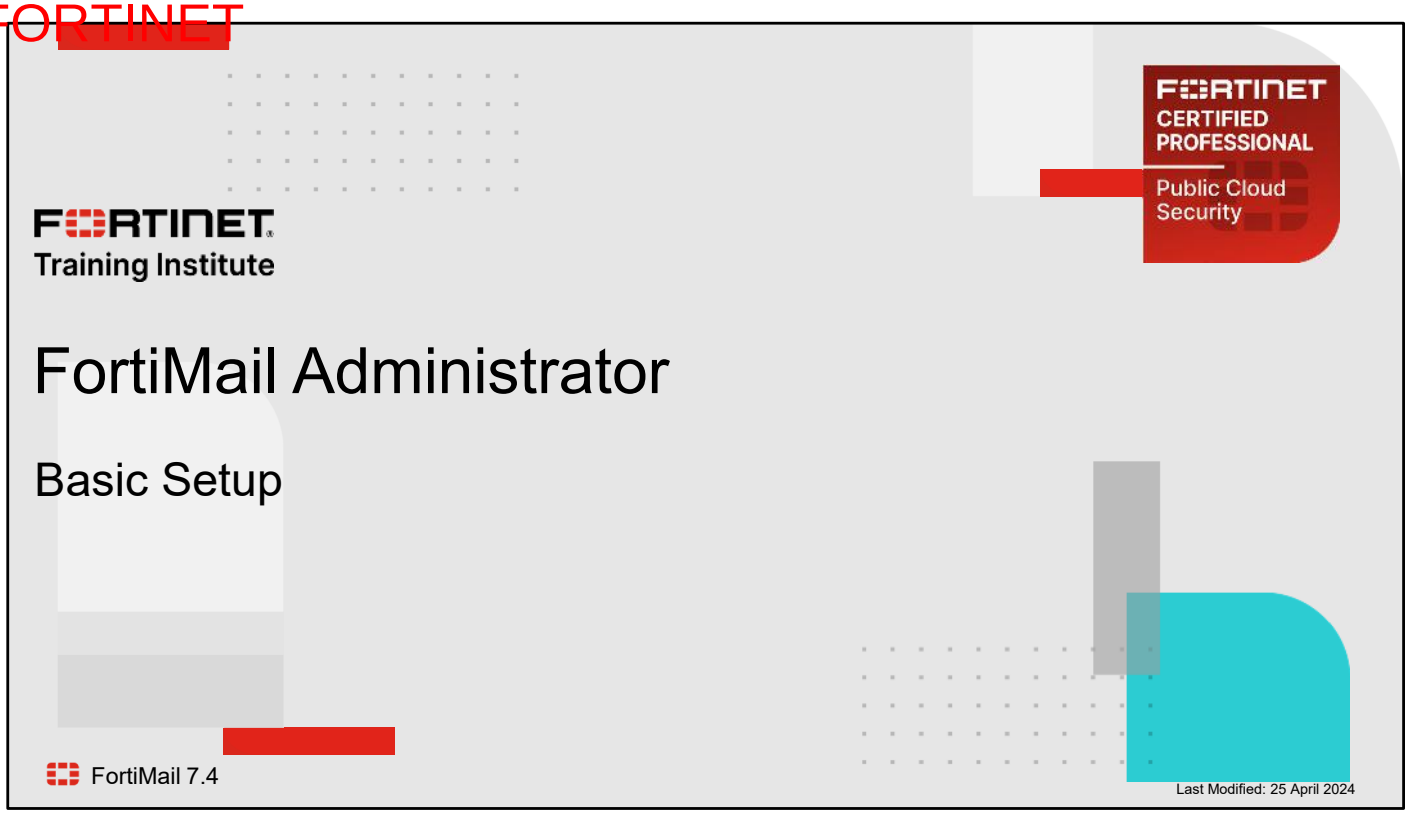
© Fortinet Inc. All Rights Reserved. 38

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about basic email concepts, and gained an understanding of SMTP and FortiMail operating modes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lesson, you will learn how to configure basic settings for your FortiMail deployments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Overview

- Navigating the GUI
- System Settings and Administrative Options
- Protected Domains
- User Management
- Email Flow Management

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 2

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Navigating the GUI

Objectives

- Access the FortiMail Management GUI
- Navigate the FortiMail GUI
- Access the CLI
- Add FortiMail to the Security Fabric

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 3

After completing this section, you should be able to achieve the objectives shown on this slide.

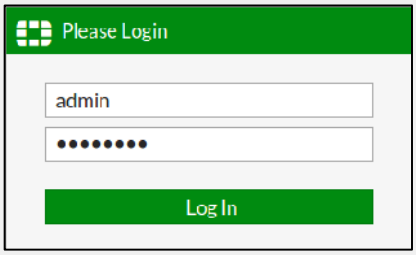
By demonstrating competence in navigating the FortiMail GUI, you will be able to access the FortiMail administrative and webmail interfaces, and navigate the GUI. You will also learn to access and use the CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

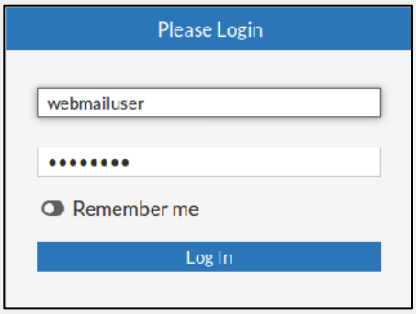
DO NOT REPRINT Brave-dumps.com
© FORTINET

Web Access

- Log in to the administration interface
  - Access the FortiMail interface:
    `https://<FortiMail FQDN or IP>/admin`



- Log in to the webmail interface
  - Access the user inbox in server mode, and the quarantine mailbox in gateway and transparent modes:
    `https://<FortiMail FQDN or IP>`



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

FortiMail has two web interfaces: an administration interface and webmail interface. Administration tasks can also be performed on a CLI. Most of the time, administrators use the GUI to configure and maintain FortiMail.

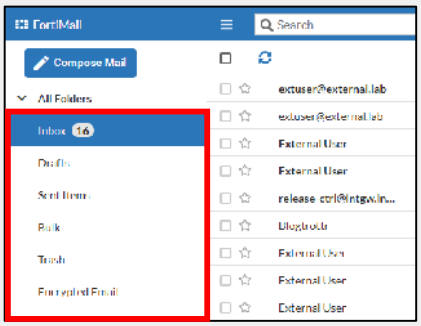
The URL formats for the two web interfaces are shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

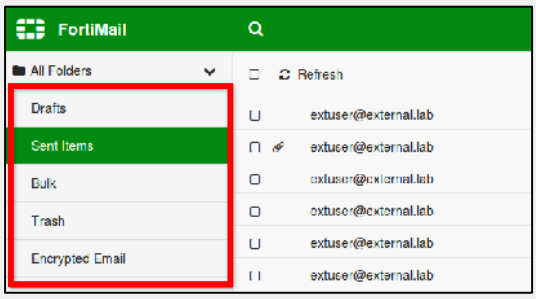
DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiMail Webmail

- The user inbox for server mode has the following folders:
  - Inbox
  - Drafts
  - Sent Items
  - Bulk
  - Trash
  - Encrypted Email



- The quarantine inbox for gateway mode has the following folders:
  - Drafts
  - Sent Items
  - Bulk
  - Trash
  - Encrypted Email



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

The quarantine mailbox for FortiMail includes additional folders, such as **Drafts**, **Sent Items**, **Trash**, and **Encrypted Email**.

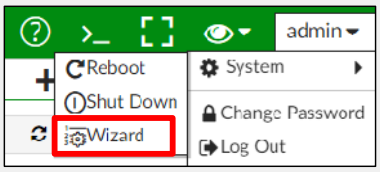
Previously, only the **Bulk** folder was available for quarantine mailboxes.

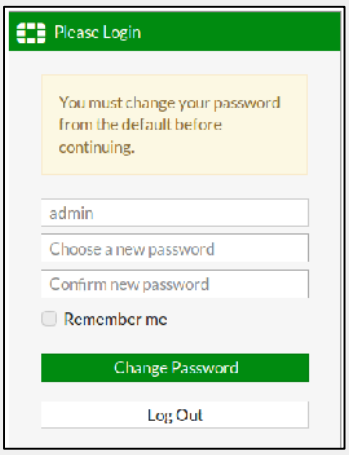
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Quick Start Wizard

- Configure the operation mode before you use the wizard.
  - **Note**: You can't select the operation mode using the quick start wizard
- Use the quick start wizard to configure the following:
  - Password for the administrator account
  - Network and time settings
  - Local host settings
  - Protected domains
  - Incoming and outgoing antispam and antivirus scan settings
  - Access control rules for SMTP relay
- Password change is enforced on first login





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

You can use the quick start wizard to complete common FortiMail deployment tasks to save time and avoid errors. The quick start wizard takes you through configuring basic settings.

When you log in for the first time, the GUI will enforce a password change.

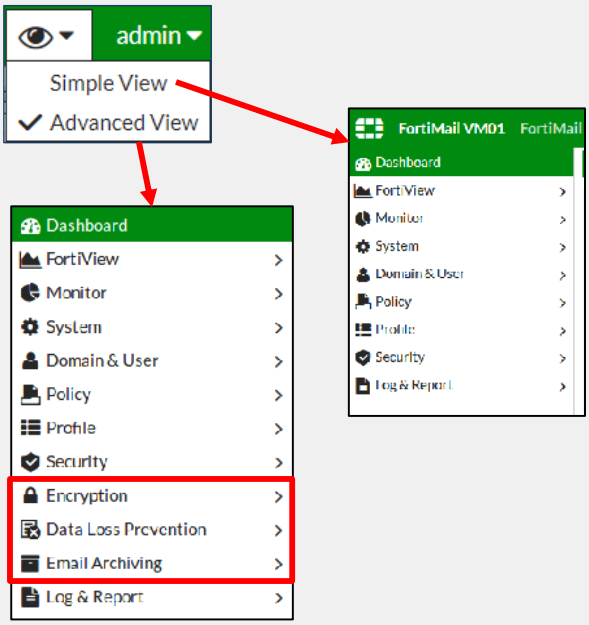
Note that you can't use the quick start wizard to select the operation mode, and that when changing operational modes most configurations are reverted to default. Because of this, you should select the operation mode before launching the wizard.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Simple and Advanced View

- Simple View
  - Commonly used options only
  - Day-to-day operation
- Advanced View
  - Complete set of menu options



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

The FortiMail GUI has two display views: advanced view and simple view. The default view is simple view.

In advanced view, all configuration menu items are visible. Simple view displays only the features and functions that you use most commonly for daily operation and maintenance. Switching between advanced view and simple view affects only what the GUI displays—the configuration doesn't change.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

CLI Syntax

- Similar to the FortiOS syntax, but not used as often for configuration tasks on FortiMail
- Very few configuration tasks require you to use the CLI
- See the CLI Reference Guide in the Fortinet Document Library at `docs.fortinet.com`

Dashboard > Console

```
FortiMail # get system status
Version:                        FortiMail-VM v7.4.1(GA-Feature), build565, 2023.09.28
Architecture:                   64-bit
Serial-Number:                  FEVMSLTM22000111
BIOS version:                   n/a
VM Registration:                Valid: License has been authorized
VM License File:                Subscription License
VM Resources:                   1 CPU/1 allowed, 1.9 GB RAM/1024.0 GB allowed, 249 GB Disk/1024 GB allowed
Log disk:                       Capacity 49 GB, Used 32 MB (0.07%), Free 49 GB
Mailbox disk:                   Capacity 198 GB, Used 1058 MB (0.53%), Free 197 GB
Filesystem mode:                Read-Write
Hostname:                       FortiMail
Operation mode:                 Server
HA configured mode:             Off
HA configured role:             Off
HA effective role:              Off
FIPS-CC status:                 disabled
Strong-crypto:                  enabled
Distribution:                   International
Branch point:                   565
Virus DB:                       90.02315(2022-05-15 08:39)
Extended DB:                    Disabled
AntiSpam DB:                    7.00545(2023-01-30 23:50)
GeoIP DB:                       2.00125(2022-05-05 18:05)
Certificate Bundle:             1.00034(2022-04-26 17:08)
Uptime:                         0 days  1 hours  12 minutes
Last reboot:                    Sun Dec 10 23:51:50 EST 2023
System time:                    Mon Dec 11 01:04:19 EST 2023
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

The FortiMail CLI syntax is similar to the FortiOS syntax, however, you can configure most of the configuration through GUI. You need to use the CLI for those features that are not commonly used, or you need specialized knowledge about the feature before you configure it.

See the *CLI Reference Guide* in the Fortinet Document Library at `docs.fortinet.com`.

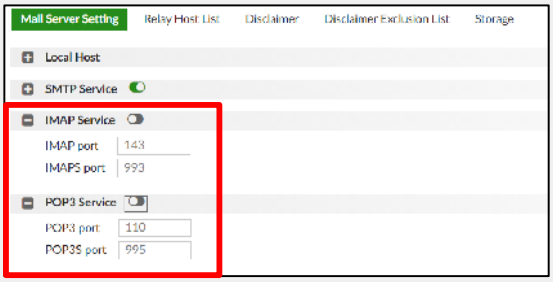
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Disable Unused Services

- To make sure FortiMail complies with information security standards, disable the local POP3 and IMAP services if not being used
- From GUI:

System > Mail Setting > Mail Server Setting



- From CLI:

```
config system mailserver
     set pop3-service <enable|disable>
     set imap-service <enable|disable>
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

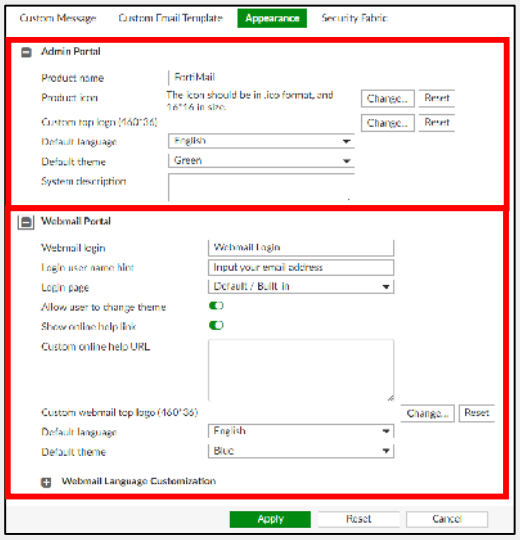
You can use the CLI or the GUI to disable cleartext POP3 and IMAP services to make sure FortiMail complies with information security standards.

Vouchers & Dumps are Available | WhatsApp +201224560923

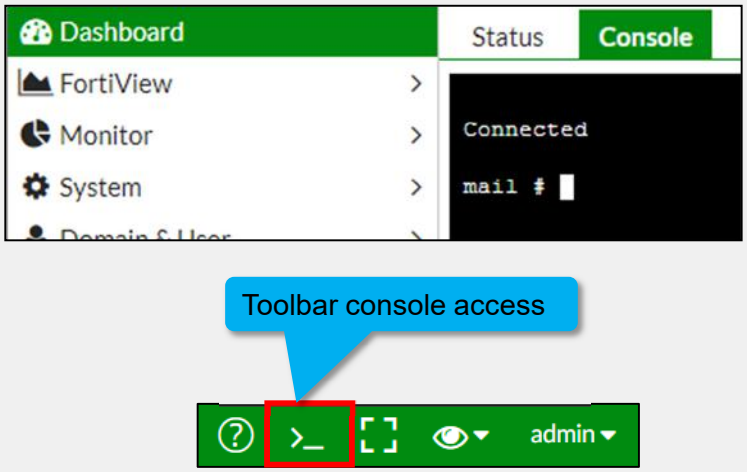
DO NOT REPRINT Brave-dumps.com
© FORTINET

User Interface Customization and Console

System > Customization > Appearance



Dashboard > Console



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

You can customize elements of both the administration and webmail GUIs to apply alternate branding, color themes, default languages, and so on.

Because you have already authenticated by logging in to the GUI, you can access the CLI with a single click using the dashboard console tab or toolbar button.

Alternatively, you can access the CLI using SSH in a separate SSH client.

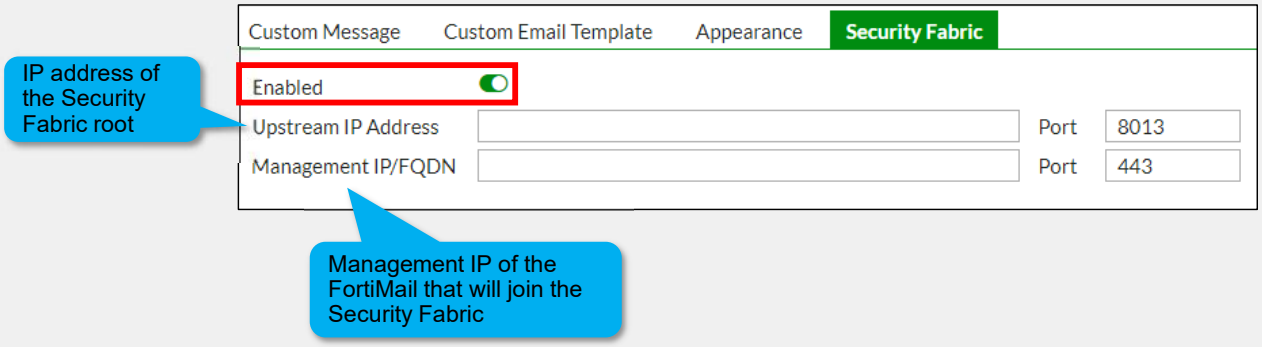
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Fortinet Security Fabric

- Add FortiMail to an upstream FortiGate
- Centrally view system information and various mail-related statistics on root FortiGate

FortiMail: **System** > **Customization** > **Security Fabric**



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

You can integrate FortiMail into the Security Fabric. The root FortiGate can then establish an administration connection to FortiMail using the IP address and port number specified.

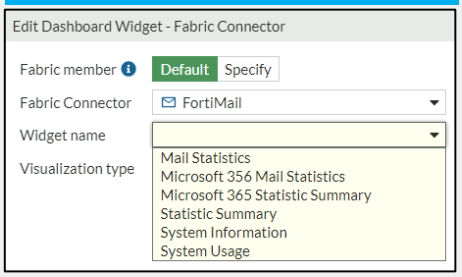
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

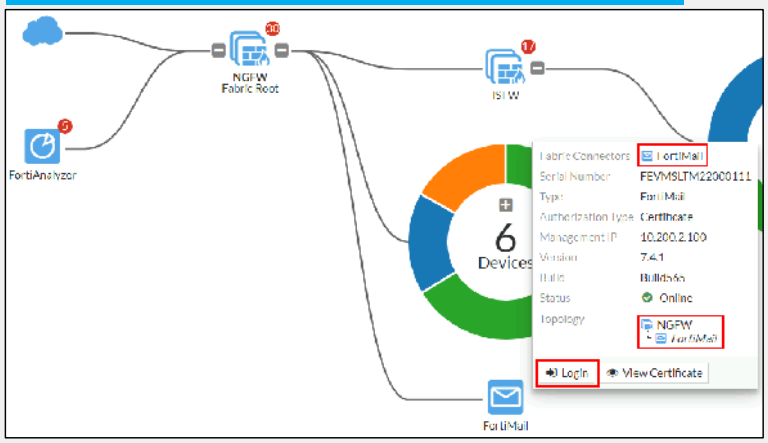
Fortinet Security Fabric (Contd)

- Add a dashboard to monitor FortiMail system information and various mail-related statistics

FortiGate: **Dashboard** > **Status**



FortiGate: **Security Fabric** > **Physical Topology**



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

You can use the **Fabric Connector** widget on the FortiGate GUI to display FortiMail system information and mail statistics.

You can integrate FortiMail with other Fortinet products, as well as third-party virtual and cloud platforms, to help establish a seamless Security Fabric across the entire attack surface. FortiMail antispam processing helps offload other devices in the Security Fabric that would typically carry out this process.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. What is the default GUI display view?
   A. Advanced view
   ✓ B. Simple view

2. Which feature can you *not* configure using the Quick Start Wizard?
   A. Administrative password
   ✓ B. Operation mode

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Navigating the GUI
- System Settings and Administrative Options
- Protected Domains
- User Management
- Email Flow Management

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

Good job! You now understand how to navigate the GUI.

Now, you will learn about system settings and administrative options.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

System Settings and Administrative Options

Objectives

- Select the operation mode
- Configure network interfaces, DNS, routes, system time, and a host name
- Configure local and remote authentication for administrator accounts
- Define levels for administrator account permissions
- Configure administrator options

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in system settings and administrative options, you will be able to select the FortiMail operation mode and configure basic network settings. You will also learn about various administrative options, such as setting up an administrator account and permissions.

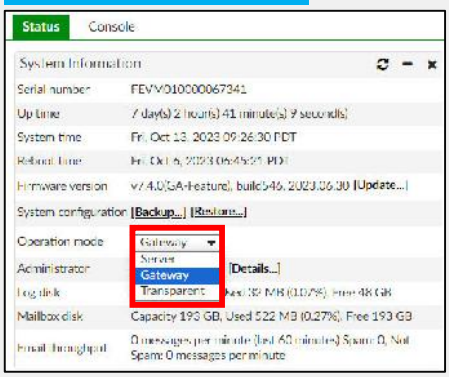
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

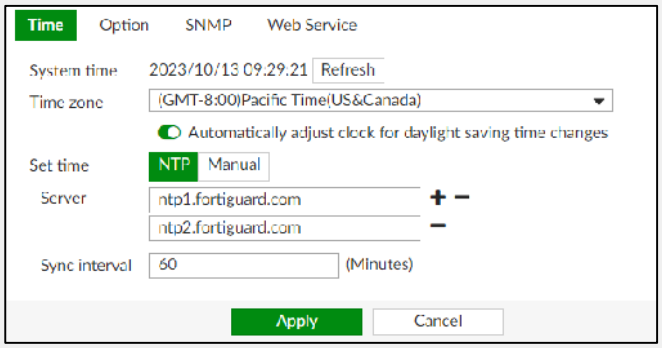
Operation Mode and NTP Synchronization

- The default operation mode is gateway mode—other modes are server and transparent mode
- Set up operation mode during initial setup
- Configure time zone for accurate timestamps in logs and for MTA functionality

Dashboard > Status



System > Configuration > Time



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

The default operation mode is gateway mode. The other modes are server mode and transparent mode.

If you change the operation mode, FortiMail reboots and most settings return to factory default values.

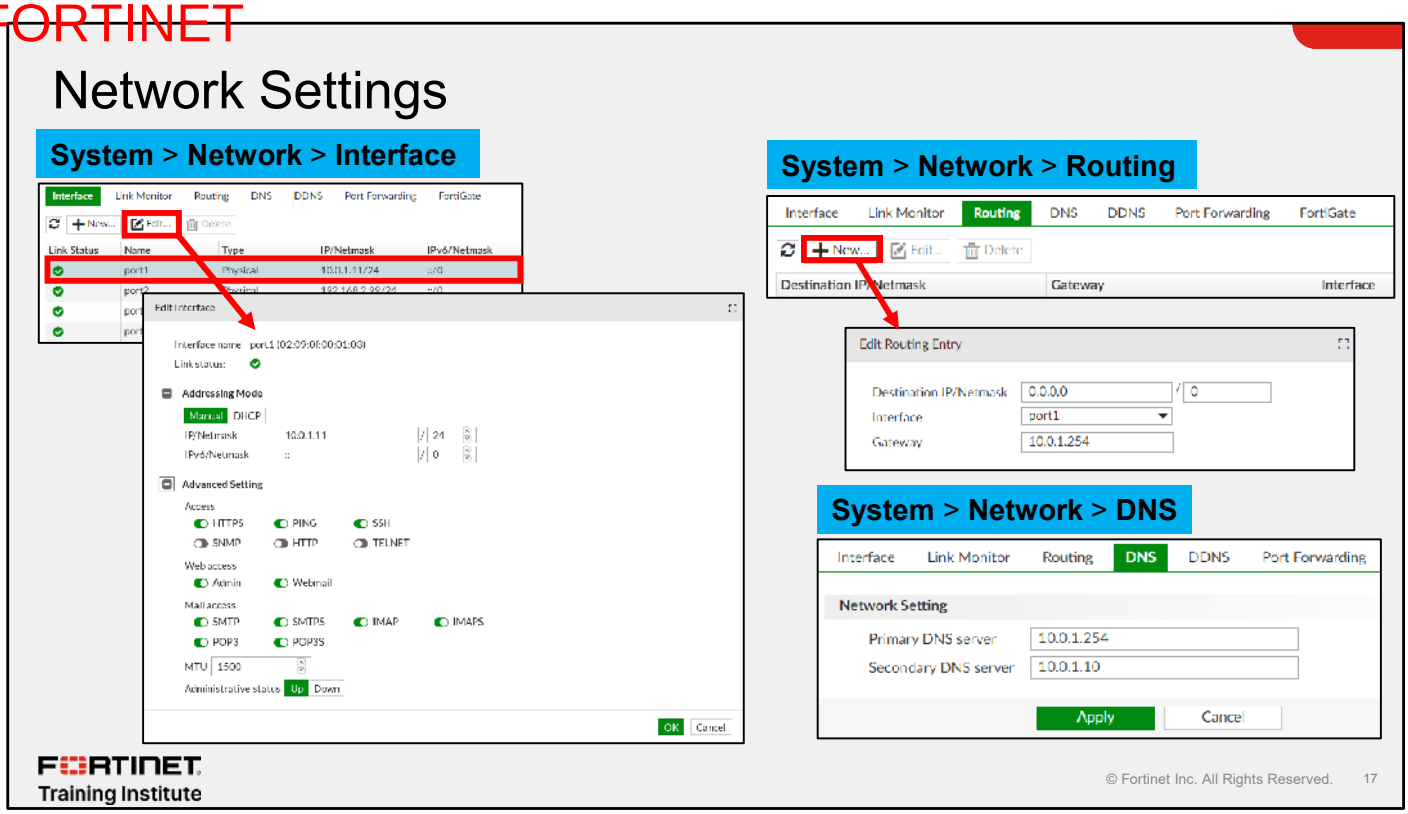
Because the operation mode affects how FortiMail functions, you should select the operation mode as soon as possible when you perform the initial setup. If you plan to use the quick start wizard to begin the configuration, you must set the operation mode before you use the quick start wizard.

Before you select server or gateway for the operation mode, verify that your public DNS MX records are up to date and are pointing to the correct IP address.

Accurate date and time values are important for timestamps in logs, mail transfer agent (MTA) functionality, and SSL/TLS transactions. FortiMail applies timestamps to various message headers that get processed by other external MTAs along the way. You can configure the date and time in FortiMail manually, but to maintain accuracy, sync FortiMail with an NTP server instead.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Typically, in gateway and server modes, only one interface is active. In transparent mode, depending on the deployment topology, multiple interfaces may be active.

The default IP address and subnet mask for the **port1** interface is `192.168.1.99/24`.

FortiMail also supports IPv6 and DHCP addresses. You can select an access option to enable or disable access to FortiMail using HTTP, HTTPS, PING, SSH, SNMP, and TELNET.

By default, there are no default or static routes configured on FortiMail. You must configure at least one default route to the internet to make sure FortiMail connects correctly to FortiGuard, and to make sure email traffic flows correctly. You can configure more static routes as needed to accommodate networks that have multiple gateways. The fields in the **New Routing Entry** dialog support both IPv4 and IPv6 addresses.

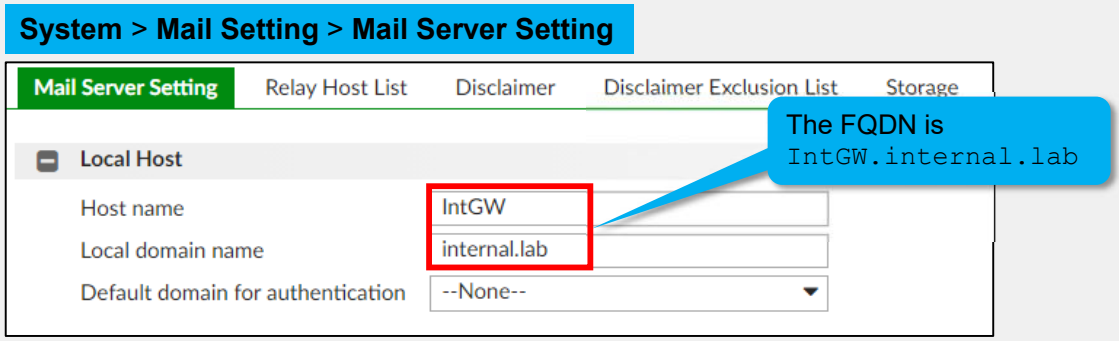
By default, FortiMail is preconfigured with FortiGuard DNS servers. DNS plays a vital role in email transmission as well as FortiGuard connectivity; therefore, the choice of DNS servers can have a significant effect on the performance of FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Domain Name

- **Host name** + **Local domain name** = fully qualified domain name (FQDN)
- Used in quarantine reports, SMTP banner, deliver status notification (DSN) emails, and so on
- FQDN should be globally resolvable, especially if FortiMail is an outbound MTA, with a DNS address (A) and pointer (PTR) record



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

By default, the system host name is set to the device serial number. This causes the device serial number to show up in the SMTP banner during regular SMTP sessions. You should set the host name and local domain name to create a unique FQDN. The FQDN of a FortiMail instance is used in a variety of places. Many functions, such as email quarantine, won't function unless the host name can be resolved correctly. For correct external MTA connectivity, you must set the FortiMail FQDN to be externally resolvable both forward and backward.

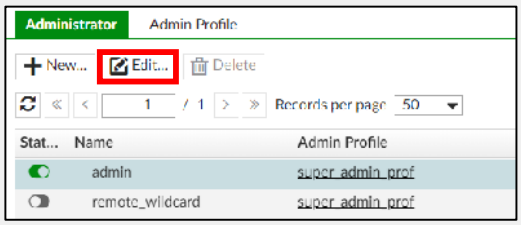
Vouchers & Dumps are Available | WhatsApp +201224560923

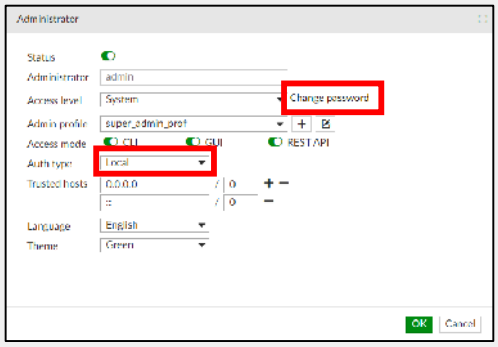
DO NOT REPRINT Brave-dumps.com
© FORTINET

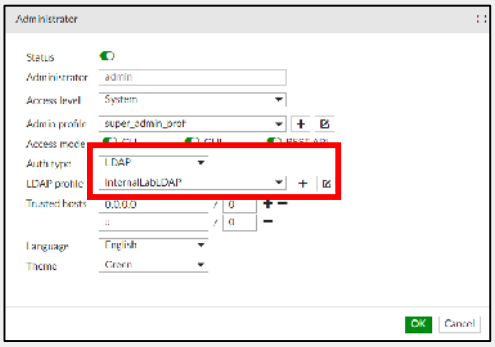
Administrator Accounts

- Change the password to secure access to the device
- Configure remote authentication for the administrator account
- Supports RADIUS, PKI, LDAP, and single sign-on authentication

System > Administrator > Administrator







FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

FortiMail is configured with a default admin user with an empty password field. You must create an admin user password to secure the device from unauthorized users.

You can set the access profile and domain to restrict administrators to certain sections of the GUI, or to specific domains. You can set the authentication type to local or remote, using RADIUS, LDAP, PKI, or single sign-on. For remote authentication types, you must also configure an additional profile that defines the details of the authentication.

You can configure trusted hosts to restrict each account to specific IP subnets or addresses. You can also set a color theme and language for the GUI for each administrator.

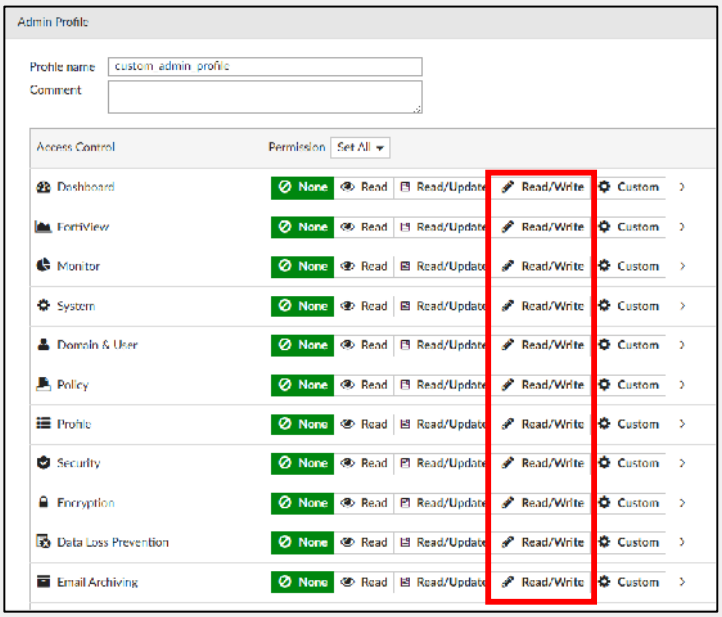
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Admin Profile

- Use access profiles to:
  - Control which configuration elements an administrator can access
  - Define the level of permissions in each element
- Applies to both the GUI and CLI

System > Administrator > Admin Profile



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

You must associate each administrator user account with an admin profile that determines which areas an administrator can access and provides permissions to modify elements within those areas. The default **super_admin_prof** admin profile is assigned to the default admin account. You can't remove or modify the **super_admin_prof** admin profile.

You can create and modify a custom admin profile to tailor which areas of FortiMail an associated administrator can access.

You can also apply admin profile levels dynamically through RADIUS. You will explore RADIUS and other authentication profiles in more detail in another lesson.

The **Read/Update** option provides the ability to modify a table entry without the ability to add or delete it.

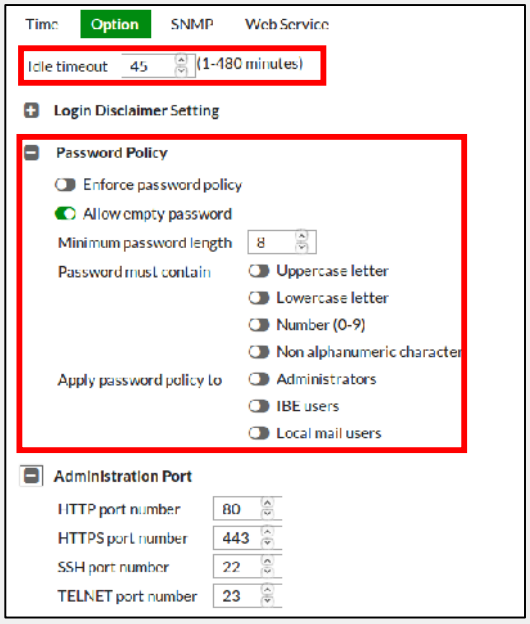
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Enforcing Password Policies

- Enforce complex passwords
- Applies to administrators, webmail, and identity-based encryption (IBE) users
- Modify the default value of 45 minutes for the idle timeout
- Enable a login disclaimer for admin, webmail, or IBE
- Modify default service ports for HTTP, HTTPS, SSH, and TELNET
- Applies to both the GUI and the CLI

System > Configuration > Option



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

You can create a single, global password policy to enforce complex passwords, and you can choose which admin users, local mail users, and IBE users to apply the policy to. The authentication server usually enforces the password policies for non-local mail users (LDAP and others).

To make sure FortiMail complies with information security standards, you can reduce the idle timeout and enable a login disclaimer. You can set the disclaimer to appear before or after the user logs in. You can also set the disclaimer to appear when an admin, webmail, or IBE user logs in. When you set the disclaimer for admin users, it also appears when the admin users access the CLI using SSH or TELNET.

You can also change the administration ports on the **Option** tab. If you change the default ports, you must update the applicable port forwarding rules on your organization's firewall to reflect the change.

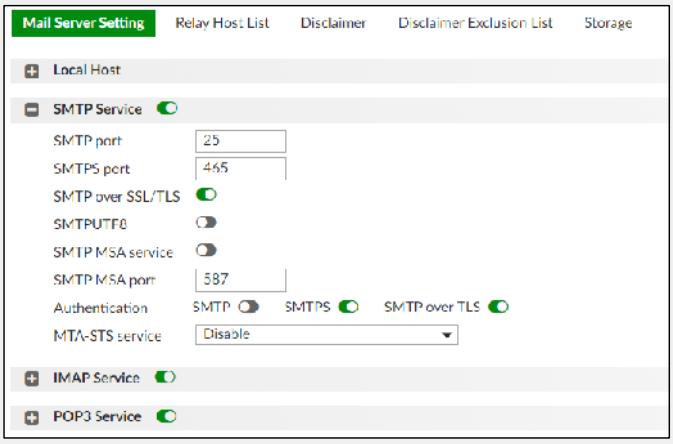
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SMTP Service Settings

- Enable or disable SMTP service
- Designate ports and security settings
- SMTPUTF8 support for internationalized email addresses as defined in RFC 6531

System > Mail Setting > Mail Server Setting



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

You can enable SMTP services and configure the port settings you want for the SMTP and SMTPS services on the **Mail Server Setting** page, as well as SMTP over SSL/TLS. SMTPUTF8 provides support for internationalized email addresses.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiMail Deployment Options and Integrations

Devices	Virtual machines	Public cloud	Integration support
Five models Email Routing 50k—3.5M per hour FortiGuard AS and AV support 40k—2.6M per hour Protected email domains: 20—3000	Four platforms • VMware • Hyper-V • KVM • Citrix XenServer	Five platforms: • AWS • Azure • Google • Oracle • Alibaba	Microsoft 365 Google Workspace

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

FortiMail provides a variety of device, VM, and public cloud deployment options to offer flexibility and scalability. This slide shows the available VMs and supported cloud platforms.

Note that the Microsoft 365 global administrator role is required to configure Microsoft 365 on FortiMail.

Before you can integrate FortiMail with Microsoft 365 or Google Workspace, you must be connected to the server and have an account created on FortiMail. Account creation for both Microsoft and Google is detailed in the *FortiMail Administration Guide*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. What is the default operation mode on FortiMail?
   A. Server mode
   ✓ B. Gateway mode
   C. Transparent mode

2. Accurate date and time values are critical to which feature on FortiMail?
   ✓ A. Log timestamps
   B. Route selection

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Navigating the GUI
- ✓ System Settings and Administrative Options
- Protected Domains
- User Management
- Email Flow Management

FORTINET Training Institute

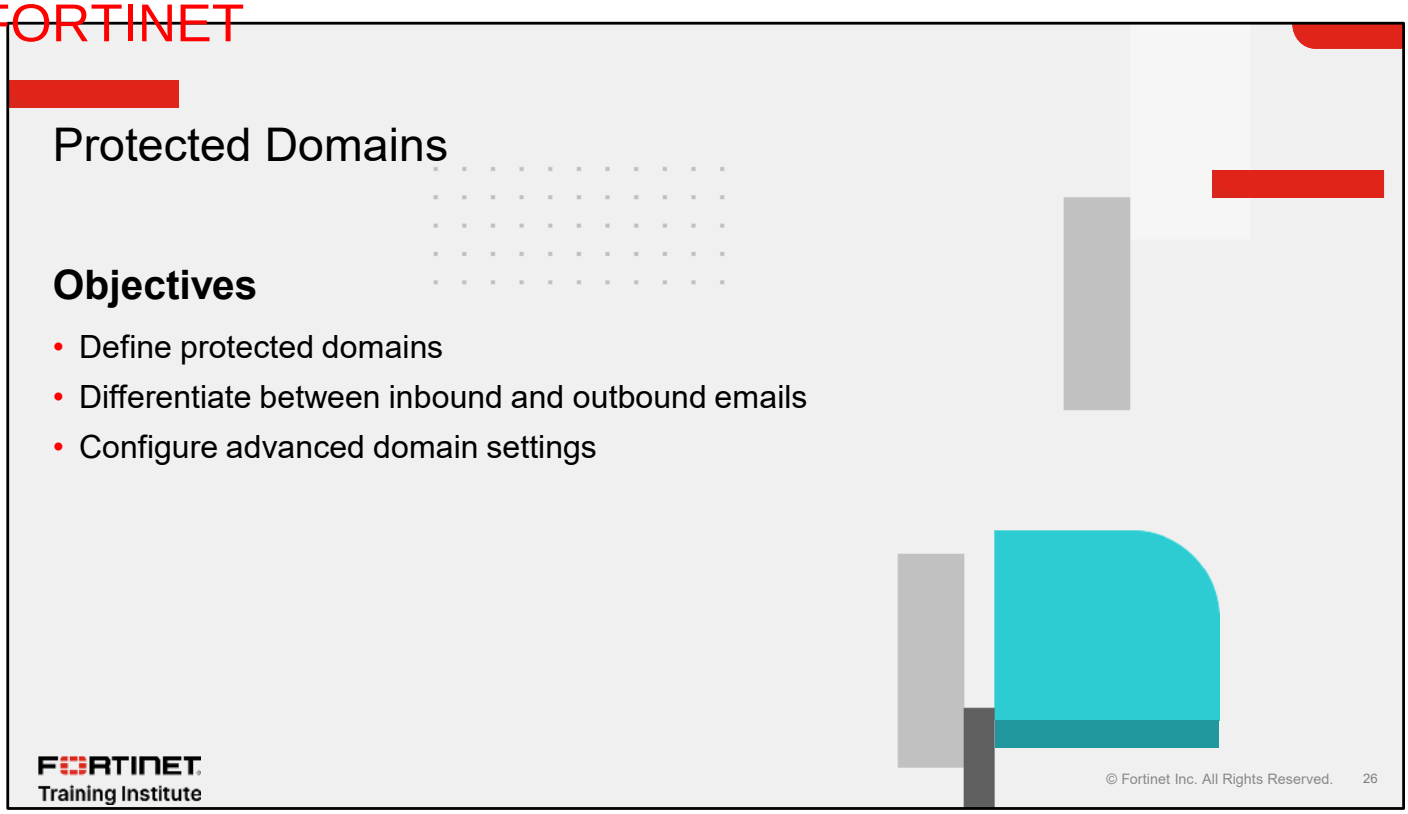
© Fortinet Inc. All Rights Reserved. 25

Good job! You now understand system settings and administrative options.

Now, you will learn about protected domains.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

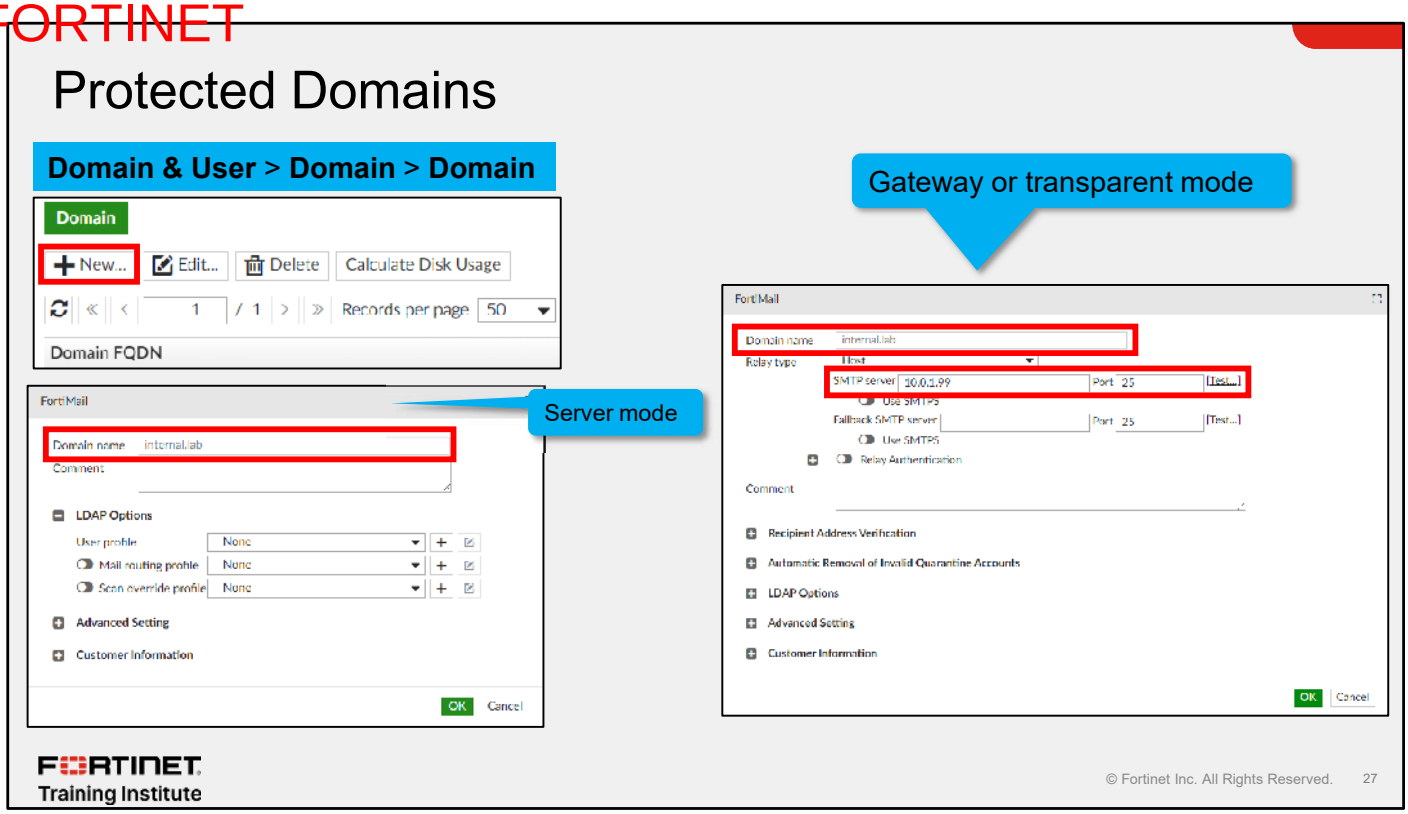


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in protected domains, you will be able to define a protected domain and configure various advanced domain settings. You will also learn how FortiMail differentiates between inbound and outbound emails.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To create a protected domain, you must select different options, depending on the operation mode of FortiMail. For gateway mode, you must define the domain and the destination SMTP server for email in that domain. For transparent mode, if you define the domain, then you must specify the destination SMTP server. For server mode, you must define only the domain, because FortiMail is the final destination of the email message.

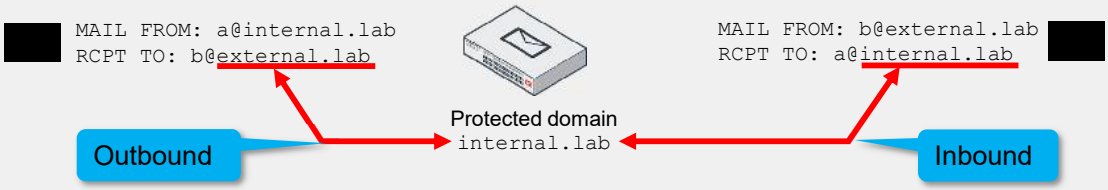
Protected domains also specify which email messages FortiMail considers to be inbound and which it considers to be outbound. An email in a protected domain is considered inbound, all other emails are outbound.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Email Direction

- FortiMail considers an email message to be inbound if the recipient domain matches a protected domain; otherwise, it is outbound



- Email direction determines FortiMail relay behavior
  - By default, FortiMail relays incoming emails
  - By default, FortiMail rejects outbound emails, unless the sender is authenticated

FORTINET Training Institute

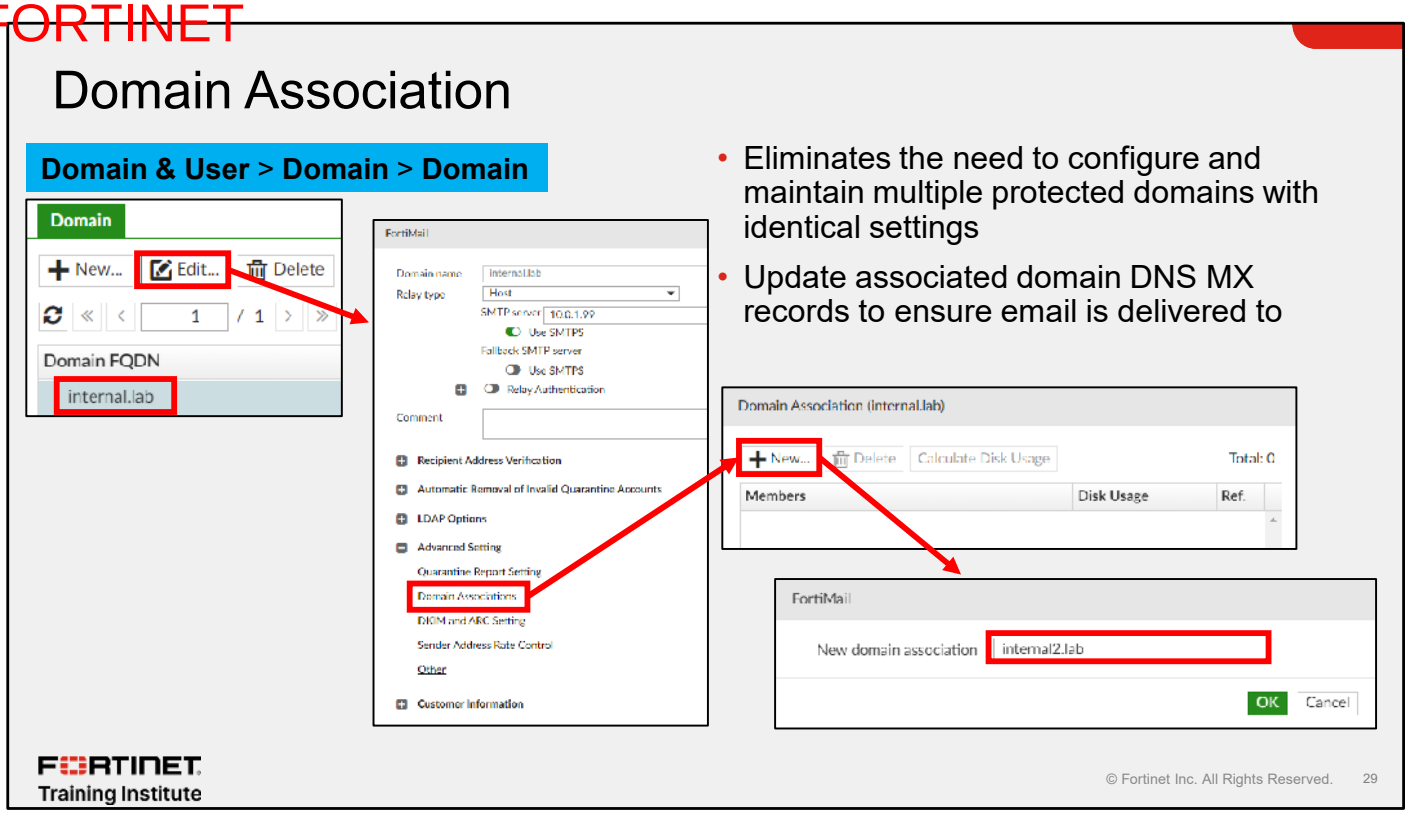
© Fortinet Inc. All Rights Reserved. 28

When FortiMail receives an email, it compares the domain part of the recipient email address with the list of protected domains. If there is a match, FortiMail considers the message to be inbound; otherwise, the message is outbound.

The direction of the email is important to FortiMail because it influences relay behavior. Inbound email is relayed by default, so no additional configuration is required to allow email into the organization. By default, FortiMail rejects outbound emails unless the sender is authenticated. This behavior is hardcoded to prevent FortiMail from being abused as an open relay.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Domain association allows multiple email domains to share a single configuration in FortiMail. For example, any recipient-based policies created for the main domain apply to the associated domains as well.

This is extremely convenient for environments that have more than one domain and you want to keep FortiMail protection consistent across all of them. This not only helps to minimize redundant configurations and speed up the deployment, but also helps to eliminate errors or drift over time in the configuration.

When adding associated domains to FortiMail, update the MX records of the domains so all inbound email is delivered to FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. When does FortiMail consider an email to be incoming?
   A. When the recipient is authenticated
   ✓ B. When the recipient domain matches a protected domain

2. What is one advantage of creating domain association?
   ✓ A. Eliminates the need to maintain multiple protected domains with identical settings
   B. Allows the creation of protected domain-specific administrator accounts

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Navigating the GUI
- ✓ System Settings and Administrative Options
- ✓ Protected Domains
- User Management
- Email Flow Management

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

Good job! You now understand protected domains.

Now, you will learn about user management.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

User Management

Objectives

- Configure and manage server mode users
- Manage gateway and transparent mode quarantine mailboxes
- Configure recipient verification

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

After completing this section, you should be able to achieve the objectives shown on this slide.

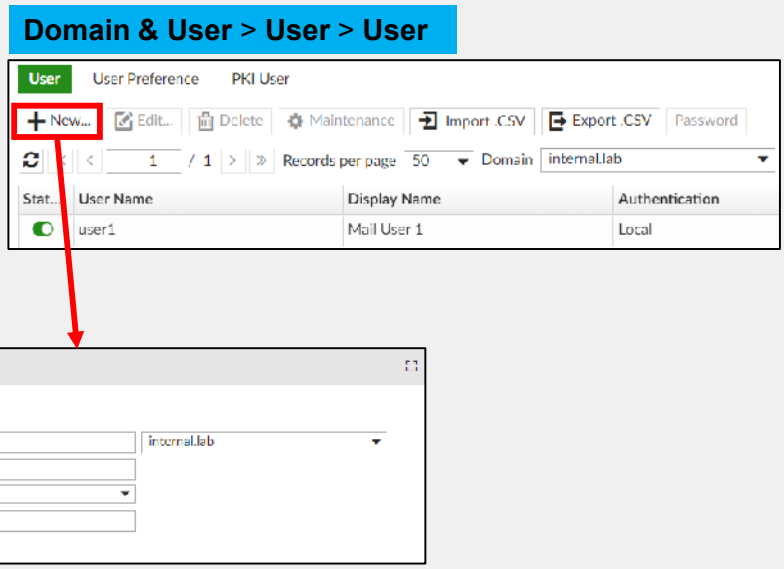
By demonstrating competence in user management, you will be able to configure and manage server mode users, gateway, and transparent mode quarantine mailboxes. You will also learn to configure recipient verification.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Server Mode Users

- When FortiMail is operating in server mode, you must define user accounts to use inboxes
- Users can authenticate locally, or from remote LDAP and RADIUS servers



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

Because user mailboxes are managed by FortiMail in server mode, you should create user account entries for each user. You can configure these user accounts to authenticate locally, or using LDAP or RADIUS. In server mode, the user inbox handles both regular email and the spam quarantine.

You can use the **User** tab to create users, while the **User Preference** tab allows you to manage user preferences. The administrator can manage user preferences using the administration interface, and the end user can manage their preferences using the webmail interface.

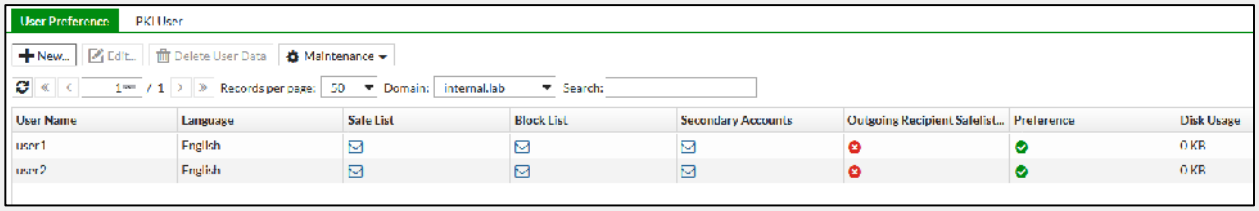
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Gateway and Transparent Mode Users

- Quarantine mailboxes are automatically created when FortiMail sends email to user quarantine
- You can manage user preferences in the administration interface as well as the end-user webmail interface

Domain & User > User > User Preference



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 34

In gateway and transparent modes, FortiMail maintains quarantine mailboxes for users. These mailboxes are created automatically when FortiMail needs to send email to quarantine as a result of spam detection.

You cannot manually create users on FortiMail when it is configured in gateway or transparent mode. You can, however, manage user preferences, such as block or allowlist entries using the administration GUI. The end user can access their quarantine mailbox and account preferences using the webmail interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Recipient Verification

- To verify a recipient email address, FortiMail can use the following features:
  - Recipient address verification
  - Automatic removal of invalid quarantine accounts
- To optimize the use of system resources, you should enable at least one of these techniques

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 35

When FortiMail is configured in gateway or transparent mode, it processes all email and attempts to relay it to the back-end server. What happens if a user account doesn't exist? In this case, the back-end server generates an error and FortiMail creates a quarantine account where the invalid user email is quarantined. Over time, this can lead to an excessive amount of storage space being used for email for invalid users.

There are two ways to deal with this: recipient address verification or automatic removal of invalid quarantine accounts. To optimize the use of storage space, you should implement at least one of these features for gateway or transparent mode deployments.

Recipient verification is built into the regular server mode email handling process; therefore, you don’t need to configure this feature for server mode deployments.

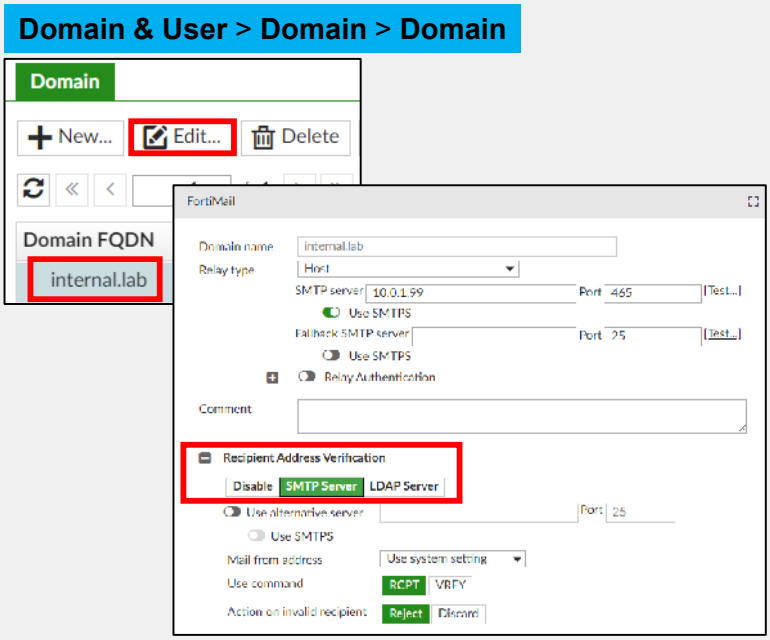
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Recipient Address Verification

- Verifies addresses provided in the `RCPT TO:` command in the SMTP envelope
  - **LDAP Server:** Queries an LDAP server. Requires an LDAP profile configuration.
  - **SMTP Server:** Queries an SMTP server using either the RCPT or VRFY command

Usually disabled on most mail servers to prevent directory harvesting attacks



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 36

Recipient Address Verification is a setting that you can configure for each protected domain entry. When you enable recipient address verification, FortiMail verifies the recipient email address after the `RCPT TO` command for each inbound email before allowing the sender to start the DATA portion of the email. If the recipient address is found to be invalid, FortiMail rejects the email. This method keeps all invalid email out of the FortiMail system, reserving storage for valid email only.

There are two methods of performing recipient address verification: SMTP and LDAP. The **LDAP Server** option requires you to configure an LDAP profile to define the LDAP server settings. The **SMTP Server** option requires the back-end server to support either the `VRFY` or `RCPT` SMTP command. Typically, `VRFY` is disabled on most mail servers to prevent directory harvesting attacks.

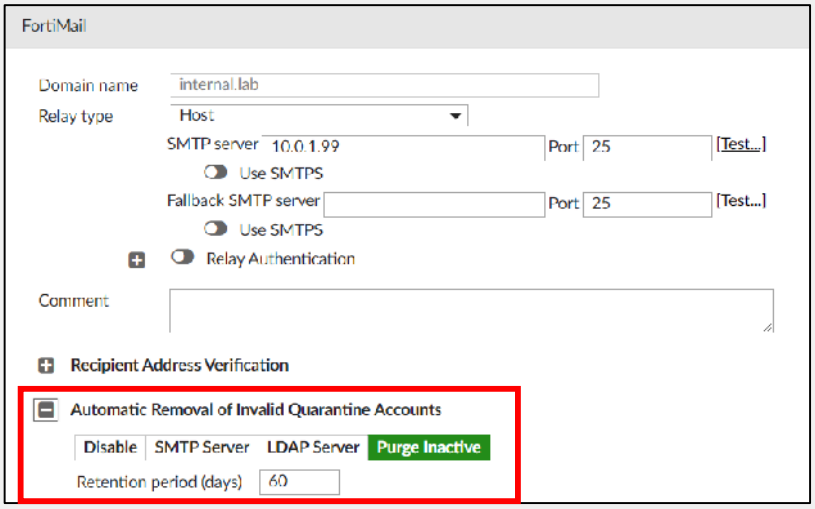
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Invalid Quarantine Account Removal

- Does not apply to FortiMail in sever mode configuration
- Applies to spam destined for invalid user accounts
- May not be necessary if **Recipient Address Verification** has been configured
- **Purge Inactive** can be used for maintaining content levels for valid accounts

Domain & User > Domain > Domain



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 37

When configured, FortiMail deletes all quarantined mail that was destined for user accounts that it cannot verify to exist. Using recipient address verification would prevent FortiMail from creating quarantine accounts for accounts that do not exist on the protected server, in which case this feature may not be necessary.

Purge Inactive cleans up accounts that have not been used for more than the designated retention period.

Vouchers & Dumps are Available | WhatsApp +201224560923

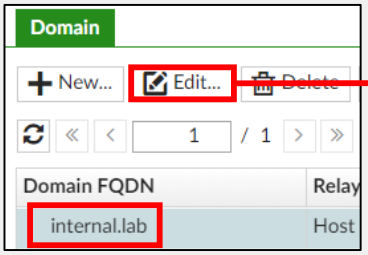
DO NOT REPRINT Brave-dumps.com
© FORTINET

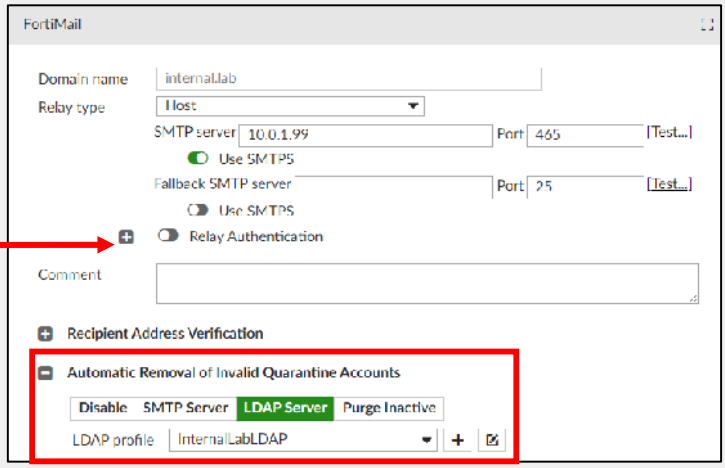
Invalid Quarantine Account Removal (Contd)

- Alternate method used to free up mail disk space by removing invalid quarantine mailboxes on a schedule
- By default, the check runs at 4:00 AM, which can be modified using the CLI

```
config antispam settings
 set backend-verify <hh:mm:ss>
end
```

Domain & User > Domain > Domain





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 38

You can use an alternate method to clean up quarantine mailboxes for invalid accounts. The **Automatic Removal of Invalid Quarantine** function removes all invalid quarantine mailboxes after FortiMail has already accepted email and created accounts for invalid accounts.

Invalid removal of quarantine uses the same options as recipient address verification: SMTP or LDAP. By default, it is scheduled to run at 4:00 am local time. If it cannot verify an account by the selected means, FortiMail purges the quarantined email. You can change the scheduled time using the CLI.

Purging of invalid quarantine accounts helps maintain storage levels on FortiMail. For example, when employees leave a company, their LDAP accounts would be removed, and this automated process would ensure their quarantine mailboxes did not continue to collect mail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which FortiMail deployment mode allows users to send and receive email through a webmail interface hosted on the FortiMail?
   A. Gateway mode
   ✓ B. Server mode
   C. Transparent mode

2. Which recipient verification method uses the VRFY command?
   ✓ A. SMTP
   B. LDAP

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 39

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Navigating the GUI
- ✓ System Settings and Administrative Options
- ✓ Protected Domains
- ✓ User Management
- Email Flow Management

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 40

Good job! You now understand user management.

Now, you will learn about email flow management.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Email Flow Management

Objectives

- Verify email flow using logs
- Manage FortiMail email queues

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 41

After completing this section, you should be able to achieve the objectives shown on this slide.

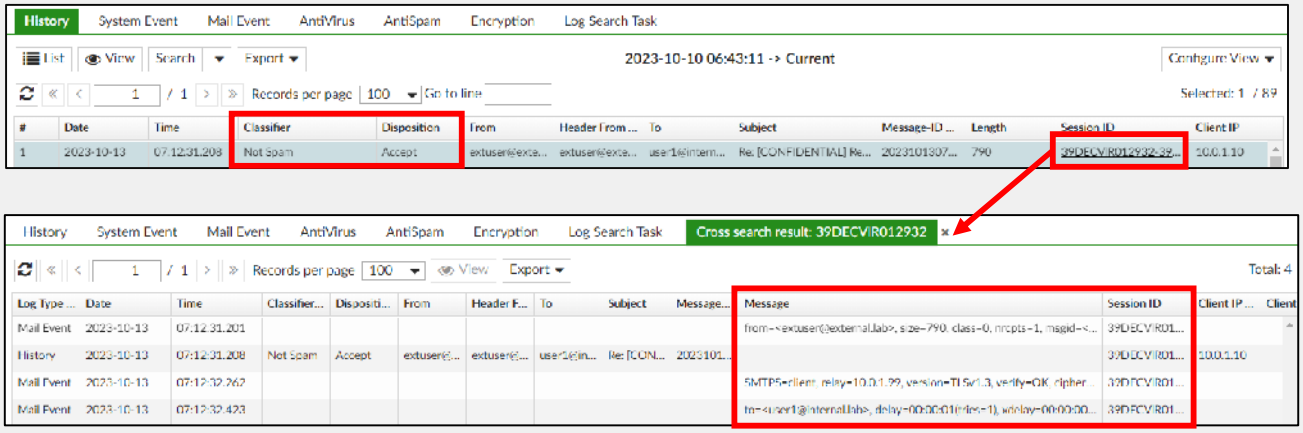
By demonstrating competence in email flow management, you will be able to verify email flow using logs, and manage FortiMail email queues when emails are not flowing because of errors.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

History Logs

Monitor > Log > History



FORTINET Training Institute
© Fortinet Inc. All Rights Reserved. 42

The logs shown on the **History** tab provide an overview of what happened to an email. A successful email transmission is classified as **Not Spam** and shows **Accept** in the **Disposition** column. For more detail, click the **Session ID** link, which gathers and displays all individual logs generated by an email. You will learn more about log review in another lesson.

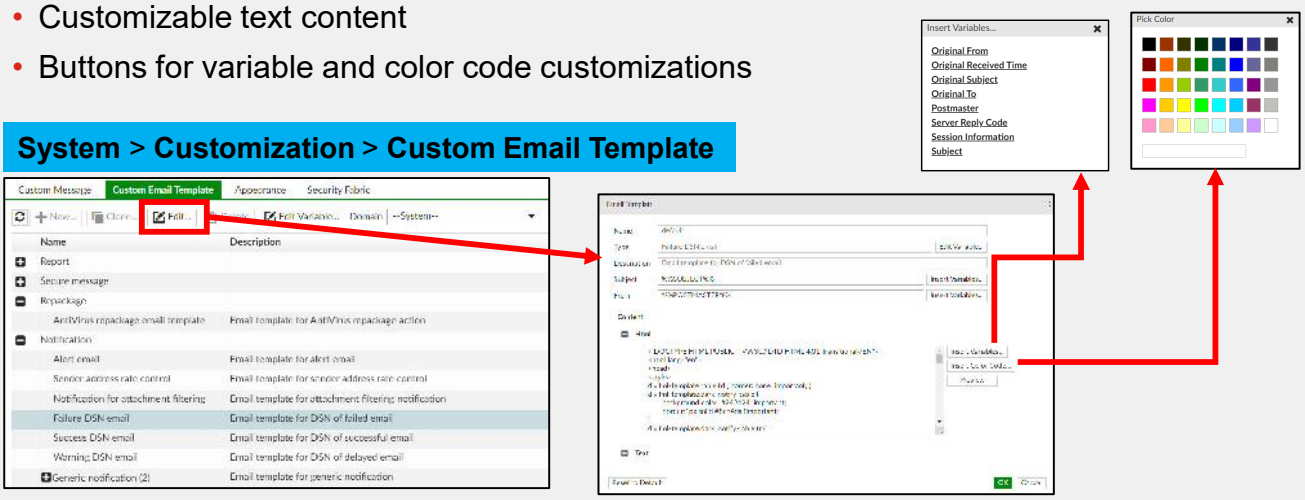
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Delivery Status Notification Template Customization

- Delivery status notification (DSN) message customization
- Customizable HTML content with preview
- Customizable text content
- Buttons for variable and color code customizations

System > Customization > Custom Email Template



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 43

You can customize the DSN email templates for both HTML and text content. Convenient buttons allow you to preview HTML updates on the fly, insert variable tags anywhere in the message, or change the color of new or existing content.

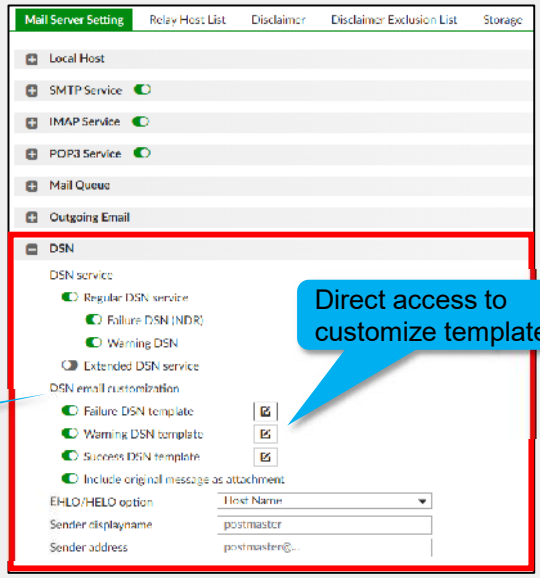
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

DSN Settings

- Enable for DSN generation
- Update users of email delivery delays or delivery failures
- Customized DSN emails can be assigned to three types of DSN messages
  - Failure
  - Warning
  - Success
- Direct access to DSN templates for customization

System > Mail Setting > Mail Server Setting



Direct access to customize templates

Provides more granular control over notifications

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 44

If you want FortiMail to issue DSNs to users, you must first enable the **Regular DSN service** setting. When email delivery is delayed or has failed, FortiMail sends notifications to the users. Customized DSN messages can be applied for failure, warning, and success messages. You can access the template customization view directly from the settings page.

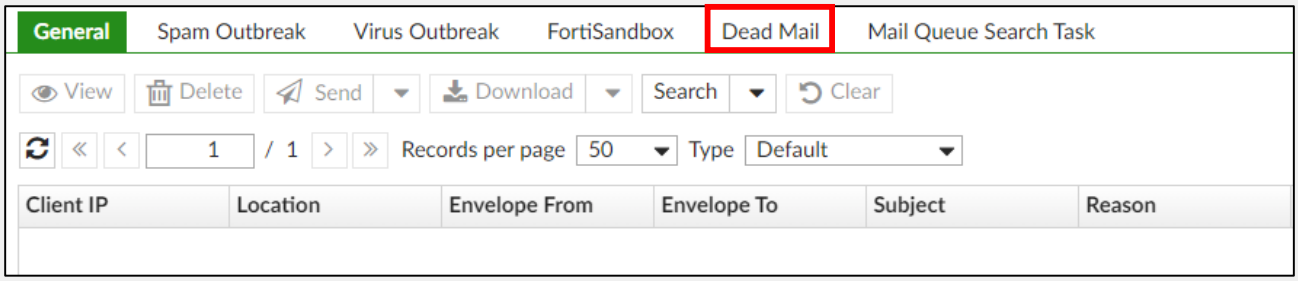
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiMail Queues

- The **Mail Queue** holds email that can't be sent immediately
  - Usually because of temporary circumstances, such as the remote MTA is busy, or temporary loss of network connectivity
- The **Dead Mail** queue is used to store the DSNs of email that has failed transmission permanently
- Behavior is controlled by mail queue timers

Monitor > Mail Queue



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 45

It might not always be possible to deliver email immediately. Delayed messages must be stored somewhere so that the MTA can attempt to resend them later. The Mail Queue holds email that can't be sent immediately. This is usually because of temporary circumstances, such as the remote MTA being busy, or the temporary loss of DNS or network connectivity.

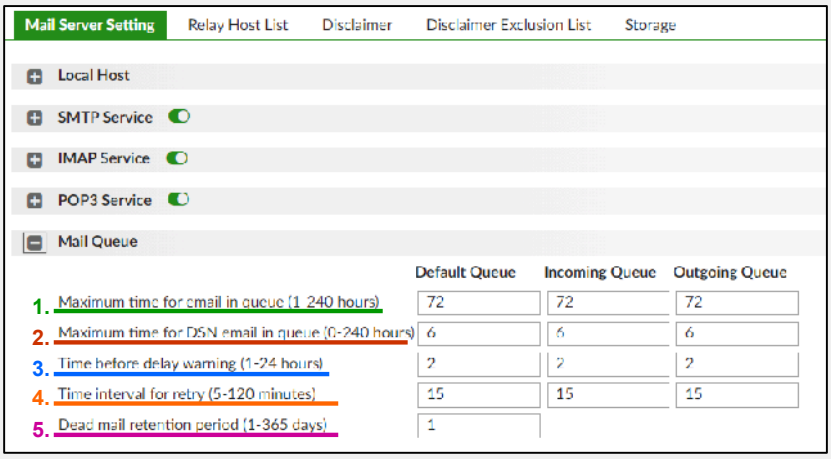
If a message can’t be delivered, it’s placed in the Dead Mail queue. Most often, messages end up in the Dead Mail queue because of permanent failures. Email moves from the Mail Queue to the Dead Mail queue after the MTA has exhausted the maximum retry period without resolution of the issues that caused the email to fail transmission in the first place.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Mail Queue Timers

System > Mail Setting > Mail Server Setting



1. The maximum number of hours that delayed emails can remain in the queue

2. The maximum number of hours that an undeliverable DSN can remain in the queue

3. The number of hours that must expire before the email is considered delayed and a DSN is sent to the sender

4. Retry interval in minutes

5. The number of days an email can stay in the **Dead Mail** queue

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 46

When messages are placed in the mail queue, several timers are used to specify how the email is handled, and when to send DSNs.

The **Maximum time for email in queue** value defines the maximum number of hours that delayed emails can remain in the queue.

The **Maximum time for DSN email in queue** value defines the maximum number of hours that an undeliverable DSN can remain in the queue.

The **Time before delay warning** value defines the number of hours that must expire before the email is considered delayed and a DSN is sent to the sender.

The **Time interval for retry** value defines how often the MTA attempts to redeliver the message.

The **Dead mail retention period** value defines the number of days an email can stay in the **Dead Mail** queue with the maximum value being 365.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. What is the purpose of the dead mail queue on FortiMail?
   - ✓ A. The dead mail queue is used to store email that has failed transmission permanently.
   - B. The dead mail queue is used to store email that can't be sent immediately.

2. What is the maximum number of days an email can stay in the dead mail queue?
   - A. 90
   - ✓ B. 365

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 47

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- Navigating the GUI
- System Settings and Administrative Options
- Protected Domains
- User Management
- Email Flow Management

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 48

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in the lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Navigate the administration GUI and the CLI
- ✓ Access the webmail GUI
- ✓ Add FortiMail to the Security Fabric
- ✓ Configure network interfaces, DNS, routes, system time, and a host name
- ✓ Configure administrative accounts and options, and protected domains
- ✓ Verify email flow and manage email queues

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 49

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure basic settings for your FortiMail deployments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FORTINET Training Institute

FORTINET CERTIFIED PROFESSIONAL Public Cloud Security

FortiMail Administrator

Access Control and Policies

FortiMail 7.4

Last Modified: 25 April 2024

In this lesson, you will learn how to configure access control rules and policies on FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- Access Control Rules
- Outbound MTA Functionality
- Policies
- Tracking Rules and Policy IDs

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 2

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Access Control Rules

Objectives

- Enforce access control rules to control SMTP sessions

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 3

After completing this section, you should be able to achieve the objective shown on this slide.

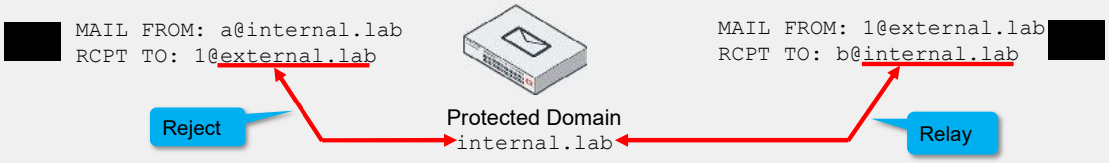
By demonstrating competence in access control rules, you will be able to harden your FortiMail security by allowing only authorized emails.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Access Receive Rules

- Specify whether FortiMail allows or denies SMTP sessions
- If a session doesn't match a rule, or if there are no rules defined, and the sender is unauthenticated, default behavior is based on the `RCPT TO:` field of the envelope
  - `RCPT TO: user@<protected domain>` → Relay
  - `RCPT TO: user@<not a protected domain>` → Reject



- A single SMTP session can match only one access receive rule
- If the sender is authenticated, no access receive rule is necessary for outbound emails

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

Access receive rules specify whether an email is allowed to use FortiMail services. You can think of these rules as a type of SMTP access control list (ACL) that allows or denies SMTP sessions.

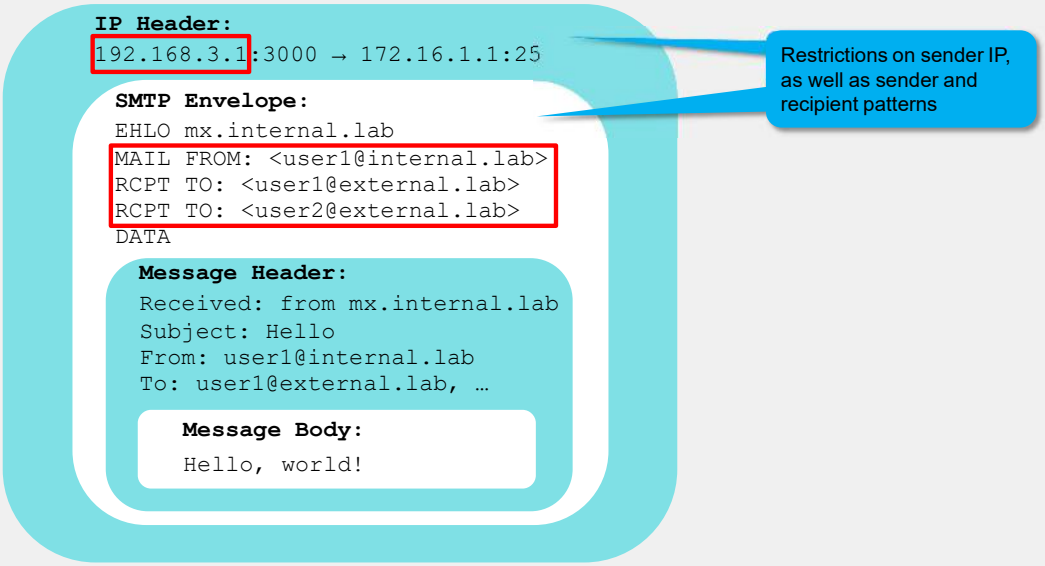
If an SMTP session doesn't match any rule, or if there are no rules defined, and the sender is unauthenticated, the default behaviour of FortiMail is based on the `RCPT TO:` field of the envelope.
• If an email *is* destined to a protected domain, FortiMail relays it.
• If an email *is not* destined to a protected domain, FortiMail rejects it.

This default behavior prevents FortiMail from acting as an open relay, which is also the reason to explicitly define an access receive rule so that FortiMail can act as an outbound MTA and relay outbound email. Later in this lesson, you will look at an example configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Access Receive Rules (Contd)



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

The selection criteria used in access receive rules provide control based on the sender IP from the IP header and recipient email addresses from the SMTP envelope. Access receive rules are applied before message header inspection.

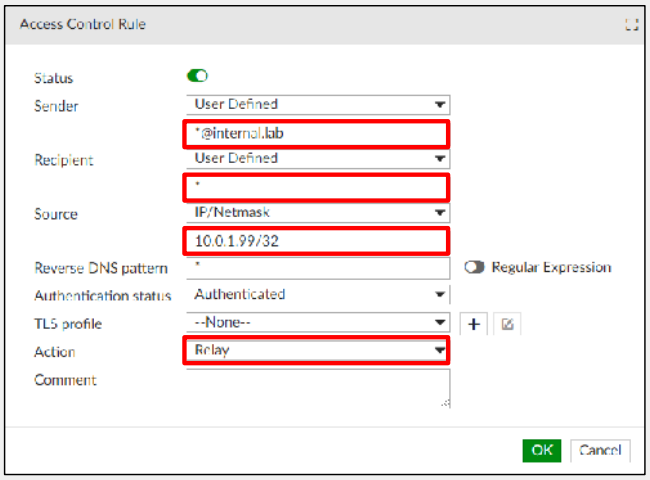
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Creating Access Receive Rules

- Control rules for SMTP sessions
- Evaluated after FortiMail initiates or receives an IP and TCP-level connection at the application layer
- Rules are evaluated from top to bottom
- Used for receipt or delivery

Policy > Access Control > Receiving



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

When creating rules, be as specific as possible. The rule shown in the example on this slide is very specific. This example rule will relay all email to any recipient, if the sender domain is `internal.lab` and the source machine is `10.0.1.99`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Access Receive Rule Actions

Action	Description
Safe	Allow the session only if one of the following conditions are met: • The recipient belongs to a protected domain • The sender is authenticated All antispam processing is skipped, but other configured scans still occur
Safe & Relay	Allow the session All antispam processing is skipped, but other configured scans still occur
Receive	Only accept incoming email to protected domains if it passes all configured scans.
Relay	Allow the session if it passes all configured scans Don't apply greylisting
Reject	Reject delivery of the email Respond to the sender with SMTP reply code 550 Relaying Denied
Discard	Accept the email, but silently delete it without informing the sender

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

There are five possible actions you can associate with an access receive rule:

- **Safe**: Deliver only if the recipient belongs to a protected domain, or the sender has authenticated. Antispam profiles are skipped, but greylisting, antivirus, and content filters are still applied.
- **Safe & Relay**: Deliver regardless of recipient or sender status and skip antispam profiles. Greylisting and other scans are still performed.
- **Receive**: Accept incoming mail to protected domains if it passes scans.
- **Relay**: Deliver and perform all scans except greylisting.
- **Reject**: Stop processing and respond to sender with SMTP reply code 550 Relaying Denied.
- **Discard**: Stop processing and silently drop the email message.

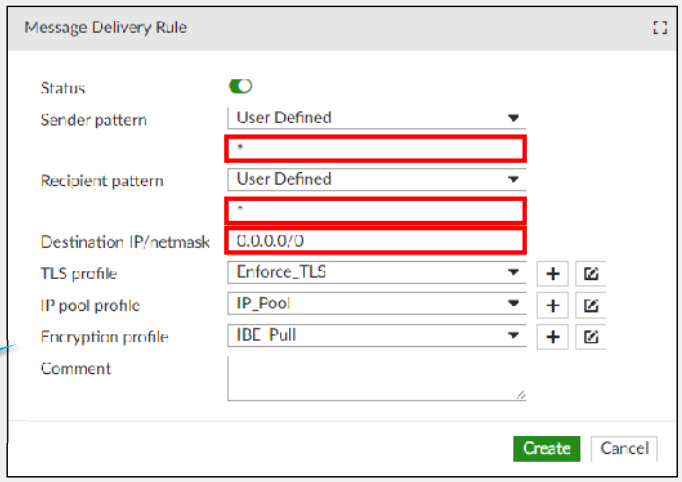
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Access Delivery Rules

- Regulate SMTP sessions initiated by FortiMail to other MTAs
- Can be used to:
  - Enforce TLS for SMTP sessions
  - Apply IBE to specific sessions
- Not required to establish mail flow

Policy > Access Control > Delivery



Enforce TLS or apply IBE to specific sessions

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

The counterpart to access receive rules is access delivery rules. Access delivery rules provide control over connections that originate from FortiMail. You can create access delivery rules to match sender and recipient patterns, as well as the destination IP address or subnet.

Access delivery rules allow you to enforce TLS and other encrypting standards for outgoing SMTP sessions. They also allow you to apply secure MIME (S/MIME) or identity-based encryption (IBE) to specific sessions. Access delivery rules aren't required to establish email flow.

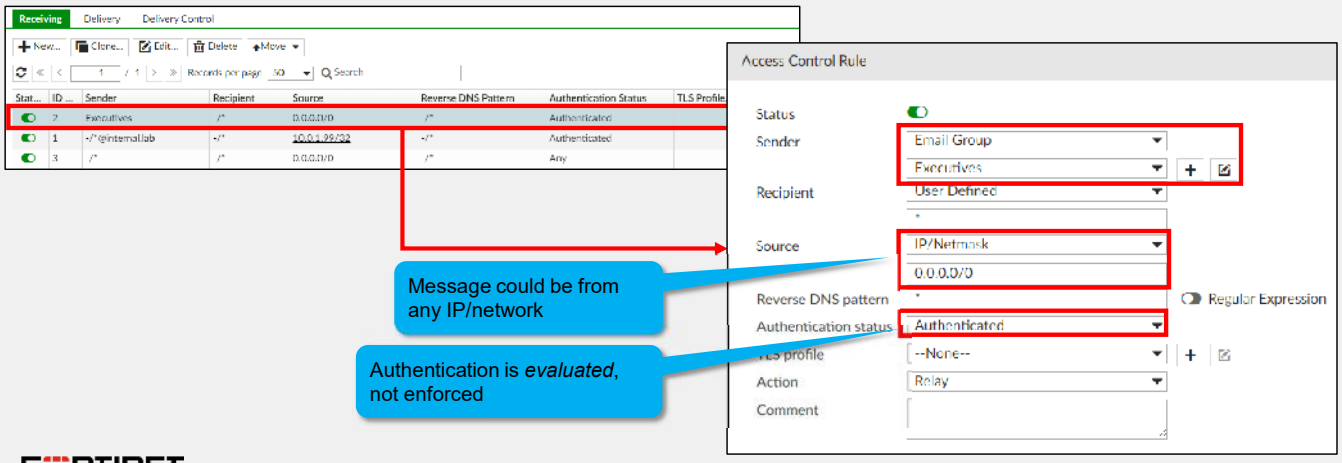
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Rule Matching Logic

- Rules are evaluated from the top down
- Rule evaluation must match all criteria

Policy > Access Control > Receiving



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

Access control rules are evaluated from the top down. Each criteria must be satisfied for a rule to match.

In the example shown on this slide, the sender *must* be a member of the **Executives** email group and *authenticated*. The source of the message can be any source IP.

If the sender is not a member of the **Executives** group, or if the sender is not *authenticated*, the message is evaluated against the next rule in the list, and so on until all rules are evaluated.

If no rules match, FortiMail processes the email in one of two ways. By default, if it's an inbound email, FortiMail accepts it and relays it, and if it's an outbound email, FortiMail drops it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. How does FortiMail process SMTP sessions if there are no access receive rules configured?
   A. If the `MAIL FROM:` domain matches a protected domain, the email will be relayed.
   ✓ B. If the `RCPT TO:` domain matches a protected domain, the email will be relayed.

2. Access receive rule selection criteria provide control based on which part of an email message?
   ✓ A. SMTP envelope
   B. MAIL FROM header

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Access Control Rules
- Outbound MTA Functionality
- Policies
- Tracking Rules and Policy IDs

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

Good job! You now understand access control rules.

Now, you will learn about outbound MTA functionality.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Outbound MTA Functionality

Objectives

- Implement outbound MTA functionality
- Configure an external relay host for outbound email

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

After completing this section, you should be able to achieve the objectives shown on this slide.

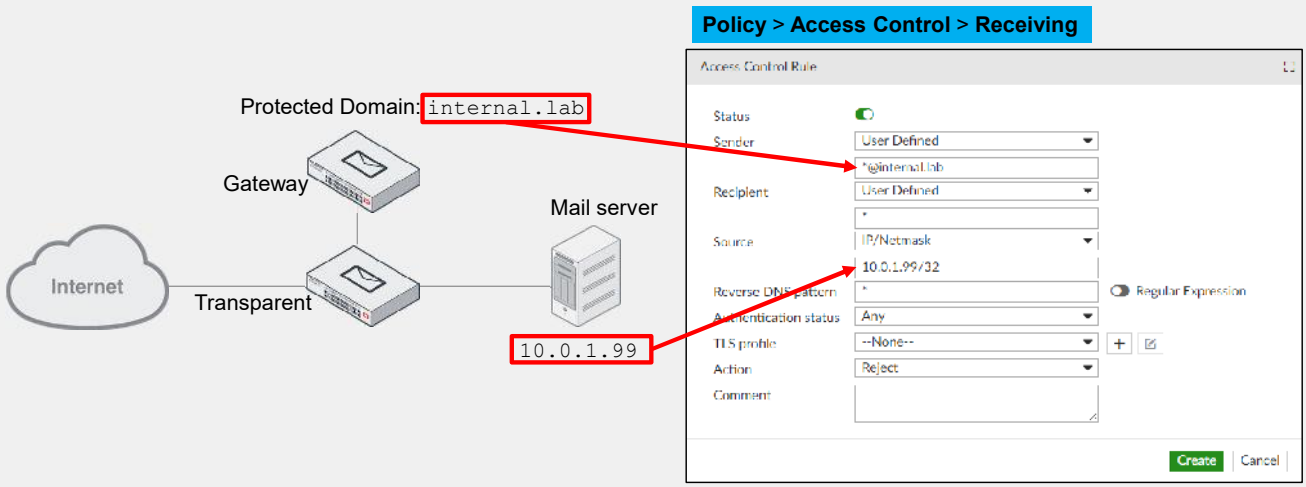
By demonstrating competence in outbound MTA functionality, you will be able to configure outbound MTA functionality on FortiMail in transparent, gateway, and server modes. You will also learn how to configure an external relay host for outbound email from FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Transparent and Gateway Mode Outbound MTA

- No rules required to handle inbound email
- Access control rule required to allow outbound email



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

You need to create access receive rules for gateway and transparent mode deployments if you intend to scan outbound email using FortiMail.

In gateway mode deployments, you must make configuration changes on the back-end mail server. These changes ensure that all outbound email from the mail server is sent to FortiMail, instead of being routed to the internet using the mail server's own MTA functionalities.

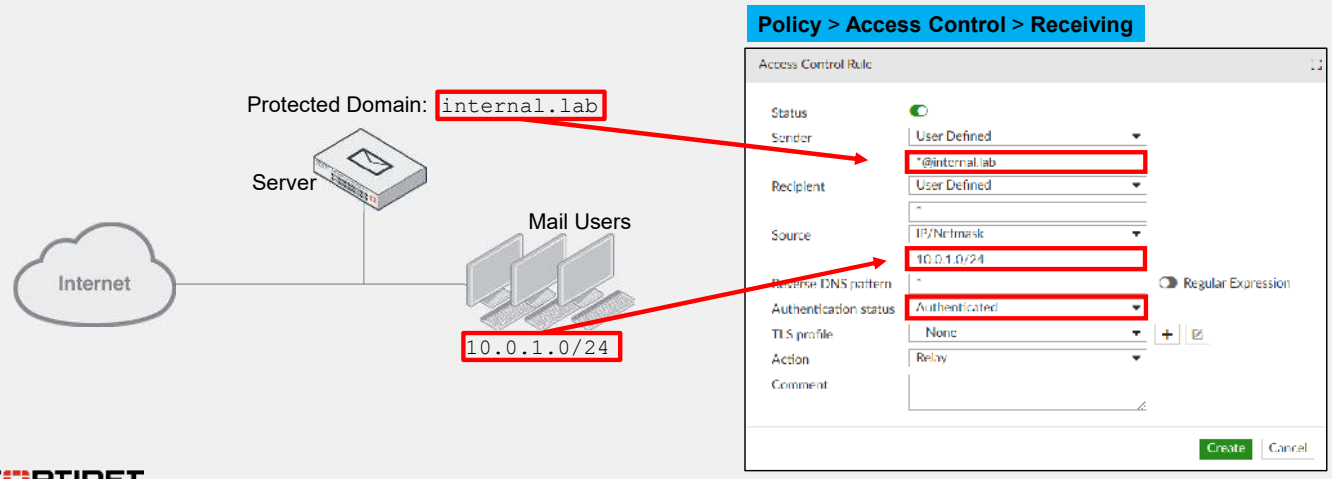
When you create access control rules use as specific matching criteria as possible. For example, when you specify a single **Source IP/Netmask** for the back-end mail server, use a /32 mask.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Server Mode Outbound MTA

- No rules required to handle inbound email
- Access control rule required to allow outbound email
- Authentication required for users to send email over SMTP



FORTINET Training Institute

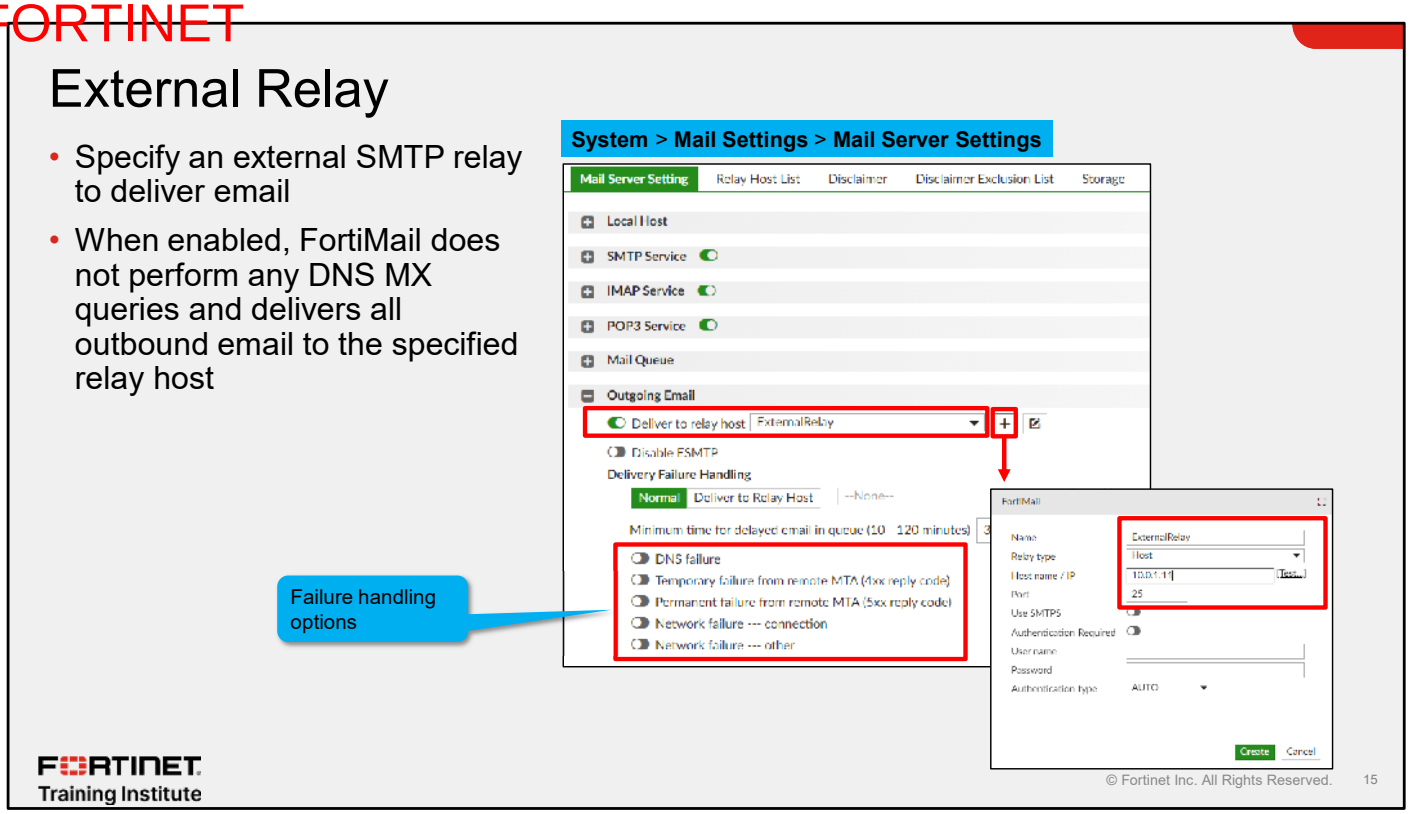
© Fortinet Inc. All Rights Reserved. 14

For server mode deployments, the access receive rule is very similar to the gateway and transparent mode example. However, in the **Source IP/Netmask** field you will most likely need to enter a subnet instead of a host address, because end users will be connecting directly to FortiMail to send email. Doing this, while convenient, is not very secure. A misconfigured printer or scanner on that subnet could potentially send documents to unintended recipients because of a more open rule with a subnet. This is one of the reasons why you should enforce authentication when you create server mode access receive rules. Requiring authentication for SMTP connections from a subnet can prevent unauthorized devices from sending unwanted email.

Authentication on FortiMail is covered in greater detail in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In certain deployments, it might be necessary to send all outbound email from the FortiMail to an external relay server instead of using the built-in MTA. For these deployments you can configure an external relay server to deliver email. When you enable this feature, FortiMail will not perform any DNS MX queries of its own and will deliver *all outbound* email for all domains to the relay host.

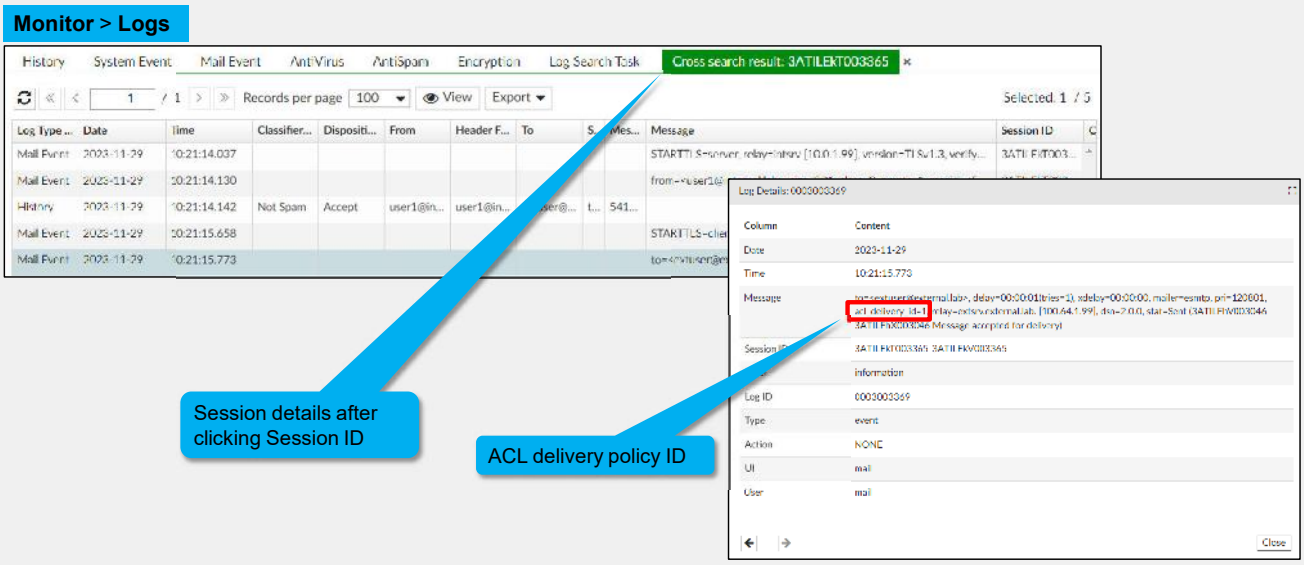
Configuring a relay host does not eliminate the need for access receive rules for outbound emails. For correct outbound email flow, you should configure both.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Detailed Logging

- View access control policy information in the logs session information



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

When access control policies are matched, log details include the matched policy ID as part of the detailed message information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which of the following statements is true regarding an external relay host?
   - ✓ A. Configuring a relay host does not eliminate the need for access receive rules for outbound email.
   - B. FortiMail will send emails only to an external relay host for protected domains.

2. What is the best practice for configuring access receive rules for outbound email in gateway mode on FortiMail?
   - A. In the **Source IP/Netmask** field, enter an actual subnet, instead of a host address.
   - ✓ B. In the **Source IP/Netmask** field, enter the IP address of the back-end mail server.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Access Control Rules
- ✓ Outbound MTA Functionality
- Policies
- Tracking Rules and Policy IDs

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

Good job! You now understand outbound MTA functionality.

Now, you will learn about policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Policies

Objectives

- Configure IP-based and recipient-based policies

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

After completing this section, you should be able to achieve the objective shown on this slide.

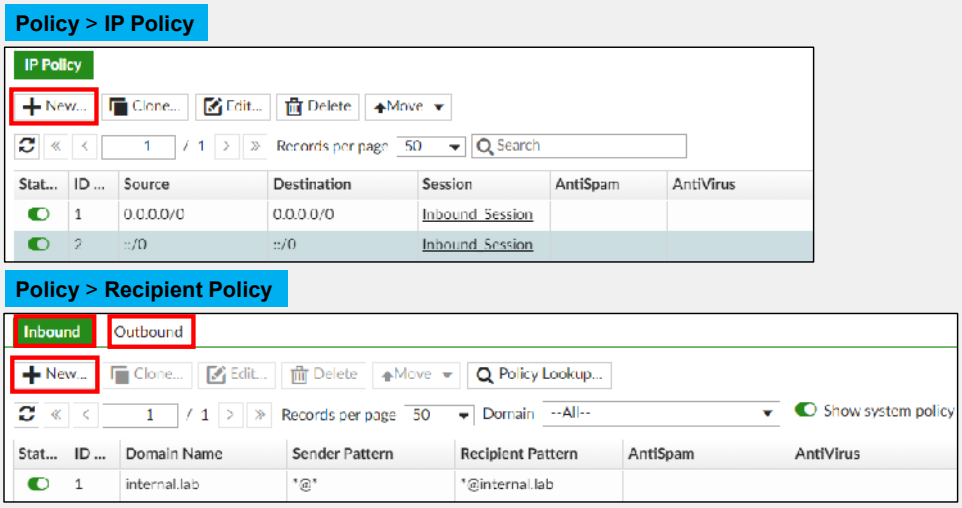
By demonstrating competence in policies, you will be able to configure IP-based and recipient-based policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Policies

- Identify email flow
- Apply inspection profiles to the flow



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

There are three types of policies:
- Access control policies
- IP-based policies
- Recipient-based policies

Use access control rules and delivery rules to control which SMTP clients can send email and how FortiMail delivers email that it proxies or relays. FortiMail applies recipient-based policies to individual email messages based on the recipient's email address. FortiMail applies IP-based policies based on the IP address of the connecting SMTP client or server.

Much like firewall rules, FortiMail evaluates policies in a top-down order. Once an email flow matches a policy, FortiMail skips any remaining policies in the list. FortiMail maintains a single global list of IP-based policies but maintains domain-specific lists for recipient-based policies if there are multiple protected domains.

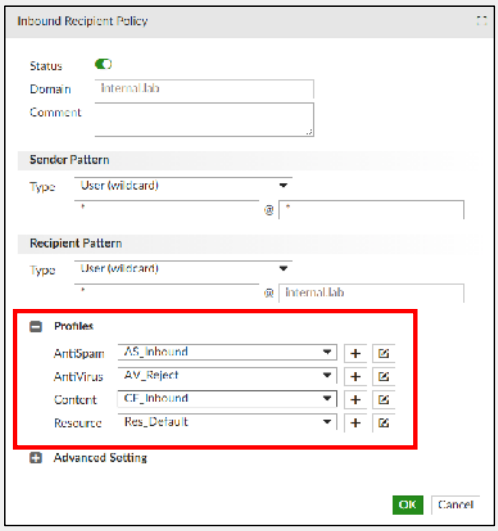
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

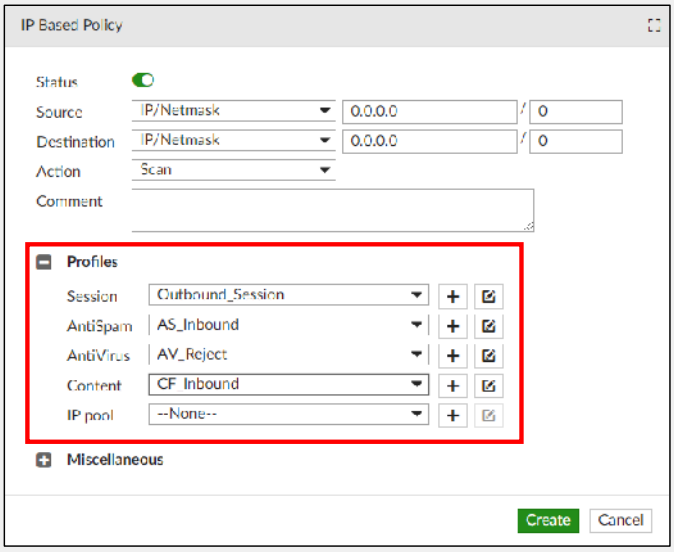
Policies (Contd)

- Define the type of inspection and actions to perform on the mail flow

Policy > Recipient Policy > Inbound



Policy > IP Policy > IP Policy



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

Policies reference profiles. Profiles define which inspections and actions FortiMail performs on email that are matched by a policy.

Different types of profiles govern different types of inspections. Profile types include session, antispam, antivirus, and so on. You can enable and configure specific processing activities in profiles. Each inspection profile, other than the session profile, has corresponding action profiles that define the action that is taken on an email as a result of the scan. Possible actions include reject, discard, personal quarantine, system quarantine, and so on.

FortiMail policies and profiles give you the flexibility to treat each email differently by allowing you to build FortiMail configurations with multiple policies, each having unique selection criteria and calling different profiles.

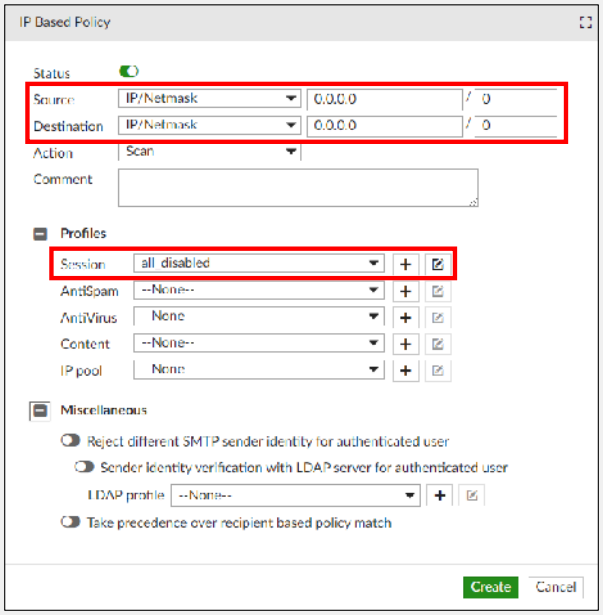
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IP-Based Policies

- Identify email flow based on the source or destination IP address of the SMTP session
  - IP/Netmask – source or destination
  - IP Group – source or destination
  - GeoIP Group – source
  - ISDB – source
- Apply session profile inspections that are performed on the TCP session and SMTP envelope
- Optionally, configure profiles for SMTP authentication

Policy > IP Policy > IP Policy



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

IP-based policies use source and destination IP information as selection criteria. This is useful in situations where it's preferable to distinguish between email traffic using IP information, such as when FortiMail is placed between the internet and a large, multi-tenant email server farm.

Source addresses can be defined using IP/Netmask, IP group, GeoIP (IP addresses based on geographic locations), or ISDB (internet service database). ISDB is a list of public IP addresses that uses IP address ranges, owners, service ports, and IP credibility, and provides a granular approach to the source address. The ISDB information is obtained from the FortiGuard service system.

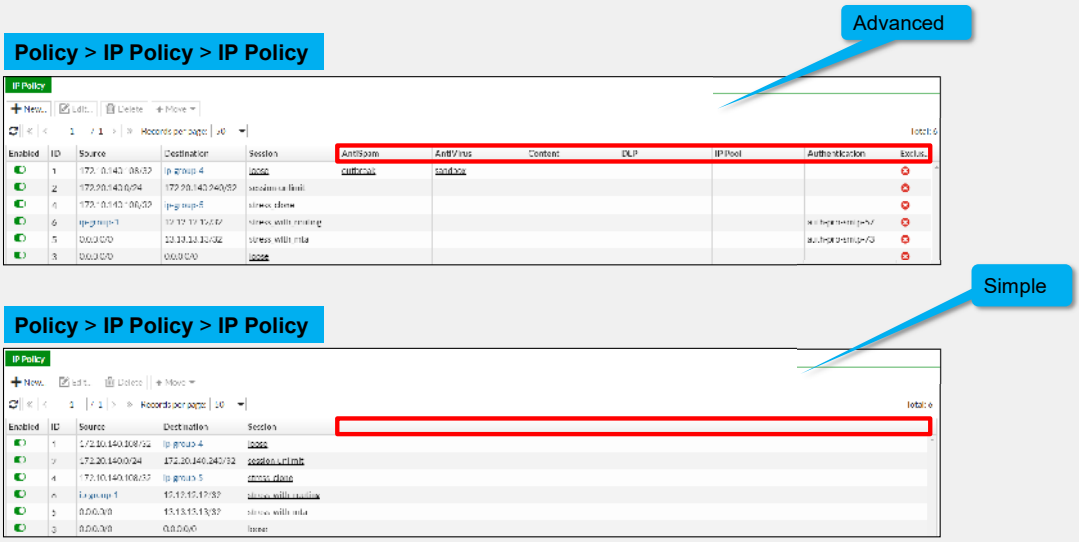
Session profiles are available only through IP policies, and perform actions that are applied to information gathered early in the SMTP connection process. This action can detect malicious activities even before FortiMail processes the SMTP header. Session profile scans eliminate the need to conduct more resource-intensive scans.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IP Policy—Simple/Advanced View

- Fields used less frequently are hidden on IP policies in simple view



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

Some fields are hidden in the **IP Policy** section in simple view. You can switch between simple view and advanced view on the GUI at any time, with no configuration loss.

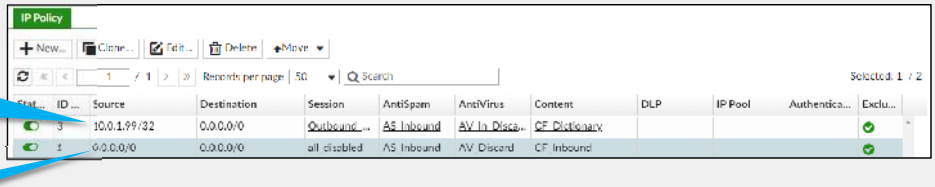
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IP-Based Policy Usage

- Required to enable the session profile
- IP policy action profiles lack user quarantine option
- Typically used by mail hosting services or ISPs
  - Not feasible to maintain a complete list of protected domains
  - Usually performing strict IP-based policy filtering

Policy > IP Policy > IP Policy



Specific IP in the **Source** field means this policy is handling sessions originated from this host only

Default IP-based policy to handle all other sessions

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

Deciding which policy type to implement doesn't necessarily mean choosing one type over the other. It's not uncommon for both IP-based and recipient-based policy types to be used concurrently. Having both policy types available to use provides flexibility, especially when deployments increase and become very large.

As mentioned earlier, the two policy types have different capabilities. The most significant differences are that you can apply session profiles to IP-based policies and IP-based policy action profiles don't support the user quarantine option.

Specific deployment types use strict IP-based filtering: large mail hosting services and ISPs. These deployment types usually require that email is inspected from a high number of domains. On such a large scale, it isn't feasible to maintain a complete list of protected domains and configure a recipient-based policies for each domain. That's why large-scale deployments usually opt for a strict IP-based filtering setup.

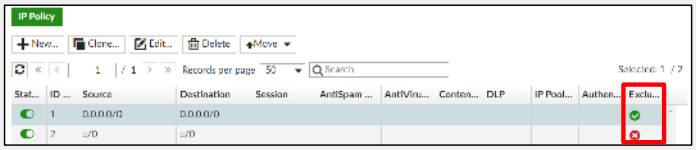
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

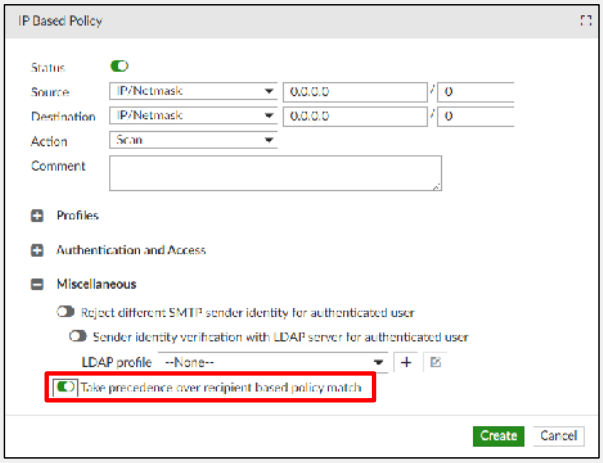
IP-Based Policy Usage (Contd)

- The **Take precedence over recipient based policy match** setting forces FortiMail to apply only profiles from the matching IP-based policy in the event that there is also a matching recipient-based policy

Policy > IP Policy > IP Policy



Policy > IP Policy > IP Policy



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

The exclusive flag forces FortiMail to apply only profiles from the matching IP-based policy in the event that there is also a matching recipient-based policy.

If both a recipient-based policy and an IP-based policy match the email, unless you have enabled **Take precedence over recipient based policy match** in the IP-based policy, the settings in the recipient-based policy will take precedence.

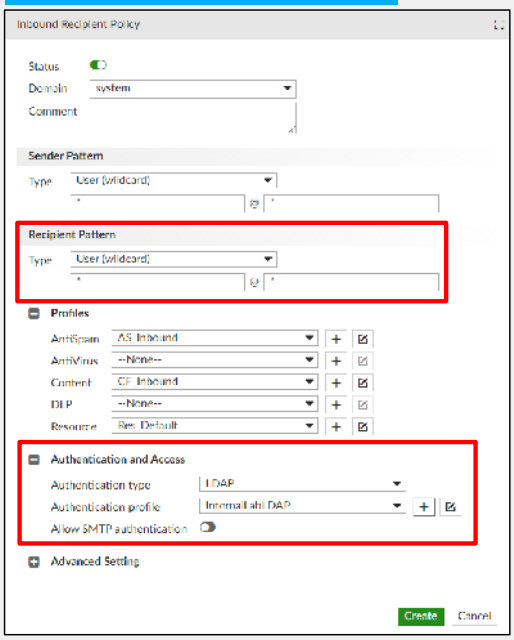
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Recipient-Based Policies

- Identify email flow based on recipient email addresses (inbound) or sender and recipient addresses (outbound)
- Apply inspection profiles on the message header and body
- Optionally, configure authentication profiles for RADIUS, LDAP, POP3, IMAP, SMTP, and webmail
- Separate inbound and outbound policies

Policy > Recipient Policy > Inbound



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

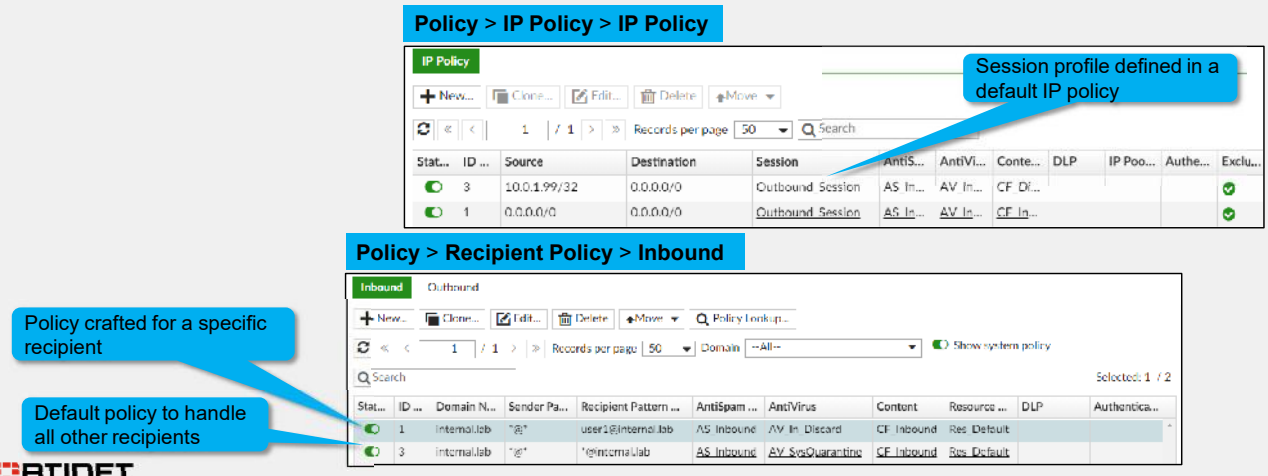
Recipient-based policies use the sender and recipient information from the email to match the policy and apply inspection profiles to the email flow. When you use recipient-based policies, you also have the option to configure profiles to support authentication for RADIUS, LDAP, POP3, IMAP, SMTP, and webmail access. FortiMail maintains separate lists for inbound and outbound recipient-based policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Recipient-Based Policy Usage

- Always used alongside IP policies
  - IP policy required to apply a session profile
  - Recipient policy defines all other inspection profiles
- Recipient policy action profiles support user-level quarantining



FORTINET Training Institute

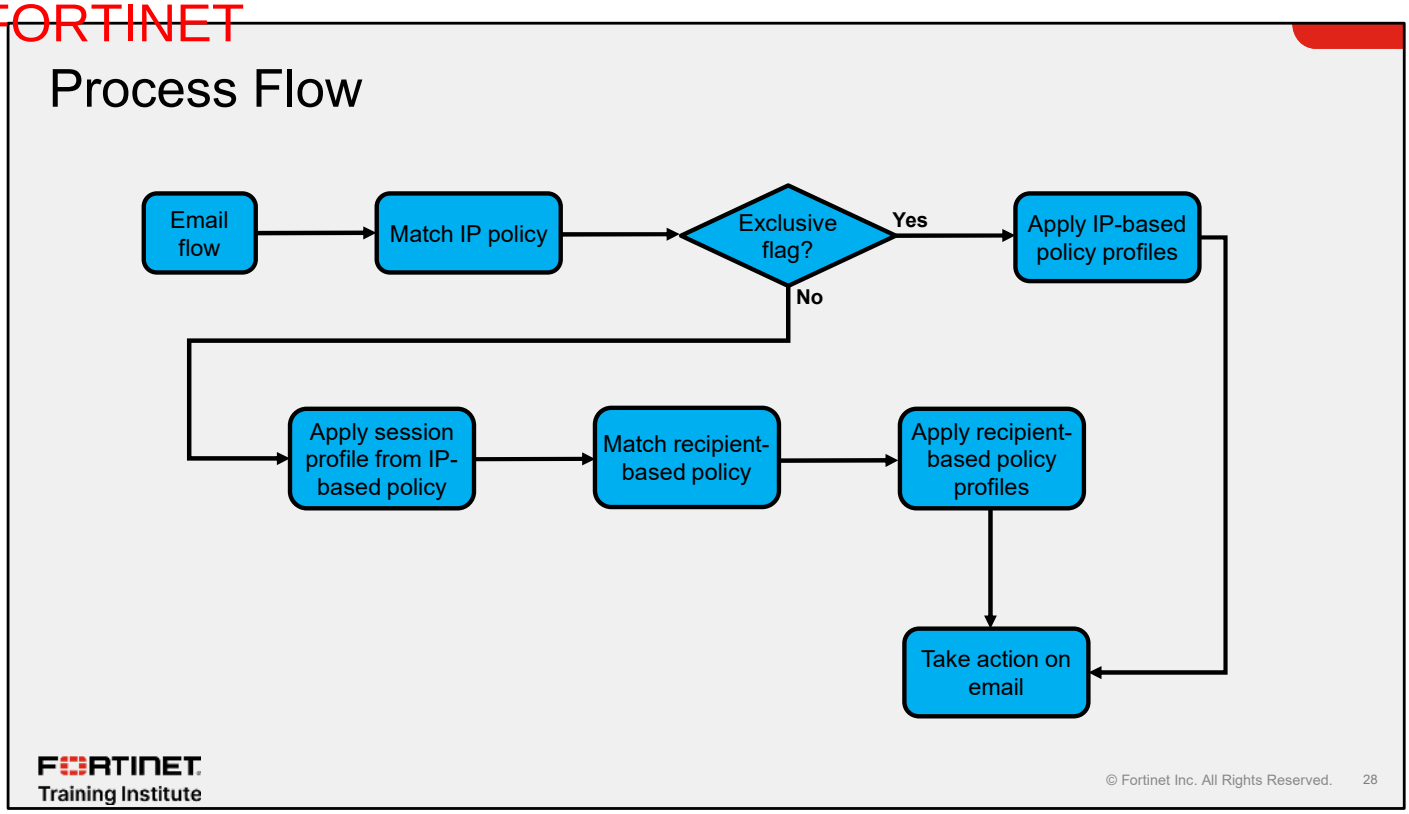
© Fortinet Inc. All Rights Reserved. 27

If you configure inspection profiles using recipient-based policies, you should have at least one IP-based policy in place to apply a session profile to all SMTP sessions. Recipient-based policies allow more granularity when applying inspection to specific email flows.

Note that system recipient-based policies take precedence over domain recipient-based policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



If you use a configuration that employs strict IP policy-based filtering, or if you set the IP policy exclusive flag, then FortiMail applies only the inspection profiles from the matching IP policy. No other policy or profiles need to be evaluated.

However, if you don't set the exclusive flag, or there are matching recipient-based policies, then the behavior changes. FortiMail applies the session profile from the matching IP-based policy, and applies the rest of the profiles, such as antispam, antivirus, and content filters from the matching recipient-based policy

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which inspection profile is supported by IP policies but not recipient policies?
   A. DLP profile
   ✓ B. Session profile

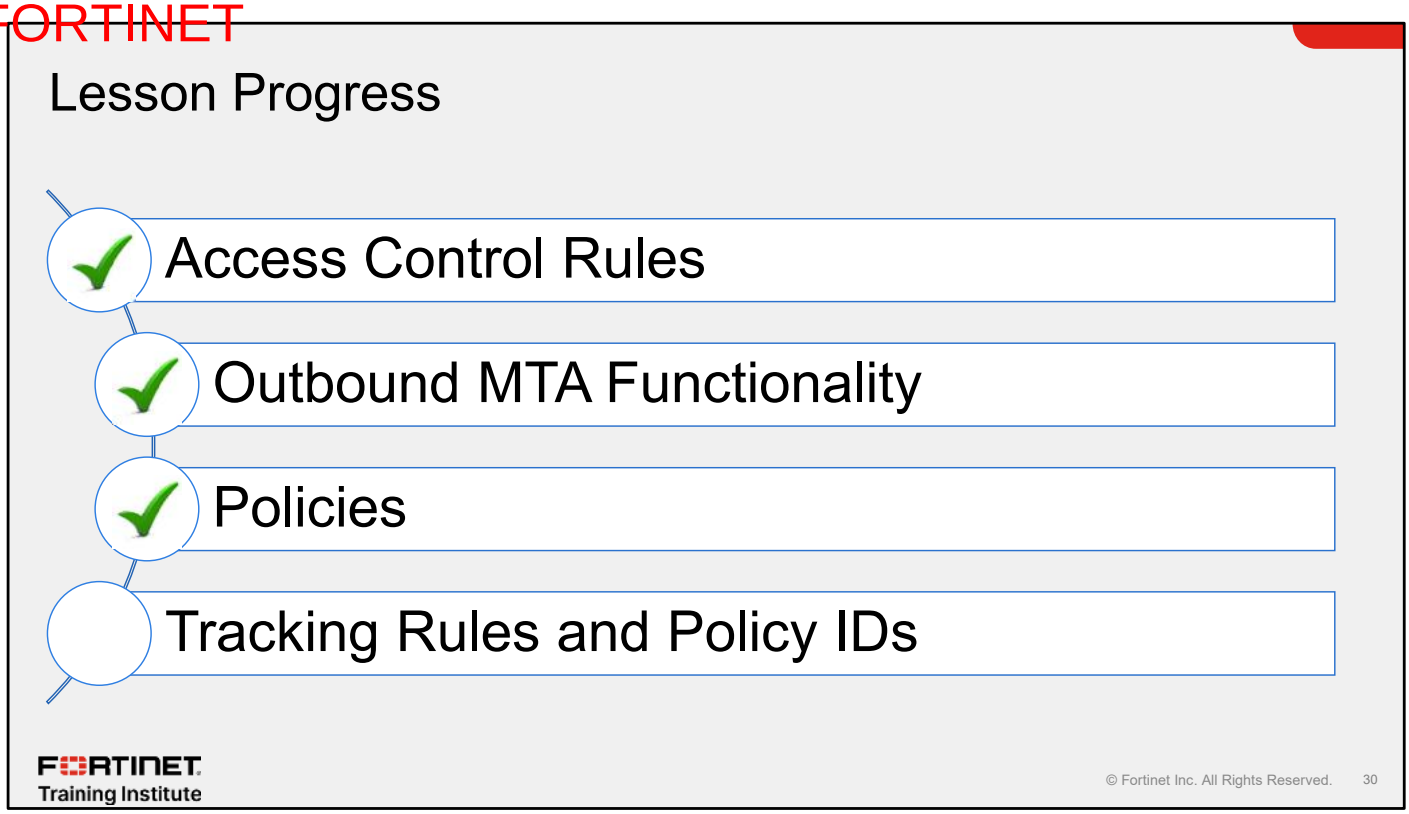
2. What is the purpose of the **Take precedence over recipient based policy match** flag in an IP-based policy?
   ✓ A. Forces FortiMail to apply the matching IP-based policy if there is also a matching recipient-based policy
   B. Applies profiles from both IP-based and recipient-based policies

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 29

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Good job! You now understand policies.

Now, you will learn about tracking rules and policy IDs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Tracking Rules and Policy IDs

Objectives

- Track access control rules and policy matches using logs

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in tracking rules and policy IDs, you will be able to track access control rules and policy matches by investigating the logs.

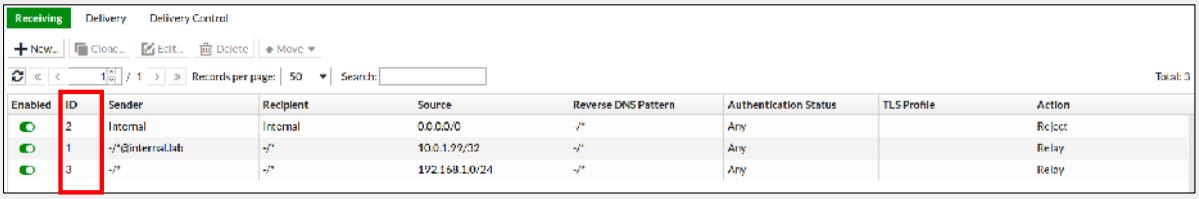
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Access Control Rule ID

- Access control rules are assigned an ID by the system at the time the rule is created
- The ID number never changes as rules move higher or lower in the sequence
- The default behavior—for example, allow all inbound email destined for a protected domain, or allow authenticated outbound email—is considered ID 0 but is not shown in the configuration

Policy > Access Control > Receiving



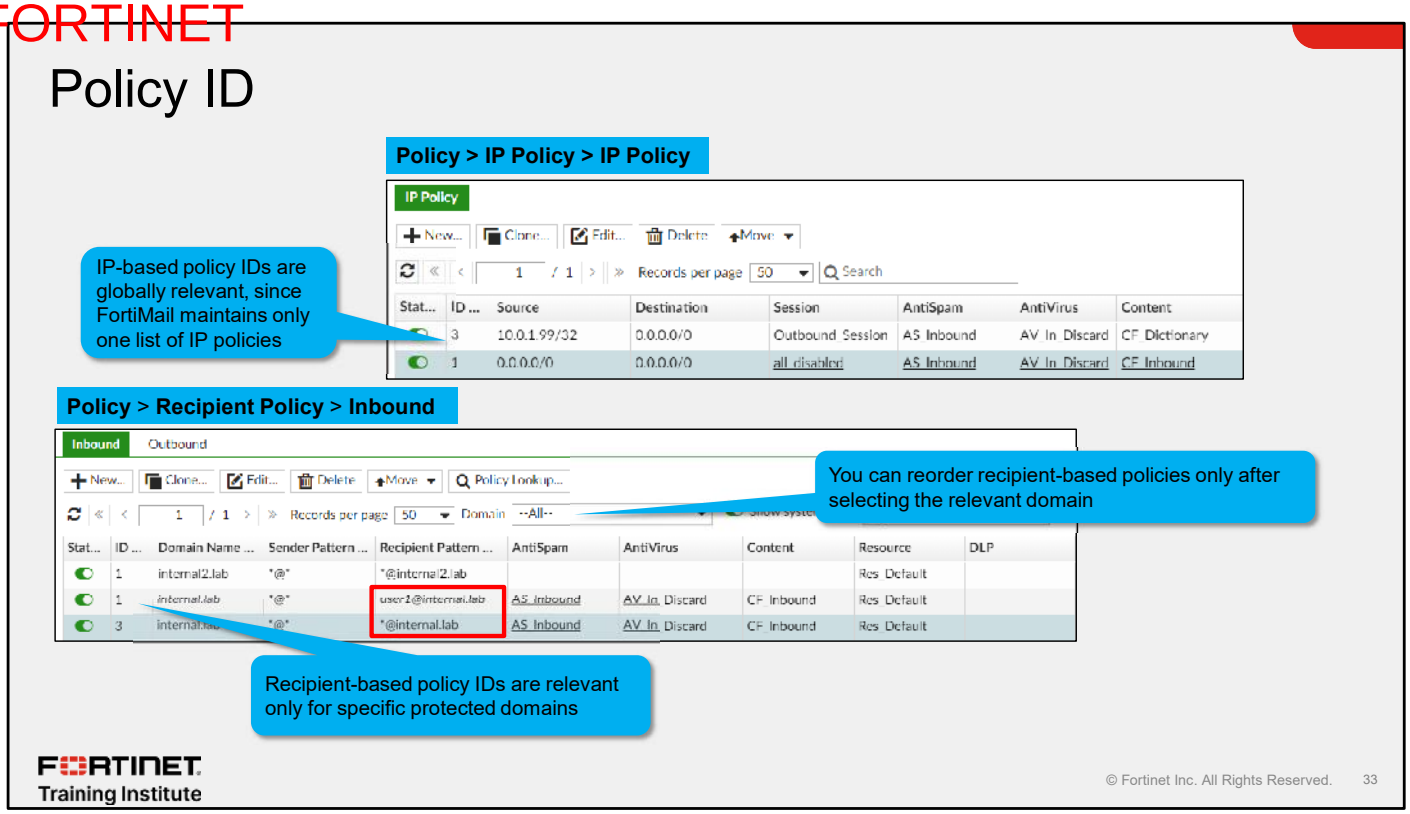
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

The system assigns an ID to the access control rule at the time it creates the rule. The ID number doesn't change as rules move higher or lower in the sequence. The default behavior—for example, allow all inbound email destined for a protected domain, or allow authenticated outbound email—is considered ID 0 by the system.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



IP-based policy IDs are globally relevant, because FortiMail maintains only a single list of IP policies for the whole system. Recipient-based policy IDs, however, are relevant only for specific protected domains. That is why you can have multiple policies with ID 1. You can reorder recipient-based policies only after selecting the relevant domain in the **Domain** drop-down list.

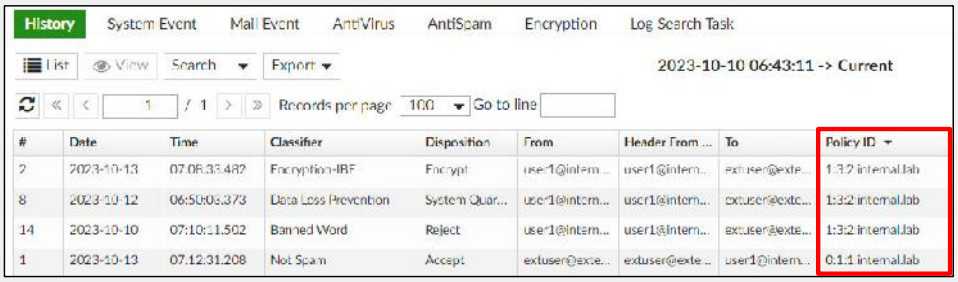
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

History Log Policy ID

- The policy IDs for each email are recorded in the history logs using the format of **X:Y:Z:<recipient policy domain name or SYSTEM>**
  - X is the ID of the access control rule
  - Y is the ID of the IP-based policy
  - Z is the ID of the recipient-based policy
  - The last field displays a protected domain name if the email matches a recipient-based policy
    - If there is no recipient-based policy match, or it's an outbound email, it displays **SYSTEM**

Monitor > Log > History



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 34

The policy IDs for each email are recorded in the history logs using the format of X:Y:Z:<recipient policy domain name or SYSTEM>, where the fields represent the following:

- X is the ID of the access control rule.
- Y is the ID of the IP-based policy.
- Z is the ID of the recipient-based policy.
- The last field displays a protected domain name if the email matches a recipient-based policy; If there is no recipient-based policy match, or it's an outbound email, it displays `SYSTEM`.

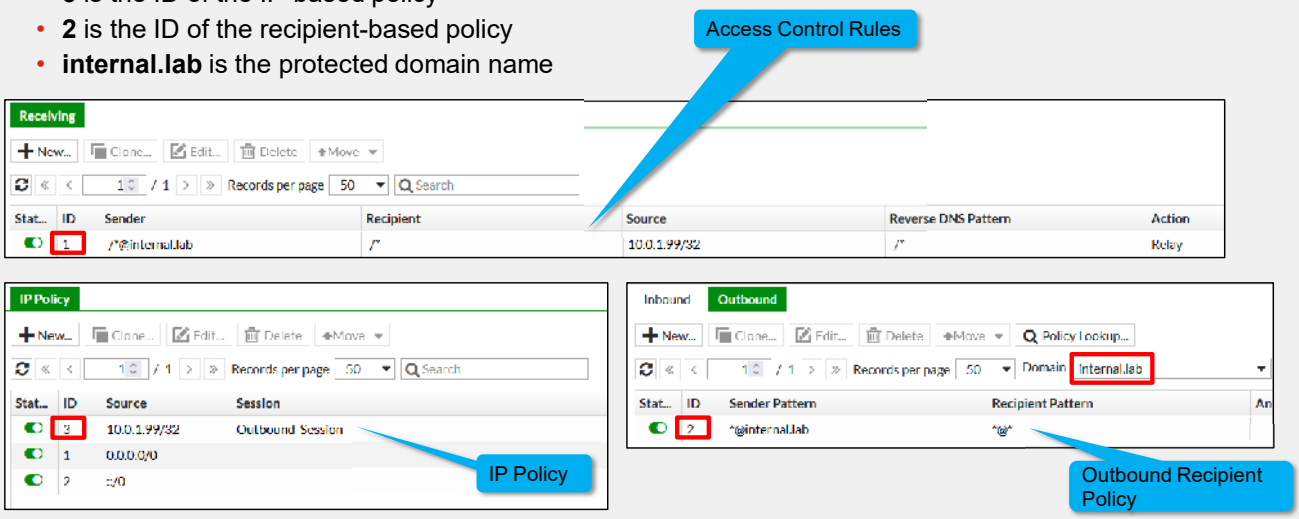
If the value in the access control rule field for incoming email is 0, it means that FortiMail is applying its default rule for handling inbound email. If the value of X, Y, Z is 0 in any other case, it means that no policy or rule could be matched.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

History Log Policy ID (Contd)

- Policy ID **1:3:2:internal.lab**
  - **1** is the ID of the access control rule
  - **3** is the ID of the IP-based policy
  - **2** is the ID of the recipient-based policy
  - **internal.lab** is the protected domain name



FORTINET Training Institute
© Fortinet Inc. All Rights Reserved. 35

The policy ID field is critical for understanding and troubleshooting email. Each entry is a reference to a policy, which can in turn have profiles associated with them performing operations. Being able to associate the policy ID with its associated policies can be critical in understanding how mail is flowing through your FortiMail.

In this example of an outgoing email, the access control rule is number **1**, indicating it was sent from `10.0.1.99`. Any other source would have probably used the default access control rule of 0.

The IP policy rule also matches the IP address of `10.0.1.99` as the source. In this case it is IP policy rule number **3**, associated with the Outbound Session profile, which will be applied to the email.

The Recipient based policy matches ID number **2**, indicating that this email is being sent from a user in the **internal.lab** protected domain. Any outbound profiles defined with recipient policy 2 will be applied to this email.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Recipient-based policy IDs are relevant for which type of domains?
   - ✓ A. Protected domains
   - B. External domains

2. The policy IDs for each email are recorded in the history logs using the format of X:Y:Z:<recipient policy domain name or SYSTEM>. What kind of policy ID does Z represent?
   - A. IP-based policy
   - ✓ B. Recipient-based policy

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 36

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Access Control Rules
- ✓ Outbound MTA Functionality
- ✓ Policies
- ✓ Tracking Rules and Policy IDs

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 37

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Enforce access control rules to control SMTP sessions
- ✓ Implement outbound MTA functionality
- ✓ Configure an external relay host for outbound email
- ✓ Configure IP-based and recipient-based policies
- ✓ Track access control rules and policy matches using logs

FORTINET Training Institute

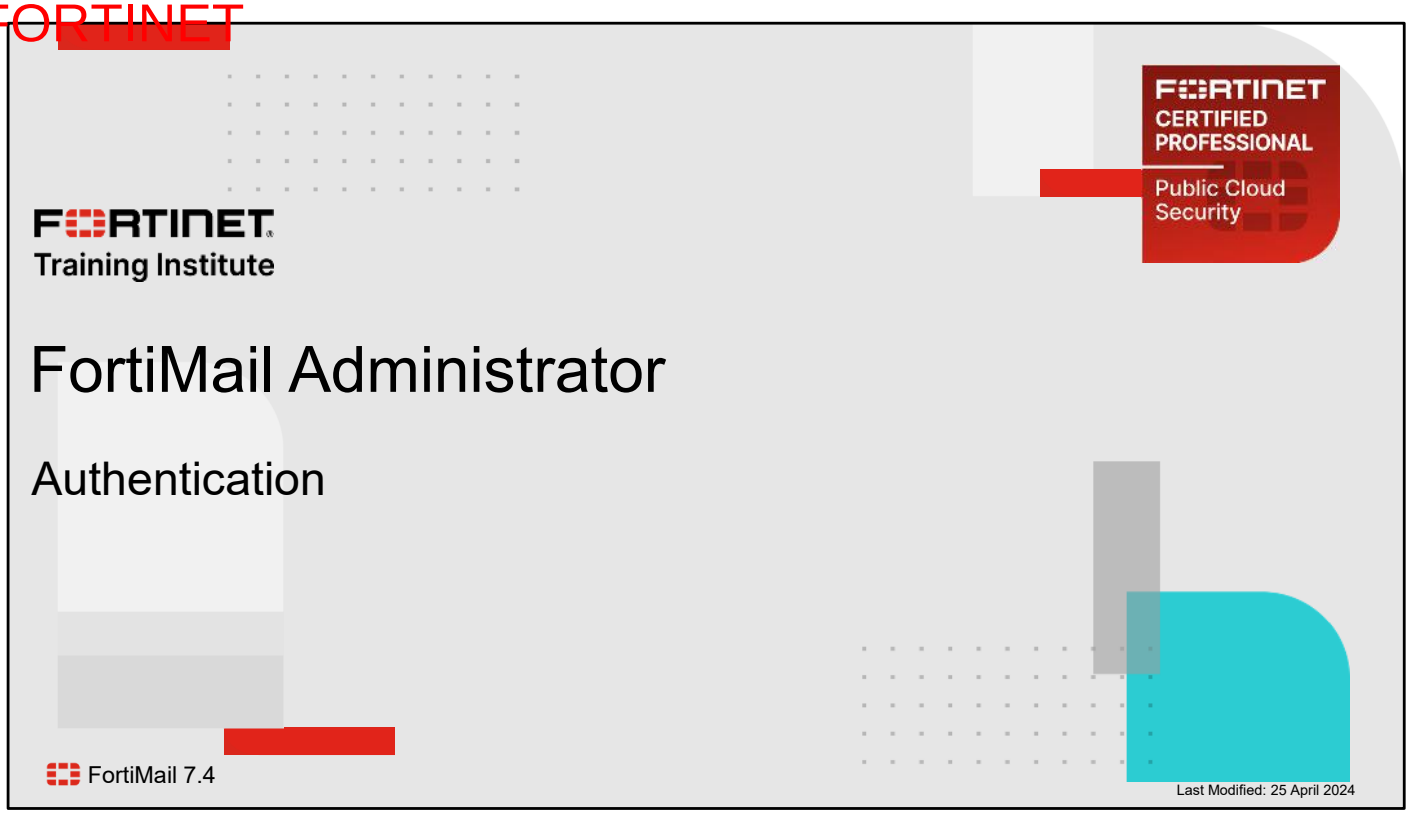
© Fortinet Inc. All Rights Reserved. 38

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure access control rules and policies on FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

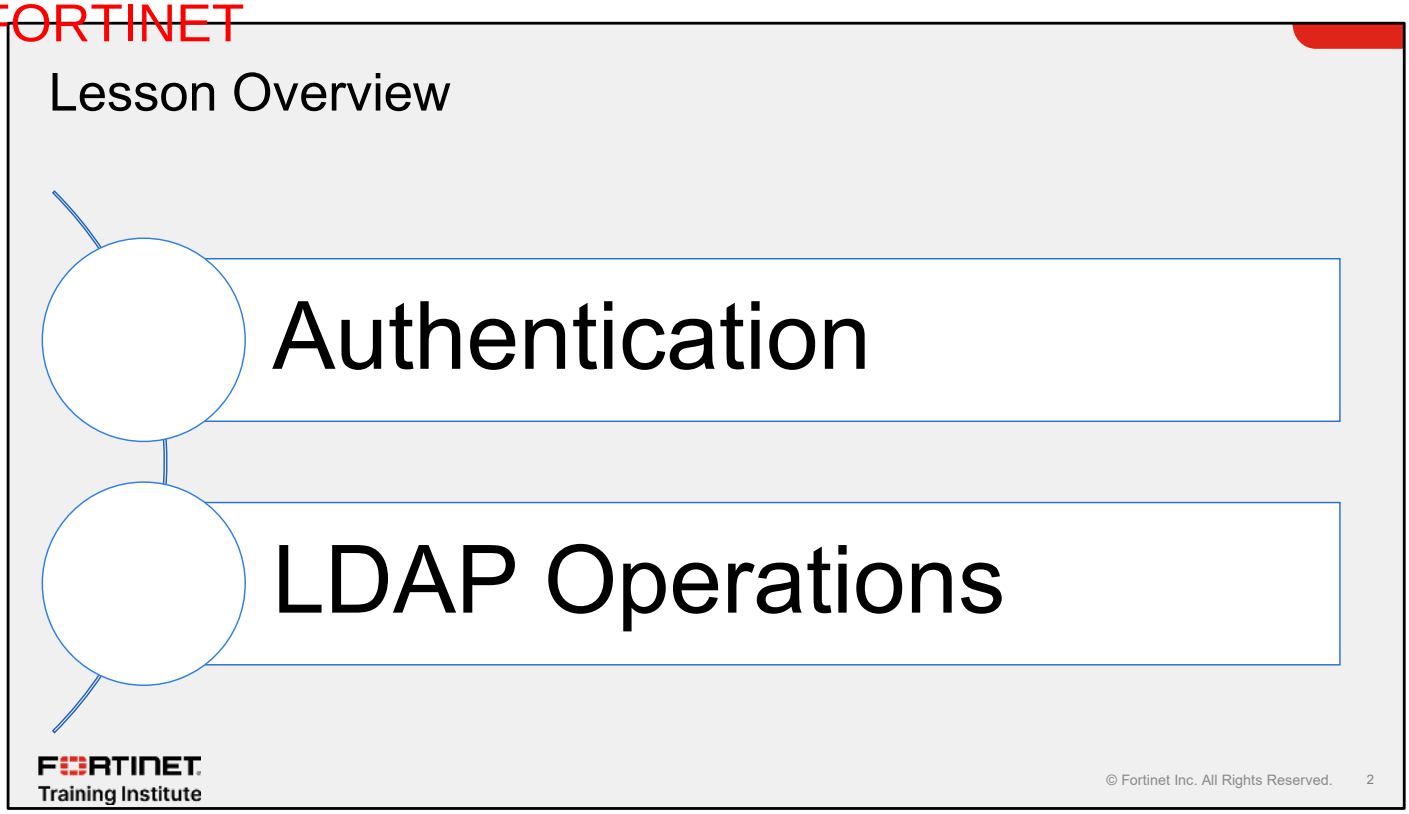
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to configure and enforce authentication on FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will explore the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Authentication

Objectives

- Use authentication profiles to define sources for user credentials
- Enable IP-based or recipient-based policy authentication
- Enforce authentication using access control rules

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 3

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in authentication, you will learn how to configure FortiMail to support and enforce authentication for SMTP, POP3, IMAP, and webmail. You will also learn how to enable remote authentication for administrative accounts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Authentication on FortiMail

- In gateway and transparent mode, FortiMail acts as an authentication proxy:
  - User credentials aren't stored locally—FortiMail must obtain them from an external source
  - FortiMail grants or denies user access based on back-end server response
  - Authentication profiles define sources for user credentials
- In server mode, FortiMail is the authentication server
  - Local database of user IDs and passwords that users can authenticate against directly using SMTP, POP3, IMAP, HTTP, or HTTPS

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

In transparent and gateway modes, FortiMail acts as an authentication proxy. User credentials are not stored on FortiMail, so you must tell FortiMail explicitly where to find this information using authentication profiles.

When a user needs to authenticate, FortiMail prompts the user for their ID and password, which it then sends to the back-end authentication server. The user is granted or denied access based on the response from the authentication server.

In server mode, FortiMail acts as the authentication server. Users authenticate directly against a local database of users and passwords using SMTP, POP3, IMAP, HTTP, or HTTPS.

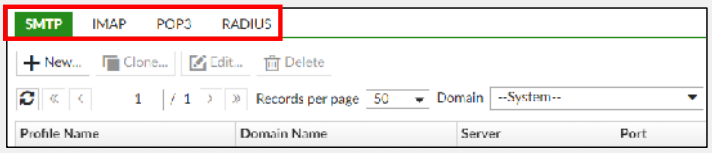
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

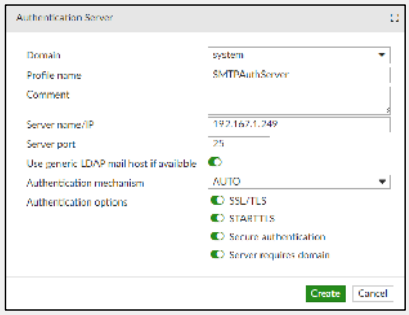
Authentication Profiles

- Authentication type:
  - SMTP, IMAP, POP3, RADIUS
- All deployment modes can use an LDAP profile for LDAP server integration

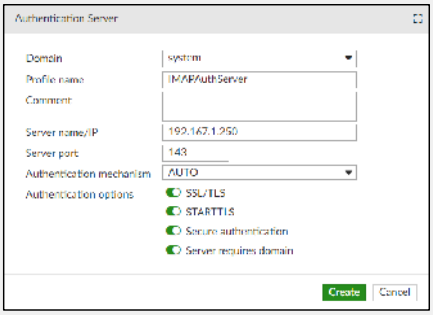
Profile > Authentication



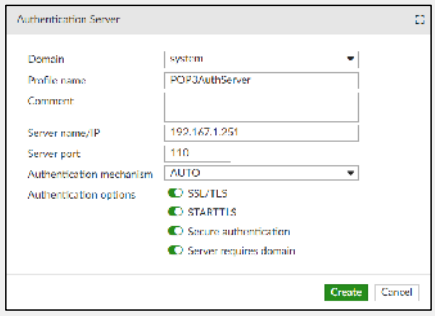
Profile > Authentication > SMTP



Profile > Authentication > IMAP



Profile > Authentication > POP3



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

On FortiMail, you can use authentication profiles to define the server details and protocol options that support authentication. FortiMail supports SMTP, IMAP, POP3, and RADIUS server integration.

All deployment modes can also use LDAP profiles for LDAP server integration. LDAP profiles provide more advanced functionality, such as alias and group lookup, which cannot be achieved using other authentication profiles. You will learn more about LDAP profiles later in this lesson.

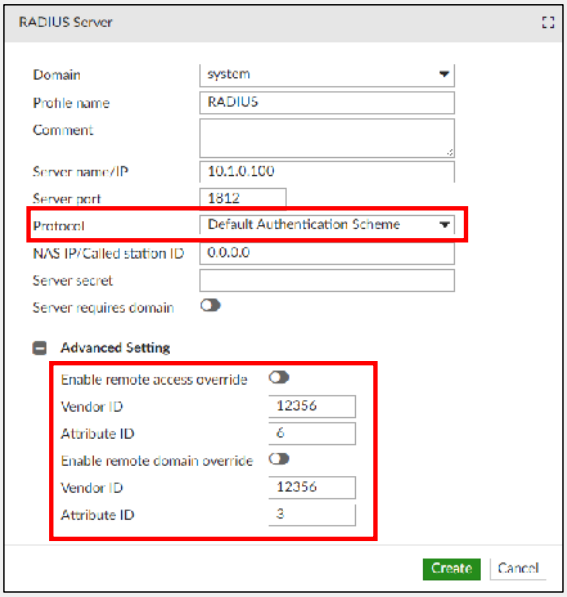
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

RADIUS Authentication Profile

- Access-challenge message support for two-factor authentication
  - Authenticates email for a day before requiring reauthentication
- PAP, CHAP, MSCHAP, MSCHAPv2 support
- Override authorization levels for administrative accounts using vendor-specific attributes:
  - **Attribute ID 6 :** Fortinet-Access-Profile
    - Defines the administrator access profile
  - **Attribute ID 3 :** Fortinet-Vdom-Name
    - Defines the administrator domain

Profile > Authentication > RADIUS



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

FortiMail supports the RADIUS access-challenge message to allow for two-factor authentication.

RADIUS authentication profiles can also be used to define the administrator account domain and access profiles dynamically, using vendor-specific attributes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Enabling and Matching Authentication

- *Enable* email user authentication using policies:
  - IP address-based policies
    - SMTP, POP3, IMAP, LDAP, and RADIUS
  - Incoming recipient-based policies
    - SMTP, POP3, IMAP, LDAP, and RADIUS
- You do not need to explicitly enable email user authentication in server mode deployment, because it is enabled by default
- *Match* email user authentication using access control receive rules
- You can configure administrator authentication for each account, or wildcard authentication if using RADIUS or LDAP
  - Supports RADIUS, PKI, and LDAP authentication profiles
- SSO support using SAML (FortiMail as a SP) for both administrator and webmail accounts

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

There are two methods of enabling authentication:
- IP address-based policies
- Inbound recipient-based policies

By default, the recipient-based policy takes precedence unless configured otherwise.

You do not need to explicitly enable user authentication in server mode deployments because it is enabled by default.

You can match authentication using access control receive rules. Access control receive rules use authentication status as a matching criteria.

You can configure administrator accounts individually using RADIUS, PKI, and LDAP authentication profiles. You can configure wildcard authentication if you are using RADIUS or LDAP.

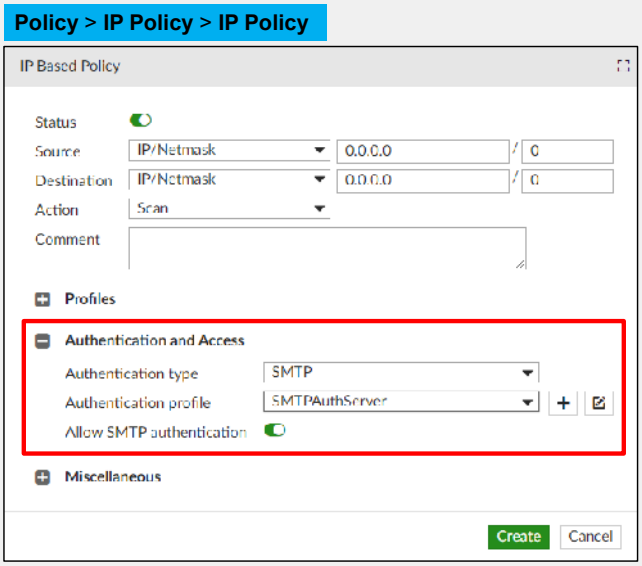
FortiMail can be configured as a service provider (SP) to support Security Assertion Markup Language (SAML) SSO for both user and administrator accounts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IP-Based Policy Authentication

- The authentication lookup is triggered by the source IP address of the client sending the email
- Doesn't involve sender or recipient addresses
- Supports SMTP, POP3, IMAP, LDAP, and RADIUS



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

Source and destination IP information triggers IP-based policies. IP policies support SMTP, POP3, IMAP, LDAP, and RADIUS authentication.

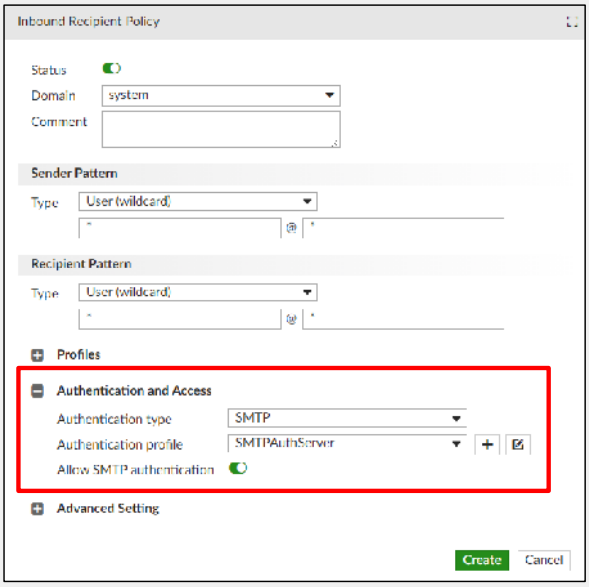
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Recipient-Based Policy Authentication

- Authentication lookup is based on sender address
- Supports SMTP authentication, as well as SMTP, POP3, IMAP, LDAP, and RADIUS

Policy > Recipient Policy > Inbound



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

Incoming recipient-based policies offer more flexibility. You can use recipient-based policy authentication to allow SMTP, POP3, IMAP, LDAP, RADIUS, and webmail access.

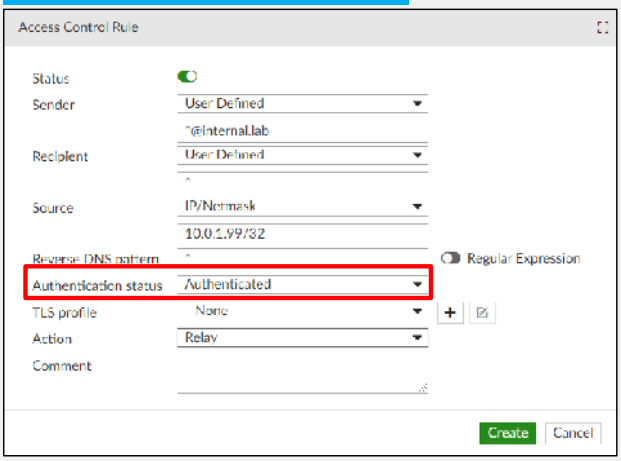
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Access Receive Rules

- Match SMTP authentication using access receive rules:
  - **Authentication status: Authenticated**
- Applicable to gateway mode only if you allow users or hosts to use FortiMail directly as a mail relay
- You should use access receive rules to enforce authentication for server mode deployments

Policy > Access Control > Receiving



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

To match SMTP authentication, you must create appropriate access control receive rules. For gateway mode deployments, access control receive rules could apply to individual accounts, such as automailers, that use FortiMail as a mail relay. However, for server mode deployments, you should enable access control receive rules for the entire user base, to ensure that FortiMail isn't being used by unauthorized users to relay potential spam.

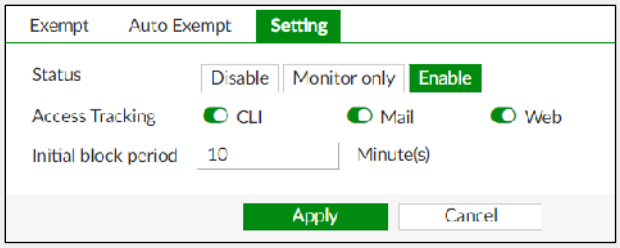
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

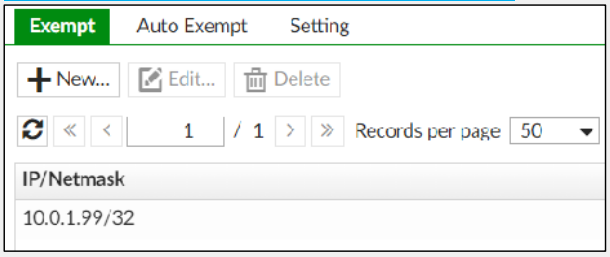
Authserver Security

- Tracks offending IP addresses attempting brute force attacks
- Temporarily locks out the attacker
- Trusted IP addresses can be exempted
- Consecutive successful logins place user's IP address in the **Auto Exempt** list

Security > Authentication Reputation > Setting



Security > Authentication Reputation > Exempt



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

SMTP authentication mitigates the problem of an SMTP brute force attack by tracking the IP addresses of the offending client attempting to connect to the box. SMTP authentication can detect and block attackers.

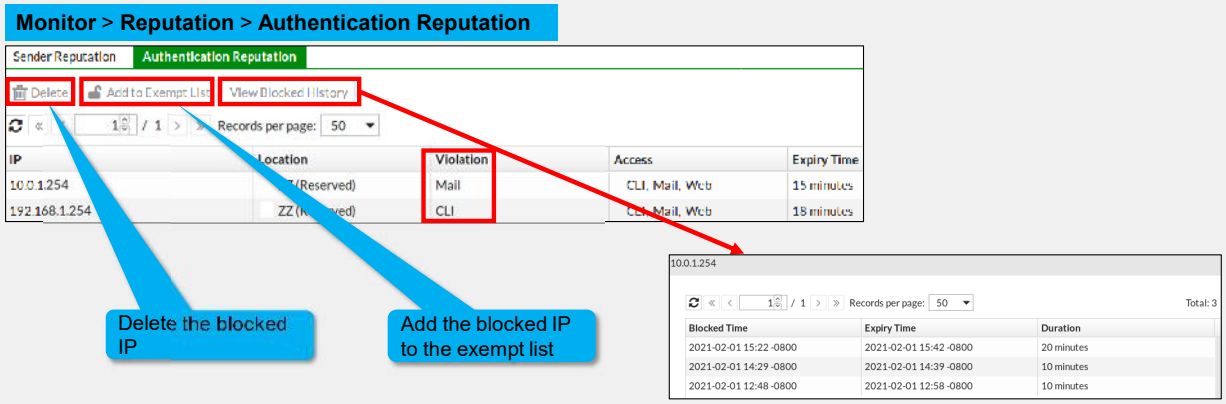
If a user has consecutive successful logins within a specified period of time, the user's IP address will be automatically added to an auto/dynamic exempt list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Authentication Reputation for Blocked IP

- Blocked IP addresses appear in the **Authentication Reputation** tab
- The attacker will be denied CLI, mail, and web access for the duration of the expiry period
- The violation column shows the cause for access violation



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

FortiMail tracks failed login attempts made from the CLI, mail, and web. Blocked IP addresses can be deleted manually or added to the exempt list.

The violation column shows the cause for access violation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Failed Authentication Logging

- Failed authentications are recorded in the history logs
  - **Classifier**: SMTP Auth Failure

Monitor > Log > History

History | System Event | Mail Event | AntiVirus | AntiSpam | Encryption

List | View | Search | Export

2021-01-26 17:40:07 -> Current

1 / 8 Records per page: 100 Go to line:

#	Date	Time	Classifier	Disposition	From	Header From ...	To	Subject	Session ID
1	2021-02-01	15:22:14.178	SMTP Auth Failure	Reject	extuser@exte...				111NMEnm016202-111N...
2	2021-02-01	15:22:13.092	SMTP Auth Failure	Reject	extuser@exte...				111NMEx0016200-111N...

Log Details: 0003016202

Column	Content
Date	2021-02-01
Time	15:22:14.178
Message	SMTP authentication failure: authid=extuser@external.lab, authtype=LOGIN, client_ip=10.0.1.254, detail=SASL(-1): generic failure: checkpass failed
Session ID	111NMEnm016202-111NMEno016202

Session rejected because of access receive rule enforcing authentication

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

If an SMTP authentication attempt is unsuccessful, the system creates an entry in the history logs and assigns it an SMTP authentication failure classifier. You can use these log entries to troubleshoot and expose brute-force authentication attacks.

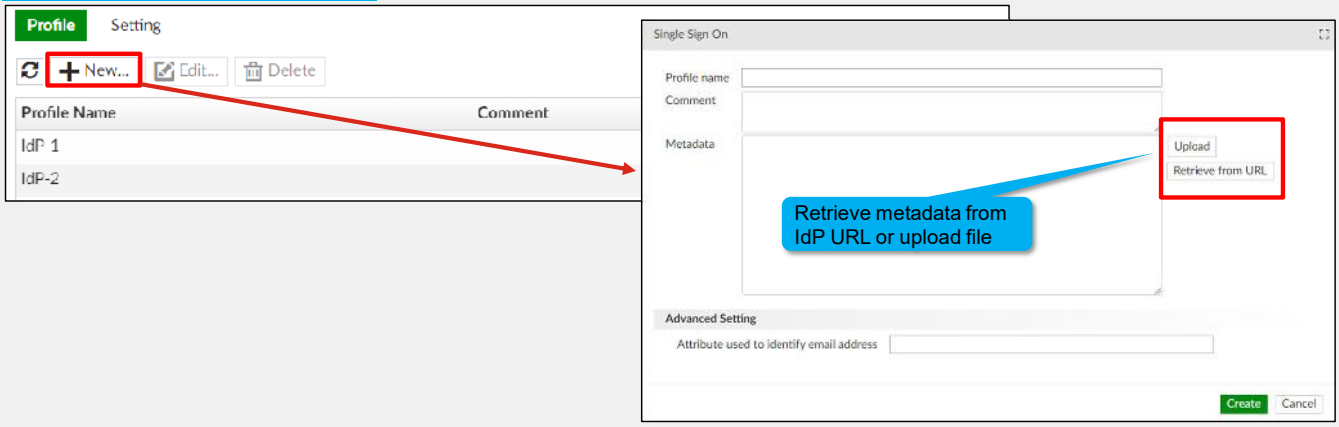
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Single Sign-On IdP Configuration

- FortiMail operates as a security assertion markup language (SAML) single sign-on (SSO) service provider to FortiOS identity provider (IdP)
- Supports multiple IdPs

System > Single Sign On > Profile



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

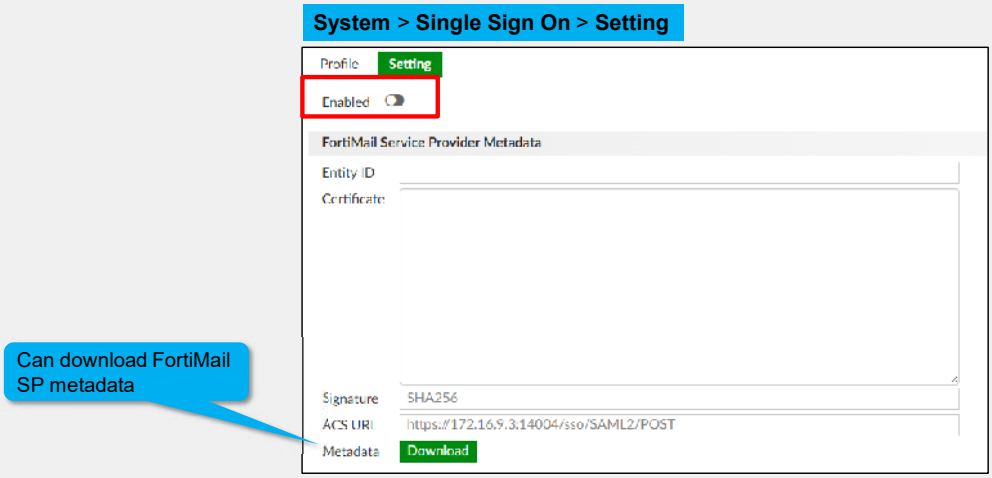
You can leverage FortiMail single sign-on capabilities using SAML by defining one or more IdPs in FortiMail, and then configuring FortiMail to act as a service provider (SP) for the defined IdPs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Single Sign-On SP Configuration

- FortiMail supports SAML SSO for:
  - Administrator login
  - Webmail login



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

FortiMail supports SAML SSO for both the administrator and webmail portals. If SSO is enabled, the administrator login page is presented with an SSO option, and the webmail login page is the SSO login page.

After you upload the IdP metadata, the FortiMail service provider metadata is automatically generated. You can download the service provider metadata and upload it to the IdP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which authentication type is supported by authentication profiles?
   A. TACACS+
   ✓ B. SMTP

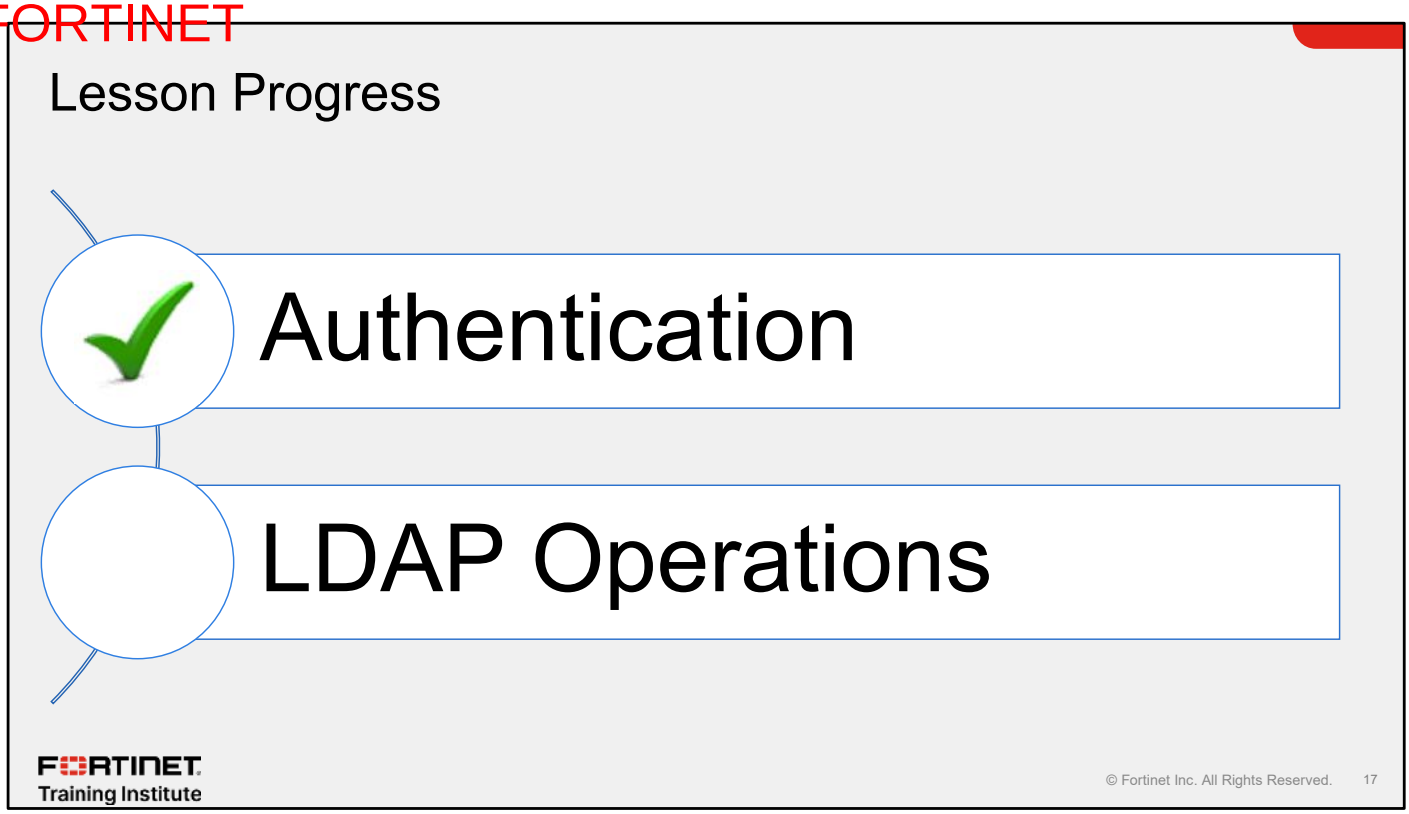
2. Which authentication protocol must you use to enable two-factor authentication for administrator logins?
   ✓ A. RADIUS
   B. LDAP

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

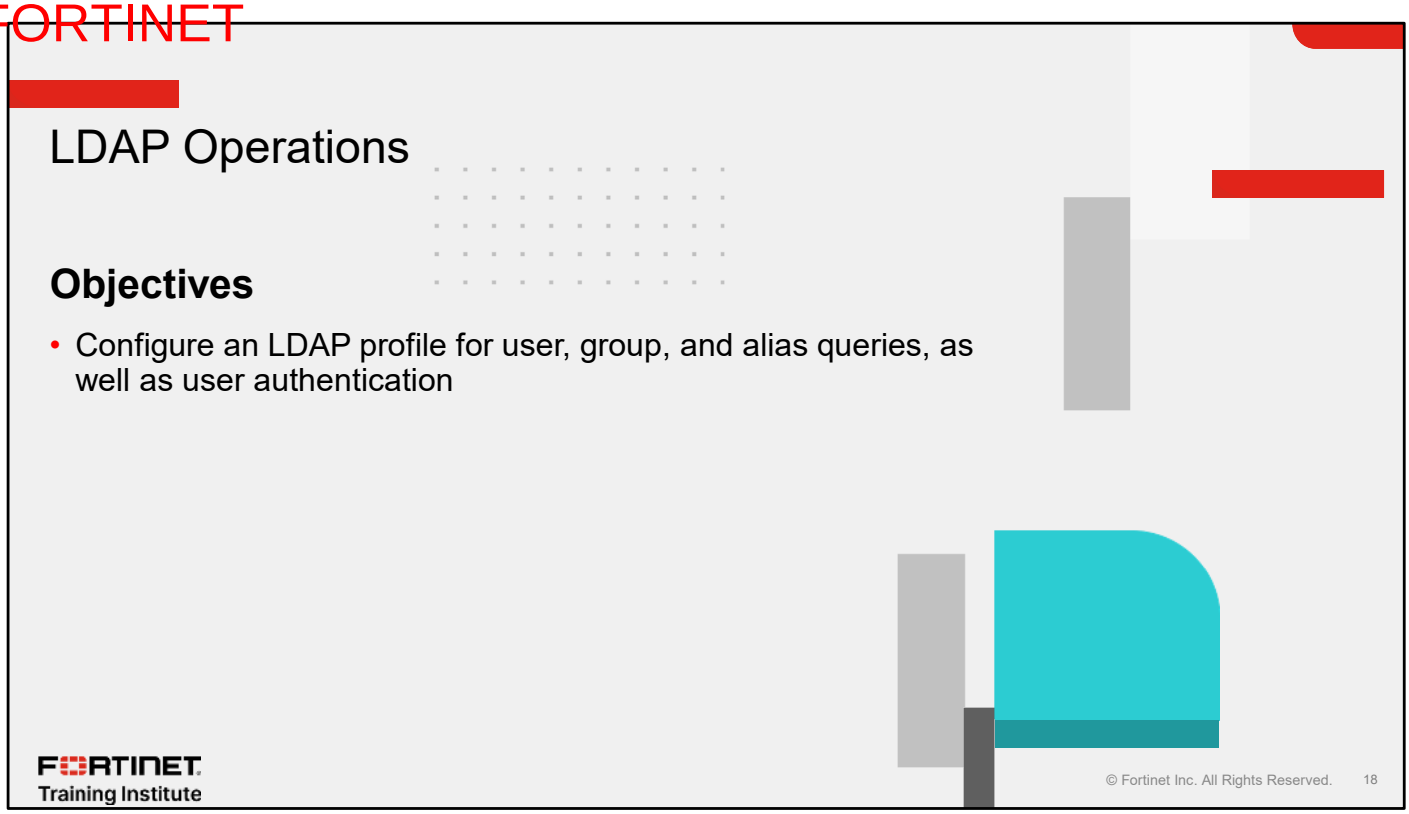


Good job! You now understand how authentication works on FortiMail.

Now, you will learn about LDAP operations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in LDAP operations, you will learn how you can use LDAP profiles on FortiMail for more than just user authentication. You can use LDAP profiles for user, alias, and group queries, as well as domain lookups and mail routing.

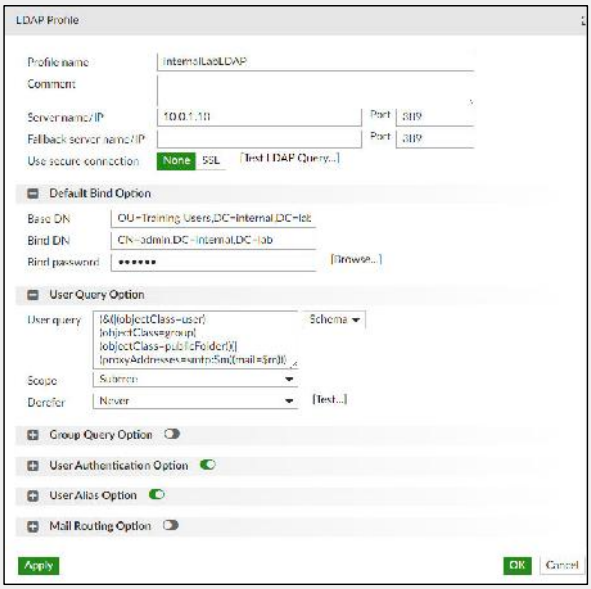
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

LDAP Profile

- Integrate FortiMail with an LDAP server for:
  - User query
  - Group query
  - User authentication
  - User alias
  - Mail routing
  - Address mapping
  - Domain lookup

Profile > LDAP > LDAP



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

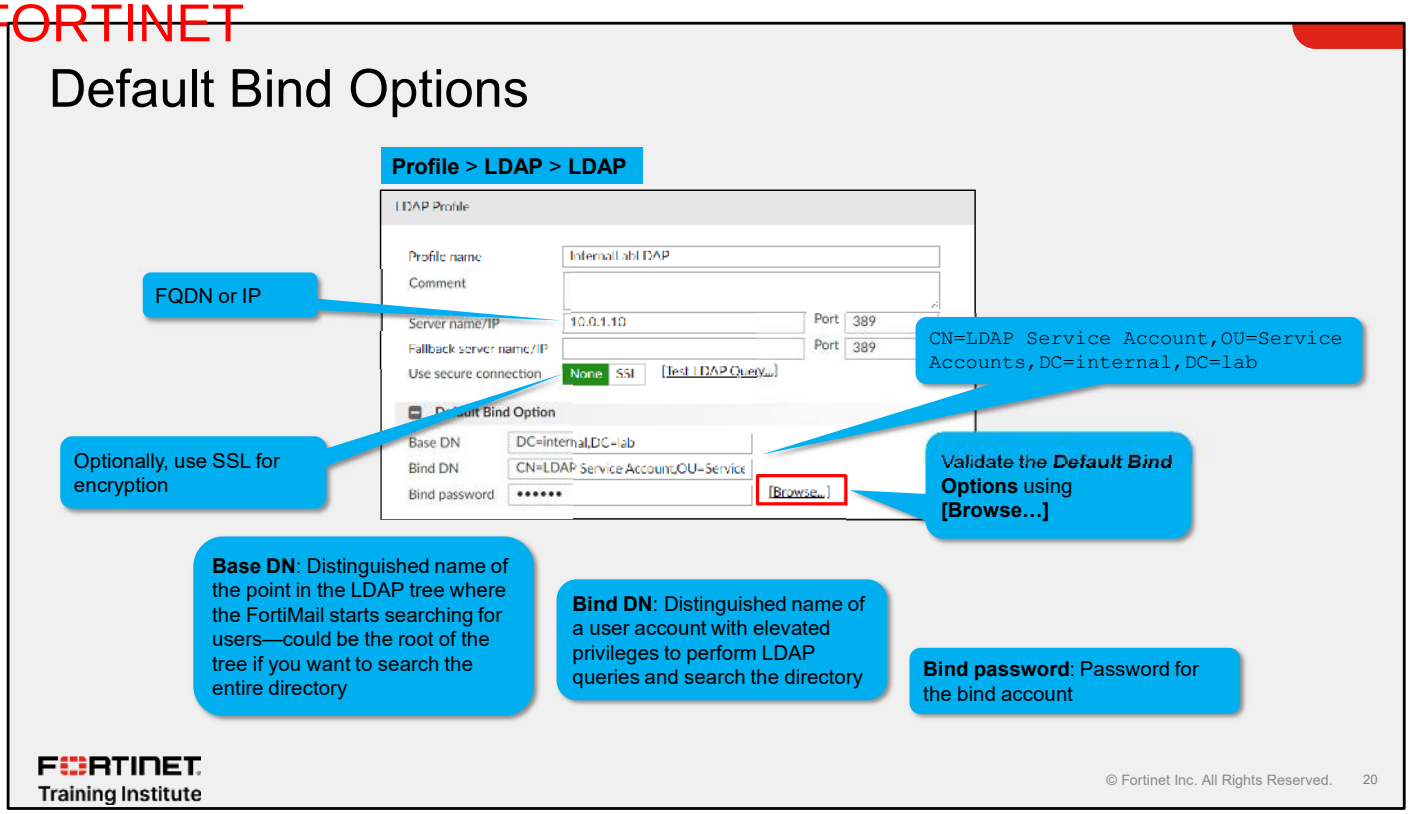
If your organization has an LDAP server, you should integrate it with FortiMail to reduce configuration overhead for FortiMail features, such as user alias and group lookups.

In this lesson, you will learn about the most commonly-used features of the LDAP profile, including the following:

- User query
- Group query
- User authentication
- User alias

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Before you can start using the LDAP profile, you must configure at least one server name and IP address, and the default bind options.

The **Base DN** field defines the distinguished name of the point in the LDAP tree where FortiMail starts searching for users. This could be the root of the tree or an organizational unit.

The **Bind DN** and **Bind Password** fields define the distinguished name and password of a user account with the necessary privileges to perform LDAP queries and search the directory. This account is also referred to as a bind account.

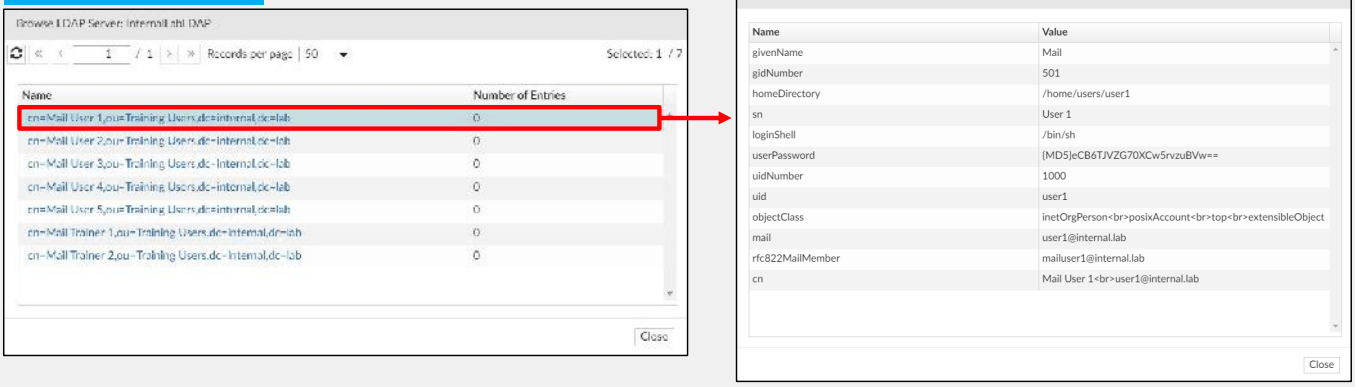
The default bind options rely solely on the backend LDAP server vendor and schema. The example shown on this slide is based on a Windows Active Directory LDAP server. To validate your settings, click **[Browse…]**. If your configuration is correct, FortiMail fetches the contents of the base DN.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Browse Directory Sample Output

Profile > LDAP > LDAP



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

This slide shows an example of the output that appears after you click **[Browse]**. FortiMail fetches all the objects in the base DN. To view more details, you can click individual objects, down to individual entries.

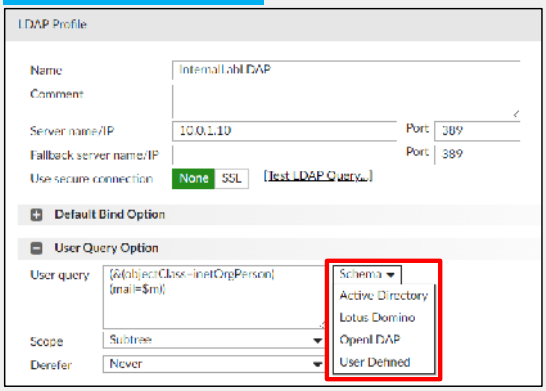
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

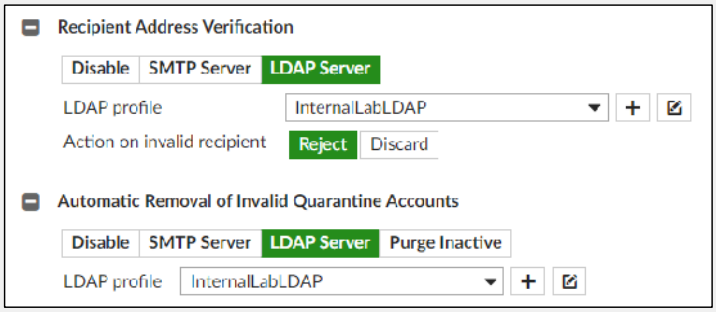
User Query Options

- Select one of the predefined schema or define your own
- Query must be able to search for users based on email address
- You can select options for recipient address verification or automatic removal of invalid quarantine accounts for protected domains

Profile > LDAP > LDAP



Domain & User > Domain > Domain



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

Use the user query options to specify a query string, which will return a user based on their email address. The query string syntax differs based on the backend LDAP server schema. FortiMail has predefined strings for an active directory, lotus domino, and open LDAP. You can also define your own query string to work with any custom LDAP implementation, as long as you define the query to search for users based on their email address.

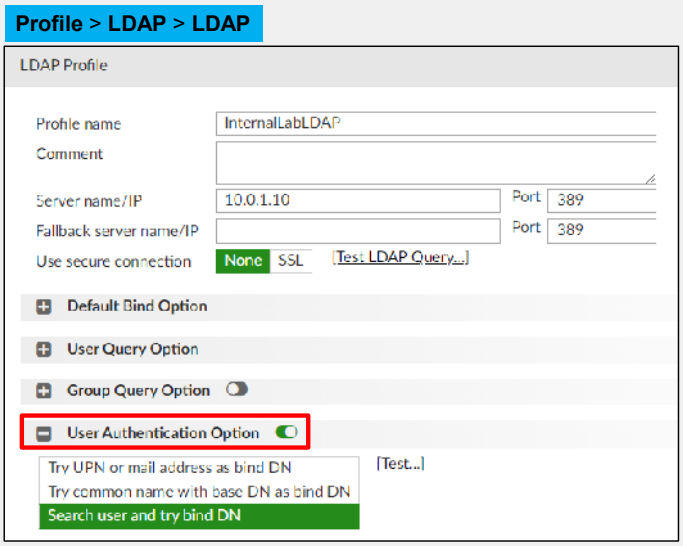
This user query function is used by **Recipient Address Verification** and **Automatic Removal of Invalid Quarantine Accounts** for protected domains.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

User Authentication Options

- LDAP profile verifies user credentials using **User Authentication Options**
- Enabled by default
- User authentication options
  - Try UPN or mail address as bind DN
  - Try common name with base DN as bind DN
  - Search user and try bind DN



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

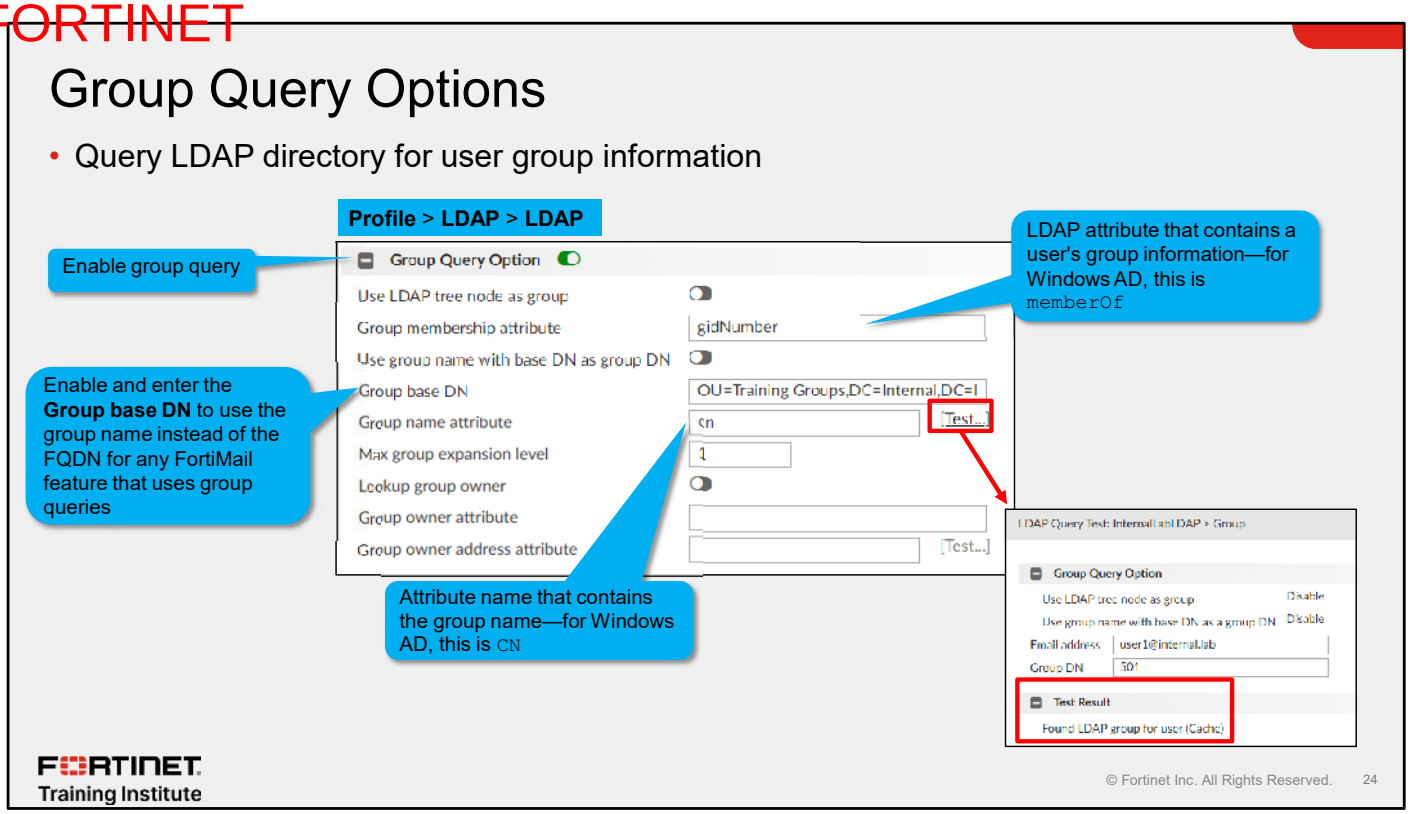
By default, **User Authentication Options** is enabled in all LDAP profiles. User authentication options are:

- **Try UPN or mail address as bind DN**: FortiMail will use the name portion of the email address in conjunction with the UPN to form the user's bind DN.
- **Try common name with base DN as bind DN**: User's bind DN is formed using the common name value and the base DN value.
- **Search user and try bind DN**: FortiMail forms the user's bind DN using the retrieved DN using the User Query Option LDAP settings.

At minimum, you must configure the **Default Bind Options** and **User Query Options** settings, to use the LDAP profile for recipient address verification, automatic removal of invalid quarantine accounts, user authentication using policies, and administrator authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **Group Query Options** section allows you to configure the necessary settings to use user group membership queries. Many FortiMail features can use group queries to create a highly customized configuration. The settings you must use depend solely on the backend LDAP server schema. For example, selecting **memberOf** as the **Group membership attribute** and **CN** as the **Group name attribute** are only relevant for Windows AD.

The **Use group name with base DN as group DN** option allows you to use the group name instead of the fully distinguished name for any FortiMail feature that uses group queries. To make configuration easier, enable **Use group name with base DN as group DN** and enter in the **Group base DN**. You will see an example of this on a later slide.

To validate your settings, click **[Test…]**. In the **LDAP Query Test** window, enter a user's email address and the group name and click **Test**. If your configuration is correct, the results show whether the user is a member of the group or not.

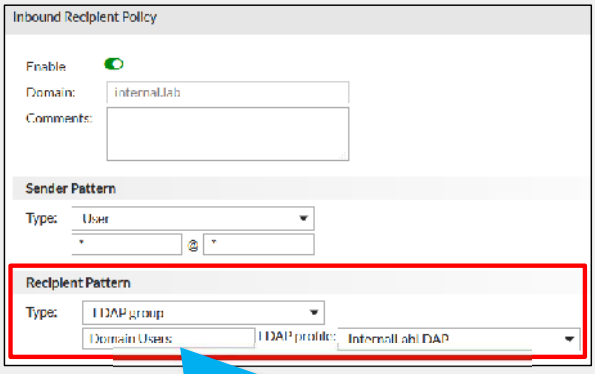
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Group Query Example

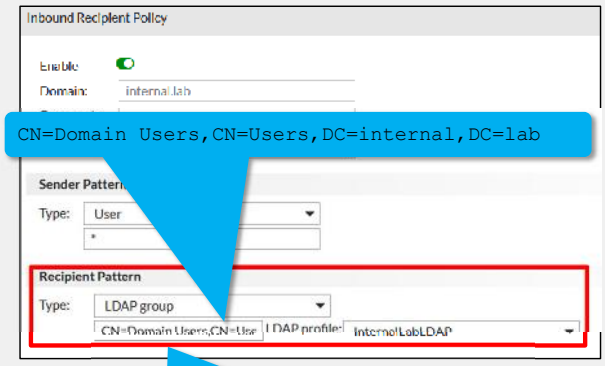
- Create inbound, recipient-based policies for specific groups
- Allows you to customize inspection profiles based on user group membership

Policy > Recipient Policy > Inbound



With **Use group name with base DN as group DN** enabled

Policy > Recipient Policy > Inbound



Without **Use group name with base DN as group DN** enabled

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

This slide shows an example of an LDAP group query being used to craft inbound, recipient-based policies. You can customize inspection profiles, based on user group membership. This example also shows the configuration requirement with and without the **Use group name with base DN as group DN** option enabled in the LDAP profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

User Aliases

- A single user may have multiple aliases
- Use the LDAP user alias query to convert these aliases dynamically into a single primary email address
- Consolidates all quarantine reports for aliases to the single primary email address for gateway and server mode deployments
  - Without user alias lookup, a user with five aliases could potentially receive a different quarantine report for each account

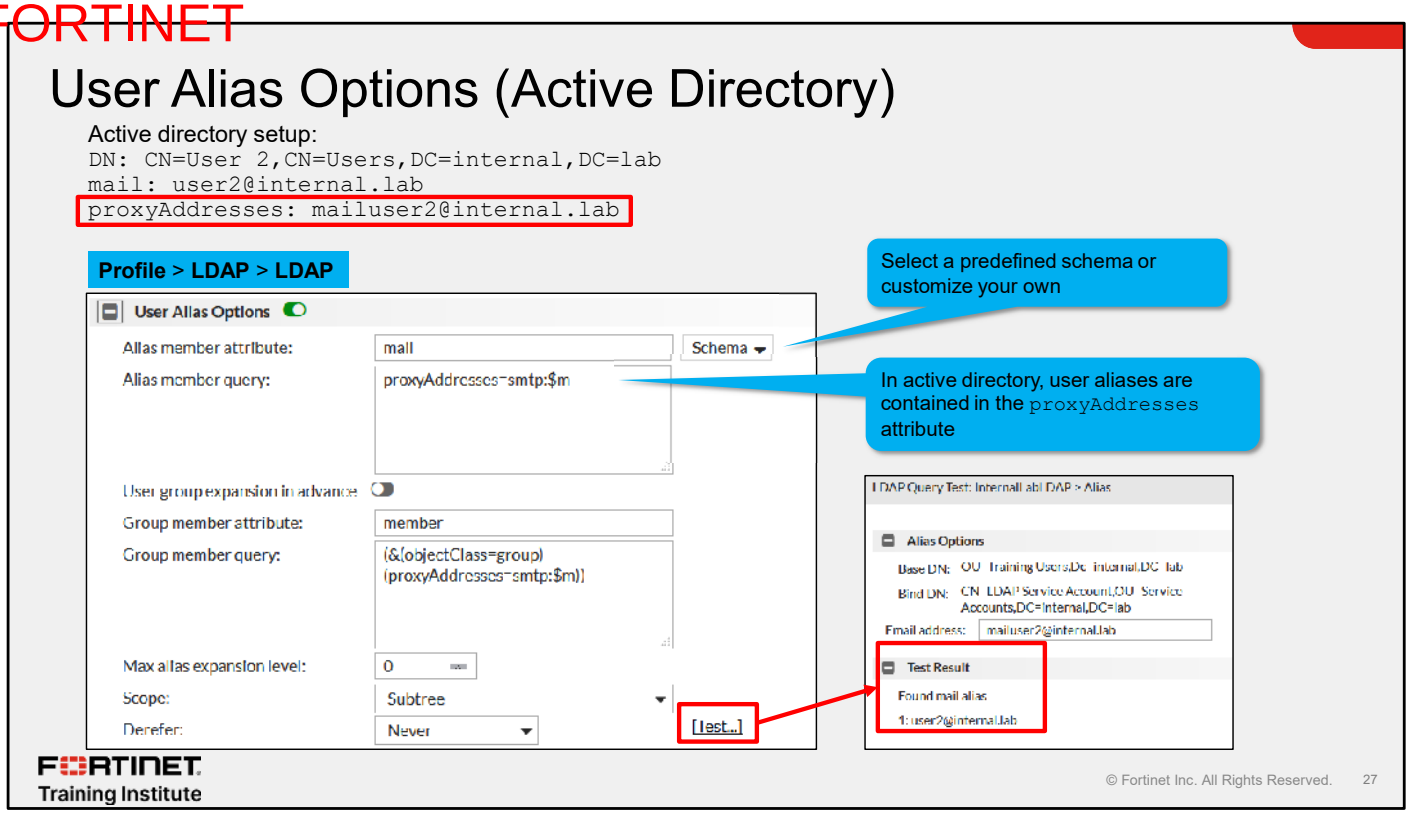
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

The **User Alias** option converts email aliases into a user's real email address. On FortiMail, use this option to consolidate objects in FortiMail that are stored using an email address as the identifier. For example, if a user has five aliases in addition to a primary email address, FortiMail can use this feature to maintain a single user quarantine, instead of six separate quarantines and quarantine reports.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To use the user alias feature, select a predefined schema or customize one to fit any LDAP server.

The default active directory schema alias member query is set up to perform alias expansion based on groups. To perform an alias expansion, you must change the query to search for proxy addresses.

To validate your settings click **[Test…]** and then enter a proxy address. If the configuration is correct, FortiMail retrieves the corresponding mail attribute.

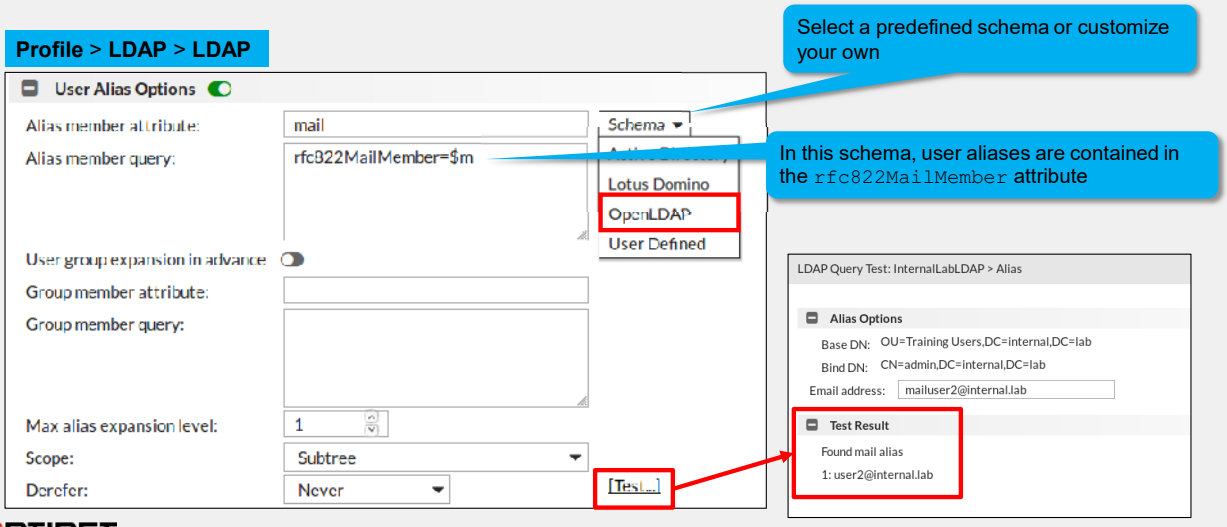
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

User Alias Options (Open LDAP)

Open LDAP setup:

```
DN: CN=User 2,CN=Users,DC=internal,DC=lab
mail: user2@internal.lab
rfc822MailMember: mailuser2@internal.lab
```



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

This slide shows an example user alias configuration with an Open LDAP server. This particular **OpenLDAP** schema is also used in the lab environment. Please note that not all **OpenLDAP** deployments are the same. You will have to match the proper attributes based on your own LDAP schema.

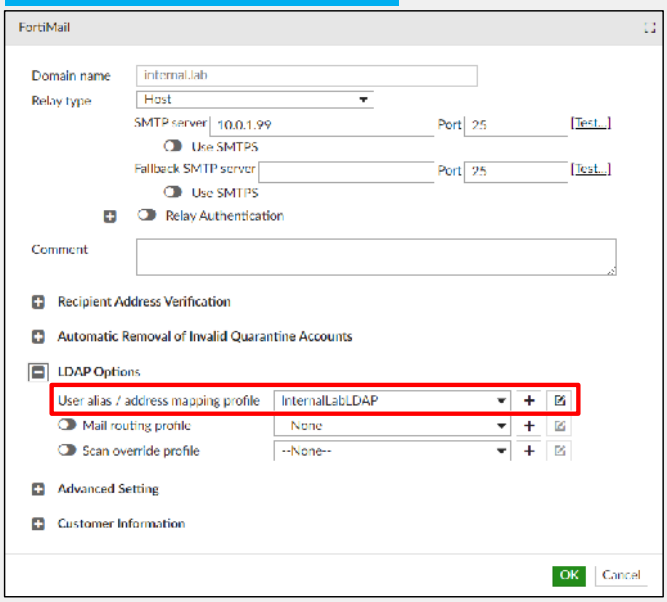
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

LDAP User Alias Mapping

- Apply the LDAP profile for alias mapping in the protected domain configuration

Domain & User > Domain > Domain



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 29

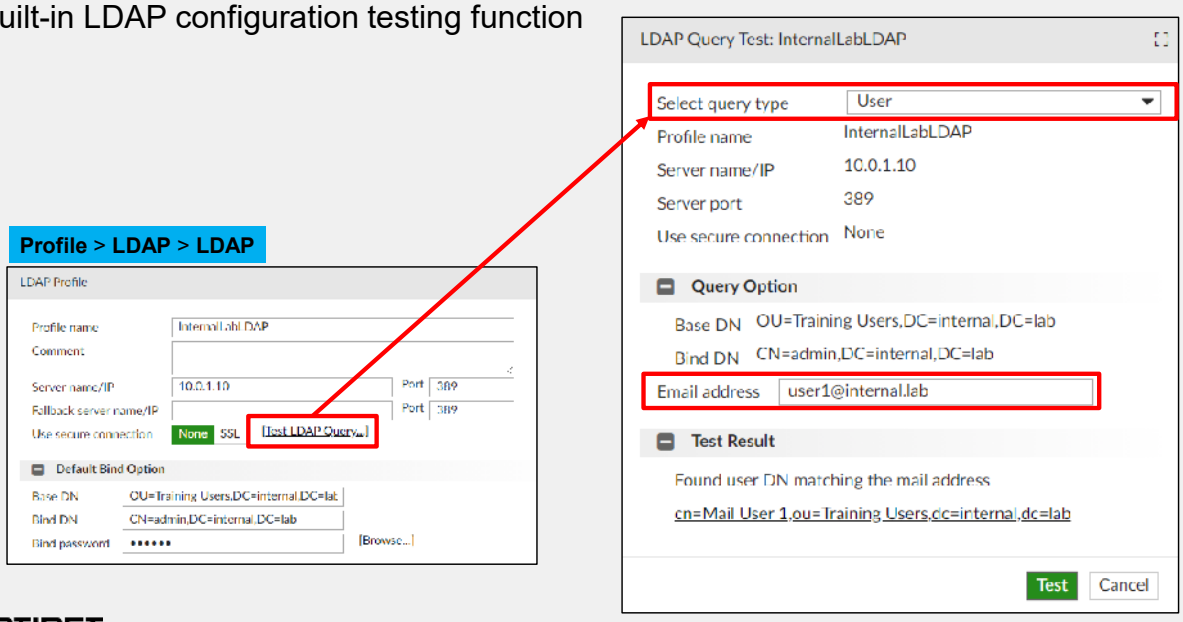
You can enable user alias mapping on the protected domain configuration page. If you do not see the **LDAP Options** section, you may need to enable the advanced view in the GUI settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Test LDAP Query

- Built-in LDAP configuration testing function



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

Click **[Test LDAP Query…]** to validate various sections of the LDAP configuration, including the following:

- User query
- User authentication
- Group lookup
- Alias expansion

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Why do you need to enable the user alias option?
   - ✓ A. It consolidates all quarantine reports for aliases with the single primary email address.
   - B. It can reduce the number of emails processed by FortiMail.

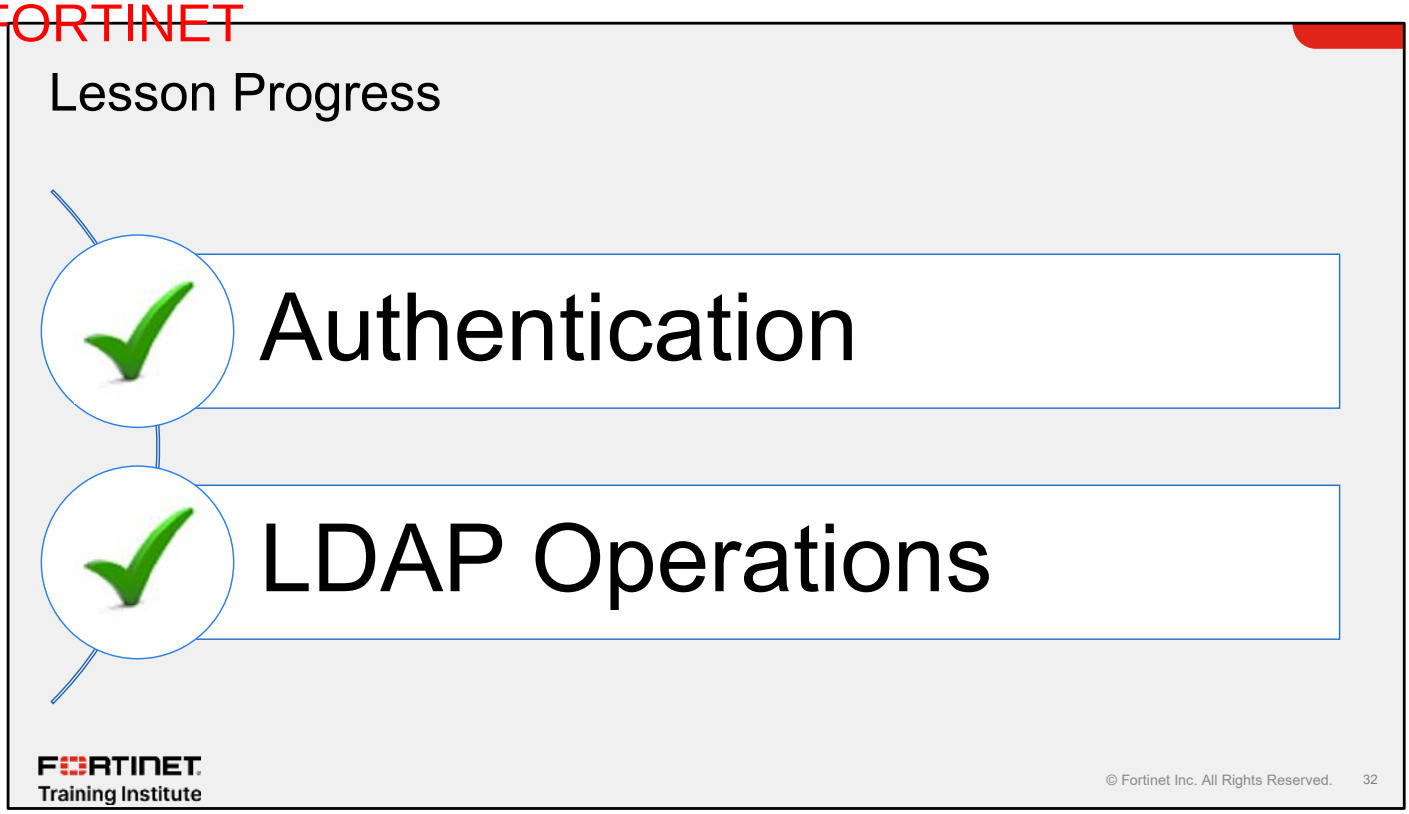
2. Which query function is used in an LDAP profile, for recipient address verification?
   - ✓ A. User query
   - B. Alias member query

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Use authentication profiles to define sources for user credentials
- ✓ Enable IP-based or recipient-based policy authentication
- ✓ Enforce authentication using access control rules
- ✓ Configure an LDAP profile for user, group, and alias queries, as well as user authentication

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure and enforce authentication on FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FORTINET
Training Institute

FORTINET
CERTIFIED
PROFESSIONAL
Public Cloud
Security

FortiMail Administrator

Session Management

FortiMail 7.4

Last Modified: 25 April 2024

In this lesson, you will learn about session management and related features.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Overview

- Session Profile
- Sender Address Rate Control
- Message Size Management

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 2

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Session Profile

Objectives

- Limit sessions from remote mail transfer agents (MTAs)
- Throttle email volume based on sender reputation
- Reject connections from blocklisted MTAs
- Validate senders using sender policy framework (SPF) and DomainKeys Identified Mail (DKIM)
- Implement outbound DKIM signing of email messages
- Detect errors and abnormalities in SMTP sessions
- Hide internal network information in email headers

FORTINET Training Institute

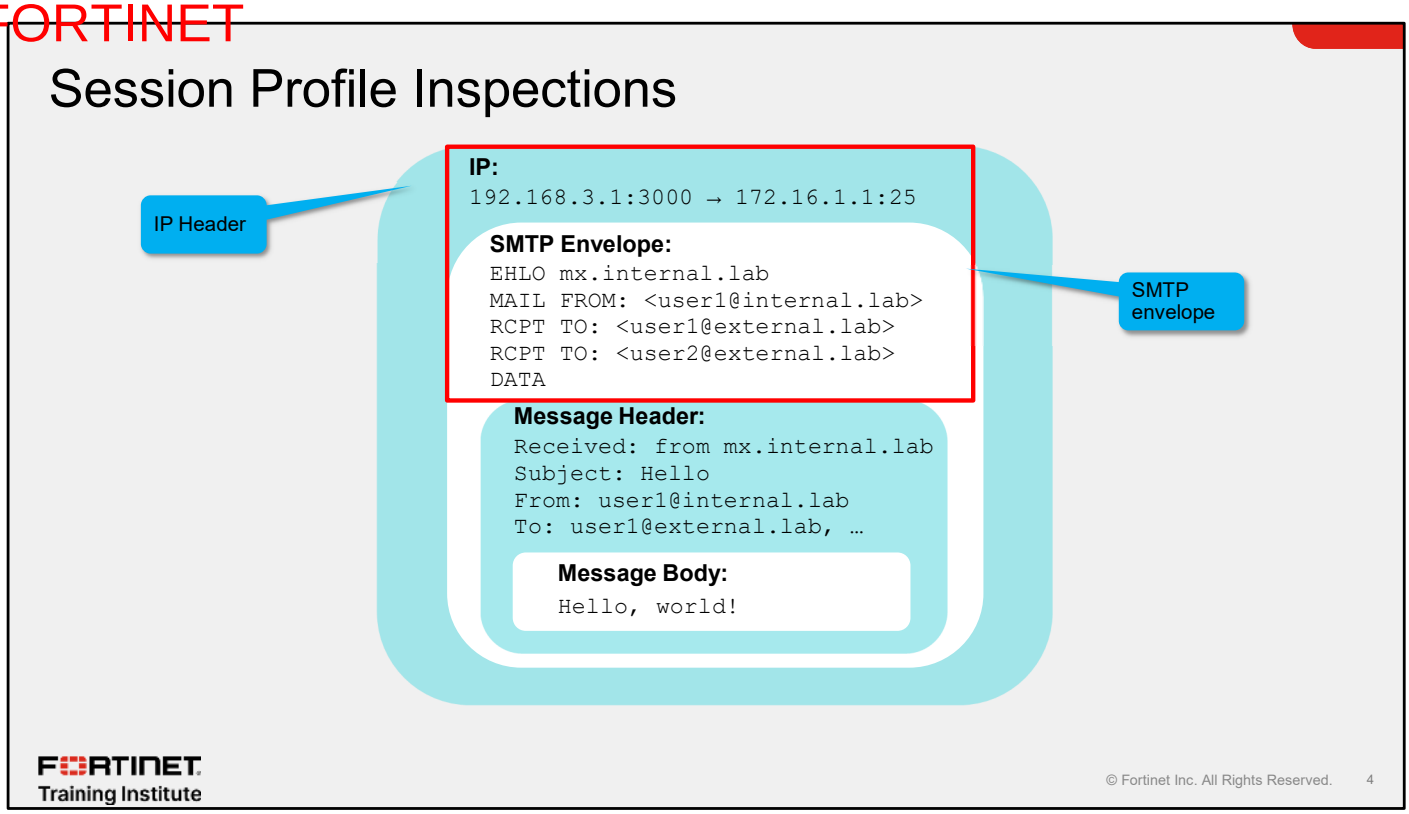
© Fortinet Inc. All Rights Reserved. 3

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the session profile, you will be able to configure the session profile to inspect properties of SMTP connections at the lowest layers—from the IP session to the SMTP envelope. You will also be able to configure and use session profile options.

Vouchers & Dumps are Available | WhatsApp +201224560923

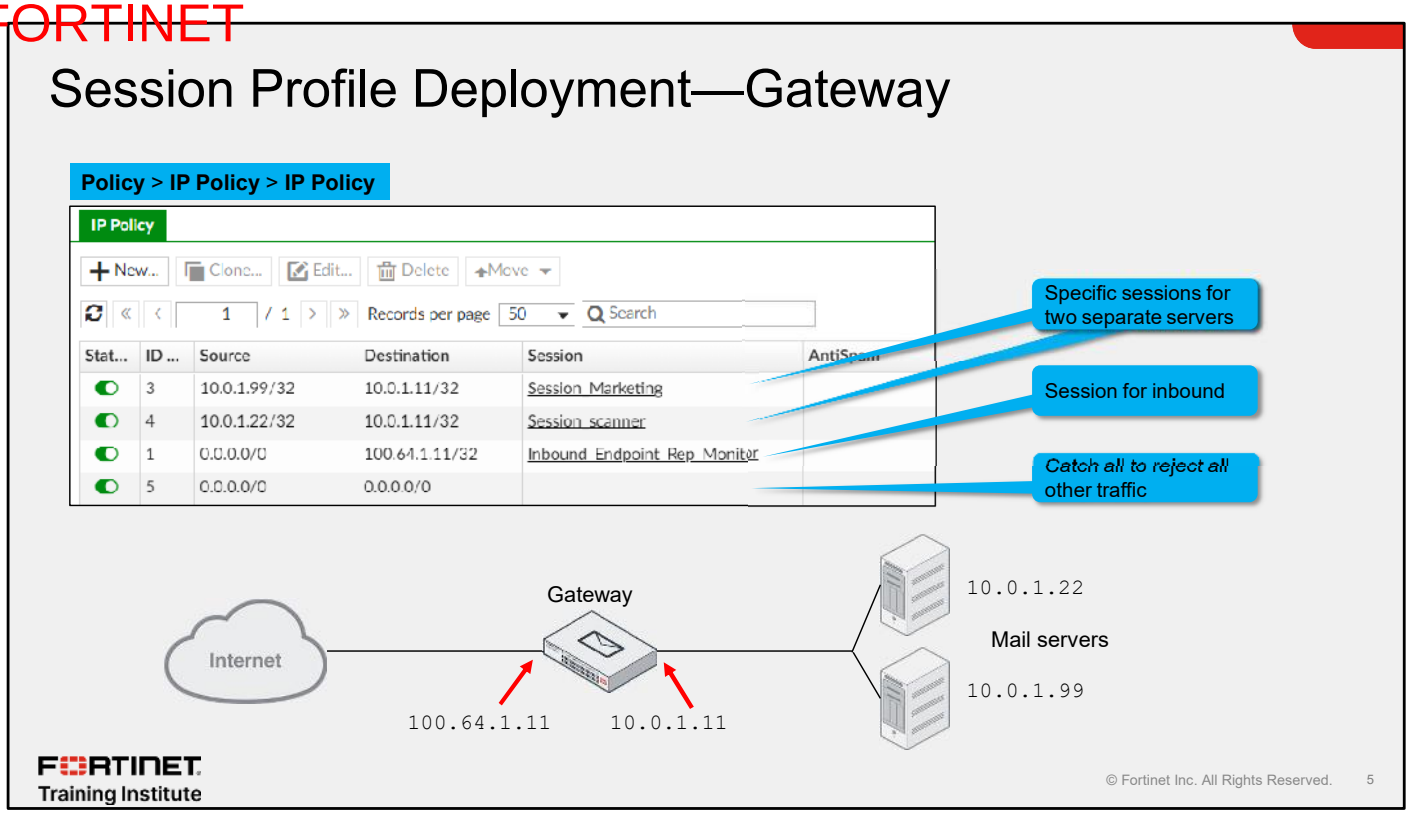
DO NOT REPRINT Brave-dumps.com
© FORTINET



The overall purpose of session profile inspections is to detect suspicious activity as soon as possible. Early detection allows FortiMail to take action early, and eliminates the need to perform some, or all, of the more resource-intensive scans that are required after the *entire* email message arrives.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



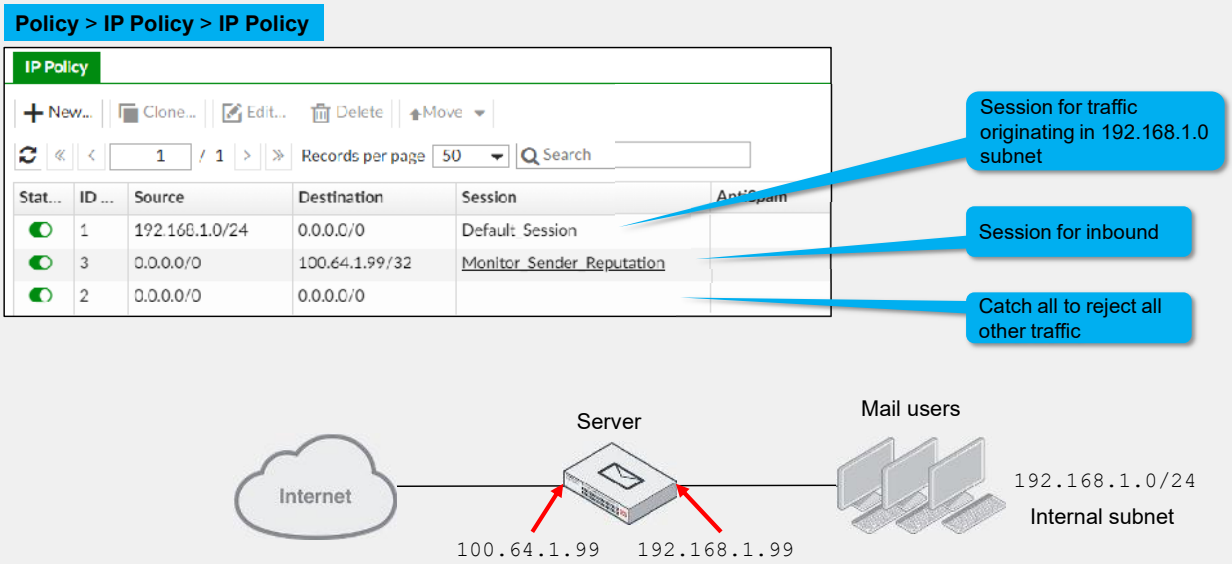
Session profiles are unique, because they can be referenced only by IP policies. You should create separate IP policies for outbound and inbound email, regardless of the deployment mode you are using.

This type of IP policy and session profile setup allows you to disable specific session profile features for your internal assets, such as sender reputation, while still enforcing those features for all inbound email.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Session Profile Deployment—Server



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

Server deployments will often have sources defined by subnets to allow MUAs installed on end user devices to send and receive mail messages. In the example shown on this slide, devices on the internal subnet can send and receive email through the server. The outbound traffic has session settings applied by policy ID 1, and inbound traffic has session setting applied by policy ID 3.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Session Profile Deployment—Transparent

Policy > IP Policy > IP Policy

IP Policy

New... | Clone... | Edit... | Delete | Move

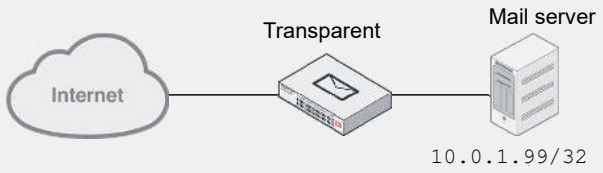
1 / 1 | Records per page 50 | Search

Stat...	ID ...	Source	Destination	Session	AntiSpam
	1	0.0.0.0/0	10.0.1.99/32	Inbound Endpoint Rep Monitor	
	3	10.0.1.99/32	0.0.0.0/0	Session_scanner	
	2	0.0.0.0/0	0.0.0.0/0		

Session for traffic destined for mail server

Session for outbound

Catch all to reject all other traffic



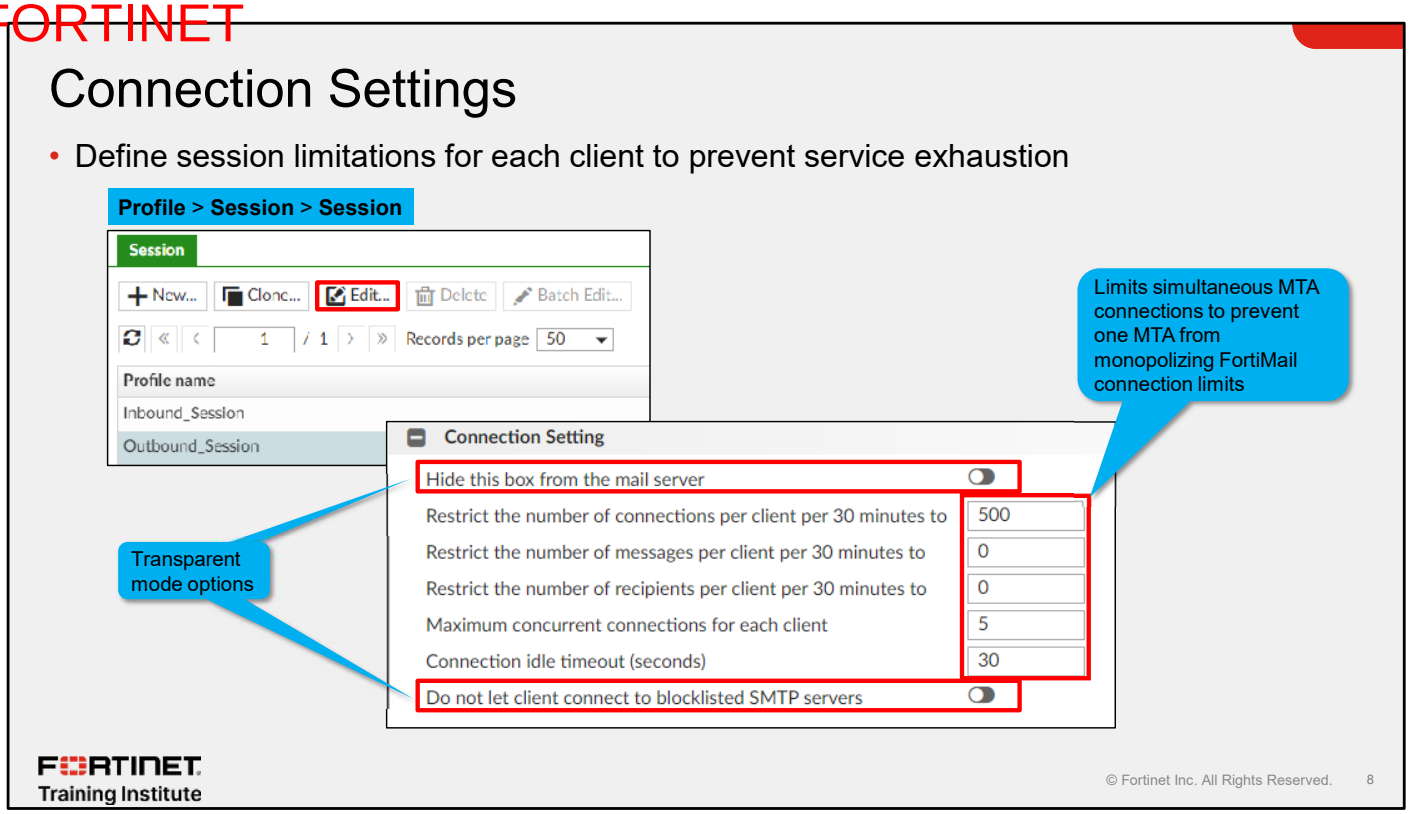
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

In a transparent mode deployment, the FortiMail acts as a relay or proxy for incoming and outgoing mail. Session settings are applied as mail passes through FortiMail on its way to or from the mail server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The session profile settings in the **Connection Settings** section allow you to set limits on the number of connections, messages, recipients, and concurrent connections for each client. Since each connection consumes resources, you can use limits to prevent a single MTA from exhausting FortiMail services.

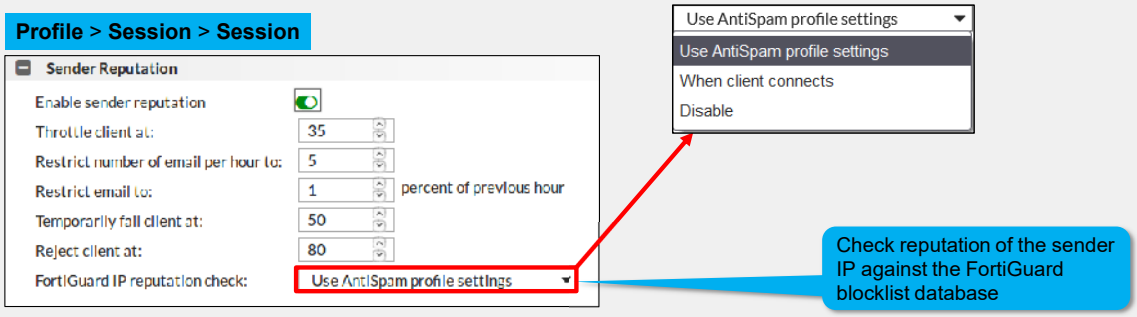
If FortiMail is operating in transparent mode, then two additional options appear on the GUI that govern FortiMail low-level connection behaviors. You will learn about transparent mode in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Sender Reputation

- Maintenance-free way to manage session volume
- 12-hour moving weighted average
- Score calculated for each client IP address as a percentage of email that is spam, is infected, or has invalid recipients or senders
- Block spammers at the connection phase to reduce inspection tasks



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

As FortiMail processes and scans email messages, it maintains a sender reputation score for the IP address of each external MTA that opens an inbound SMTP connection. This score is calculated as the percentage of email from this sender that is spam, contains a virus, or has invalid recipients or senders, during a 12-hour period. The higher the score, the worse the sender's reputation. You can use the sender reputation score in the session profile to set score thresholds for FortiMail to throttle the client, issue a temporary fail message, or reject the client at this early stage. FortiMail can also check the reputation of the sender IP address against the FortiGuard blocklist database.

The **FortiGuard IP reputation check** drop-down list has three possible settings. If you select **Use AntiSpam profile settings**, FortiMail applies the action that is defined in the matching antispam profile. Unlike most session profile inspections, if you select **Use AntiSpam profile setting**, FortiMail processes the entire message before applying the action. If you select **When client connects**, FortiMail applies the FortiGuard IP reputation check immediately during the connection phase.

You will learn more about antispam profiles and actions in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

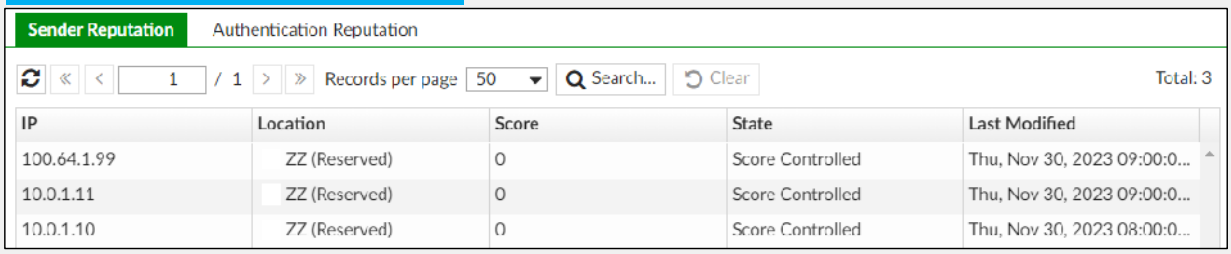
DO NOT REPRINT Brave-dumps.com
© FORTINET

Sender Reputation List

- Use the CLI to clear the sender reputation database

```
# execute db reset sender-reputation
```

Monitor > Reputation > Sender Reputation



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

You can view the current sender reputation statuses on the **Sender Reputation** page. By default, this view shows the scores sorted in descending order, with the worst reputation at the top. You can use this view to identify the worst offenders and troubleshoot the possible causes of delayed or rejected messages.

Any changes that you make to the sender reputation configuration will take some time to manifest because of the scoring system. To clear the reputation list and force all scores to be recalculated from a blank state, use the CLI command shown on this slide.

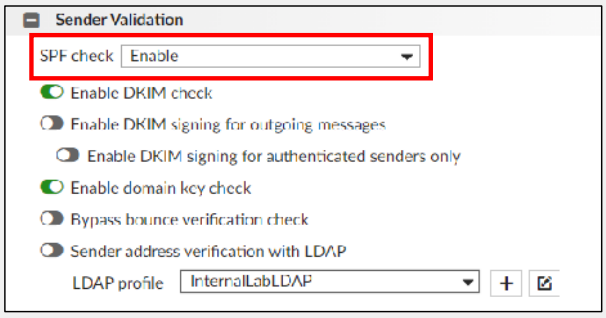
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Sender Validation

- Sender policy framework (SPF):
  - Check the DNS TXT record of the sender domain for permitted servers
  - Unauthorized client IP address increases the client sender reputation score
  - To be compliant with SPF checks of other organizations, publish your own SPF record in external DNS
  - To use, you must enable SPF checking in the session profile or the antispam profile

Profile > Session > Session



Partial SPF record for Fortinet

```
"v=spf1 ip4:208.91.113.0/24 ip4:208.91.114.0/24 mx include:Fortinet.co.jp -all"
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

A common sender validation technique is to use SPF. Using SPF, a domain owner publishes specially formatted DNS text (TXT) records. The records contain the authorized MTAs of the domain. The domain security relies on the fact that only authorized domain administrators are allowed to make changes to the domain DNS records.

If you enable SPF verification in the session profile, FortiMail performs a DNS TXT record lookup for the sending domain of any email session. If an SPF entry exists, FortiMail compares the address with the address of the sending MTA. The sender reputation decreases for authorized clients and increases for unauthorized clients.

While SPF is not universally adopted, it is still a simple and effective way to validate a sender's IP address. Enabling the SPF check in the session profile for all email won't be detrimental because, if FortiMail doesn't receive any responses for the DNS TXT record lookup, it skips the SPF check and continues processing the email.

SPF checking can be enabled in either a session profile or an antispam profile, or in both. However, if you select **Bypass SPF checking** in the session profile, SPF checking will be bypassed, even though you enable it in the antispam profile.

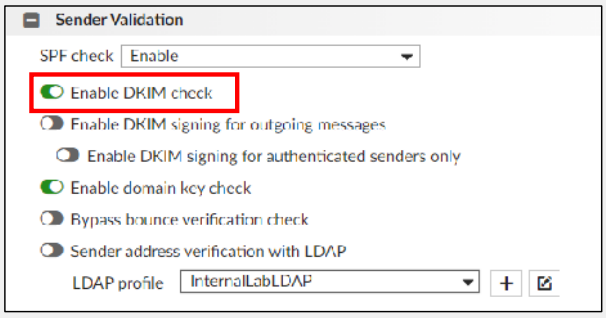
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Sender Validation (Contd)

- DKIM
  - Validates both MTA and email content
- Sending servers use a private key to generate a DKIM signature, and affix that signature to the email header
- Recipients query the DNS TXT record of the sending domain for the DKIM public key, and use it to validate the DKIM signature in the header
  - Public key is published in DNS as a TXT record
- Requires more processing than SPF validation

Profile > Session > Session



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

Unlike SPF, DKIM validates that the sending server is authorized to send mail for the domain. It also validates that mail content has not changed since being sent by the server. DKIM uses a public/private key signing process using DKIM keys stored in DNS.

With DKIM, the sending MTA uses its DKIM private key to generate a signature. The sending MTA then inserts the generated signature into the email header. The receiving MTA queries DNS for the sender domain TXT records, which contain the DKIM public key. The receiving MTA then uses the DKIM public key to validate the DKIM signature in the email header.

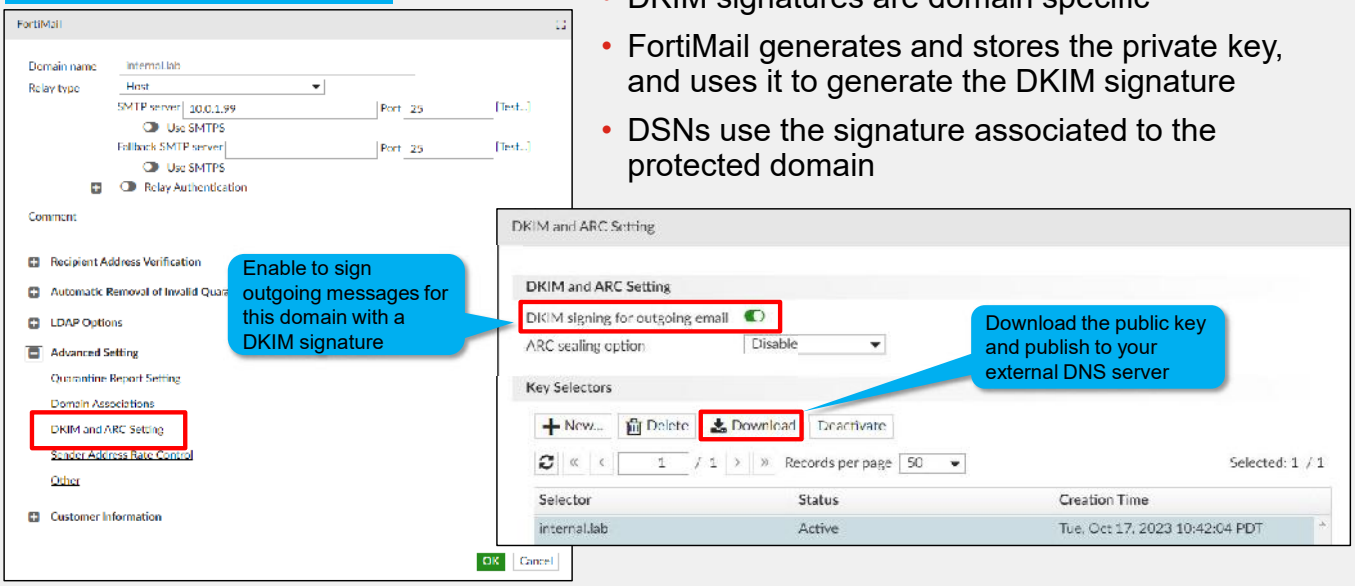
DKIM validation requires more processing than SPF validation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

DKIM Signing for Outbound Email

Domain & User > Domain > Domain



- DKIM signatures are domain specific
- FortiMail generates and stores the private key, and uses it to generate the DKIM signature
- DSNs use the signature associated to the protected domain

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

To configure DKIM signing for outgoing messages, you must first generate a public and private key pair for the domain. DKIM signatures are domain specific. FortiMail generates and stores the private key and uses it to generate the DKIM signature. After the key is created and activated, you must download the public key and publish it to your external DNS server. Enabling **DKIM signing for outgoing email** in the Domain settings to enable DKIM signing for all messages in that protected domain.

You can also in an appropriate session profile select **Enable DKIM signing for outgoing messages**, to start affixing the DKIM signature to all outbound email headers for that session.

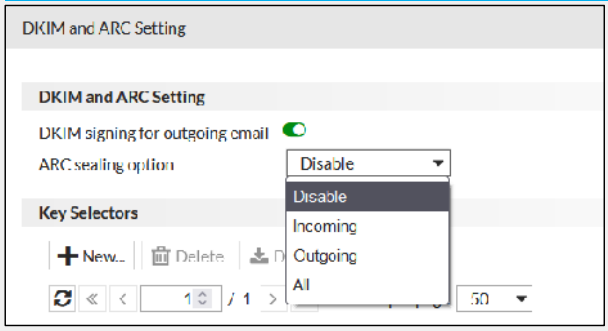
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

DKIM and ARC

- Authenticated Received Chain (ARC)
- Allows intermediary servers to validate a DKIM signature and seal it with a signature
- FortiMail can sign (seal) messages for a domain based on direction
- Allows trust in a DKIM signature when it passes through an intermediary and is changed

Domain & User > Domain > Domain > DKIM and ARC Setting



FORTINET Training Institute

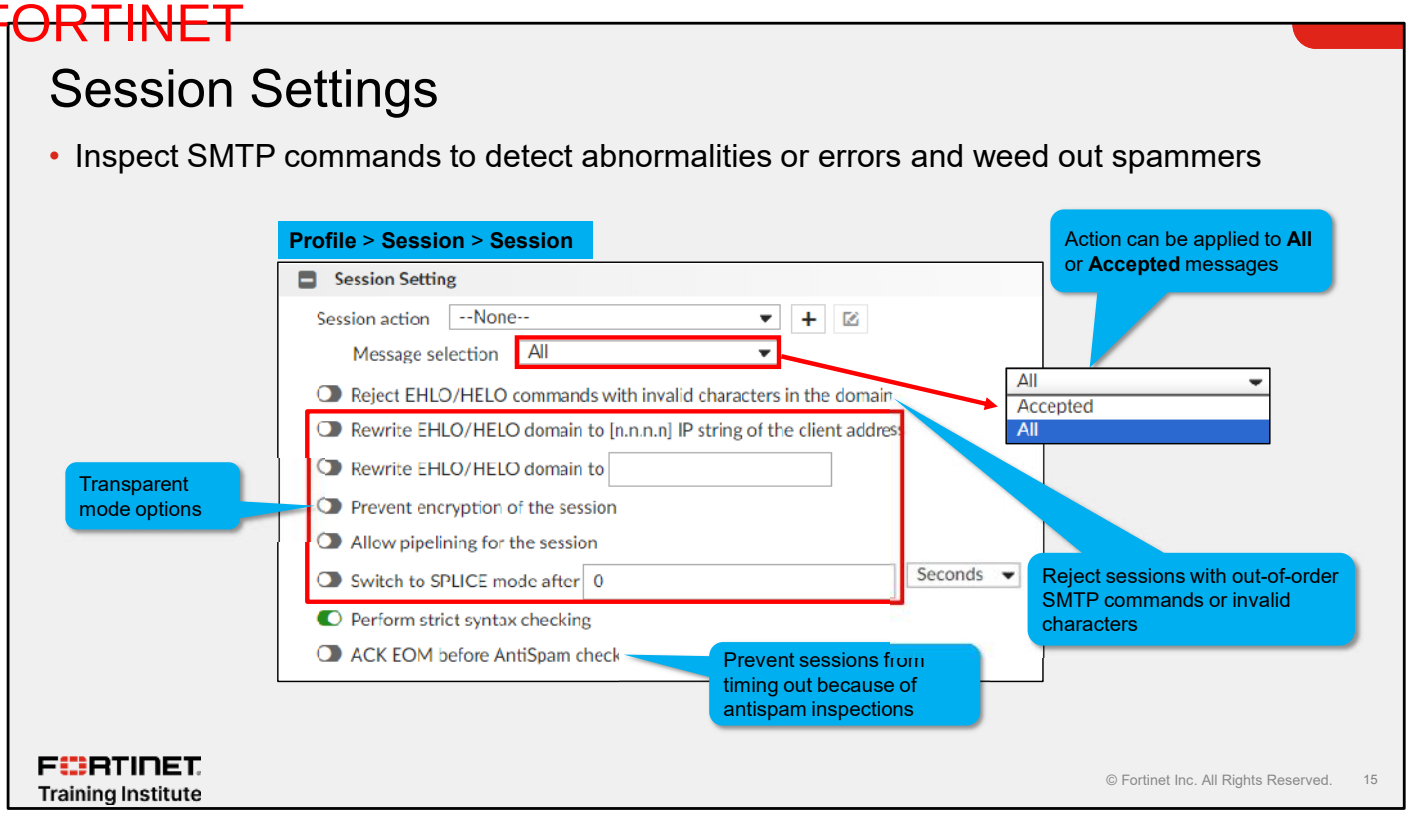
© Fortinet Inc. All Rights Reserved. 14

ARC permits intermediate email servers (such as mailing lists or forwarding services like FortiMail) to sign the original DKIM results of an email. This allows a receiving service to validate an email, in the event the SPF and DKIM records of the email are rendered invalid by the processing of an intermediate server. You can find further information about ARC in *RFC 8617* and in the *FortiMail Administration Guide*.

Support for ARC sealing started in FortiMail 7.2.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **Session Settings** section of the session profile contains the settings that you use to inspect and control many aspects of the SMTP protocol.

Most legitimate MTA implementations are based on mature codebases and are compliant with standards. The chance of SMTP protocol errors occurring is almost zero. Spammers, on the other hand, are known to use homegrown scripts and code that often exhibit protocol errors. You can use strict syntax and invalid character checking to identify suspicious behavior and reject sessions that show abnormalities. You can also have FortiMail acknowledge end-of-message or, if using transparent mode, switch to splice mode, to prevent the session from timing out because of antispam inspections.

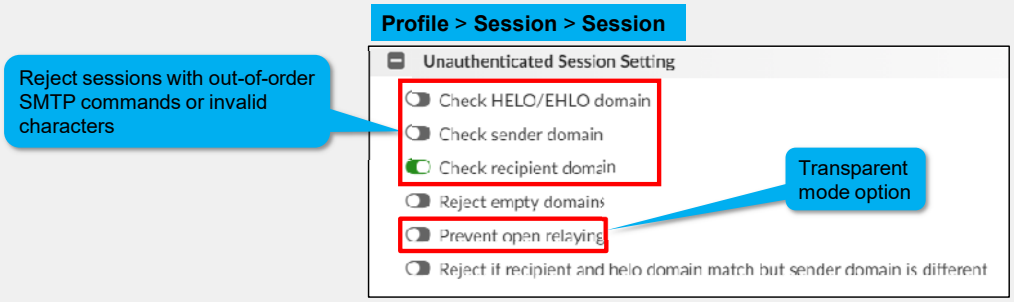
FortiMail instances operating in transparent mode have additional options that you can use to manipulate the SMTP session. These options include the ability to rewrite the `EHLO` or `HELO` greeting strings, and prevent session encryption negotiations, so that the message is sent in clear text. This enables FortiMail to scan the contents of email messages that would otherwise be encrypted.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Unauthenticated Session Settings

- For devices that can't authenticate using SMTP AUTH, for example, other MTAs
- Validate HELO or EHLO, sender, and recipient domains using DNS MX or A record lookup



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

Unauthenticated session settings are used to control sessions that are not authenticated using SMTP AUTH. These settings enable you to enforce stricter checks.

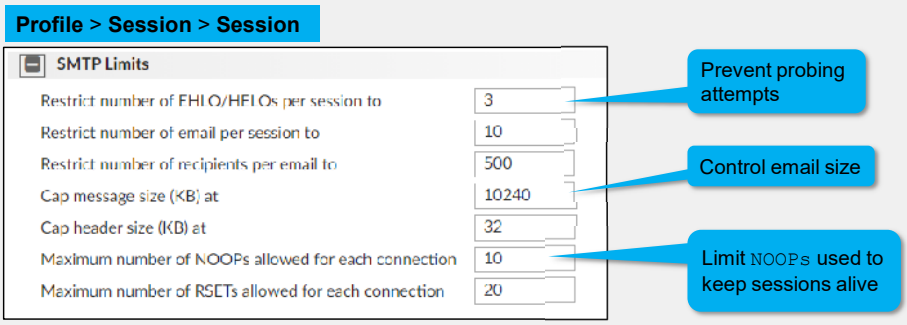
When the domain checks are being used, the domain claimed by the `EHLO` or `HELO`, sender domain (`MAIL FROM:`), and recipient domain (`RCPT TO:`) must be resolvable in DNS for either an A or an MX record type. If the domain can't be resolved, the SMTP command is rejected with an appropriate error code.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SMTP Limits

- Used to discourage common spamming techniques
- Control message size (header size + body size)



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

Using the **SMTP Limits** settings, you can set limits on SMTP sessions to restrict common spamming techniques. The default settings work well, but you can adjust them, if necessary.

Noteworthy settings include restrictions on the number of SMTP greetings (`EHLO` or `HELO`), `NOOPs`, and `RSETs`. Legitimate connections typically require only a few of these commands in a given session, and spammers may try to abuse them. Closing the sessions when these limits are reached forces spammers to reconnect if they want to continue; however, they are just as likely to abandon the attack and move on to their next target.

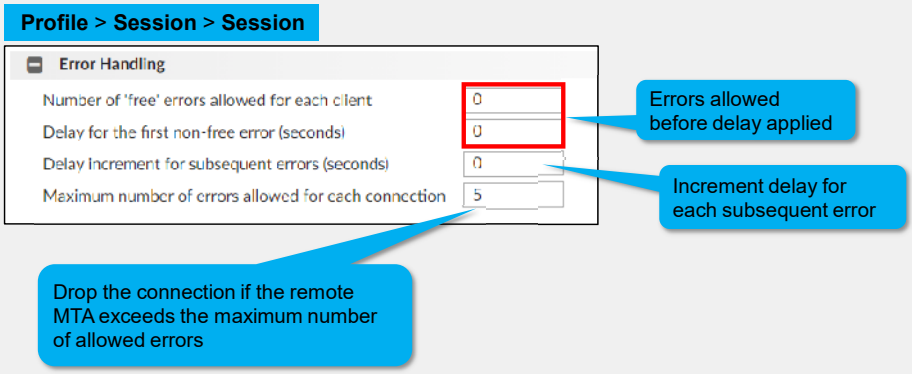
The **Cap message size (KB) at** option is commonly used to control email size. You will learn more about this later in the lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Error Handling

- Standards-compliant SMTP servers don't generate errors
- Protocol errors often indicate spammers or poorly coded or configured servers



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

Usually, correctly configured SMTP servers don't generate errors. So, SMTP protocol errors can indicate server misuse. FortiMail can penalize misbehaving clients, including disconnecting them, if they exceed the maximum number of errors.

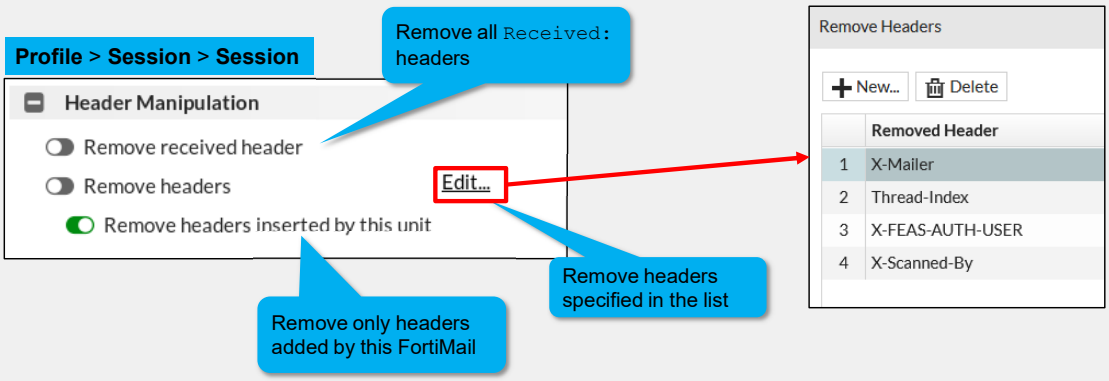
The first limit you can set is the number of free SMTP errors that is tolerated before delays are imposed on the client. After that value is reached, the client is delayed for the number of seconds specified in the **Delay for the first non-free error (seconds)** field. During this time, FortiMail won't accept any SMTP commands from the remote MTA in the session. Any subsequent errors result in additional incremental delays, as specified in the **Delay increment for subsequent errors (seconds)** field. After the number of errors exceeds the value in the **Maximum number of errors allowed for each connection** field, FortiMail drops the connection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Header Manipulation

- Reduce overall message size by removing header content
- Hide internal network information



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

As an email message travels from MTA to MTA, each MTA adds a new `Received:` header entry to the email. This not only increases the size of the header, but might also reveal details about your internal network that you want to keep private. You can use the header manipulation settings of the session profile to remove these `Received:` headers, typically on outbound emails.

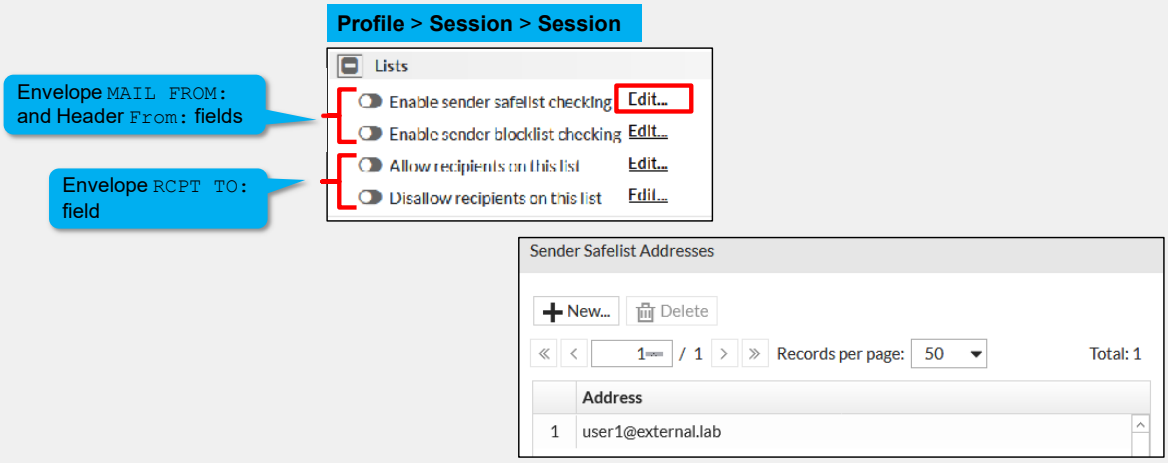
Be careful not to violate SMTP standards when deleting specific headers because there may be unintended consequences if other mail processing devices require or verify these headers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Session Lists

- Sender and recipient block and safe lists
- FortiMail applies session profile lists very early in its order of execution



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

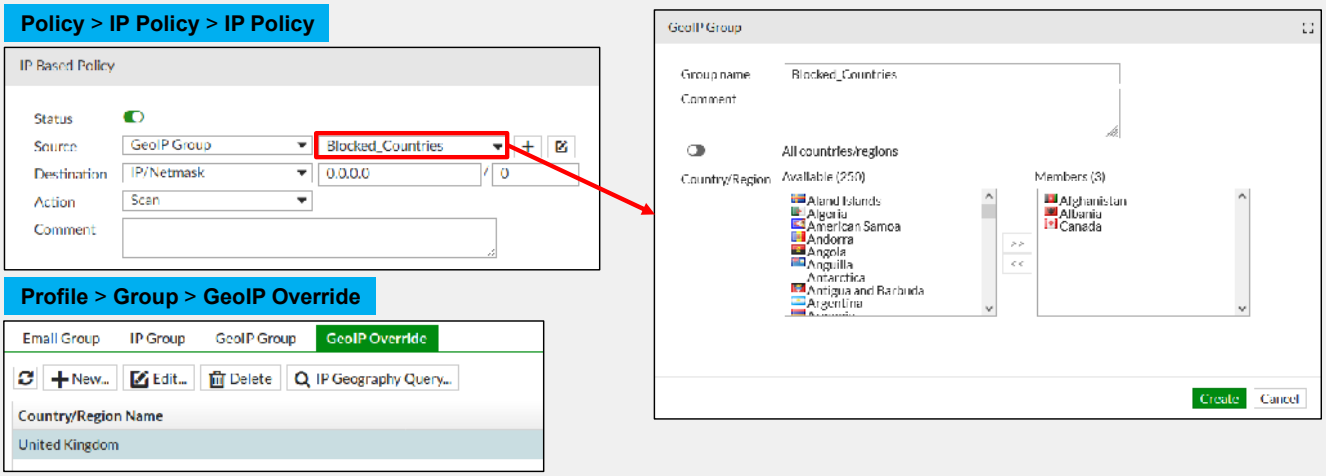
You can also configure each session profile to use independent sender and recipient block and safe lists. The lists contain email addresses to either block or allow certain senders or recipients when a specific session profile is used. FortiMail applies session profile lists very early in its order of execution, which are overridden only by the system safe and block lists.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGuard GeoIP

- GeoIP database from FortiGuard
- GeoIP groups can be used in IP policies and access control rules
- Embellish reports and logs with region/country flags



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

FortiMail utilizes the GeoIP database to map the geolocations of client IP addresses. You can use GeoIP groups in access control rules and IP-based policies.

The GeoIP service looks up the IP address geolocations in the GeoIP database. However, in some cases, the lookup might not be accurate, for example, when clients use proxies. With FortiMail, you can override the GeoIP lookup by manually specifying the geolocations of some IP addresses and IP ranges. When you create GeoIP groups, you can use the override geolocations in the groups.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about the sender reputation feature is true?
   A. A high score means that the client IP is a safe sender.
   ✓ B. Client IP scores are calculated based on the percentage of malicious and invalid email.

2. Sender policy framework (SPF) provides protection from forged email identities by performing which action?
   A. Comparing the IP address of the sender's MTA with a list of FortiGuard-approved IP addresses
   ✓ B. Comparing the IP address of the sender's MTA with a list of approved IP addresses in the sender domain DNS records

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Session Profile
- Sender Address Rate Control
- Message Size Management

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

Good job! You now understand how to configure a session profile.

Now, you will learn about sender address rate control.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Sender Address Rate Control

Objectives

- Control outbound email rate based on sender address

FORTINET Training Institute

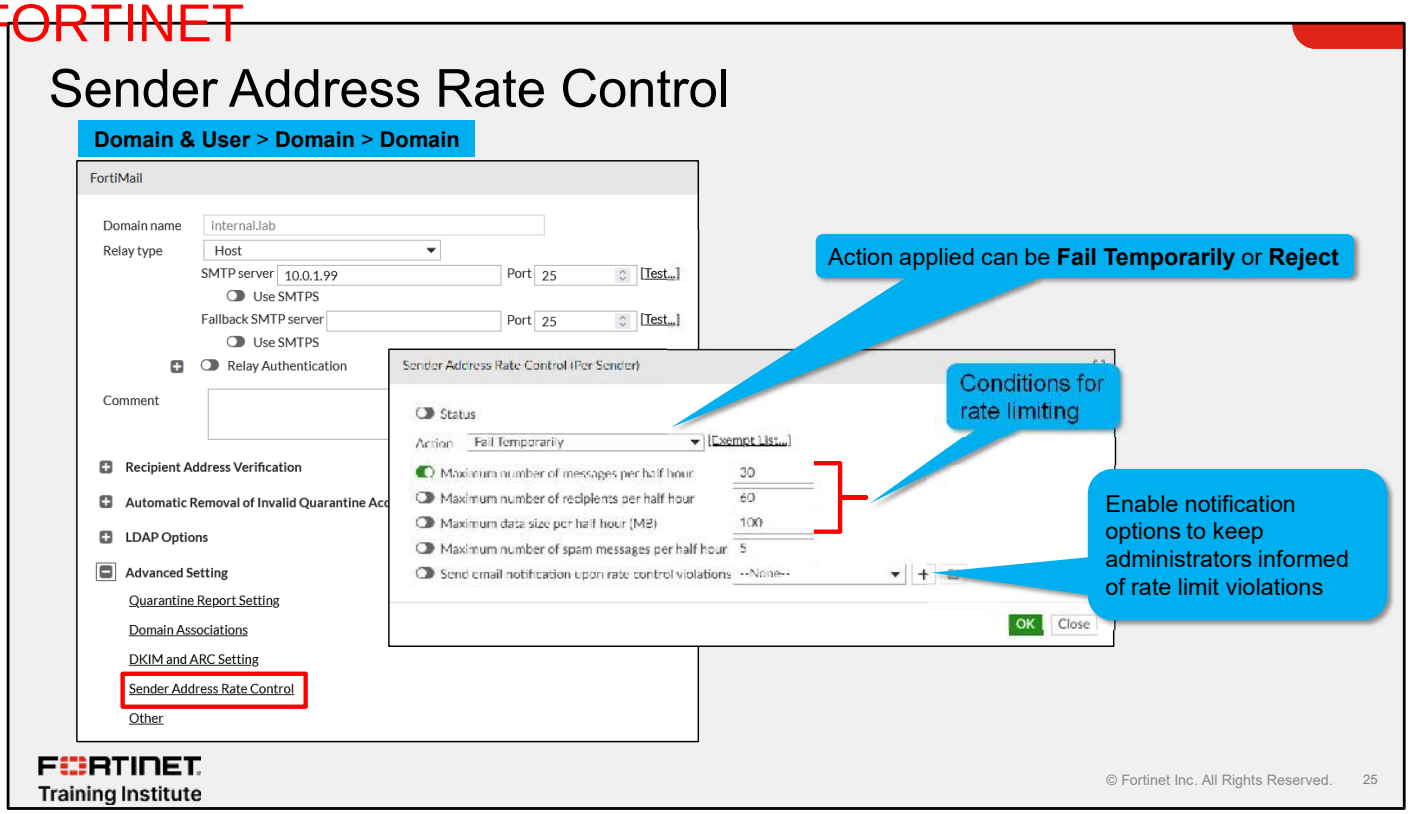
© Fortinet Inc. All Rights Reserved. 24

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in using sender address rate control, you will be able to control the outbound email rate based on sender address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Without any rate limits, a single sender can potentially monopolize FortiMail capabilities by sending an unlimited number of messages which, under some circumstances, could result in a poor reputation being assigned to the MX IP address of the organization. In the worst-case scenario, the MX IP address could be placed on an internet block list if a compromised endpoint, which has been infected with a spam bot, starts sending out mass spam email.

The sender address rate control settings are part of the domain entry for each protected domain. They provide granular control of messages sent in terms of the number of messages, the total size in megabytes, and even the ability to notify someone when the rate limit function is triggered. You can choose to either reject sessions from senders that have triggered the rate limits, or temporarily fail them to allow transmission later.

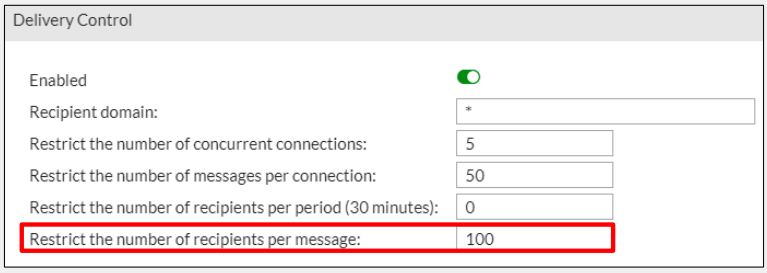
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Access Delivery Control

- Enable delivery control to avoid your MTA IP from being blocklisted by domain name system blacklists (DNSBL) due to excessive outgoing email
- Marketing mail campaigns can cause the corporate IP addresses to be registered in DNSBL
- Access delivery control is enhanced with **Restrict the number of recipients per message**

Policy > Access Control > Delivery Control



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

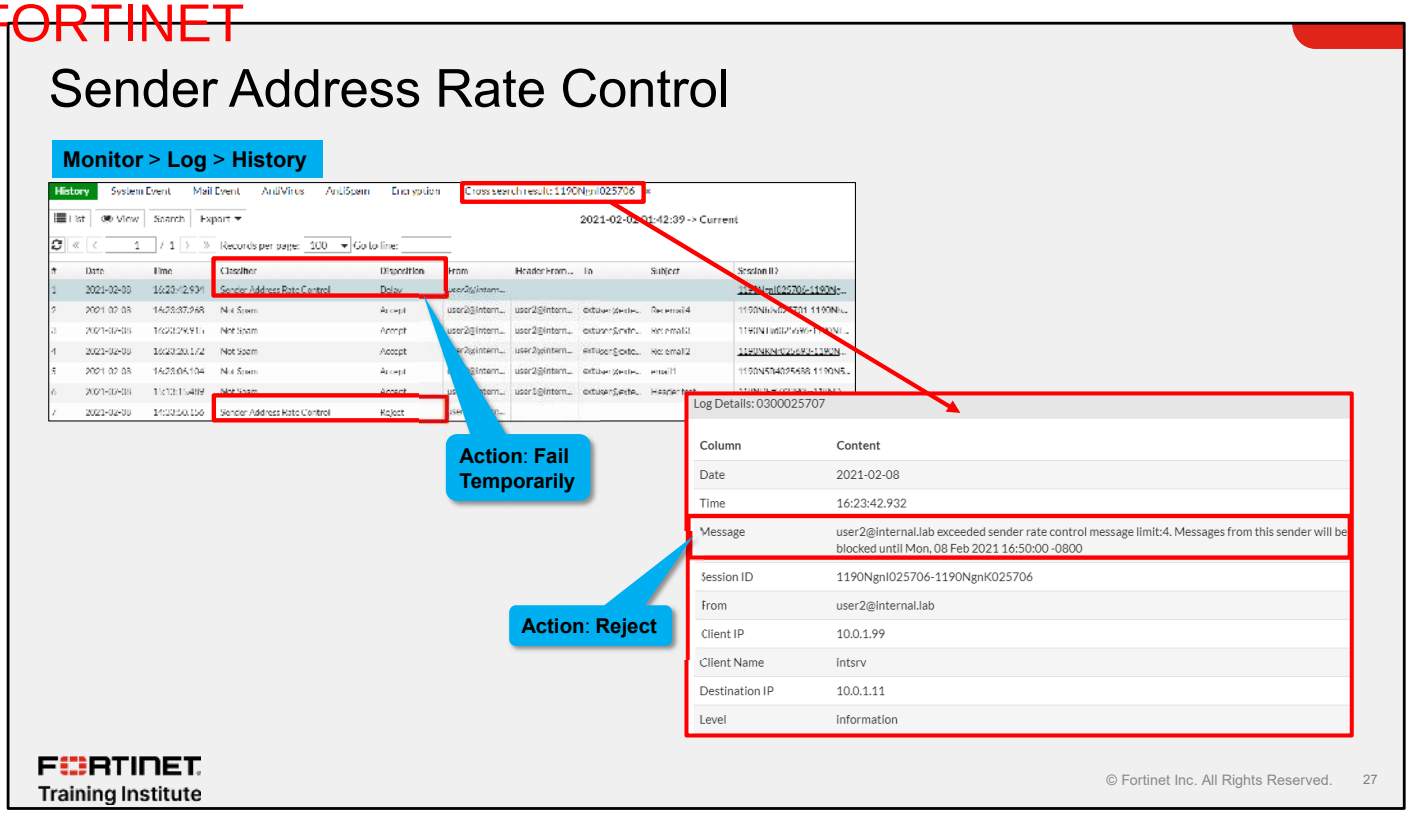
MTA IP addresses can be blocklisted if sending outgoing email at too high a rate. Marketing mail campaigns can sometimes cause the corporate IP addresses to be registered in DNSBL. To solve this problem, you can rate limit email delivery at the system level.

In the **Recipient domain** field, you must specify the recipient domain that the policy will be applied to. You can use a wildcard (*) to make this policy apply to all recipient domains.

Starting with FortiMail 6.4, you can restrict the number of recipients per message in the access delivery control configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In FortiMail logs, you can see sender address rate control in action. In the **History** logs, look for entries with a **Classifier** of **Sender Address Rate Control**.

The search result contains details of the rate limit violation, as well as how long the user will be blocked from sending any new messages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. What is the purpose of access delivery control?
   A. It applies rates to limit excessive incoming emails.
   ✓ B. It applies rates to limit outgoing email delivery at the system level.

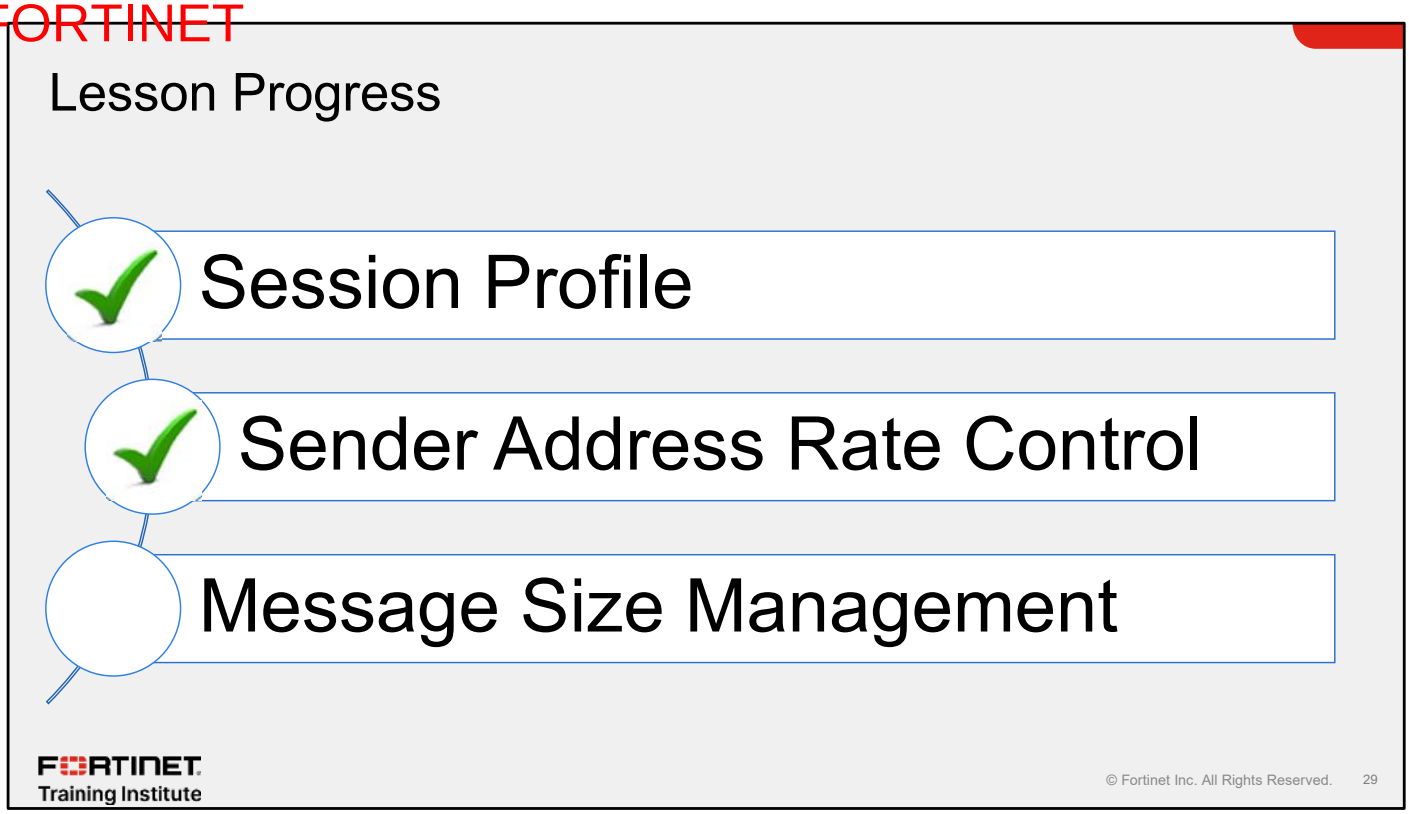
2. What *cannot* be restricted using sender address rate control?
   A. Emails with too many recipients
   ✓ B. An MTA that is sending too many emails

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

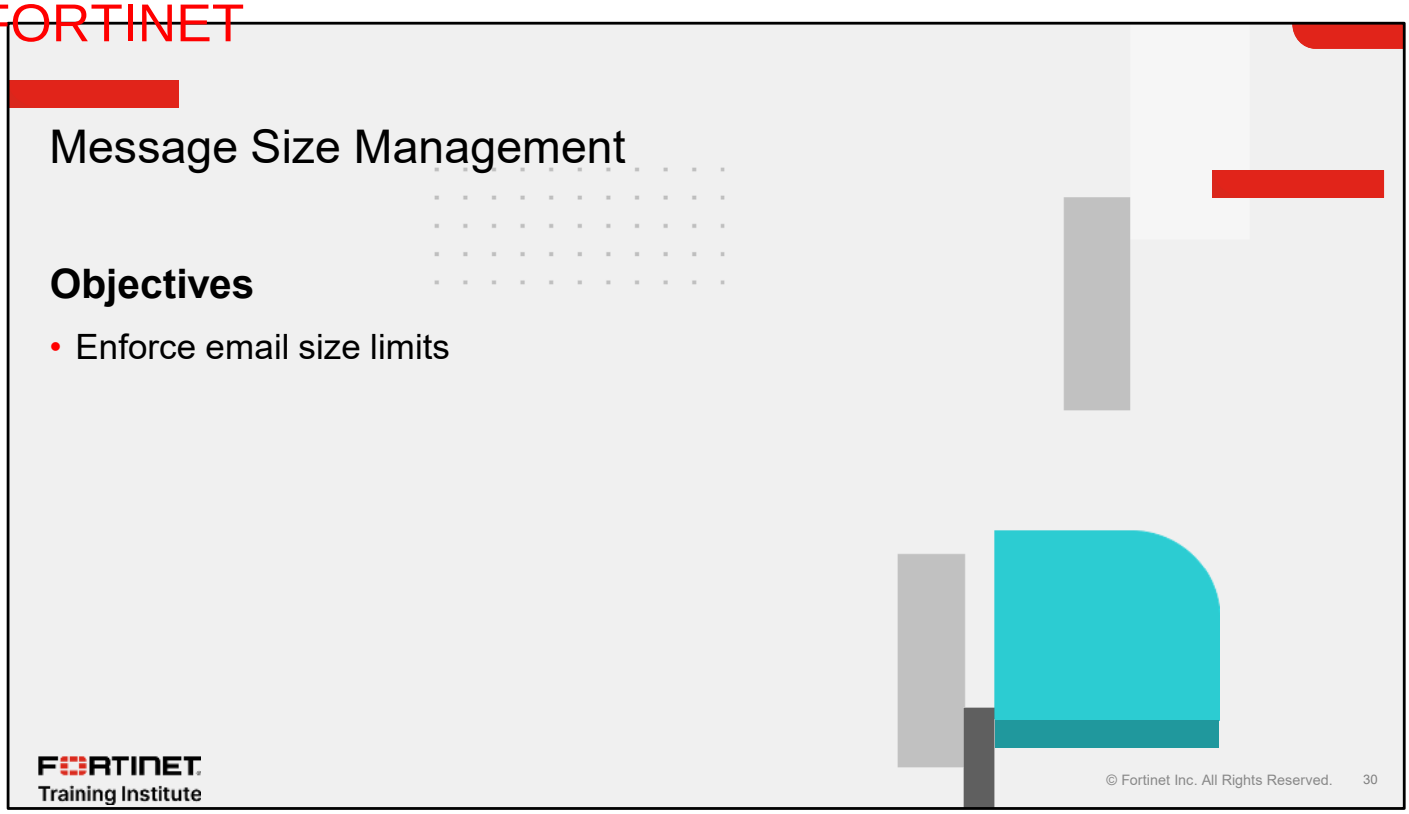


Good job! You now understand how sender address rate control can be used to limit the number of outbound emails based on sender address.

Now, you will learn about message size management.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

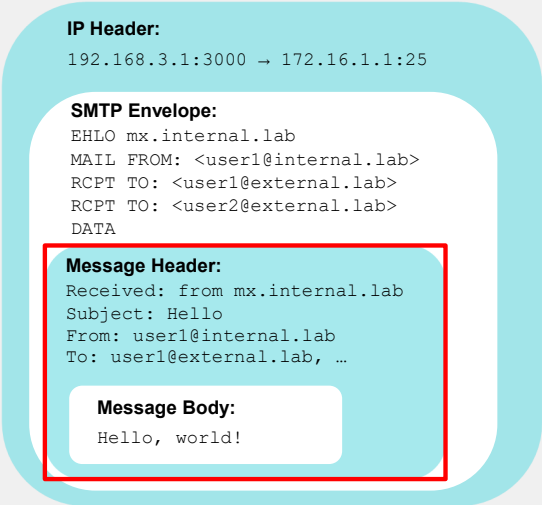
By demonstrating competence in message size management, you will be able to enforce size limits for all email passing through FortiMail, including attachments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Maximum Email Size

- By default, FortiMail rejects all email larger than 10 MB
- Includes message header and message body
- You can override this limit in two ways:
  - Cap message size
    - Session profile configuration
  - Maximum message size
    - Protected domain configuration



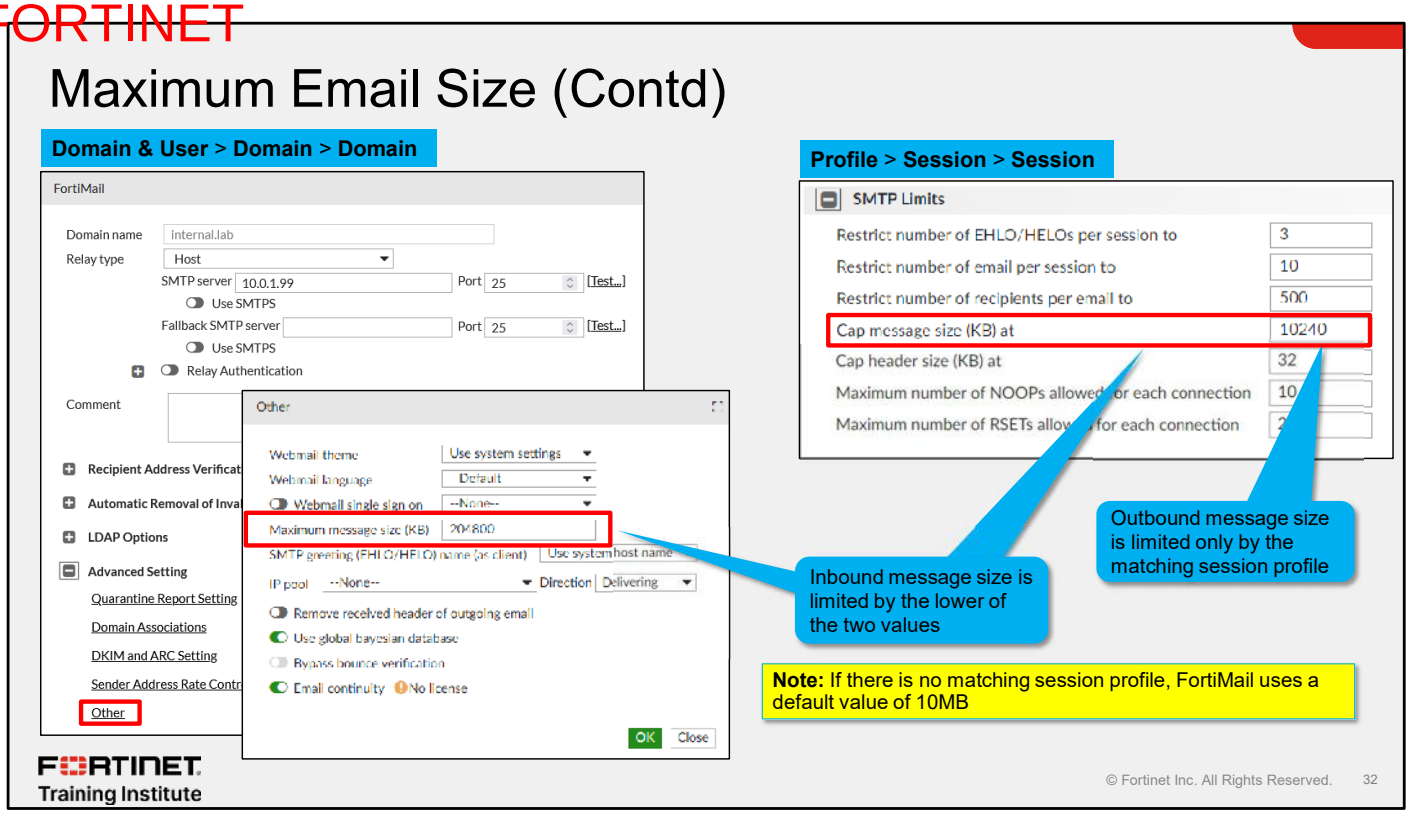
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

FortiMail rejects all email larger than 10 MB. This size limit is enforced by the kernel and includes the SMTP header size as well as the message body size, which includes attachments. You can override this value in two places: the session profile or each protected domain definition.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiMail behavior varies, depending on whether the email is incoming or outgoing. For outgoing email, FortiMail uses only the session profile value, if a session profile matches the email. If no session profile matches, FortiMail still uses the default limit of 10 MB.

For incoming messages, FortiMail evaluates both the session profile and the protected domain values and selects the smallest value. If no session profile or IP-based policy matches, FortiMail compares the default size of 10 MB to the limit defined in the domain setting.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which statement about oversize email messages is true?
   A. By default, there is no maximum message size value defined on FortiMail.
   ✓ B. The default maximum message size defined on FortiMail is 10 MB.

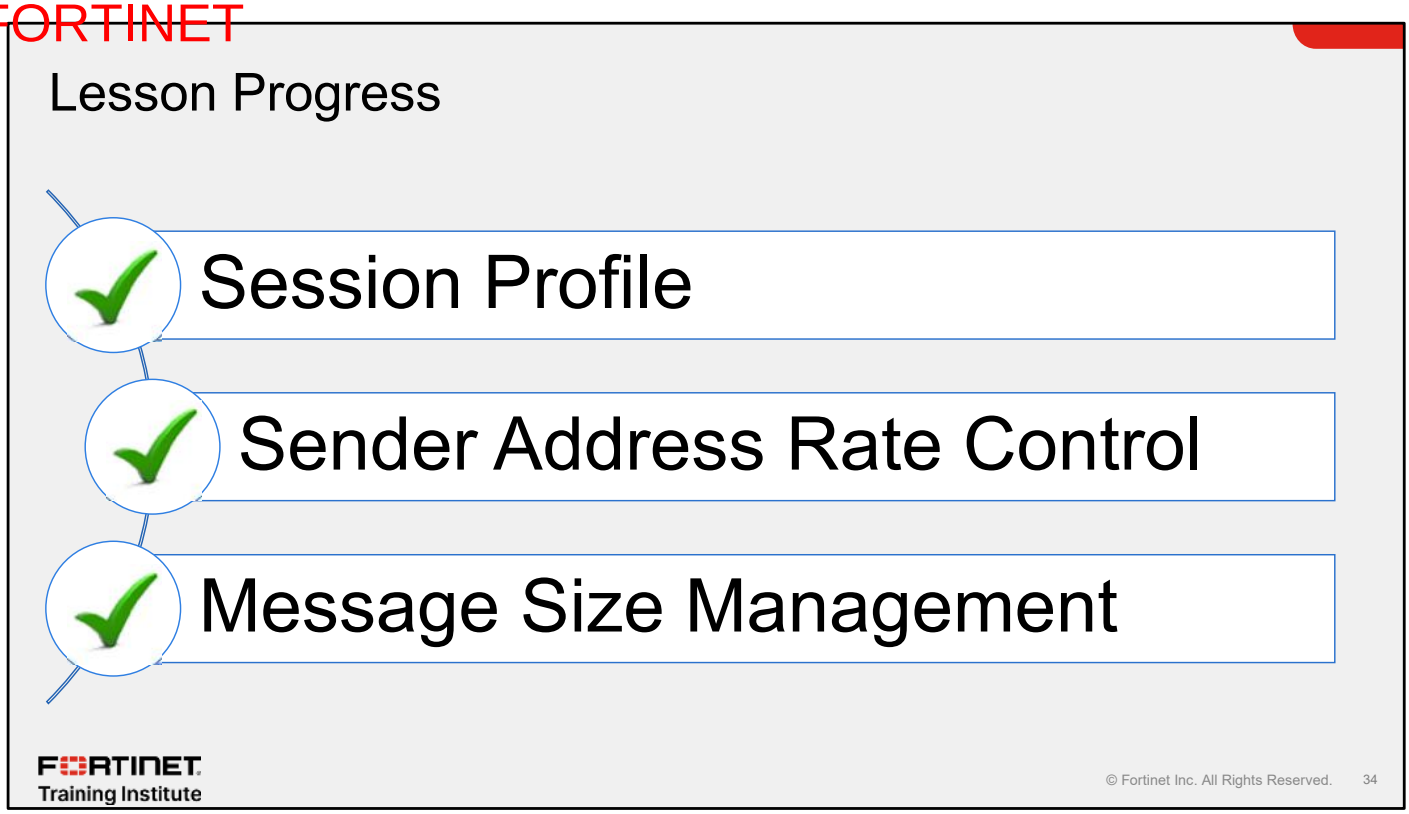
2. Inbound message size is limited by which value?
   A. The message size specified in the matching session profile
   ✓ B. The lower of the two message sizes specified in the protected domain and in a matching session profile

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in the lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Limit sessions from remote MTAs
- ✓ Throttle email volume based on sender reputation
- ✓ Reject connections from blocklisted MTAs
- ✓ Validate senders using SPF and DKIM
- ✓ Implement outbound DKIM signing of email messages
- ✓ Detect errors and abnormalities in SMTP sessions
- ✓ Hide internal network information in email headers
- ✓ Control outbound email rate based on sender address
- ✓ Enforce email size limits

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 35

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to effectively use session management and related features.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FORTINET Training Institute

FORTINET CERTIFIED PROFESSIONAL
Public Cloud Security

FortiMail Administrator

Antivirus and Antispam

FortiMail 7.4

Last Modified: 25 April 2024

In this lesson, you will learn about antivirus and antispam techniques on FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- Antivirus
- Antispam Profiles
- Antispam Techniques
- Personal Quarantine Management

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 2

In this lesson, you will explore the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Antivirus

Objectives

- Configure antivirus profiles and antivirus action profiles to implement local malware detection

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 3

After completing this section, you should be able to achieve the objective shown on this slide.

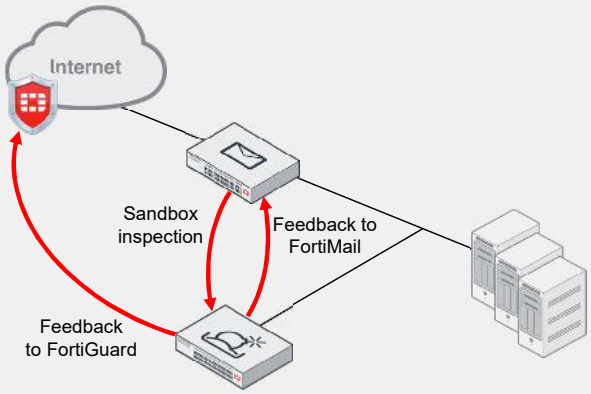
By demonstrating competence in antivirus, you will be able to configure and apply antivirus profiles to recipient-based or IP-based policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiSandbox Integration

- FortiMail for email prefiltering
  - Submit objects to FortiSandbox
  - Queue emails during analysis
  - Automatically handle emails based on results
- FortiSandbox for payload analysis
  - Analyze all objects and activity
  - Assign and return a rating for the submission
  - Update FortiGuard security services



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

FortiSandbox integrates with FortiMail to provide protection against email-borne threats. Unlike network traffic, FortiMail handles email traffic using a store-and-forward system—so, it is generally okay to introduce a small amount of latency into the system. Because of this, you can use FortiMail with FortiSandbox and FortiGate to prevent advanced threats contained in email from reaching the end user.

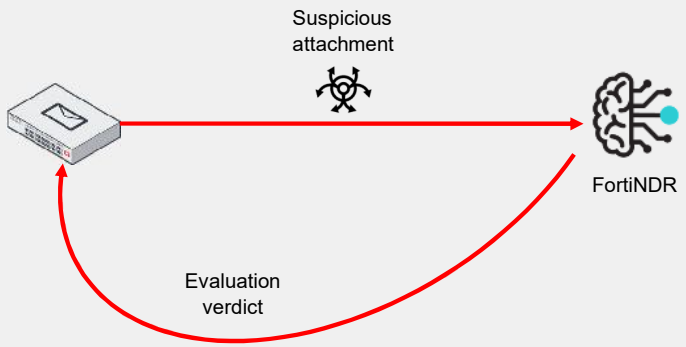
When you make this simple integration, at-risk email traffic is sent to FortiSandbox and held until it has been analyzed. If FortiSandbox finds a suspicious or malicious, it can block that email from being delivered.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiNDR Integration

- Next generation malware detection
  - Rapid malware detection and verdict
  - FortiMail can pass suspicious email attachments to for inspection
  - Results returned to FortiMail for action



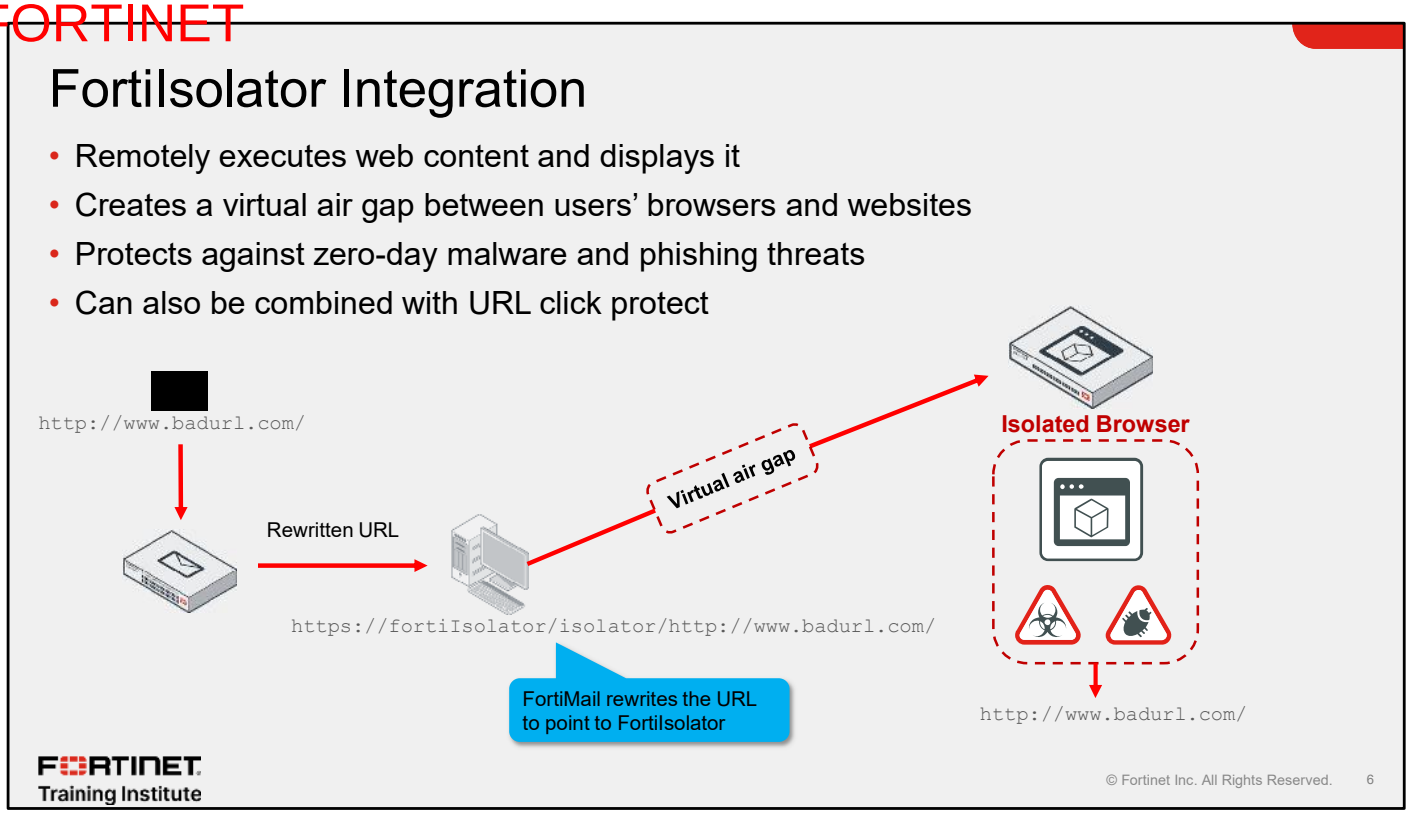
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

FortiNDR provides rapid evaluation of suspicious attachments. When FortiMail is integrated with FortiNDR, FortiMail will pass suspicious email attachments to the FortiNDR for evaluation. A verdict is made based on file behavior or contents of malware and returned to FortiMail. FortiMail actions can then be performed based on the FortiNDR verdict.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiIsolator is a browser isolation solution that protects users against zero-day malware and phishing threats that are delivered over the web and in email. These threats might result in data loss, compromise, or ransomware.

This protection is achieved by creating a virtual air gap between users' browsers and websites, which prevents content from breaching the gap. With FortiIsolator, web content is executed in a remote disposable container and displayed to users.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Local Malware Detection

- FortiGuard antivirus service
  - Signature-based detection
  - Includes grayware
  - Database updated through FortiGuard Distribution Network (FDN)
- Heuristic
  - Local sandbox emulation to detect virus-like attributes in files
- Malware outbreak
  - Uses data analytics by FortiGuard to generate rating information on known bad-sender IPs, content, and attachments

FortiGuard Antivirus

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

FortiGuard antivirus is included in the FortiGuard antivirus subscription. FortiMail uses the FortiGuard antivirus service to protect against the latest threats. The Fortinet unique content pattern recognition language (CPRL) allows a single signature to protect against different and variant malware strains. FortiMail antivirus scanning uses the same FortiGuard virus signature databases that are used in FortiGate firewalls. The databases are kept up-to-date by regular updates from the FortiGuard Distribution Network (FDN).

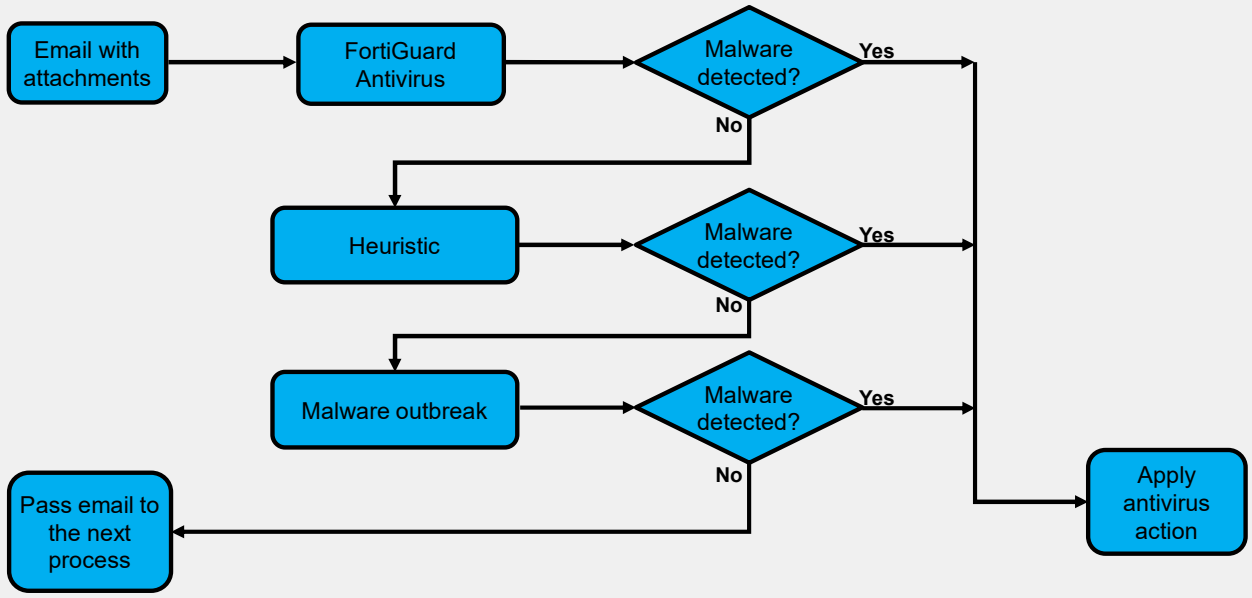
The FortiGuard real-time sandbox is also included in the FortiGuard antivirus subscription. FortiMail uses a local sandbox to evaluate executable content that has passed the FortiGuard antivirus signatures. The local sandbox examines the construction of files to look for characteristics commonly found in viruses. It also emulates the execution of the content to look for typical virus behavior.

FortiGuard labs receive global requests for ratings of sender IPs, content, and attachments. Using data analytic techniques, FortiGuard can quickly detect and respond to new outbreaks, blocking suspicious virus objects without the need for antivirus signatures.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Local Malware Detection Flow



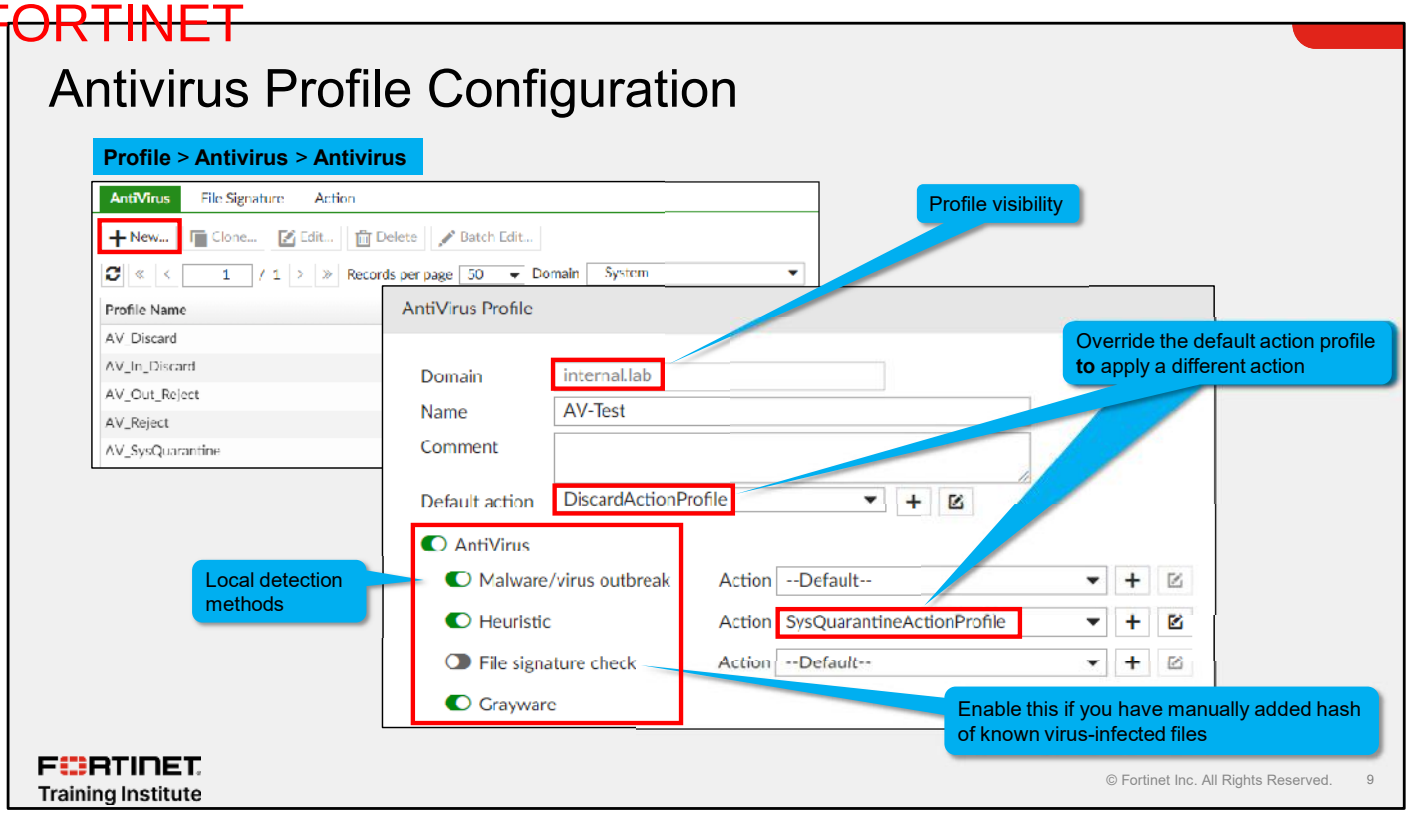
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

This slide shows the process flow for malware detection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To enable local antivirus scanning techniques and actions, you must create an antivirus profile first. Each antivirus profile specifies a default action that FortiMail runs when it detects a virus. You can override the default action if you select a different action on a technique-by-technique basis. When you create an antivirus profile, set the domain attribute to determine the visibility of the profile within the system. You can set the domain attribute to be available for use across the system, or in only a specific protected domain.

FortiMail scans the email header, body, and attachments (including compressed files, such as ZIP, PKZIP, LHA, ARJ, and RAR files), for virus infections. If FortiMail detects a virus, it takes the actions you define in the antivirus action profiles.

FortiMail keeps its antivirus scan engine and virus signature database up to date by connecting to the FDN antivirus services.

Enable **File signature check**, if you already have hash values of some known virus-infected files. You can add those checksums on the **File Signature** page.

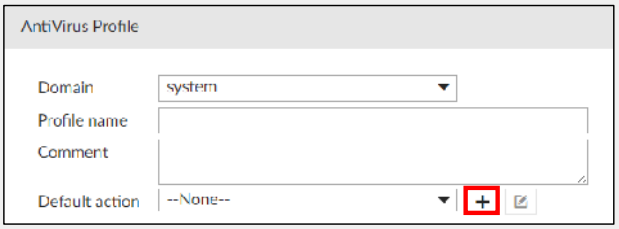
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

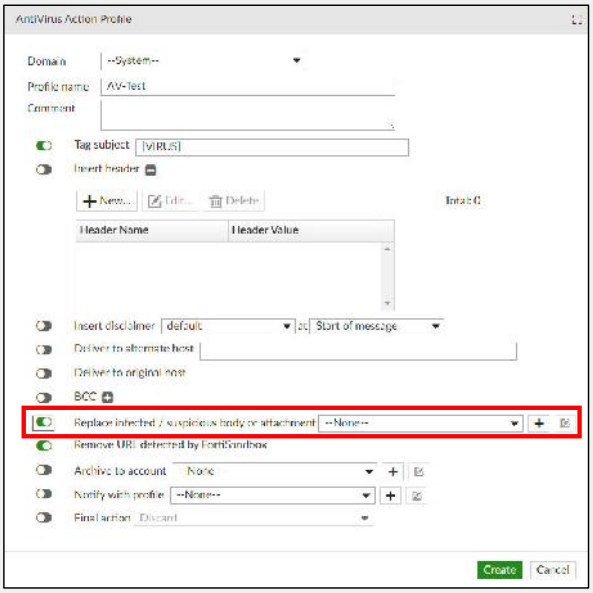
Antivirus Action Profile Configuration

- Replace an infected or suspicious body or attachment:
  - Email is delivered to the recipient without the infected attachment
- No personal quarantine option available:
  - Protect the end user from accidentally releasing infected content

Profile > Antivirus > Antivirus



Profile > Antivirus > Action



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

You can create a new action profile in the **Antivirus Profile**. The most commonly used action is **Replace infected/suspicious body or attachment(s)**. This option allows the body of the email to be delivered to the intended recipient, without the malicious attachments. Other commonly used actions include **Discard** and **Reject**. You can customize the replace message by defining a new replacement message profile; otherwise, a default message is used.

Note that there is no personal quarantine option in an antivirus action profile. This protects the end user from releasing infected content accidentally on their local computer.

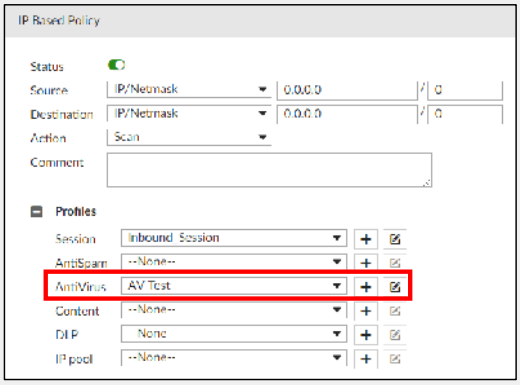
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

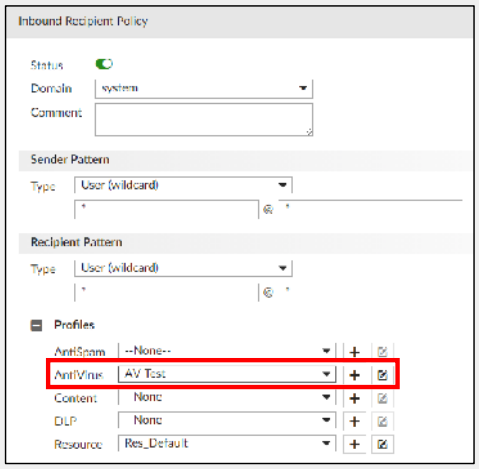
Applying Antivirus

- Enable antivirus scanning using either IP-based or recipient-based policies
- Enable antivirus processing to protect your MX IP reputation by prevent malware from leaving your network

Policy > IP Policy > IP Policy



Profile > Recipient Policy > Recipient Policy



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

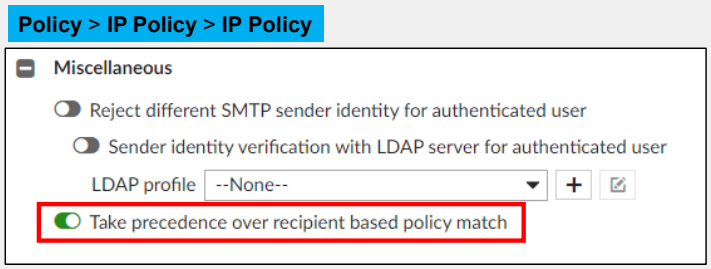
The antivirus profile can be referenced by IP-based policies or recipient-based policies. For complete protection, enable antivirus scanning on outbound policies to prevent malicious content from accidentally leaving your organization.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Prioritizing IP-Based Antivirus Policies

- If **Take precedence over recipient based policy match** is enabled in the IP policy, then content inspection in recipient policy will be ignored



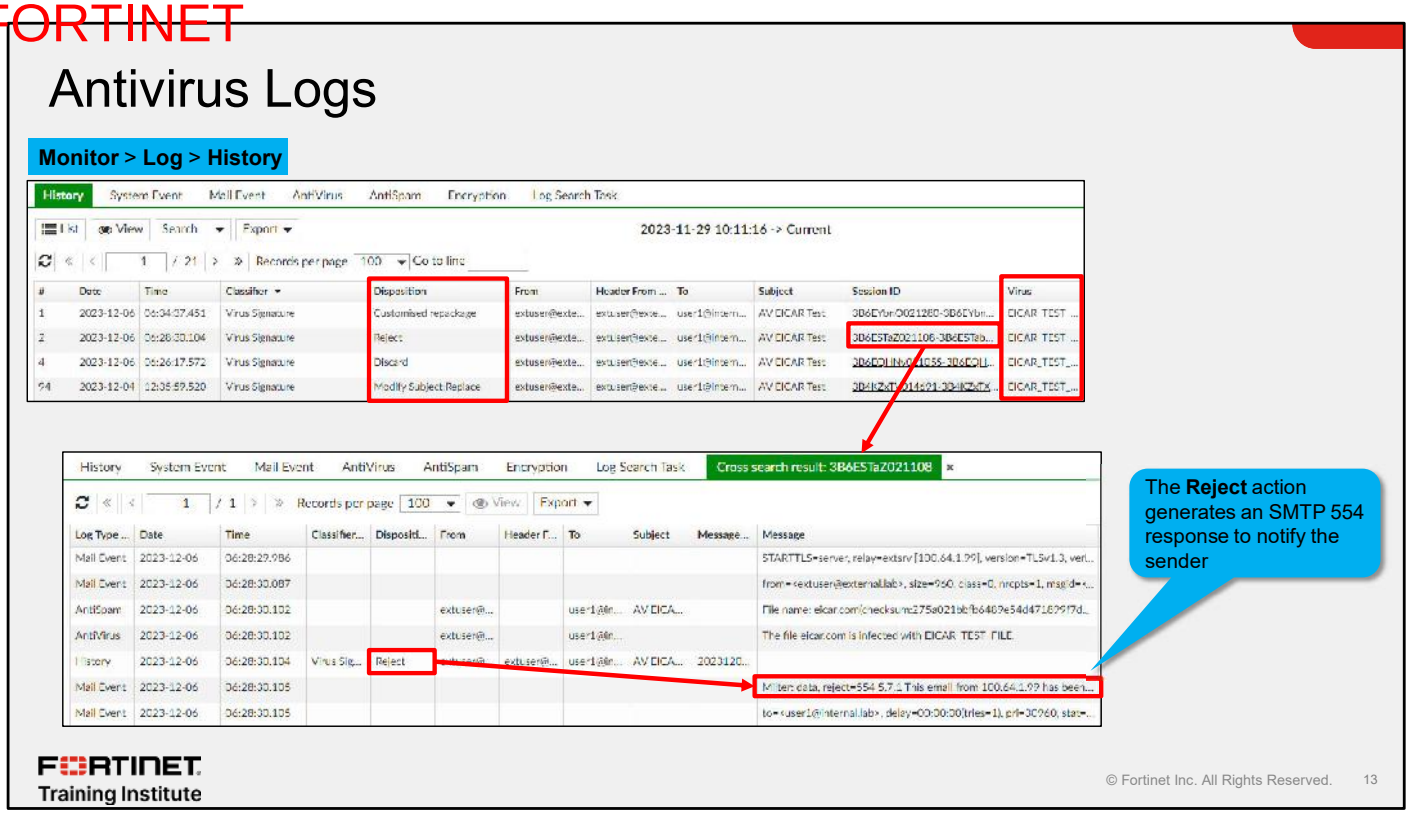
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

As a general rule, recipient-based policies override IP-based policies. This means that if an email message matches both a recipient-based policy and an IP-based policy, the settings in the recipient-based policy will be applied, and the IP-based policy will be ignored, unless you have enabled **Take precedence over recipient based policy match** in the IP policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **History** logs provide an overview of the events that have occurred, including classifier, disposition, and virus name**.** For more detail, click the **Session ID** link to see a cross-search result of all the logs for that single event.

This slide shows an example of a reject action in response to the detection of a virus. FortiMail generates an SMTP 554 message that explains the reason for the rejection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Antivirus Customized Message

Profile > Antivirus > Action

Notify with profile --None--

Final action Repackage email with customized content *

* Original email will be wrapped as attachment

From External User <extuser@external.lab>
Subject AV EICAR Test
To Me

The original message contains one or more viruses:

From : External User <extuser@external.lab>
To : user1@internal.lab
CC :
Subject : AV EICAR Test
Date : Wed, 06 Dec 2023 06:34:31 -0800
Email Size :
Files Infected

File Name	Virus/Malware/Spyware
eicar.com	EICAR_TEST_FILE

2 attachments 1.1 KB
original.eml 1.1 KB eicar.com 68 bytes

Monitor > Log > History

History | System Event | Mail Event | AntiVirus | AntiSpam | Encryption | Log Search Task

List | View | Search | Export | 2023-11-29 10:11:16 -> Current

1 / 21 | Records per page 100 | Go to line

#	Date	Time	Classifier	Disposition	From	Header From ...	To	Subject
1	2023-12-06	07:00:02.094	Virus Signature	Modify Subject;Customized repackage;...	extuser@exte...	extuser@exte...	user1@intern...	AV EICAR Test

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

When you enable **Repackage email with customized content**, and FortiMail detects an infected attachment, FortiMail replaces the infected attachment with a text attachment that contains the details of the original file and the detected virus. This allows the recipient to stay informed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which malware detection technique is used by FortiMail?
   - ✓ A. FortiGuard antivirus service
   - B. Extended proxy engine

2. Why is the personal quarantine option unavailable in an antivirus action profile?
   - A. It is resource-intensive.
   - ✓ B. It protects the end user.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Antivirus
- Antispam Profiles
- Antispam Techniques
- Personal Quarantine Management

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

Good job! You now understand how antivirus works on FortiMail.

Now, you will learn about antispam profiles.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Antispam Profiles

Objectives

- Identify the spam detection methodologies used by FortiMail
- Identify antispam profiles and action profile features

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

After completing this section, you should be able to achieve the objectives shown on this slide.

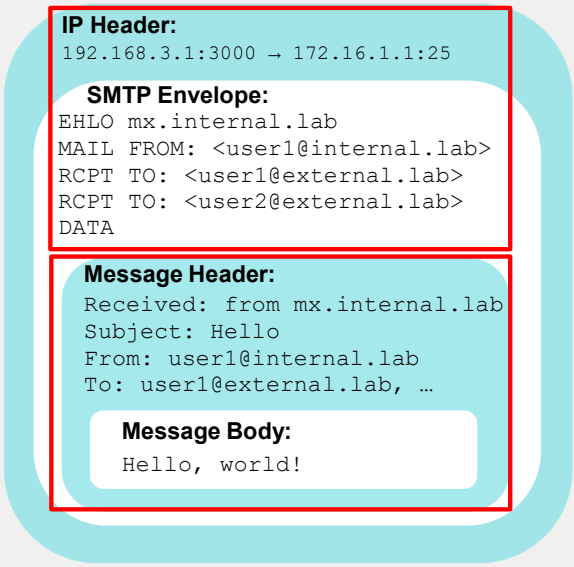
By demonstrating competence in using antispam profiles, you will be able to identify the spam detection methodologies used by FortiMail and apply the appropriate antispam action profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Spam Detection

- Industry-standard definition of spam:
  - **Unsolicited**: The recipient hasn't granted permission
  - **Bulk**: The message is sent as part of a collection of messages that have identical content
- Two tiers of spam defense:
  - FortiGuard antispam service
  - FortiMail antispam techniques
- Two layers of spam inspection:
  - Session based: IP header and SMTP envelope
    - FortiMail Session profile
  - Application based: Message header and body
    - FortiMail Antispam profile



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

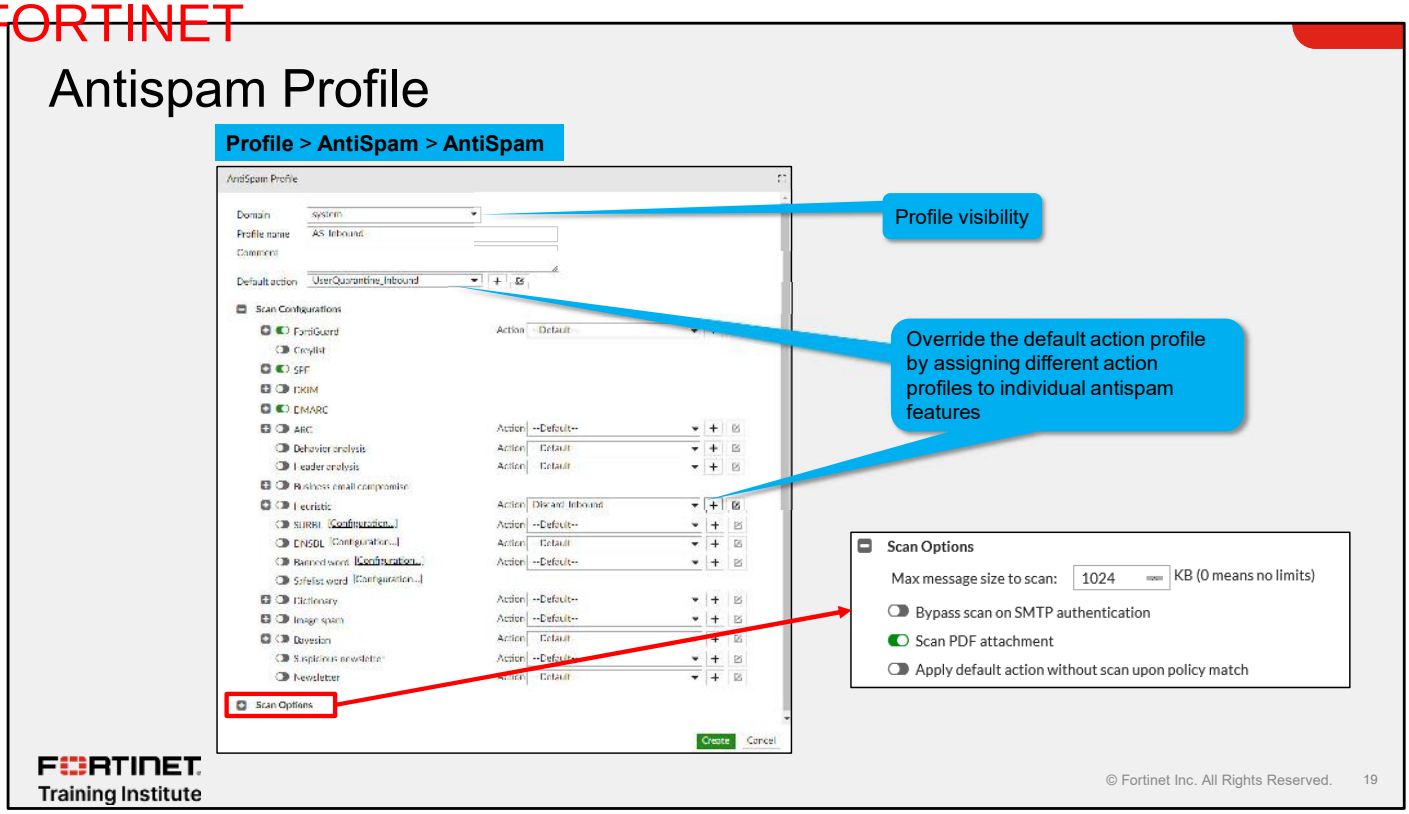
The industry-standard definition of email spam has two components. First, the email messages are unsolicited; that is, the recipient hasn't requested or granted permission for the email. Second, the email messages are considered bulk mailings because they are sent out in mass quantities and contain identical (or nearly identical) content. The industry term for this is unsolicited bulk email (UBE).

FortiMail antispam service is a combination of two tiers of spam defense: the FortiGuard antispam service, combined with FortiMail built-in antispam detection techniques. By leveraging the FortiGuard antispam service, FortiMail has access to the latest knowledge of emerging spam threats and outbreaks.

Email messages are inspected at two distinct layers: the session layer and the application layer. The session layer analyzes the attributes and behaviors of the IP connection and SMTP session for traits that are common to spam activity. FortiMail can detect spam even before the message headers and message body are sent. This saves valuable resources and improves the performance of the FortiMail server. The application layer detection analyzes the content of the message headers and body after they arrive. FortiMail uses this data to perform in-depth spam detection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When an email message matches the selection criteria specified in an IP or a recipient policy, you can activate an antispam profile to perform any of the available antispam scanning techniques. In the antispam profile, select the default action to be executed if the message is verified to be spam, or associate different action profiles with different antispam techniques.

In the **Scan Options** section, you can define a size limit for messages to scan. If an email is larger than the specified value, FortiMail skips antispam inspections on that email. You can also bypass an email from antispam inspections if the user is authenticated. Be careful with this setting because an authenticated user isn't always a safe sender.

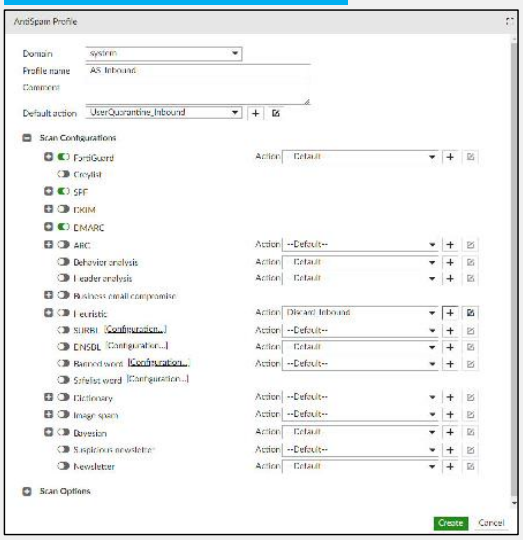
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Antispam Profile Options

- FortiMail antispam can perform the following operations and checks on email defined in the antispam profile:
  - FortiGuard MX reputation, and URL scanning
  - Spam outbreak
  - Greylisting
  - SPF, DKIM, DMARC with ARC validation
  - Header and behavioral analysis
  - Impersonation detection
  - Word lists, dictionaries, URL block lists
  - Image spam detection
  - Newsletter detection

Profile > AntiSpam > AntiSpam



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

In addition to other options listed in the *FortiMail Administration Guide*, this slide lists a summary of some of the commonly used options in the antispam profile. These include:

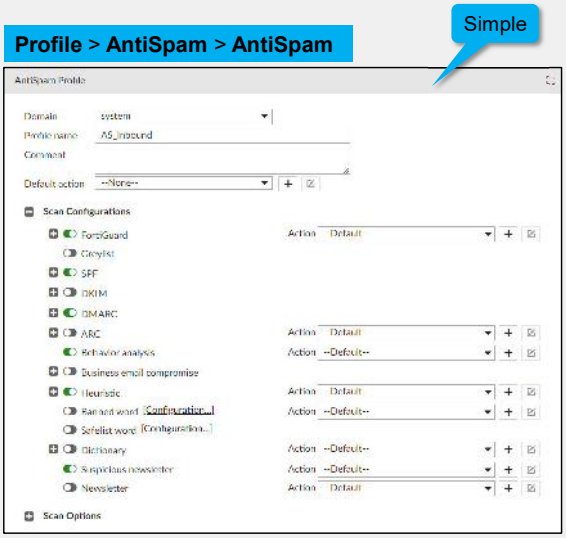
- FortiGuard MX reputation and URL scanning which uses FortiGuard lists and reputation scores to identify known spammers and to verify embedded URLs are safe.
- Spam outbreak, which holds new and unidentified emails for a predefined period to combat zero-day spam.
- Greylisting, which performs analyses on the behavior of the sending mail exchanger, and blocks or delays emails, based on their session behavior and not their contents.
- SPF, DKIM, and DMARC with ARC validation, which verifies the identity of the sending mail exchanges and signatures embedded in email headers.
- Header and behavioral analysis, which examines the content of the email headers and bodies and compares them to known spam emails to determine if the new email has spam-like characteristics.
- Impersonation detection, which detects if an email sender is attempting to impersonate another user.
- Word lists, dictionaries, and URL block lists, which are updated by FortiGuard services with words and URLs that are commonly found in spam email. These lists are highly customizable.
- Image spam detection which examines GIF, JPG, and PNG files to determine if they are known images in spam messages.
- Newsletter detection, which detects spam messages masquerading as known and accepted newsletter emails.

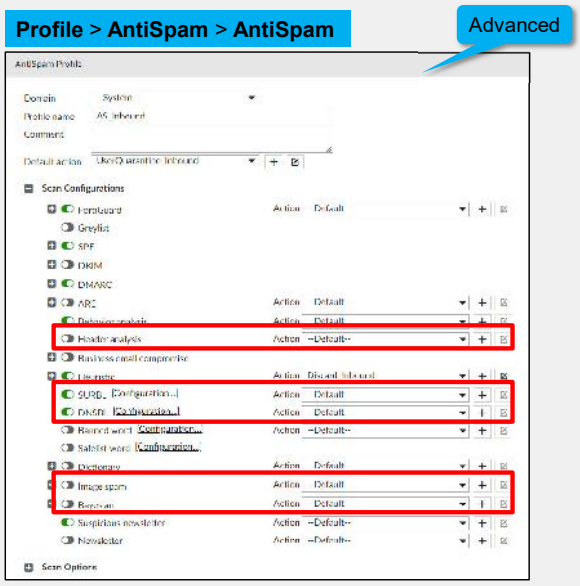
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Antispam—Simple vs. Advanced View

- Some features are unavailable in the simple view of the antispam profile





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

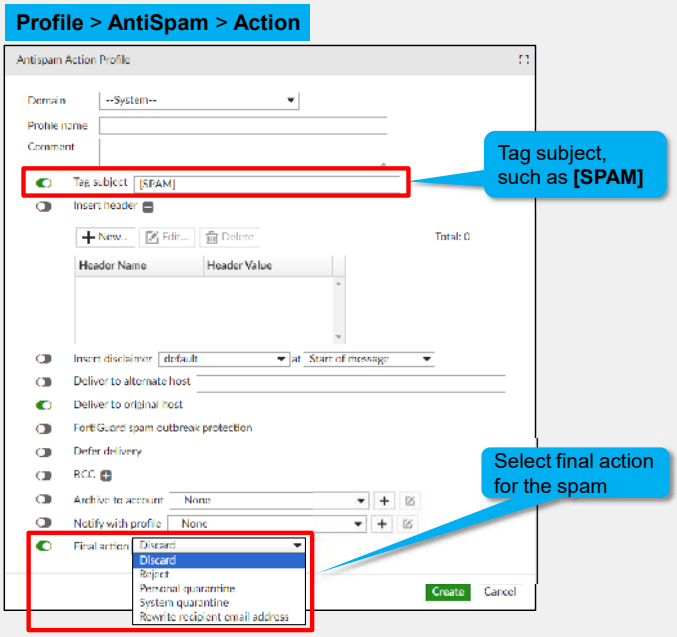
Some features are unavailable in the antispam profile in simple view. To access all available antispam features, use the advanced view GUI display.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Antispam Action Profiles

- **Reject**: Reject the email and reply to SMTP client with SMTP reply code 550
- **Discard**: Accept the email and delete it without notifying the SMTP client
- **Personal quarantine**: Redirect incoming email to the recipient's personal quarantine and outgoing email to the system quarantine
- **System quarantine**: Redirect spam to the system quarantine folder
- **Rewrite recipient email address**: Change the recipient address of any email message detected as spam



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

The antispam action profile provides options that you can apply to an email, if it is detected as spam. You can tag the subject field of that email to warn the user that the email is potential spam. You can also insert a header or a disclaimer into the email. If you want to deliver a spam email to an alternate host, such as a specialized quarantine server, you can configure that in the antispam action profile using the **Deliver to alternate host** option.

There are other actions that you can configure in the antispam action profile, such as archiving the email or sending a notification to a valid email address. These actions are considered nonfinal actions, because FortiMail continues antispam scanning.

You can also configure a final action. FortiMail stops all processing after applying a final action. There are five different final action options: discard, reject, personal quarantine, system quarantine, and rewrite recipient email address. FortiMail will not perform any additional scanning, after applying one of these five final actions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which part of an email message is analyzed by the session layer inspection features?
   A. Message body
   ✓ B. IP header

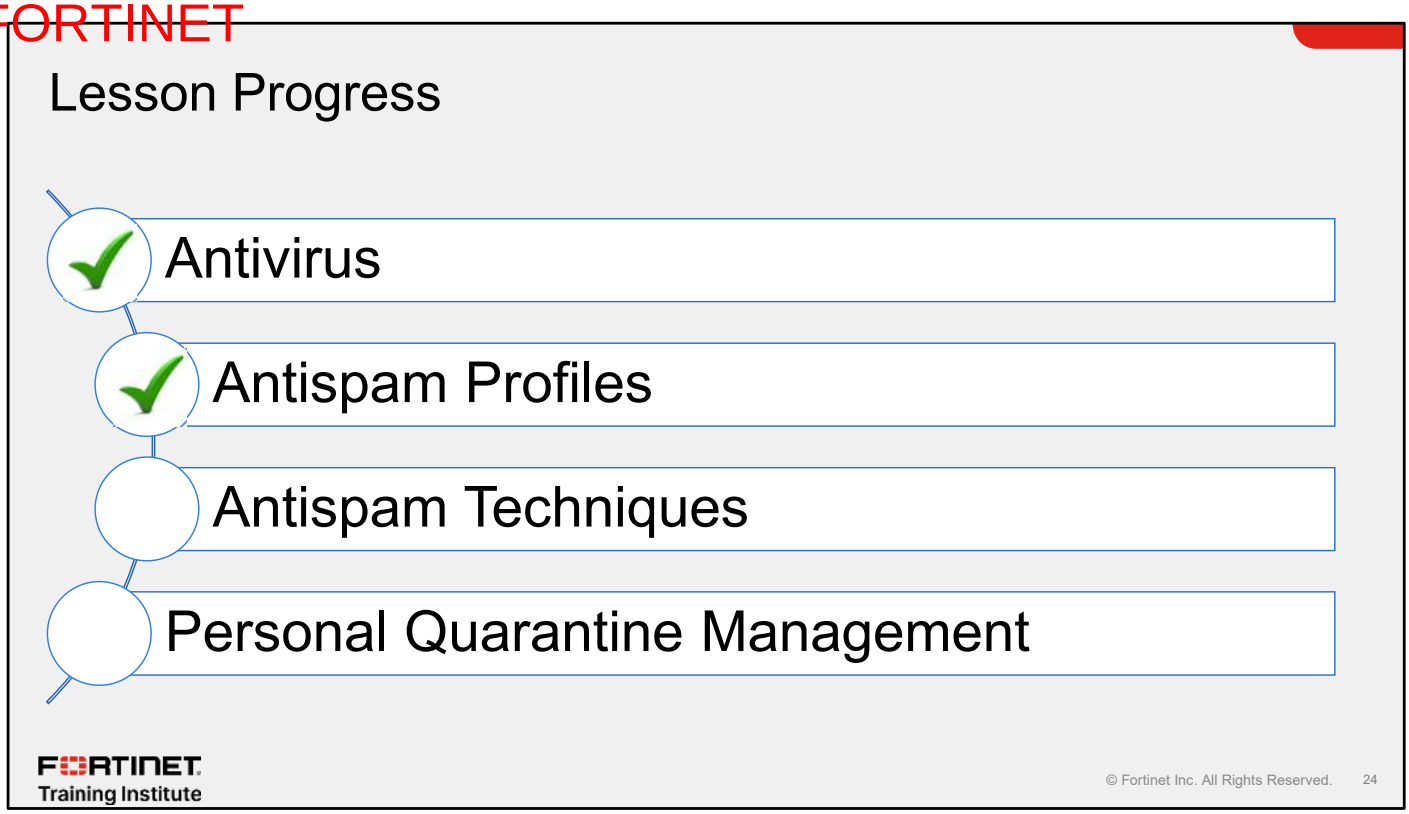
2. Which is a possible final action in an antispam action profile?
   A. Tag subject
   ✓ B. Rewrite recipient email address

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Good job! You now understand how to use antispam profiles on FortiMail.

Now, you will learn about antispam techniques.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Antispam Techniques

Objectives

- Use outbreak protection and behavior analysis to detect zero-day spam
- Use bounce address tag validation to combat backscatter attacks
- Identify the headers added by FortiMail antispam
- Establish the scanning order of execution

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using antispam techniques, you will be able to configure FortiMail to block spam and backscatter attempts.

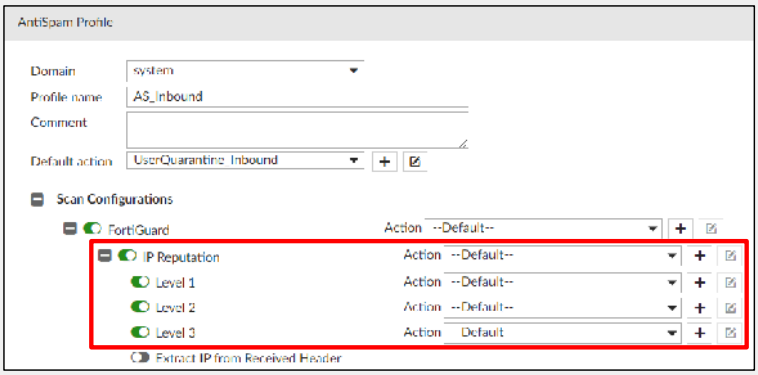
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGuard IP Reputation

- **IP Reputation:**
  - Checks the sender IP address against the FortiGuard blocklist databases
- **Extract IP from Received Header:**
  - Checks every MTA address that appears in the **Received** headers of the email against the FortiGuard blocklist databases

Profile > AntiSpam > AntiSpam



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

When you enable the FortiGuard IP reputation option, FortiMail queries the FortiGuard antispam service to determine if the remote MTA IP address is in the FortiGuard blocklist database.

FortiGuard categorizes the blocklisted IP addresses into three levels. **Level 1** has the worst reputation, **Level 2** has a better reputation, and **Level 3** has an even better reputation. To help prevent false positives, you can choose to take different actions on different IP reputation levels. Usually, you should take strict actions, such as reject or discard, on **Level 1** IP addresses, and take loose actions, such as quarantine or tag, on **Level 3** IP addresses. The default action for address Levels 1, 2, and 3 is the same as the **IP Reputation** action. If you use the default action for IP reputation, the **FortiGuard** action is used. If you use the FortiGuard default action, the **AntiSpam Profile Default action** is used.

If you want to check all SMTP servers in the **Received** lines of the message header, enable the **Extract IP from Received Header** option.

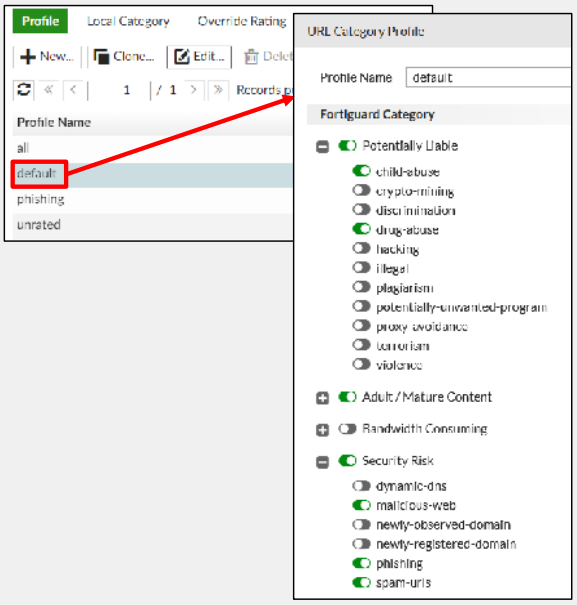
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

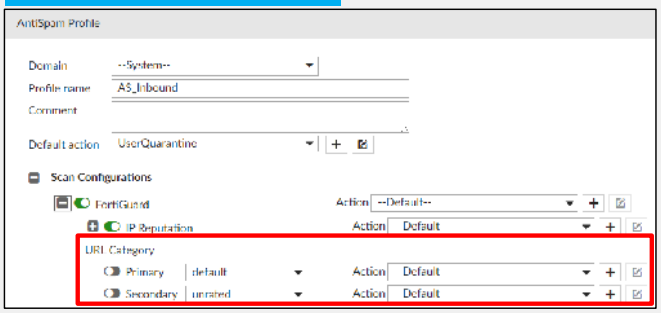
FortiGuard URL Filter

- FortiMail queries FortiGuard for URL categories
- If the rating response matches what is enabled in the URL category profile, the email is treated as spam

Security > URL Filter > Profile



Profile > AntiSpam > AntiSpam



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

FortiGuard URL filtering sorts known URLs into categories, such as phishing, spam, and malicious. You can configure the URL category profile to check for specific categories. If an email message contains any URLs that match the categories enabled in the URI filter profile, FortiMail can treat that message as spam.

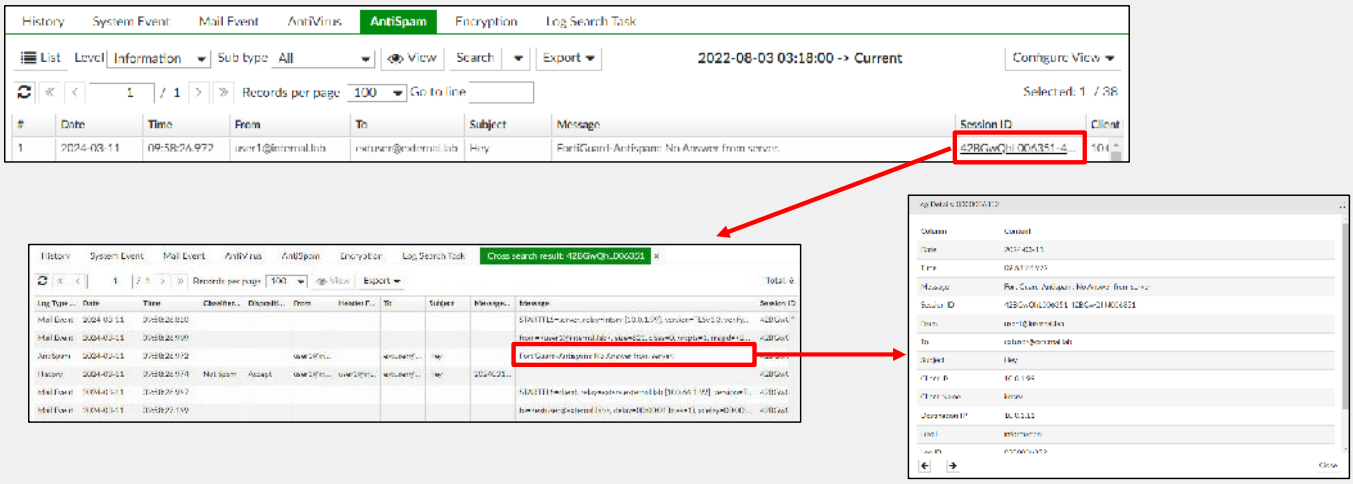
You can also customize URL filters in most deployments. You should always enable the **Security Risk** category. However, you can customize the URL category profile to filter email messages containing URLs that traditionally would not be considered suspicious or malicious.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGuard Connectivity

- If FortiMail cannot contact FortiGuard for a URL category rating the email will be passed
- AntiSpam error logs show the connection issue



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

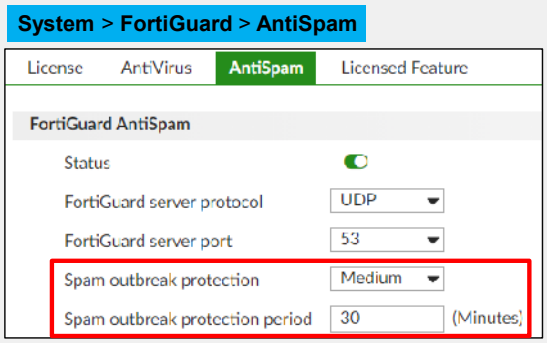
If FortiMail is unable to query FortiGuard to determine if a detected URL matches a defined category the email will be passed. A failure to contact FortiGuard will generate an error in the AntiSpam logs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGuard Spam Outbreak Protection

- Delays suspicious emails for a re-evaluation
  - FortiGuard may be updated in between and rate the email as spam
- Default outbreak protection level is **Medium**
- Default hold period in a dedicated queue is 30 minutes



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 29

Regular FortiGuard updates ensure that FortiMail has the most current threat information available. Even so, it's still possible for FortiMail to receive a spam message that it hasn't seen before and has little or no information about. This feature is effective against zero-day spam outbreaks.

By default, the hold period is 30 minutes, and the outbreak protection level is medium.

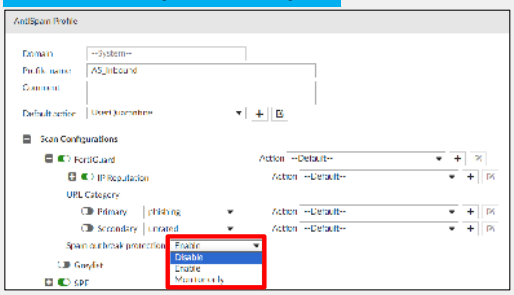
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

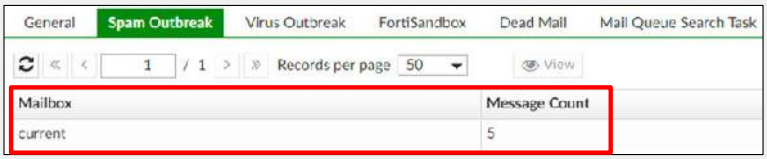
FortiGuard Spam Outbreak Protection (Contd)

- Spam outbreak protection can be set to one of the following:
  - **Enable**—Holds the email in a dedicated queue for a specific time period, and, after the time period expires, queries FortiGuard servers again
  - **Monitor only**—Email is not deferred. Instead, "`X-FEAS-Spam-outbreak: monitor-only`" is inserted as its header, and the email is logged
- Intelligent detection of zero-day spam outbreaks

Profile > AntiSpam > AntiSpam



Monitor > Mail Queue > Spam Outbreak



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

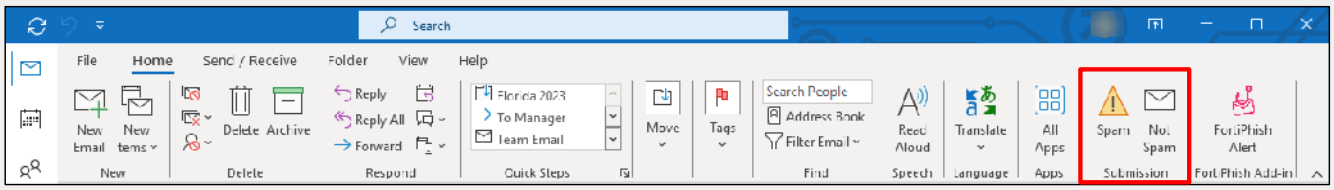
When Spam outbreak protection is enabled, the suspicious email is held in a dedicated queue, for a specific period of time, and then re-evaluated. This gives FortiGuard an opportunity to learn about the potential spam outbreak and update its databases. After the timeout value for the email expires, FortiMail queries the FortiGuard servers again. If the ratings come back as clean, FortiMail releases the email to the recipient; otherwise, it applies the antispam action. When set to **monitor only**, email is not deferred. Instead, "`X-FEAS-Spam-outbreak: monitor-only`" is inserted as its header, and the email is logged.

Vouchers & Dumps are Available | WhatsApp +201224560923

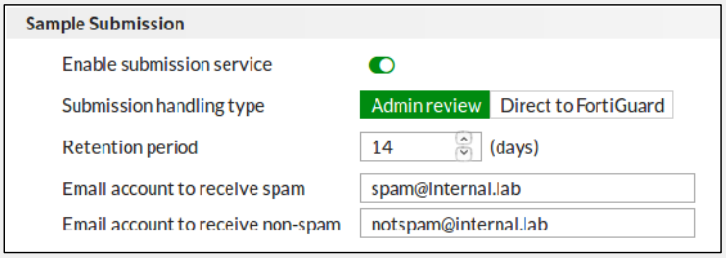
DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGuard Spam Submission

- Outlook plugin to submit suspicious email as spam to either an administrator or FortiGuard



System > FortiGuard > AntiSpam



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

End users can submit suspicious email as spam using an Outlook plugin. These emails can then be either reviewed by an administrator or sent to FortiGuard for immediate evaluation.

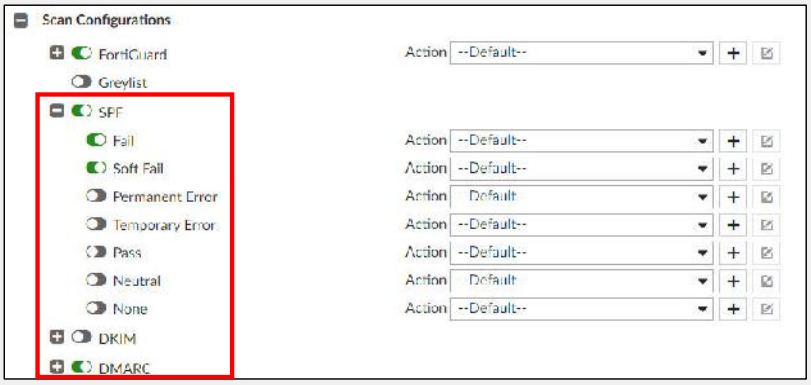
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SPF DKIM and DMARC Validation

- Sender policy framework (SPF):
  - Check the sender domain DNS TXT records for permitted servers
- DomainKeys Identified Mail (DKIM):
  - Messages are signed with a private key that can be validated upon receipt
- Domain-based message authentication, reporting, and conformance (DMARC):
  - Performs email authentication by validating both the SPF and DKIM signature
  - Both SPF check and DKIM check must fail for DMARC check to fail

Profile > Antispam > Antispam



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

SPF is a technique that you can use to validate senders. Using SPF, a domain owner publishes specially formatted DNS text (TXT) records. The records contain the authorized MTAs of the domain. Using the SPF check feature, FortiMail performs a DNS TXT record lookup for the sending domain of any email session. If an SPF entry exists, FortiMail compares the address of the SPF entry with the address of the sending MTA, and, if no match is found, treats the email as spam. In the antispam profile, you can configure the various granular settings available with SPF validation. Configure the **None** setting to deal with domains for which there are no SPF records. Configure the **Neutral** setting for SPF records that don't want to assert that a particular IP address is authorized to send from the sending domain. A neutral result is treated the same as a none result. SPF records with a neutral result are typically using the ? qualifier. Configure the **Pass** setting to deal with IP addresses that are authorized to send from the sending domain. This result is generated when the sender IP is correctly identified in the SPF record of the sending domain with the correct syntax. Configure the **Fail** setting to deal with IP addresses that are not authorized to send from the sending domain. This means that the SPF record of the sending domain does not contain the sending server or IP address.

DKIM utilizes public and private keys to digitally sign outbound emails to prove that email has not been tampered with in transit. Enabling this will allow FortiMail to validate the key signature against the public key to verify if the email is authentic.

DMARC is much more comprehensive. Using DMARC, FortiMail validates both SPF and DKIM. However, the email only has to pass one of these checks. If the email fails both the SPF and DKIM checks, then it is treated as spam. DMARC validation isn't universally adopted yet; however, it's slowly becoming more popular.

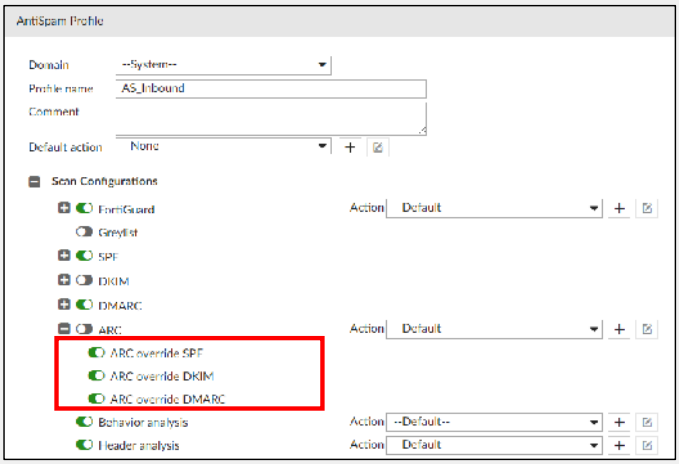
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

ARC Validation for SPF, DKIM, and DMARC

- Authenticated received chain (ARC)
  - Allows intermediate email servers to sign email
  - Helps verify email chains with SPF, DKIM, and DMARC
  - Sealed with a message header entry by the upstream mail server

Profile > Antispam > Antispam



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

ARC permits intermediate email servers, such as mailing lists or forwarding services, to sign the original authentication results of an email. This allows a receiving service to validate an email, in the event the SPF and DKIM records of the email are rendered invalid by the processing of an intermediate server. This setting allows FortiMail to validate these services even when an original message has been altered by an upstream email server, but has been signed and sealed with a valid ARC entry in the message header.

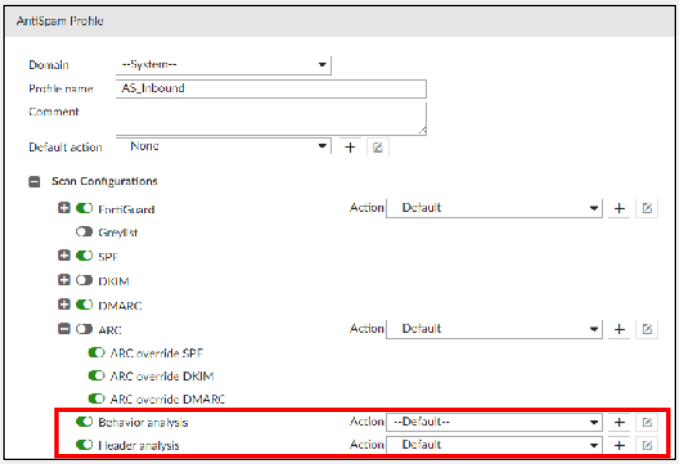
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Behavior and Header Analysis

- **Behavior Analysis:**
  - Analyzes suspicious email using characteristics of known spam samples recently caught by the device
  - Can detect changing spam samples and protect against zero-day outbreaks
- **Header Analysis:**
  - Looks for the presence of header entries commonly found in spam email

Profile > Antispam > Antispam



FORTINET Training Institute

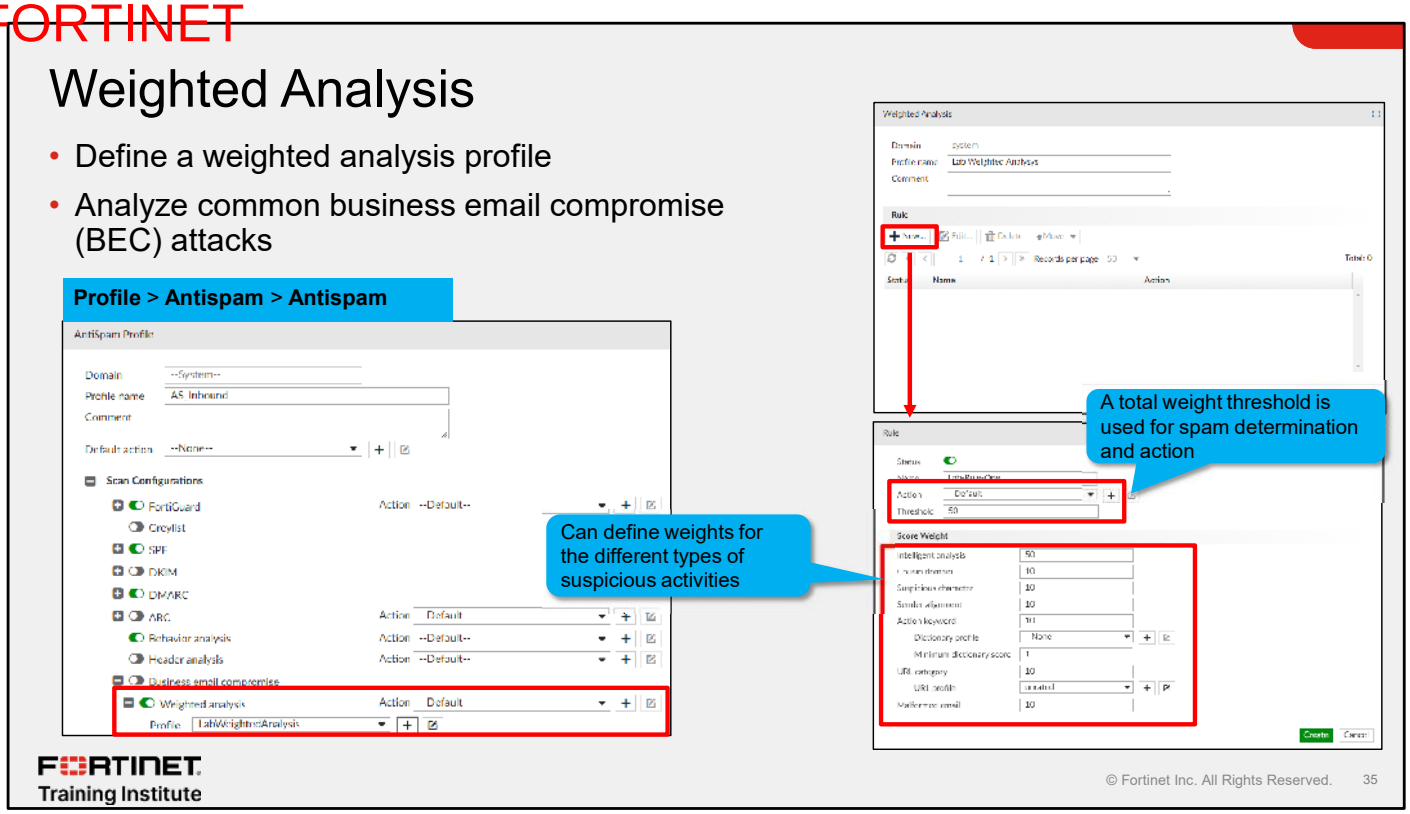
© Fortinet Inc. All Rights Reserved. 34

Behavior analysis uses a variety of methods to identify spam that is not caught directly by FortiGuard. By applying elements of heuristics and a fuzzy matching algorithm, which compares spam recently detected (within the past 6 hours) by FortiGuard signatures on the FortiMail, behavioral analysis can detect changing spam samples. Behavior analysis is useful for detecting and preventing new zero-day spam outbreaks.

Header analysis looks for the presence of header entries that are commonly found together in spam email.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The weighted analysis option allows you to combine and define the importance of the different types of BEC attacks. A weighted analysis profile contains one or more ranked rules. Within the rules, weights are assigned to the different BEC attack evaluation techniques. As possible BEC attacks are identified, the weight of each matching spam evaluation technique is added together to determine if the threshold has been met. Once the threshold is met or exceeded, the mail is designated as spam and the associated action is triggered.

Three spam identification techniques are available only as part of a weighted analysis rule:

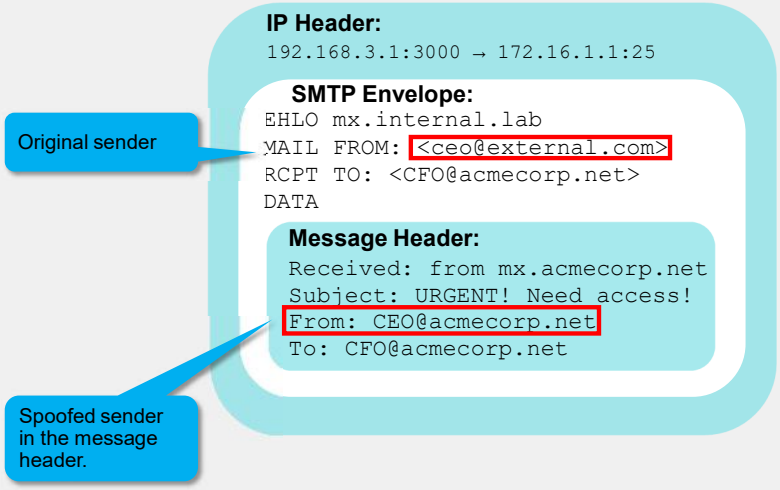
- **Intelligent analysis**: Uses multiple BEC attack identification techniques (including SPF, DKIM, and DMARC) to reduce false positives.
- **Suspicious character**: Identifies URLs and emails with Unicode characters from different languages.
- **Malformed email**: Detects malformed data in the email structure, header, or body as defined in *RFC 7103*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Impersonation Analysis

- Prevents whaling attacks against C levels
- Map display name to correct email address
- Needs license and is available only as part of the enterprise ATP bundle
- Two types of mapping:
  - Manual—manually enter mapping entries and create impersonation analysis profiles
  - Dynamic—mapping entries can be learned dynamically from mail statistics service



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 36

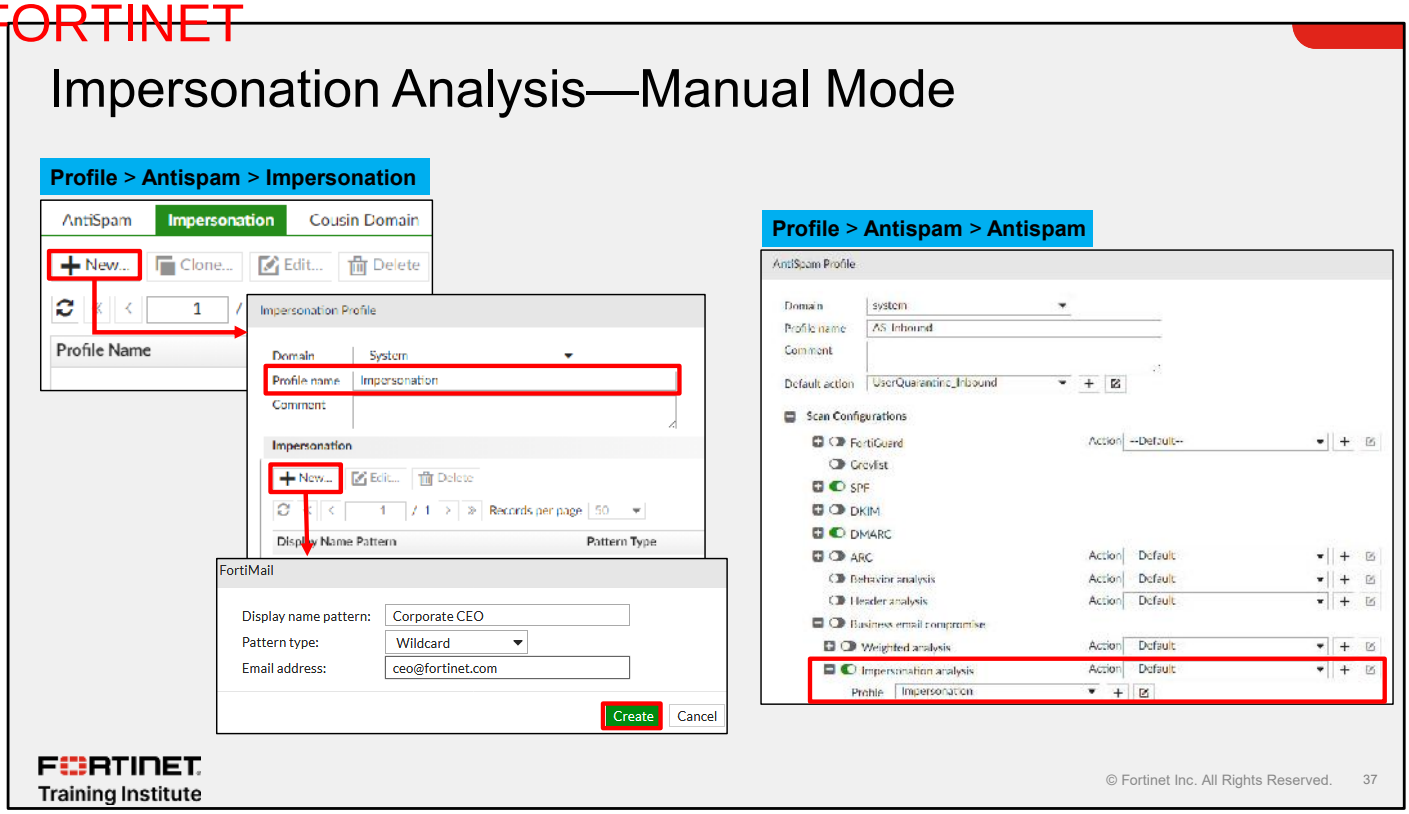
Email impersonation is a type of email spoofing attack that attempts to deceive the recipient by using a forged header to make the message appear to be from a trusted sender. *Whaling* is a specific type of impersonation attack that targets key executive personnel whose names and email addresses are publicly posted or easily available. Using the impersonation analysis feature on FortiMail, you can map high-value target display names with their correct email addresses.

There are two types of mapping—dynamic and manual. Dynamic mode matches learned entries such as “Doe, John” as “John Doe”; whereas in manual mode, you must specify both explicitly.

To activate impersonation analysis, FortiMail must have the Enterprise ATP bundle license.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Enter the display name of the high-profile user that the impersonation profile will protect. You can enter this name using either a wildcard or regular expression. Next, enter the email address that is associated with the user's display name, and then click **Create**.

If the user wants to associate multiple email addresses with their display name, create an impersonation entry for each email address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Impersonation Analysis—Dynamic Mode

- Default mapping type is manual
- Enable FortiMail mail statistics service to activate dynamic mode
  - Enable in the CLI
- Can run dynamic and manual mode simultaneously

```
config antispam settings
set impersonation-analysis dynamic manual
end
```

- Also enable the Mail Statistics service

```
config system global
set mailstat-service enable
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 38

In addition to manually entering mapping entries and creating impersonation analysis profiles, FortiMail Mail Statistics Service can automatically learn the mapping in the incoming email **Header To** fields and track the mapping dynamically.

To use FortiMail manual impersonation analysis scanning, dynamic impersonation analysis scanning, or both, use the commands shown on this slide. By default, FortiMail uses manual analysis only.

You can also enable the FortiMail mail statistics service with the commands shown on this slide. This service is also disabled by default.

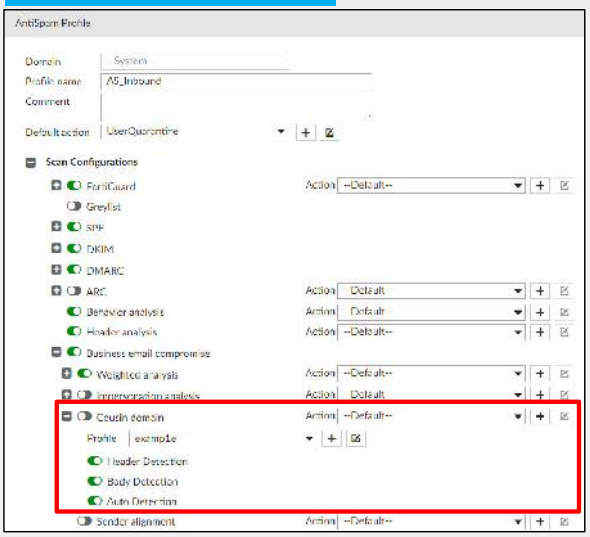
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

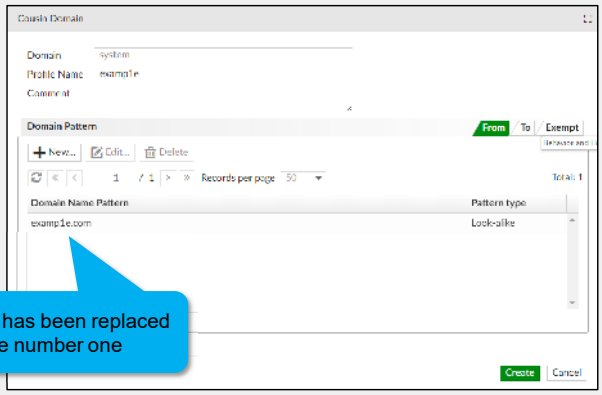
Cousin Domain

- Identify deliberately misspelled domain names

Profile > Antispam > Antispam



- Cousin domain configuration contains one or more domain patterns



The "l" has been replaced with the number one

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 39

Identifying cousin domains helps safeguard against intentionally misspelled domain names that are intended to look like legitimate domain names. A common practice used by spammers is to change one character in a URL to trick an end user into clicking the URL. In the example shown on this slide, the "l" in example.com has been replaced by the number one.

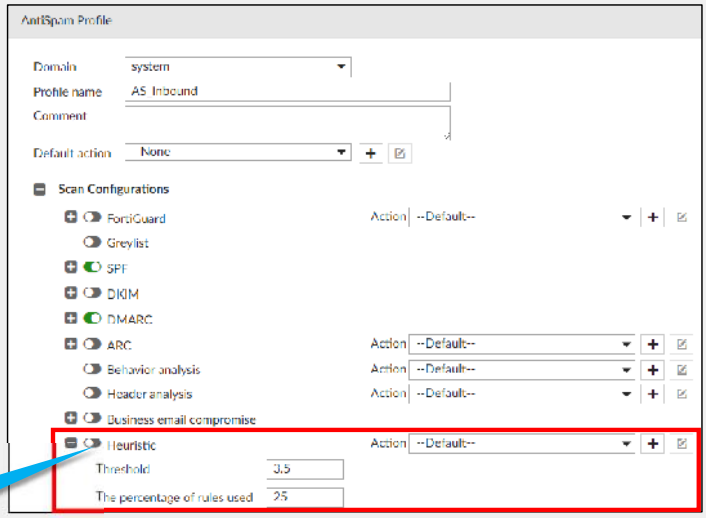
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Heuristic Scan

- Header and body of emails scanned against a set of predefined heuristic rules created using PCRE:
  - Each of the rules has a score associated with the likelihood of it being spam
- When a rule is matched, its associated score is added to the total score for the email
- When the total score of the email reaches a predefined threshold, the email is determined to be spam
- Rules are continuously updated by FortiGuard subscription services
- Disabled by default

Profile > Antispam > Antispam



By default, **Heuristic** is not enabled.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 40

FortiGuard maintains a set of heuristic rules based on known spam content. These heuristic rules use PERL-compatible regular expressions (PCRE), a powerful form of regular expression matching, to locate spam-identified attributes within each message. These rules are continuously updated as new spam threats emerge.

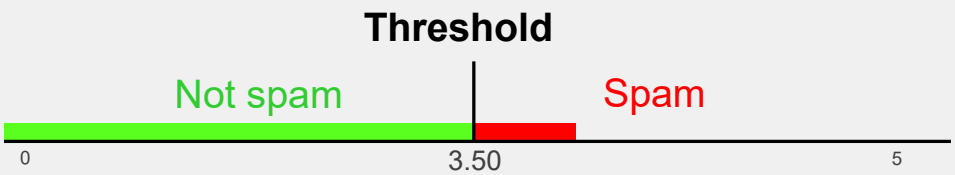
As each rule is evaluated against the message, a score is generated, reflecting how much of the rule criteria was found in the message. When FortiMail finishes processing a rule, it adds the score to the total score of the message. If the total score meets or exceeds the set threshold, FortiMail determines that the message is spam.

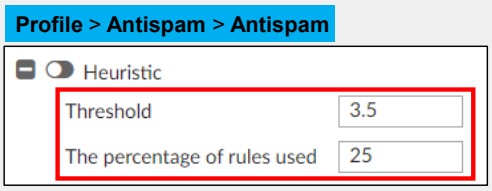
Heuristics scanning can be very resource intensive.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Heuristic Scan (Contd)





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 41

When you enable heuristic scanning in an antispam profile, you use two settings to fine-tune the behavior. The first setting, **Threshold**, determines what total score is necessary to decide that an email is spam. The default value might be appropriate for most environments, but you can increase it, if there are false positives, or decrease it as necessary. Expect to tune this value multiple times because there is no universal value that suits all deployments. If the threshold is not set correctly, it can generate unnecessary false positives or negatives.

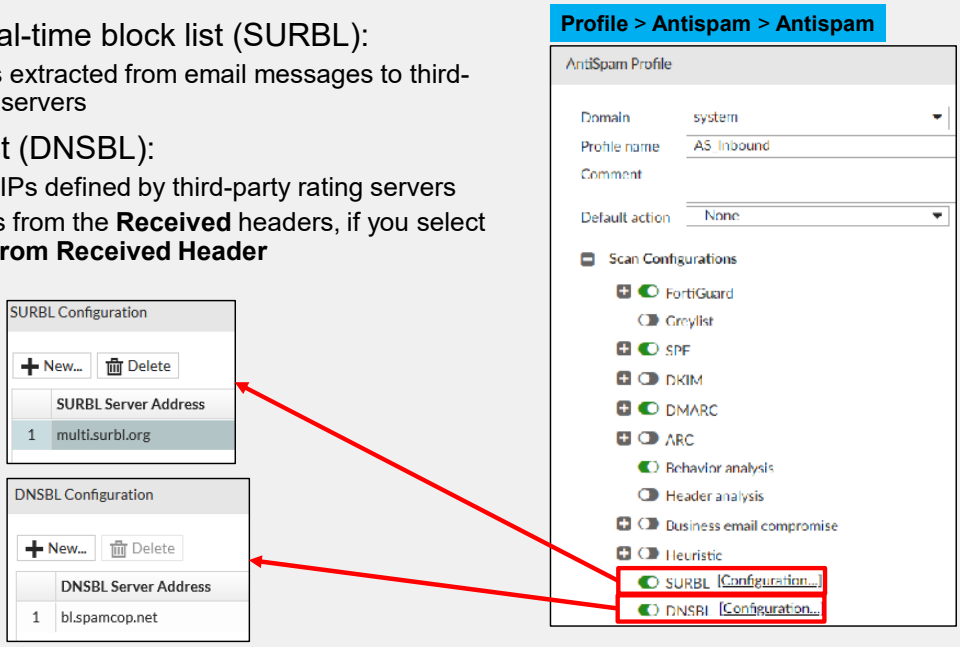
The second setting, **The percentage of rules used**, specifies how much of the rule list is applied to each message. The rule ordering is maintained by FortiGuard. The rules that detect the most prevalent spam are at the top of the list, and rules for older, more obscure spam are lower. The rule ordering changes over time as FortiGuard responds to the ever-changing spam landscape. Heuristic rule processing is a resource intensive process, so you can use this setting to strike a balance between performance and thoroughness.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SURBL and DNSBL

- Spam URI real-time block list (SURBL):
  - Sends URIs extracted from email messages to third-party rating servers
- DNS block list (DNSBL):
  - Verifies the IPs defined by third-party rating servers
  - Includes IPs from the **Received** headers, if you select **Extract IP from Received Header**



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 42

A SURBL is similar, in concept, to the FortiGuard URI filter, but it uses third-party SURBL servers. FortiMail extracts URIs from email messages and sends them to the SURBL servers. The SURBL servers identify if the URIs are known to be associated with spam.

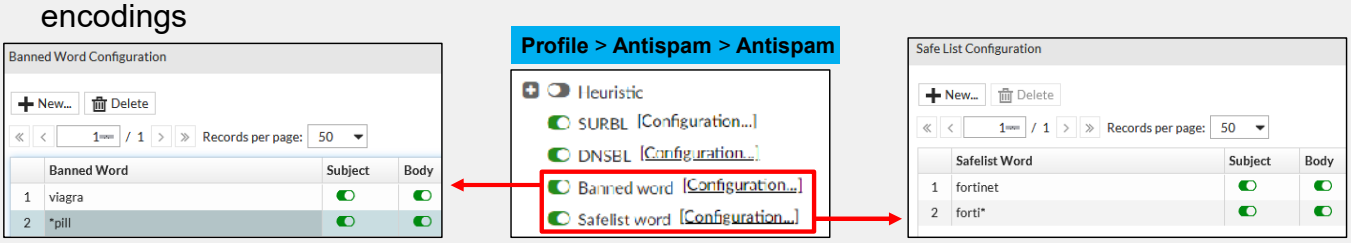
The DNSBL is similar, in concept, to the FortiGuard IP reputation feature, but it uses third-party DNSBL servers. FortiMail will include the IPs from the chain of **Received** headers in DNSBL scans, if you select **Extract IP from Received Header,** in the antispam profile. Just like the FortiGuard IP reputation scan, the DNSBL scan ignores any RFC 1918 addresses. If an IP is blocklisted by the DNSBL server, FortiMail treats the email as spam, and executes the configured action.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Banned and Safe Word Lists

- Banned word:
  - Subject or body of an email is scanned for words against a list of prohibited words
  - If a match is found, the email is treated as spam
- Safelist word:
  - Subject or body of an email compared against a list of safe words
  - If a match is found, the email is exempt from all antispam inspections
- Supports wildcard characters but not regular expressions or extended character set encodings



Note: If a word exists in both lists, then the safelist word match takes precedence.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 43

When you enable the **Banned word** scan option in an antispam profile, FortiMail scans the subject and message body for the presence of any word on a list of prohibited words. If a message contains one or more of the words on the list, FortiMail treats the message as spam.

The **Safelist word** scan option scans the subject or body of an email for the presence of any word on a list of safe words. If a match is found, FortiMail exempts the email from antispam inspections. Other inspection profiles that you enable still apply. The safelist words take precedence over banned list words if a word matches an entry in both lists.

To maintain efficiency, the word lists support wildcard characters, but not regular expressions or extended character set encodings.

Vouchers & Dumps are Available | WhatsApp +201224560923

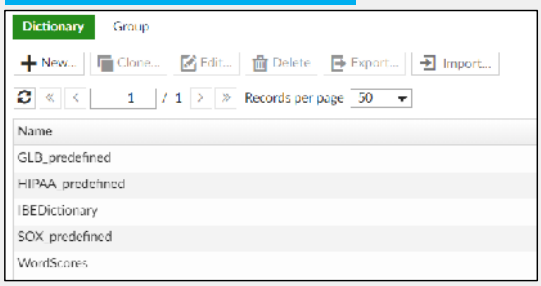
DO NOT REPRINT Brave-dumps.com
© FORTINET

Dictionary Scan

- Scan emails against a single dictionary, or a group of dictionaries

Profile > Antispam > Antispam

Profile > Dictionary > Dictionary



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 44

A dictionary scan provides a more flexible way to identify email messages that contain specific words or phrases. To use this feature, you must create a dictionary profile containing words or phrases of interest. This can include regular expressions as well as extended character set encodings. If the scan finds one or more dictionary entries in the email message, FortiMail adds the `X-FEAS-DICTIONARY` header to the email header, followed by the dictionary word or pattern that was found in the email, and treats the email as spam.

Dictionary scans are more resource intensive than banned word scans because they provide more flexibility. For simple lists of words, consider using banned word scans to improve performance.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Image Spam Scan

- Analyzes embedded images for spam characteristics
- Select **Aggressive** to analyze image in attachments
- Analyzes characteristics of the images, including the depth of the color, the grey level, the space, and the color change
- Supports GIF, JPEG, and PNG formats
- Can be process intensive

Profile > Antispam > Antispam

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 45

FortiMail is capable of detecting spam messages that consist mainly of embedded GIF, JPEG, or PNG images with little or no text in the message body. Many of the other spam detection techniques have difficulty with messages like this because of the lack of text.

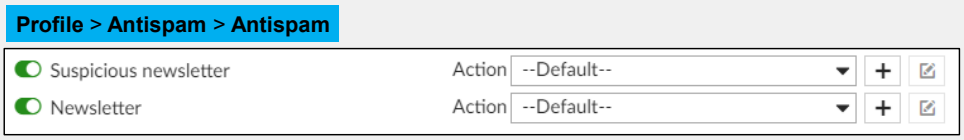
The image spam feature analyzes the characteristics of embedded images using fuzzy logic developed by FortiGuard, to determine if the message is spam. If you enable **Aggressive**, FortiMail also analyzes image attachments too. Image spam scanning can be resource intensive, especially if you enable **Aggressive**. However, you should use image spam scanning if image-based spam messages are passing through the other spam techniques undetected.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Newsletter Detection

- Newsletter:
  - Detects messages that are likely to be legitimate newsletters
  - Usually tagged instead of quarantined or rejected
- Suspicious newsletter:
  - Detects spam disguised as newsletters



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 46

The newsletter scan detects messages that are likely to be legitimate newsletters and treats them as spam. One interesting possibility is to tag the subject line of these email messages with “[newsletter]” so that the end user can filter them at their MUA email client.

Spammers sometimes disguise email to look like legitimate newsletters. The suspicious newsletter scan examines the content to detect spam characteristics, and executes the configured antispam action.

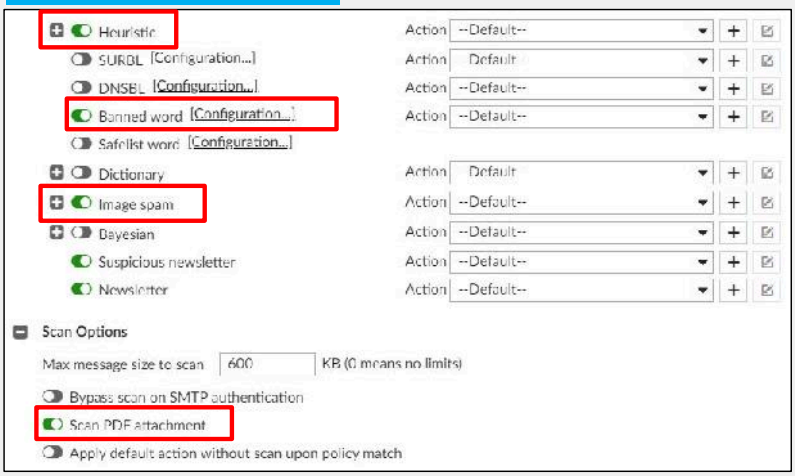
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

PDF Scanning

- Submits the first page of PDF to banned word, heuristic, and image spam scanners
  - You must enable at least one of these three techniques

Profile > Antispam > Antispam



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 47

Like image-based spam, spammers may attempt to evade detection by sending messages containing only a PDF attachment. PDF scanning converts only the first page of the PDF document to a format that is suitable for analysis by the banned word, heuristic, and image scanning methods. Enable at least one of these three methods in the antispam profile, if you wish to perform PDF scanning.

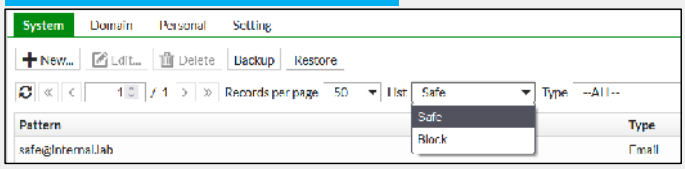
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

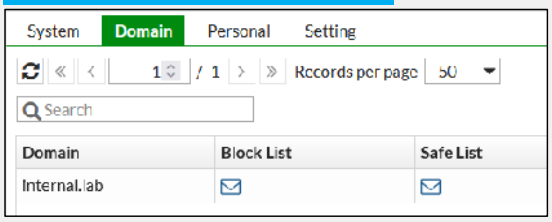
Block and Safe Lists

- Block or allow email from email addresses, domains, or IP addresses

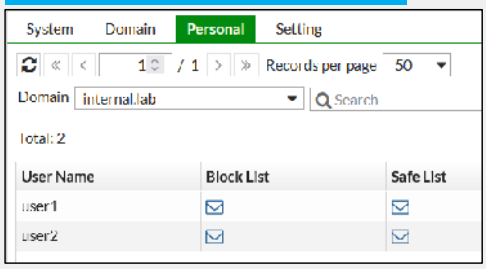
Security > Block/Safe List > System



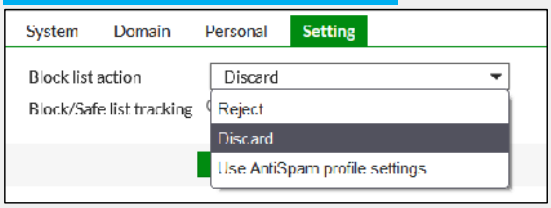
Security > Block/Safe List > Domain



Security > Block/Safe List > Personal



Security > Block/Safe List > Setting



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 48

FortiMail uses four levels of blocklisting and safelisting. The order of processing priority is system, then session, then domain, and finally, personal.

System-level list entries apply to all protected domains. Domain-level list entries apply to all users in that protected domain. Personal list entries are relevant for the user only.

You can also configure blocklist and safelist entries in a session profile. The list entries will affect only email messages being handled by the IP policy that uses that session profile.

For any messages matching a safelist, FortiMail bypasses all antispam checks and the message is processed through any other configured inspection profiles from the matching policy. List entries can take the form of email addresses, domains, or IP addresses. If a message matches an entry on a blocklist, the message is processed by the blocklist action in the **Setting** tab. You can set the blocklist action to reject or discard the message, or to invoke the action in the matching antispam profile.

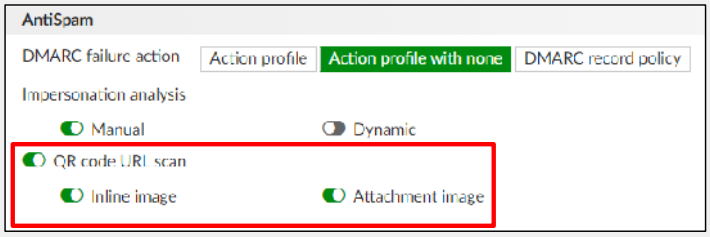
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

QR Code Scanning

- Scans QR codes
  - Inline image
  - Attachment image
- Identifies QR code images that contain known spam URLs.

Security > Option > Preference



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 49

QR codes containing spam URLs are another method for getting spam delivered to intended targets. FortiMail can scan both inline and attached QR code images and compare URLs to a list of known spam URLs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Spoofed Header Detection

IP:
172.16.1.1:3000 → 192.168.3.1:25

SMTP Envelope:
```
EHLO mx.external.lab
MAIL FROM: <spam@external.lab>
RCPT TO: <user1@internal.lab>
RCPT TO: <user2@internal.lab>
DATA
```

Message Header:
```
Received: from mx.external.lab
Subject: Policy change notice!
From: CEO@internal.lab
To: user1@internal.lab, …
```

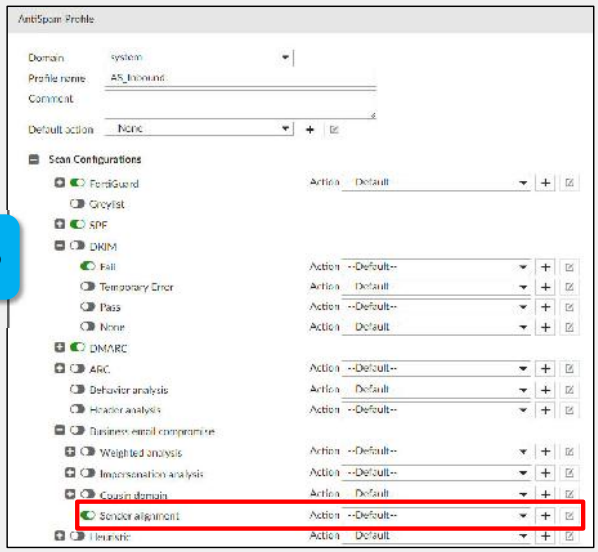
Message Body:
```
See new policy document!
```

Legitimate sender in the envelope

Sender alignment compares these two values

Spoofed sender in the message header

Profile > AntiSpam > AntiSpam Profile



FORTINET Training Institute

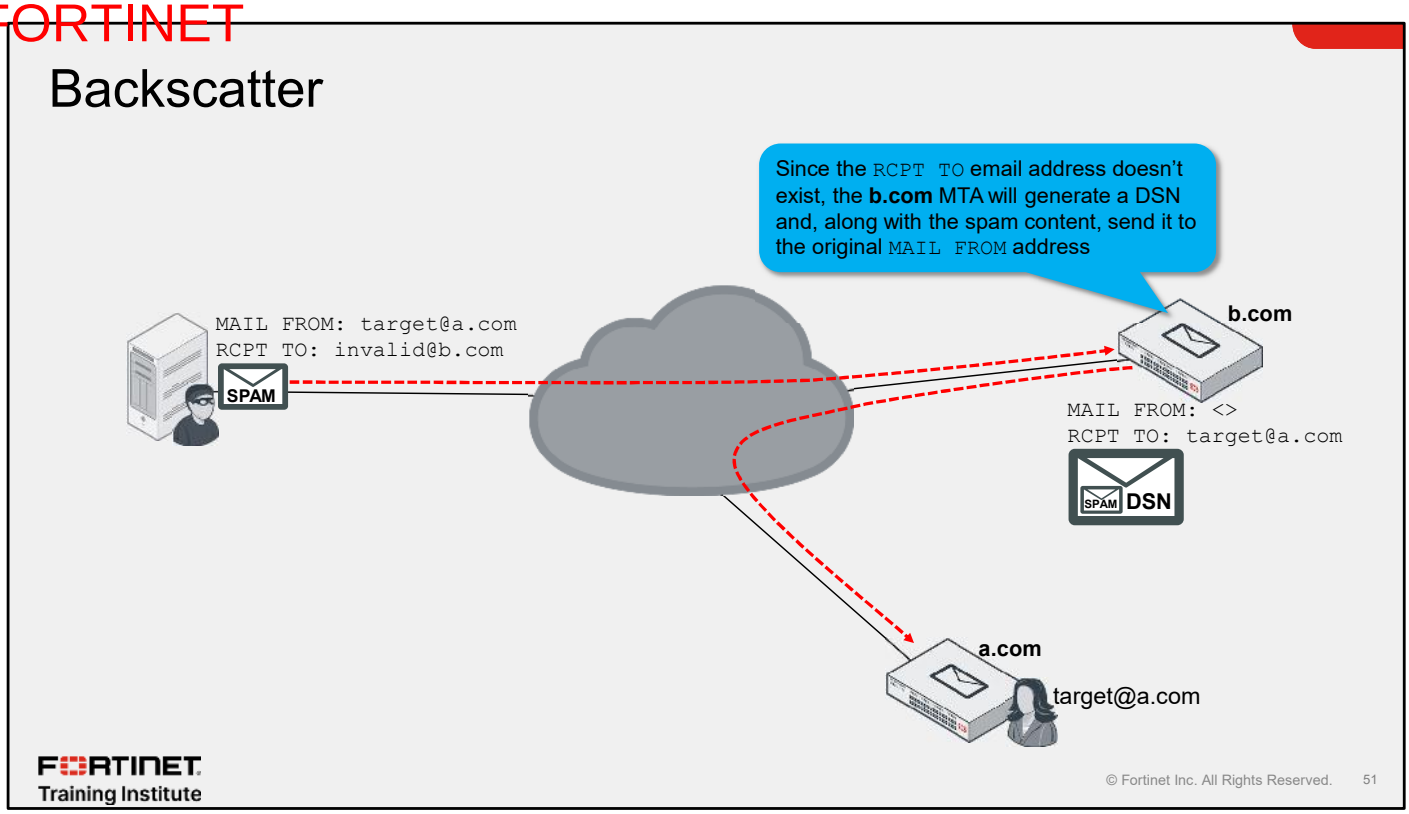
© Fortinet Inc. All Rights Reserved. 50

Spammers use many tricks to bypass security mechanisms. One of these tricks is to spoof SMTP header addresses. The spammer might use a legitimate sender in the envelope `MAIL FROM` address, but when they craft the header, they spoof the `From` address. Since MUAs use the header addresses to display email information, such as the `From`, and `To` fields, the recipients see the spoofed email sender.

You can enable the **Sender Alignment** setting to verify the email message `From:` header is the same as the SMTP envelope to block spoofed headers.

Vouchers & Dumps are Available | WhatsApp +201224560923

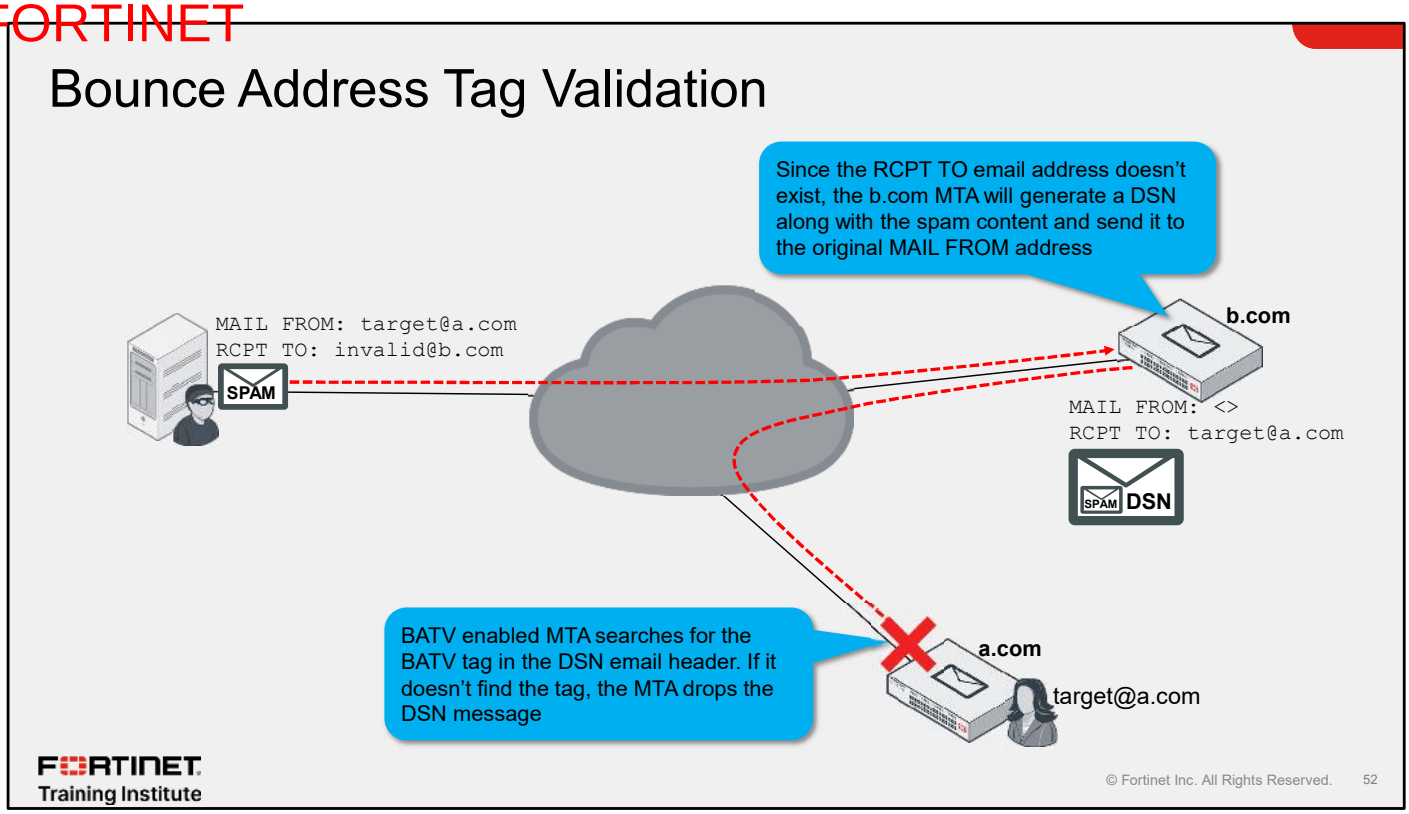
DO NOT REPRINT Brave-dumps.com
© FORTINET



Spammers sometimes try to bypass antispam measures by hiding spam content in delivery status notifications (DSN) or bounce messages. DSN messages don't undergo the same level of antispam processing as regular email, if any at all. In a clever abuse of SMTP, spammers forge the email address of the intended target as the `MAIL FROM` address and use a non-existent recipient in `RCPT TO` address. Then, the spammers send the message out to a relay MTA, which, since it cannot deliver the message, creates the DSN and sends it out to the spammer's intended target, with the original spam content attached. This technique is typically referred to as backscatter.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



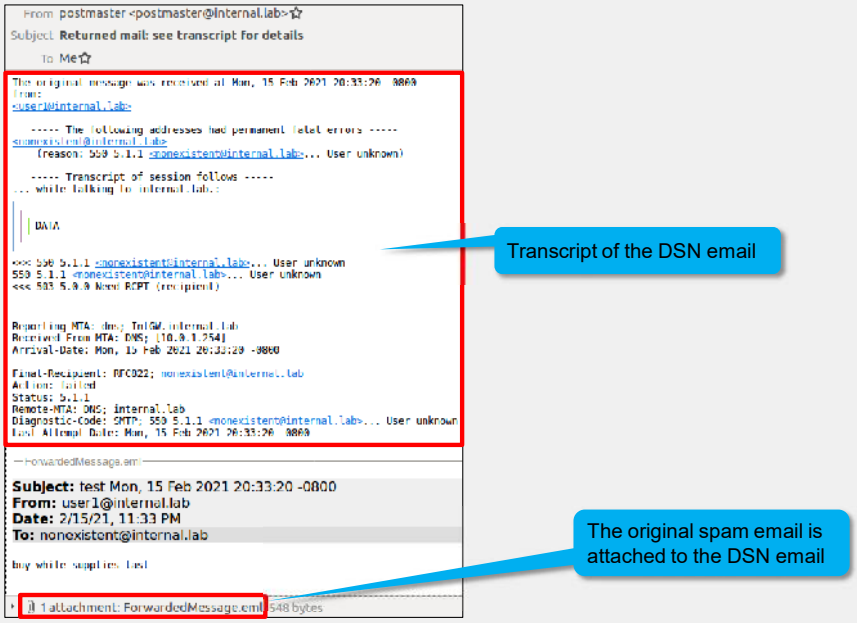
If you look at the same backscatter attack attempt but this time with bounce address tag validation (BATV) enabled on the a.com MTA, the outcome looks very different. The BATV-enabled MTA searches for the BATV tag in the DSN email header. If it doesn't find the tag, the MTA drops the DSN message instead of delivering it to the end user.

BATV provides a mechanism that can distinguish between legitimate DSN messages and backscatter spam, provided that the DSN was generated because of a message sent by a particular FortiMail-protected domain.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

DSN Email With Spam Attached



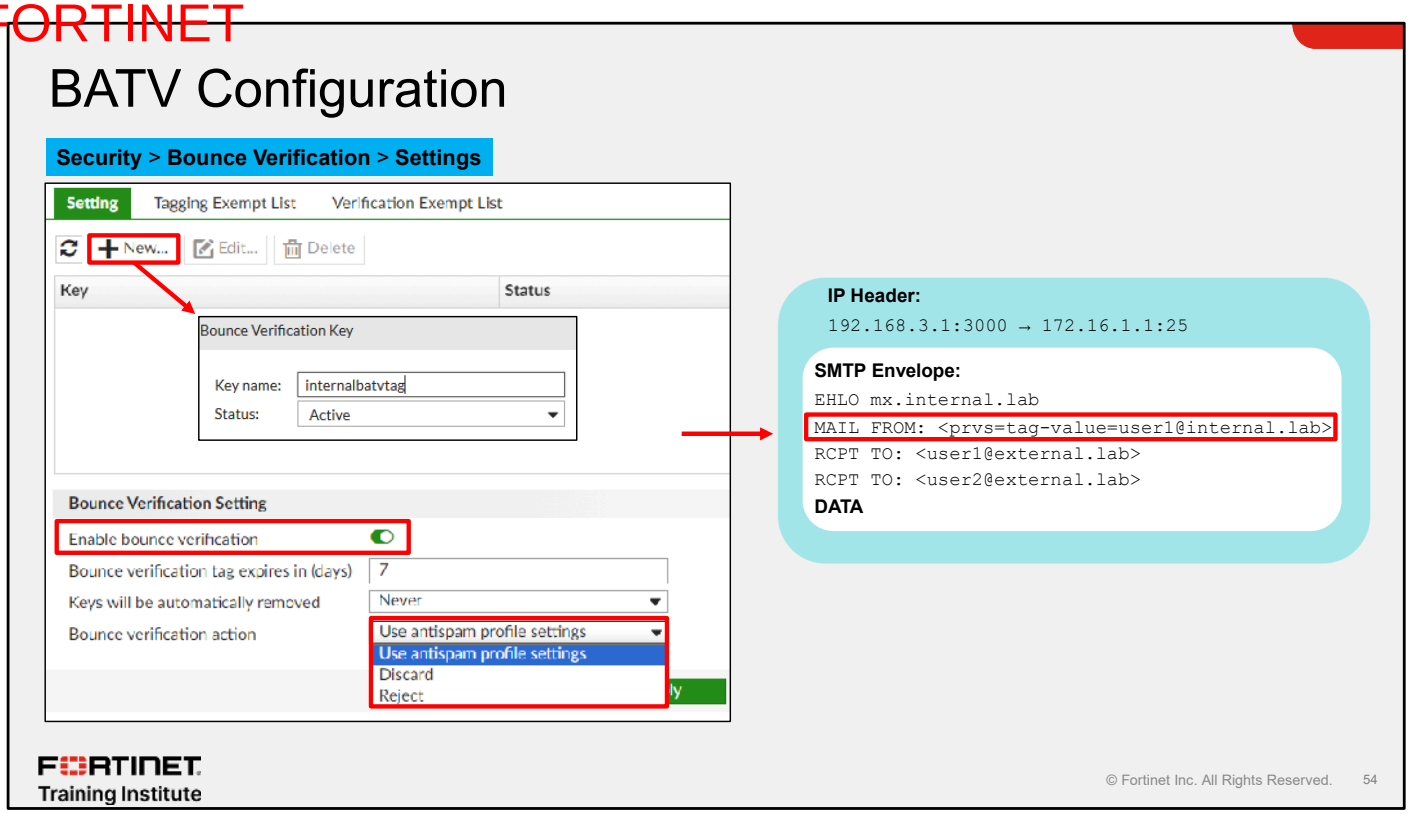
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 53

On the email client, when you open the DSN email, you see the DSN transcript along with the original email, which is attached.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To configure BATV on FortiMail, you must first enter a key. The key can be any sequence of ASCII characters. The key, along with a cryptographic salt value, generates a unique tag for each message. You can create new keys if necessary, but only one key in the list can be active at any time. Once an active key is available, enable BATV and set the action to execute if tag validation fails.

After you enable BATV, FortiMail starts prepending the key to the sender's email address in the SMTP envelope `MAIL FROM` field. FortiMail doesn't alter the sender's email address. If the tagged message is undeliverable, the resulting DSN contains the tagged version of the sender's address, since the original message is appended to the DSN. When the DSN arrives on FortiMail, FortiMail searches for this tag. If the tag exists, it means the DSN was generated for an email sent out from one of the protected domains, and FortiMail delivers the DSN to the recipient. If the tag doesn't exist, FortiMail drops the DSN.

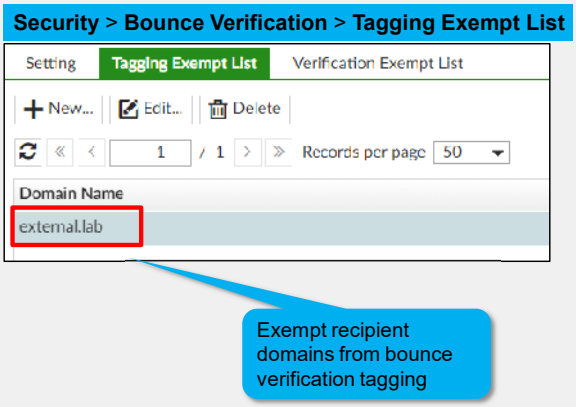
For inbound DSN messages, the envelope `MAIL FROM` field must be blank; otherwise, FortiMail won't perform bounce verification on it. The `MAIL FROM` envelope address of a DSN message is typically blank, to avoid the potential to create continuous bounce messages that bounce back and forth forever between MTAs.

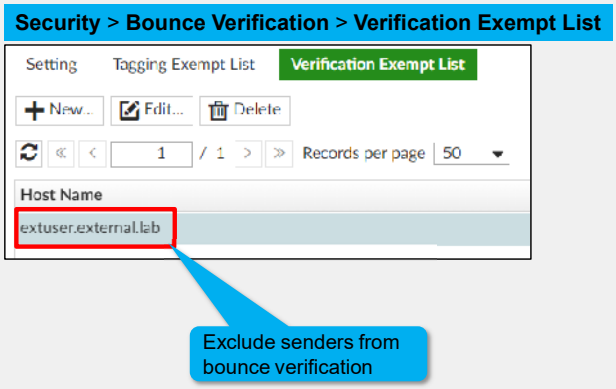
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

BATV Exemptions

- FortiMail will not include BATV tags for domains in the **Tagging Exempt List**
- Hosts added to the **Verification Exempt List** will not be subject to tag verification





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 55

Certain MTAs reject email messages that have BATV tags in the email header, either deliberately or because of configuration mistakes. To allow successful email transmission between FortiMail and these MTAs, you can exclude these MTAs from BATV tagging. Email sent from FortiMail to the MTAs in the tagging exempt list will not have the BATV tags added to their headers.

Other MTAs won't append the original email to the DSN email. If the original email isn't appended to the DSN, the email won't have a BATV tag, and tag verification fails. To exclude these MTAs from tag verification, add them to the **Verification Exempt List**.

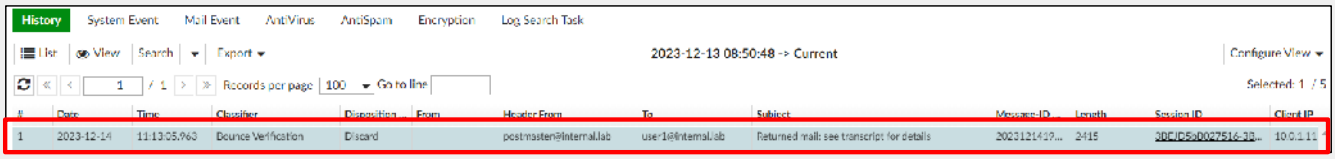
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

BATV Logs

- Bounce verification details

Monitor > Log > History



FORTINET Training Institute
© Fortinet Inc. All Rights Reserved. 56

This slide shows an example of a log showing that an email was discarded because it failed bounce verification.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Order of Execution

- FortiMail performs each of the antispam scanning actions and other actions, in a specific order
- Actions that are taken as a result of scanning can be categorized as follows:
  - Final actions
    - Reject, discard, personal quarantine, and system quarantine
    - If these actions are taken, no further scanning will be processed
  - Nonfinal actions:
    - Tag, add header, replace, archive, notify, BCC, rewrite, and encrypt
    - If one or more of these actions is taken, FortiMail will continue processing the email with other scans
- Execution sequence of antispam techniques can be found in the *FortiMail Administration Guide*

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 57

FortiMail performs each of the antispam scanning actions and other actions, in a specific order. Actions that are taken as a result of scanning can be categorized as either final or nonfinal.

When no other actions can be applied to an email message after taking an action, then it is considered a final action. For example, reject, discard, personal, and system quarantine. If FortiMail applies a final action, no further scanning will be performed.

FortiMail can apply multiple nonfinal actions to an email, but only one final action.

You can find the detailed execution sequence of antispam techniques in the *FortiMail Administration Guide.*

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. What is the default mapping mode when you use the impersonation analysis feature on FortiMail?
   - ✓ A. Manual
   - B. Dynamic

2. Which three antispam techniques can you use to scan PDF files? (Choose three.)
   - ✓ A. Banned word
   - ✓ B. Heuristics
   - C. Behavior analysis
   - D. Impersonation analysis
   - ✓ E. Image spam

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 58

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Antivirus
- ✓ Antispam Profiles
- ✓ Antispam Techniques
- Personal Quarantine Management

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 59

Good job! You now understand antispam techniques and different ways to block spam.

Now, you will learn about personal quarantine management.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Personal Quarantine Management

Objectives

- Implement and manage quarantine mailboxes for users

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 60

After completing this section, you should be able to achieve the objective shown on this slide.

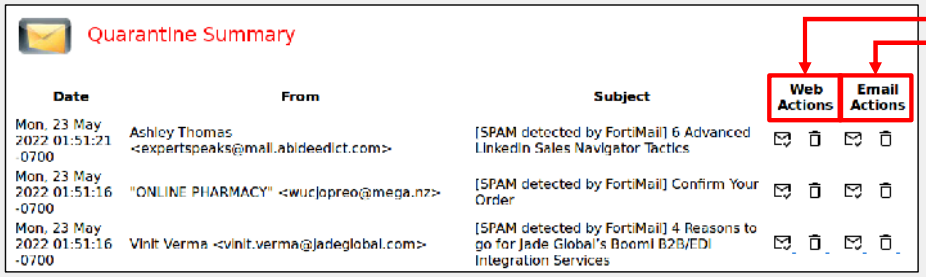
By demonstrating competence in personal quarantine management, you will be able to manage quarantine reports and access a personal quarantine through webmail.

Vouchers & Dumps are Available | WhatsApp +201224560923

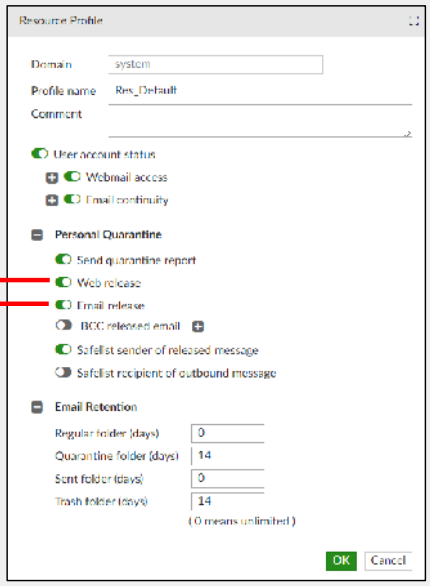
DO NOT REPRINT Brave-dumps.com
© FORTINET

Quarantine Reports

- Scheduled reports for users with quarantined email
- Email and web actions to release or delete quarantined emails



Profile > Resource > Resource



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 61

FortiMail can generate a quarantine report for each end user, to notify them of any email in their quarantine mailbox. FortiMail sends the reports on a schedule. The reports are generated only for mailboxes that contain quarantined email.

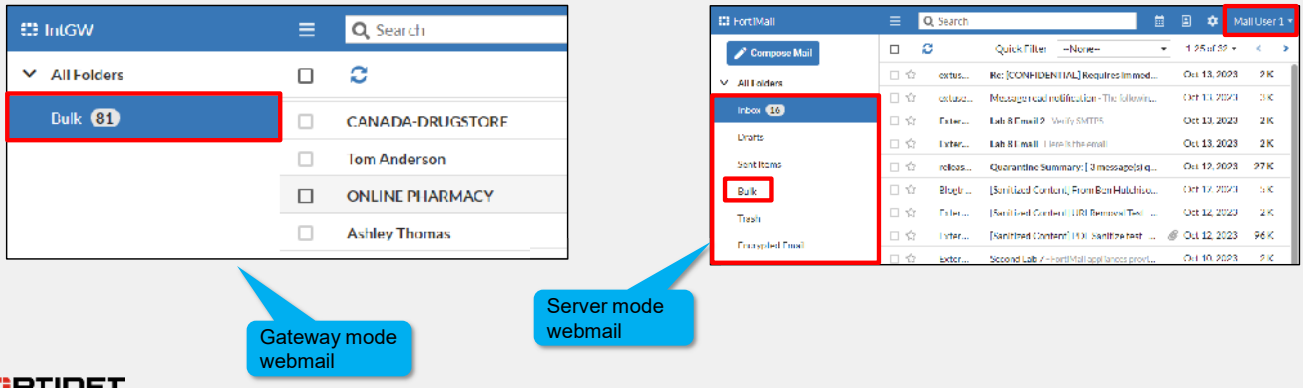
Depending on the action profile configuration, users can use either email actions or web actions to release or delete quarantined messages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Accessing a Personal Quarantine Using Webmail

- Personal quarantine access through webmail
- In Gateway mode, the quarantine mailbox contains only the **Bulk** folder
- In Server mode webmail, you can access all mailbox folders, including **Bulk**



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 62

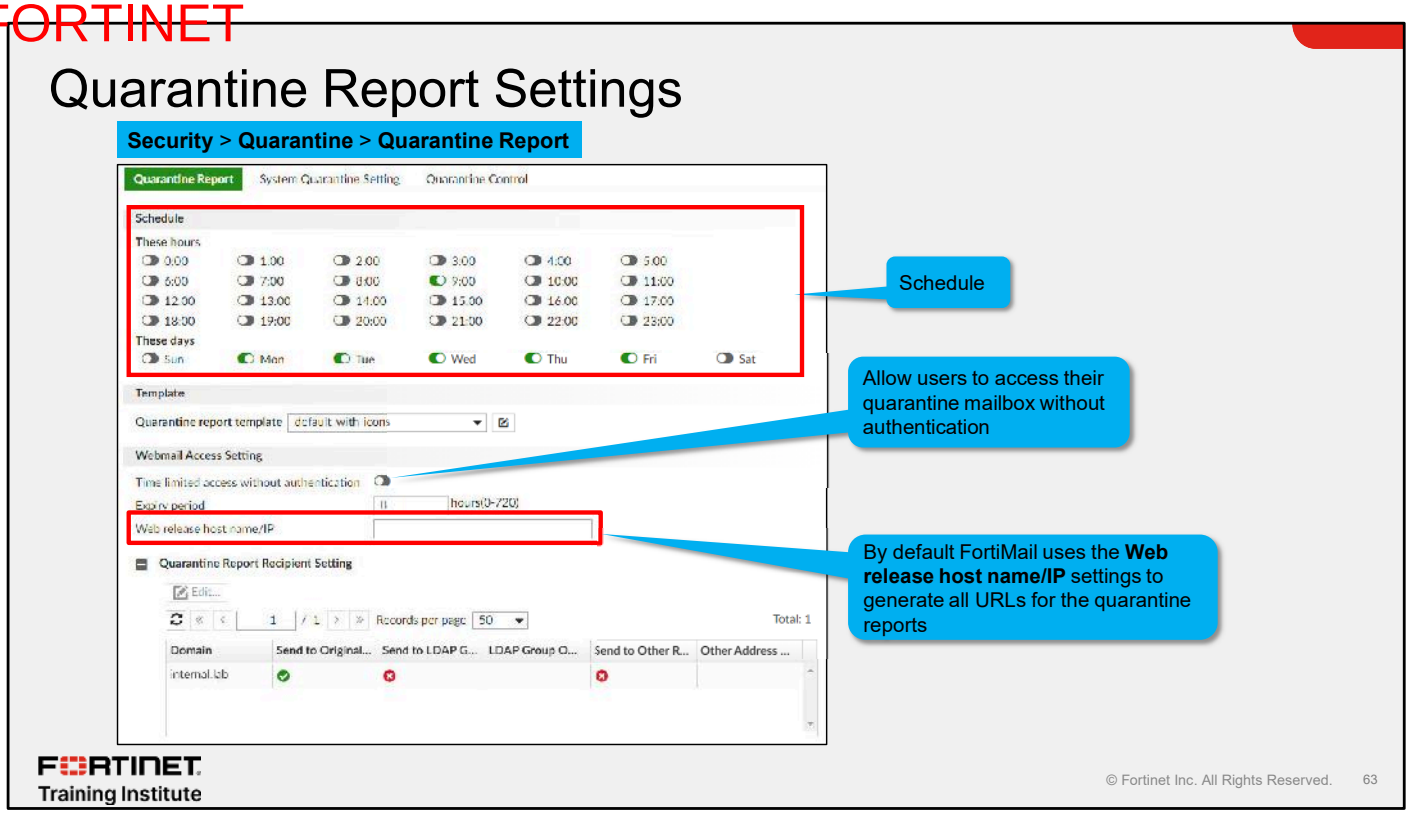
Users can access their personal quarantine through the web.

The quarantine mailbox for FortiMail has additional folders such as **Drafts**, **Sent Items**, **Trash**, and **Encrypted Email**, in addition to the **Bulk** folder.

In addition to personal quarantine access, in server mode, FortiMail webmail also provides access to the inbox, address book, and other features.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **Quarantine Report** tab lets you configure various system-wide aspects of the quarantine report, including scheduling when FortiMail sends reports.

Configuring an alternate host name for web release and delete links can be useful if the local domain name or management IP of FortiMail is not resolvable from everywhere that email users use their quarantine reports. In that case, you can override the web release link to use a globally resolvable host name or IP address.

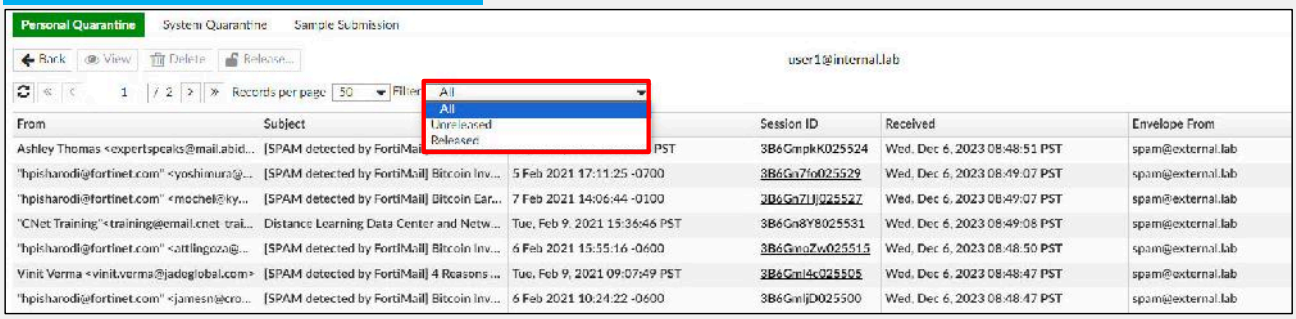
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Quarantine Mailbox Message Tracking

- Personal quarantine for released and unreleased records
  - Keep track of user behavior

Monitor > Quarantine > Personal Quarantine



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 64

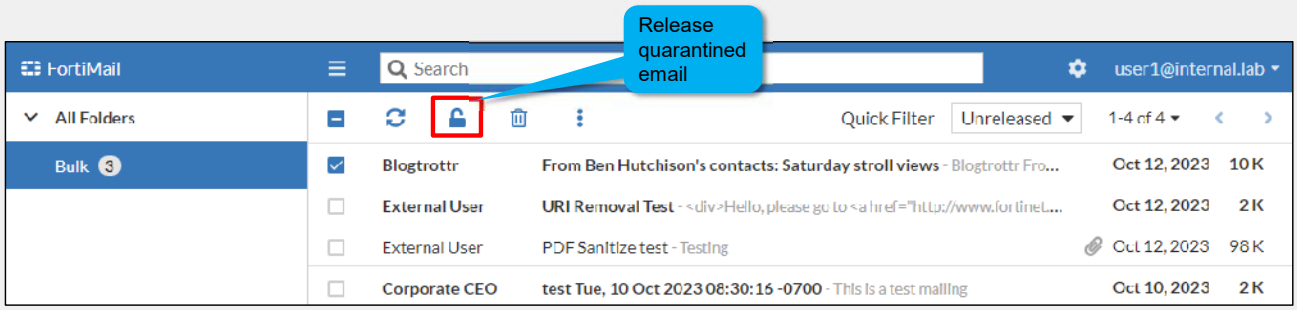
When you configure FortiMail to send spam email to a user's personal quarantine, the user can delete the quarantined email or release it to their inbox. The administrator GUI can display the messages contained in the user's quarantine and distinguish between released and unreleased messages. When users release email messages from their personal quarantine, the messages are tagged as **Released**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Quarantine Webmail

- Users can release quarantined messages through webmail



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 65

By logging in to the webmail GUI, users can review email message details and release any email messages that are false positives. The email message will then be released from quarantine and delivered to the user's inbox.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which user mailbox folder stores quarantine emails?
   - ✓ A. Bulk
   - B. Encrypted

2. How can a user access their personal quarantine mailbox?
   - A. POP3
   - ✓ B. Webmail

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 66

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- Antivirus
- Antispam Profiles
- Antispam Techniques
- Personal Quarantine Management

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 67

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Configure antivirus profiles and antivirus action profiles to implement local malware detection
- ✓ Identify the spam detection methodologies used by FortiMail
- ✓ Configure antispam and action profile features
- ✓ Use outbreak protection and behavior analysis to detect zero-day spam
- ✓ Use bounce address tag validation to combat backscatter attacks
- ✓ Identify the headers added by FortiMail antispam
- ✓ Establish the scanning order of execution
- ✓ Implement and manage quarantine mailboxes for users

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 68

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about antivirus and antispam techniques on FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FORTINET Training Institute

FORTINET CERTIFIED PROFESSIONAL Public Cloud Security

FortiMail Administrator

Content Inspection

FortiMail 7.4

Last Modified: 25 April 2024

In this lesson, you will learn how to configure the FortiMail antivirus and content inspection features.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- Content Inspection
- DLP
- Email Archiving

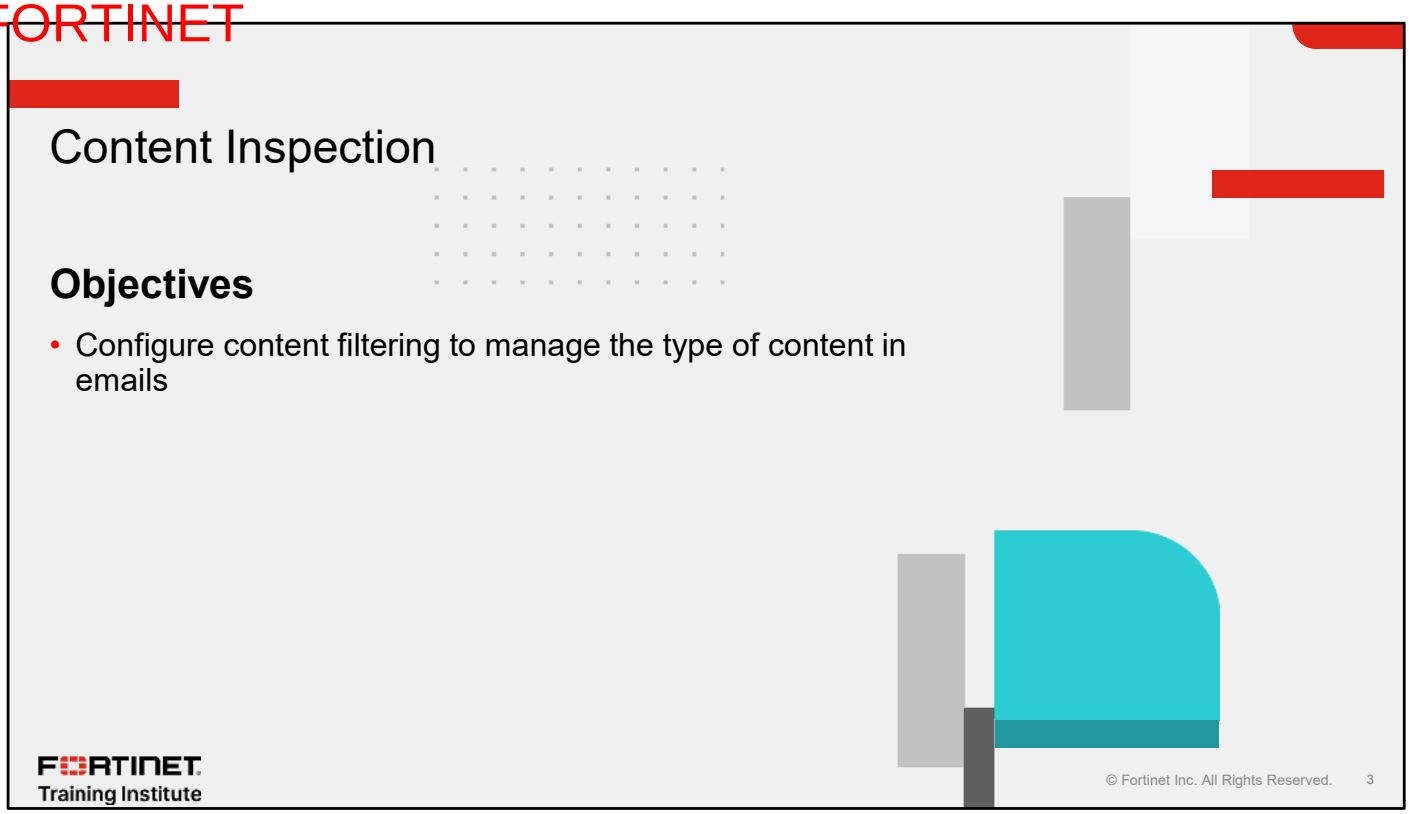
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 2

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in content inspection, you will be able to configure content filtering to manage the type of content in an email.

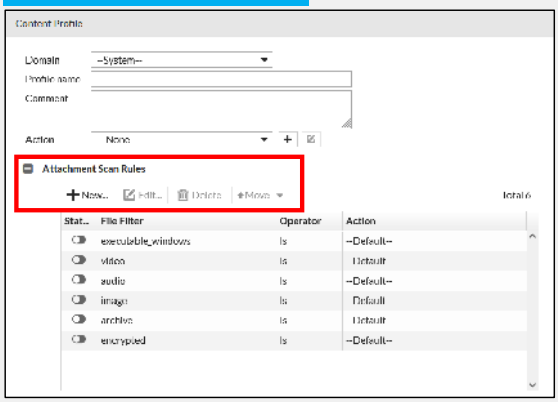
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Content Profiles

- **Attachment Scan Rules**
  - Use file filters to filter email that has specific attachments
  - Based on MIME types or file extensions

Profile > Content > Content



- **Content Monitor and Filtering**
  - Use dictionary profiles to monitor and filter very specific content
  - Based on regular or wildcard expressions

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

Content profiles support attachment detection based on MIME types or file extensions. Content profiles also support dictionary profiles to detect the content of words or phrases using regular or wildcard expressions.

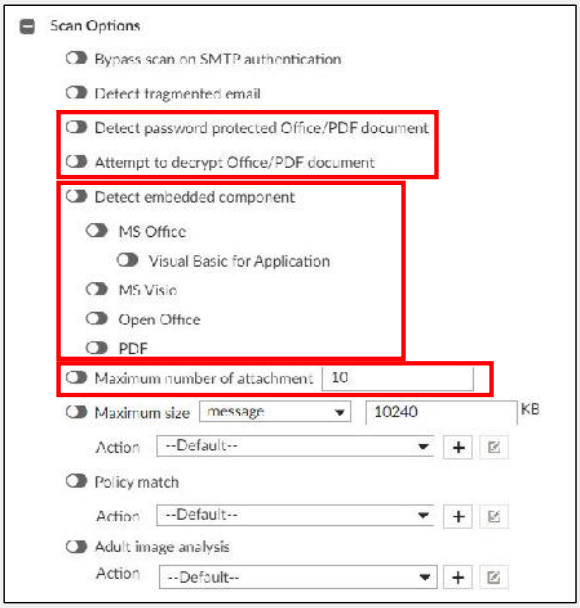
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Content Profiles (Contd)

- **Scan Options**
  - Allows the detection of various properties of email or attachments
    - Password-protected Microsoft Office files
    - Detect embedded components
    - Number of attachments

Profile > Content > Content



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

You can use **Scan Options** to detect various properties of email or attachments. You can configure a content profile to detect and act on password-protected Microsoft Office or PDF documents. If you enable the password decrypt feature, FortiMail tries to brute-force all password-protected Microsoft Office and PDF documents to attempt to scan the contents. You will learn more about this later in this lesson.

Another common use of the content profile is attachment limiting. You can configure the **Maximum number of attachment** setting to limit how many attachments per email FortiMail allows.

Sometimes, attached documents will have embedded content. For example, Microsoft Office documents can have embedded visual basic macros which can be exploited by remote attackers if the user mistakenly enables the macro after opening the document. If you enable the **Detect embedded component** setting, FortiMail can detect and act on such documents.

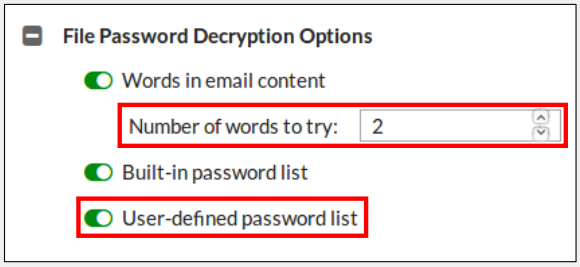
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

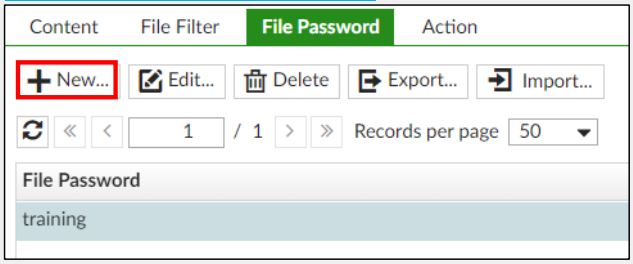
Password Decryption

- **File Password Decryption Options**
  - Look for words in email for passwords
  - Use a built-in password list
  - Create a password list
- **File Password**
  - Decrypt PDF documents and archived files and attachments
  - Specify the passwords to use for decrypting

Profile > Content > Content



Profile > Content > File Password



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

If you want to decrypt and scan password-protected PDFs and archive attachments, you can specify which kind of passwords you want to use to decrypt the files.

When you enable **Words in email content**, FortiMail searches the email message body for keywords to use as passwords to attempt to decrypt password-protected files.

You can enable **Built-in password list** to use the predefined passwords on FortiMail. The built-in password list is hidden and contains more than 1000 popular passwords.

You can also create your own list of passwords, as this slide shows. To use your own list of passwords for decryption, enable **User-defined password list** in the file password decryption settings.

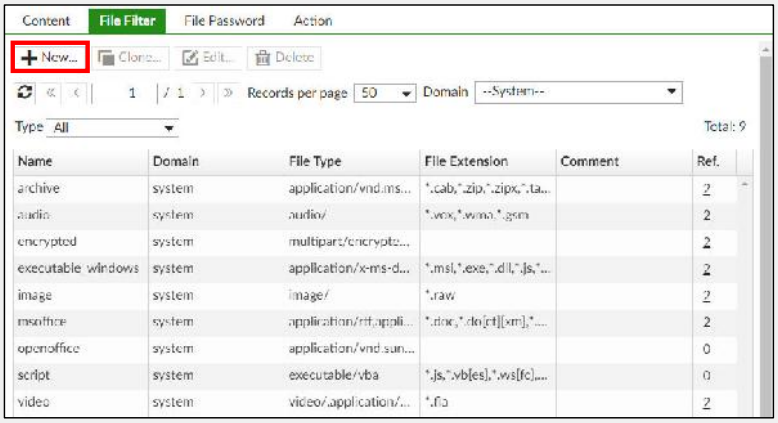
Vouchers & Dumps are Available | WhatsApp +201224560923

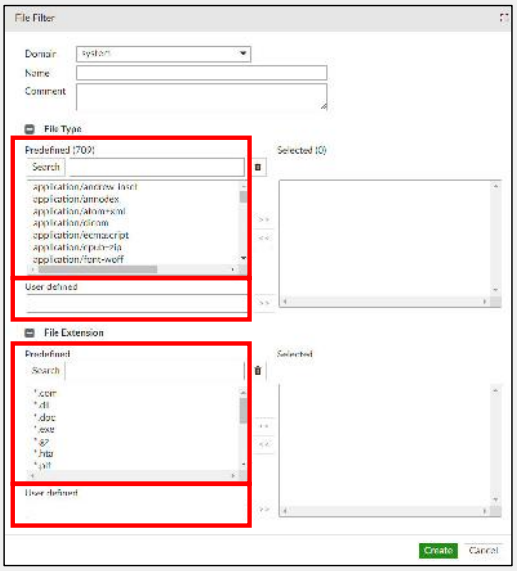
DO NOT REPRINT Brave-dumps.com
© FORTINET

File Filters

- Predefined MIME type and file extension definitions
- Used by both content and DLP profiles
- Define new filters to fit your specific needs

Profile > Content > File Filter





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

You can use file filters to match email attachments based on the file extension or type. The predefined **File Type** definitions can detect files based on their MIME header. This allows FortiMail to detect mismatched MIME/extension pairs such as an executable file masked with a .txt extension.

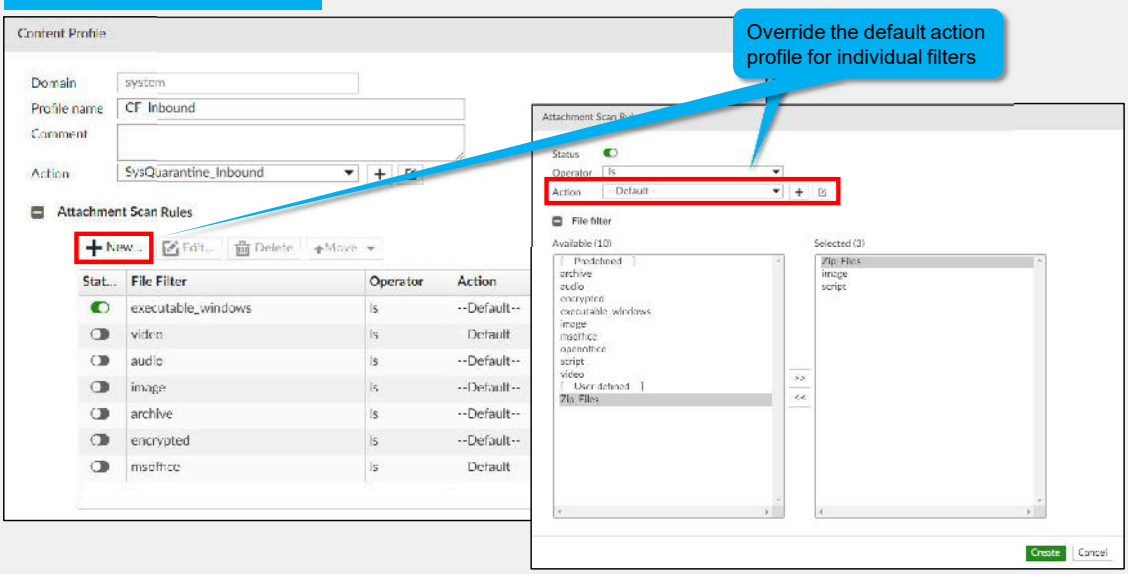
If the predefined set of file filters doesn't include the file type you need, you can add entries on the **File Filter** tab and specify MIME types, file extensions, or both.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Attachment Scan Rules

Profile > Content > Content



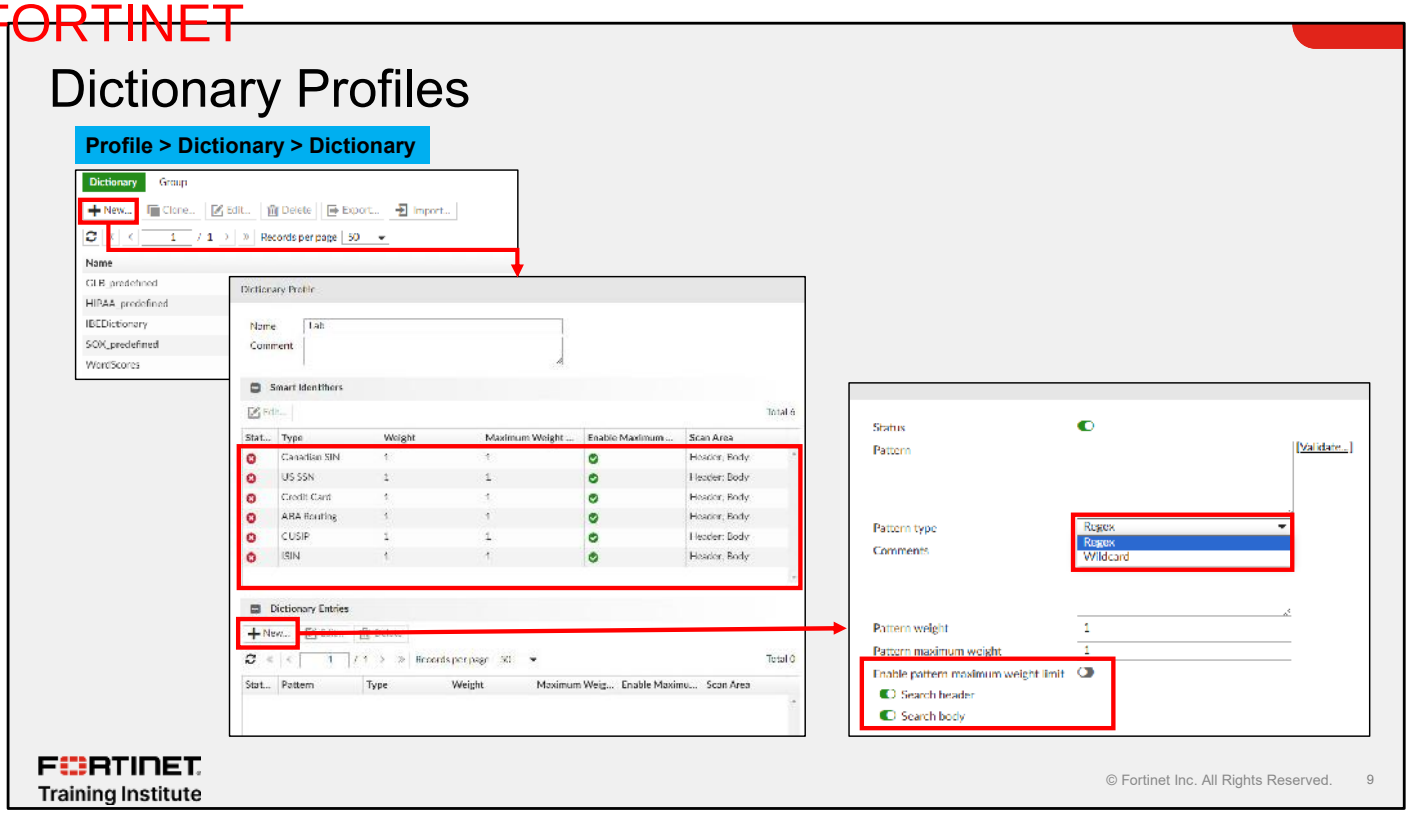
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

You can add file filters to the **Attachment Scan Rules** content profile, and then select a default action profile. You can also override the default action profile for each file filter individually if, for example, you want to always block email with suspicious .exe file attachments but only quarantine email with suspicious .txt file attachments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

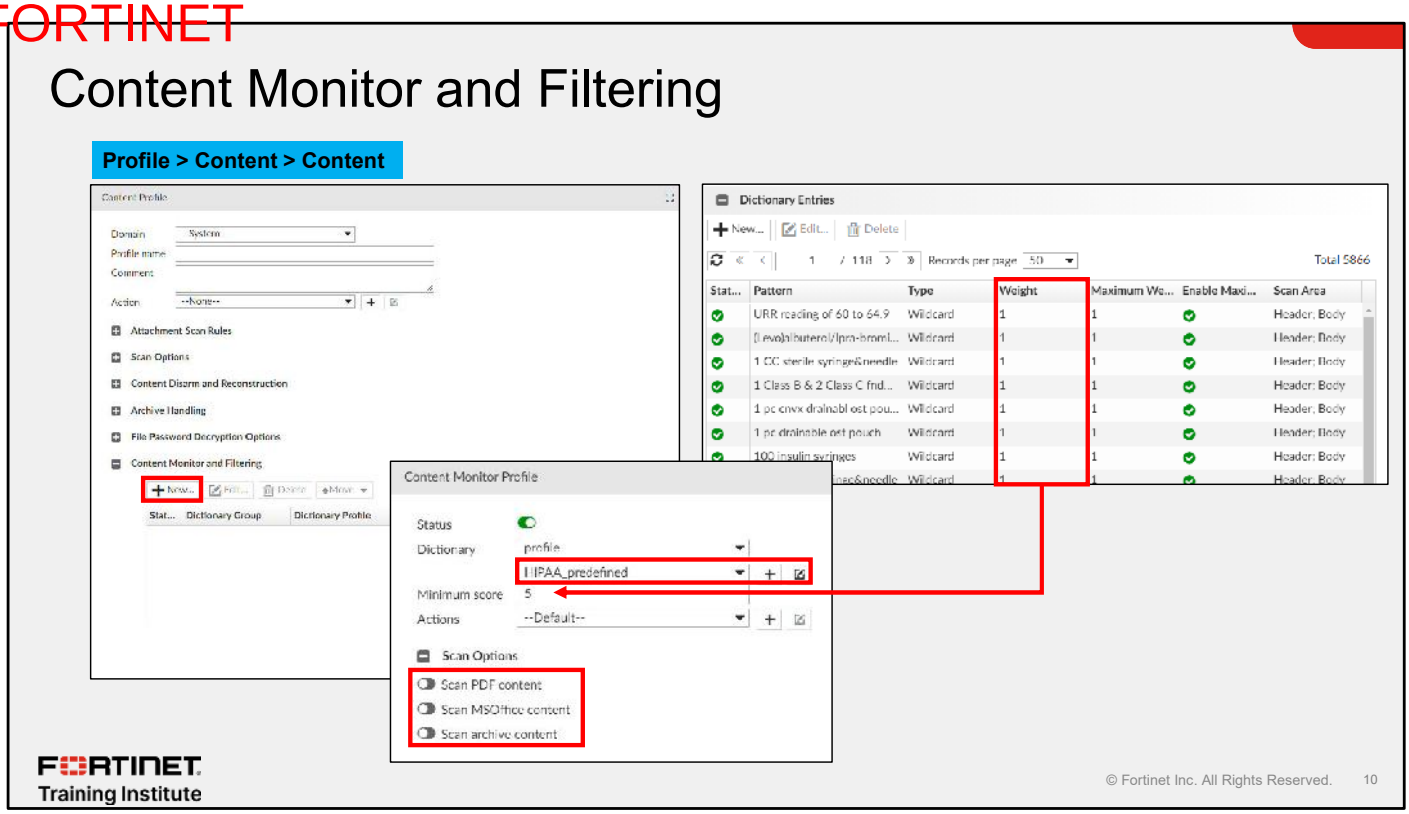


A dictionary profile is a list of words or phrases defined using either regular or wildcard expressions. FortiMail has three predefined dictionaries for HIPAA, SOX, and GLB. You can also add new dictionary profiles to use the predefined **Smart Identifiers**, or user-defined **Dictionary Entries**.

Dictionary profiles allow you to inspect email content on a deeper level. You can search for words or phrases in the email header, body, and attachments. Dictionary matching, while granular, is also very resource intensive.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can add dictionary profiles to content profiles in the **Content Monitor and Filtering** section. You can also enable different **Scan Options** to apply the dictionary lookups to PDF, Microsoft Office, and archive content.

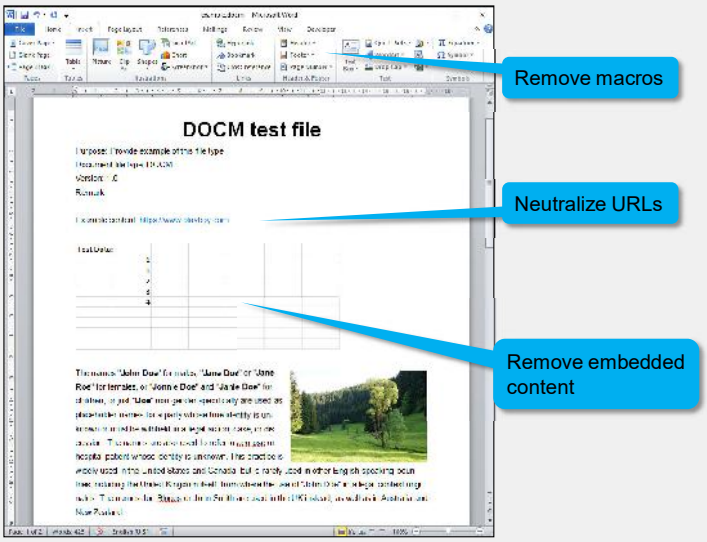
When you create dictionary profiles, you can associate each pattern entry with a score. For each **Content Monitor and Filtering** entry, FortiMail runs the defined action only if the total score meets or exceeds the minimum score value. A minimum score value of 1 causes FortiMail to run the action if it finds *any* of the listed dictionary words or phrases in the email.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Content Disarm and Reconstruction (CDR)

- Removes exploitable content and replaces it with content that is known to be safe
- Disarms Microsoft Office and PDF attachments from hazardous macros, active scripts, and other active contents



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

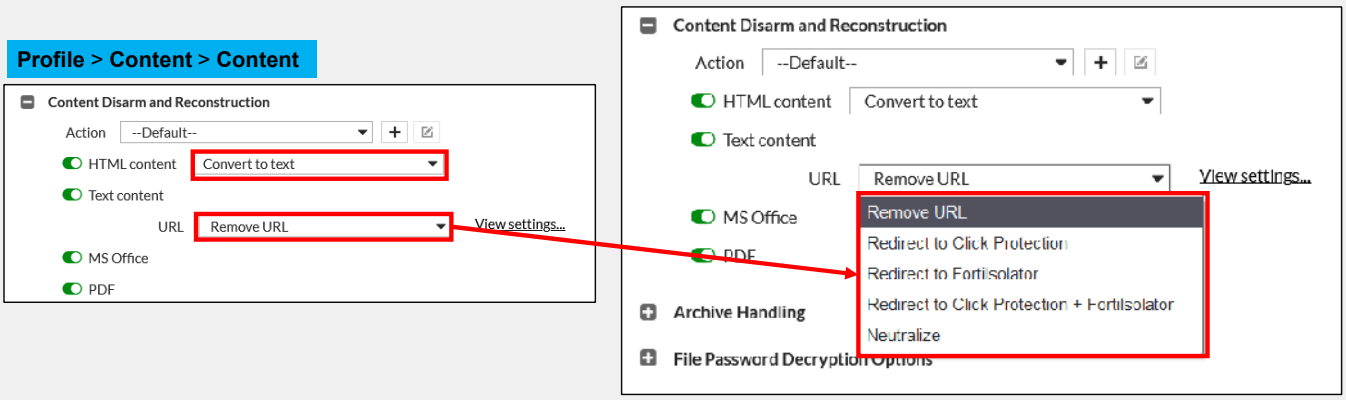
HTML content in the email body and attachments might contain potentially hazardous tags and attributes (such as hyperlinks and scripts). Microsoft Office and PDF attachments might contain potentially hazardous macros, active scripts, and other active content. FortiMail can use the content disarm and reconstruction (CDR) feature to remove or neutralize the potentially hazardous content and reconstruct the email message and attachment files.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Content Disarm and Reconstruction (Contd)

- Neutralizes HTML content in an email by converting it to text, removing hyperlinks, and producing new HTML content without tags and attributes
- Replaces URLs with text and can remove malicious URLs completely



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

FortiMail provides the capability to remove or neutralize the potentially hazardous contents and reconstruct the email messages and attachment files. You can also remove all HTML URLs in the email body, or apply click protection and FortiIsolator inspection.

For text content, such as URLs in the email body, FortiMail can use CDR to remove all URLs, or apply click protection and FortiIsolator inspection.

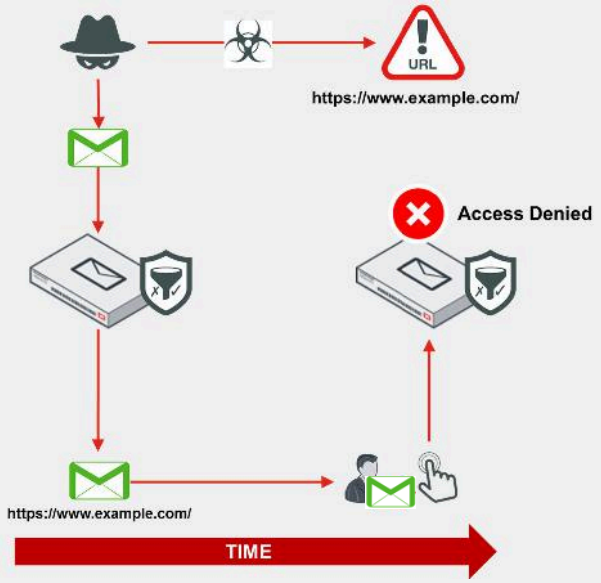
FortiMail can also apply CDR to Microsoft Office and PDF files.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Content Disarm and Reconstruction—URL Click Protection

- Rewrite URLs to point at FortiMail
- FortiMail rescans the URL when users click links to detect status changes since the first rating



FORTINET Training Institute

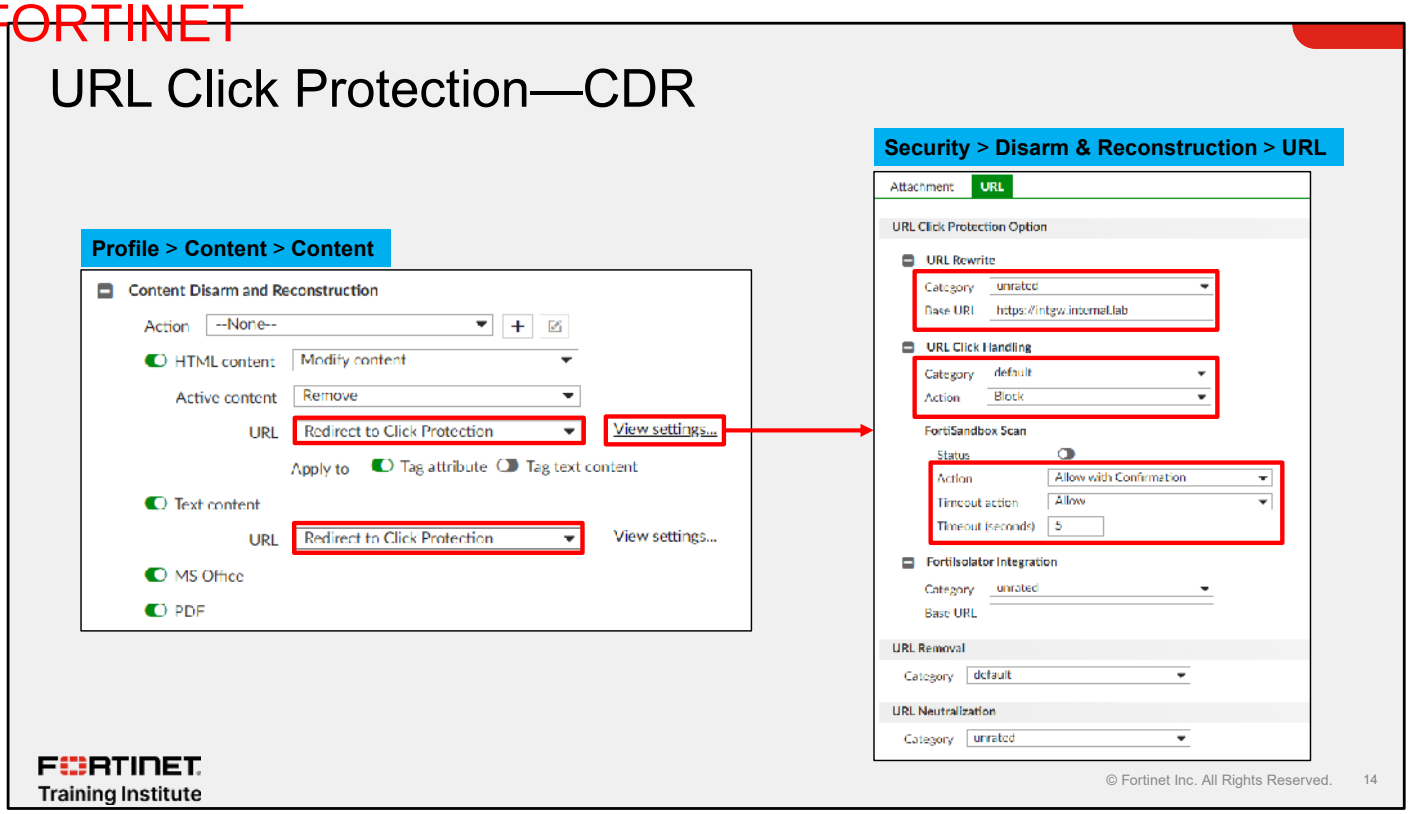
© Fortinet Inc. All Rights Reserved. 13

If you're using URL click protection, FortiMail rewrites any URLs in the email body that were categorized as non-malicious or unrated to point to itself. So, when the user clicks on the email URL at a later time, the URL request goes through FortiMail for a second rating query. If the URL rating changes from a non-malicious rating to a malicious rating, FortiMail is then able to block the request.

The diagram on this slide shows an example scenario in which URL click protection is useful. In this scenario, a spammer sends an email containing the URL `https:/www.example.com`. When FortiMail initially processes the email, the URL rating query might return with either a non-malicious rating or an unrated rating. FortiMail rewrites the URL in the email body to point to FortiMail, and then delivers it to the end user. Later, the user clicks the URL, and because that URL has been rewritten, the request goes through FortiMail. At this point, FortiMail requires a rating of the URL and, based on a malicious rating reply, blocks the request.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



URL click protection is available for HTML and text content. To protect users from harmful or spam URLs, such as phishing or advertising websites, FortiMail uses the FortiGuard URL filter service and FortiSandbox to scan URLs after users click them. Depending on the inspection results from the FortiGuard and FortiSandbox scans, you can decide to allow users to access URLs or block them.

If you select the **Allow with Confirmation** action, FortiMail allows access to the URL with a warning. Selecting **Block** means that FortiMail blocks access, and selecting **Submit only** means that FortiMail allows access while it sends the URLs for scanning.

When FortiMail sends URLs to FortiSandbox for scanning, it might take a while for FortiSandbox to return the results. In the **Timeout (seconds)** field, specify how long you want to wait for results *before* you select **Block**, **Allow**, or **Allow with Confirmation** in the **Timeout action** field.

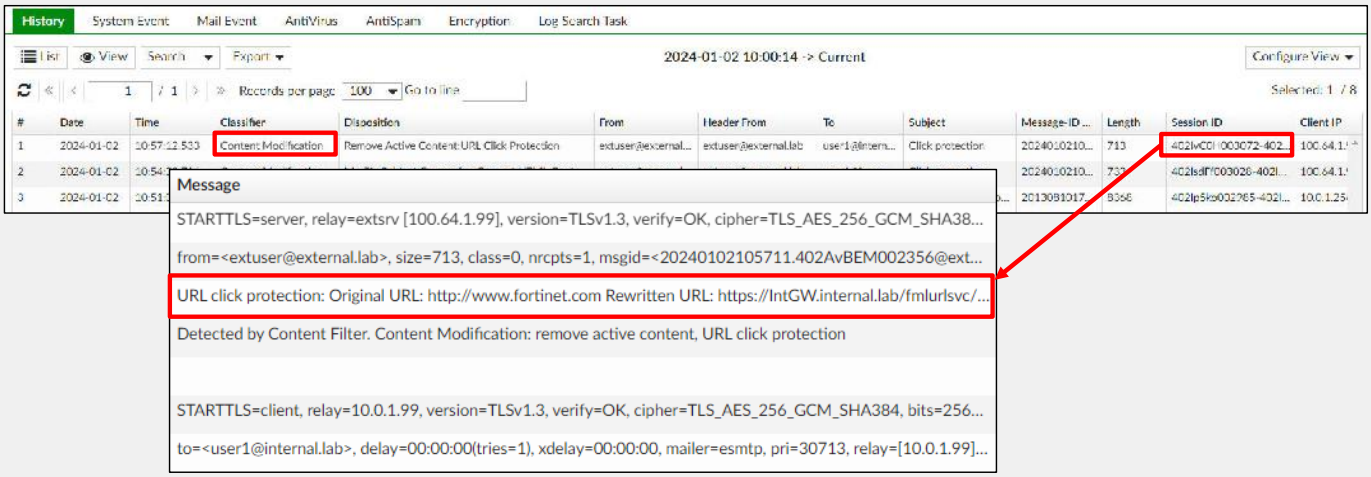
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Click Protection—Log Original URLs

- Original URL and rewritten URL are logged

Monitor > Log > History



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

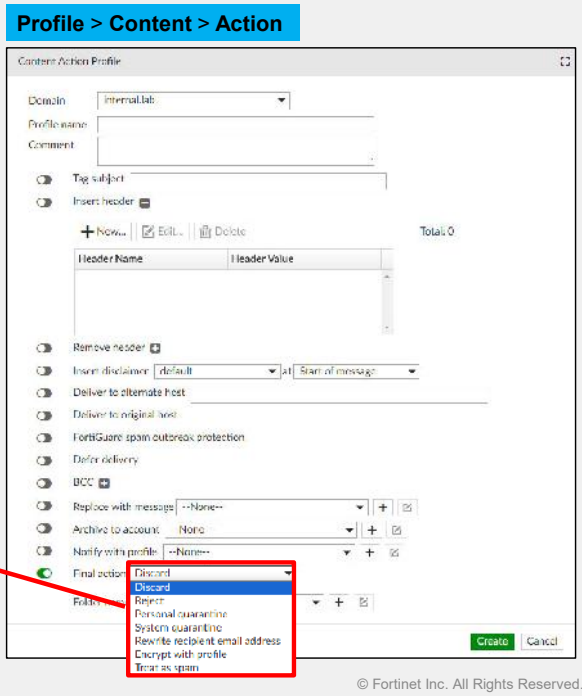
When you enable **Redirect to Click Protection**, both the original and rewritten URLs are logged.

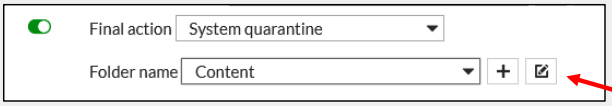
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Content Action Profile

- **Deliver to alternate host**: Routes email to a specific SMTP server or relay
- **Deliver to original host**: Routes email to the original SMTP server or relay
- **Notify with profile**: Sends a notification email to the sender, recipient, or other contacts
- **Replace with message**: Replaces the email content with another message





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

You can use the **Personal quarantine** option only for incoming content action profiles. The rest of the options are identical. The most used actions are **Reject** and **System quarantine**. When you select a quarantine action, you can specify the folder to save the email in. It is recommended that you use the **Content** folder for email quarantined from a content profile.

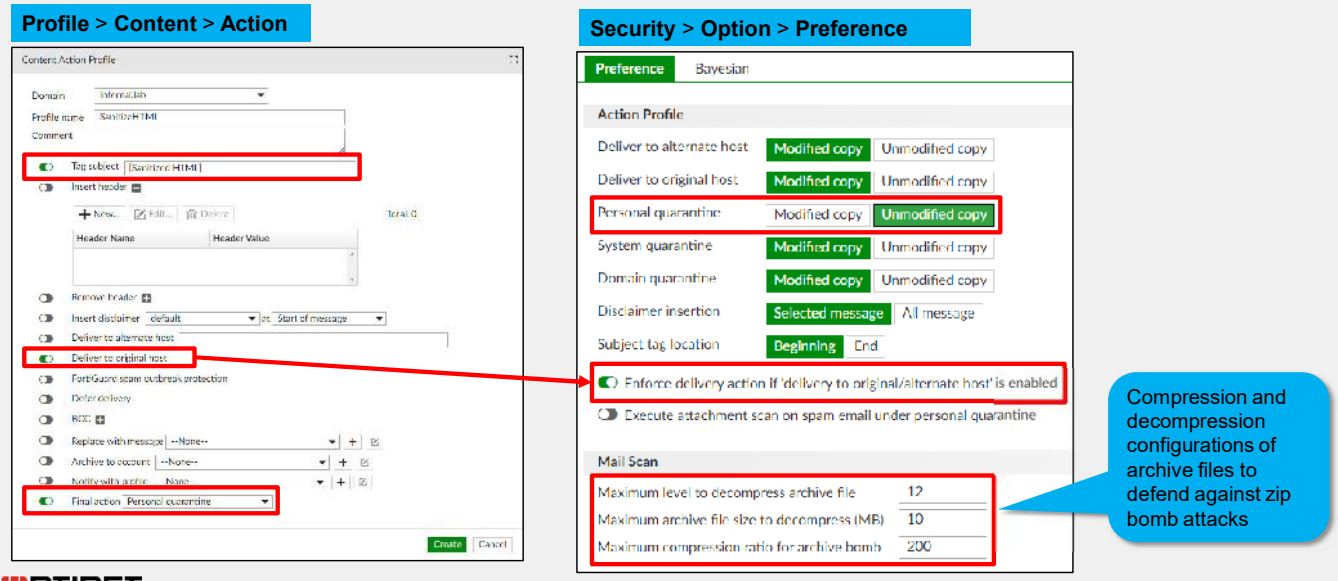
Another common action is **Encrypt with profile**. You can use a dictionary match of a specific word or phrase to trigger identity-based encryption. You will learn more about identity-based encryption in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Action Profile Preferences

- Control how certain action profile settings are applied



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

You can configure how certain action profile settings are applied. The **Action Profile Preference** settings change how the **Deliver to alternate host**, **Deliver to original host**, **System quarantine**, and **Personal quarantine** actions handle content in emails.

If you select **Modified copy**, FortiMail delivers or quarantines the email *after* modifying the content. If you select **Unmodified copy**, FortiMail delivers or quarantines the email *without* modifying the content.

This is useful for the CDR feature. You can deliver a modified copy of the email content to the original host, and at the same time, send an unmodified copy of the email to the system quarantine for further examination.

Mail scan settings can be used to defend against malicious archive files (often referred to as a zip bombs), that are used to overwhelm system resources when they are decompressed.

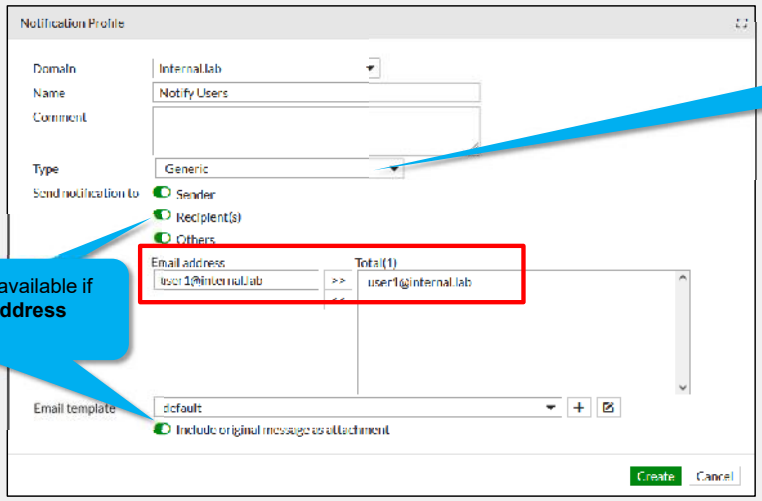
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Notification Profile

- Inform users when FortiMail acts against emails
- Attach the original email to the notification email

Profile > Notification > Notification



Three types: **Generic**, **Sender address rate control**, and **Attachment filtering**

These options are unavailable if the **Type** is **Sender Address Rate Control**

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

When FortiMail acts against emails, you might want to inform email senders, recipients, or other users what happened to the email. To do this, you must create notification profiles and use them in antispam, antivirus, or content action profiles.

You can use a generic notification profile for antispam, antivirus, and content profiles to notify the sender, recipient, or other email accounts. If you want to configure a sender address rate control notification in the domain settings, then you must set the type to **Sender Address Rate Control** in the notification profile. In this case, you must notify only the senders, not the recipients. You do not need to include the original message as an attachment. Therefore, these two options are unavailable.

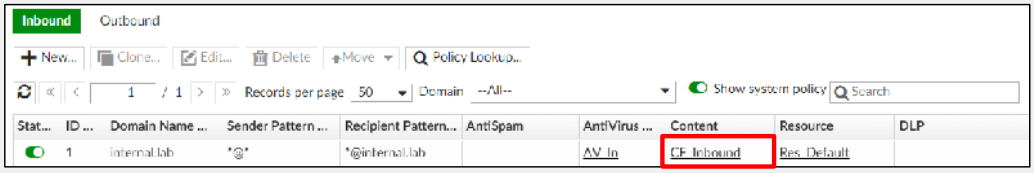
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

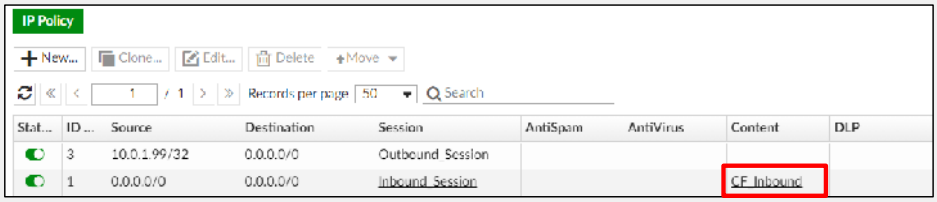
Applying Content Inspection

- Enable content inspection using either IP-based or recipient-based policies
- If you enable **Take precedence over recipient based policy match** in an IP policy, then content inspection in the recipient policy is ignored

Policy > Recipient Policy > Inbound



Policy > IP Policy > IP Policy



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

Like other inspection profiles, you can apply content profiles to email flows by enabling them in IP-based or recipient-based policies. As a rule, recipient-based policies override IP-based policies. This means that if an email matches both a recipient-based policy and an IP-based policy, FortiMail applies the settings in the recipient-based policy and ignores the IP-based policy, unless you enable **Take precedence over recipient based policy match** in the IP policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Content Filter Logs

Monitor > Log > History

History | System Event | Mail Event | AntiVirus | AntiSpam | Encryption

List | View | Search | Export

2021-03-08 15:48:53 - > Current

Records per page: 100 Go to line:

#	Date	Time	Classifier	Disposition	From	Header From ...	To	Subject	Message-ID
1	2021-03-08	17:42:35.491	Attachment Filter	System Quarantine	extuser@exte...	extuser@exte...	user1@intern...		
2	2021-03-08	17:36:07.679	Content Monitor and Filter	System Quarantine	extuser@exte...	extuser@exte...	user1@intern...		

Log Details: 0300003850

Column	Content
Date	2021-03-08
Time	17:42:35.488
Message	File name: cap2.jpg, detected by Content Filter, filetype image/jpeg, attachment scan rule: image
Session ID	1291gZrO003849-1291gZrQ003849
From	extuser@external.lab
To	user1@internal.lab
Subject	Attached is image
Client IP	100.64.1.99
Client Name	extsrv
Destination IP	10.0.1.11
Level	information
Log ID	0300003850
Type	spam

Triggered by an attachment scan rule

Log Details: 0300003794

Column	Content
Date	2021-03-08
Time	17:36:07.678
Message	Identified by Content Profile ;Dictionary:WordScores Score: 3(fortimail)
Session ID	1291a76Y003793-1291a76a003793
From	extuser@external.lab
To	user1@internal.lab
Subject	Dictionary test
Client IP	100.64.1.99
Client Name	extsrv
Destination IP	10.0.1.11
Level	information
Log ID	0300003794
Type	spam

Triggered by a dictionary match

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

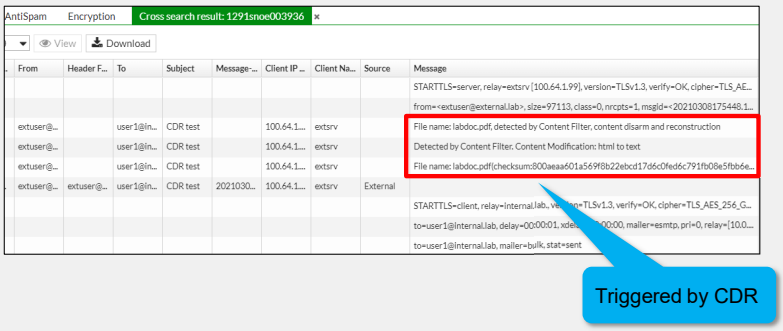
The logs that the content profile generates show whether the log was triggered by an attachment scan rule or dictionary match. The cross-search results include details such as filename, attachment filter rule, dictionary profile name, and the dictionary word or phrase.

Vouchers & Dumps are Available | WhatsApp +201224560923

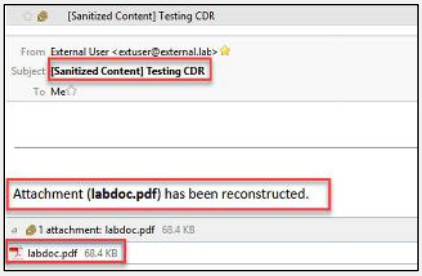
DO NOT REPRINT Brave-dumps.com
© FORTINET

Content Filter Logs—CDR

Monitor > Log > History



Thunderbird



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

Content filter logs are generated by the CDR, which detects suspicious HTML content in an attachment, and reconstructs the file by removing offending content. The end user receives an email that is safe.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. The content monitor and filtering feature performs which function?
   - ✓ A. Uses dictionary profiles to monitor and filter very specific content based on regular or wildcard expressions
   - B. Uses file filters to filter email that has specific attachments based on MIME types or file extensions

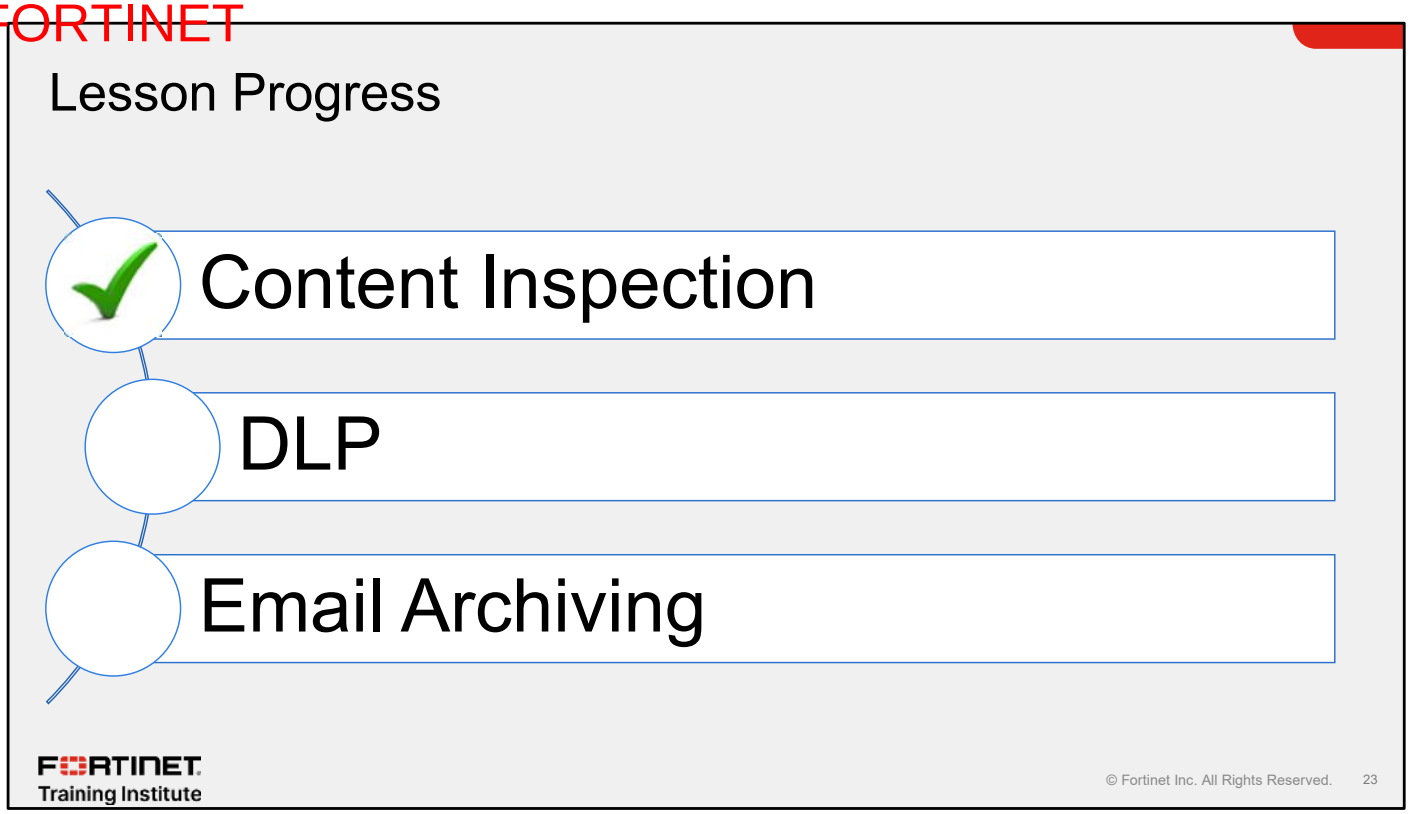
2. URL click protection is available for which type of content?
   - ✓ A. PDF
   - B. HTML

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

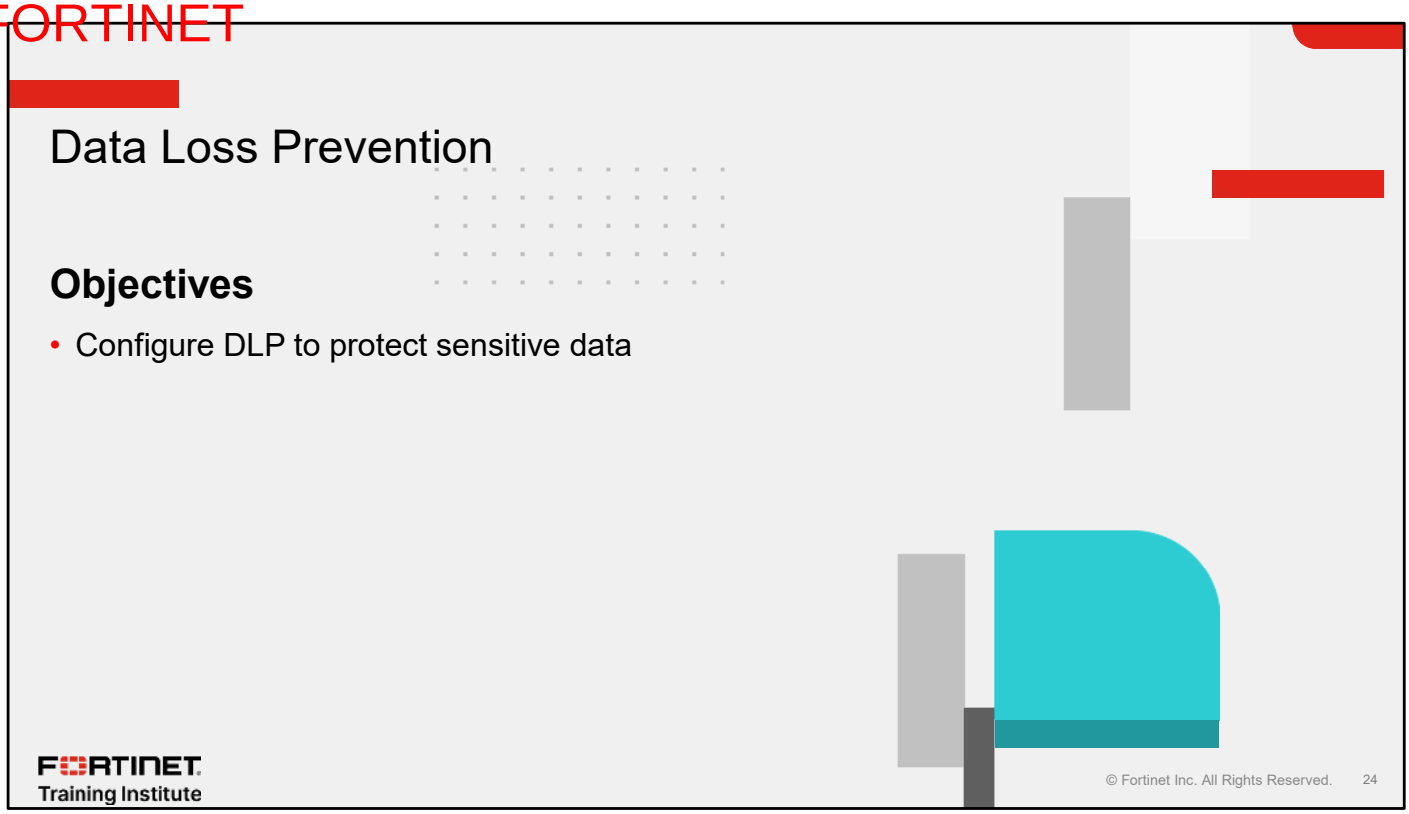


Good job! You now understand content inspection and different content inspection methodologies on FortiMail.

Now, you will learn about data loss prevention (DLP).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in data loss prevention (DLP), you will be able to use the FortiMail DLP feature to control, with a high level of granularity, the type of data that is allowed to enter or leave your organization by email.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

DLP

- Create DLP rules based on document fingerprints, file filters, prebuilt data templates, or email header and body patterns
- A single DLP profile can contain multiple rules
- Feature disabled in entry-level FortiMail models because of performance considerations
- You can control dictionary and DLP scan rule aggressiveness using the following CLI command:

```
config mailsetting mail-scan-options
    set content-scan-level <high| medium| low>
end
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

You can define custom patterns, or use a prebuilt data template or file filters to build DLP rules. A single DLP profile can contain multiple rules. The DLP feature is disabled on entry-level models.

You can control dictionary and DLP scan rule aggressiveness. The higher the level, the more aggressive the scan, and therefore more resources are required. The default setting is `medium`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

DLP Configuration Workflow

1. Define sensitive data
   - Predefined patterns: file filters and data templates
   - User-defined patterns: document fingerprints and string or regular expression-based patterns
2. Define the DLP scan rules
   - Specify what to scan for in what part of the email
3. Define the DLP profile
   - Pair scan rules with action profiles
4. Apply the DLP profile to an IP or recipient policy

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

When you configure DLP, you must define sensitive data first. You can define sensitive data using predefined patterns, such as file filters and data templates; user-defined patterns, such as document fingerprints and strings; or regular expression-based patterns. Next, you must configure DLP scan rules that define where to look for sensitive data in an email, for example, in the email header or body. Then, you must add the DLP scan rules to DLP profiles to define what action to take. After the DLP profile is complete, you can apply it to an IP-based or recipient-based policy.

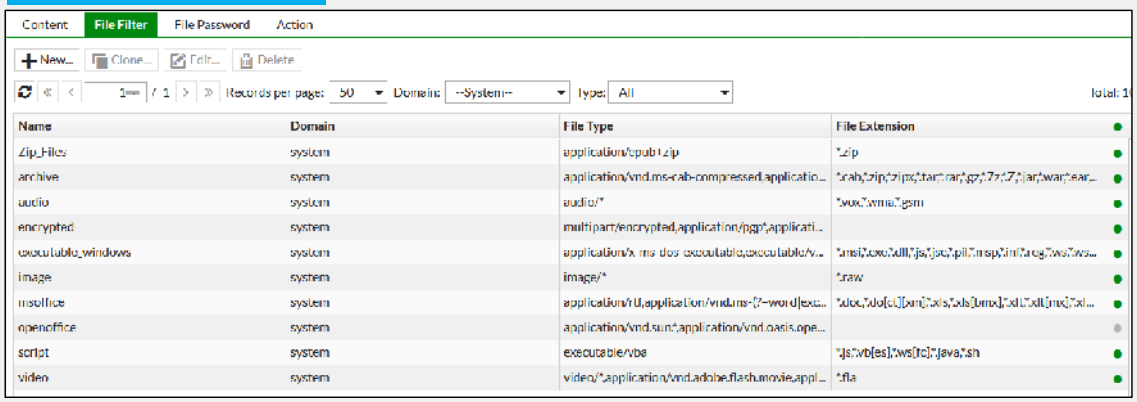
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Predefined Patterns—File Filters

- Predefined file type and file extension definitions
- Customize new filters to your needs
- Used by both DLP and content filter profiles

Profile > Content > File Filter



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

You can use file filters to match email attachments based on the file extension or file type. FortiMail comes with nine predefined filters. You can also create new filters. File filters are used by the DLP and content filter features.

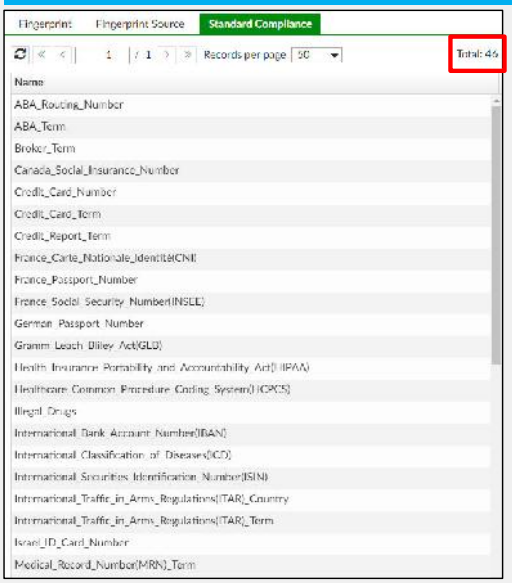
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Predefined Patterns—Data Templates

- To simplify configuration, FortiMail comes with a list of predefined data types, such as:
  - Credit card numbers
  - Social security numbers (SSNs)
  - Social insurance numbers (SINs)
- Match based on file contents
- 46 predefined templates

Data Loss Prevention > Sensitive Data > Standard Compliance



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

FortiMail comes with a list of predefined data types, such as credit cards, social security numbers, and social insurance numbers. You can use these data templates to define your sensitive data based on file content in DLP rules. Using these templates means that you don't have to perform extra configuration steps in attempting to define certain well known data types.

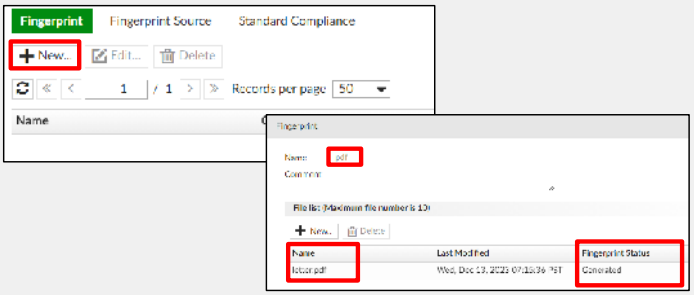
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

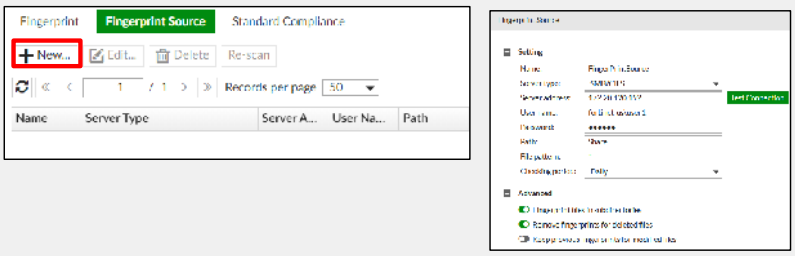
User-Defined Patterns—Document Fingerprints

- Fingerprinting is useful when FortiMail must protect specific document types
- FortiMail generates and stores a file checksum fingerprint and compares it with all future email attachments
- Two methods of creating fingerprints:
  - Upload files manually
  - Create a fingerprint source
- A new **Fingerprint Status** column is added when you upload files

Data Loss Prevention > Sensitive Data > Fingerprint



Data Loss Prevention > Sensitive Data > Fingerprint Source



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 29

Another technique you can use to detect sensitive data is fingerprinting. When you use fingerprinting, you must provide a file. FortiMail generates and stores a file checksum fingerprint. FortiMail then compares the fingerprint with all future email attachments to check for a match.

You can manually upload files to FortiMail to generate fingerprints. You can also create a Server Message Block (SMB) or Common Internet File System (CIFS) fingerprint source that FortiMail can use to generate fingerprints automatically from the contents of the shared folder.

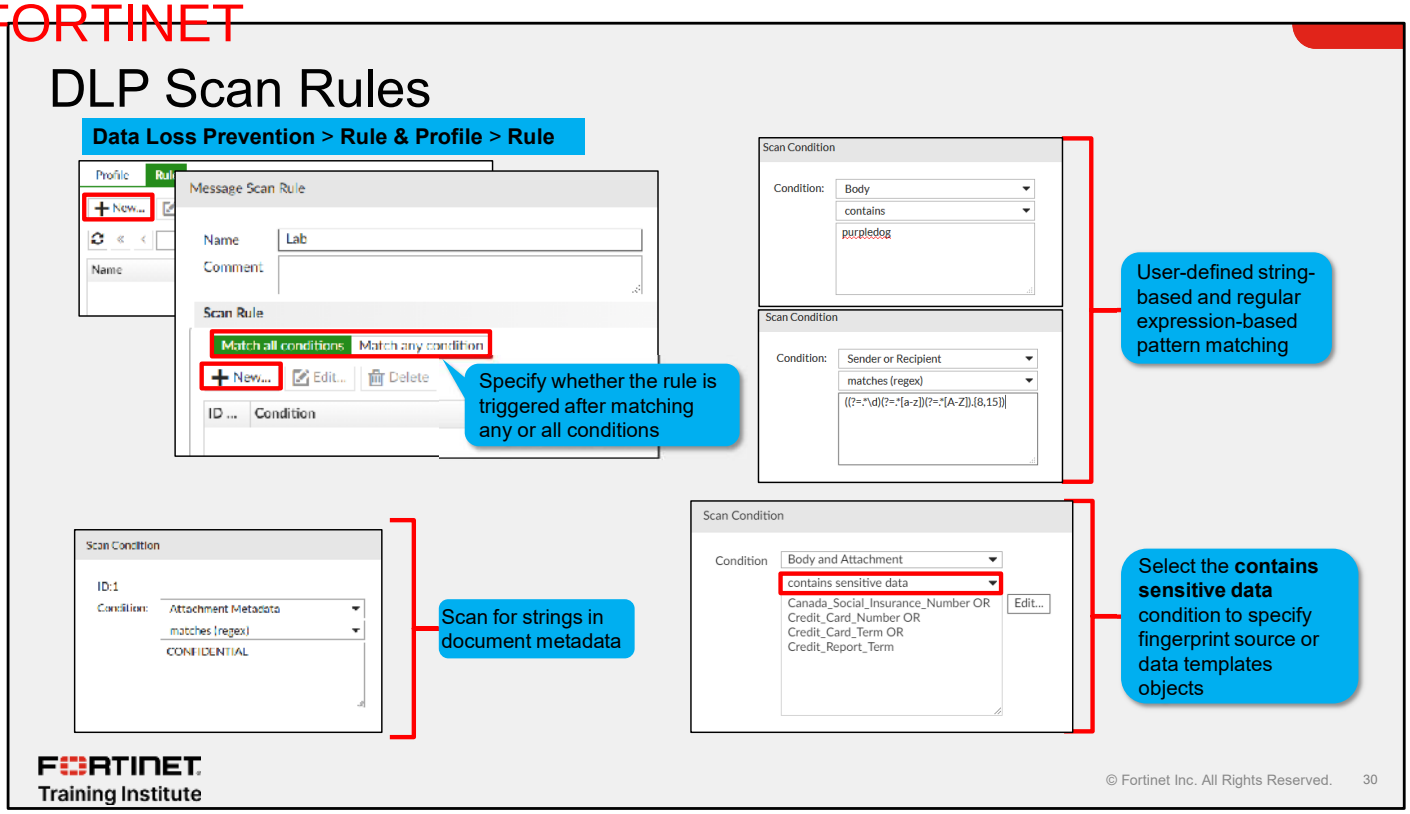
The manual method is sufficient when you have only a few documents to fingerprint. If you have a large list of documents that go through many version changes, you should use a fingerprint source.

In the **Fingerprint Status** column, one of the following statuses is displayed:

- **To be generated**, which is displayed when you have uploaded the file to the fingerprint list before clicking **Create**.
- **Being generated**, which is displayed when the fingerprint generating process is executing.
- **Generated**, which is displayed when the fingerprint has been generated.
- **Not generated**, which is displayed when no fingerprint has been generated for the file because there is not enough text or the fingerprint generation is in progress.
- **File type not supported**, which is generated when the file type is not supported to generate a fingerprint.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



A single DLP scan rule can have multiple conditions. You can specify whether the rule is triggered after matching any or all of the conditions. In the DLP scan rule, you can define string-based or regular expression-based patterns to match any part of the email. You can select **contains sensitive data** to apply the sensitive data definitions, such as fingerprint source, or data templates.

FortiMail currently supports metadata string matching for Microsoft Office, OpenOffice, PDF, TIFF, IGS, and TXT files.

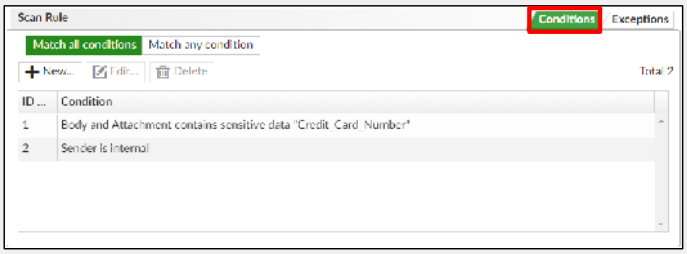
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

DLP Scan Rule Example

- This specific rule matches if:
  - The sender is internal (from a protected domain)
  - The body or attachment contain credit card numbers
- Exempt emails from the DLP scan rule if:
  - The email is sent from `sales@internal.lab`

Data Loss Prevention > Rule & Profile > Rule



Data Loss Prevention > Rule & Profile > Rule

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

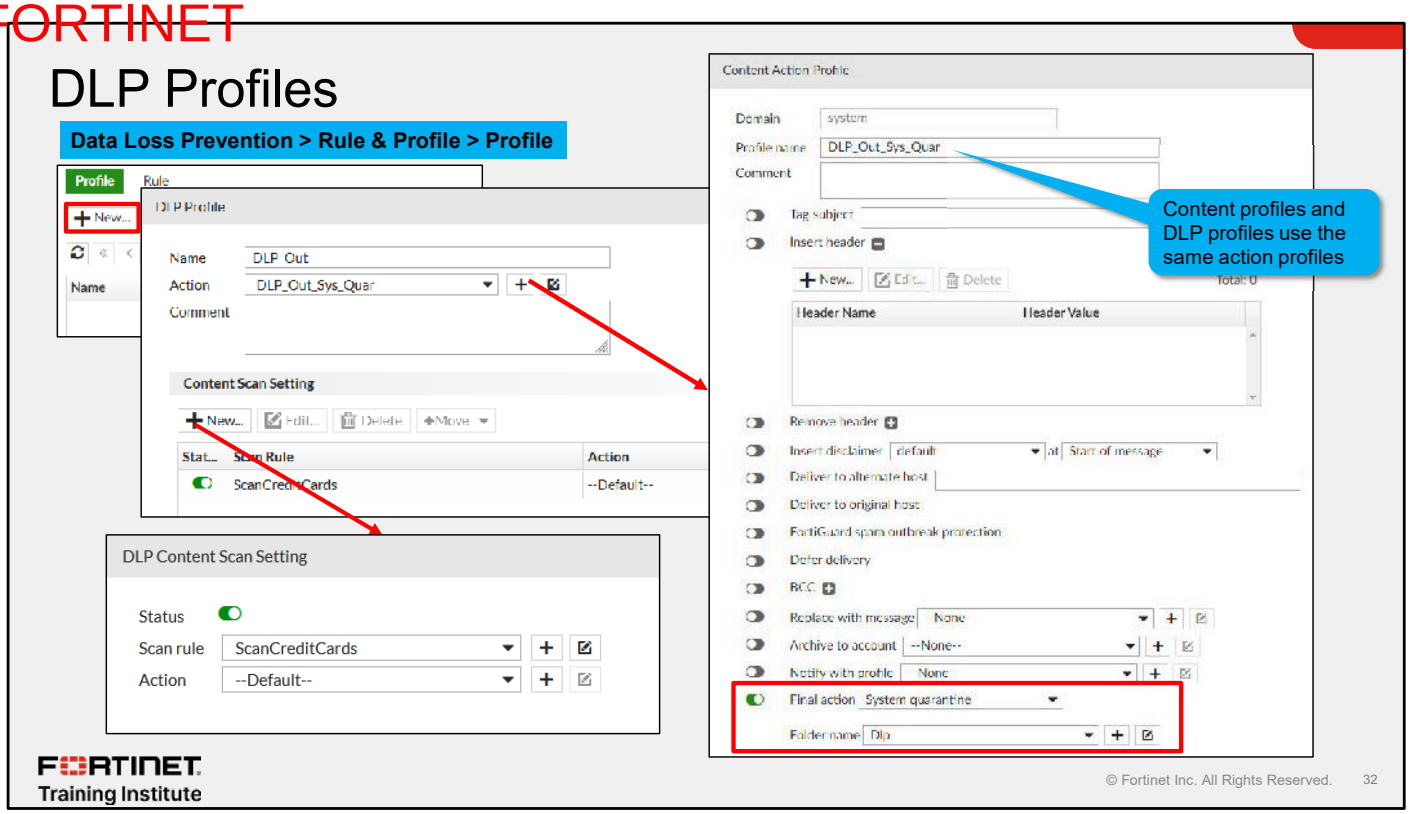
This slide shows an example DLP scan rule. The DLP rule matches if the following conditions are met:

- The sender is internal (from a protected domain)
- The body or attachment contain credit card numbers

You can use exceptions to exempt specific email from the DLP scan rule. In this example, FortiMail ignores the DLP rule for all email sent from `sales@internal.lab`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After you define the DLP scan rules, you can add them to DLP profiles. You can also modify the action profile to specify how to handle email that the DLP profile identifies. This example shows that the identified emails are sent to the system quarantine DLP folder.

DLP profiles use the same action profiles as content profiles. To configure an action profile for DLP, click **Profile** > **Content** > **Action**.

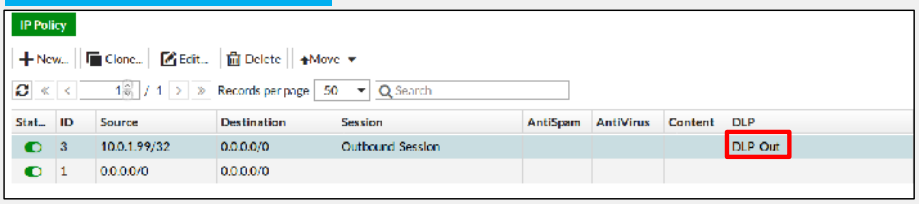
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

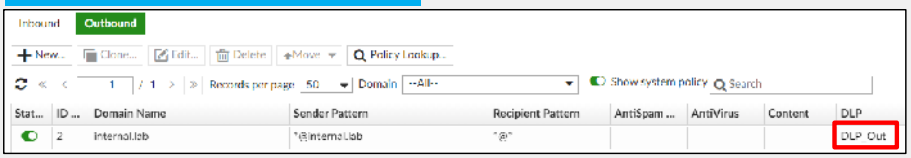
Applying DLP

- Because DLP policy is usually applied to outbound email, this example is applied to an outbound recipient-based policy
- If you enable **Take precedence over recipient based policy match** in the IP policy, then FortiMail ignores the DLP profile in the recipient policy and uses only the one defined in the IP policy

Policy > IP Policy > IP Policy



Policy > Recipient Policy > Outbound



FORTINET Training Institute

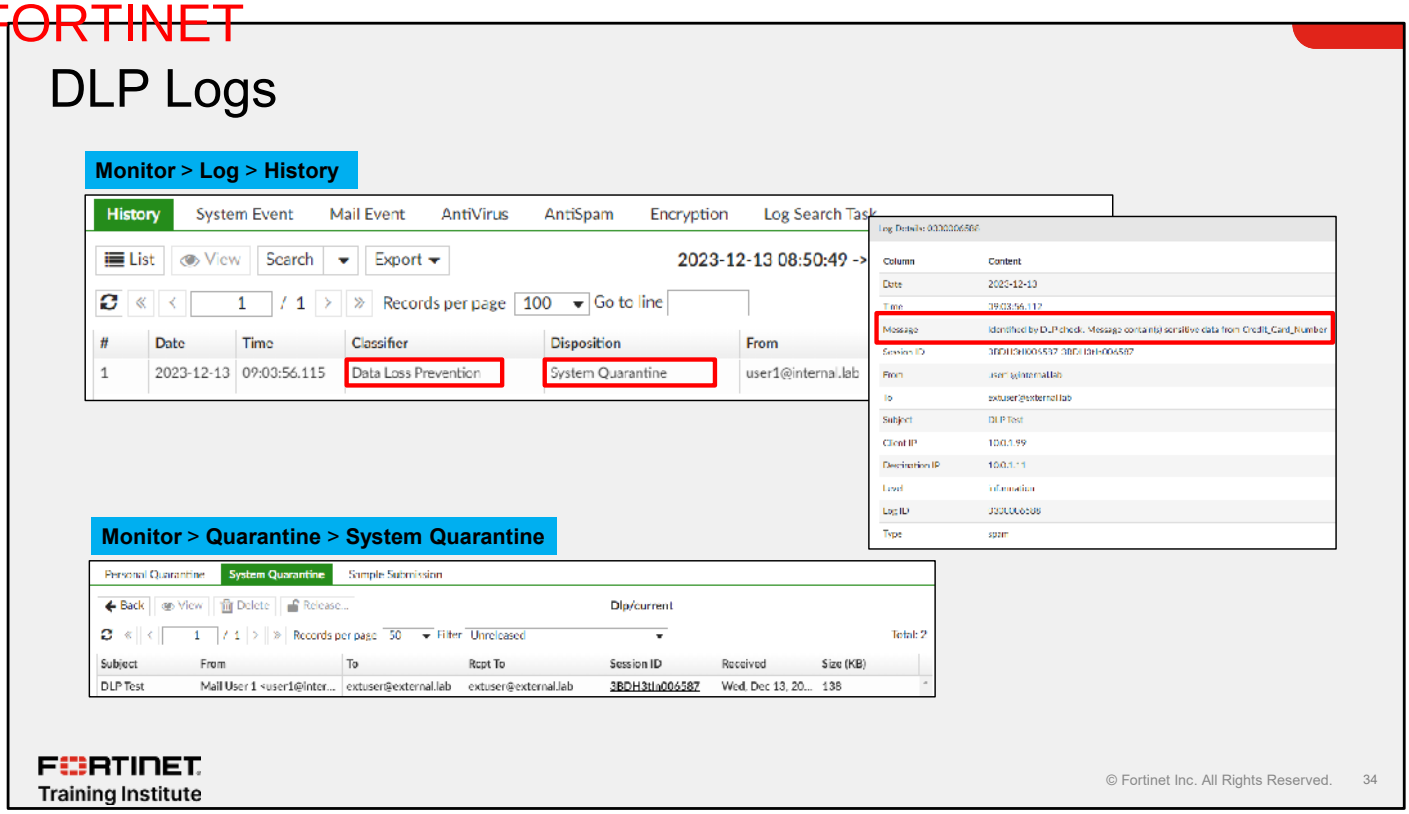
© Fortinet Inc. All Rights Reserved. 33

The DLP profile can be referenced by IP-based or recipient-based policies. Because this DLP profile is intended to inspect outbound emails, FortiMail applies it to an outbound recipient-based policy.

As a general rule, recipient-based policies override IP-based policies. This means that if an email matches both a recipient-based policy and an IP-based policy, FortiMail applies the settings in the recipient-based policy and ignores the IP-based policy unless you enabled **Take precedence over recipient based policy match** in the IP policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Logs that a DLP event generates are assigned the **Data Loss Prevention** classifier. To see exactly which email content FortiMail caught, click the session ID to view the cross-search results for that event.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Why is the DLP feature disabled on entry-level FortiMail models?
   A. DLP configuration is disabled if you do not have at least two interfaces.
   ✓ B. It is disabled because of performance considerations.

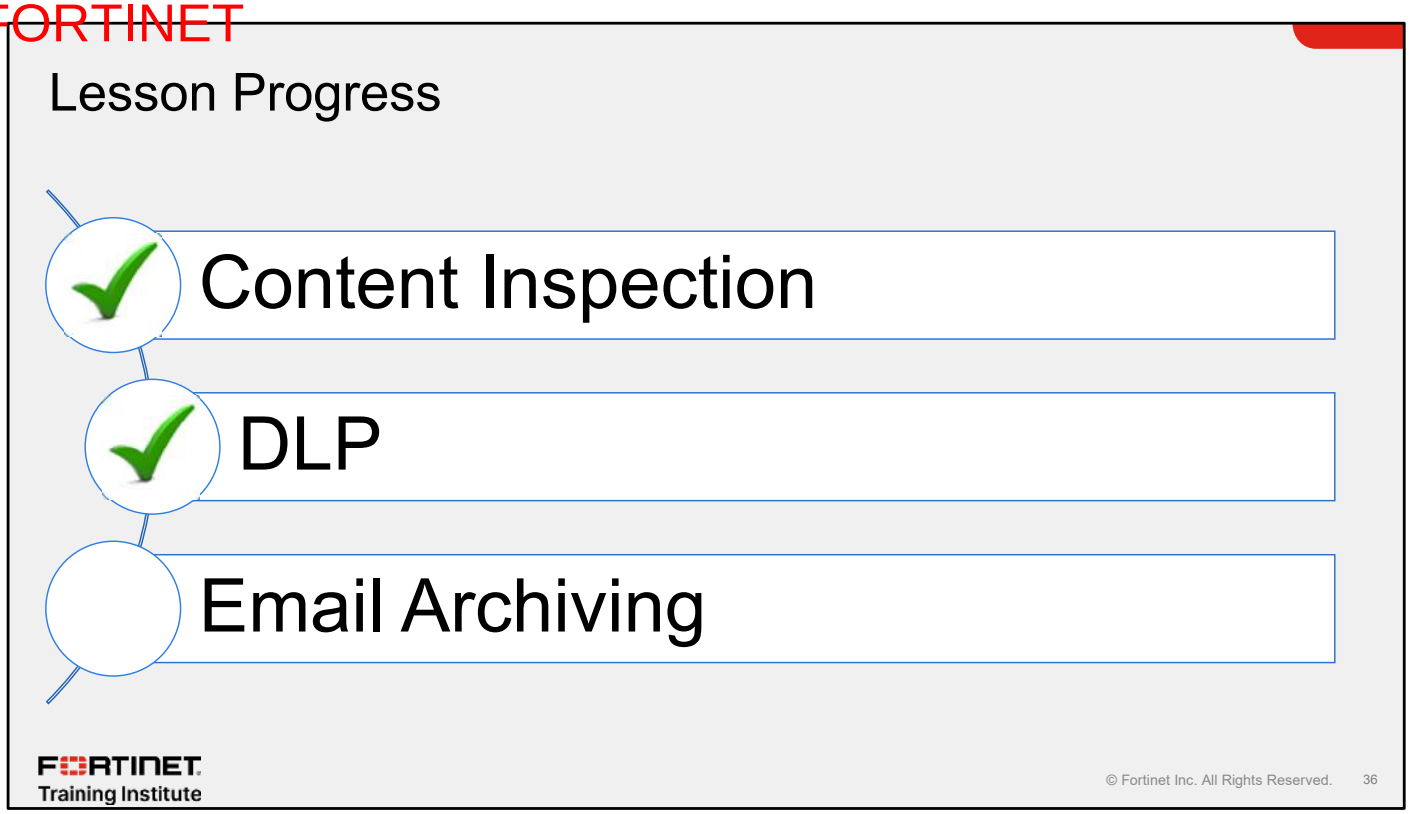
2. Which method can you use to create fingerprints on FortiMail for DLP?
   ✓ A. Upload files manually.
   B. Upload hash values of files.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 35

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

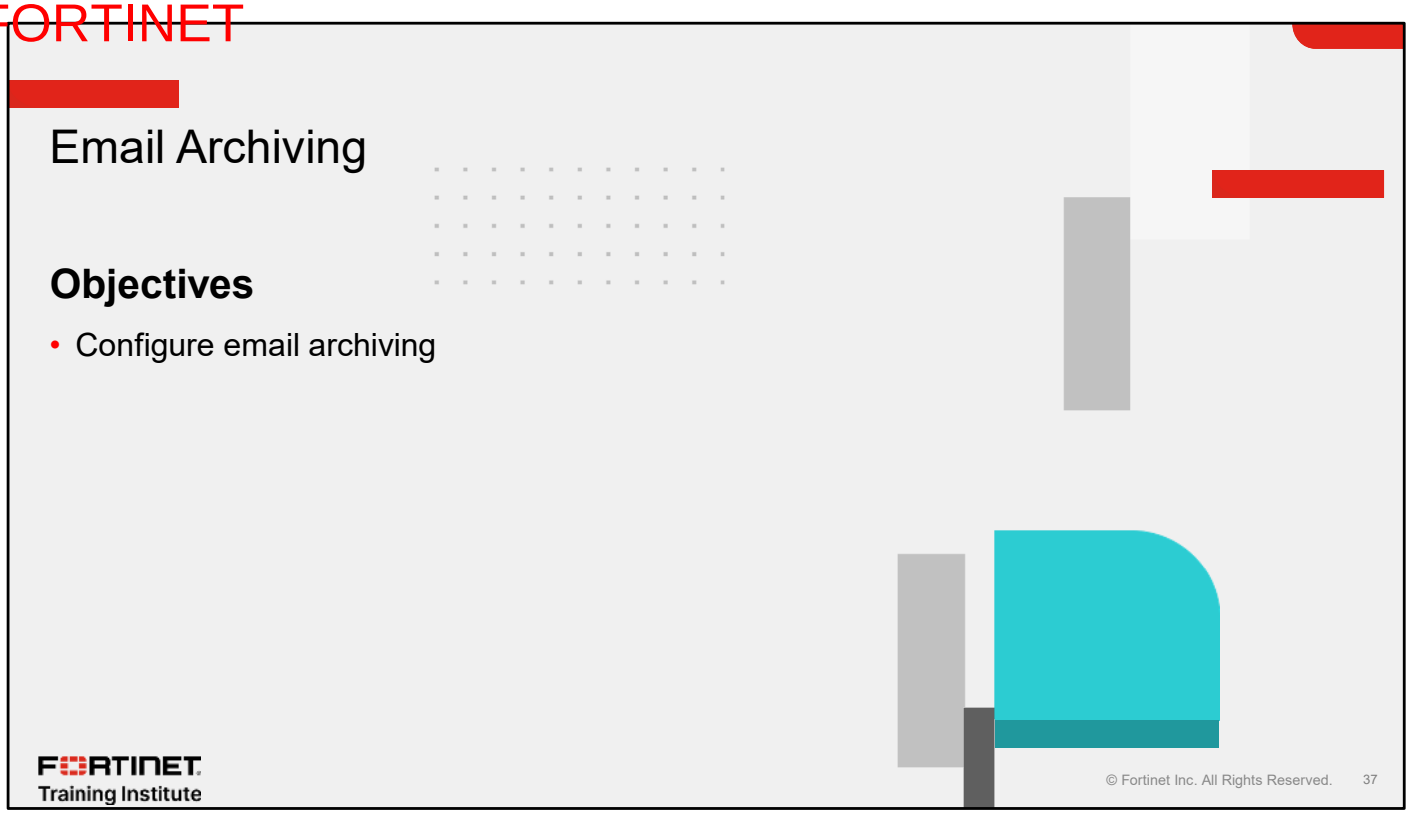


Good job! You now understand DLP.

Now, you will learn about email archiving.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in email archiving, you will be able to configure FortiMail to archive incoming and outgoing messages to meet organizational or compliance requirements.

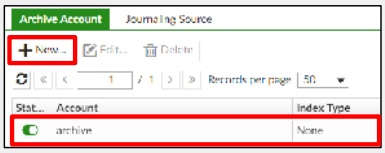
Vouchers & Dumps are Available | WhatsApp +201224560923

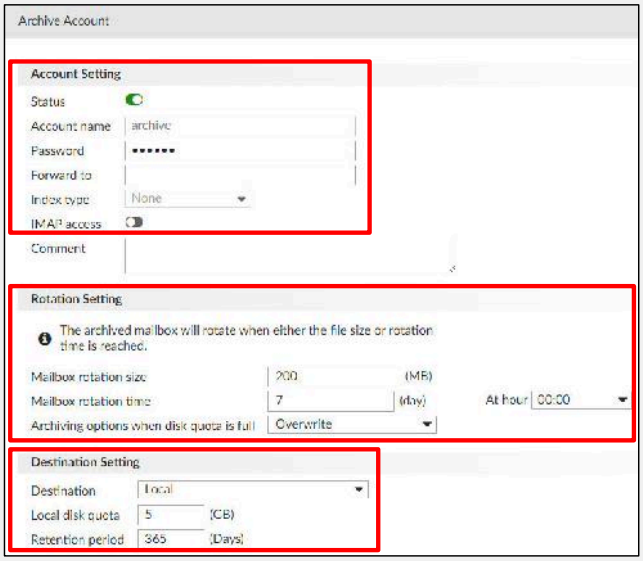
DO NOT REPRINT Brave-dumps.com
© FORTINET

Archive Account

- **Archive Account**
  - Password
  - IMAP access
- **Rotation Setting**
  - How often FortiMail should start a new mailbox file
- **Destination Setting**
  - **Local** or **Remote** storage options
    - Remote storage can be either FTP or SFTP
  - Retention period feature has been added for archive retention

Email Archiving > Archive Account > Archive Account





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 38

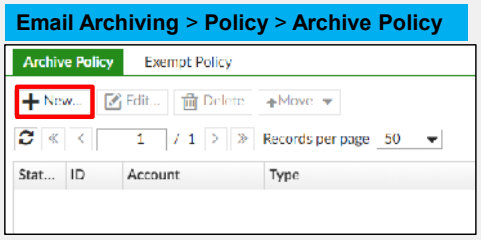
To use FortiMail email archiving, you must create archive mailboxes by adding an archive account. You can use the default account or create a new one. You can then define an archive account password, access options, mailbox rotation schedules, and disk quota. You can also define the archive storage location, which can be either local or remote. FTP and SFTP are the only supported remote storage options. You can now configure the retention period in days.

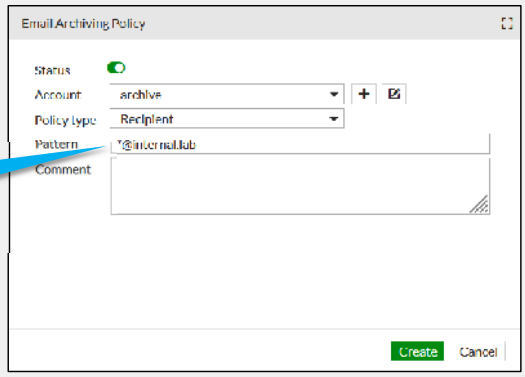
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Archive Policy

- Define which email to archive and where, by defining patterns based on:
  - Sender address
  - Recipient address
  - Keyword in subject
  - Keyword in body
  - Attachment filename





Archive any email destined to ***@internal.lab**, and save it in the **archive** mailbox

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 39

Archive policies allow you to define which emails FortiMail archives.

The **Account** option allows you to define where FortiMail saves the archived emails. The **Pattern** option allows you to define a string that FortiMail searches to make archiving decisions. The **Policy type** option allows you to define where FortiMail searches for the **Pattern**.

You can search for the defined pattern in an email sender, recipient, subject, body, or attachment filename by configuring the **Policy type** setting appropriately.

After you create a valid archive policy, FortiMail immediately begins archiving email that matches the policy.

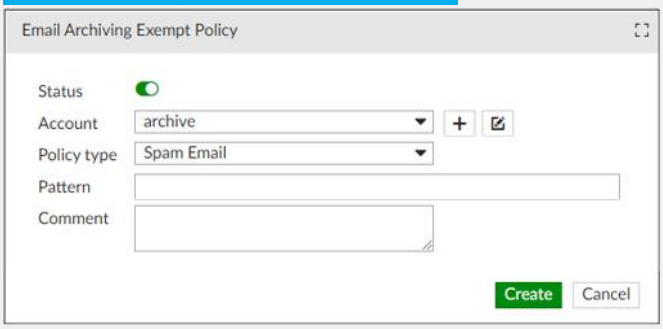
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Exempt Policy

- Exempt certain email from being archived
- Typically used to exclude spam email

Email Archiving > Policy > Exempt Policy



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 40

You can use exempt policies to exempt specific emails from being archived. You typically configure an exempt policy to exclude spam email from being archived in order to use the archive storage more efficiently.

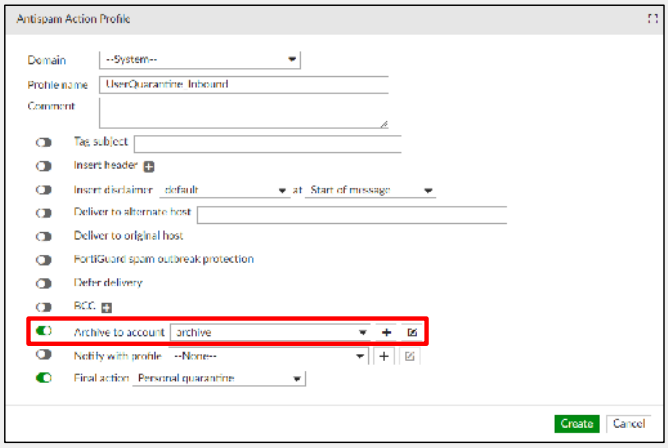
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

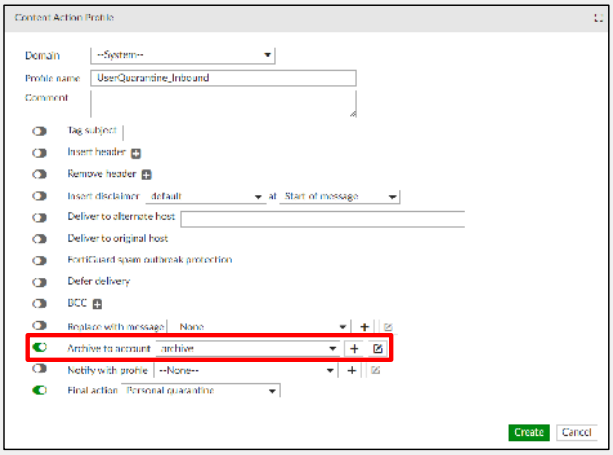
Archiving Using Action Profiles

- You can also use antispam or content action profiles to archive email to a configured account

Profile > Antispam > Action



Profile > Content > Action



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 41

You can also use antispam action profiles and content action profiles to archive emails. For each action profile, select **Archive to account**, and then select a destination archive account.

A typical use case scenario involves using dictionary profiles, which are supported by both antispam and content profiles, to monitor and archive emails that contain specific words or phrases.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Logs

Monitor > Log > History

History | System Event | Mail Event | AntiVirus | AntiSpam | Encryption | Log Search Task

List | View | Search | Export | 2024-01-02 10:00:14 -> Current | Configure View

1 / 1 | Records per page 100 | Go to line | Selected: 1 / 10

#	Date	Time	Classifier	Disposition	From	Header From	To	Subject	Message-ID ...	Length	Session ID	Cli
1	2024-01-02	11:39:51.939	Not Spam	Accept	extuser@external...	extuser@external.lab	user1@intern...	Archive Test	2024010211...	562	402Jdp2H003433-40...	

History | System Event | Mail Event | AntiVirus | AntiSpam | Encryption | Log Search Task | Cross search result: 402Jdp2H003433

1 / 1 | Records per page 100 | View | Export | Total: 6

Log Type ...	Date	Time	Classifier...	Dispositi...	From	Header F...	To	Subject	Message...	Message
Mail Event	2024-01-02	11:39:51.727								STARTTLS=server, relay=extsrv [100.64.1.99], versi
Mail Event	2024-01-02	11:39:51.842								from=<extuser@external.lab>, size=562, class=0, n
Mail Event	2024-01-02	11:39:51.938								to=<archive> stat=Sent
History	2024-01-02	11:39:51.939	Not Spam	Accept	extuser@...	extuser@...	user1@in...	Archive Test	2024010...	
Mail Event	2024-01-02	11:39:51.985								STARTTLS=client, relay=10.0.1.99, version=TLSv1.2
Mail Event	2024-01-02	11:39:52.163								to=<user1@internal.lab>, delay=00:00:01, tries=1),

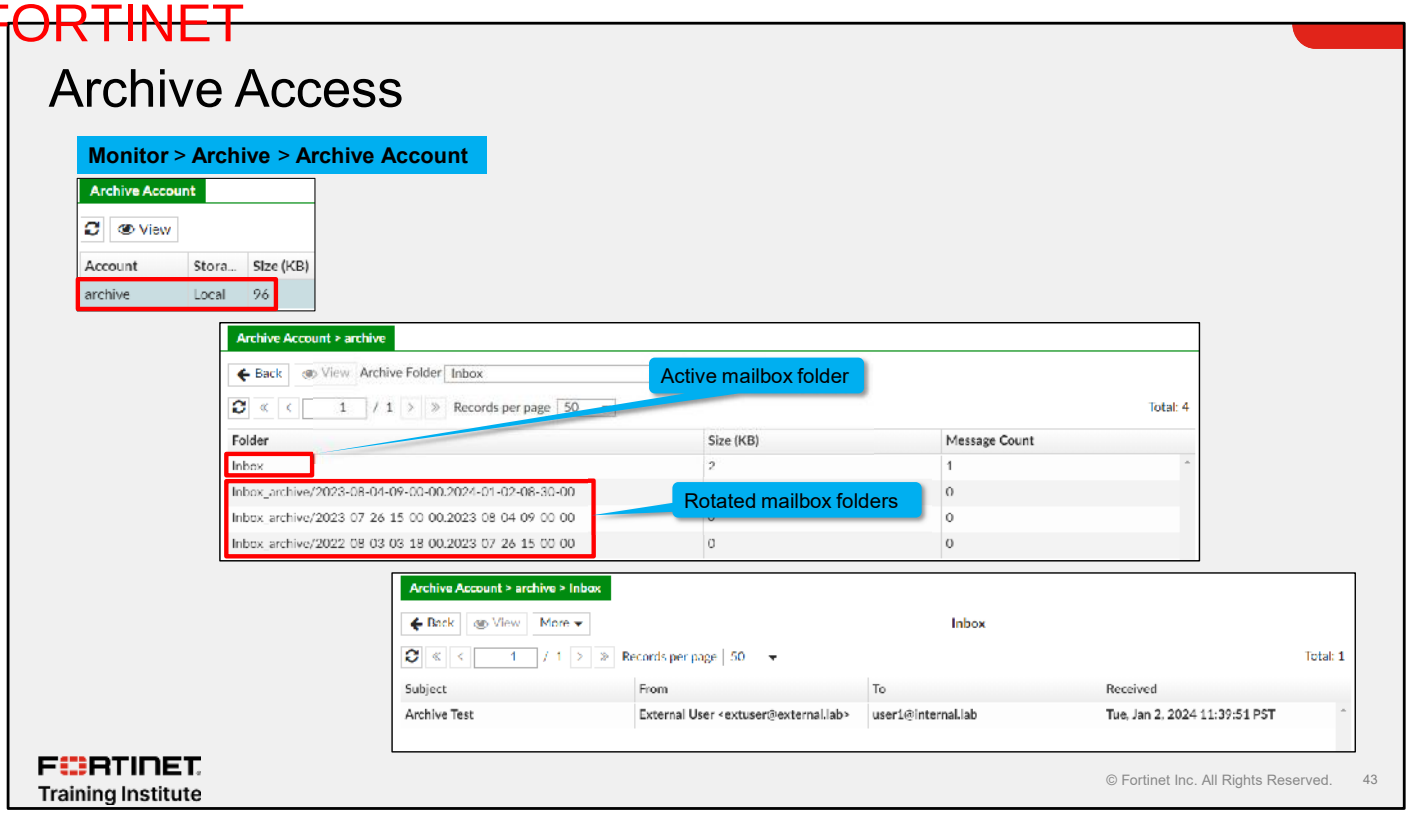
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 42

You can use the cross-search results of the logs to verify that FortiMail is archiving email correctly.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can access the archived email using the FortiMail management GUI. You can also access the archive mailbox using IMAP if the relevant access options are configured in the archive account options.

You can export archived emails in `.mbox` or `.eml` formats. You can't delete emails from the archive. The only way to delete archived emails is to format the mail disk.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. In which two locations can you store FortiMail archives? (Choose two.)
   - ✓ A. Local disk
   - B. FortiCloud storage
   - ✓ C. SFTP server
   - D. CFS file share

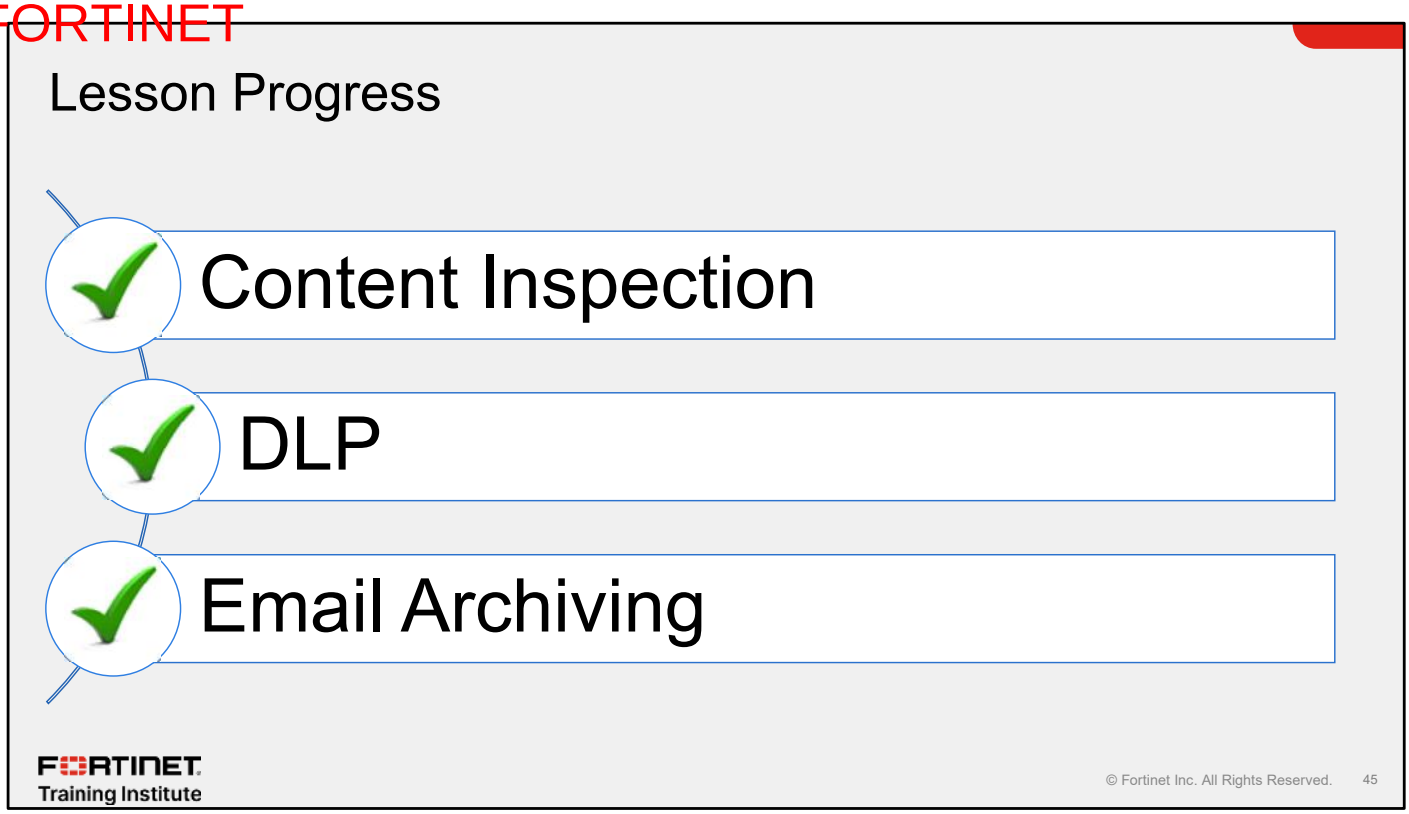
2. Which management interface do you use to access archived email on FortiMail?
   - A. Webmail GUI
   - ✓ B. Management GUI

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 44

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Configure content filtering to manage the type of content in emails
- ✓ Configure DLP to protect sensitive data
- ✓ Configure email archiving

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 46

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure FortiMail antivirus and content inspection features.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FORTINET Training Institute

FORTINET CERTIFIED PROFESSIONAL
Public Cloud Security

FortiMail Administrator

Securing Communications

FortiMail 7.4

Last Modified: 25 April 2024

In this lesson, you will learn about the diverse methods for securing communications on FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Overview

- Encryption
- IBE Advantage
- IBE Delivery Methods
- IBE Configuration
- IBE User Experience
- IBE User Management and Customization

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 2

In this lesson, you will explore the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Encryption

Objectives

- Configure SMTPS
- Manage TLS encryption with TLS profiles and access control rules

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 3

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in encryption, you will be able to configure Simple Mail Transfer Protocol Secure (SMTPS) and manage transport layer security (TLS) encryption with TLS profiles and access control rules.

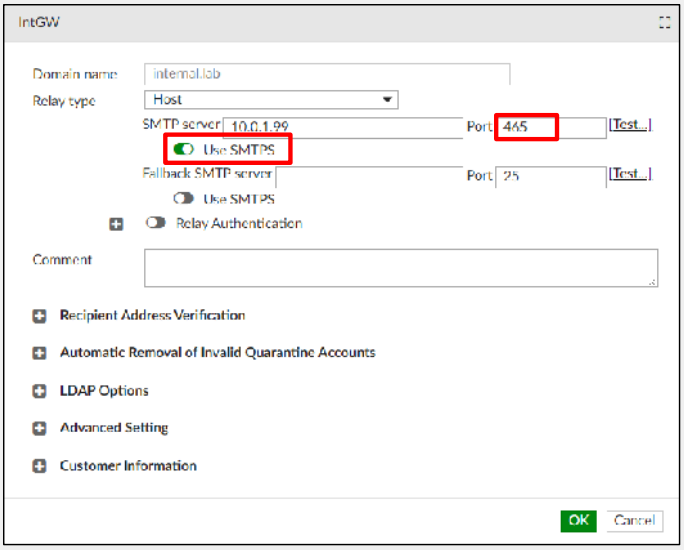
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Initiating SMTPS Connections

- For FortiMail gateway and transparent modes, enable SMTPS in the protected domain configuration
- If the back-end server doesn't support SMTPS, the connection reverts to standard SMTP

Domain & User > Domain > Domain



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

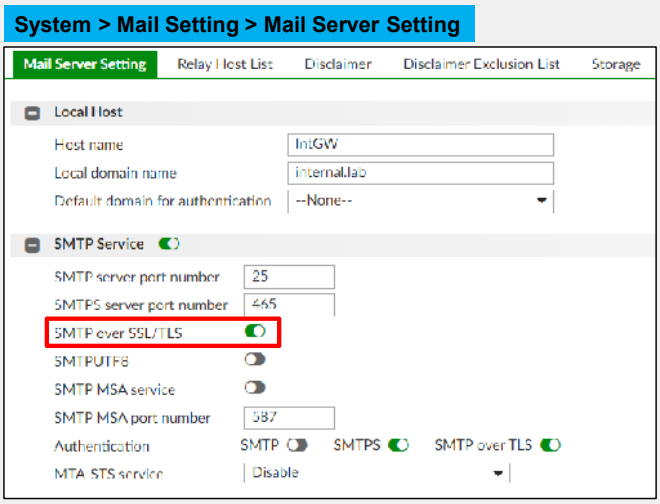
While SMTPS is usually deprecated in favor of STARTTLS, SMTPS is still supported on FortiMail for backward compatibility. For gateway and transparent modes, you can enable SMTPS support in the protected domain configuration. By default, if the back-end server doesn't support SMTPS, the connection reverts to SMTP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Accepting SMTPS Connections

- FortiMail as the recipient MTA accepts SMTPS sessions only if you enable **SMTP over SSL/TLS**
- This also enables the STARTTLS extension
- Recommended for all deployment modes



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

You can also configure FortiMail to accept all connections as SMTPS by enabling **SMTP over SSL/TLS**. This also enables the STARTTLS extension for clients to use. You should enable this option for all deployment modes.

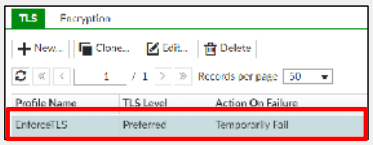
Vouchers & Dumps are Available | WhatsApp +201224560923

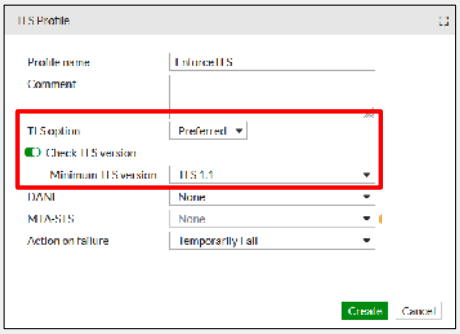
DO NOT REPRINT Brave-dumps.com
© FORTINET

TLS Profile

- You can configure TLS profiles with different TLS options and the action to take if the TLS level can't be established

Profile > Security > TLS





TLS Option	Description
None	Disables TLS, requests for TLS will be ignored.
Preferred	Allow TLS, but do not require it. This is the default behavior. No Action on failure setting applicable.
Secure	Requires a certificate-authenticated TLS connection. CA certificates must be installed on the FortiMail unit before they can be used for secure TLS connections.

Action on failure	Description
Temporarily Fail	Drop connection. Retry at a later time.
Fail	Drop connection and generate DSN.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

The TLS profile is configured with one of three security levels and associated sets of failure actions. The possible settings are shown on this slide.

By default, FortiMail uses the **Preferred** setting. This means that FortiMail will choose TLS when sending and allow TLS when receiving. Failure actions aren't applicable.

DANE (DNS-based Authentication of Named Entities) allows the retrieval of PGP public keys using DNS as outlined in RFC 7929.

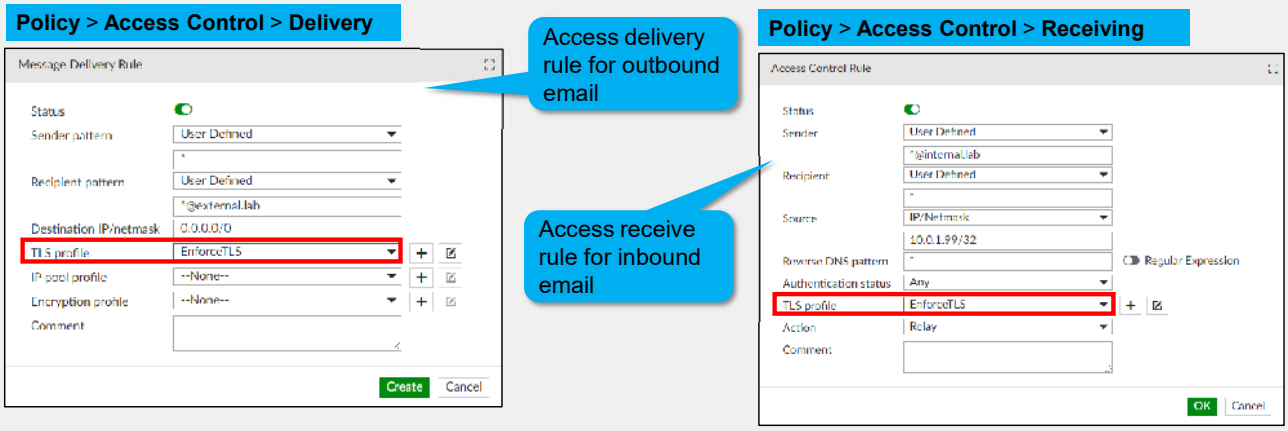
MTA-STS support allows the checking of MTS-STS profile records when allowing email to be delivered to the FortiMail. You can enable MTA-STS in the **System > Mail Setting** and then select it in a TLS profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Enforcing TLS

- By default, FortiMail uses STARTTLS if the recipient MTA supports it, and reverts to plain text if the recipient MTA doesn't support it
- Using access control rules and TLS profiles, FortiMail can enforce TLS



FORTINET Training Institute

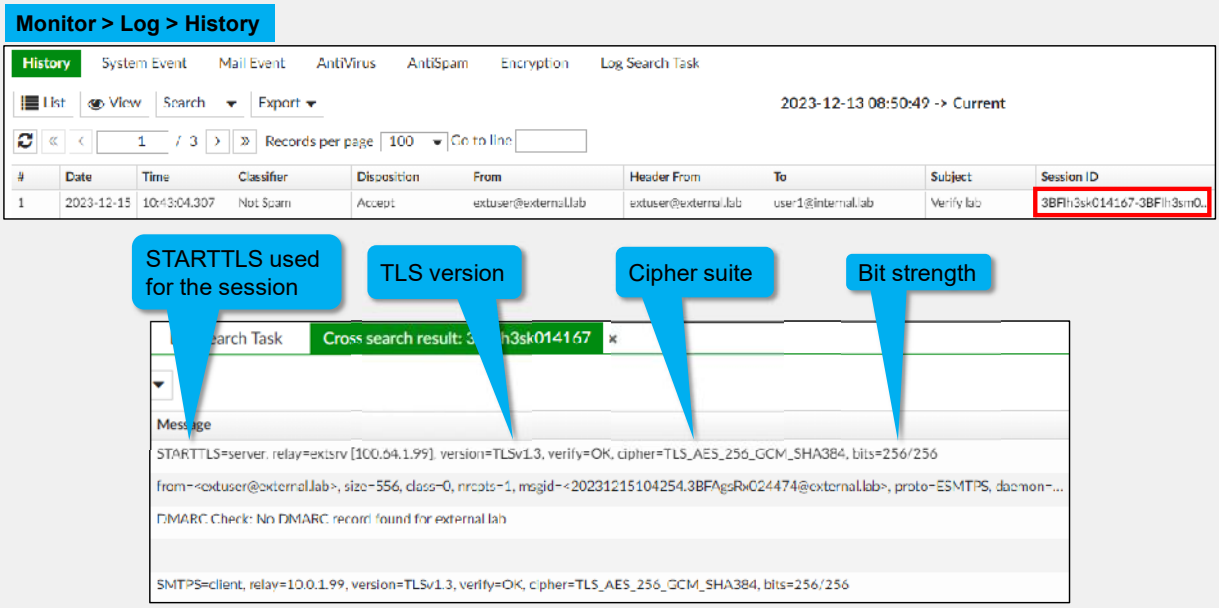
© Fortinet Inc. All Rights Reserved. 7

By default, FortiMail uses STARTTLS if the recipient MTA supports it, and reverts to plain text if the recipient MTA doesn't support it. Using access control rules and TLS profiles, FortiMail can enforce TLS in both directions. For example, you can configure an access receive rule that has a TLS profile to accept email only if the sender selects STARTTLS. In the reverse direction, you can configure an access delivery rule that has a TLS profile to force FortiMail to always select STARTTLS and close the connection if the recipient MTA doesn't support STARTTLS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

TLS Logs



FortiMail logs all TLS-related entries as event logs. To view TLS-related events, in a history log, click the **Session ID** link. The log entry contains the TLS version, cipher suite, and bit strength.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. What is the default FortiMail behavior when TLS is involved in outbound SMTP sessions?
   A. TLS is always required. Failure to negotiate TLS ends the SMTP session.
   ✓ B. FortiMail negotiates TLS if the remote server supports it.

2. Which TLS option always enforces TLS?
   A. Preferred
   ✓ B. Secure

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Encryption
- IBE Advantage
- IBE Delivery Methods
- IBE Configuration
- IBE User Experience
- IBE User Management and Customization

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

Good job! You now understand encryption.

Now, you will learn about the advantages of using identity-based encryption (IBE).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

IBE Advantage

Objectives

- Differentiate between traditional email encryption methods and identity-based encryption (IBE)

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

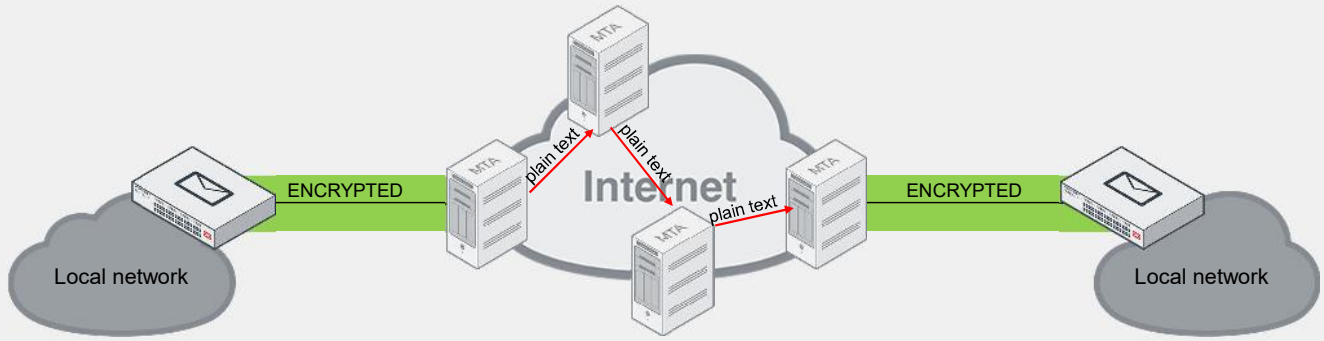
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding the advantages of using identity-based encryption (IBE), you will be able to differentiate between traditional email encryption methods and IBE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

When TLS Is Not Enough



- Only a portion of an email's path *may* be encrypted
- No control over which public MTA the email passes through
- Eavesdropping possible if email passes between two MTAs in plaintext
- To guarantee privacy and security, encryption must be present end-to-end

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

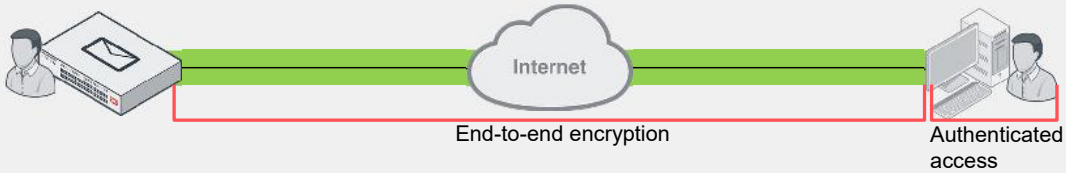
SMTP, as a store-and-forward protocol, is detrimental to security because the contents of a message can travel through multiple locations from sender to recipient. Even with traditional TLS encryption methods, if there are multiple hops, there is no way to ensure that all sessions are encrypted. To make matters worse, the message contents are available in plaintext at each MTA along the path. This provides multiple opportunities for unscrupulous individuals to observe the content of the message.

To guarantee privacy and security, the contents of the message must remain encrypted over the entire journey from sender to recipient, and receipt of the message must be authenticated.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IBE



- Public key encryption technology used for end-to-end encryption
- Encryption keys generated from identity elements such as email addresses
- Authenticated access for decryption
- Simplified administration; no need to exchange keys or digital certificates in advance

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

IBE leverages the best parts of public key cryptography and provides a powerful, yet simplified solution for environments requiring end-to-end encryption for secure delivery of sensitive email content.

At the time an email message is created, the identities of the participants are already known from their email addresses. IBE uses email addresses as the source input to automatically generate a key pair for each user identity. These key pairs are held and managed securely by FortiMail, and not distributed to the end users, eliminating the need for any cumbersome key exchange mechanisms.

Because there is no key management overhead, IBE messages can be sent by FortiMail users to arbitrary external recipients, without needing any prior preparations. The only requirement for the recipient of an IBE-secured message is a relatively modern browser capable of SSL. No specialized software is needed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about IBE is true?
   - ✓ A. IBE uses public key cryptography as the encryption architecture.
   - B. Recipients can access their IBE email without authentication, if they have the sender's public key.

2. How is the encryption key generated for IBE?
   - ✓ A. It is generated from identity elements, such as email addresses.
   - B. It is generated from biometric data.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Encryption
- ✓ IBE Advantage
- IBE Delivery Methods
- IBE Configuration
- IBE User Experience
- IBE User Management and Customization

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

Good job! You now understand the advantages of using IBE.

Now, you will learn about delivery methods.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

IBE Delivery Methods

Objectives

- Differentiate between push and pull delivery methods

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in delivery methods, you will be able to differentiate between push and pull delivery methods.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Pull Delivery Method

- Sender generates an email with confidential data
- Confidential email triggers encryption policy on FortiMail
- FortiMail generates a notification email to the recipient with an embedded HTTPS URL
- Recipient accesses the HTTPS link and logs into the FortiMail secure message portal
- Decrypted email is displayed using HTTPS webmail interface

FORTINET Training Institute

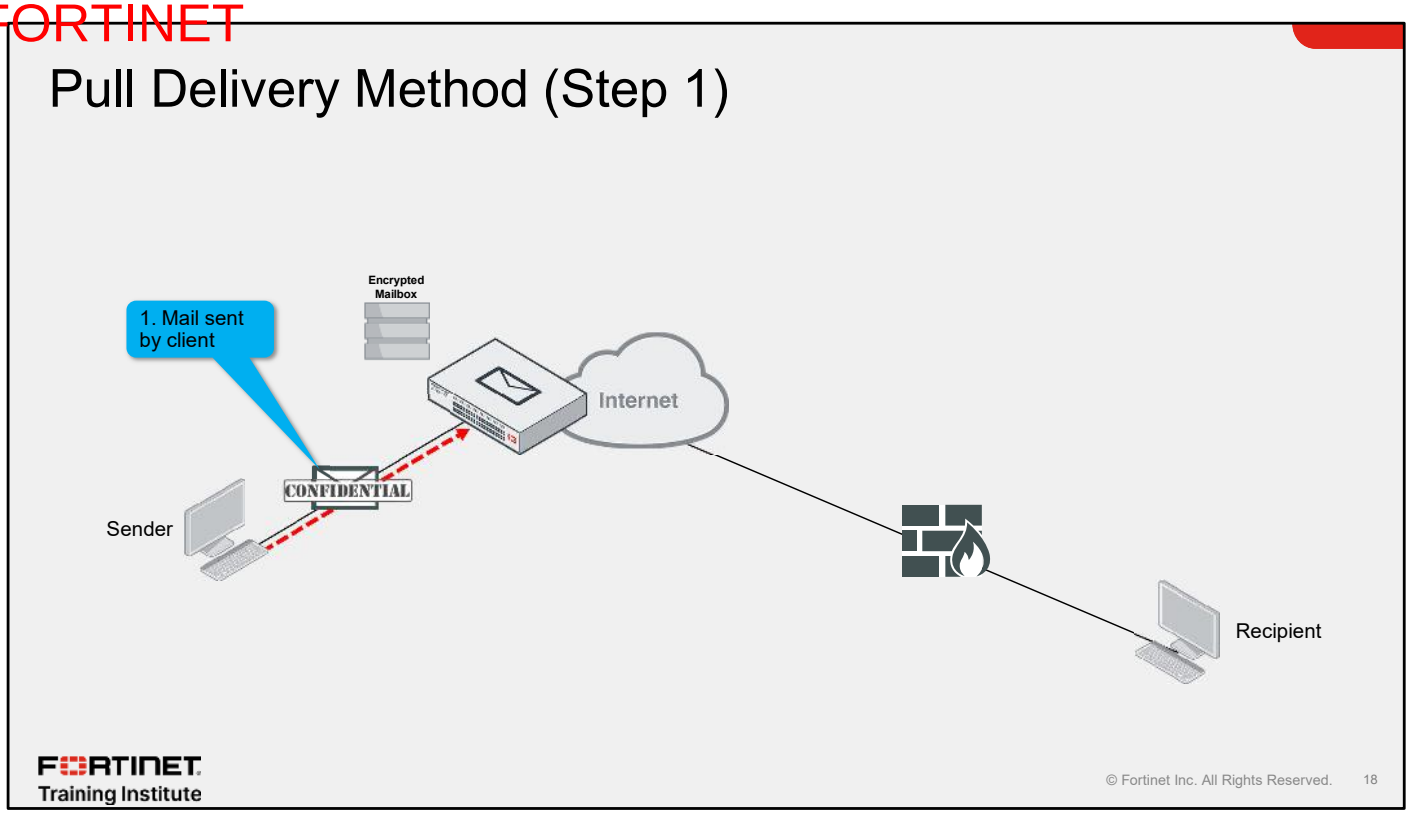
© Fortinet Inc. All Rights Reserved. 17

IBE provides two options for message delivery.

If you configure FortiMail to use the pull method, messages remain on FortiMail in a secure mailbox. A notification email is sent to the recipient's address stating that they have been sent an encrypted email message. The notification also contains instructions to click the embedded HTTPS URL to access the encrypted email message. When the recipient clicks the link, their browser opens and establishes an HTTPS connection to FortiMail. After the recipient authenticates, the secured message is decrypted and displayed using a webmail interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

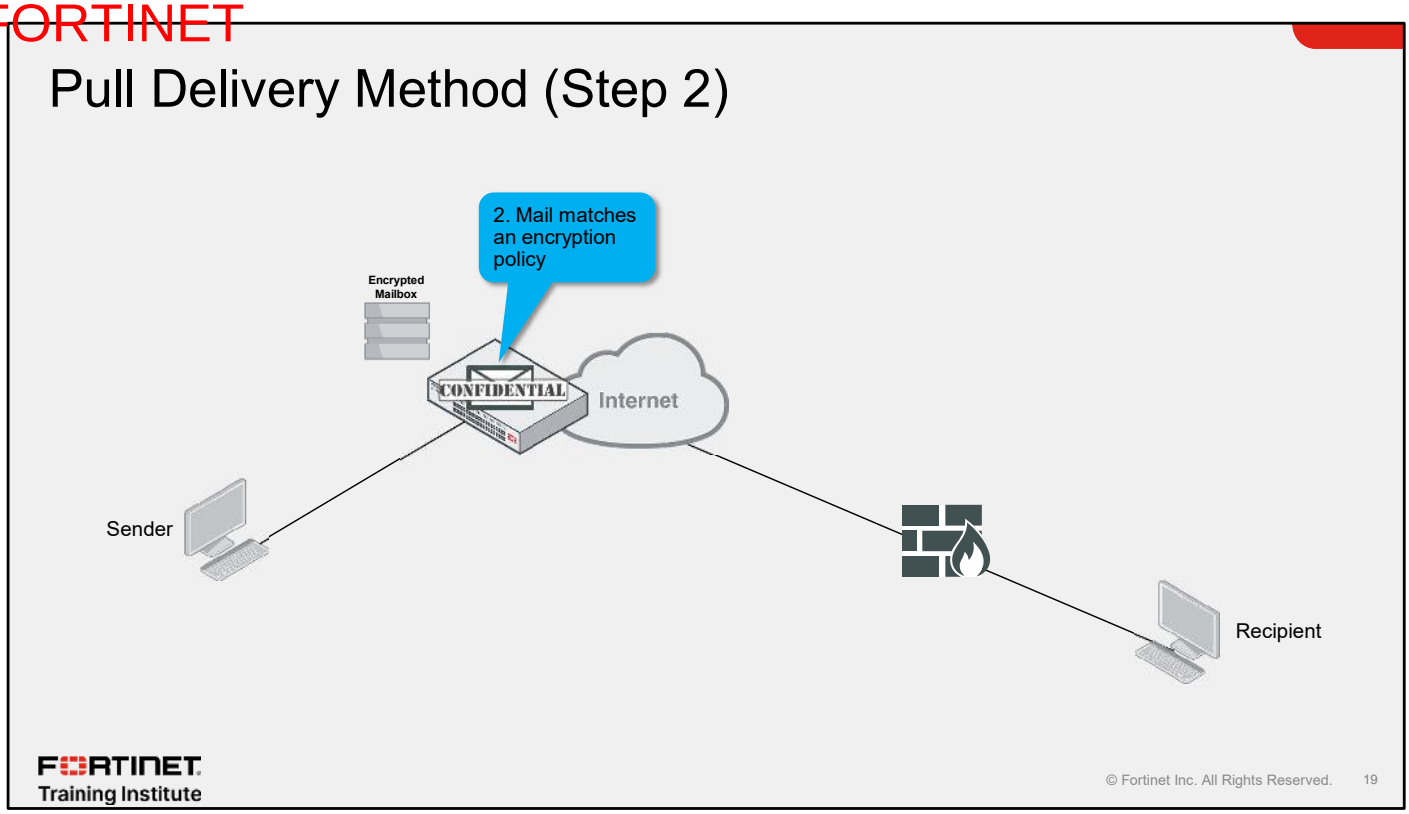
DO NOT REPRINT Brave-dumps.com
© FORTINET



Step 1: A client composes and sends a regular email through FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

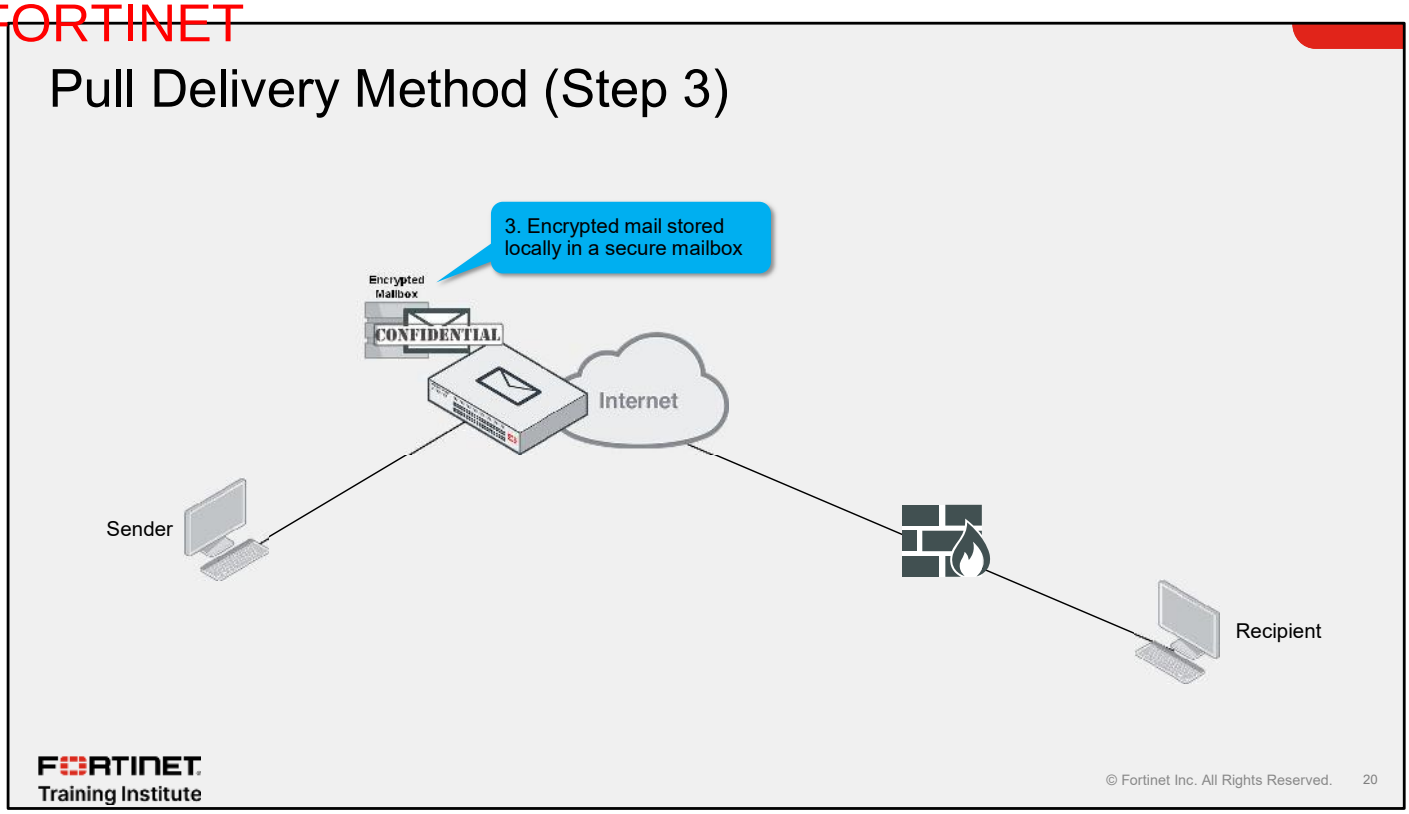
DO NOT REPRINT Brave-dumps.com
© FORTINET



Step 2: The email matches a policy in FortiMail that is configured to trigger IBE encryption. Matches are made using either an inbound access delivery rule, or an outbound recipient-based policy using a content profile with a dictionary word.

Vouchers & Dumps are Available | WhatsApp +201224560923

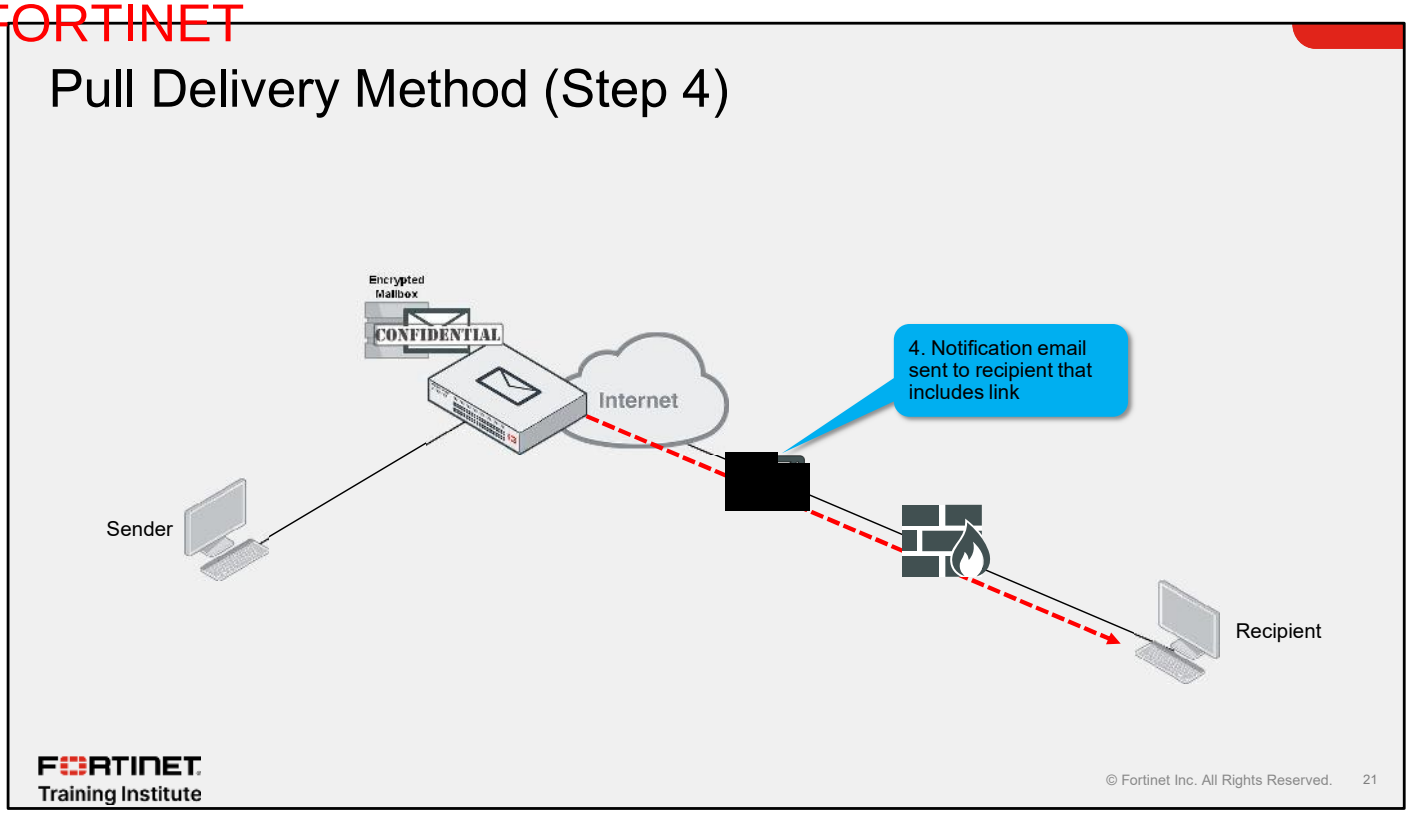
DO NOT REPRINT Brave-dumps.com
© FORTINET



Step 3: FortiMail encrypts the message and stores it in a secure mailbox.

Vouchers & Dumps are Available | WhatsApp +201224560923

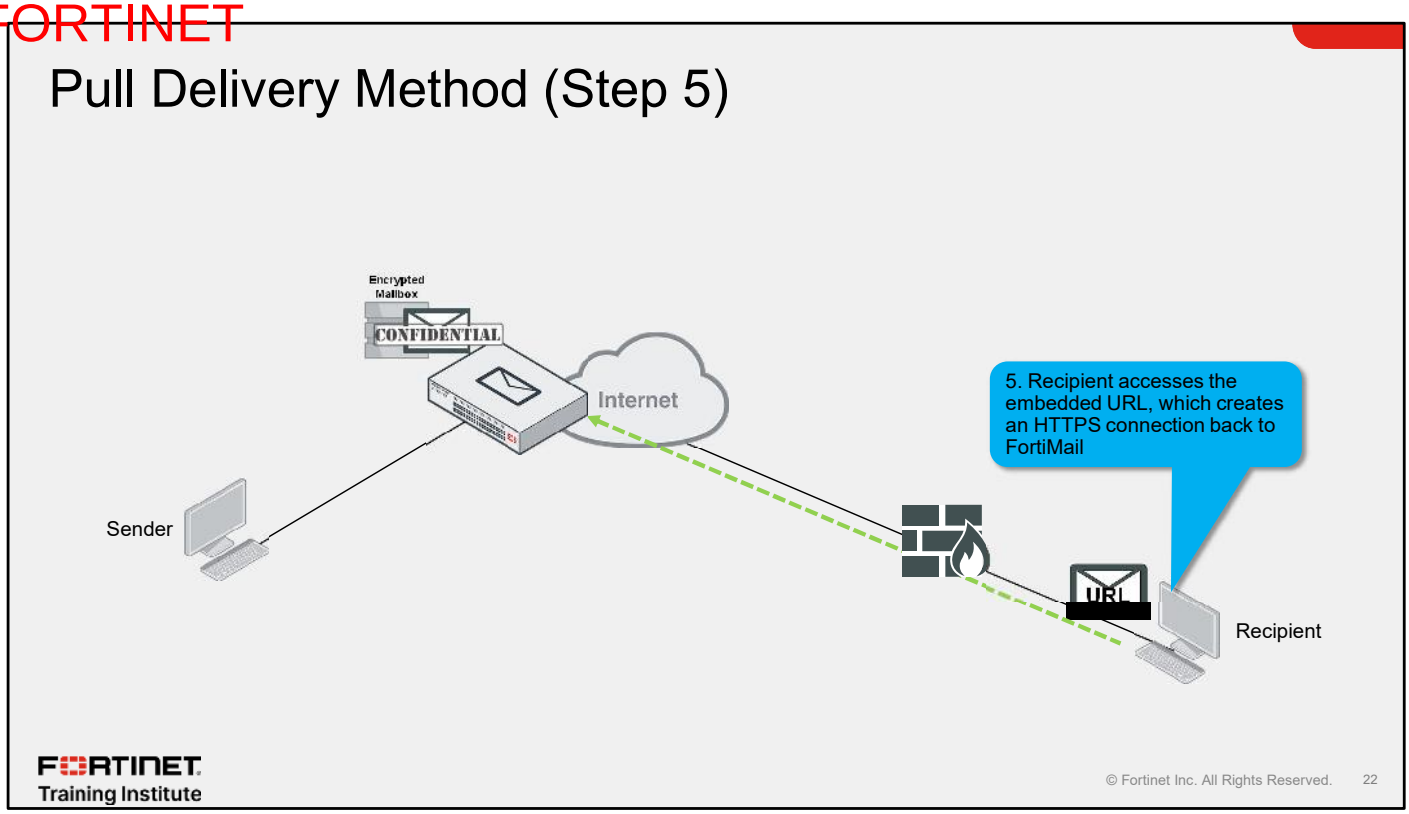
DO NOT REPRINT Brave-dumps.com
© FORTINET



Step 4: After the email contents have been encrypted and stored, a notification email is sent to the recipient containing instructions and the SSL link.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

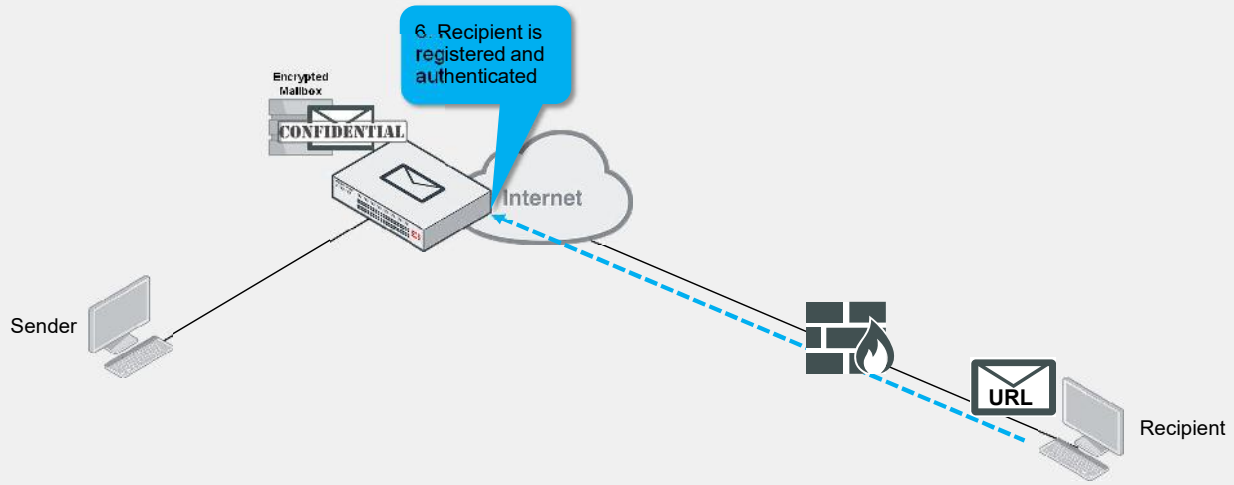


Step 5: The recipient opens the notification email and clicks the HTTPS link connecting them to the secure mail gateway on the FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Pull Delivery Method (Step 6)



FORTINET Training Institute

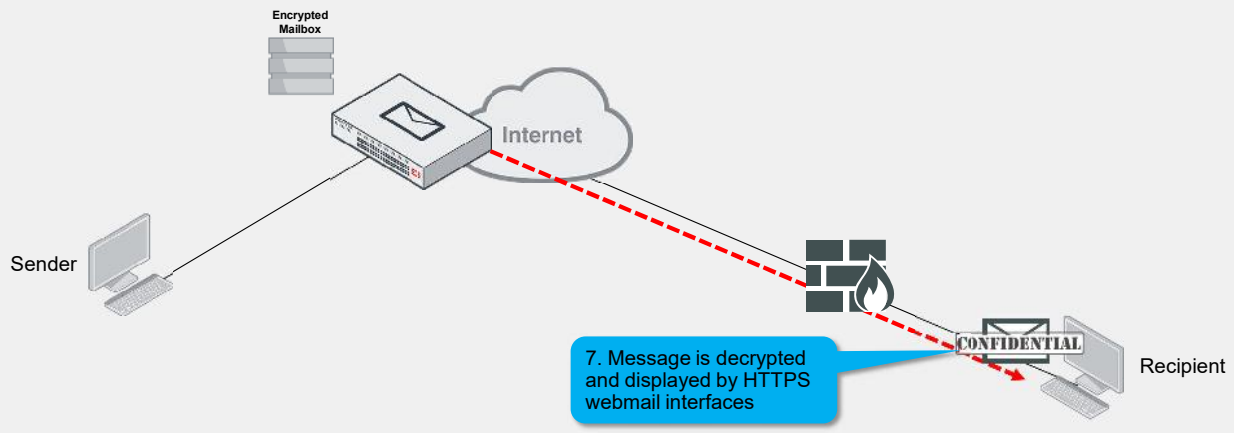
© Fortinet Inc. All Rights Reserved. 23

Step 6: If this is the first time the recipient has accessed an IBE message on this FortiMail, the recipient is prompted to register for a new IBE account. Otherwise, the recipient authenticates using the credentials from a previous registration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Pull Delivery Method (Step 7)



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

Step 7: The message is decrypted and displayed for the recipient by a webmail interface using HTTPS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Push Delivery Method

- Sender generates an email with confidential data
- Confidential email triggers encryption policy on FortiMail
- FortiMail encrypts the confidential email and adds it to the notification email as an HTML attachment
- Recipient accesses the encrypted payload and logs in to FortiMail secure message portal
- Decrypted email is displayed using HTTPS webmail interface

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

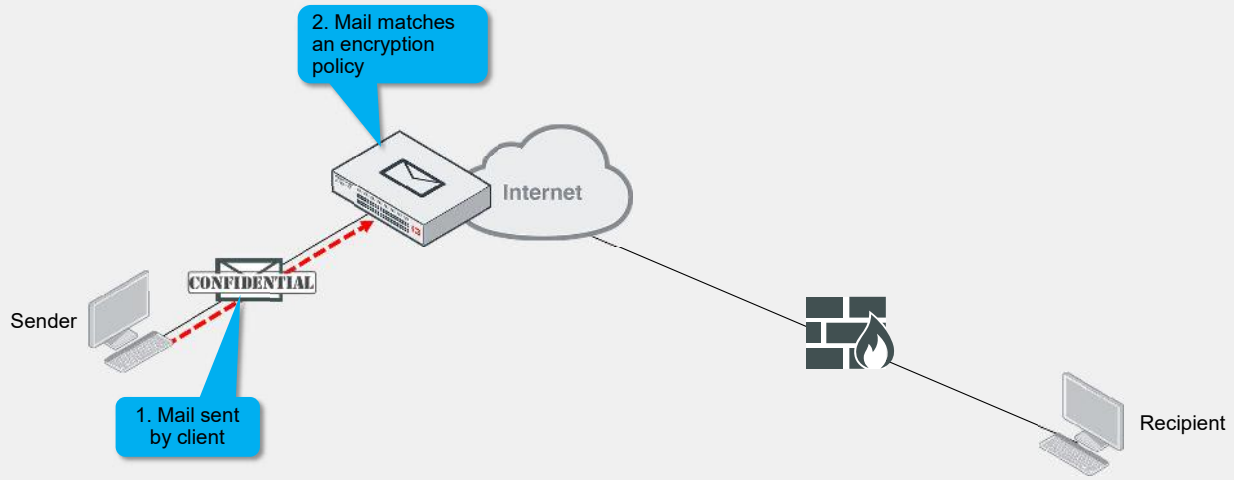
When you configure the push method, the recipient receives a plaintext email message containing the encrypted message as an HTML attachment, as well as instructions on how to authenticate and view the secured message. The attachment opens in a browser that connects automatically to FortiMail by through SSL and pushes the encrypted contents back to FortiMail. After the recipient authenticates, FortiMail decrypts and displays the now decrypted message using a webmail interface.

The major difference between these two methods is the storage of the encrypted message. Using the pull method, the message is stored in FortiMail until it is deleted. The push method delivers the message to the recipient, who is then responsible for its storage and then delivery to FortiMail for decryption.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Push Delivery Method (Step 1 and Step 2)



FORTINET Training Institute

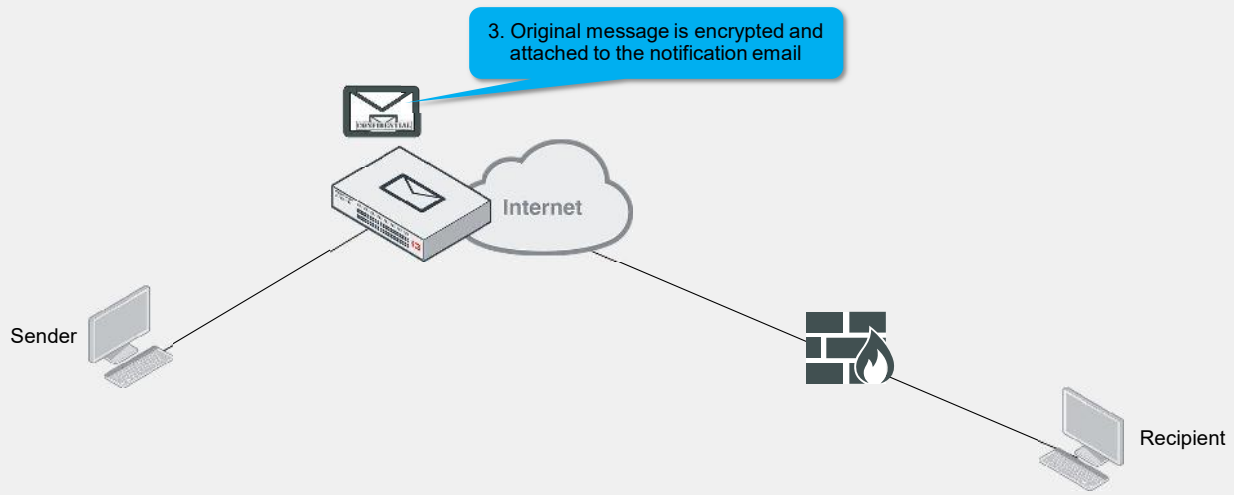
© Fortinet Inc. All Rights Reserved. 26

Steps 1 and 2: The first two steps in the push method are like the pull method, except that the encryption configuration on FortiMail is set to use push.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Push Delivery Method (Step 3)



FORTINET Training Institute

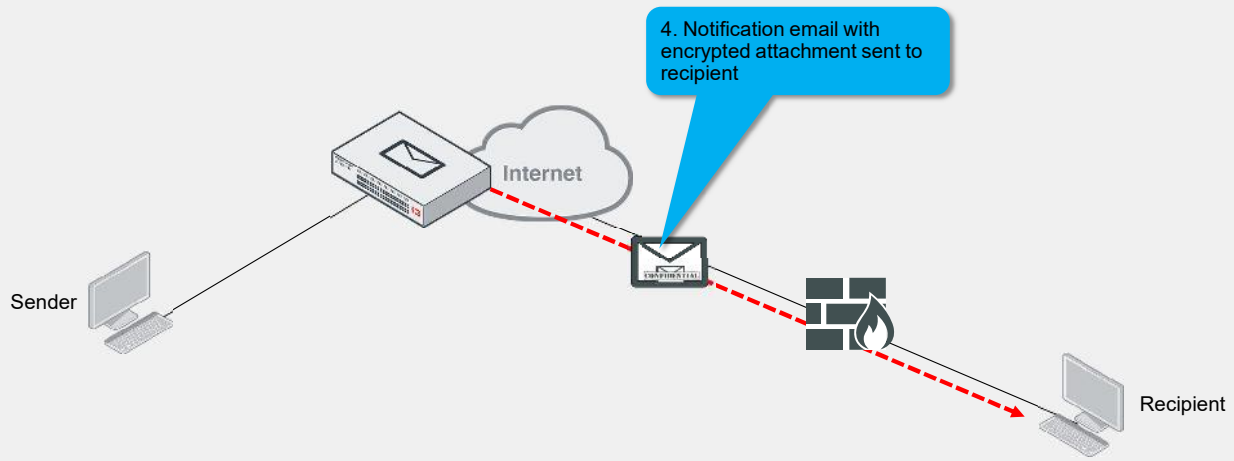
© Fortinet Inc. All Rights Reserved. 27

Step 3: Using the push method, the original message is encrypted, and packaged as an HTML attachment in the notification email.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Push Delivery Method (Step 4)



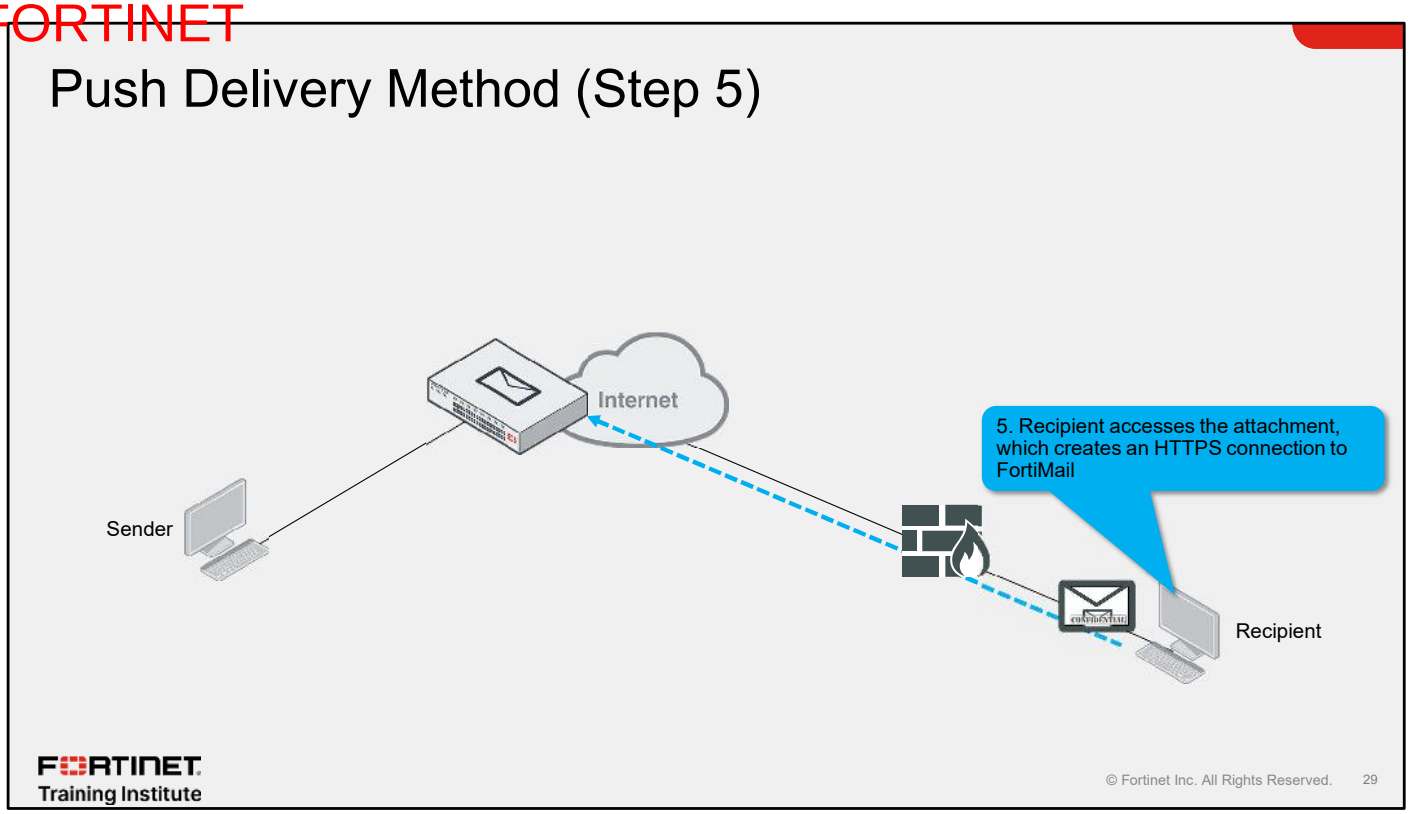
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

Step 4: A notification email is sent to the recipient containing instructions and the encrypted email message as an attachment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

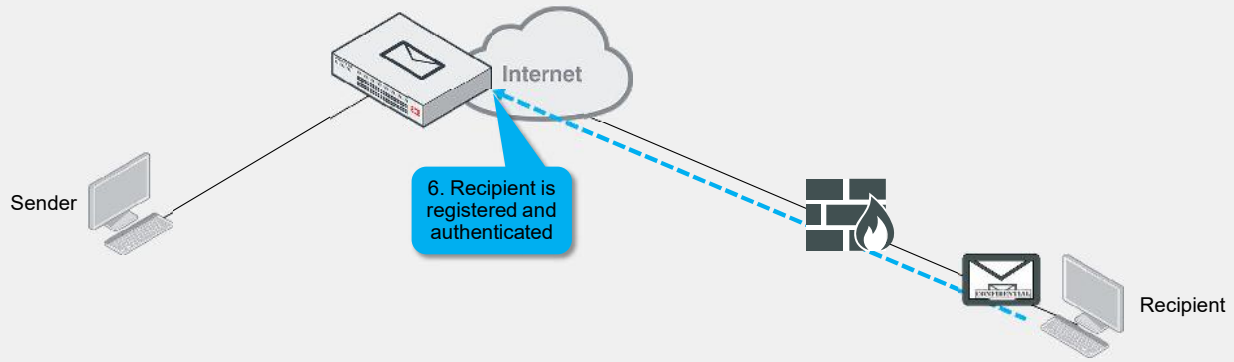


Step 5: When the recipient opens the attachment, the MTA creates an HTTPS connection to FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Push Delivery Method (Step 6)



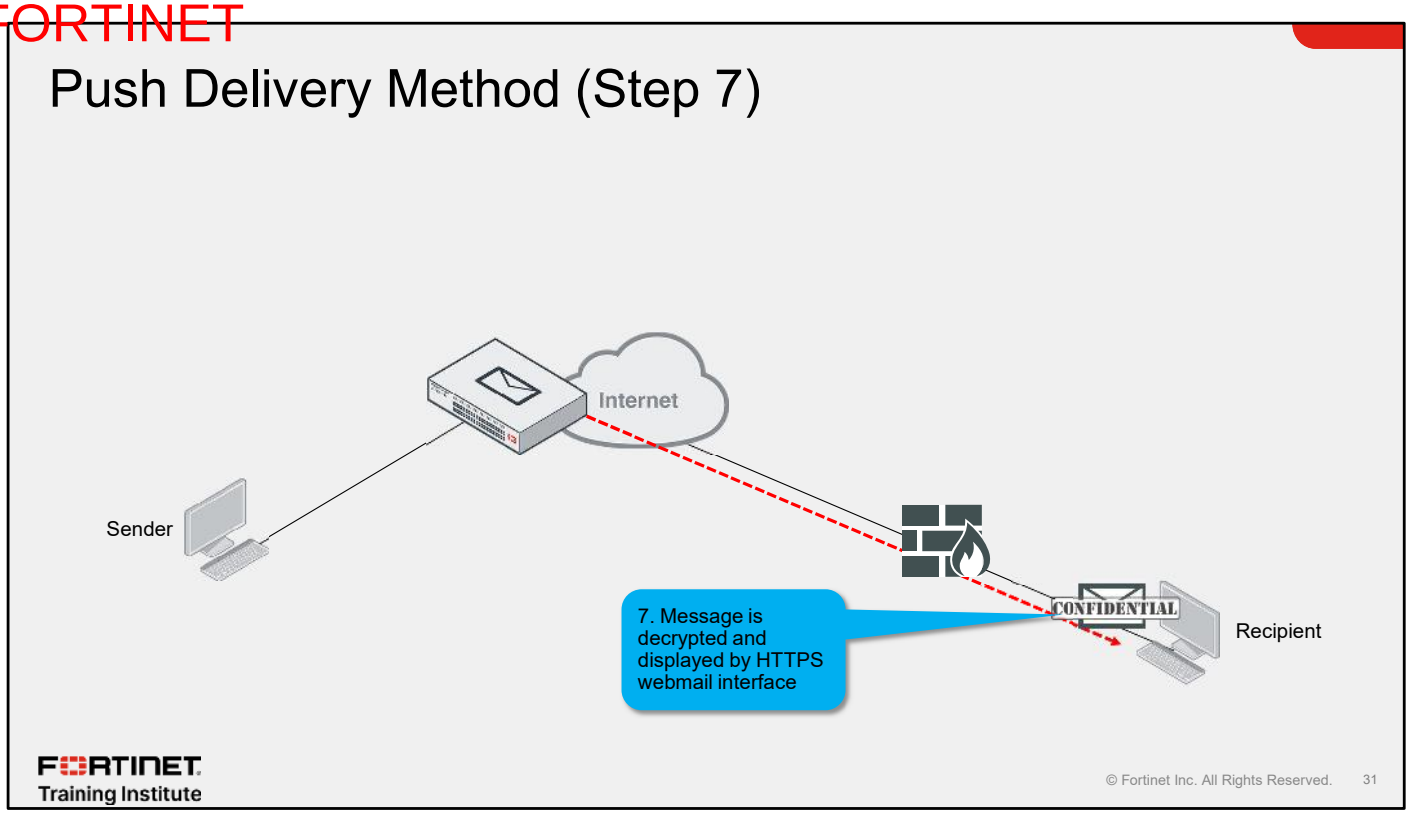
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

Step 6 : If this is the first time the recipient has accessed an IBE message on this FortiMail, the recipient is prompted to register for a new IBE account. Otherwise, the recipient authenticates using the credentials from a previous registration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Step 7: FortiMail decrypts and displays the message to the recipient using a webmail interface over HTTPS., When the webmail connection with the recipient is closed, no traces of the encrypted message exist except at the recipient's inbox, because the encrypted message isn't stored in FortiMail when the push method is used.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement accurately describes the pull delivery method used by IBE?
   A. FortiMail encrypts the confidential data and delivers it as an HTML email message.
   ✓ B. FortiMail generates a notification email message with an embedded HTTPS URL.

2. Where does FortiMail store an encrypted message when using the push delivery method?
   A. The encrypted message is stored in the recipient's mailbox.
   ✓ B. The encrypted message is stored on FortiMail.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Progress

- ✓ Encryption
- ✓ IBE Advantage
- ✓ IBE Delivery Methods
- IBE Configuration
- IBE User Experience
- IBE User Management and Customization

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

Good job! You now understand delivery methods.

Now, you will learn about IBE configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IBE Configuration

Objectives

- Configure encryption profiles for different IBE methods
- Verify IBE events using logs

FORTINET Training Institute

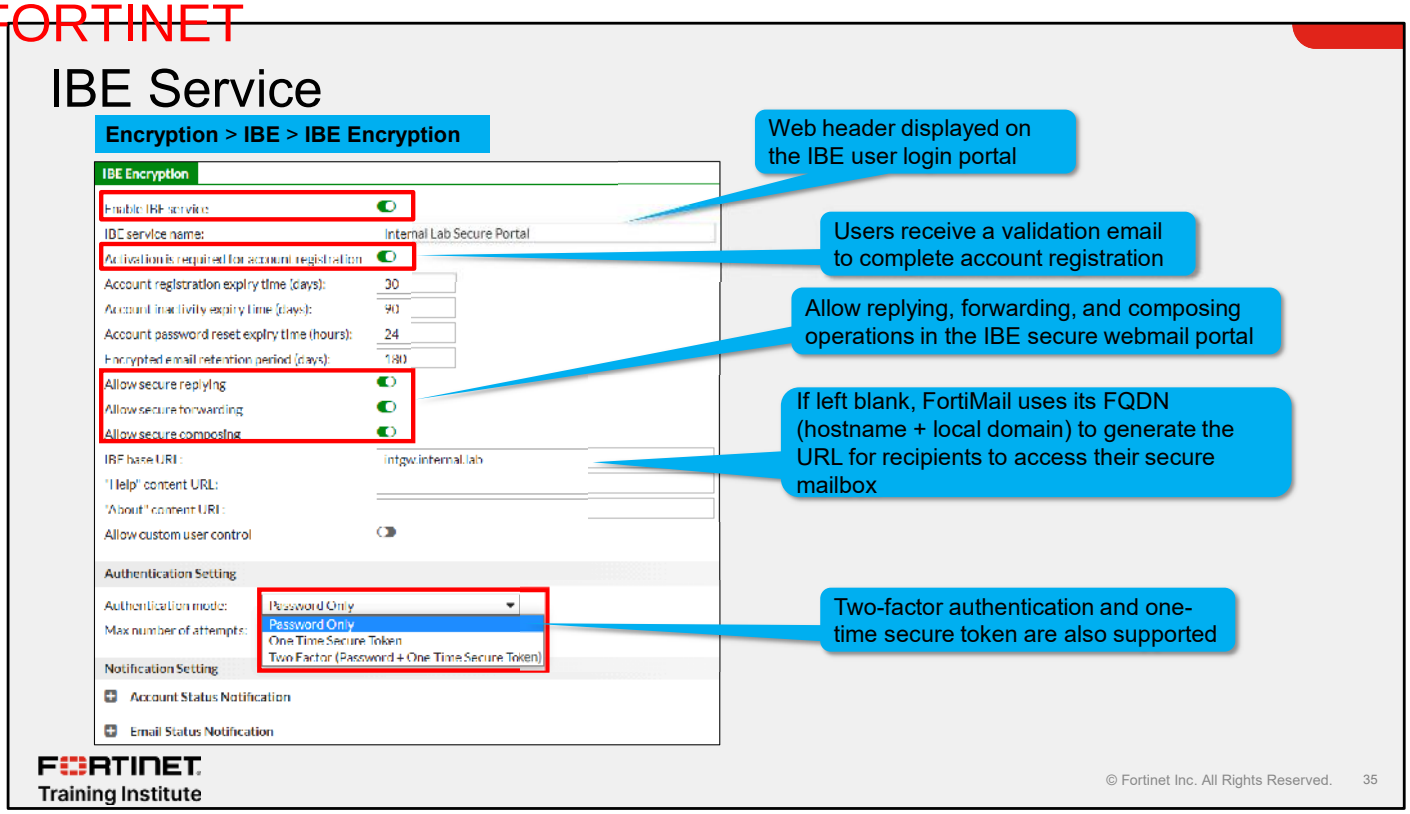
© Fortinet Inc. All Rights Reserved. 34

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in IBE configuration, you will be able to configure encryption profiles for different IBE methods and trigger IBE on outbound email using a dictionary word.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



On FortiMail, IBE is enabled globally. On the **IBE Encryption** tab, you can enable IBE system-wide, and define various options.

FortiMail uses the **IBE service name** field as a header that it displays on the IBE user login portal.

When **Activation is required for account registration** is enabled, users receive an email that contains an activation link to complete the account registration.

You can use the secure editing options to control the actions allowed in the IBE webmail interface. You can enable or disable replying, forwarding, and composing of email messages for IBE users within the secure webmail portal.

FortiMail uses the **IBE base URL** in notification email messages, either in the encrypted attachment or the URL, to enable the recipient to access their secure mailbox. If you leave the field empty, FortiMail uses its fully qualified hostname and local domain to generate the URL. Customize this field only if you want to use a different URL to enable the recipient to access their secure mailbox.

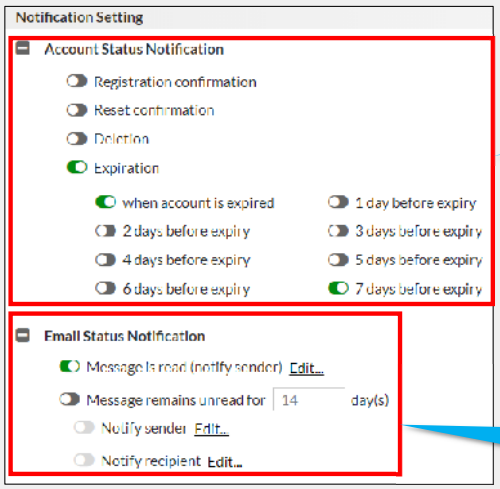
Starting with FortiMail 6.4, two-factor authentication and one-time secure token—no password required—are supported for IBE authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IBE Service (Contd)

Encryption > IBE > IBE Encryption



Account notifications sent to users, including expiration notification

Send notifications to the sender, or recipient when the secure email is read, or remains unread

FORTINET Training Institute

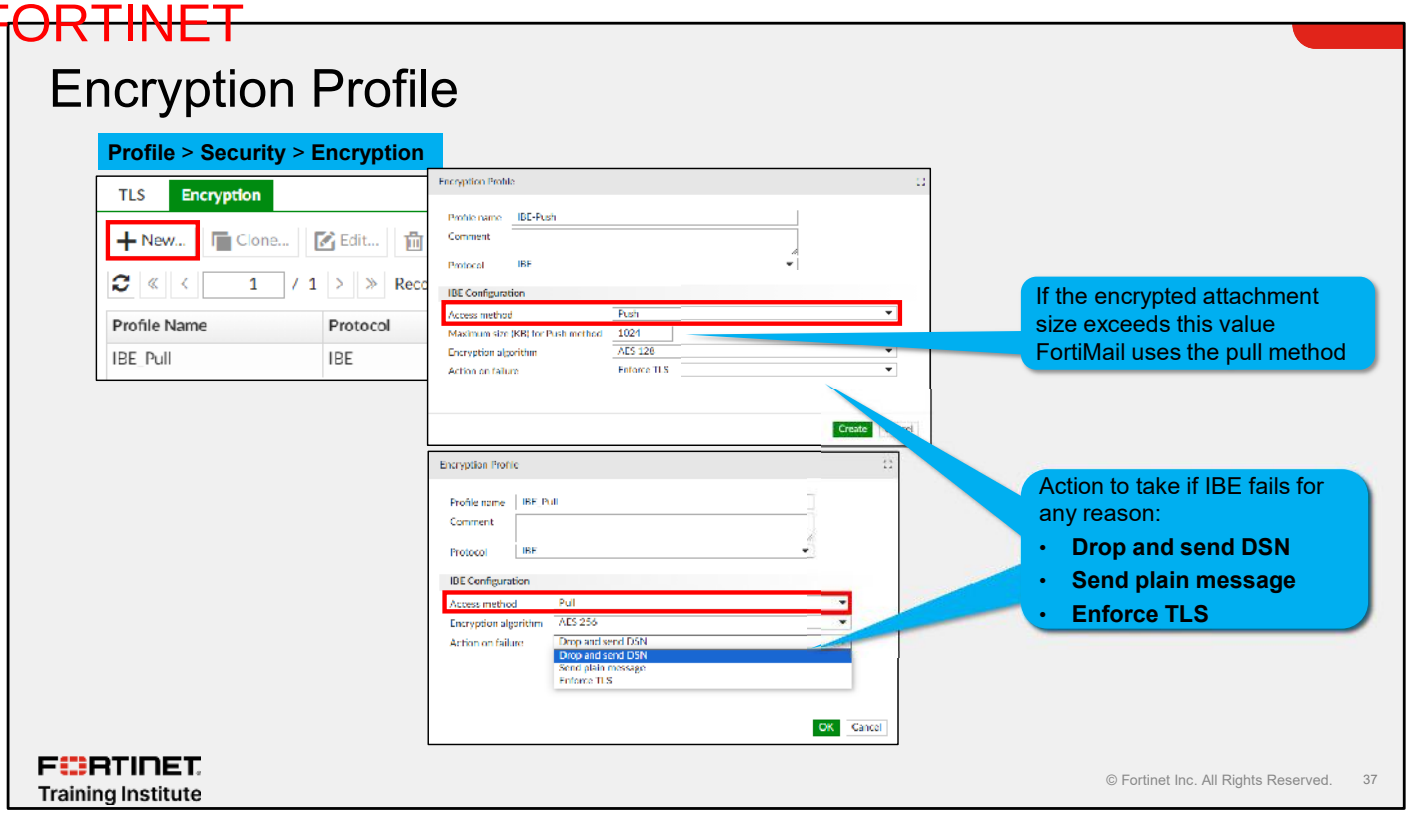
© Fortinet Inc. All Rights Reserved. 36

You can configure the various setting in the **Account Status Notification** section to control the type of notifications you want to send to the IBE recipients. You can enable the **Expiration** and configure settings to control when account expiration notifications should be sent.

The settings in the **Email Status Notification** section allow you to enable or disable notifying the sender or recipient when the secure email is read or remains unread for a specified period.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When IBE encryption is triggered, the encryption profile determines how FortiMail handles the email message.

Options in the encryption profile include which IBE message delivery method FortiMail invokes, as well as which encryption algorithm and strength FortiMail uses.

When FortiMail uses the **Push** method, the maximum size option limits the size of the encrypted attachment. If the encrypted attachment size exceeds this value, FortiMail will revert to the **Pull** method.

To define how FortiMail handles email in the event the IBE service fails, in the **Action on failure** field, select an action. Possible actions include **Drop and send DSN, Send plain message**, and **Enforce TLS**. Since IBE is used for highly confidential emails, it is prudent to use the **Drop and send DSN** failure action in most cases.

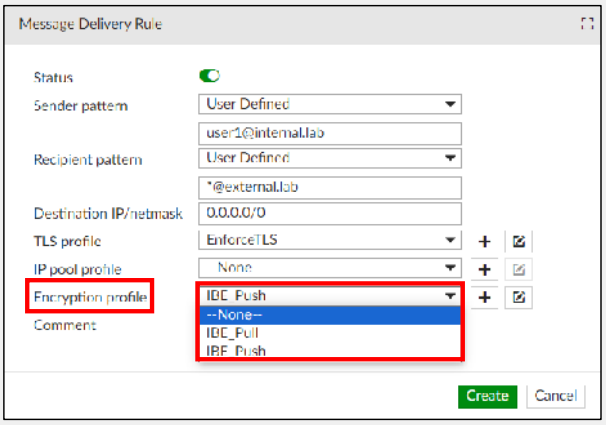
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

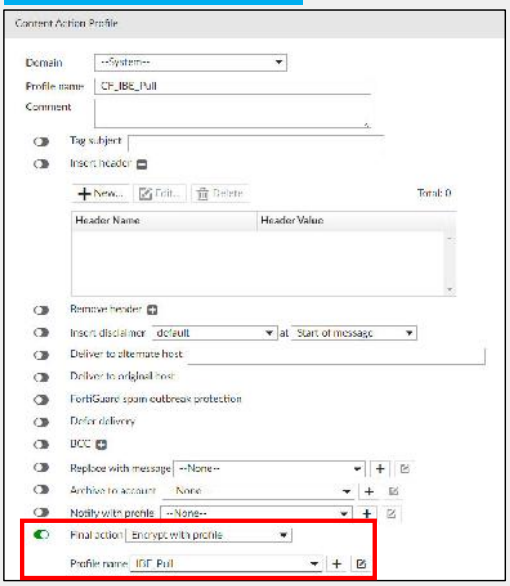
How to Trigger IBE

- Apply an encryption profile using either:
  - Access delivery rule
  - Content action profile

Policy > Access Control > Delivery



Profile > Content > Action



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 38

You can apply encryption profiles using either access delivery rules or content action profiles.

It's not common practice to use access delivery rules to apply IBE because of its rigid matching criteria. A delivery rule always applies the encryption profile to any email messages that match its configured patterns.

It's more common to apply IBE using a content profile **Content Monitor and Filtering** rule that is configured to match a specific trigger word. After the trigger word is matched in an email, the content action profile can apply the encryption profile.

While the latter method is more common, using access delivery rules is still a viable method for testing your IBE configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Content Inspection-Based IBE Configuration Workflow

1. Configure the dictionary profile
   - Establish a trigger word
2. Configure a content action profile to apply an encryption profile
3. Apply the dictionary profile and content action profile to a content profile
4. Apply the content profile to an outbound recipient-based policy

FORTINET Training Institute

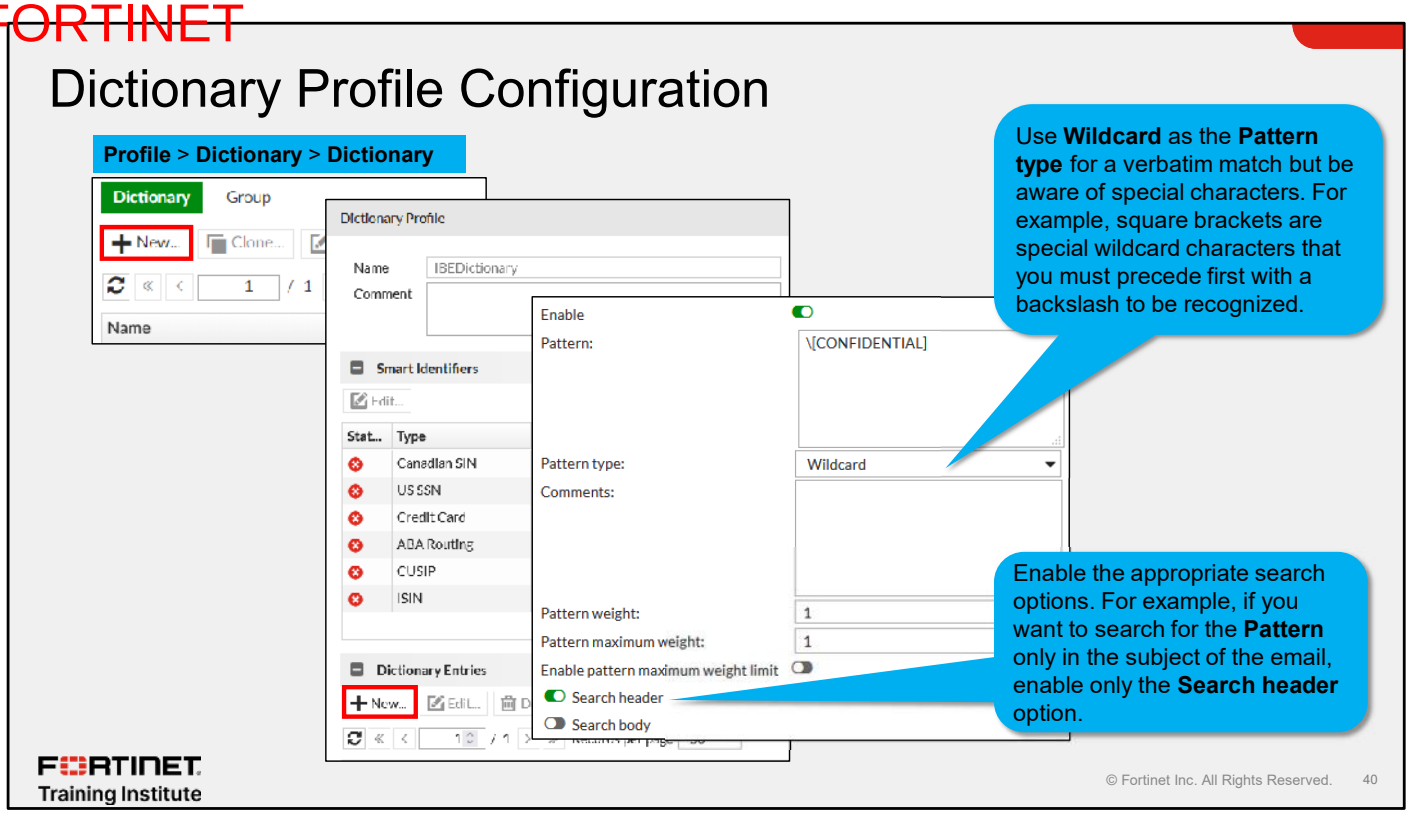
© Fortinet Inc. All Rights Reserved. 39

This slide shows an outline of the configuration steps required to establish IBE, based on content inspection.

First, you must identify a trigger word, and create a dictionary profile using the trigger word. FortiMail applies the dictionary profile to a content profile as a content monitor and filtering rule. When the trigger word is matched, a content action profile applies an encryption profile. An outbound recipient-based policy applies the content profile to all applicable email.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The example on this slide uses the word “confidential” inside square brackets to trigger IBE. You can use wildcard patterns for an exact match or use regular expressions for more complex matching logic. Whichever pattern type you select, be aware of special characters. For example, square brackets are special wildcard characters that must be preceded by a backslash.

Enable the appropriate search options for the dictionary entry. For example, if you want to search for the pattern only in the headers and subject of an email, enable only the **Search header**.

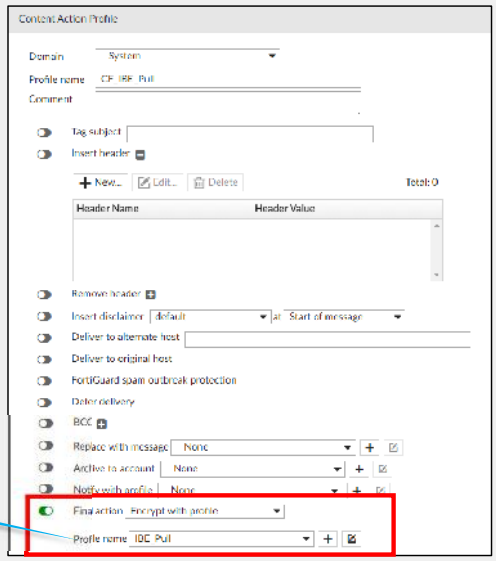
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Content Action Profile Configuration

- Configure **Final action** for encryption
- Select encryption profile

Profile > Content > Action



Encryption profile

FORTINET Training Institute

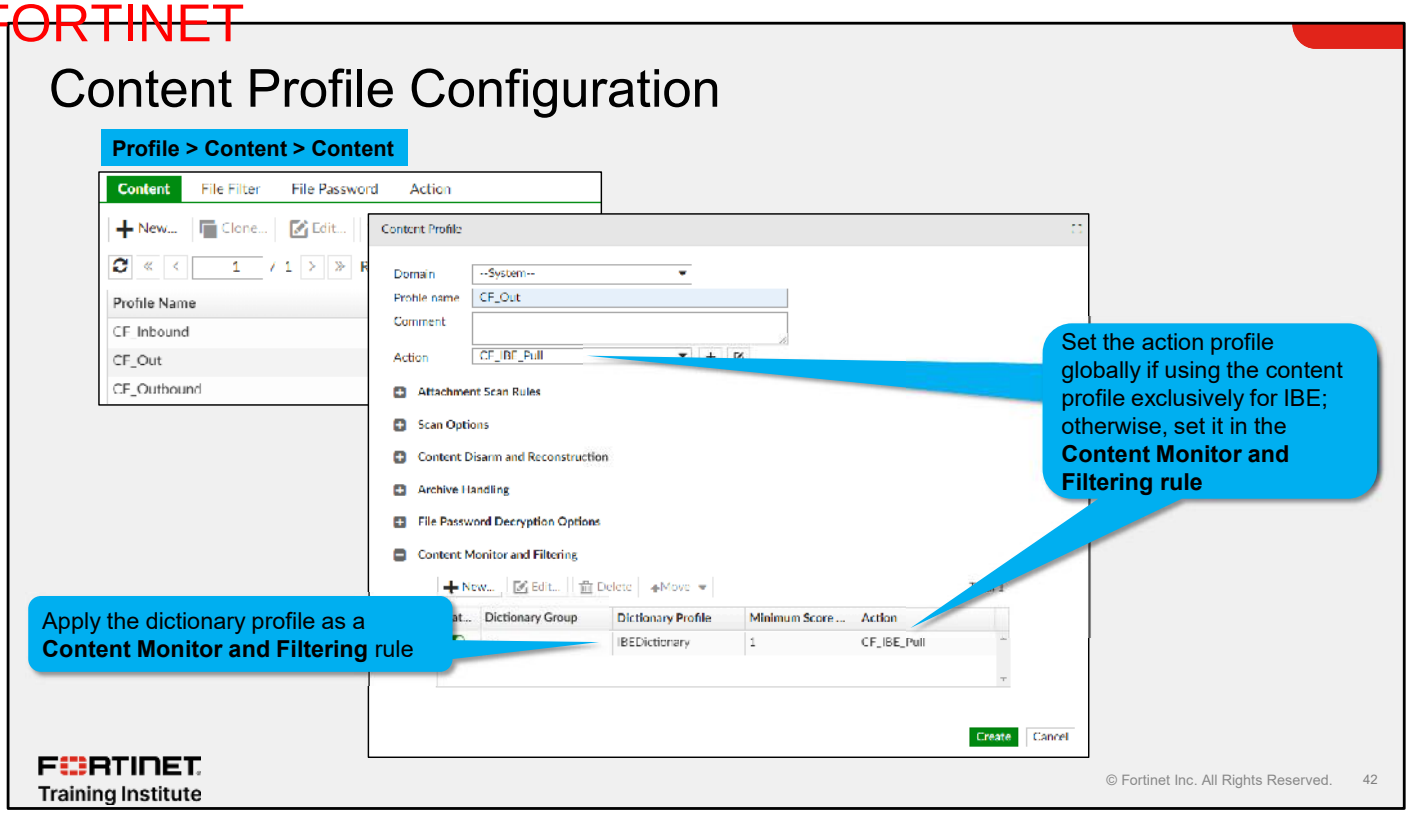
© Fortinet Inc. All Rights Reserved. 41

On the **Content Action Profile** screen, enable **Final action** and select **Encrypt with profile**.

In the **Profile name** field, select the profile name.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



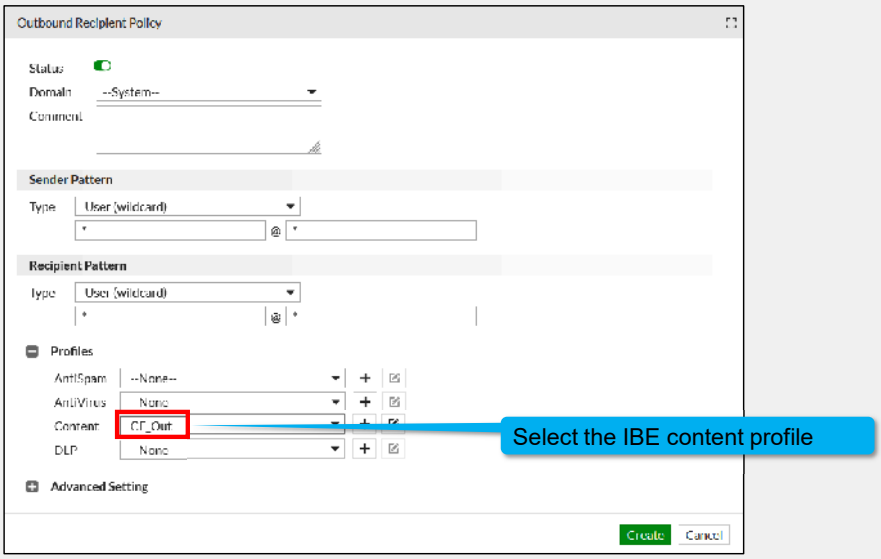
After you create the dictionary profile and content action profiles, you must apply them to a content profile. Apply the dictionary profile as a **Content Monitor and Filtering** rule. Set the **Action** profile globally if you are using the content profile exclusively for IBE. Otherwise, if the content profile is multipurpose, set the appropriate action profile in the **Content Monitor and Filtering** rule.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Recipient Policy Configuration

Policy > Recipient Policy > Outbound



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 43

You should apply the content profile using an outbound recipient-based policy because it provides more configuration flexibility. Recipient policies allow configuration for specific domains or recipients, which IP policies lack.

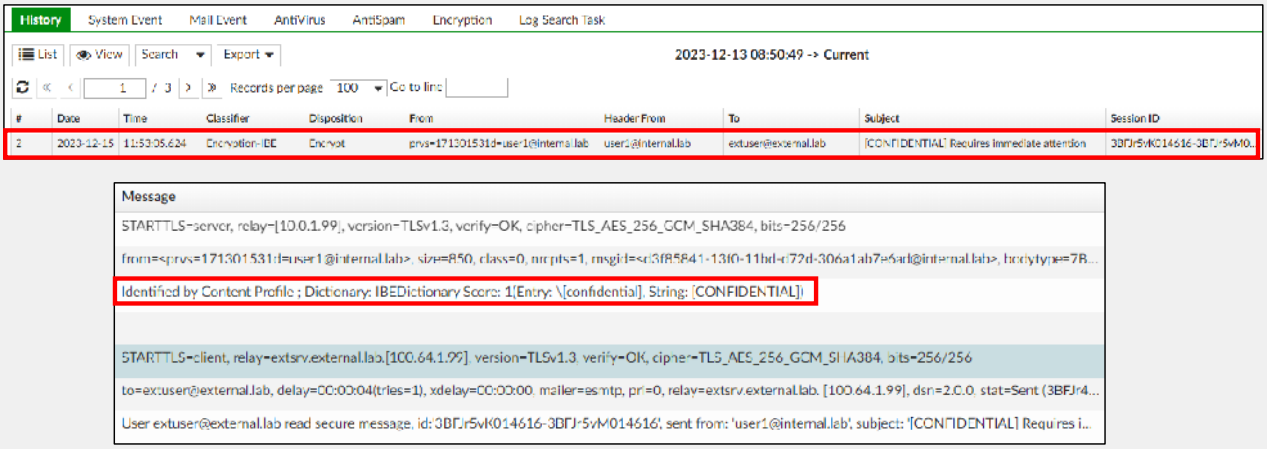
After you apply the content profile to an outbound recipient policy, the IBE feature is ready for you to use.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IBE Logs

Monitor > Log > History



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 44

The **History** tab displays IBE logs with **Encryption-IBE** in the **Classifier** column and **Encrypt** in the **Disposition** column. The cross-search result provides more detail, such as the dictionary profile name and entry that triggered IBE, the IBE method, and the specific word or phrase that triggered the **Content Monitor and Filtering** rule.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Where does the FortiMail administrator enable or disable replying, forwarding, and composing of email messages for IBE users within the secure webmail portal?
   A. Content profile
   ✓ B. IBE encryption settings

2. Which profile can you apply the dictionary profile to in order to trigger IBE?
   A. Antivirus profile
   ✓ B. Authentication profile

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 45

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Encryption
- ✓ IBE Advantage
- ✓ IBE Delivery Methods
- ✓ IBE Configuration
- IBE User Experience
- IBE User Management and Customization

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 46

Good job! You now understand IBE configuration.

Now, you will learn about the user experience with IBE.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IBE User Experience

Objectives

- Access IBE emails

FORTINET Training Institute

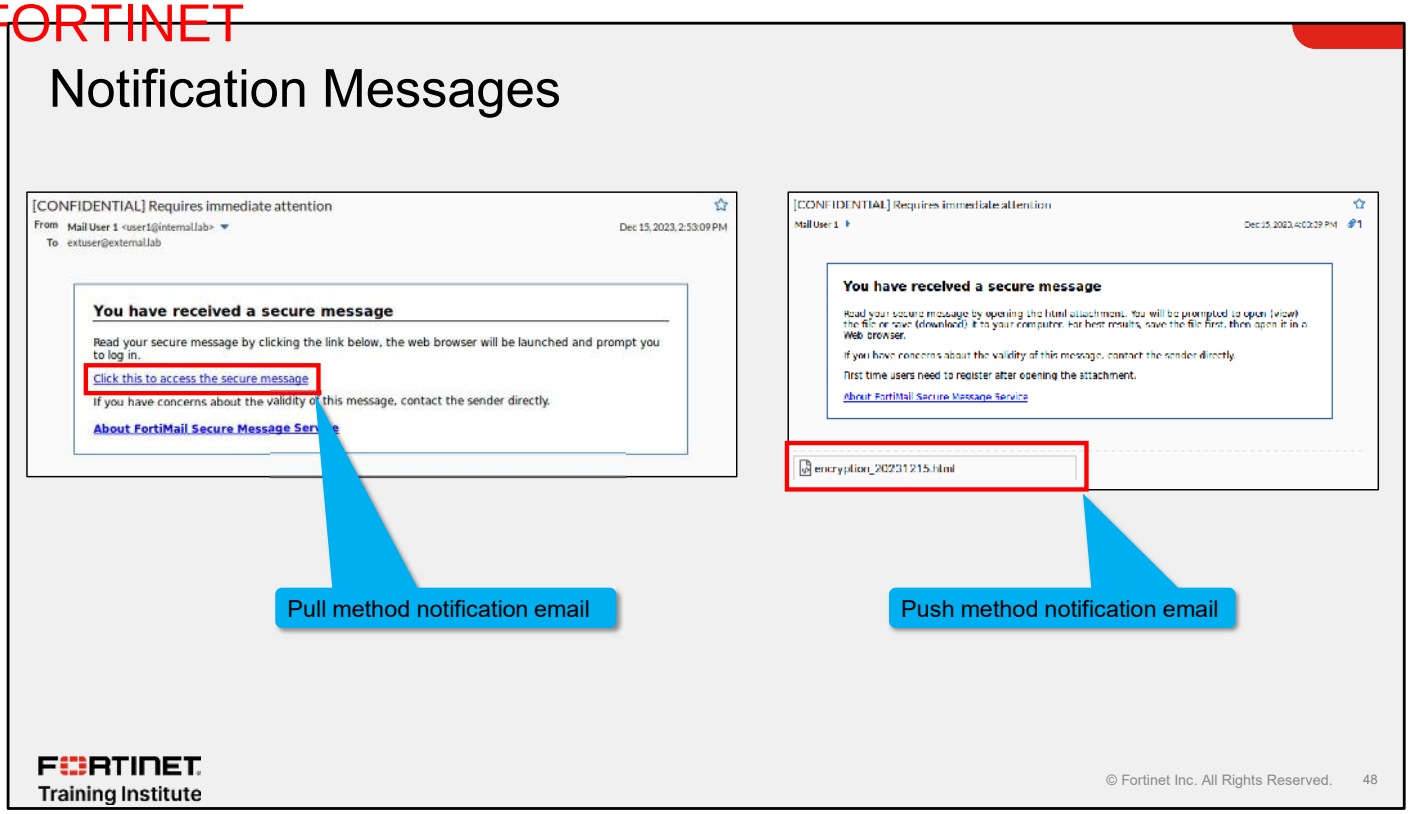
© Fortinet Inc. All Rights Reserved. 47

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in the user experience, you will be able to differentiate between push and pull notification messages, register an IBE user, and access IBE emails.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



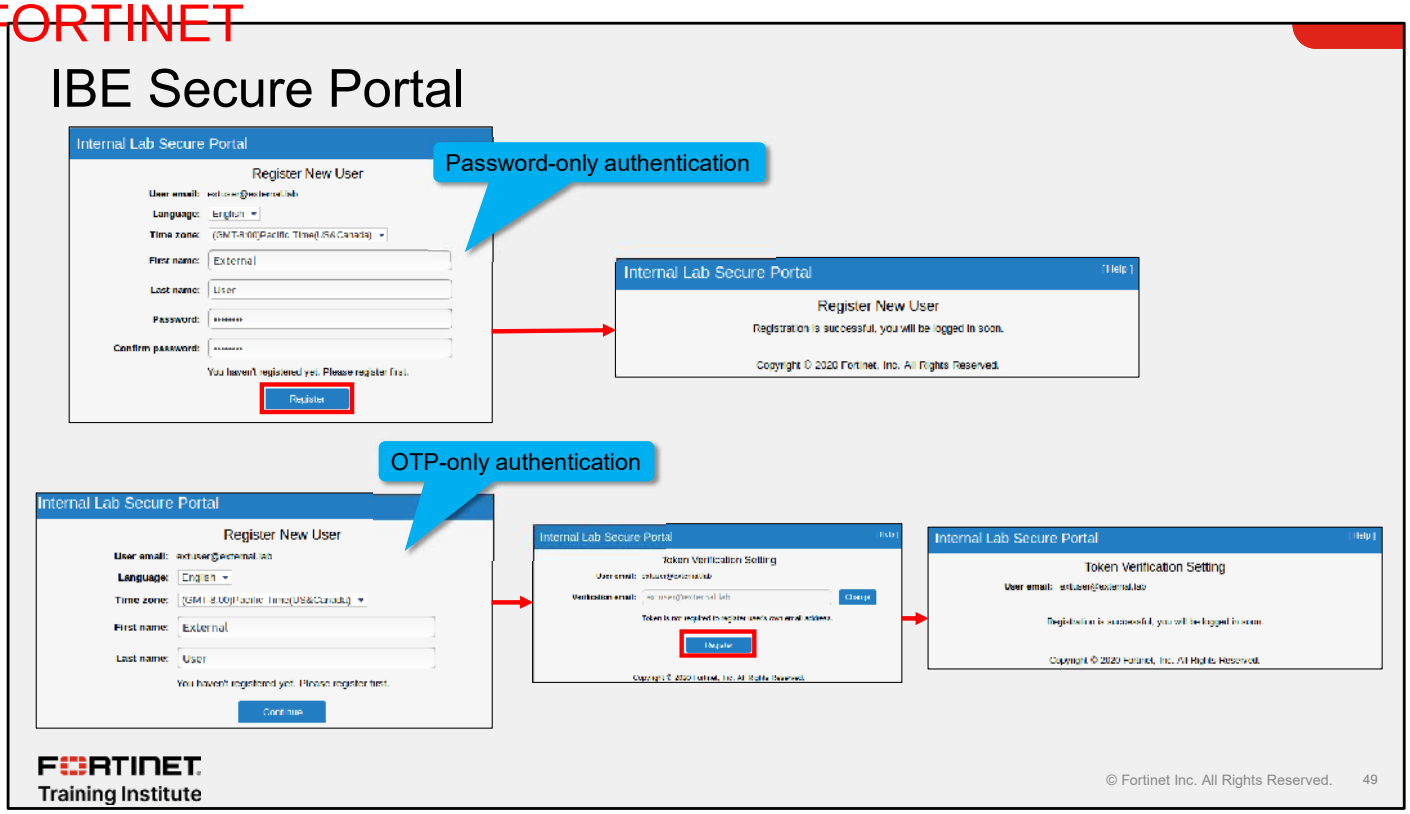
When IBE is triggered to encrypt an email message using the pull method, the recipient receives a notification that a secured email has been sent to them. The notification includes an HTML link that opens a new browser window for the IBE portal on FortiMail.

The push method notification email contains an HTML attachment. When the recipient opens the attachment, a new browser window opens for the IBE portal on FortiMail.

Make sure you configure the correct firewall and destination NAT rules to allow HTTPS access to FortiMail from the internet. Otherwise, the IBE users won't be able to reach the FortiMail IBE portal.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

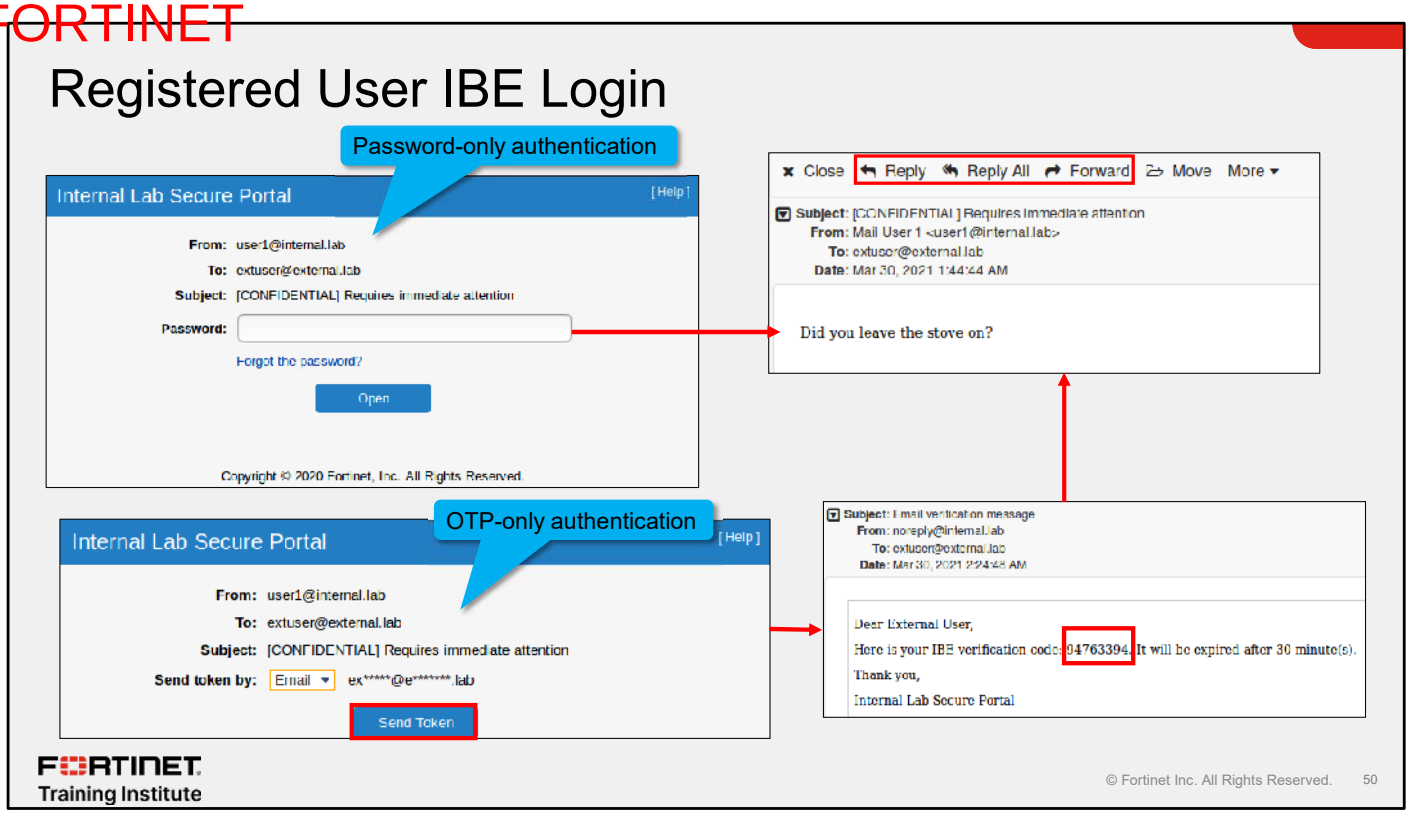


A first-time user is prompted to register as an IBE user.

To register, a new user must submit their first name, last name and password (if selected under IBE settings). Starting with FortiMail 6.4, two-factor authentication and one-time password (OTP) are also supported for IBE authentication. If OTP is used for then the IBE user does not have to provide a password during registration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After registration, users can enter their password or request a token through SMS or email, to view the secured message in a standard FortiMail webmail interface. If you enable secure replying and forwarding, those controls appear on the interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which token authentication method is supported by FortiMail for IBE authentication?
   A. FortiToken
   ✓ B. Email/SMS

2. Which protocol needs to be allowed for IBE users to reach the FortiMail IBE portal from the internet?
   ✓ A. HTTPS
   B. SMTPS

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 51

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- ✓ Encryption
- ✓ IBE Advantage
- ✓ IBE Delivery Methods
- ✓ IBE Configuration
- ✓ IBE User Experience
- IBE User Management and Customization

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 52

Good job! You now understand the user experience.

Now, you will learn about IBE user management and customization.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

IBE User Management and Customization

Objectives

- Manage IBE users and settings

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 53

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in IBE user management and configuration, you will be able to manage IBE users and customize IBE settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

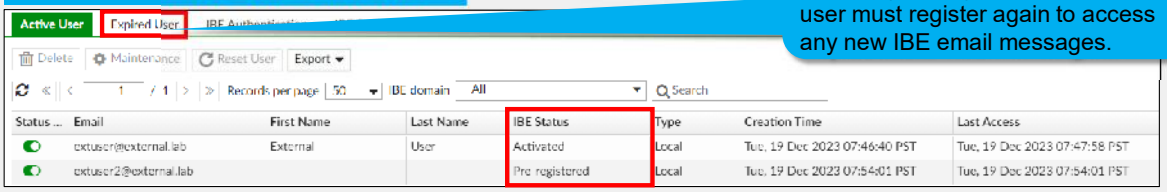
DO NOT REPRINT Brave-dumps.com
© FORTINET

IBE User Management

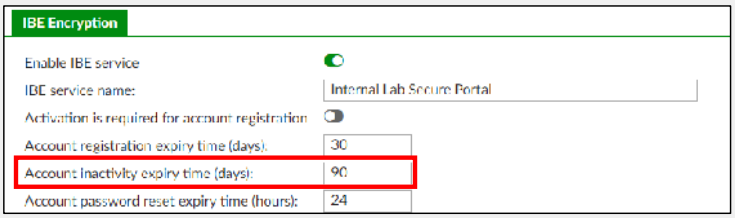
- **Activated**: User successfully registered
- **Pre-registered**: IBE notification email sent

An IBE user is moved to the **Expired User** tab after the **User inactivity expiry time** elapses. The user must register again to access any new IBE email messages.

Domain & User > IBE User > Active User



Encryption > IBE > IBE Encryption



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 54

The system creates IBE user accounts automatically whenever an IBE message is sent to a new recipient. Until a new IBE user registers, their account status is listed as **Pre-registered** in the IBE user list. After they register, the status changes to **Activated**. An IBE user account remains in the active state until the account expires because of inactivity. You can set the length of time before an inactive account expires in the global IBE configuration settings. An expired user must register their account again to access any new IBE emails.

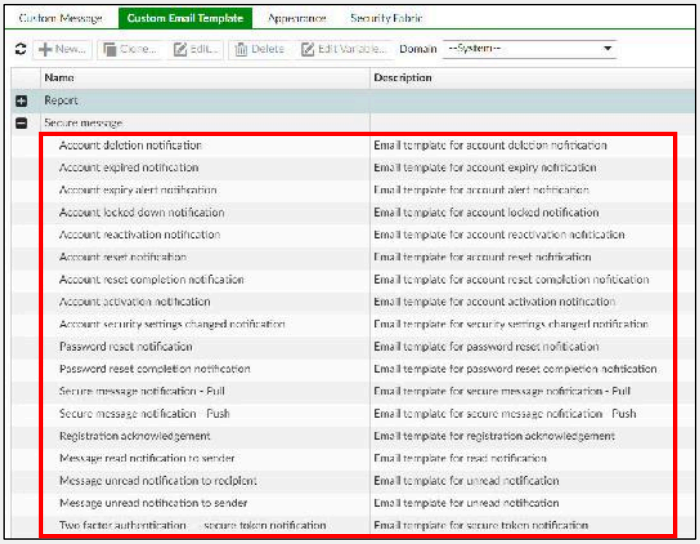
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Customization

System > Customization > Custom Message

System > Customization > Custom Email Template



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 55

FortiMail allows you to customize the IBE login page, user registration page, and email notifications. You must modify the HTML code to rebrand the pages for your organization.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Until a new IBE user registers, what is their account status in the IBE user list?
   A. Activated
   ✓ B. Pre-registered

2. When is an IBE user moved to the expired user tab?
   ✓ A. After the user inactivity expiry time
   B. When the IBE email is read and deleted

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 56

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Progress

- Encryption
- IBE Advantage
- IBE Delivery Methods
- IBE Configuration
- IBE User Experience
- IBE User Management and Customization

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 57

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in the lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Configure SMTPS
- ✓ Manage TLS encryption with TLS profiles and access control rules
- ✓ Differentiate between traditional email encryption methods and IBE
- ✓ Differentiate between push and pull delivery methods
- ✓ Configure encryption profiles for different IBE methods
- ✓ Verify IBE events using logs
- ✓ Access IBE emails
- ✓ Manage IBE users and settings

FORTINET Training Institute

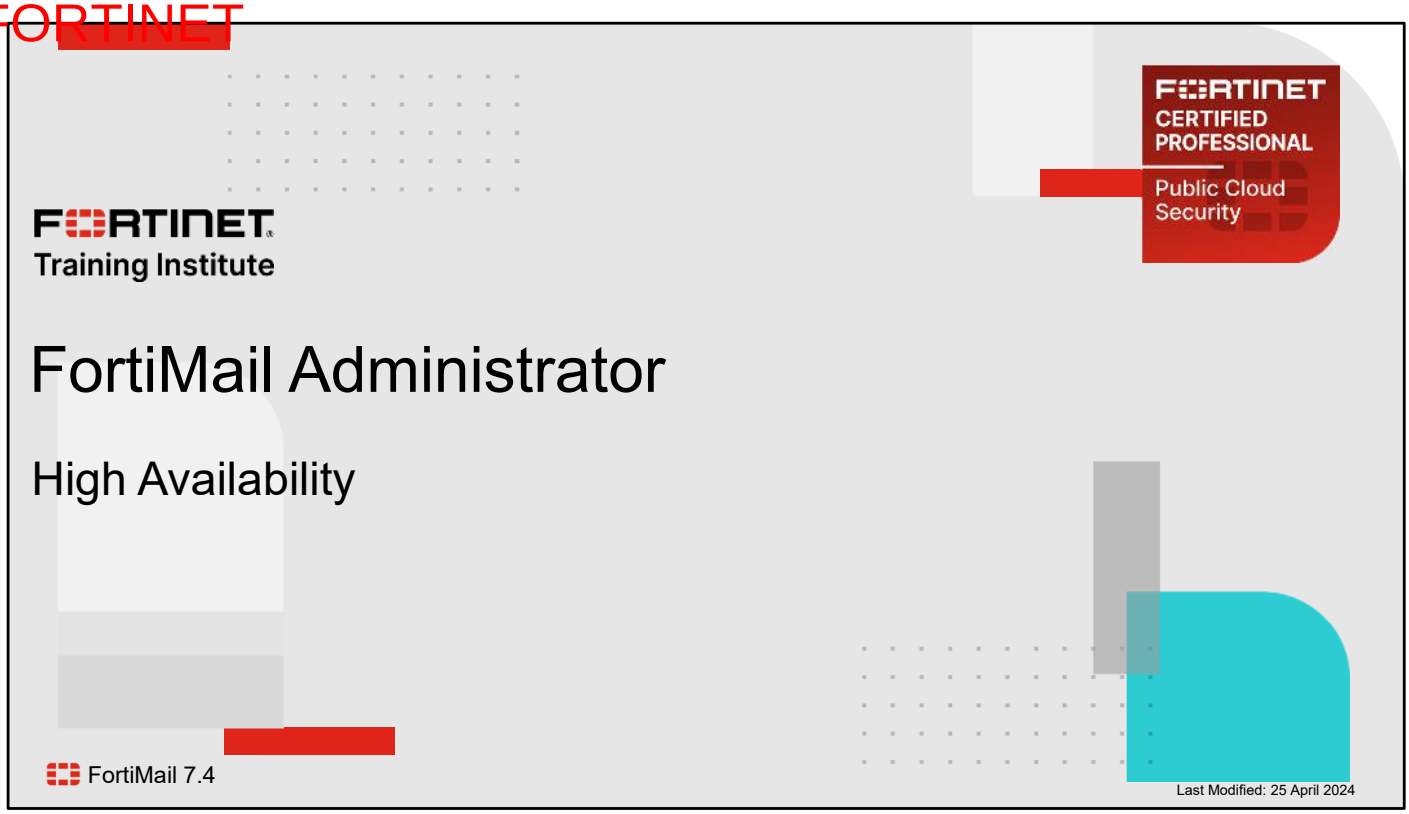
© Fortinet Inc. All Rights Reserved. 58

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about the diverse methods for securing communications on FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to deploy and configure FortiMail in high availability (HA) mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Lesson Overview

- FortiMail HA
- Active-Active Mode
- Active-Passive Mode
- Managing FortiMail HA Clusters

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 2

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiMail HA

Objectives

- Identify FortiMail HA modes and their benefits
- Differentiate the synchronization behavior between HA modes

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 3

After completing this section, you should be able to achieve the objectives shown on this slide.

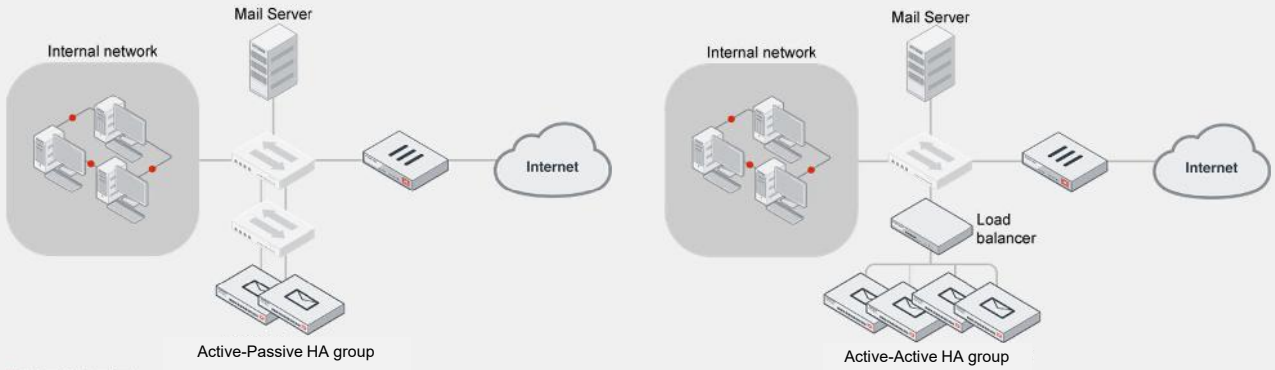
By demonstrating competence in FortiMail HA, you will be able to identify the different HA modes and differentiate synchronization behavior between HA modes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

HA Modes

- Active-Passive
  - Configuration and mail data synchronized between two FortiMail devices for failover protection
- Active-Active
  - Configuration synchronized for up to 24 FortiMail devices that each operate independently
  - Typically deployed behind a load balancer for increased processing capacity and redundancy



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

FortiMail supports two different modes of HA: active-passive and active-active.

Active-passive HA is a traditional pair-based architecture in which one FortiMail acts as the primary device and a second acts as the secondary device, standing by to take over processing if the primary device fails. FortiMail uses heartbeat connections to synchronize the configuration and the stateful mail data, to ensure no data is lost.

Active-active mode HA allows larger clusters, containing up to 24 FortiMail devices, to be built to provide increased processing capacity in larger environments. In an active-active cluster, all the standby devices synchronize their configuration with the primary device.

The FortiMail HA architecture also supports clusters that include mismatched hardware. For example, you can build an active-passive cluster using a FortiMail 200F and a FortiMail 400F. However, the cluster is limited to the hardware and software limitations of the device with the lowest model number.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configuration Synchronization

- All configuration settings on the primary device are synchronized with the secondary device, except the following:

All HA Modes	
Operation mode	SNMP system information
Host name	RAID configuration
Static routes	HA configuration
Gateway and server mode interface configuration	HA service monitoring configuration
Transparent mode management IP address	Product name and icon

Active-Active HA	
Everything from the **All HA Modes** table	IP pools
Local domain name	Quarantine report host name
Default certificates	IBE base URL, help URL, and about URL
iSCSI initiator name	Centralized quarantine client IP address
iSCSI ID for remote storage	Centralized IBE IP address
SNMP settings	

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

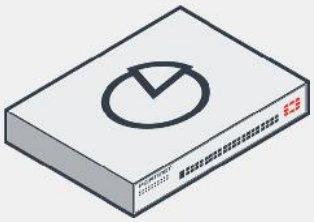
In both active-active and active-passive modes, you must always manage the entire cluster's configuration on the primary FortiMail, except for settings that aren't synchronized. Not all configuration items are synchronized between clustered devices. For the unsynchronized elements listed in the tables, you must access the secondary devices to modify their values.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Logging and HA

- The configuration of an HA cluster may be synchronized but mail queues and logs may be stored in multiple locations
  - In an active-passive, the relevant logs are on the FortiMail device that is actively passing traffic
  - In an active-active cluster, the logs are spread across every FortiMail device that is passing traffic
  - In active-active mode, you can use external storage to unify the mail queue and quarantine mailboxes
- In HA configurations, centralize logging in one location so that logs are easier to search:
  - FortiAnalyzer (FAZ)
  - Syslog server
  - Centralized monitoring license feature



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

Members of an HA cluster do not share logging information or mail queues. It is important in active-active mode to have external storage so all members can have a centralized mail queue and quarantine repository.

Logging information is stored on the local FortiMail device that transmits the email. If centralized logging is required, you must configure FortiMail to send logging information to a centralized server like FortiAnalyzer or a syslog server. You can acquire a separate centralized monitoring license to enable the primary cluster member to search the log files of the members of a cluster.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

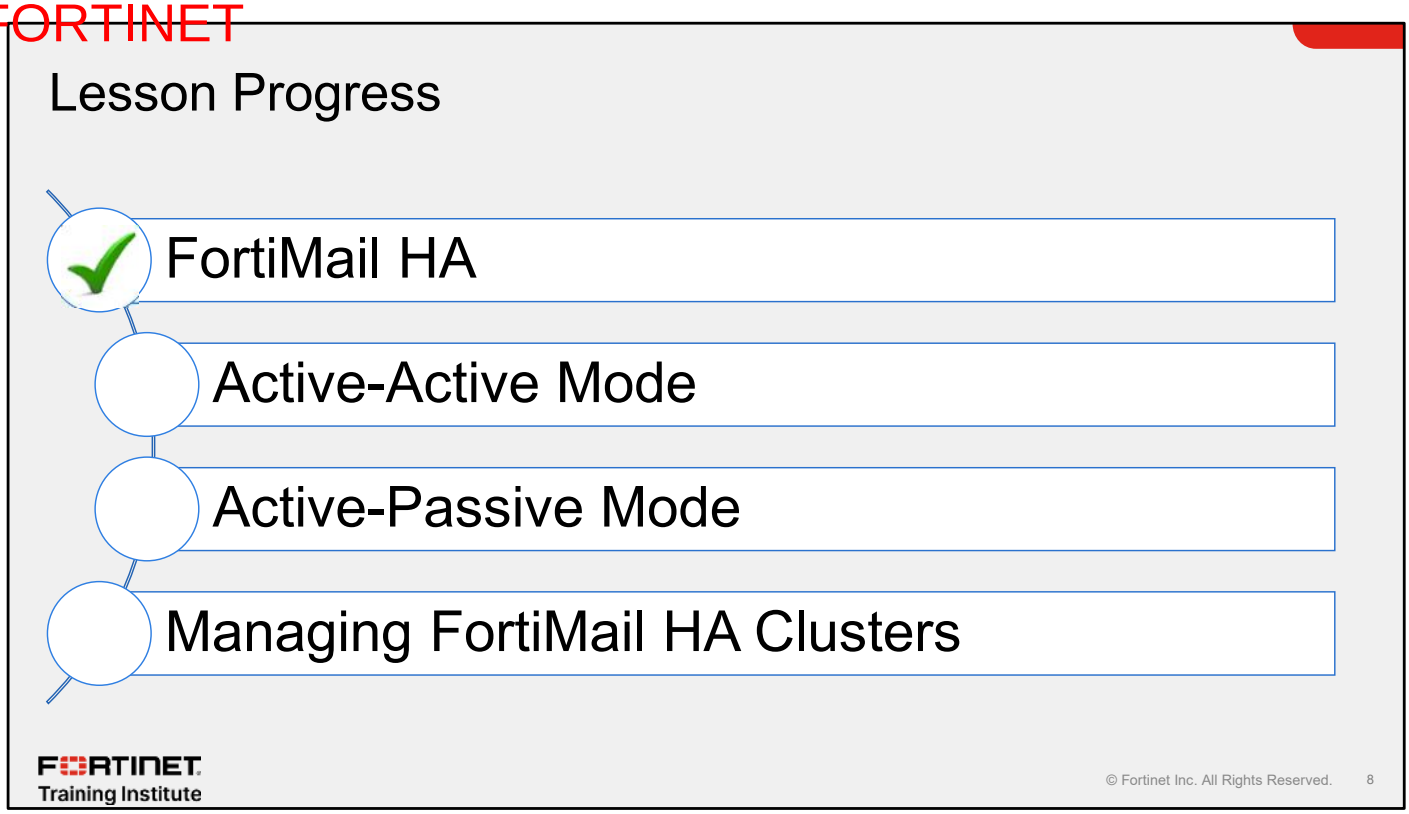
1. What is the maximum number of devices that an active-active HA cluster can support?
   - ✓ A. 24
   - B. 16
2. Which configuration element does FortiMail synchronize only when deployed in active-active mode?
   - A. Operation mode
   - ✓ B. Local domain name

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Good job! You now understand FortiMail HA.

Now, you will learn about active-active HA mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Active-Active Mode

Objectives

- Identify requirements for active-active cluster implementation
- Configure active-active FortiMail clusters

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

After completing this section, you should be able to achieve the objectives shown on this slide.

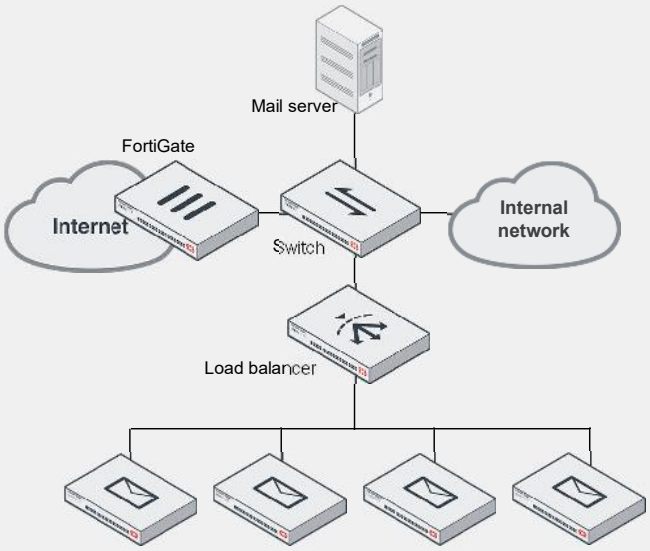
By demonstrating competence in active-active mode, you will be able to identify requirements for active-active cluster implementation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Active-Active Clusters

- Each device operates independently
- Typically deployed behind a load balancer
- Server mode clusters are usually operated as a server farm
- External storage is recommended for gateway and transparent mode clusters to provide centralized quarantine
- External storage is *required* to store mail data for server mode clusters



Active-Active Cluster

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

Although their configurations are kept in sync, active-active cluster members operate independently of each other, handling SMTP connections and performing their configured scans individually. Because their configurations are identical, active-active clusters in gateway mode or transparent mode are often positioned behind a load balancer, multiplying the capacity over that of any single FortiMail instance. Another use case for active-active clusters is to deploy them in server mode to maintain an email server farm.

The members of the cluster are operational peers of each other, because they process the email traffic. However, one member is elected as the configuration primary and all configuration changes are made on that device. Any configuration changes made on the configuration primary are instantly propagated to the other devices, keeping them synchronized.

The main motivation for deploying active-active HA clusters is to create increased capacity. However, when positioned behind load balancers, a measure of HA or redundancy is also provided. If a device fails, the load balancer stops sending traffic to the failed device and shares the traffic with the rest of the remaining devices.

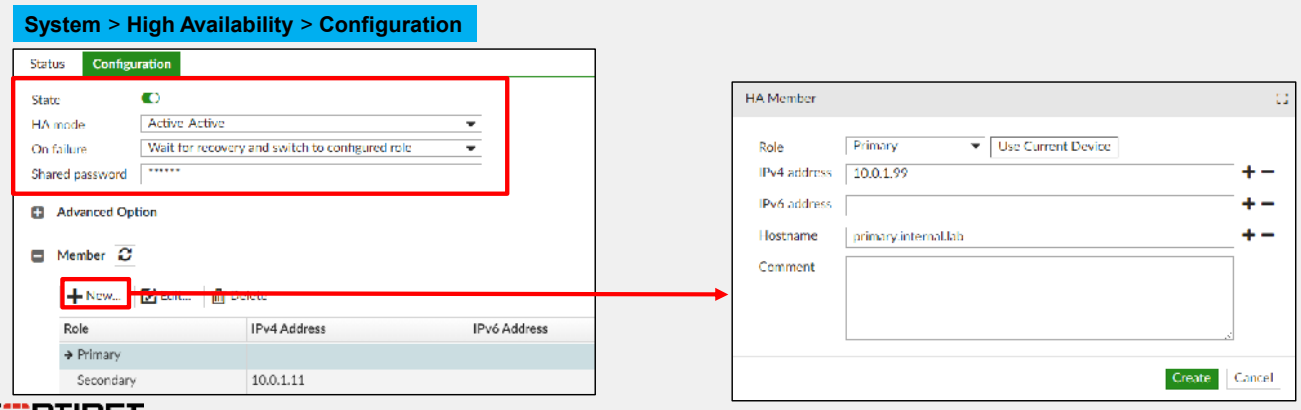
Each FortiMail in the cluster maintains its own set of mail transfer agent (MTA) queues and mail storage, which are not synchronized across the devices. Any messages held in a queue when a device fails, are lost. For this reason, you should use an external network attached storage (NAS) device for gateway or transparent mode clusters. Server mode clusters require external NAS storage; otherwise, user mailbox data becomes incoherent because it’s spread randomly across the devices in the server farm.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Active-Active HA Configuration

- For each cluster member:
  - Enable HA
  - Set **HA mode** to **Active-Active**
  - Set **On failure** action
  - Type the shared password
- Each cluster member is added to the **Member** section
  - Only one cluster member will have the primary role



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

To create an active-active HA cluster, in the **HA mode** field, select **Active-Active**. The action you select in the **On failure** field determines how the cluster behaves after a failure:

- If you select **Switch off**, the failed device's mode of operation is set to off. In this state, the device is not part of the cluster and doesn't process email. To restore the device, you must manually select an HA mode.
- If you select **Wait for recovery then switch to original role**, the failed device, after recovery, returns to its original HA mode. For example, if a device's HA mode was primary before failure, after recovery, it resumes its primary role.
- If you select **Wait for recovery then restore secondary role**, if the device fails after recovery, it will remain in the secondary role.

Enter a **Shared password**. This password is shared by all members of the cluster.

In the **Member** section, you must add all the devices that will participate in the active-active cluster. Only one of these devices can be configured with the **Primary** role.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. What is the primary motivator for deploying an active-active cluster?
   - ✓ A. Redundancy
   - B. Increased storage and logging capacity

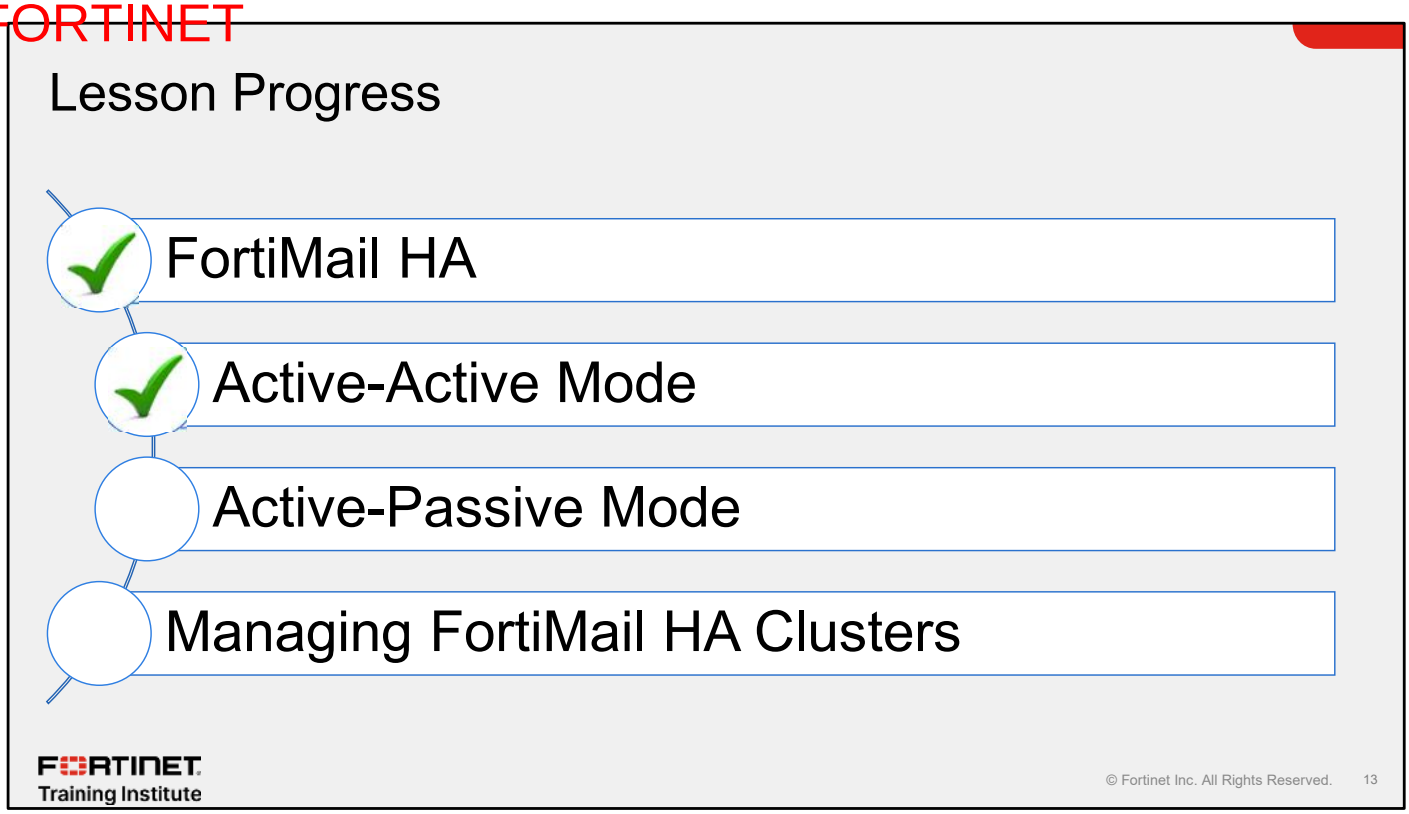
2. Which statement about an active-active HA cluster is true?
   - A. In an active-active HA cluster, only the primary device processes email.
   - ✓ B. An active-active HA cluster is typically deployed behind a load balancer.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Good job! You now understand active-active HA mode.

Now, you will learn about active-passive HA mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Active-Passive Mode

Objectives

- Identify requirements for active-passive cluster implementation
- Configure active-passive FortiMail clusters

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

After completing this section, you should be able to achieve the objectives shown on this slide.

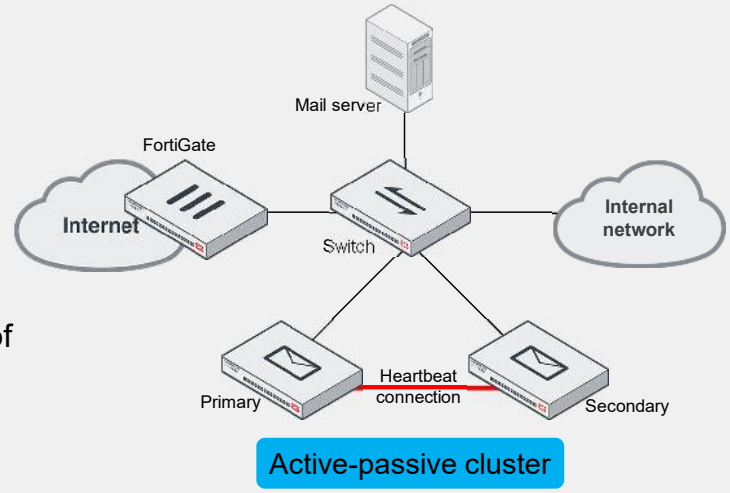
By demonstrating competence in active-passive mode, you will be able to identify requirements for active-passive cluster implementation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Active-Passive Clusters

- Primary device performs all the work, such as email processing and FortiMail services
- Secondary device monitors the primary device for failure using the heartbeat connection
- Synchronized configuration and mail data
- Failover happens with minimal chance of data loss



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

Active-passive HA clusters operate in the traditional fashion, in which the primary device performs all the email processing, and the secondary device monitors the primary device, ready to take over the services if the primary device fails.

While the cluster is operating, the active device synchronizes not only the configuration, but all email data, such as the MTA queues, the user's quarantined messages, identity-based encryption (IBE) messages, and, for server mode, the user mailboxes. Because the secondary device has all the data that is on the primary device, a failover can occur without any data loss. Additionally, any SMTP sessions interrupted during the failover are retransmitted by the sender, so no email is lost.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Heartbeat

- Keepalive mechanism between clustered devices
  - Secondary device monitors heartbeat packets from the primary device
  - Absence of heartbeat packets triggers failover
- Primary heartbeat interface
  - Handles both heartbeat and synchronization
- Secondary heartbeat interface
  - Handles the heartbeat while the primary performs synchronization
- Use dedicated links, isolated subnets, or VLANs

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

FortiMail uses heartbeat packets as a keepalive mechanism between clustered devices. The secondary device monitors heartbeat packets from the primary device. If the heartbeat is undetected for 30 seconds(default), the secondary device takes over.

At minimum, you must set a network interface on each device as the primary heartbeat interface. If you use only a primary heartbeat, then the primary interface carries the heartbeats, as well as all the configuration synchronization and email data replication traffic. For increased reliability, you should configure secondary heartbeat interfaces in addition to the primary interface. When a secondary heartbeat link exists, the traffic load is divided between the primary interface that is handling the synchronization and replication traffic, and the secondary interface dedicated only to the heartbeat.

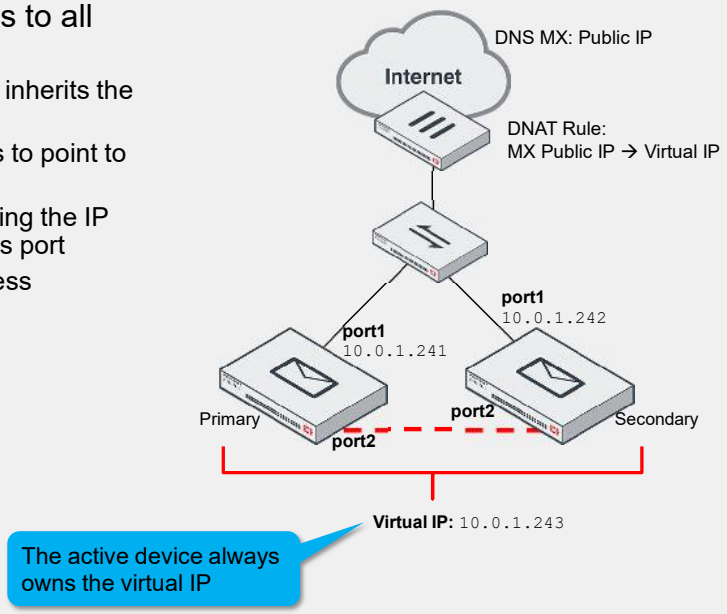
You should configure heartbeat interfaces to use dedicated links. If that’s not possible, use isolated subnets or VLANs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Virtual IP

- Primary device, while active, responds to all ARP requests for the virtual IP
  - If a failover occurs, the secondary device inherits the same virtual IP address
  - You should configure all DNS MX records to point to the virtual IP address
  - You can still access individual devices using the IP address of their dedicated network access port
  - Can be used for both email and GUI access



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

Active-passive HA clusters use a virtual IP address for email processing and other user-facing services. If a failover occurs, the secondary device inherits this virtual IP address. For clustering to work correctly, the virtual IP address must be the address used in all domain name system (DNS) mail exchange (MX) records. Or, the appropriate firewall rules must be in place to perform destination network address translation (DNAT)—from DNS MX public IP addresses to the cluster's virtual IP address. This way, any failover event is transparent to the rest of the IP infrastructure.

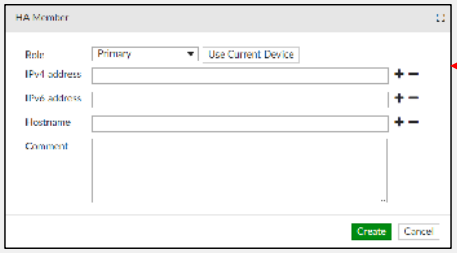
While the cluster shares a virtual IP address, you can access each device individually using the IP address of its dedicated network access port.

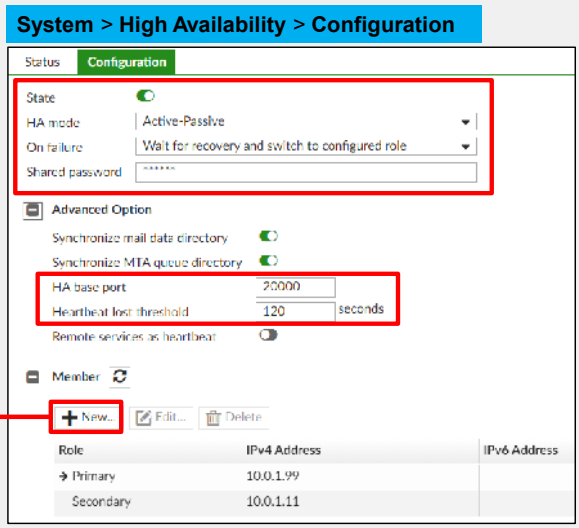
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Active-Passive Configuration

- **HA mode**: Select **Active-Passive**
- Select one of the following options in the **On failure** field:
  - **Switch off immediately**
  - **Wait for recovery**
  - **Wait for recovery and switch to configured role**
- In the **Shared password** field, type a shared password
- Add primary and secondary members





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

To configure an active-passive cluster, in the **HA mode** field, select **Active-Passive**. The action you select in the **On failure** field determines how the cluster behaves after a failure. These options work the same as they do in the active-active configuration.

You should select **Wait for recovery and switch to configured role** because it gives you time to investigate the cause of a failure before putting the device back into operation.

You must also type a shared password and configure the backup options.

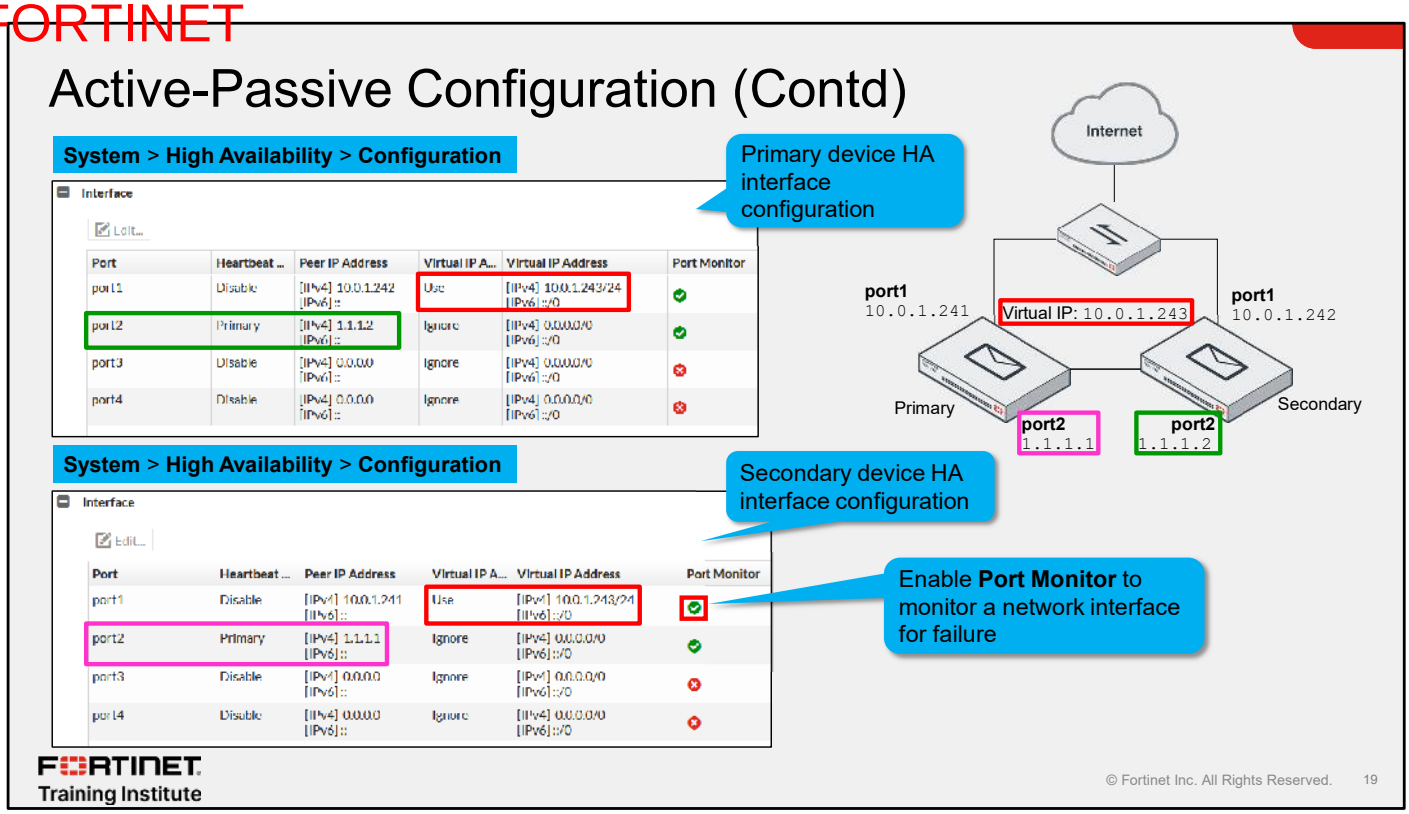
The **HA base port** value specifies the TCP ports that are used for heartbeat signal, sync control, data sync, and configuration sync.

You can also configure the **Heartbeat lost threshold** value. This is the amount of time, in seconds, that the primary device can be unresponsive for before it triggers a failover to the secondary device.

In the **Member** section, you must add all devices that will participate in the active-passive cluster. Only one of these devices can be configured with the **Primary** role.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Each clustered device requires at least one primary heartbeat interface, a peer device IP address, and the virtual IP address.

To designate an interface as a heartbeat interface, you must select a heartbeat status (primary or secondary), and enter a peer IP address. In the example shown on this slide, port2 has been designated as the primary heartbeat interface on both devices, because it is directly connected by a dedicated link.

You should designate the interface that is connected to the rest of the network as the virtual IP address. In the example show on this slide, this is port1 on both devices.

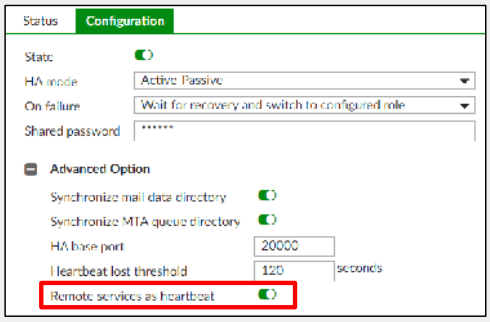
You can also enable the **Port Monitor** option to monitor a network interface for failure. If there is a port failure on the active device, it triggers a failover to the secondary device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

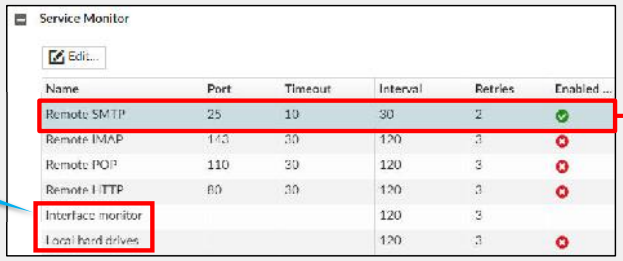
Remote Services as a Heartbeat

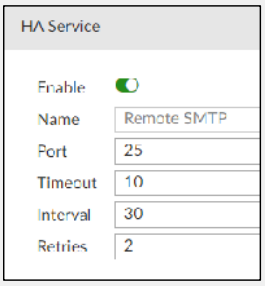
System > High Availability > Configuration



- Standby device can monitor services on the active device
  - SMTP, POP, IMAP, HTTP
- Triggers a failover if any of the monitored services become unresponsive

Local services tested by the active device





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

The HA service monitor provides an optional way to verify the status of the active device, beyond the heartbeat interfaces. On the standby device, the service monitor can check the status of the network services running on the active device, such as SMTP, POP, IMAP, and HTTP. A failure of any of these services can then be used in the decision to trigger a failover event. On the active device, the service monitor can monitor the proper operation of local network interfaces and local hard drives.

You should configure each device independently, with the appropriate service monitors for the situation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. In an active-passive deployment, which cluster node responds to ARP requests for the configured virtual IP?
   - ✓ A. Active device
   - B. Passive device

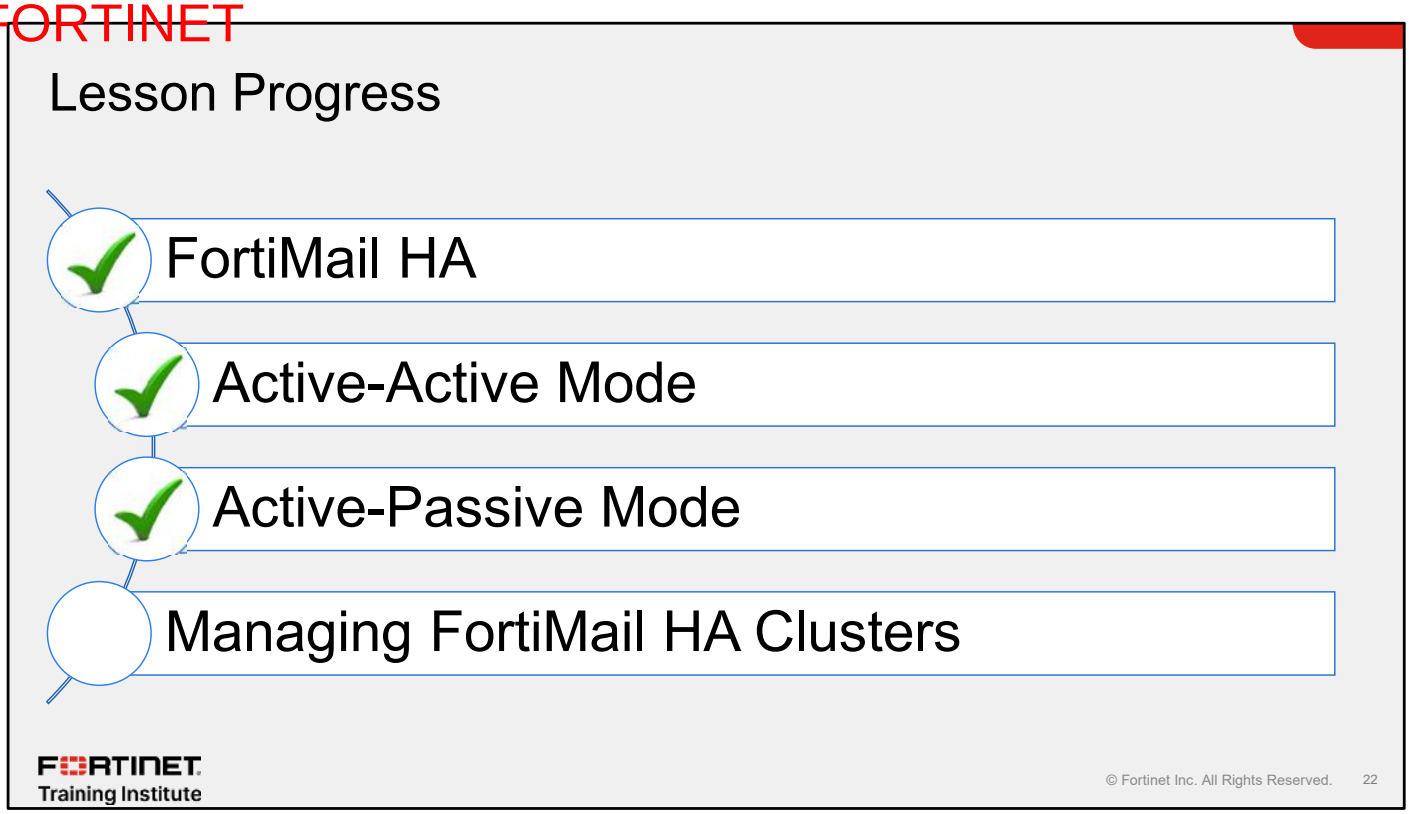
2. What is the purpose of a secondary heartbeat interface?
   - A. It acts as a redundant heartbeat monitor if the primary interface fails.
   - ✓ B. It handles the heartbeat while the primary performs synchronization.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Good job! You now understand active-passive HA mode.

Now, you will learn about managing FortiMail HA clusters.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Managing FortiMail HA Clusters

Objectives

- Monitor a FortiMail HA cluster centrally
- Manage HA operations on clustered devices
- Upgrade FortiMail cluster firmware

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

After completing this section, you should be able to achieve the objectives shown on this slide.

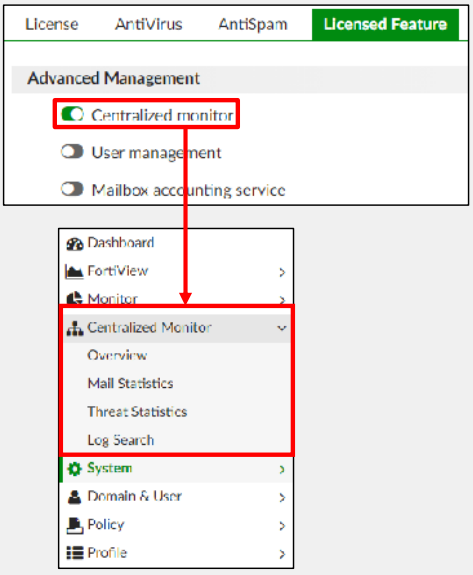
By demonstrating competence in managing FortiMail HA clusters, you will be able to manage HA operations on clustered devices and upgrade a FortiMail HA cluster.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

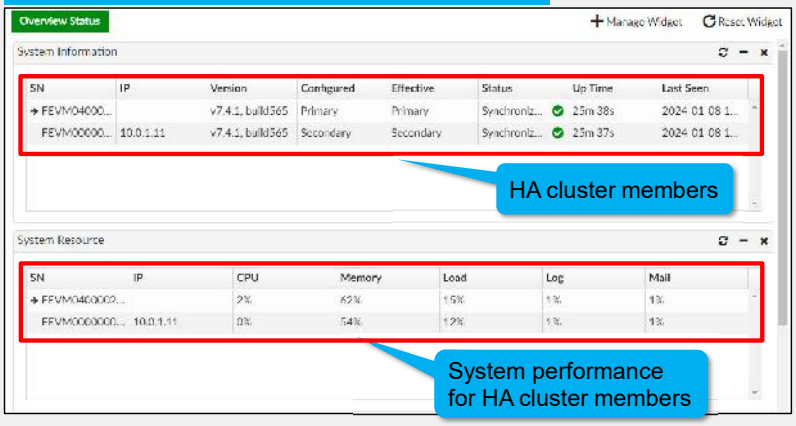
Monitor a FortiMail HA Cluster Centrally

System > FortiGuard > Licensed Feature



- Available only with an Advanced Admin and MSSP license add-on
- Status, performance, and statistics from all cluster members available on the primary device
- Enables cross-device log search

Centralized Monitor > Overview > Overview Status



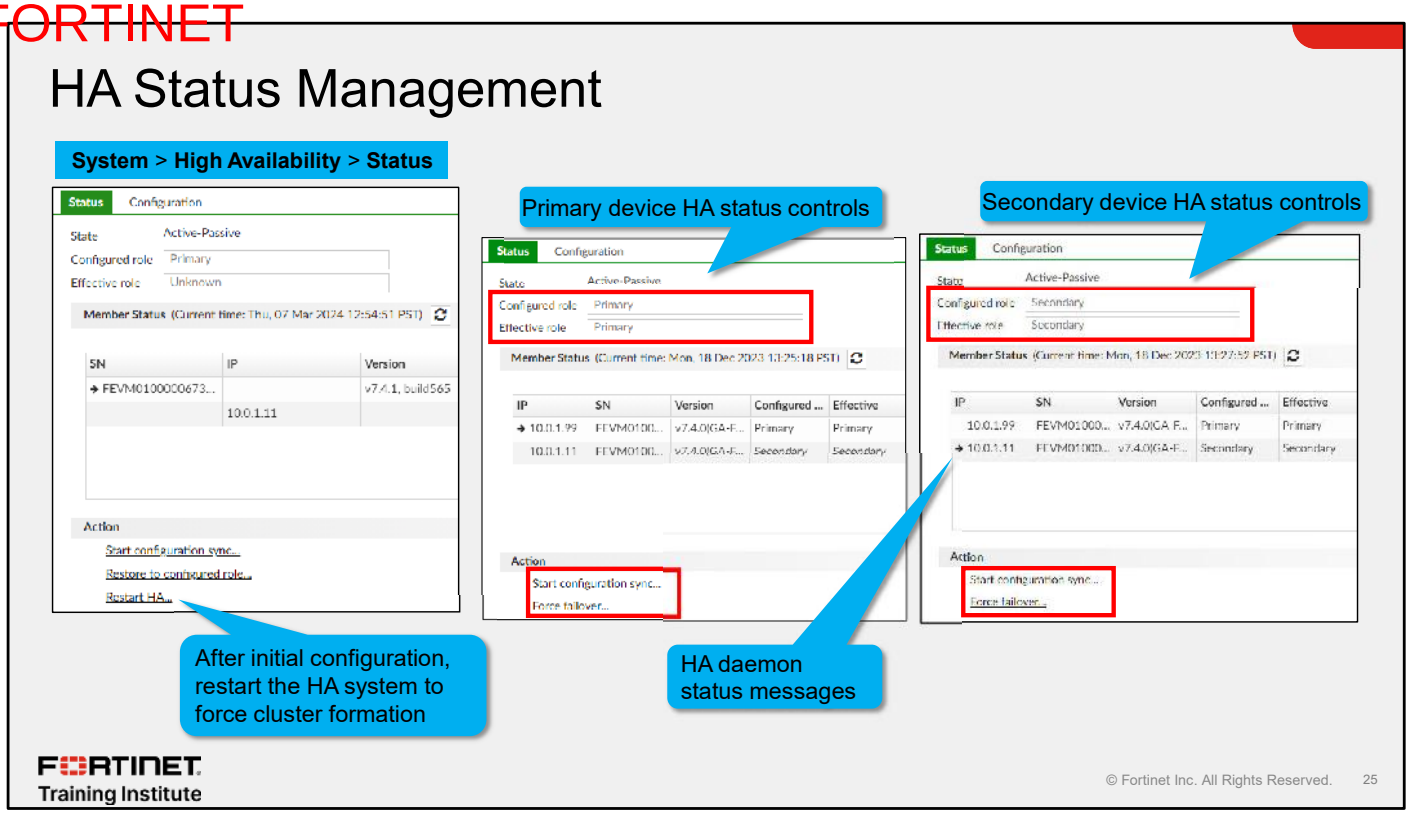
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

The centralized monitoring feature is available only after you apply an MSSP license. The **Centralized Monitor** menu allows you to monitor the state and activity of each HA cluster member, including CPU, memory, disk usage, email throughput, and other mail statistic summaries on the primary FortiMail in an HA cluster. You can also perform cross-device log searches across all cluster devices from the primary FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



On the HA **Status** tab, you can perform management tasks, such as restarting the HA system, starting configuration synchronization, promoting or demoting devices, and removing a device from the cluster. The **Member Status** section displays messages about the status of the cluster.

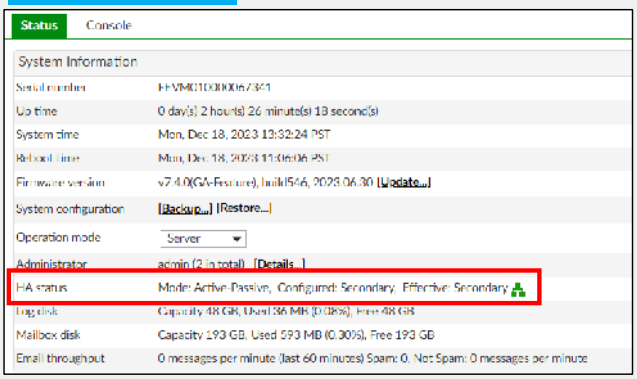
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

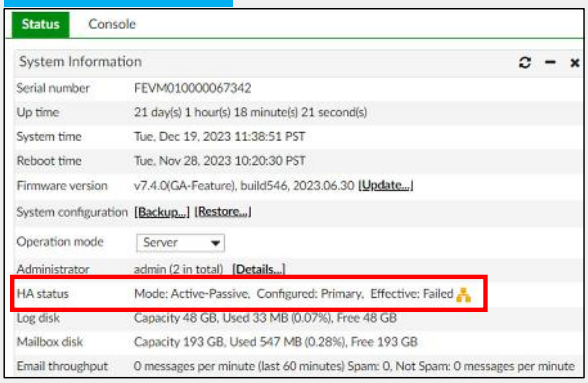
HA Status Management (Contd)

- Dashboard status widget
  - Shows configured and effective status
  - Indicates HA failure or configuration sync problems
  - For display only—changes must be made under **System** > **High Availability**

Dashboard > Status



Dashboard > Status



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

On the dashboard, in the **Status** widget, the **HA status** field displays the configured and effective state of the HA system, problems with synchronization, and if a failure requires investigation.

You can make changes to the HA configuration on the high availability configuration page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Firmware Upgrade Procedure

- Active-passive clusters
  - Upgrade the firmware on the secondary device and wait for it to reboot
  - Upgrade the firmware on the primary device
  - The primary device halts email processing and sends an interrupt to the secondary device to prevent failover during upgrade
  - After the firmware upgrade completes, normal HA and email operations resume
- Active-active clusters
  - Upgrade the firmware on each secondary device individually
  - Upgrade the firmware on the primary device

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

Before you perform a firmware upgrade, check the release notes to make sure you follow the supported upgrade paths, and to note any major changes that may be applicable to your configuration because of the upgrade.

In an active-passive cluster, start by upgrading the firmware on the secondary device. The upgrade causes FortiMail to reboot. This procedure won't affect the primary device's email processing capabilities. After the secondary device restarts, upgrade the firmware on the primary device. The primary device stops all email processing and sends a signal to the secondary device to prevent a failover. After the upgrade on the primary device finishes, normal HA and email processing operations resume.

For active-active clusters, you must upgrade the firmware on each device individually. Upgrade the firmware on all the secondary devices first, and then upgrade the firmware on the primary device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. In an active-passive cluster, which device should you upgrade first?
   - ✓ A. Secondary device
   - B. Upgrade both simultaneously

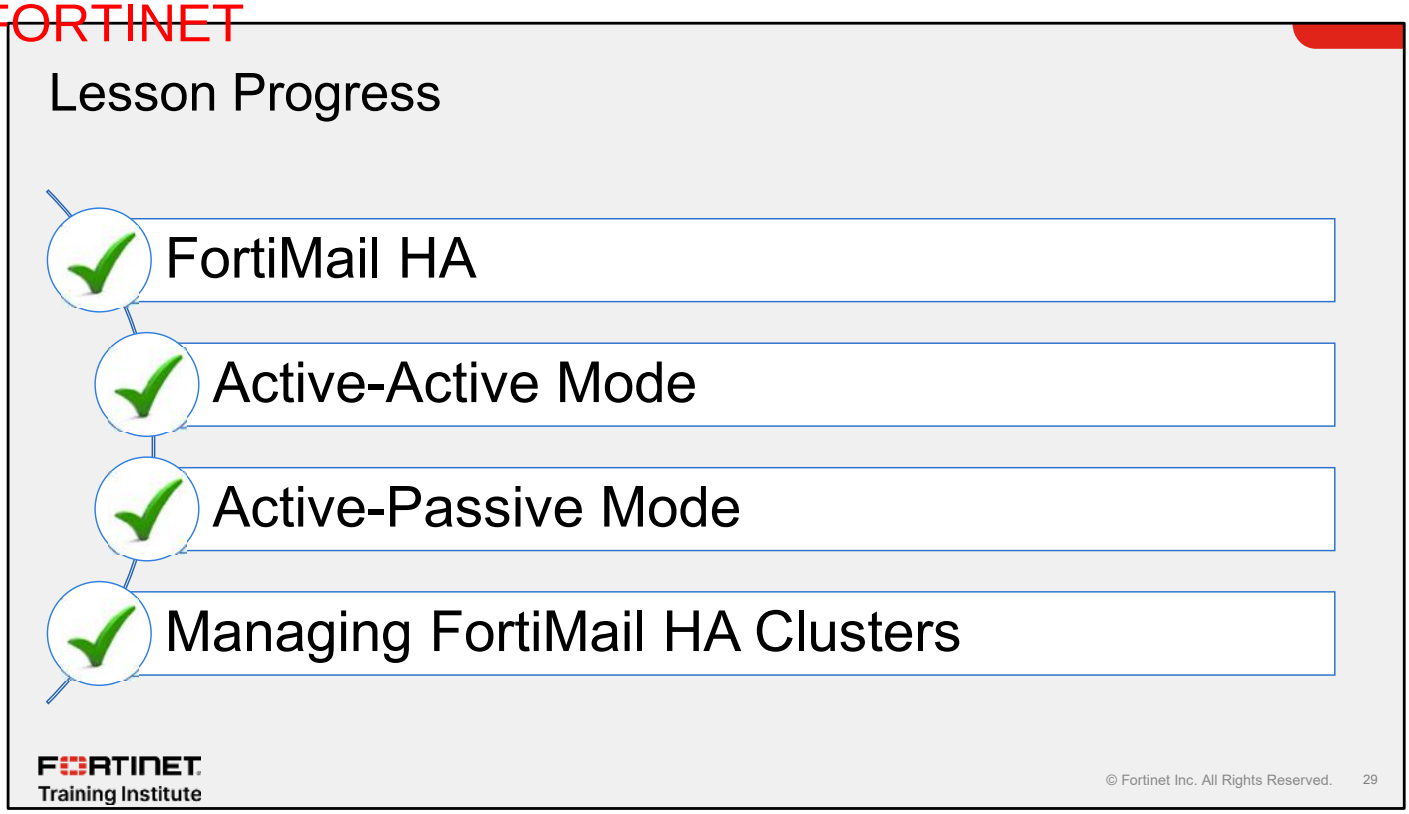
2. In an active-active cluster, which device should you upgrade first?
   - ✓ A. Upgrade all secondary devices first, individually
   - B. Upgrade all the devices in the cluster simultaneously

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in the lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Identify FortiMail HA modes and their benefits
- ✓ Differentiate the synchronization behavior between HA modes
- ✓ Identify requirements for active-active cluster implementation
- ✓ Configure active-active FortiMail clusters
- ✓ Identify requirements for active-passive cluster implementation
- ✓ Configure active-passive FortiMail clusters
- ✓ Monitor a FortiMail HA cluster centrally
- ✓ Manage HA operations on clustered devices
- ✓ Upgrade FortiMail cluster firmware

FORTINET Training Institute

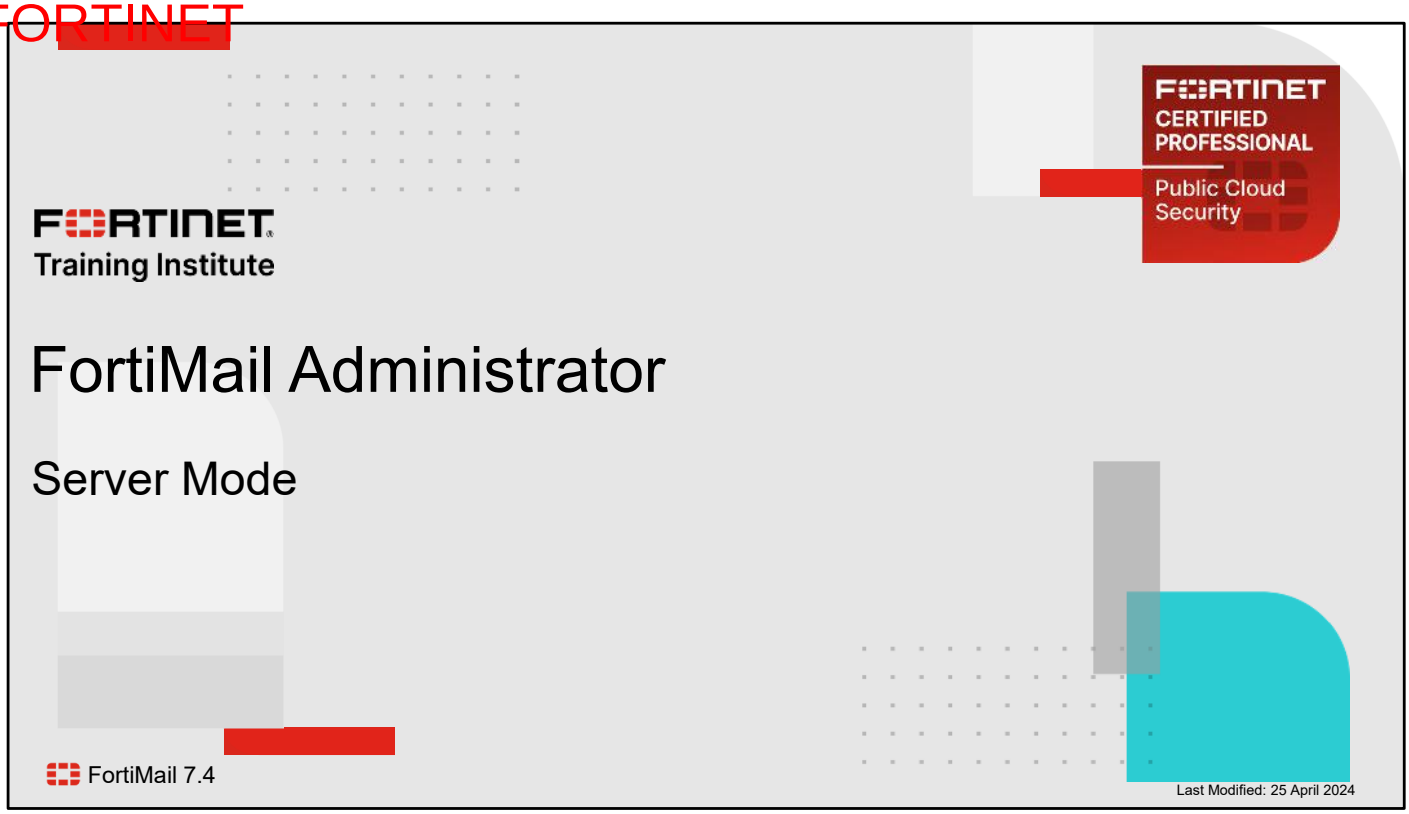
© Fortinet Inc. All Rights Reserved. 30

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to identify various HA modes and differentiate synchronization behavior between HA modes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lesson, you will learn how to deploy and configure FortiMail in server mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- Implementation Requirements
- Server Mode Configuration
- Server Mode User Experience

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 2

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Implementation Requirements

Objectives

- Establish network topology and DNS requirements
- Configure access receive rules for bidirectional email flow

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 3

After completing this section, you should be able to achieve the objectives shown on this slide.

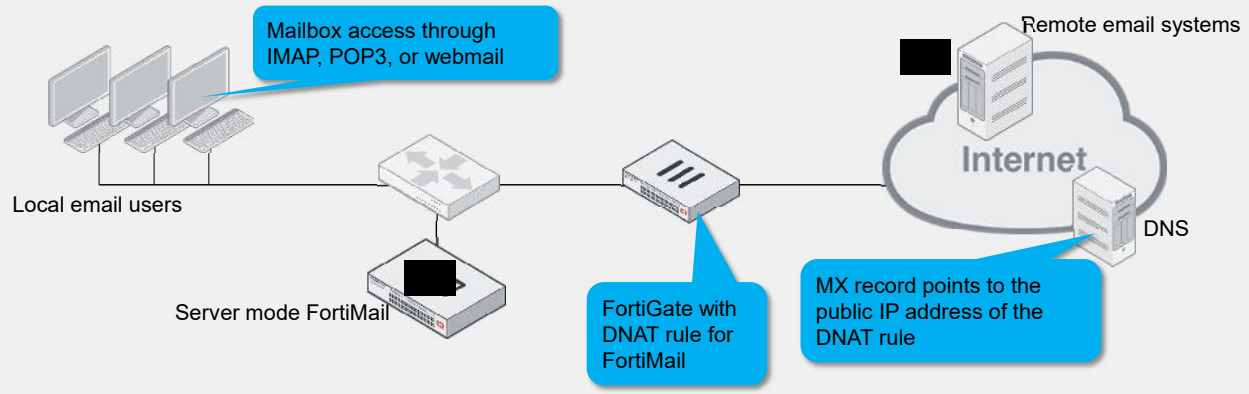
By demonstrating competence in understanding network topology requirements and traffic flow rules, you will be able to deploy FortiMail in server mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Server Mode Review

- Full-featured MTA functionality
- User mailboxes stored locally
- Mailbox access provided by POP3, IMAP, or webmail
- Route and host SMTP traffic for all protected domains directly to FortiMail



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

After you configure FortiMail to operate in server mode, FortiMail provides all the services of a full-featured mail transfer agent (MTA), along with all the FortiMail security benefits. The user mailboxes are stored locally, and user access is provided by POP3, IMAP, or webmail.

Just like you would in gateway mode, you should route SMTP traffic for all protected domains directly to FortiMail by publishing the necessary mail exchange (MX) records in DNS. These MX records typically resolve to an external IP address that you should set to the destination network address translation (DNAT) on the perimeter firewall for the FortiMail IP address.

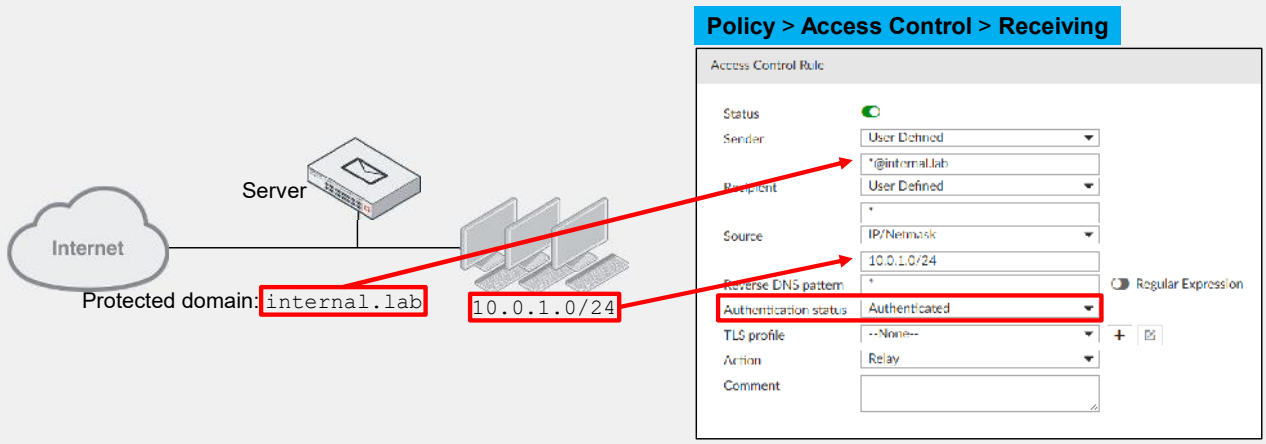
After the email message arrives at the FortiMail server, FortiMail inspects it and, if it is clean, delivers it to the recipient's local mailbox.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Access Receive Rule Review

- Inbound (email destined to a protected domain) → Relay
  - Access receive rule not required for inbound email
- Outbound (email not destined to a protected domain) → Reject
  - Access receive rule required for outbound email if sender is unauthenticated



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

For server mode implementation, inbound email doesn't require access receive rules. By default, FortiMail accepts all email destined for protected domains. However, to allow outbound email from you local users, you still must configure the appropriate access receive rule. To prevent unauthorized relaying, you should configure authentication enforcement when you set up access receive rules for server mode. For more information about authentication enforcement, see the *Authentication* lesson.

For more information about access control rules, see the *Access Control and Policies* lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. In which operation mode are user mailboxes stored on FortiMail?
   A. Gateway mode
   ✓ B. Server mode

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Progress

- ✓ Implementation Requirements
- Server Mode Configuration
- Server Mode User Experience

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 7

Good job! You now understand the implementation requirements.

Now, you will learn about server mode configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Server Mode Configuration

Objectives

- Configure and manage mail users
- Configure resource profiles for user account quotas and privileges
- Configure remote storage for mail data
- Configure and manage global, domain, and user address books

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

After completing this section, you will be able to achieve the objectives shown on this slide.

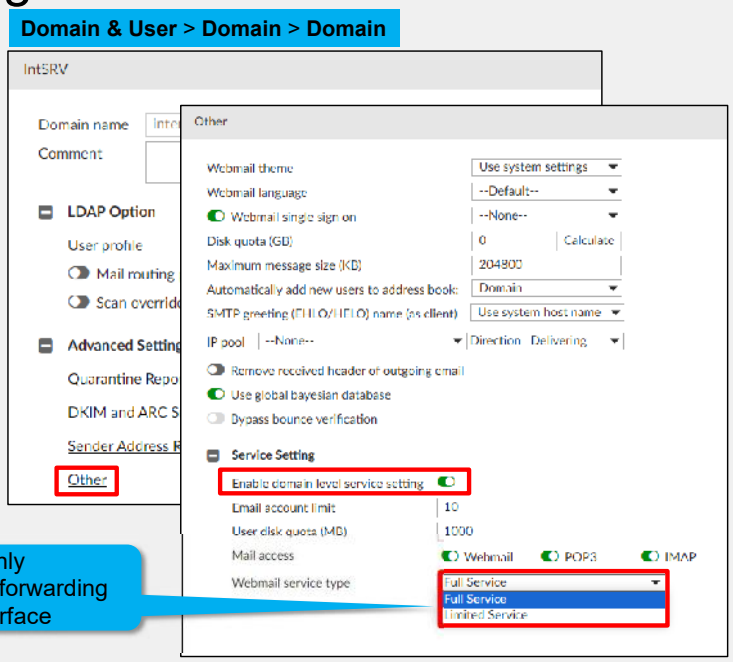
By demonstrating competence in configuring service settings, mail servers, quotas, accounts, and more, you will be able to configure FortiMail server mode options.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Domain Service Settings

- Domain-level service settings control:
  - Account limit for each domain
  - Disk quota for each domain
  - Disk quota for each user
  - Mail access options for users
- Useful for managed security service provider (MSSP) billing models



Limited Service enables only password change and mail forwarding options for the webmail interface

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

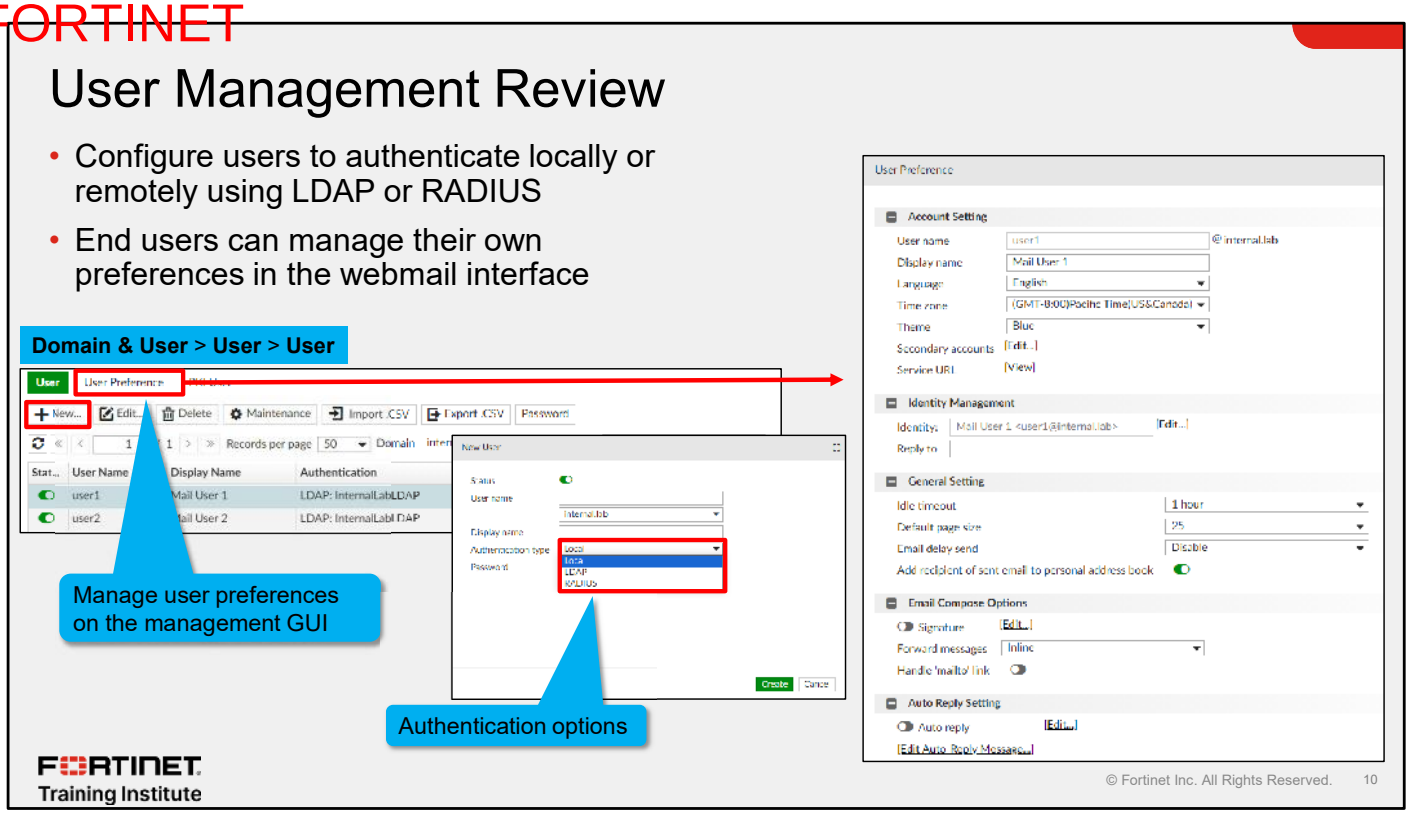
In a server mode domain configuration, you can define domain-level service settings to control the account limit for each protected domain, the disk quota for each domain, the disk quota for each user, and the mail access options for users.

These settings give you granular control in environments where FortiMail may be hosting many domains at the same time, such as in a managed service security provider (MSSP) environment.

For more information about how to configure protected domains, see the *Basic Setup* lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In server mode, you must set up a user account for each end user. You can configure these user accounts to authenticate locally or remotely using LDAP or RADIUS and an appropriate authentication profile. For more information about authentication profiles, see the *Authentication and Encryption* lesson.

Creating a user account in server mode creates the user's mailbox, which handles both regular email and the spam quarantine.

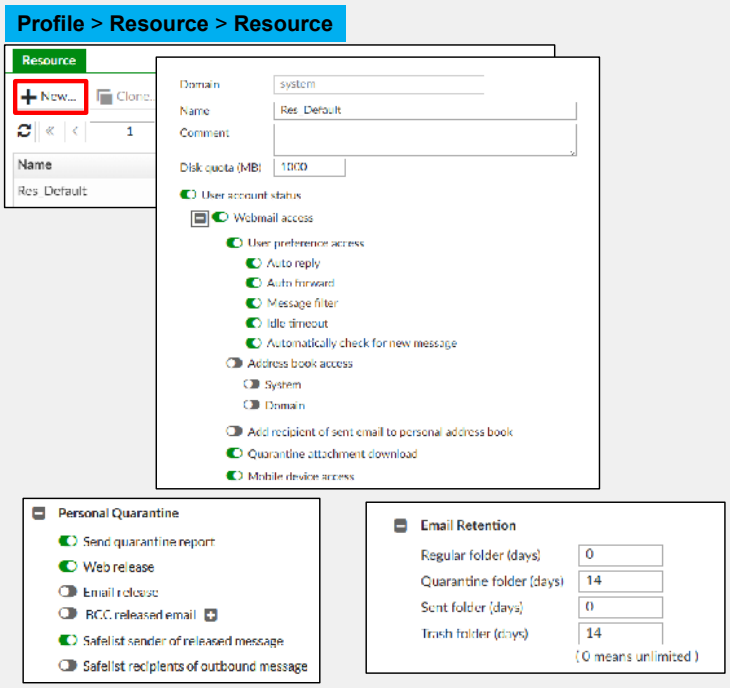
Create users on the **User** tab and manage user preferences on the **User Preferences** tab. End users can manage their own preferences when they log in to the webmail interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Resource Profiles

- Allows policy-level control of user account options
  - Disk space quota
  - Webmail access options
  - Address books permissions
  - Personal quarantine
  - Email retention periods
- Must apply using recipient-based policies



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

Resource profiles allow you to control user account options at the policy level. You can define disk space quotas, webmail access options, address book permissions, personal quarantine, and email retention periods. Use recipient-based policies to apply resource profiles.

For more information about recipient-based policies and other policies, see the *Authentication and Policies* lesson.

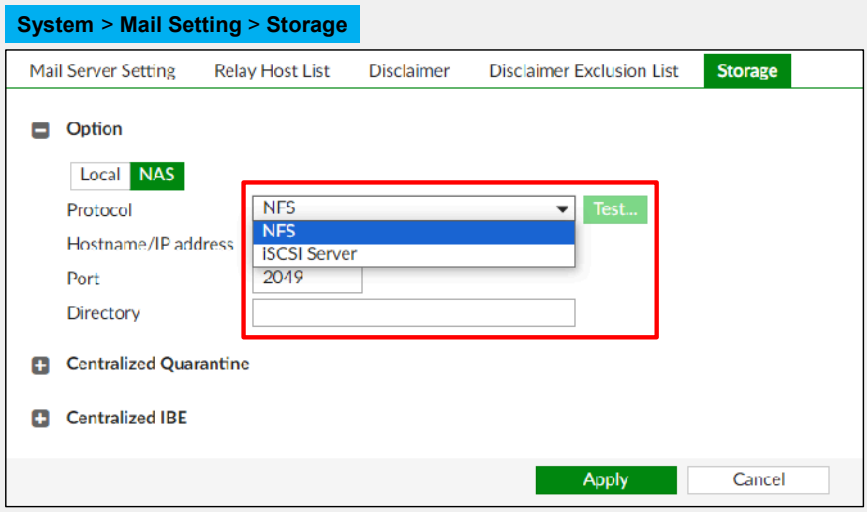
For more information about other inspection profiles, see the *Session Management*, *Antivirus and Antispam*, and *Content Inspection* lessons.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Mail Storage

- FortiMail can store email either locally or on an external NAS device using NFS or iSCSI
- See the *FortiMail Administration Guide* for a list of supported NFS servers



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

Because FortiMail maintains user mailboxes when operating in server mode, the amount of storage FortiMail needs when operating in server mode can be far greater than it is in other operating modes. When you install FortiMail in server mode, you must decide whether to use the FortiMail internal storage or an external storage solution. In some configuration scenarios, such as configuration-only high availability (HA) clusters, external storage for user mailboxes is a requirement when FortiMail is operating in server mode.

See the *FortiMail Administration Guide* for a list of supported network file share (NFS) servers.

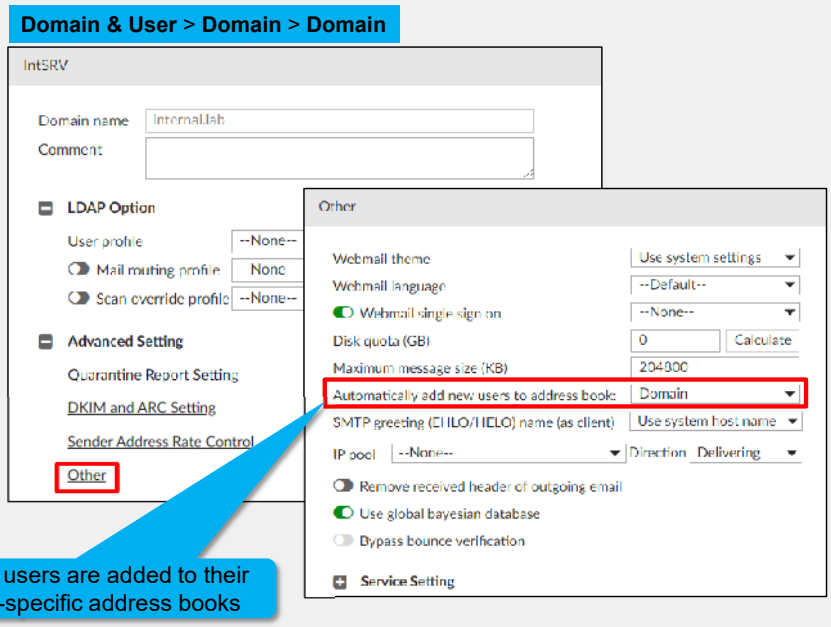
For more information about FortiMail clustering, see the *High Availability* lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Address Books

- **Domain**: Domain specific; managed by the administrator
- **System**: System wide; managed by the administrator
- **Personal**: Managed by the user



By default, all new users are added to their respective domain-specific address books

FORTINET Training Institute

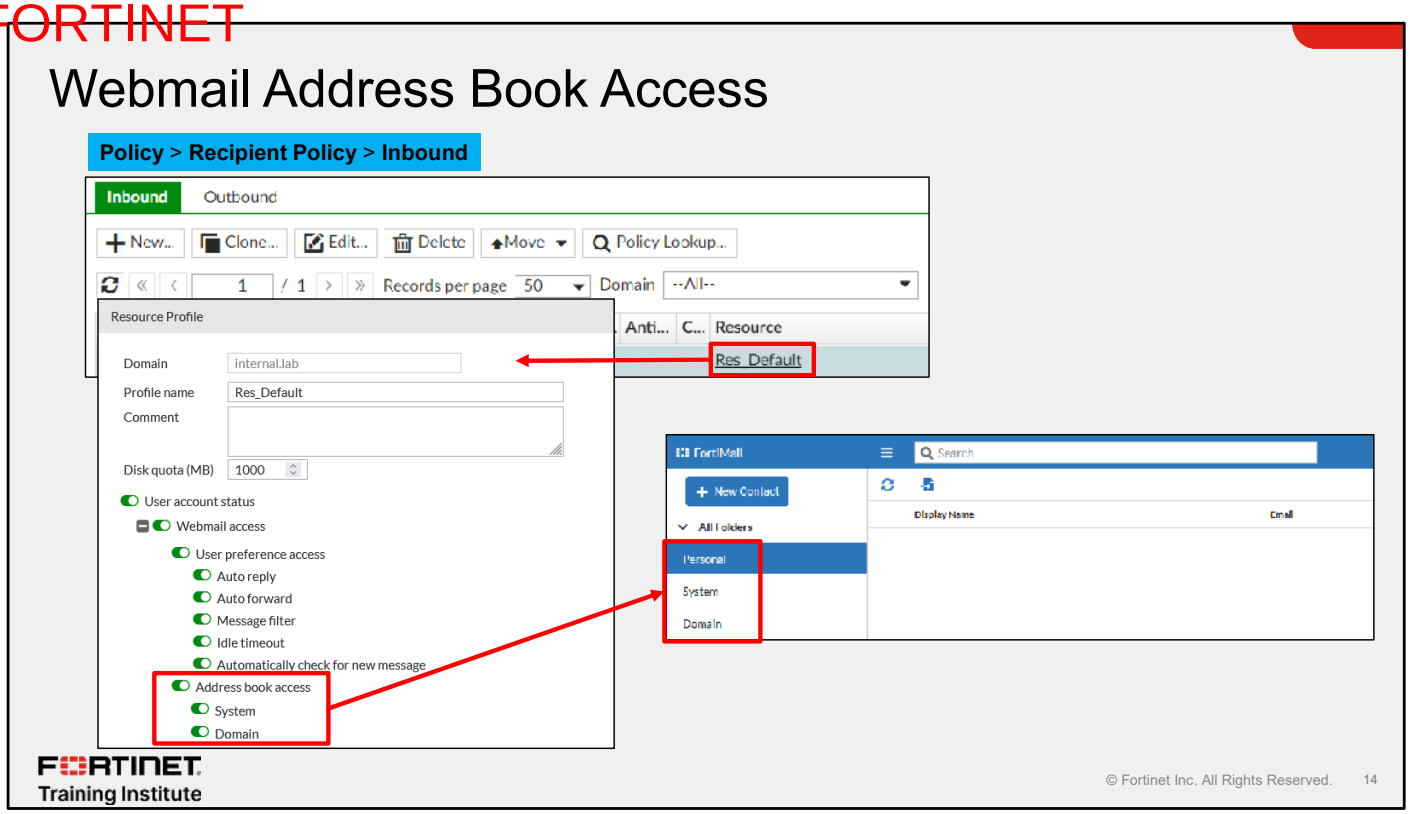
© Fortinet Inc. All Rights Reserved. 13

There are three levels of address books—personal, domain, and system. The user manages their own personal address book. The administrator manages the domain address books, which contain entries of users within a particular protected domain. The administrator also manages the system address book which is provided as read-only to users across all domains.

While the webmail interface provides direct access to address books, third-party email clients, such as Outlook and Thunderbird, can access address books using the LDAP protocol. The FortiMail server contains an embedded LDAP server that acts as a bridge for address book access.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



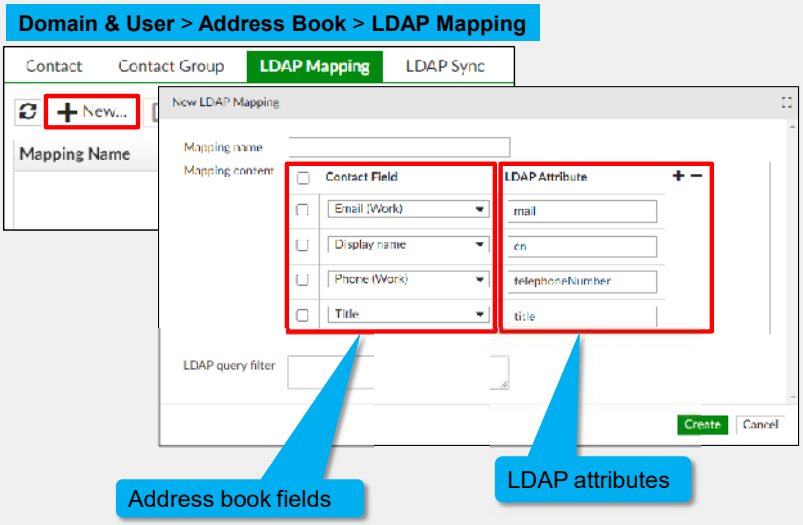
End users always have access to their personal address books. Access to the domain or global address books depends on the matching resource profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

LDAP Mapping

- Populate global or domain address books from an existing LDAP server
- Create the mapping profile to map LDAP attributes to address book fields



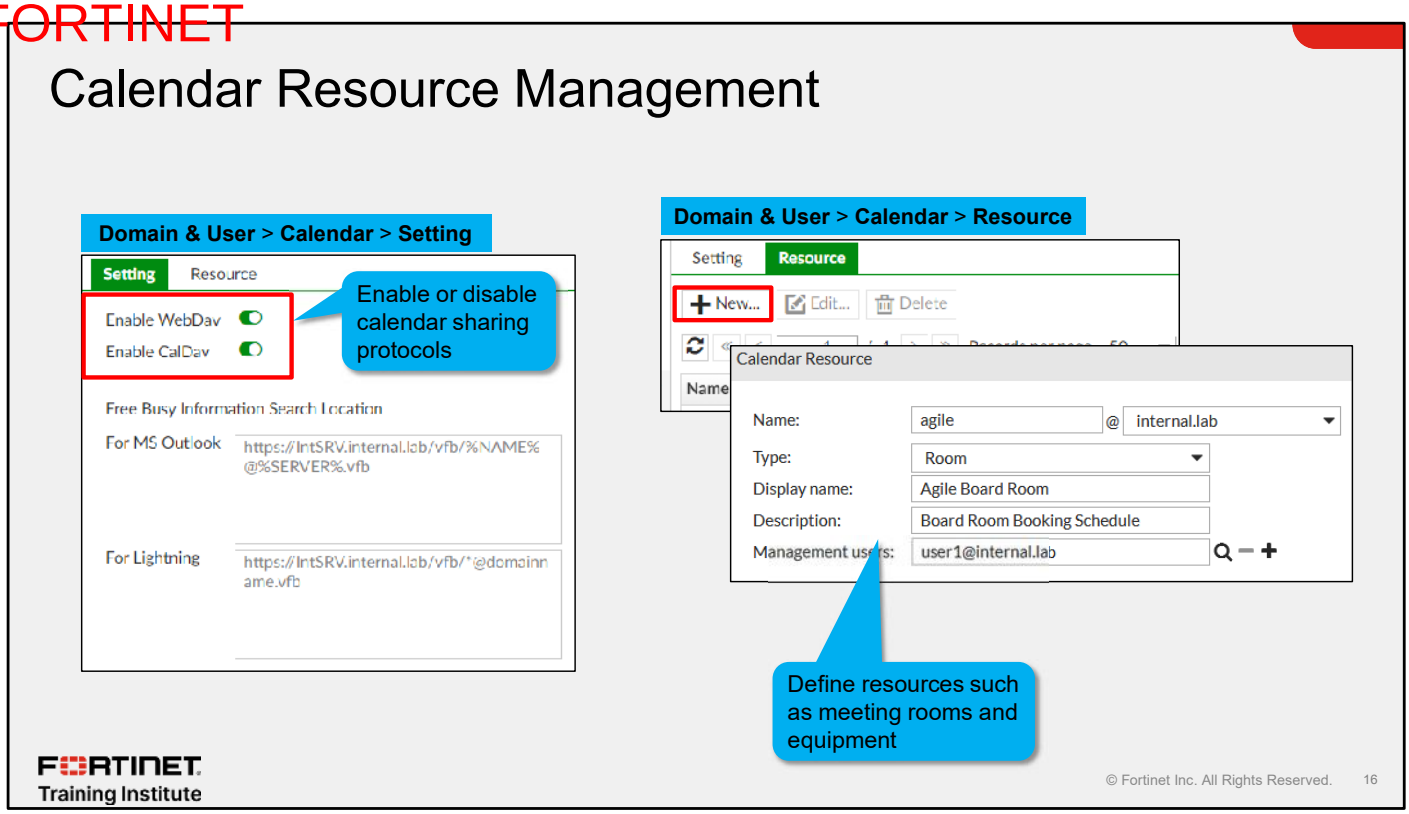
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

You can populate the system or domain address books by retrieving entries from an existing LDAP server. The mapping profile maps attributes from LDAP to address book fields. The LDAP attributes differ, based on the LDAP server architecture. The example shown on this slide uses attributes from a Windows Active Directory LDAP server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To support calendar sharing, you must enable the sharing protocols. The calendar service also supports resource management, such as meeting rooms and equipment.

Of the two most popular email clients, only Thunderbird implements full, real-time calendar syncing because of its support of CalDAV. Outlook users can publish their local calendar to the FortiMail server and subscribe to other calendars using WebDAV, but their local, personal calendars remain owned by Outlook. Outlook through WebDAV does provide full functionality to schedule meetings and view free or busy status.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which FortiMail feature is available only in server mode?
   A. Webmail interface
   ✓ B. Calendar resource management

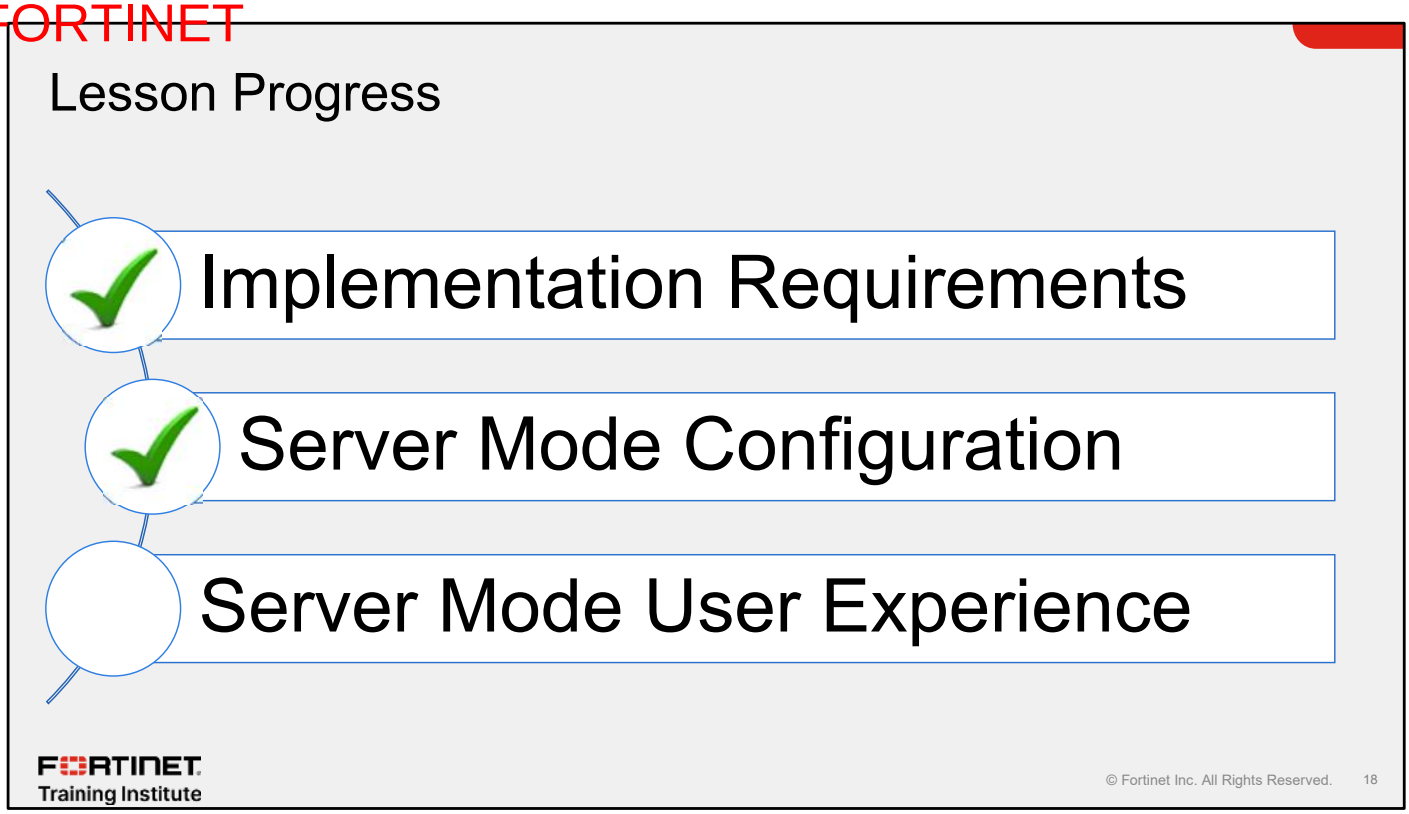
2. By default, a server mode FortiMail user has access to which address book?
   A. Domain
   ✓ B. Personal

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Good job! You now understand server mode configuration.

Now, you will learn about the server mode user experience.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Server Mode User Experience

Objectives

- Configure and manage end-user features

FORTINET Training Institute

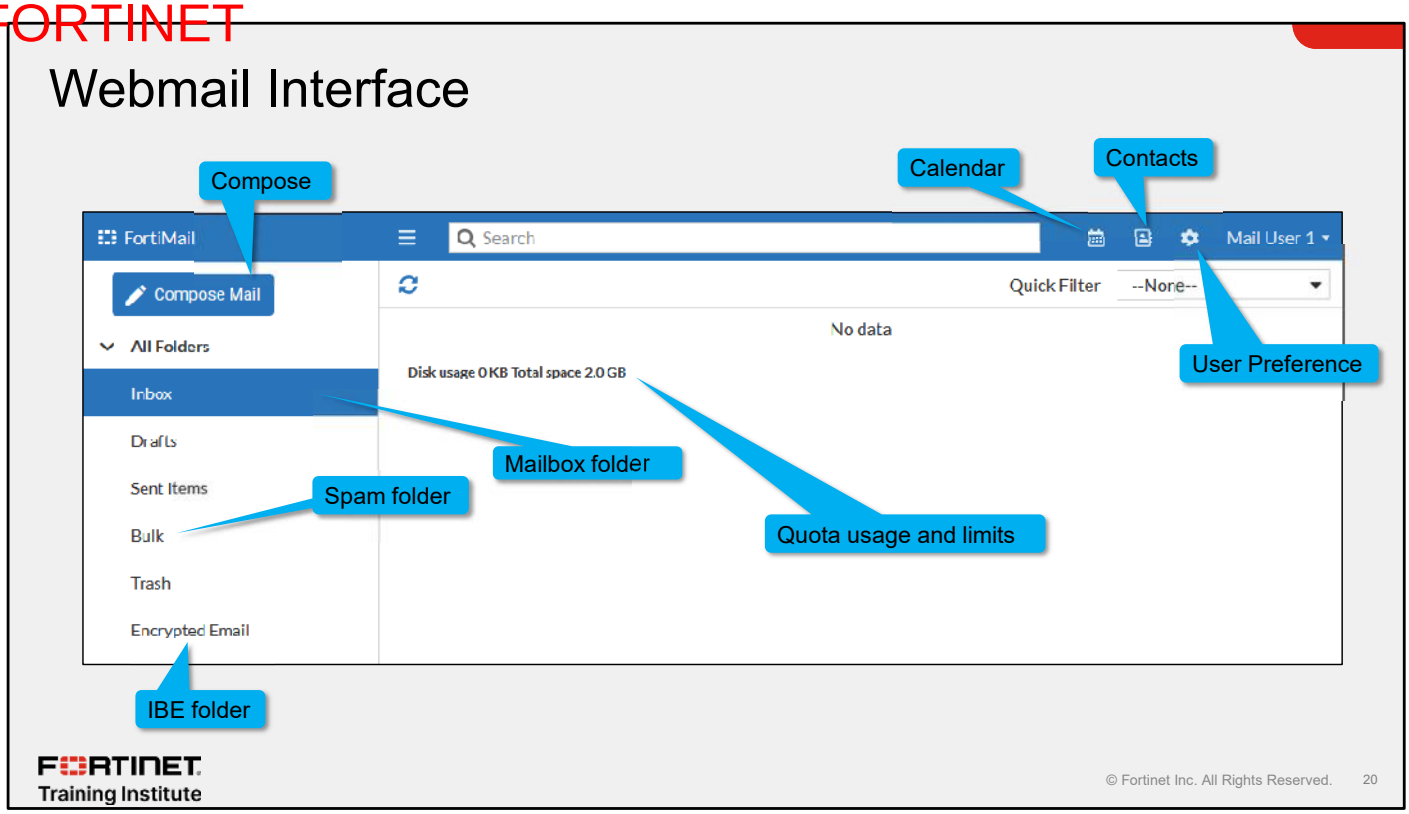
© Fortinet Inc. All Rights Reserved. 19

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding the server mode webmail interface features, you will be able to configure and manage those features for end users.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

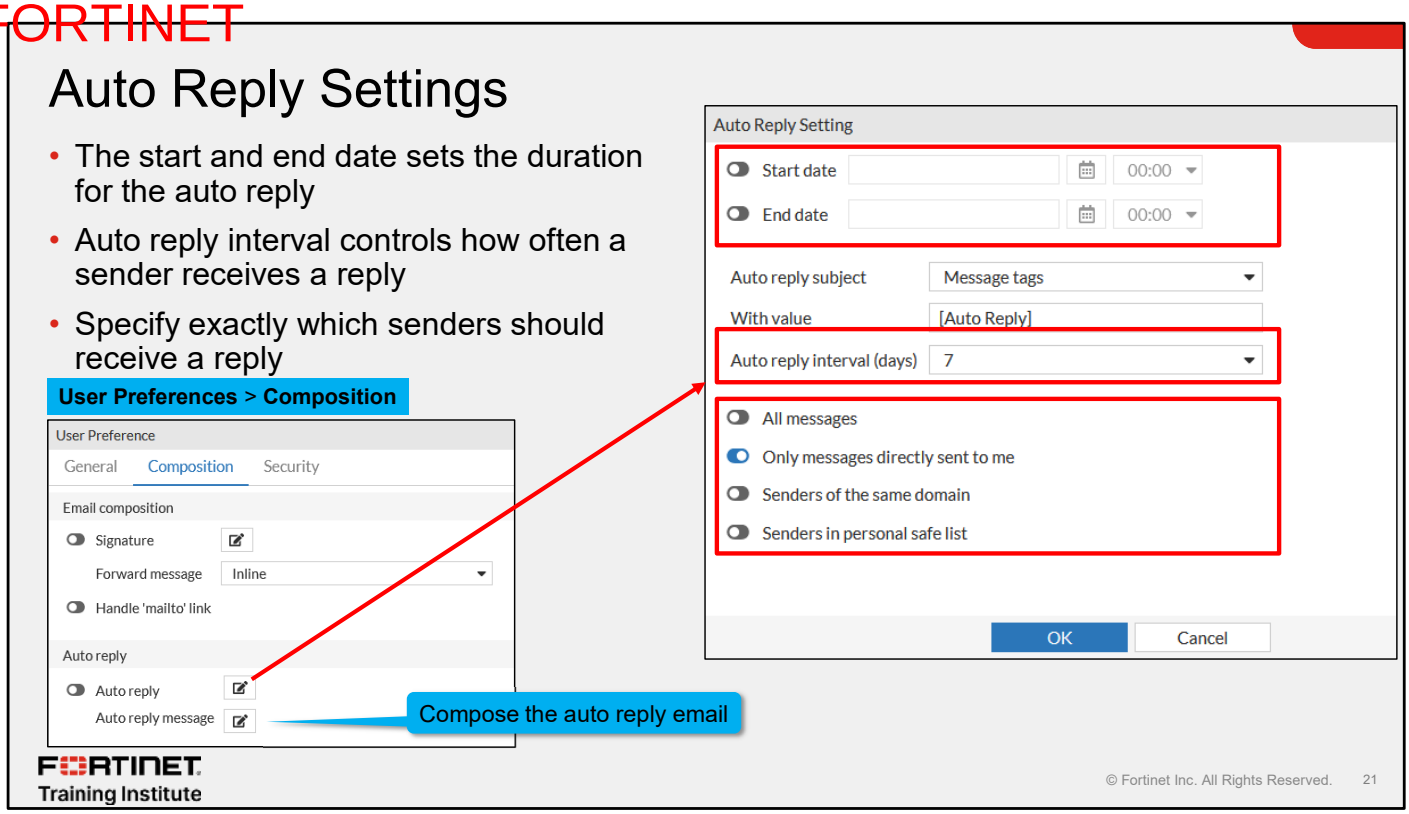


The server mode webmail interface comes with all the standard mailbox features. Spam email is sent to the **Bulk** mailbox folder and identity-based encryption (IBE) email is sent to the **Encrypted Email** folder.

To access account settings, in the top-right corner of the screen, click the account settings icon.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Email users can manage their out-of-office settings using the webmail user interface. To set an out-of-office auto reply, click **User Preferences** > **Composition**.

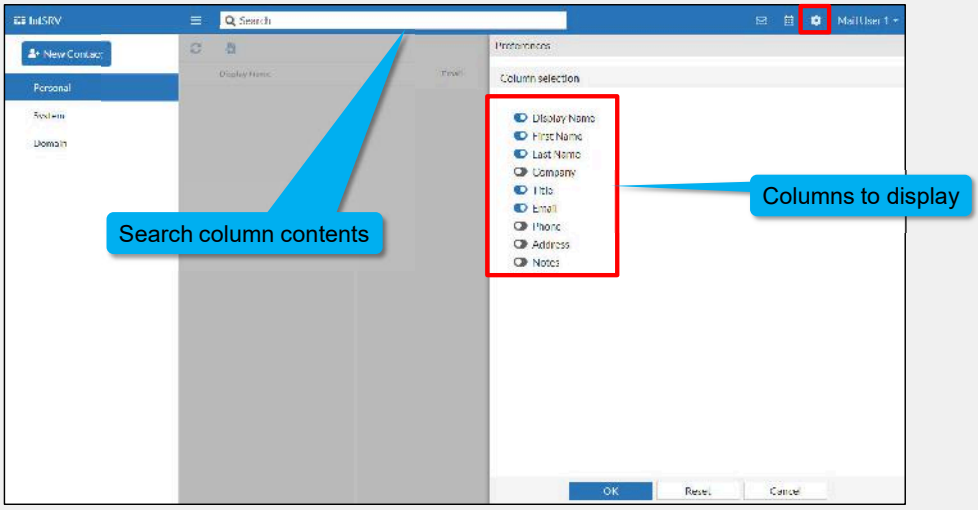
Set specific start and end dates, which will prevent the user from accidentally leaving the auto reply active. Use the **Auto reply interval** option to control how often a sender receives an auto reply. You can also define exactly which senders should receive an auto reply.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Contacts Columns and Search

- Customizable column selection
- Search on column contents



FORTINET Training Institute

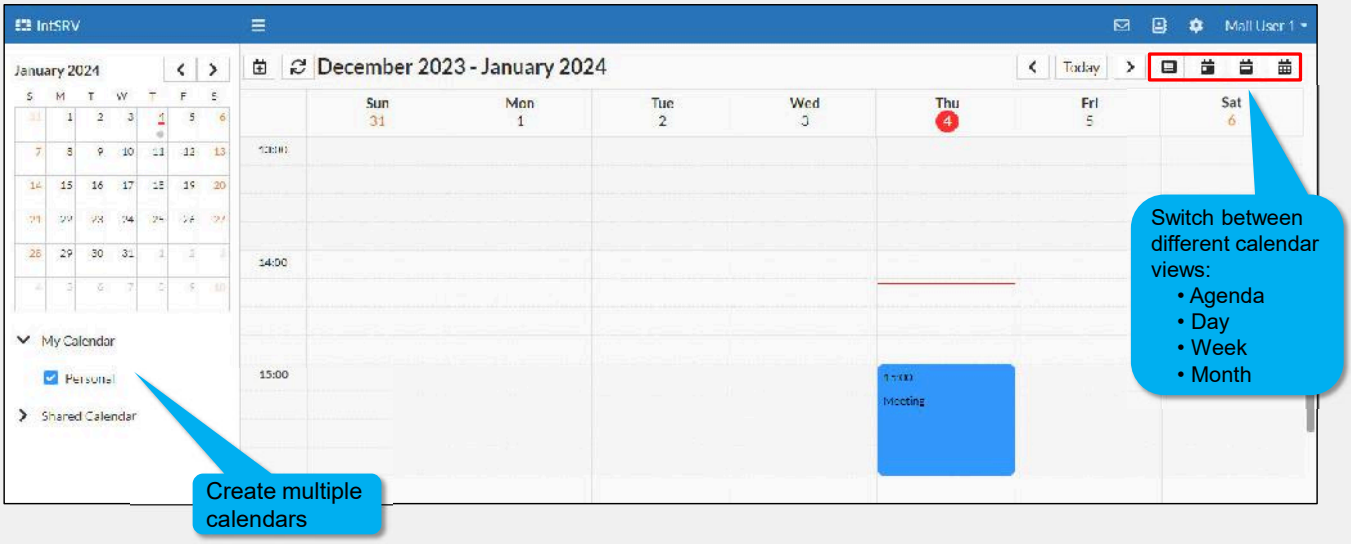
© Fortinet Inc. All Rights Reserved. 22

You can select which columns are displayed in the contacts view, and you can search the contents of the columns.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Webmail Calendar Access



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

In addition to providing email services, FortiMail in server mode provides full calendar support for personal and shared calendars; free or busy status; and the scheduling of resources, such as conference rooms and equipment.

The webmail interface provides the user with full access to their calendars. A fully-interactive drag-and-drop interface allows for the easy creation, editing, moving, and deletion of calendar events. Users can create multiple personal calendars to keep their appointments organized.

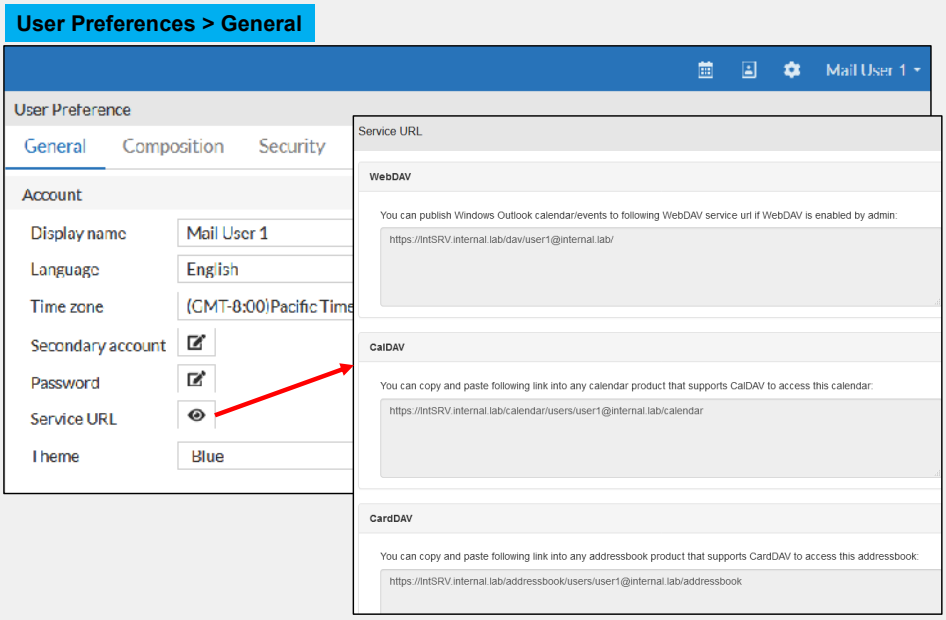
Along with traditional day, week, and month views, users can view calendar entries in the agenda view, which shows upcoming calendar events in a compact list view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

MUA Calendar Integration

- Users can subscribe or publish to and from their calendar
- MUA must support CalDAV or WebDAV
- Get service URLs from the **User Preference** section



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

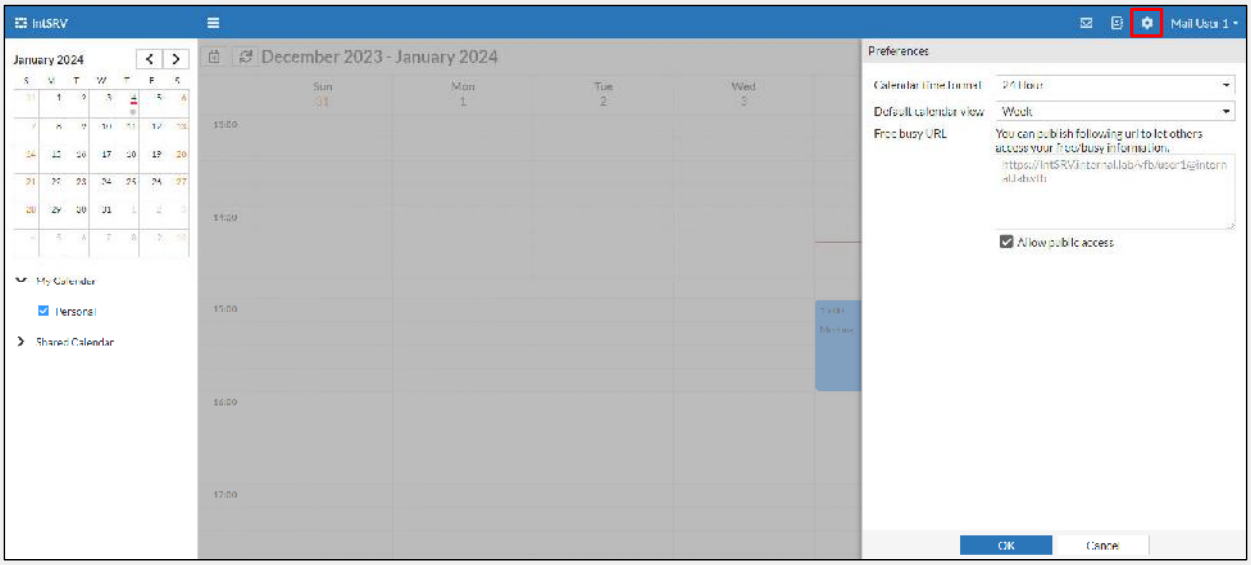
FortiMail calendars support the industry-standard access protocols CalDAV and WebDAV. This provides third-party email clients, such as Outlook and Thunderbird, with the ability to access user calendars stored on the FortiMail server. This allows the end user to control their calendars completely, using their email client of choice, assuming the client supports either CalDAV or WebDAV.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Free or Busy Status Tracking

- Share your own, or view someone else's free or busy status



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

FortiMail operating in server mode also provides users with the ability to publish their free or busy status. To access the URL, on the calendar screen, click the account settings icon to access preferences.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

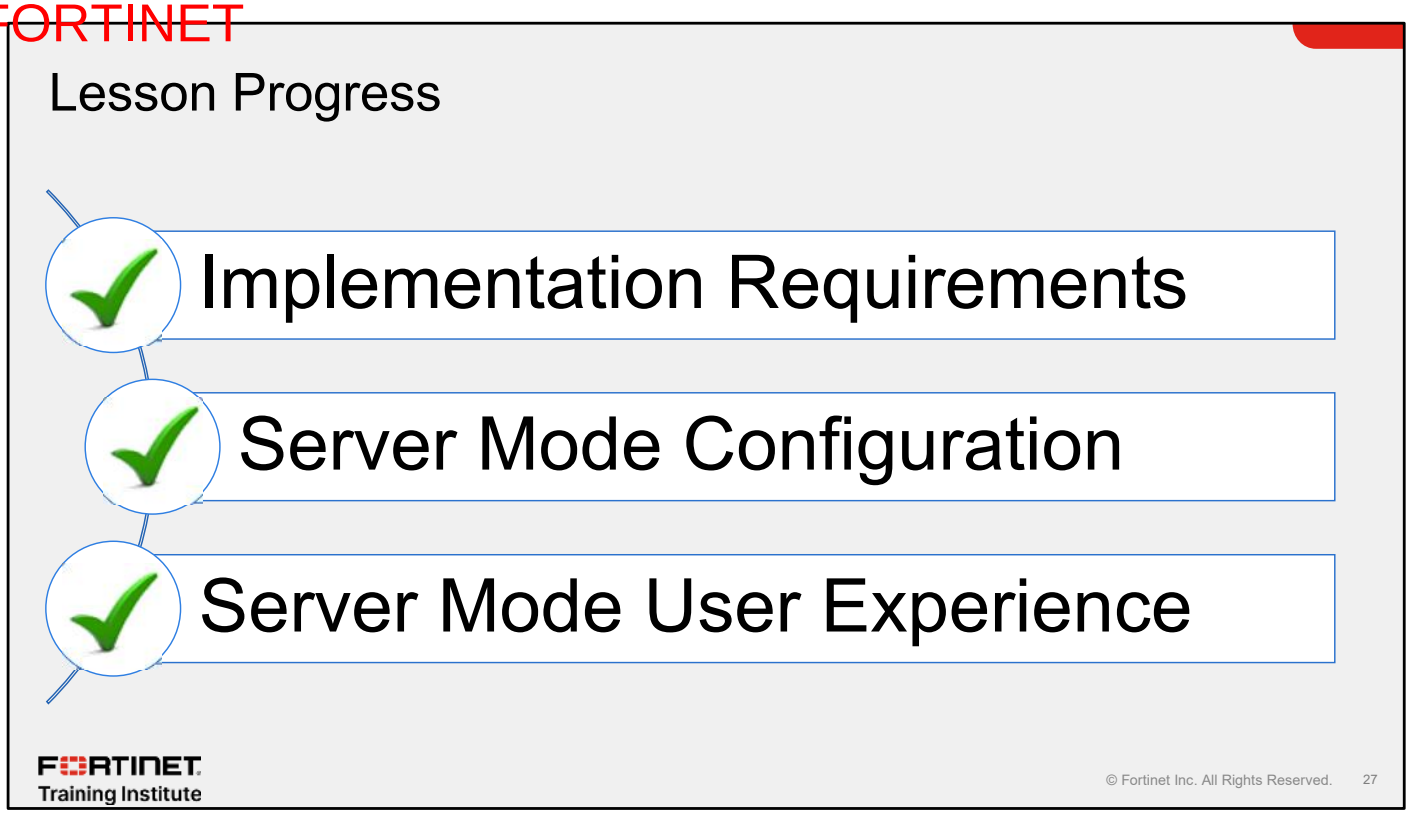
1. Which access protocols are supported by the FortiMail calendar?
   - ✓ A. CalDAV and WebDAV
   - B. ActiveSync

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Establish network topology and DNS requirements
- ✓ Configure access receive rules for bidirectional email flow
- ✓ Configure and manage mail users
- ✓ Configure resource profiles for user account quotas and privileges
- ✓ Configure remote storage for mail data
- ✓ Configure and manage global, domain, and user address books
- ✓ Configure and manage end-user features

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to deploy FortiMail in server mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FORTINET Training Institute

FORTINET CERTIFIED PROFESSIONAL Public Cloud Security

FortiMail Administrator

Transparent Mode

FortiMail 7.4

Last Modified: 25 April 2024

In this lesson, you will learn how to deploy FortiMail in transparent mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- Implementation Requirements
- Transparent Mode Configuration
- Deployment Examples

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 2

In this lesson, you will explore the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Implementation Requirements

Objectives

- Describe transparent mode network topology requirements
- Configure access receive rules for bidirectional email flow

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 3

After completing this section, you should be able to achieve the objectives shown on this slide.

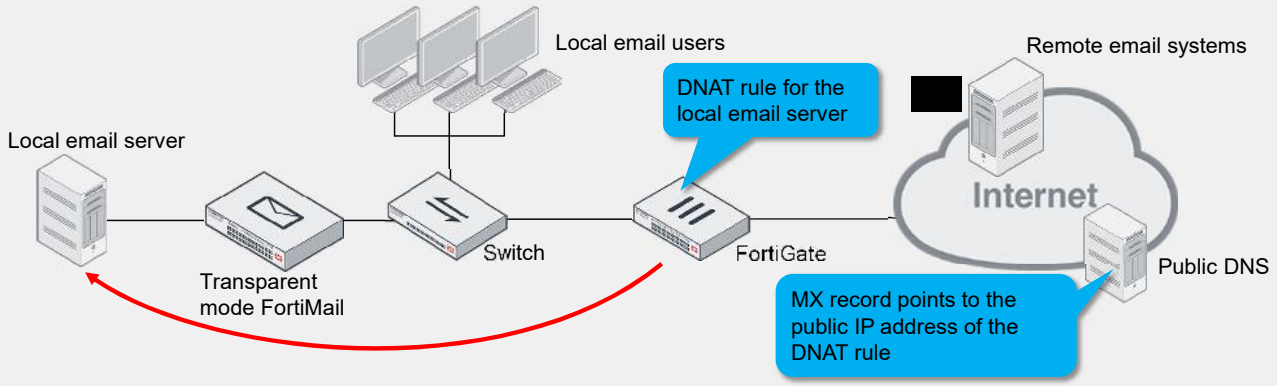
By demonstrating competence in determining network topology requirements and configuring rules for email flow, you will be able to implement transparent mode on FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Transparent Mode Review

- Sits in the SMTP network path
- Intercepts email even though destination IP address isn't FortiMail
- DNS MX record or DNAT rule changes are not required



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

In transparent mode, FortiMail sits in the email path to intercept email traffic transparently, based on the destination IP address, and perform the antispam and antivirus scans. In the example deployment shown on this slide, FortiMail isn't the intended IP destination of the email messages; therefore, no DNS or DNAT rule change is required.

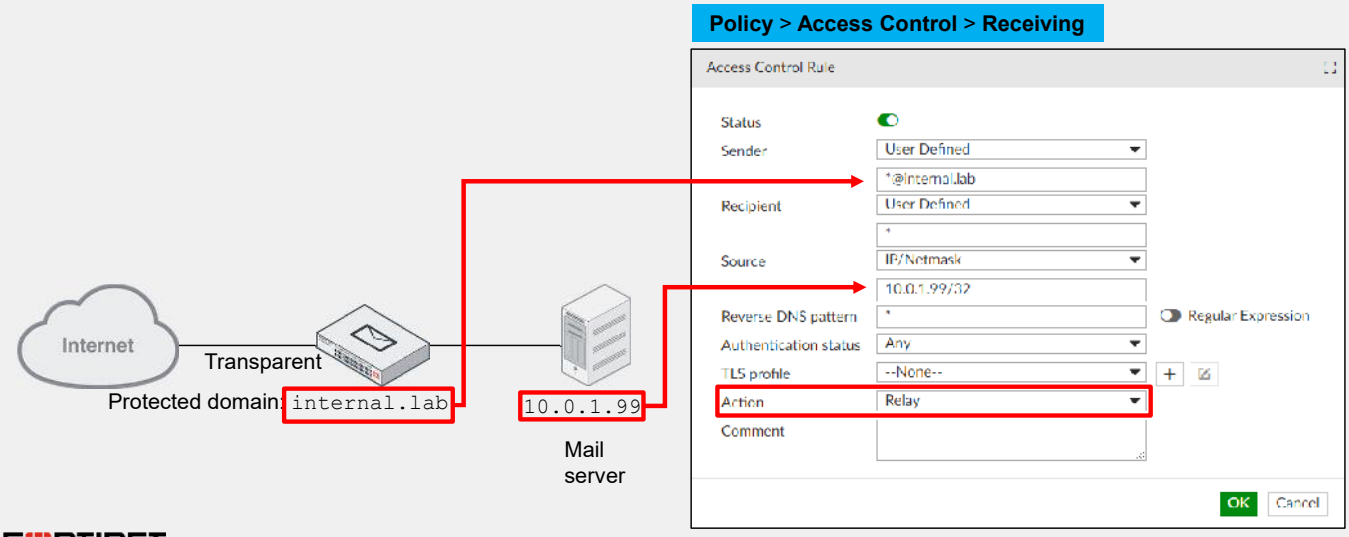
In some environments, such as large managed service providers (MSP) and carriers, the infrastructure changes required by the other deployment modes are impractical. Because of these constraints, MSPs and carriers usually deploy FortiMail in transparent mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Access Receive Rule Review

- No rules required to handle inbound email
- Access control rule required to allow outbound email



FORTINET Training Institute
© Fortinet Inc. All Rights Reserved. 5

In transparent mode, like all other deployment modes, no access receive rules are required for inbound email. By default, FortiMail accepts all email destined for protected domains. However, to allow outbound email, you must configure the appropriate access receive rule. You must create access receive rules if you intend to use FortiMail to scan outbound email.

For more information about access control rules, see the *Access Control and Policies* lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. What is a primary motivator for deploying FortiMail in transparent mode?
   - ✓ A. You can deploy it with minimal network configuration changes.
   - B. There is no message queuing feature, so mail delivery is expedited.

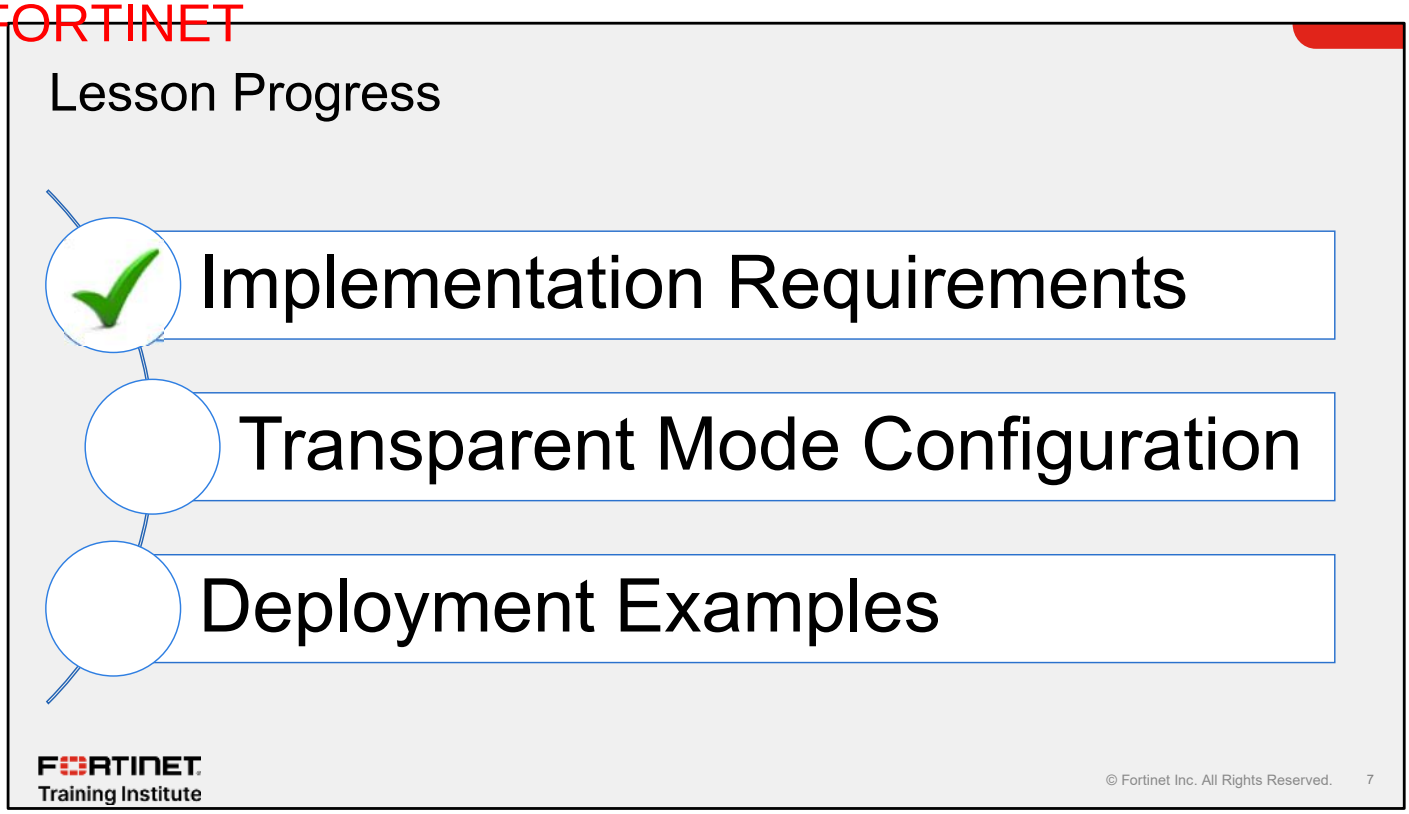
2. No access receive rule is required for inbound emails in transparent mode.
   - A. False
   - ✓ B. True

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Good job! You now understand the implementation requirements of transparent mode.

Now, you'll learn about transparent mode configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Transparent Mode Configuration

Objectives

- Configure bridge and out-of-bridge interfaces
- Configure transparent mode protected domain options
- Configure transparent mode mail routing features
- Configure transparency

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in transparent mode configuration, you will be able to apply specific transparent mode configuration options.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Built-In Bridge

- By default, all FortiMail interfaces are members of a built-in bridge
  - FortiMail bridges non-SMTP traffic through without any inspection.
- The management IP is permanently tied to port1
  - Uses the management IP for all management and FortiGuard-related traffic
  - Bridge member interfaces belong to the same subnet as the management IP

System > Network > Interface

Interface | Link Monitor | Routing | DNS | DDNS | Port Forwarding | FortiGate

New... | Edit... | Delete

Link Status	Name	Type	Bridge Member	IP/Netmask	IPv6/Netmask
✓	port1/Management IP	Physical	✓	10.200.1.98/24	::/0
✓	port2	Physical	✓	0.0.0.0/0	::/0
✗	port3	Physical	✓	0.0.0.0/0	::/0
✓	port4	Physical	✗	192.168.1.103/24	::/0

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

By default, all interfaces are configured as a bridge in transparent mode. You must assign the management IP statically to port1. The management IP is used for all management-related traffic as well as FortiGuard communication. Bridge member interfaces must belong to the same subnet as the management IP of port1, if assigned an IP address.

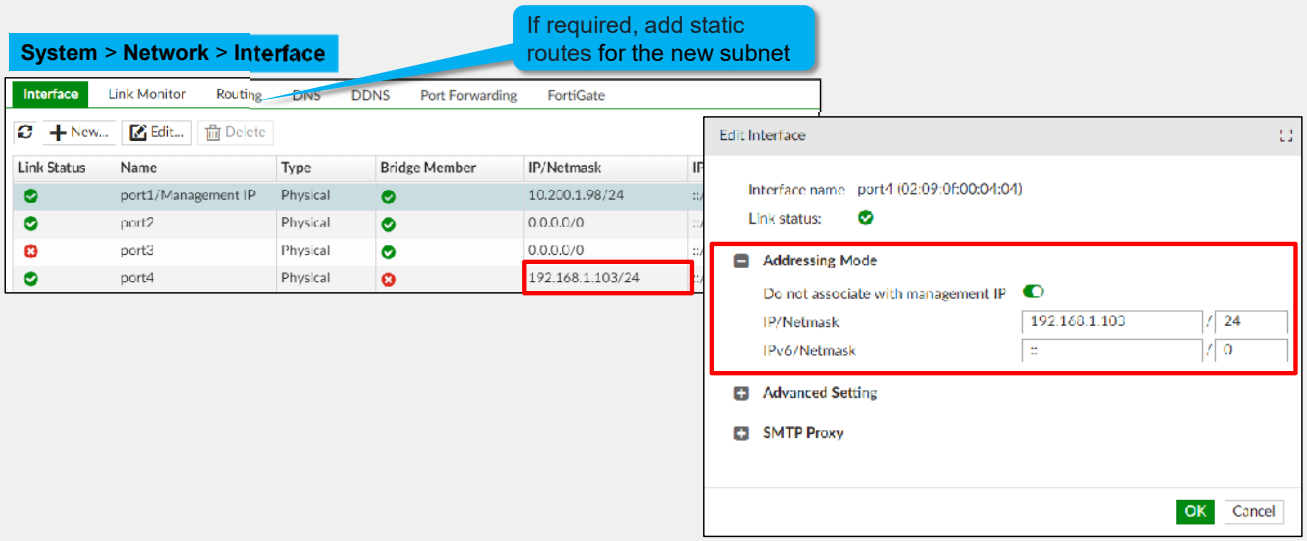
The built-in bridge forwards everything, not just SMTP traffic. Therefore, you can deploy transparent mode without having to make extensive topology changes. All SMTP traffic is picked up for inspection, and any non-SMTP traffic is bridged across the interfaces.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Out-Of-Bridge Interfaces

- You can remove any interface, except port1, from the bridge



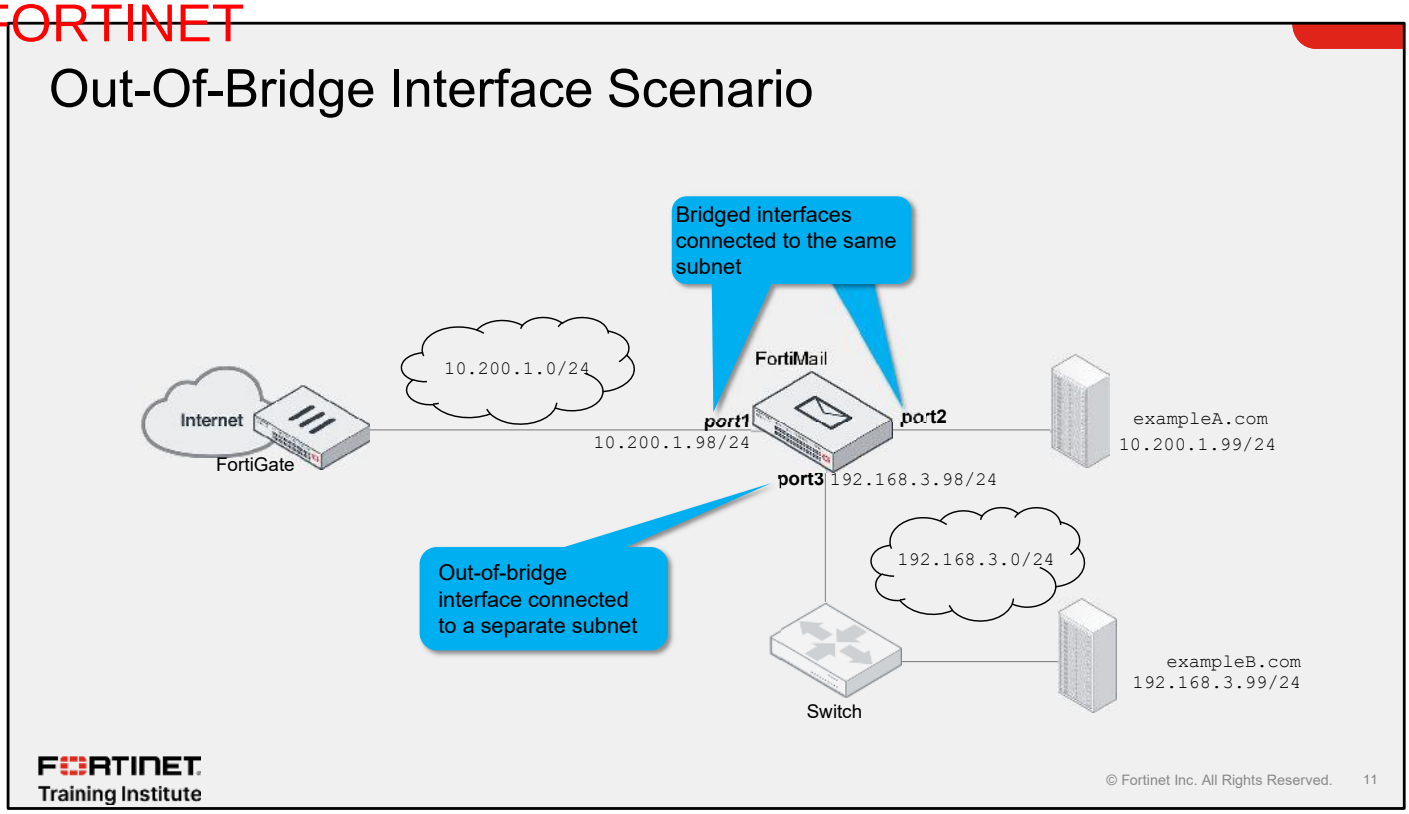
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

You can remove any interface, except port1, from the built-in bridge. This allows FortiMail to access more than one subnet, if the topology design requires it. Make sure you configure any additional static routes or define the gateway address for the new subnet.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In the example deployment shown on this slide, **port1** and **port2** are bridge members and are processing email for the `exampleA.com` domain in the `10.200.1.0/24` subnet. **port3** has been removed from the bridge and connected to the `192.168.3.0/24` subnet to process email for the `exampleB.com` domain.

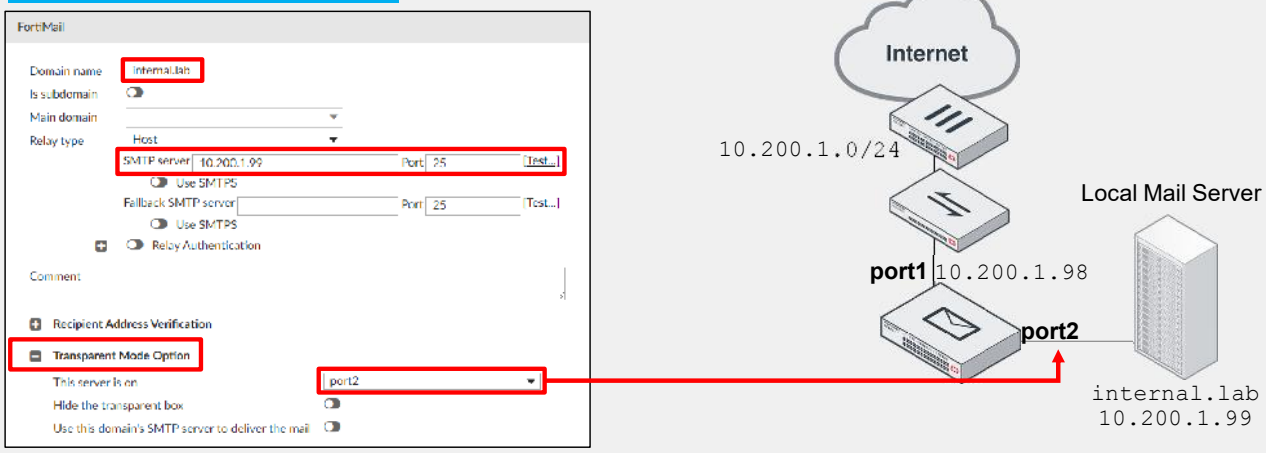
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Protected Domains

- Transparent mode domain configurations are similar to gateway mode
- Configure the settings in **Transparent Mode Options** to define the network interface to which the SMTP server is connected

Domain & User > Domain > Domain



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

Configuring a transparent mode protected domain is like configuring a gateway mode protected domain. You must configure the domain name and provide the back-end server IP address in the **SMTP server** field. However, in transparent mode you must also define the interface that the SMTP server is connected to.

Expand **Transparent Mode Options** and then, in the **This server is on** field, select an interface. This ensures FortiMail forwards all inspected email using the correct interface.

For more information about protected domains, see the *Basic Setup* lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiMail SMTP Session Handling—Transparent Mode

- FortiMail has two methods of handling SMTP sessions
  - Relay
  - Proxy
- Configured for incoming and outgoing connections
- It is important to understand session and email direction (inbound, outbound) when configuring SMTP session handling

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

When operating in transparent mode, FortiMail has two methods of handling an SMTP session—relay or proxy. Relay and proxy settings are configured for incoming and outgoing connections separately. Depending on the topology setup, these two methods can produce vastly different results in email routing. For this reason, it is important to understand session and email direction.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Relay

- FortiMail can use its built-in MTA to route SMTP sessions
  - Ignore original destination set by the SMTP client and uses its own MX record lookup to deliver email
- Can queue undeliverable messages and generate delivery status notification (DSN) email messages
- Default implicit method of handling sessions
  - The built-in MTA is used even though SMTP clients don't explicitly establish a connection to it

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

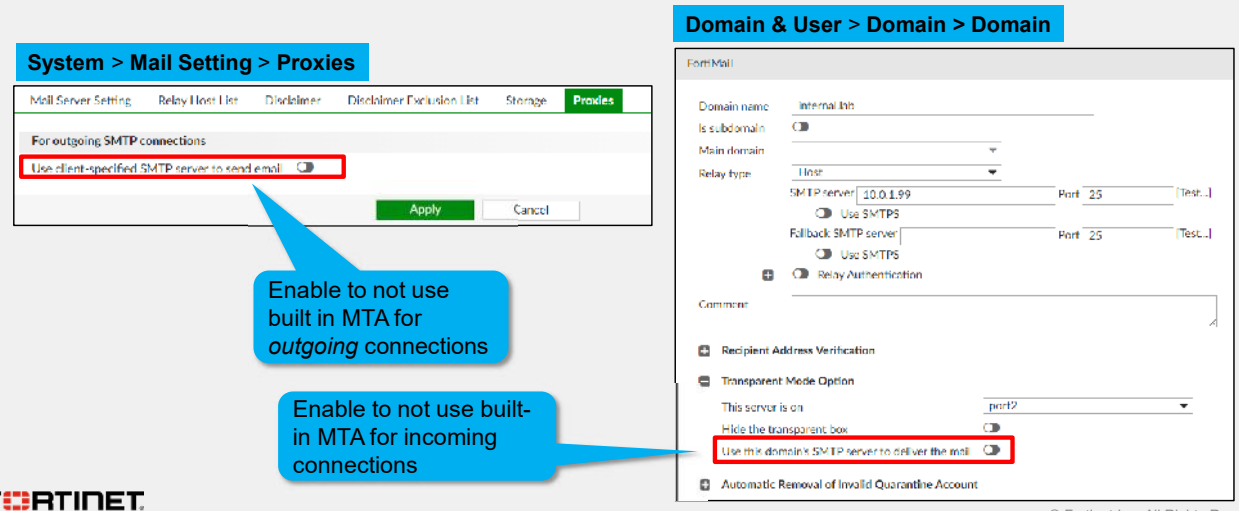
When using the built-in MTA to relay email, FortiMail uses MX record lookups to deliver email. Using this method, FortiMail can queue undeliverable messages and generate DSNs. The built-in MTA is used implicitly. This means SMTP clients don't explicitly establish a connection to it. This is also the default method for handling SMTP sessions in transparent mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Proxy

- FortiMail proxies a connection if you enable the proxy options applicable to the connection's directionality
- If you disable these settings, FortiMail uses the built-in MTA to relay email



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

FortiMail has two transparent proxies: an incoming proxy and an outgoing proxy. When configured to use the proxies, FortiMail doesn't do any DNS lookups of its own, and only attempts to deliver the message to the destination specified by the SMTP client. The incoming proxy supports message queuing; however, the outgoing proxy does not. Therefore, when using the outgoing proxy, FortiMail can't queue undeliverable messages or generate DSN email messages.

You can enable the proxy separately for each message flow direction. For outgoing sessions, on the **Proxies** tab, select **Use client-specified SMTP server to send email**. For incoming sessions, on the **Domains** tab, select the **Use this domain's SMTP server to deliver the email**.

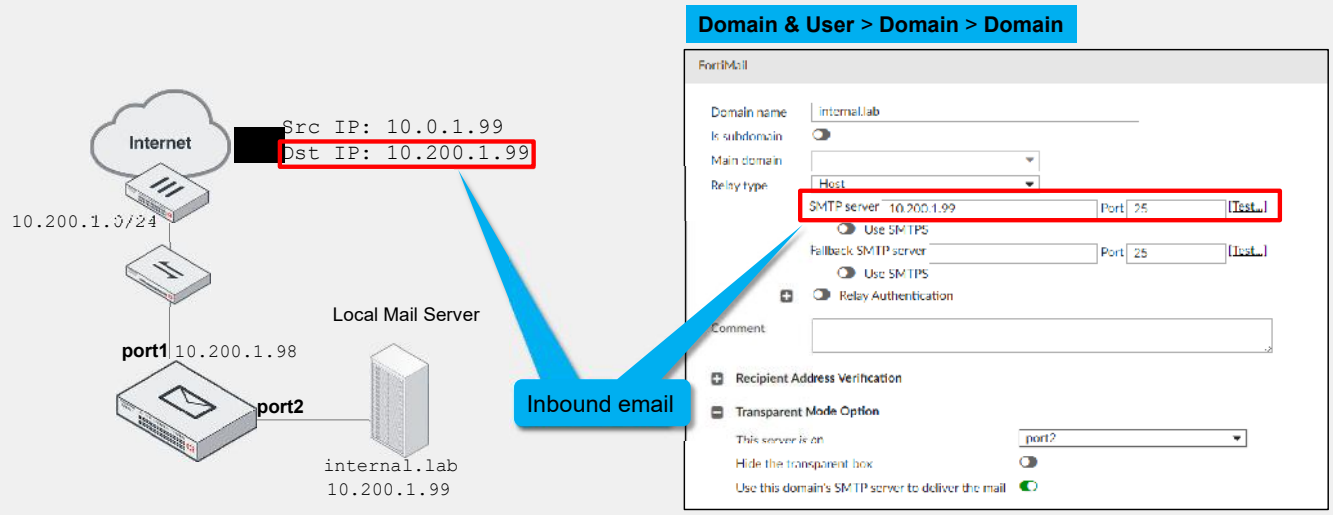
If you disable these options, FortiMail uses the built-in MTA to relay email.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Session Direction

- Destination IP matches **SMTP server** → incoming connection
- Destination IP does not match **SMTP server** → outgoing connection



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

At the network connection level, directionality is determined if the destination IP address of the IP header matches the defined relay server.

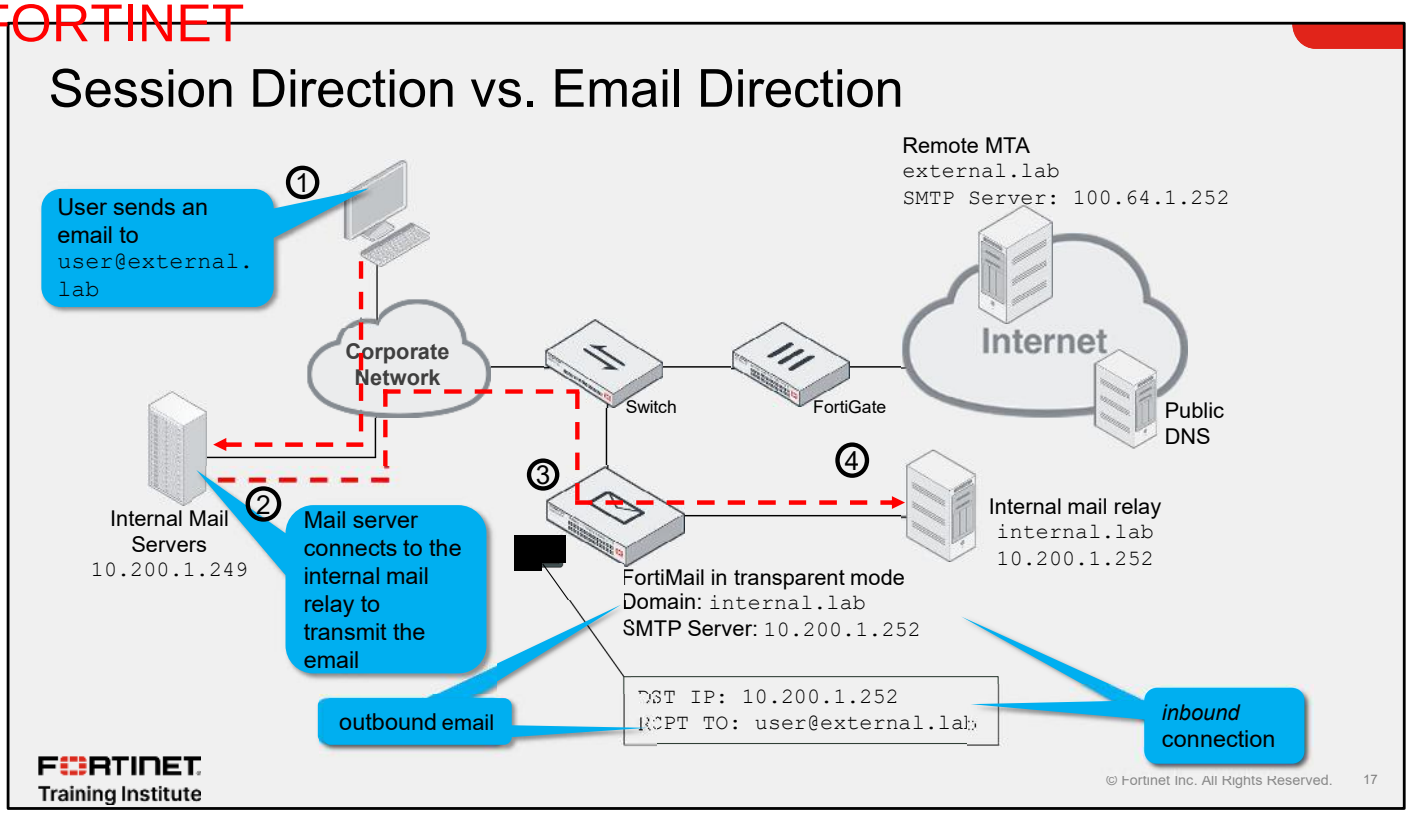
If the destination IP address *matches* a protected domain's SMTP server IP address, then it is an incoming connection.

If the destination IP address *does not* match any protected domain's SMTP server IP address, then it is an outgoing connection.

Unlike application-layer directionality, connection-level directionality does not consider the email's recipient domain (`RCPT TO:`). This can sometimes mean that the *session direction* is not the same as the *email direction*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



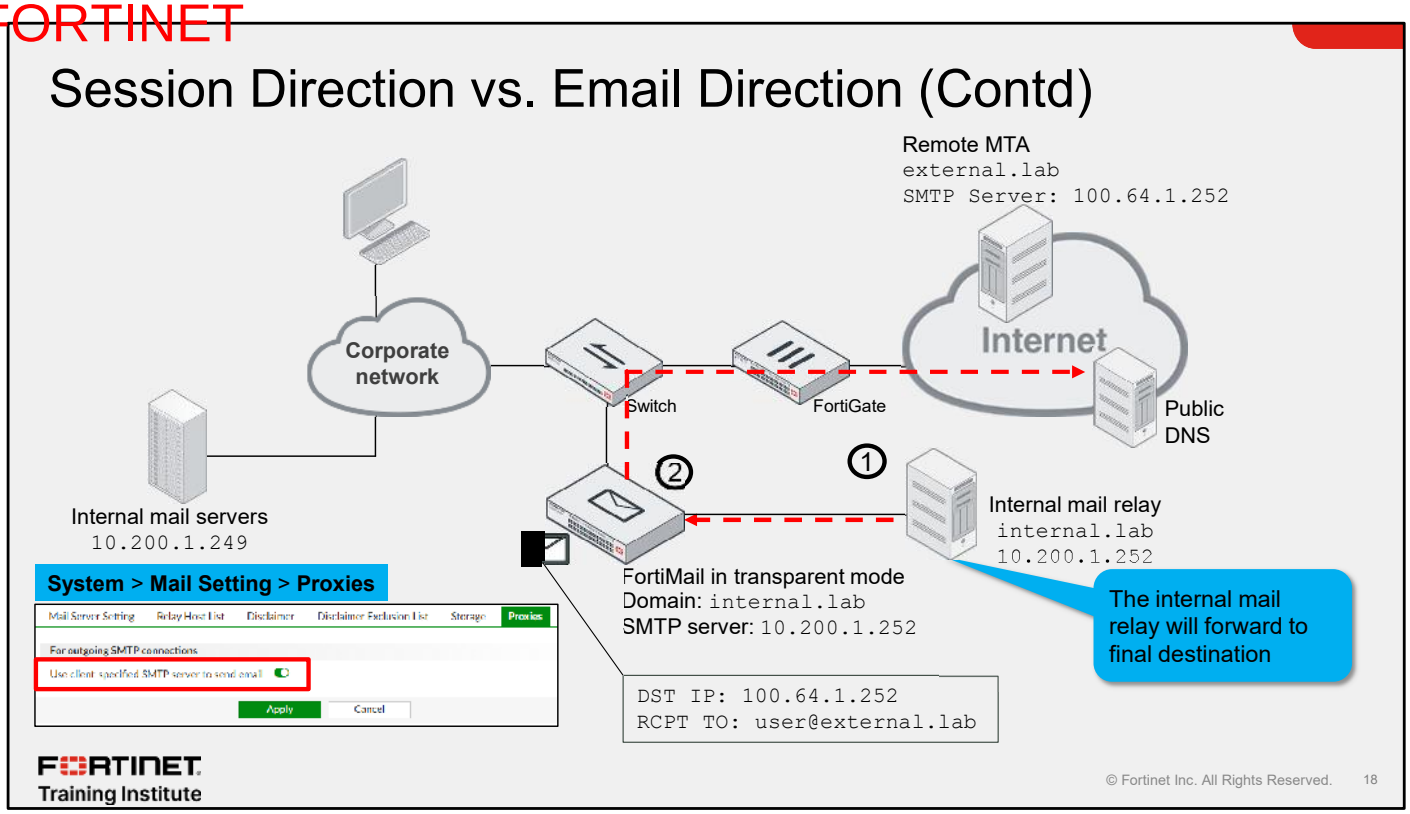
The example deployment scenario shown on this slide illustrates the difference between application-layer and network-layer directionality.

In this network, there is an internal mail relay server with the IP address `10.200.1.252`. All inbound email from remote MTAs for the `internal.lab` domain are delivered to this relay server. All outbound email generating from the internal mail servers also must flow through this relay server. Therefore, the transparent mode FortiMail is deployed in front of the internal mail relay server and configured to protect the `internal.lab` domain with the SMTP server `10.200.1.252`.

Users connect to an internal mail server to send an external email. When that email is sent to the internal relay server, it arrives at FortiMail with a destination IP of `10.200.1.252`, and a recipient domain of `external.lab`. According to FortiMail's directionality rules, this is an *inbound* connection sending an *outbound* email.

Vouchers & Dumps are Available | WhatsApp +201224560923

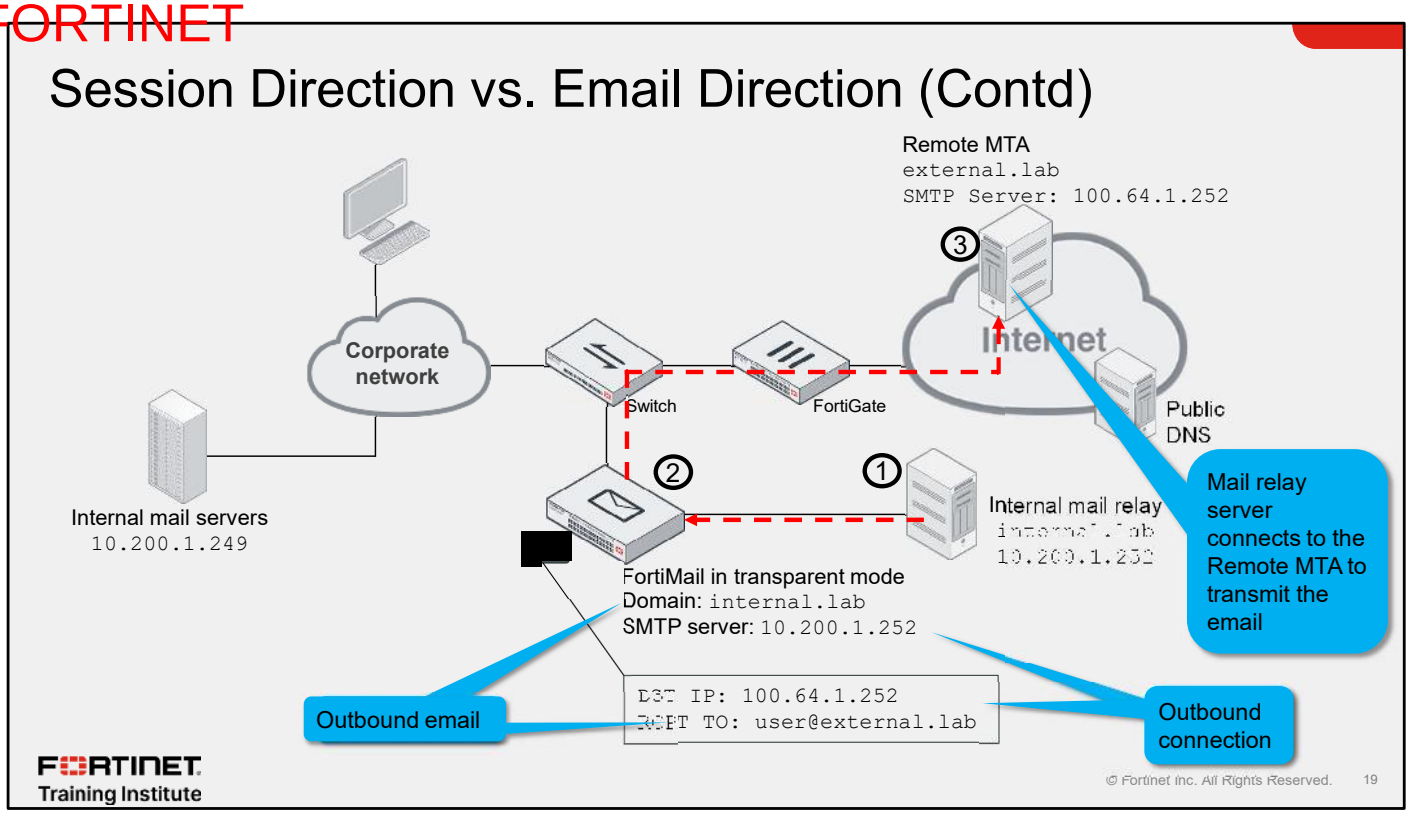
DO NOT REPRINT Brave-dumps.com
© FORTINET



The internal mail relay server will query the public DNS server to resolve the `external.lab` domain. If **Use client-specified SMTP server to send email** is enabled, then the transparent mode FortiMail device will route the email message based on the destination IP that has been resolved by the internal mail relay server, which in this example is `100.64.1.252`. If not, FortiMail performs its own lookup and attempts to deliver the mail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When the email message is sent to the remote MTA server, it arrives at FortiMail with a destination IP address of `100.64.1.252`, and a recipient domain of `external.lab`. According to FortiMail directionality rules, this is an *outbound* connection sending an *outbound* email.

Vouchers & Dumps are Available | WhatsApp +201224560923

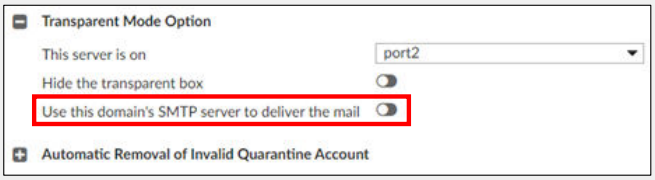
DO NOT REPRINT Brave-dumps.com
© FORTINET

Transparent Mode Mail Routing

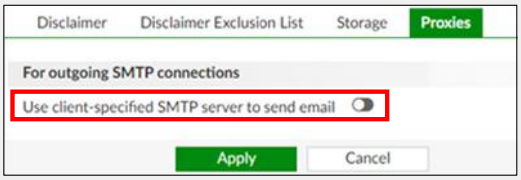
- The **Mailer** column in the history log indicates which subsystem handled the connection:
  - `mta`: The connection was handled by the built-in MTA
  - `proxy`: The connection was handled by either the incoming proxy or the outgoing proxy

Destination IP	Recipient Domain is a:	Configuration	Result
SMTP server (inbound session)	Protected domain (inbound email)	N/A	Built-in MTA
	Not a protected domain (outbound email)	Use this domain's SMTP server to deliver the mail enabled	Incoming proxy
		Use this domain's SMTP server to deliver the mail disabled	Built-in MTA
Not an SMTP server (outbound session)	N/A	Use the client-specified SMTP server to send email enabled	Outgoing proxy
		Use the client-specified SMTP server to send email disabled	Built-in MTA

System > Mail Setting > Proxies



Domain & User > Domain > Domain



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

The flow chart on this slide shows which sessions are handled by the built-in MTA and which sessions are handled by the proxies.

Any *inbound* session with an *inbound* email (email domain is a protected domain), is always processed by the built-in MTA, regardless of the proxy configuration.

Any *inbound* session with an *outbound* email is processed, depending on the proxy configuration.

Any *outbound* session processing also depends on the proxy configuration.

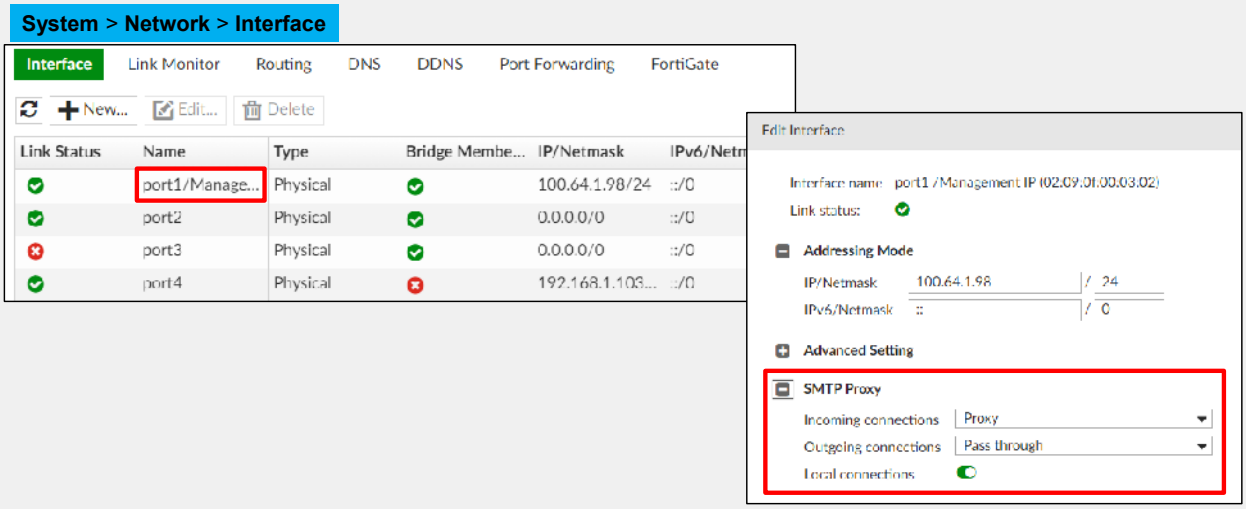
To determine whether a connection was handled by the built-in MTA or one of the proxies, in the history log messages, view the **Mailer** column.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Connection Pickup

- To perform inspection on specific mail flows, the administrator must enable connection pickup on the interfaces



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

The SMTP proxy settings for each interface define which email flows are picked up by FortiMail. Be careful not to confuse the terminology used here, which includes the term, “proxy”, with seperate discussions about transparent proxy versus built-in MTA. For each interface, you can select an action for each direction of SMTP sessions.

When you select **Proxy**, FortiMail will inspect the email messages that arrive at the interface. If you select **Pass through**, FortiMail forwards the email message to its original destination without any inspection. If you select **Drop**, FortiMail drops the email message.

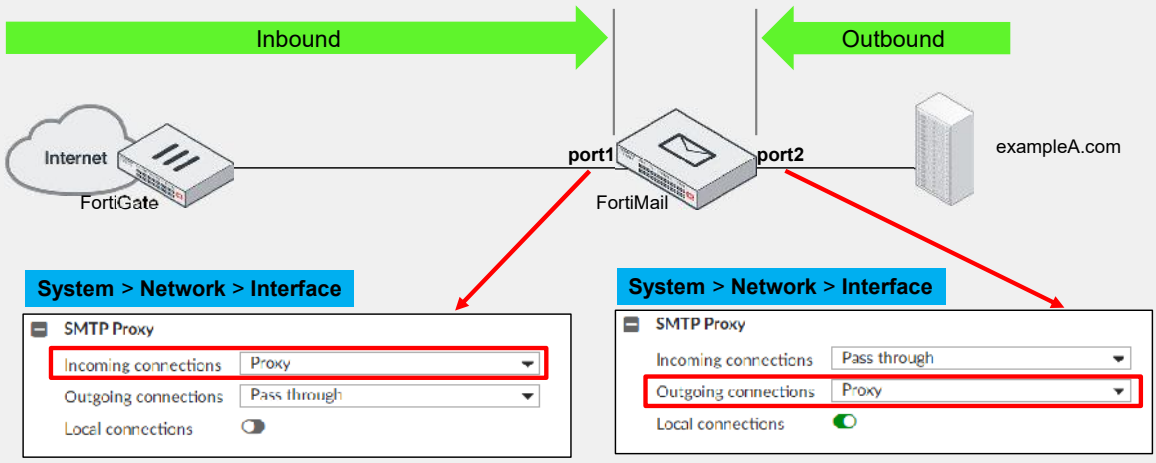
The **Local connections** setting controls whether clients can connect to that interface for FortiMail services like webmail access, IBE access, and the administration interface. How you configure these settings depends on your FortiMail setup.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Connection Pickup (Contd)

- Sessions should be picked up closest to the source



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

When configuring SMTP proxy pickup, it is important to make sure that you aren't scanning the same traffic twice. A good rule to follow is to pick up sessions closest to the source.

In the example deployment shown on this slide, **port1** is the closest interface to the source for all inbound email (internet); therefore, **port1** incoming connections are proxied. **port2** is the closest interface to the source for all outbound email; therefore, **port2** outbound connections are proxied.

Note that this rule might not apply to all deployments. For example, a transparent mode FortiMail without any protected domains would need to proxy only outgoing connections, since all email for that specific deployment would be considered outgoing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configuring Transparency

- Regardless of the routing method used, by default, a transparent mode FortiMail doesn't hide its presence
  - IP sessions
    - Bridged interfaces use the management IP
    - Out-of-bridge interfaces use the interface IP
  - SMTP envelope
    - EHLO/HELO greeting
  - SMTP header
    - `Received:` headers
- You must explicitly configure FortiMail to remove these traces to have true transparency

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

By default, FortiMail in transparent mode is not truly transparent. Evidence of its existence can be found in the IP headers, SMTP session banner, EHLO/HELO greetings, and email message headers.

IP sessions are sourced from the management IP, if using a bridge member interface, or the interface IP, if using an out-of-bridge interface. This will be evident in any packet captures of email messages traversing a transparent mode FortiMail. The SMTP session banner and EHLO/HELO greetings are also replaced by the transparent mode FortiMail interface IP address. The email message headers will also include information about the transparent mode FortiMail that processed the email.

You must explicitly configure transparency, whether using the proxies or the built-in MTA.

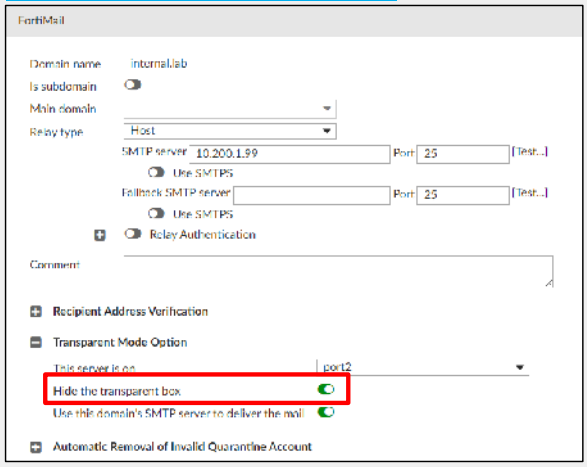
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Inbound Transparency

- **Transparent Mode Options** in the protected domain configuration
  - **Hide the transparent box**
    - Preserves the remote sender's IP address and domain in all inbound sessions

Domain & User > Domain > Domain



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

To hide FortiMail in all inbound sessions, on the **Domain** tab, in the **Transparent Mode Options** section, enable **Hide the transparent box**. This preserves the session originator's source IP in the IP header, the SMTP greeting messages in the envelope, and the email message headers.

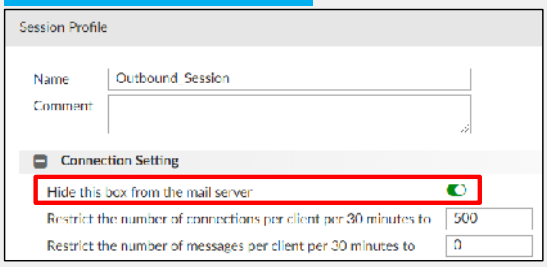
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

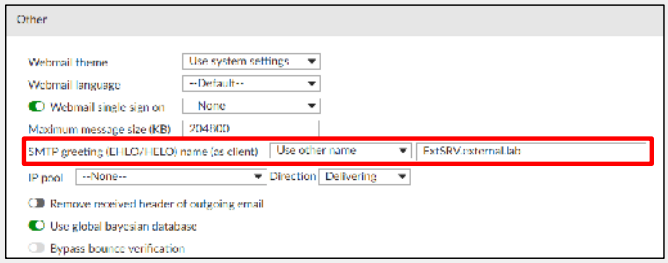
Outbound Transparency

- Preserve the SMTP server's IP address in all outbound sessions
  - **Connection Settings** in a session profile
    - **Hide this box from the mail server**
- Replicate SMTP server's SMTP greetings to preserve received headers
  - **Other** settings menu under the Domain **Advanced Settings**
    - **SMTP Greeting (EHLO/HELO) Name (As Client)**

Profile > Session > Session



Domain & User > Domain > Domain > Advanced Setting



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

To hide FortiMail in outbound sessions, you need to configure a session profile as shown on this slide. This preserves the protected SMTP server's source IP in the IP header.

You can apply session profiles using an IP-based policy only. For more information about how to create outbound IP policies, see the *Access Control and Policies* lesson.

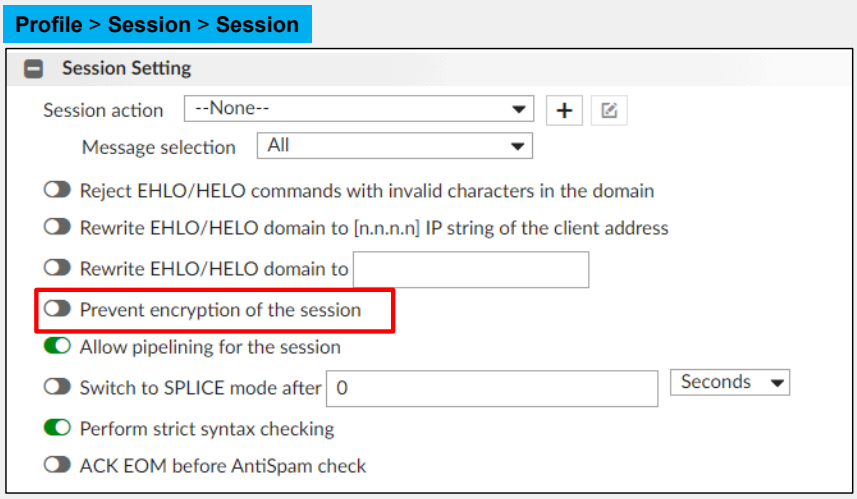
To replicate the back-end server's SMTP greetings, and preserve email message headers, you must configure the protected domain settings as shown on this slide. Typically, this value should be the same HELO/EHLO greeting that the back-end mail server uses.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Encrypted Sessions

- Transparent mode FortiMail can't scan encrypted sessions
- Enable **Prevent encryption of the session** to allow FortiMail to block the STARTLS command



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

Transparent mode FortiMail can't scan encrypted sessions. If the back-end server supports STARTTLS, you must configure a session profile as shown on this slide and apply it using an IP-based policy. When you enable **Prevent encryption of the session**, FortiMail blocks the STARTTLS command during the SMTP message exchanges.

You can enable this option in a session profile and apply it using IP-based policies. For more information about how to configure IP-based policies, see the *Access Control and Policies* lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. How does the built-in bridge handle non-SMTP traffic on a FortiMail device that is operating in transparent mode?
   - ✓ A. It bridges the non-SMTP traffic through without any inspection.
   - B. It drops all non-SMTP traffic.

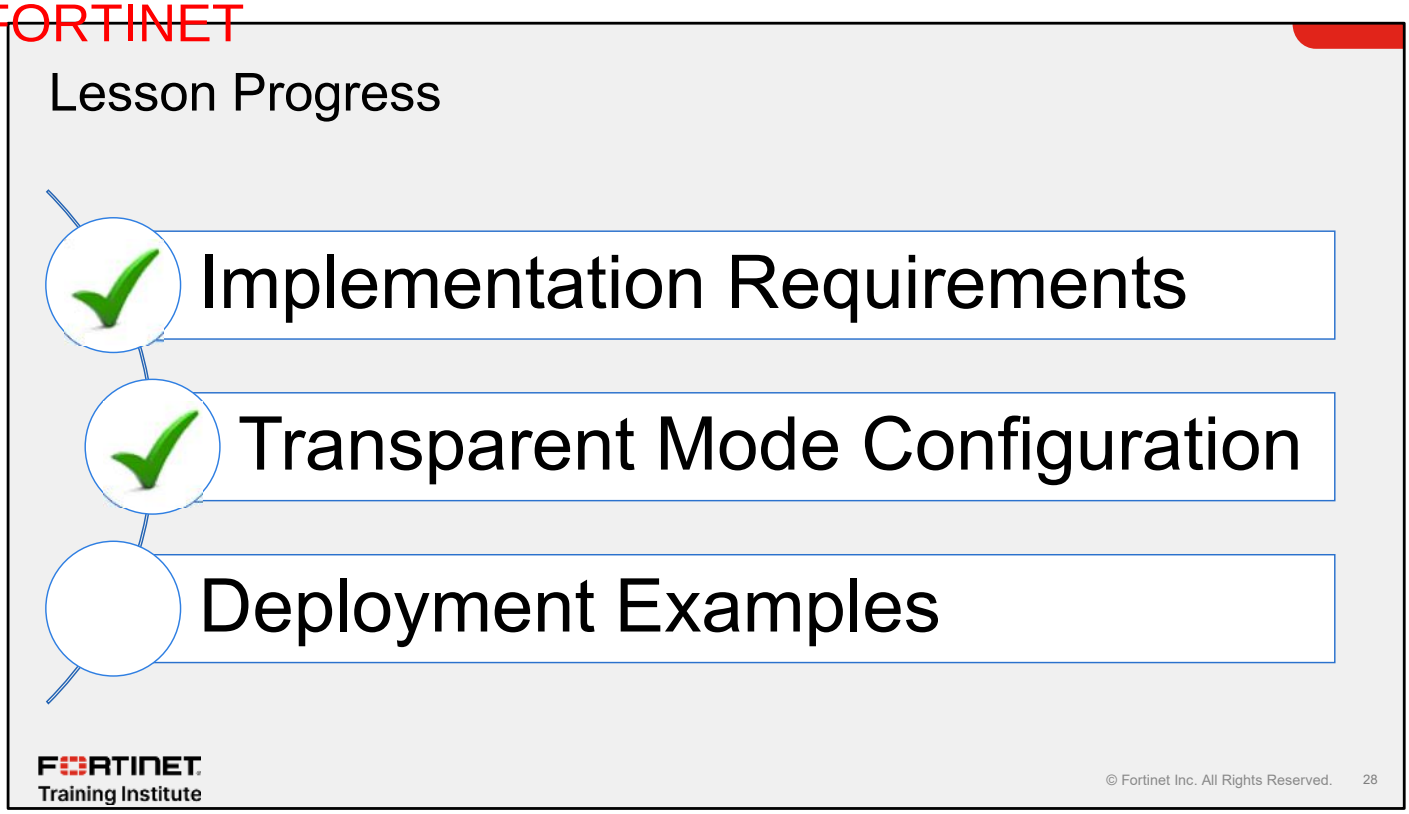
2. Which feature must you enable for inbound email transparency?
   - A. **Hide this box from the mail server**, in the session profile
   - ✓ B. **Hide FortiMail**, in the domain settings

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Good job! You now understand transparent mode configuration.

Now, you'll learn about some deployment examples.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Deployment Examples

Objectives

- Identify deployment requirements for transparent mode FortiMail in different sized networks

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 29

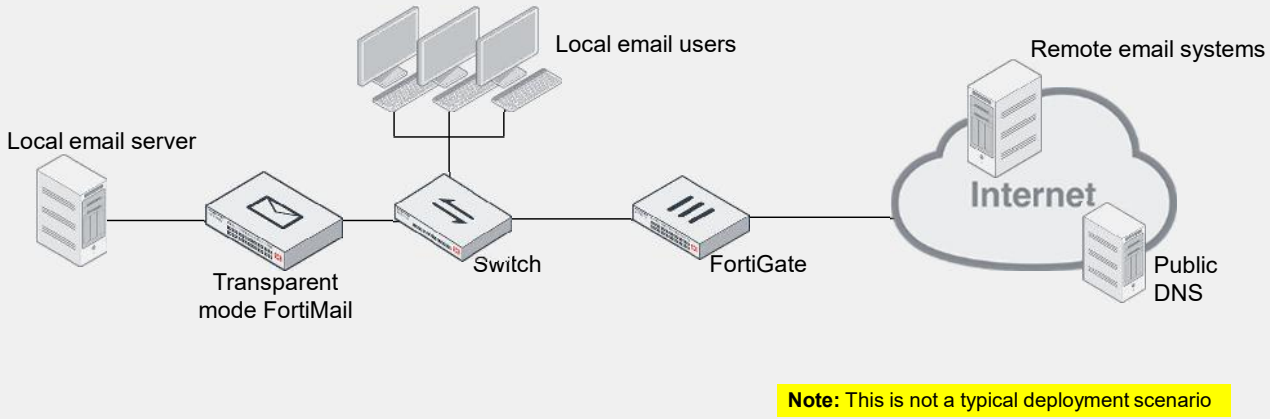
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding different deployment scenario requirements, you will be able to determine how to most effectively use a transparent mode FortiMail in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SMB Example



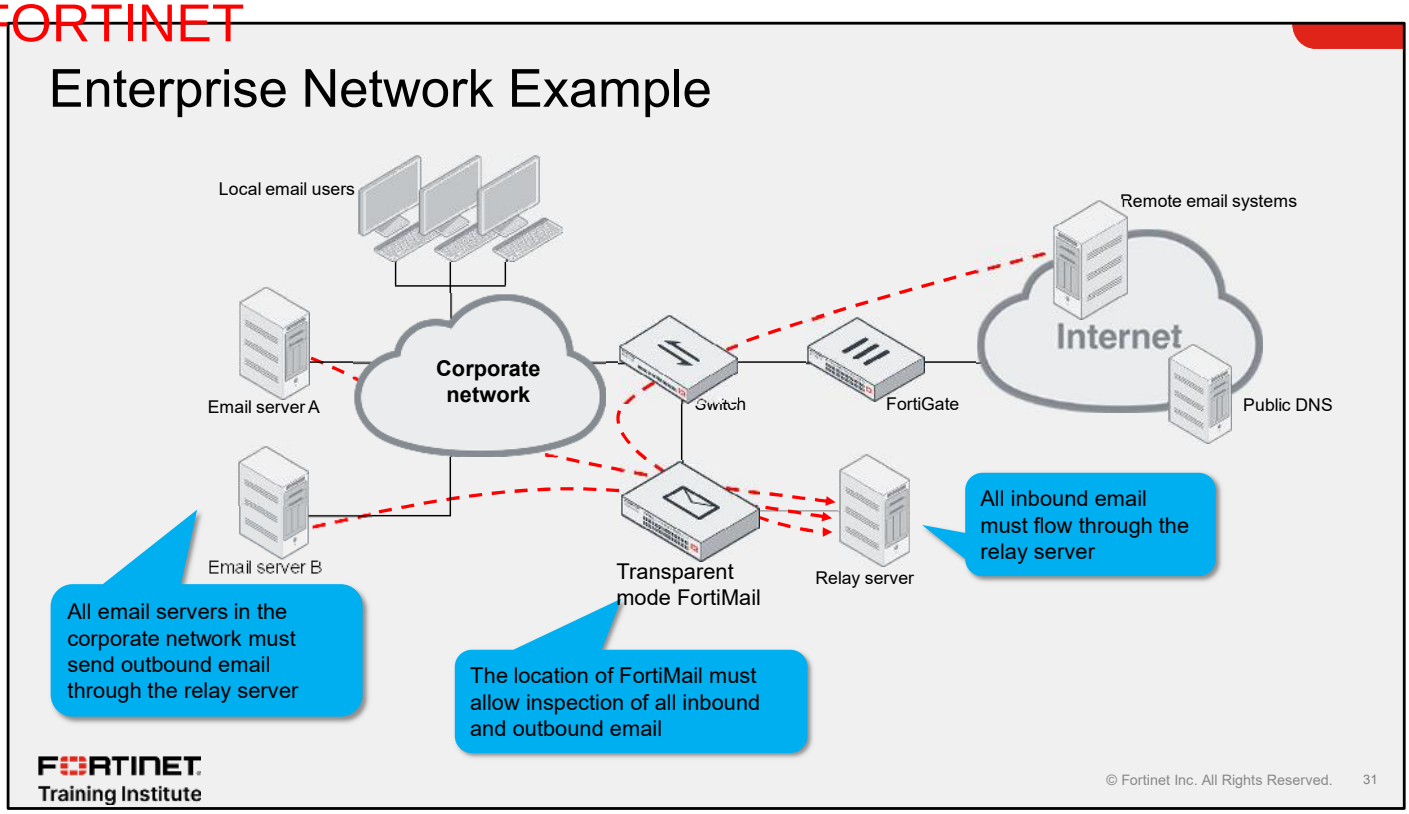
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

In SMB deployments, the networks are less complicated. Deploying FortiMail in transparent mode is as simple as positioning FortiMail directly in front of the local mail server. If there are no additional relay servers, then you should use the built-in MTA for outbound connections. If there are relay servers, you should proxy connections in both directions.

Vouchers & Dumps are Available | WhatsApp +201224560923

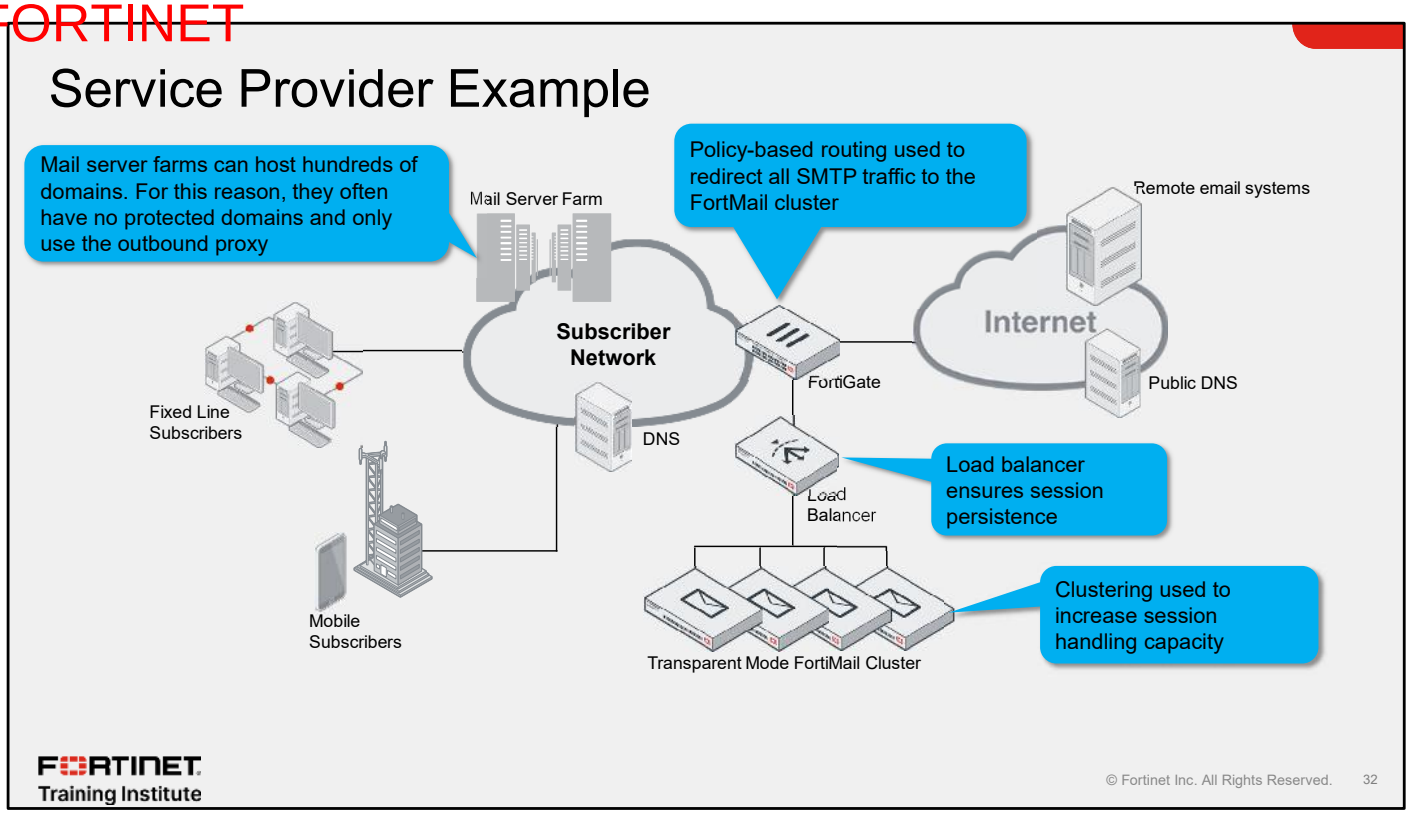
DO NOT REPRINT Brave-dumps.com
© FORTINET



Enterprise networks might have multiple branch offices with their own mail servers connected to the corporate network. The challenge with these deployments is to position FortiMail where it can inspect all inbound and outbound connections. If there is a global relay server for the whole corporate network, then you should position FortiMail in front of the global relay server, and proxy connections in both directions. If there are no relay servers, then you can use a methodology like the one used in SMB deployments and position FortiMail in front of the corporate email servers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



For service providers, it is more common to find transparent mode FortiMail devices deployed without any protected domains. The scope of these deployments is so large that it is not feasible to maintain a full list of protected domains. These types of deployments usually use strict IP policy-based inspection.

Clustering is typically used to increase session handling capacity. Load balancers are used to maintain session persistence. Policy-based routing is used to redirect all SMTP traffic to the FortiMail cluster.

When not configured with any protected domains, all emails are considered outbound by the transparent mode FortiMail. Since there can be hundreds of subscribers with different MUA settings, the FortiMail devices are usually configured to use only the outbound proxy, with full transparency.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Why do service providers typically deploy transparent mode FortiMail devices without any protected domains?
   A. There is a limit of 10 protected domains on FortiMail.
   ✓ B. It is not feasible to maintain a full list of protected domains for a service provider.

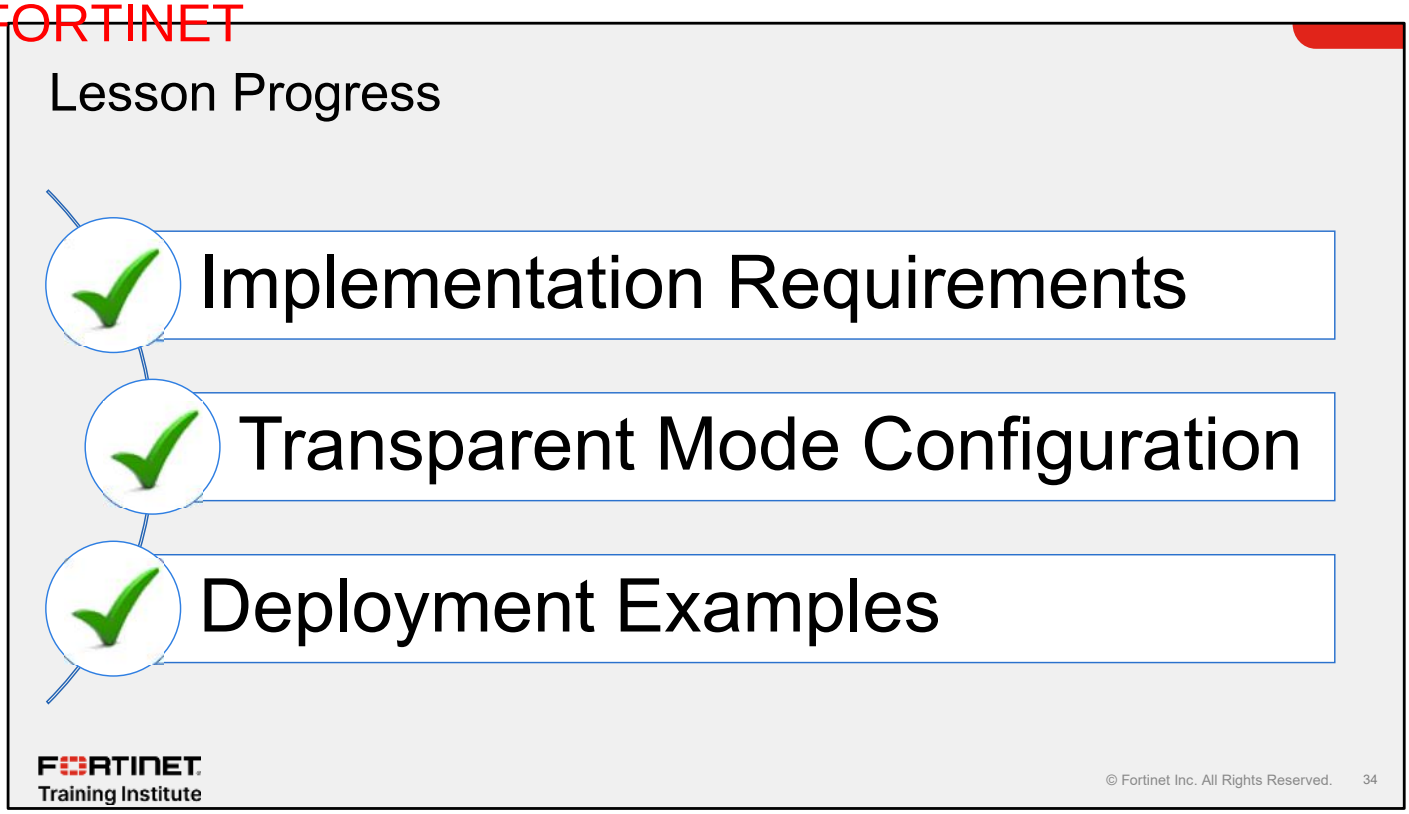
2. Where should you deploy transparent mode FortiMail in an enterprise network?
   A. At the edge of the corporate network
   ✓ B. In front of the global mail relay server

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Congratulations! You have completed this lesson.

Now, you will review the objectives covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Describe transparent mode network topology requirements
- ✓ Configure access receive rules for bidirectional email flow
- ✓ Configure bridge and out-of-bridge interfaces
- ✓ Configure transparent mode protected domain options
- ✓ Configure transparent mode mail routing features
- ✓ Configure transparency
- ✓ Identify deployment requirements for transparent mode FortiMail in different sized networks

FORTINET Training Institute

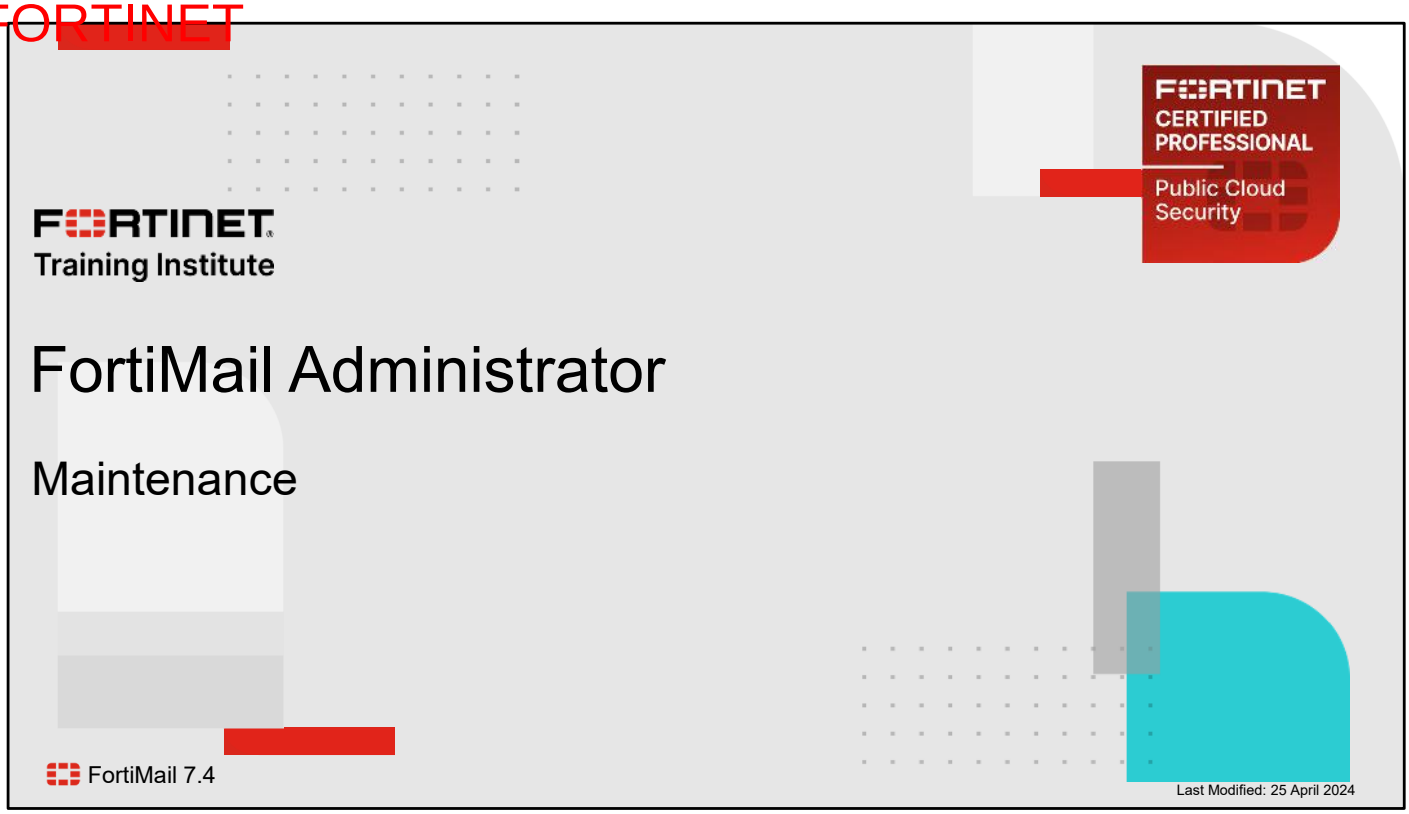
© Fortinet Inc. All Rights Reserved. 35

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you have learned how to deploy FortiMail in transparent mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

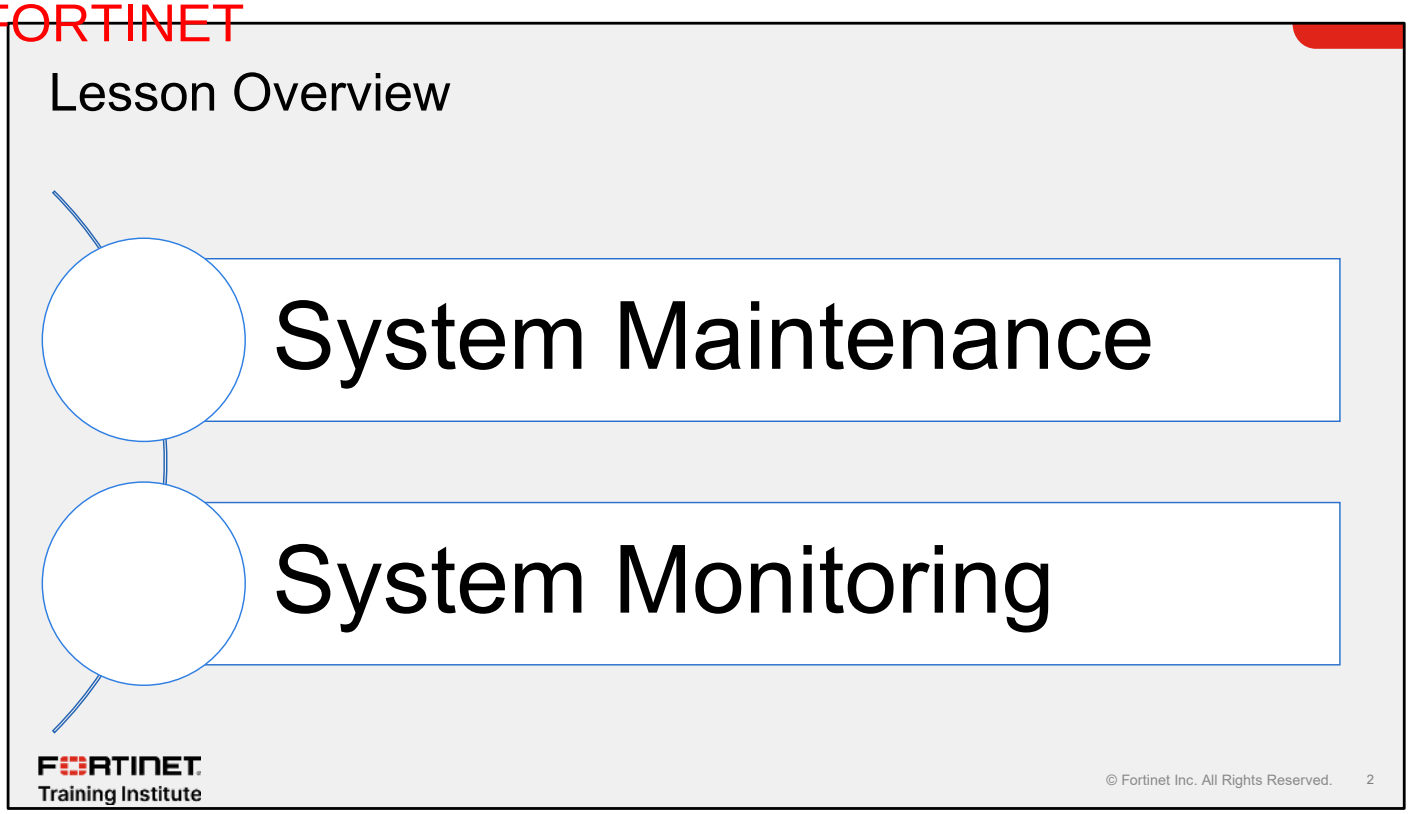
DO NOT REPRINT Brave-dumps.com
© FORTINET



In this lesson, you will learn some useful tips for maintaining your FortiMail device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

System Maintenance

Objectives

- Perform local storage management tasks
- Verify FortiGuard service status
- Monitor system resource use and network interface status
- Back up and restore system configuration and mail data
- Reset FortiMail configuration

FORTINET Training Institute

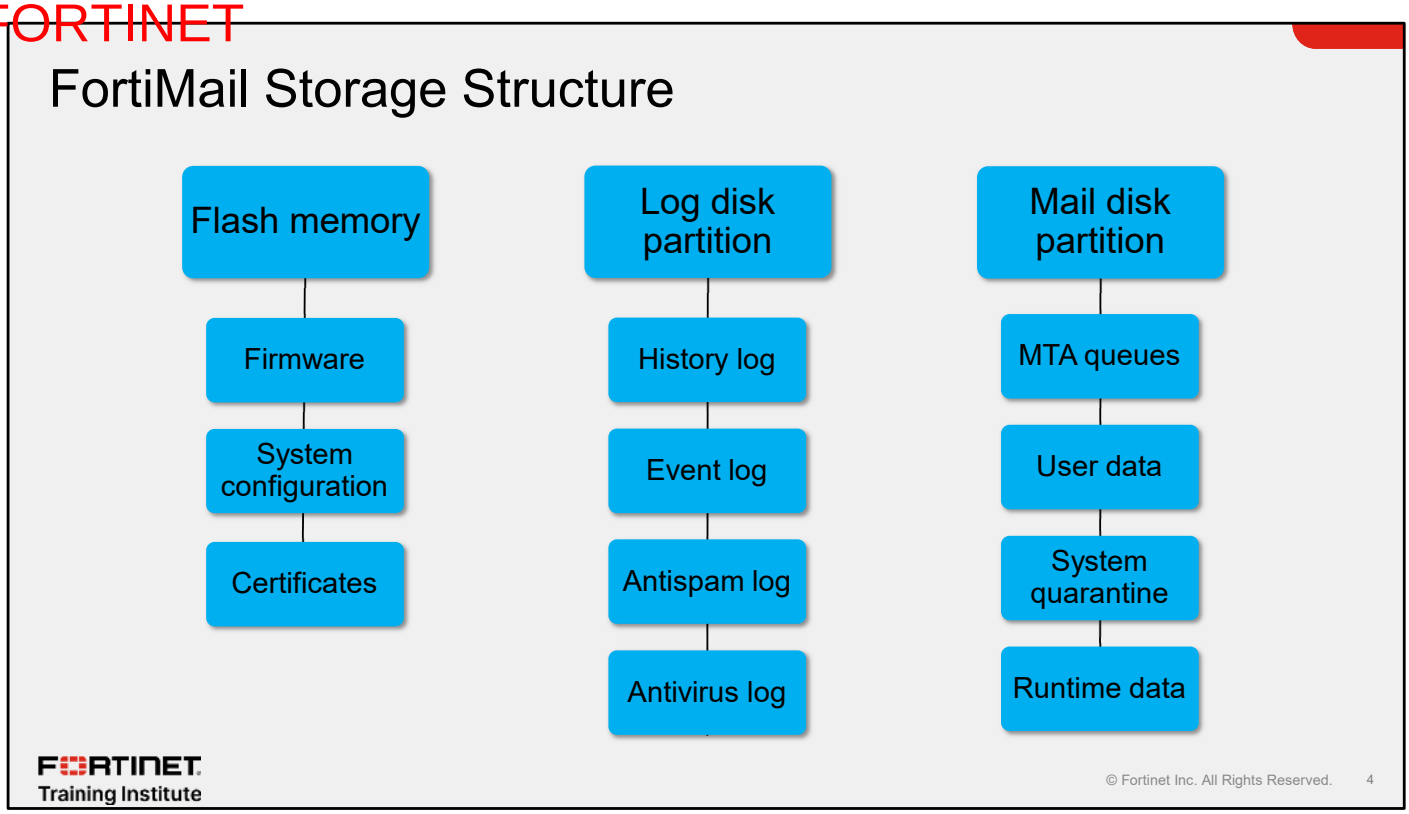
© Fortinet Inc. All Rights Reserved. 3

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in performing system maintenance, you will be able to effectively maintain FortiMail operation.
.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiMail stores stateful information in three separate areas of storage.

The flash memory stores the FortiMail firmware, current system configuration, and the certificate store.

The log disk stores all log data in a dedicated fixed-size partition.

The mail disk is used for mail transfer agent (MTA) queues, system quarantine, user data and quarantines, user mailboxes (server mode), identity-based encryption (IBE) messages, and runtime data.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Storage Partitioning

- By default, mail disk partition size is 80% of total disk
- Partition size can be modified using the CLI:

```
# execute partitionlogdisk <amount>
```

- Partition amount is a percentage of total disk space to give to log disk (min is 5%, max is 95% and remainder is given to mail disk)
- **Caution:** All mail and log data will be lost when the partition size is modified!

FORTINET Training Institute

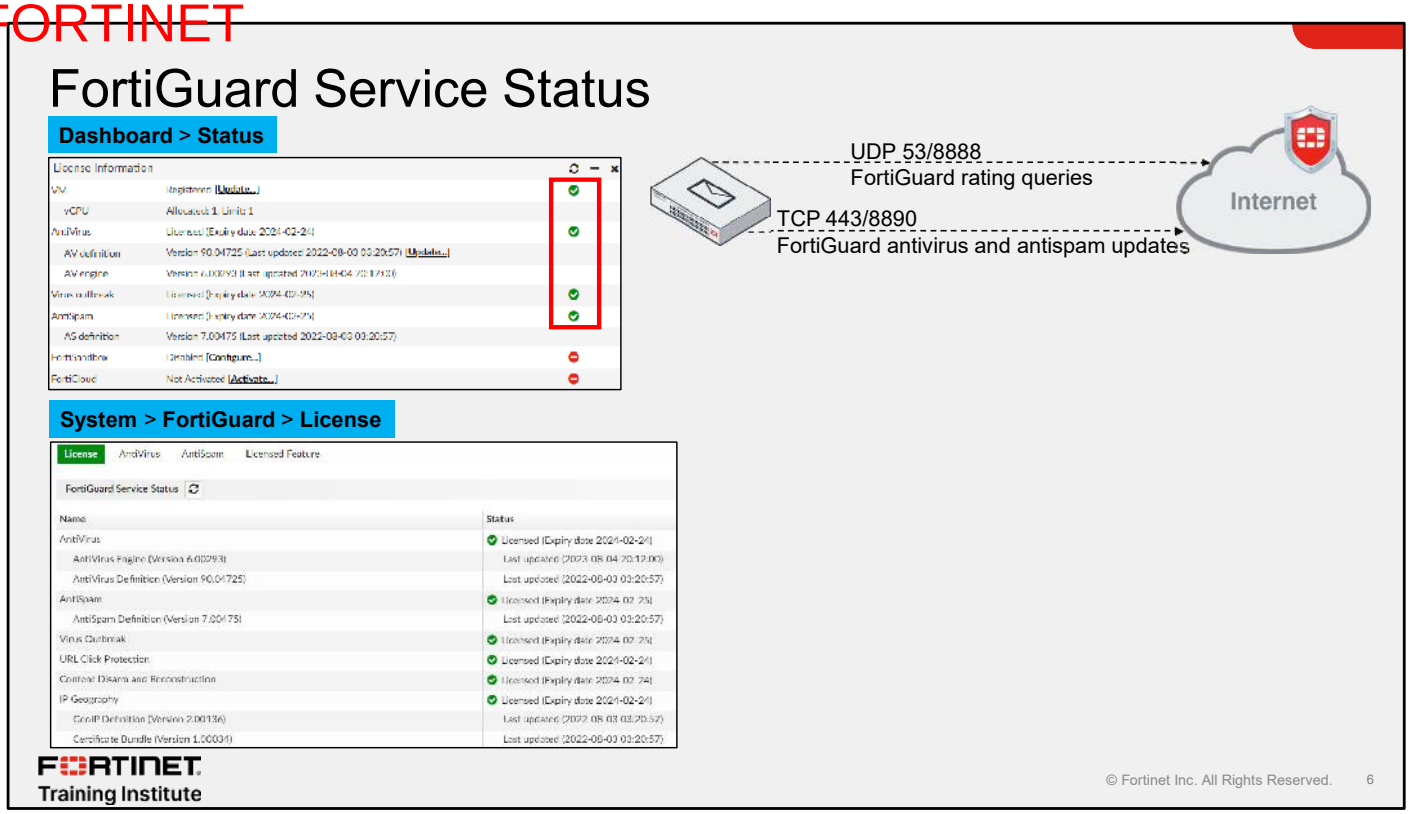
© Fortinet Inc. All Rights Reserved. 5

One of the important decisions that you must make when you install FortiMail is how to allocate the storage for logs and mail data. By default, the storage is split so that 80% is used for mail data and 20% is used for logging. With some implementations, it may make sense to adjust the default allocation. For example, because FortiMail doesn't store user mailboxes in gateway mode, it might be advantageous to reduce the size of the mail data disk and expand the size of the logging disk so more log data is available.

You can use the CLI to change the percentage of storage allocated to logging and mail data but be aware that both storage partitions will be reformatted, and any existing data will be lost. Because of this, plan to perform the partitioning task during the initial stages of deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

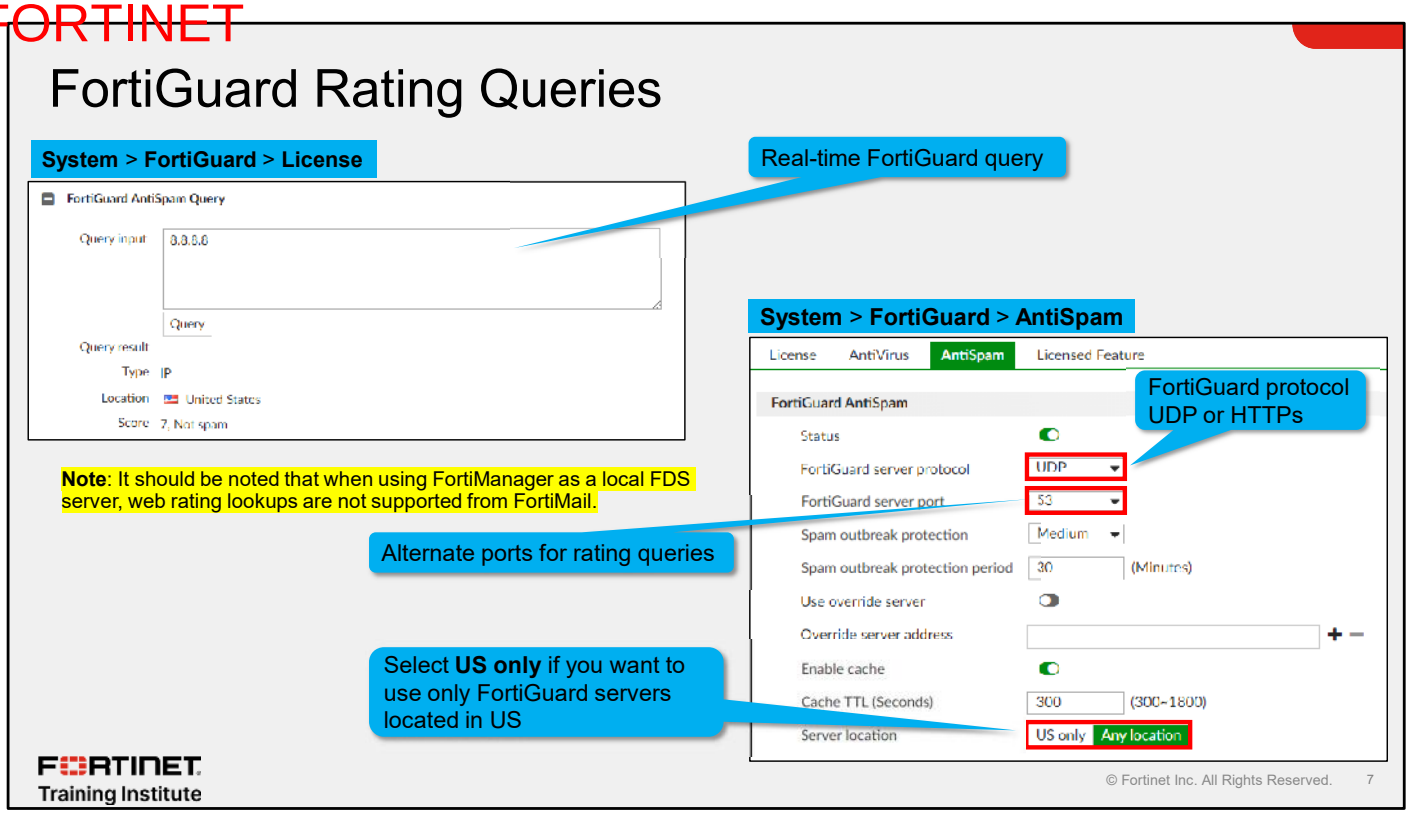


FortiGuard subscription services are integral to FortiMail. Regular updates to the FortiGuard antispam and antivirus databases are required to ensure that FortiMail accurately detects these threats as they emerge and change over time. In addition, several antispam scan techniques involve real-time communications with the FortiGuard Distribution Network (FDN). Monitoring the status of these FDN communications ensures accurate results.

Use the **License Information** widget on the dashboard to quickly view the current status of FortiGuard connectivity. For more information about the last update timestamp, as well as version information for the antivirus engine, and various other definition databases, use the **License** page, as shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Use the FortiGuard query tool to validate that FortiMail can successfully communicate with the FDN for rating queries. A successful response means FortiMail is communicating with FDN accurately.

By default, FortiMail submits all rating requests on UDP port 53. This makes all rating query traffic appear as DNS traffic. Certain firewalls perform special inspection tasks on all DNS traffic, which may have an adverse effect on the rating queries. In these scenarios, use one of the alternate service ports as a workaround, but make sure the proper firewall rules are in place to allow traffic on the alternate port.

It should be noted that when using FortiManager as a local FDS server, web rating lookups are not supported from FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

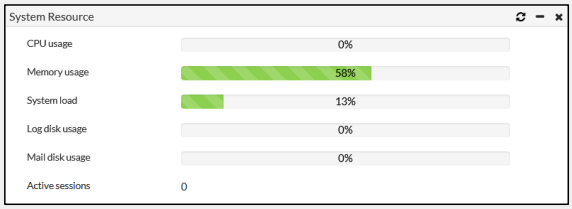
CPU and Memory Usage

- CLI

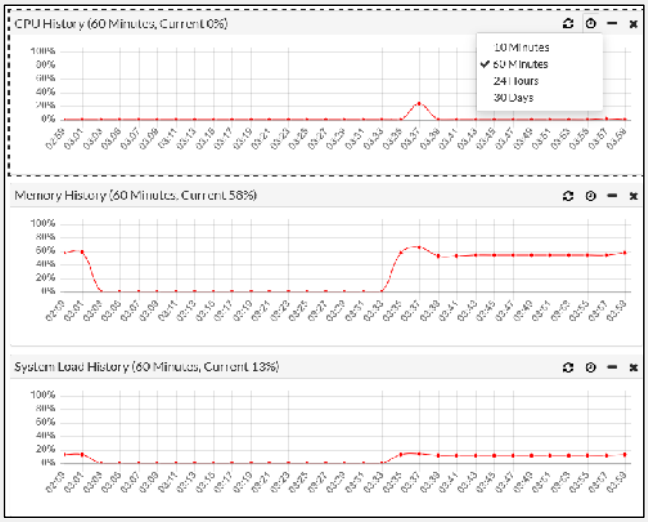
```
# get system performance
CPU usage:  0% used, 100% idle
Memory usage: 30% used
System Load: 7
Uptime:    9 days 8 hours 32 minutes
```

- GUI

Dashboard > Status



Dashboard > Status



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 8

You can display CPU and memory use on both the GUI and the CLI. Observing changes in these values can be useful when enabling or tuning various features FortiMail features. In the **System Resource** widgets, you can access historical resource usage data for the last 24 hours.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Resource Usage

- Real-time CPU and memory monitor

```
# diagnose system top
```

```
System Time:  2024-01-10 12:09:37 PST (Uptime: 2d 0h 21m)
CPU:   0.2% usr  0.1% sys  0.0% nice  0.4% idle  0.2% io  0.0% irq  0.0% sirq
Mem: 1491M total, 591M free, 44M buff, 540M cached
     COMMAND        PID  STAT  CPU %CPU     RSS %MEM
       dbmanager   9582  S      0   0.0    104m  6.9
     mailfilterd   9805  S      0   0.0   93884  6.1
        admin.fe   9821  S      0   0.0   79992  5.2
         cmdbsvr   9583  S <    0   0.0   66120  4.3
      expiremail   9781  S N    0   0.0   62576  4.0
       expireenc   9804  S N    0   0.0   58948  3.8
         dlpsmbd   9783  S      0   0.0   54764  3.5
             cli  10559  S      0   0.0   40452  2.6
          smtpd:   9787  S      0   0.0   39928  2.6
      ipcheck.fe   9822  S      0   0.0   39616  2.5
         smtpqd:   9788  S      0   0.0   38140  2.4
            msa:   9791  S      0   0.0   35828  2.3
       urlfilter   9773  S      0   0.0   31260  2.0
```

Status codes:
- **R** = running
- **S** = interruptible sleep
- **D** = uninterruptable sleep
- **T** = stopped
- **N** = low priority
- **<** = high priority

Processes in **D** state are an indication of disk I/O latency. You can attempt to reload a process using the command: `execute reload <process name>`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

Use the command shown on this slide to display CPU and memory usage in real-time in the CLI. The output lists the internal FortiMail processes that are currently consuming the most CPU time, as well as the memory use of each process. This display continuously refreshes every five seconds until you press q.

This information can be invaluable for tuning the performance of FortiMail as well as diagnosing issues, such as I/O performance and runaway processes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Network Interface Status

- Errors at the interface indicate data link layer and physical layer issues

```
# diagnose net interface list <interface-name>

if=port1 family=00 type=1 index=4 mtu=1500 link=0 master=0 flags=up
broadcast run multicast
Qdisc=pfifo_fast hw_addr=00:0c:29:f3:53:a4:
broadcast_addr=ff:ff:ff:ff:ff:ff:
stat: rxp=1222436 txp=1140364 rxb=251546955 txb=186120344 rxe=0 txe=0
rxd=0 txd=0 mc=0 collision=0
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
```

Link is up

RX/TX packets and bytes

RX/TX errors/drops in packets/frames

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

Solid network I/O is critical to the successful operation of FortiMail. Issues at Layer 1 and Layer 2 can cause behaviors that are odd and difficult to diagnose.

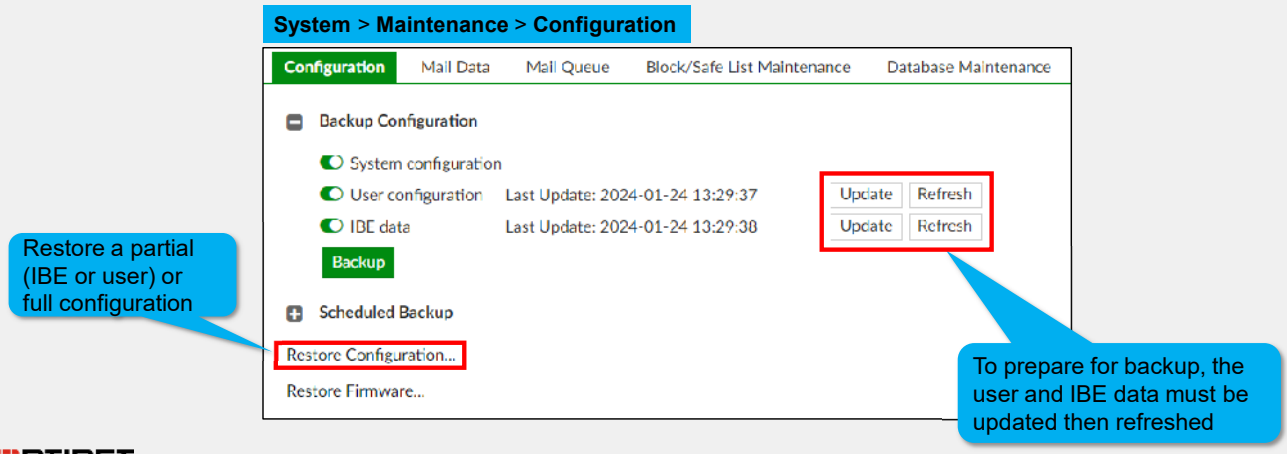
Use the command shown on this slide to help expose networking issues at these lower layers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configuration Backup and Restore

- You can back up system, user, and IBE configuration parameters individually, or as a complete configuration archive file
- A configuration-only backup file will generate a `.cfg` file, including user configuration or IBE data will generate a `.tzg` file



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 11

You can back up system, user, and identity-based encryption configuration parameters individually, or as a complete configuration archive file. Configuration-only backups will have cfg extensions. Backup files with user and/or identity-based encryption configurations will be tzg archive files.

Before you can back up user configuration or IBE data, you must update and refresh the user configuration or IBE data, to activate their respective checkboxes.

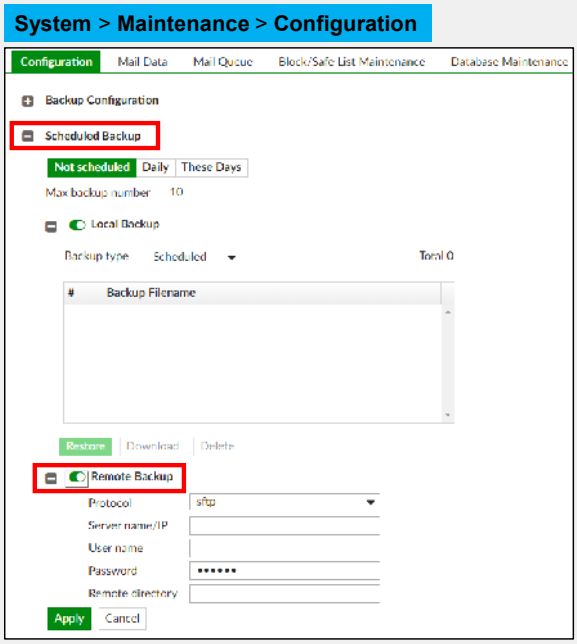
You can restore a configuration—either partial or full—on the same screen.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Scheduled Configuration Backups

- You can back up configuration locally on a defined schedule
- Remote backups supported by FTP or SFTP



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 12

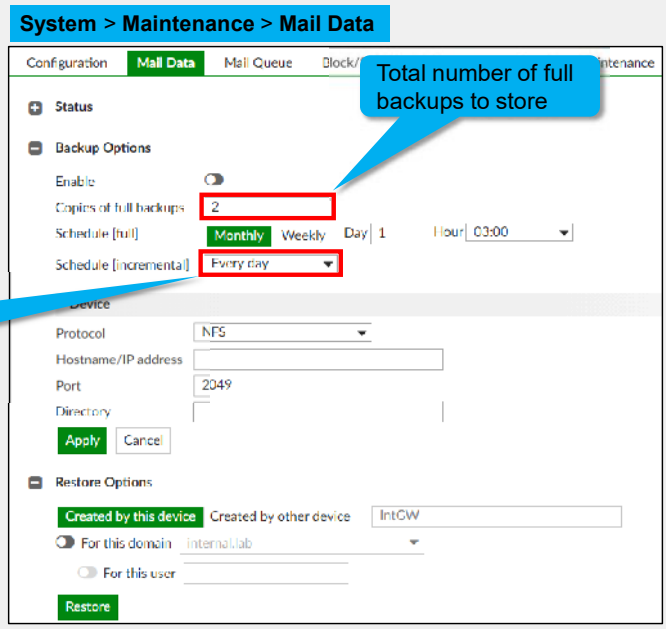
You can schedule FortiMail configurations for backup, store the backup files locally, remotely, or both. You can set scheduled backups to occur daily, or on selected days of the week. Configure the **Max backup number** value to limit the number of configuration backups. FortiMail deletes the oldest backups when the maximum limit is reached.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Mail Data Backup

- Personal quarantine, preferences, mail archives and user mailboxes can be backed up to remote storage
- Remote storage can be NFS, SMB/CIFS, SSH, iSCSI, or an external USB drive



Frequency of incremental backups to perform between full backups

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 13

The data FortiMail stores beyond the simple configurations is called mail data backup and includes the contents of personal quarantines, system quarantines, user preferences, email archives, and server mode user mailboxes. NFS, SMB/CIFS, SSH file system, iSCSI, or external USB drives are supported as remote storage options.

Mail data backups are based on a periodic full backup with frequent incremental backups in between. In configuring mail data backups, choose how many full backups to retain, how often to perform full backups, and the frequency of the incremental backups.

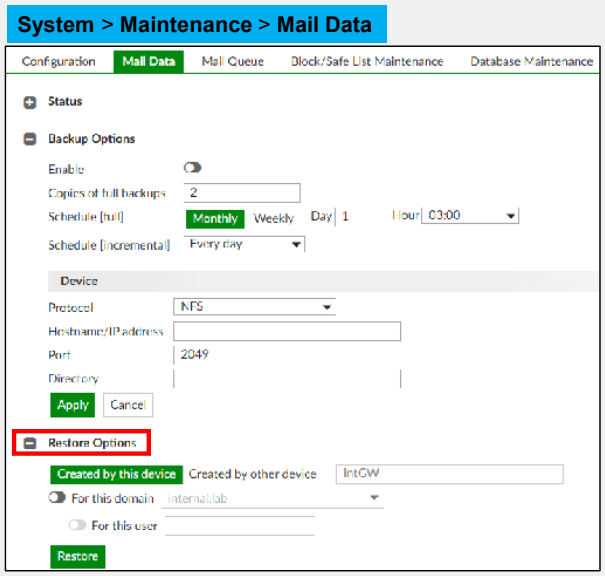
Because of the potential volume of mail data involved, backups of mail data are recommended for any deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Mail Data Restore

- You can restore mail data for the entire system, a specific protected domain, or a specific user



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 14

Restoring mail data is straightforward. Choose the granularity of the data to restore, which can be the entire system, a specific protected domain, or a specific user. Keep in mind you can restore mail data from different FortiMail devices and for specific users and domains.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

RAID

- You can configure specific FortiMail appliances to use redundant array of independent disks (RAID) with their hard disks
  - Software and hardware RAID support
- Depending on the FortiMail model and drive count, the RAID levels differ
  - Software RAID: RAID 0 and 1
  - Hardware RAID: RAID 1, 5, 10, 50, and hot spare

Caution: Changing the RAID level erases all existing data

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

Specific FortiMail models provide RAID support at various levels, depending on the model. To know which FortiMail models support RAID, refer to the *FortiMail Data Sheet*.

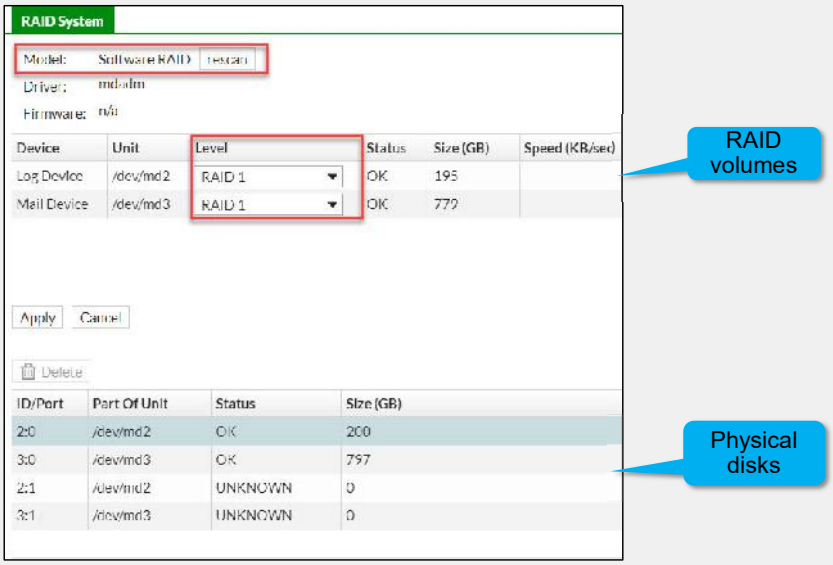
Changing the RAID level erases all existing data in the log and mail data areas. So, either perform RAID configuration tasks during the initial configuration stages or perform backups if the existing data needs to be restored.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Software RAID Status

System > RAID > RAID System



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

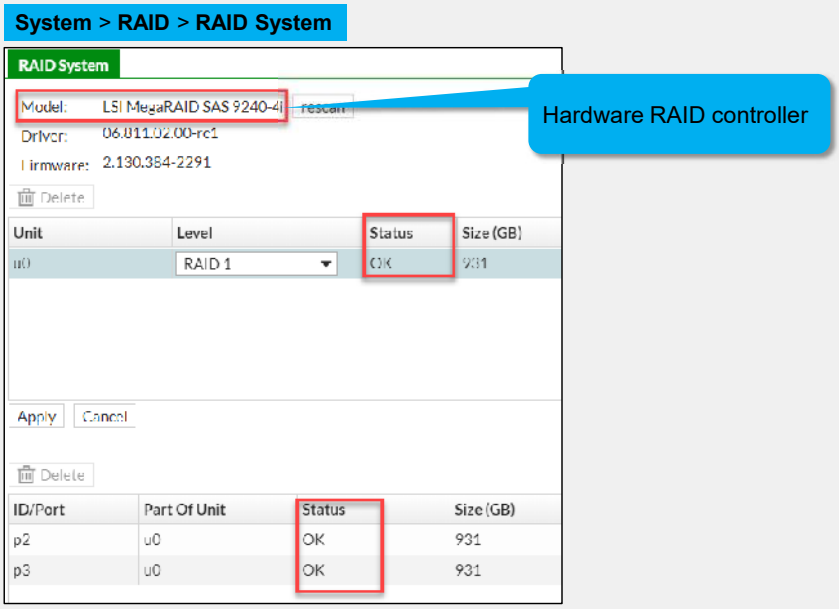
FortiMail models that have software RAID support RAID levels 0 and 1 and come with two hard drives. By default, the RAID layout consists of two RAID 1 volumes for each of the log and mail data storage areas.

After the software RAID is operational, you can monitor its status in the GUI. Any RAID events, such as drive failures and RAID rebuilding events, are logged, and optionally, trigger email alerts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Hardware RAID Status



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

For most situations, you should use the default RAID layout. However, requirements may dictate that you change the RAID configuration to alter the balance of performance, availability, and total storage size.

Like software RAID, once the RAID is operational, you can monitor its status on the GUI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

RAID Status Messages

Status	Description
OK	The unit is optimal and is functioning normally.
Rebuilding	The unit is in the process of writing data to a newly added disk in a redundant unit, in order to restore the unit to an optimal state. The unit is not fully fault tolerant until the rebuilding is complete.
Initializing	The unit is in the process of writing to all of disks in the unit in order to make the array fault tolerant.
Verifying	The unit is in the process of ensuring that the parity data is valid.
Degraded	One or more drives in the unit is no longer being used by the controller.
Inoperable	One or more drives is missing from the unit, causing the underlying file system to be unreadable.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 18

FortiMail will display different status messages depending on the health of the disk array. The different status messages are shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Reset FortiMail configuration

- To reset to factory defaults but keep the current VM license

```
# execute factoryreset keeplicense
```

- To reset the configuration only and keep network settings

```
# execute factoryreset config2
```

- To reset to factory defaults and shutdown

```
# execute factoryreset shutdown
```

Caution: If configuration changes are being made remotely (SSH, GUI CLI), resetting a configuration without keeping network settings will result in loss of connection to FortiMail.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

The `execute factoryreset keeplicense` command, resets the entire configuration to factory default settings but keeps the VM license. The `factoryreset config2` command can be used to reset the configuration while keeping the network settings. The `execute factoryreset shutdown` command can be used to reset the configuration and disk partition to factory default settings and then shut down the system. Note that remote connections will be lost unless network settings are kept.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which statement about the service ports used by FortiMail for FortiGuard connectivity is true?
   - ✓ A. UDP 53/8888 is used for FortiGuard rating queries.
   - B. UDP 53/8888 is used for FortiGuard firmware updates.

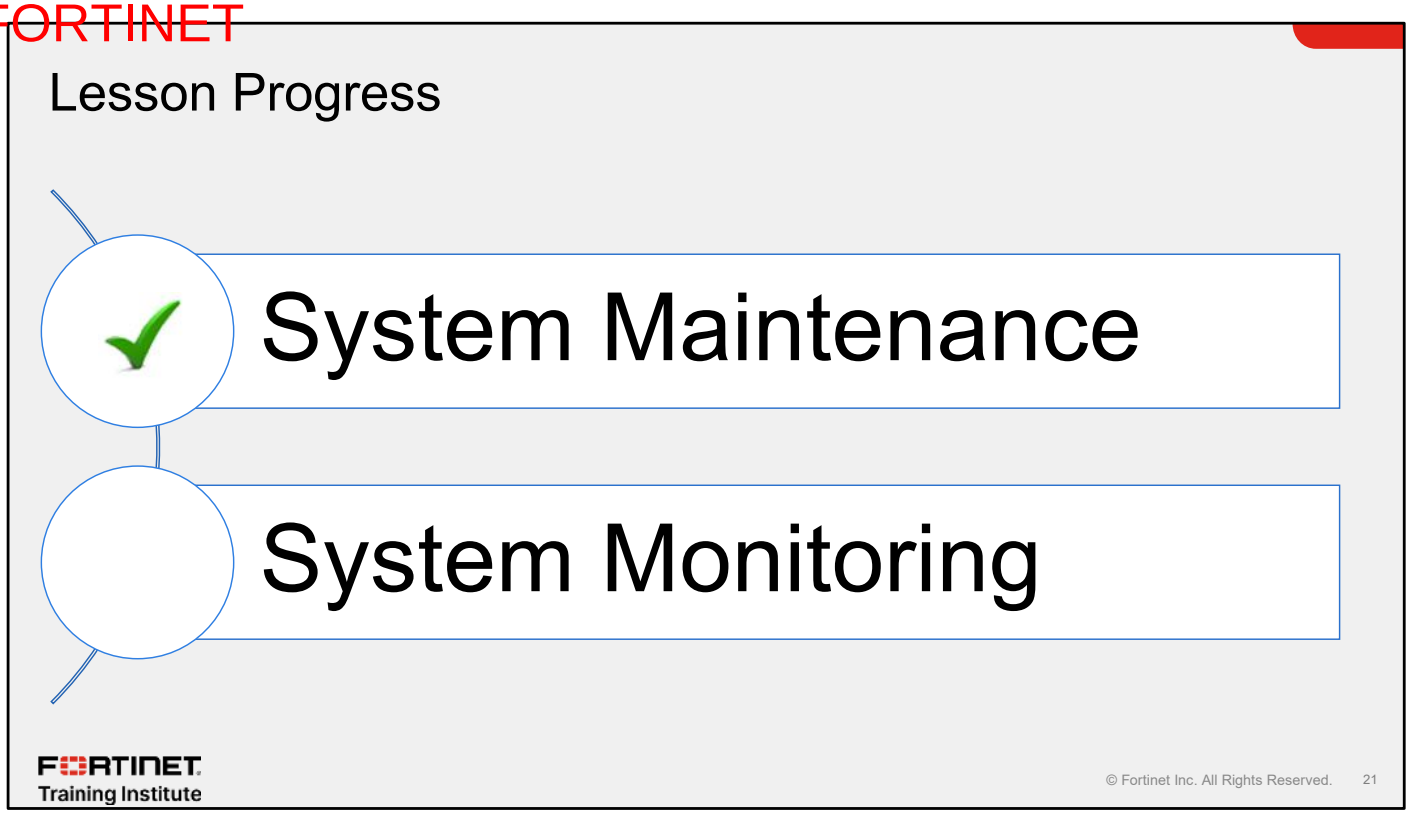
2. Why do you need to perform RAID configuration tasks during the initial configuration stages?
   - A. Configuring RAID later can be very complex.
   - ✓ B. Changing the RAID layout erases all existing data in the log and mail data areas.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 20

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Good job! You now understand FortiMail system maintenance.

Now, you'll learn about FortiMail system monitoring.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

System Monitoring

Objectives

- Use system status, statistics, and reports to maintain optimal system performance
- Configure SNMP monitoring

FORTINET Training Institute

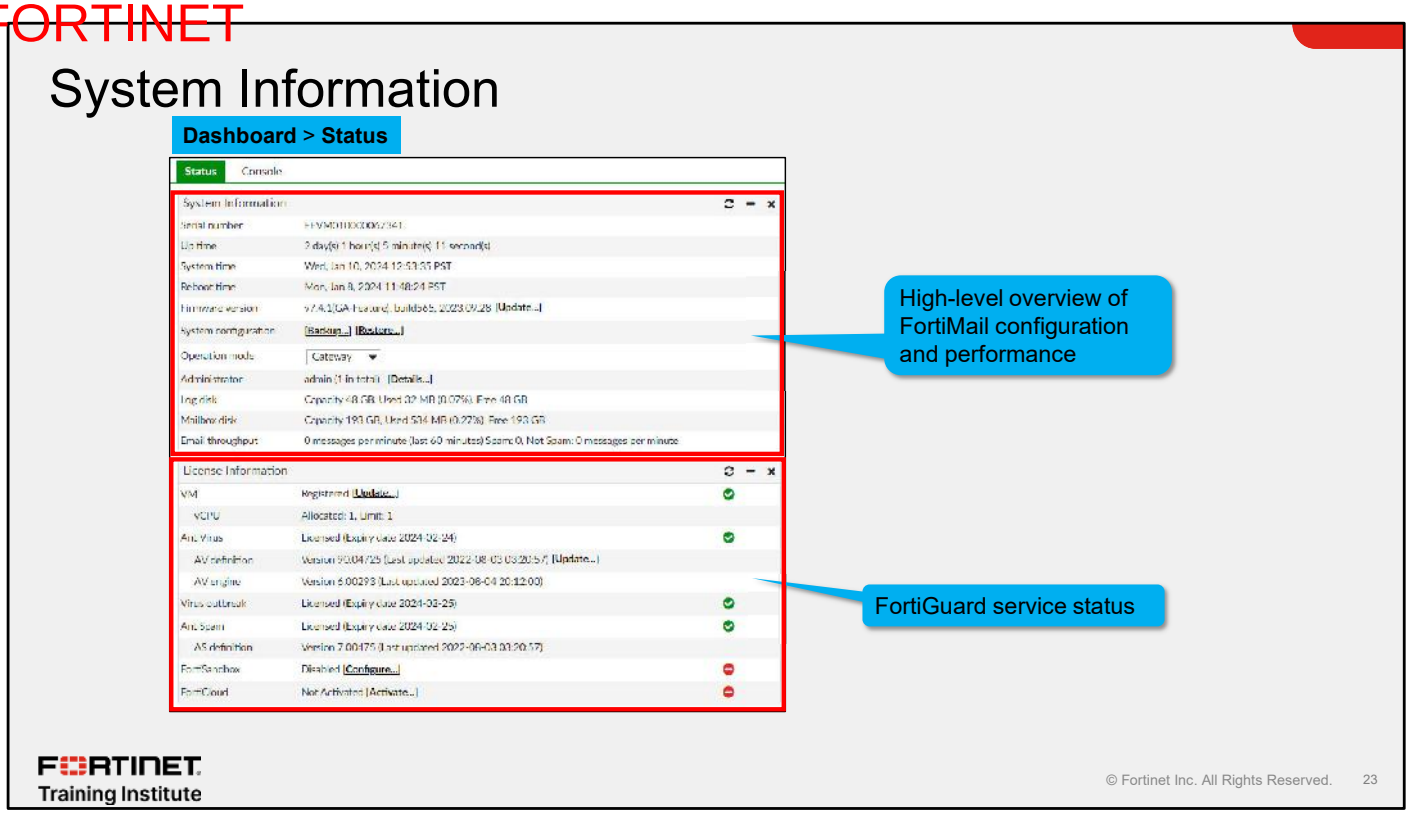
© Fortinet Inc. All Rights Reserved. 22

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence using monitoring tools and system options, you will be able to monitor and maintain FortiMail operation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After you log in to the GUI, the **System Status** page opens. The **System Information** widget shows high-level information, such as the FortiMail serial number, uptime, firmware version, operating mode, storage utilization, and email throughput. The **License Information** widget shows the details of the FortiGuard subscription currently active for the device. Viewing this information is a quick way to verify crucial information about FortiMail status and operations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

System Status

```
IntGW # get system status
Version:                          FortiMail-VM-KVM v7.4.1(GA-Feature), build565, 2023.09.28
Architecture:                     64-bit
Serial-Number:                    FEVM010000067341
BIOS version:                     n/a
VM Registration:                  Valid: License has been authorized
VM License File:                  License file and resources are valid
VM Resources:                     1 CPU/1 allowed, 1.5 GB RAM, 1.5 GB maximum, 1024.0 GB allowed, 244 GB Disk/1024 GB allowed
Log disk:                         Capacity 48 GB, Used 32 MB (0.07%), Free 48 GB
Mailbox disk:                     Capacity 193 GB, Used 534 MB (0.27%), Free 193 GB
Filesystem mode:                  Read-Write
Hostname:                         IntGW
Operation mode:                   Gateway
HA configured mode:               Off
HA configured role:               Off
HA effective role:                Off
FIPS-CC status:                   disabled
Strong-crypto:                    enabled
Distribution:                     International
Branch point:                     565
Virus DB:                         90.04725(2022-08-03 01:39)
Extended DB:                      Disabled
AntiSpam DB:                      7.00475(2022-07-27 17:02)
GeoIP DB:                         2.00136(2022-07-26 16:09)
Certificate Bundle:               1.00034(2022-04-26 17:08)
Uptime:                           2 days  1 hours  7 minutes
Last reboot:                      Mon Jan 08 11:48:24 PST 2024
System time:                      Wed Jan 10 12:56:17 PST 2024
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

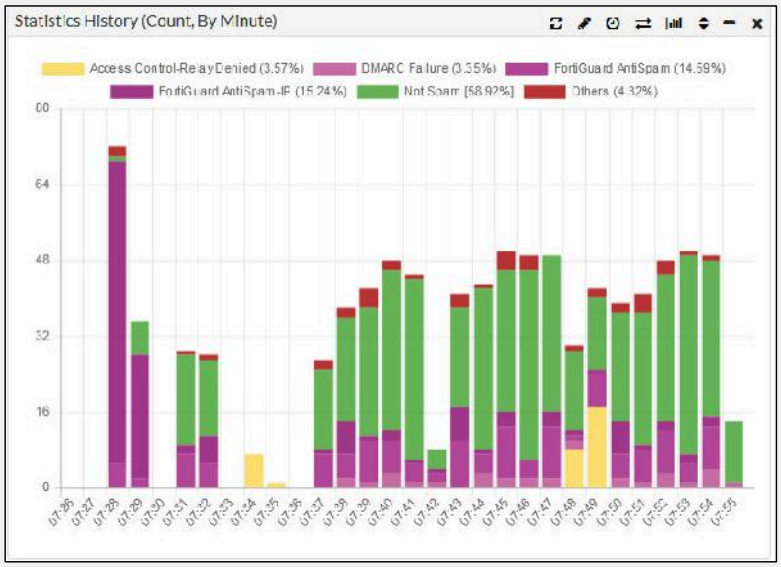
You can display the same high-level information on the CLI using the commands shown on this slide. The information displayed on the CLI includes a few additional items, such as antivirus and antispam database version numbers, timestamps of the latest database updates, and the status of FIPS support and cryptography level.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Statistics History

Dashboard > Status



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

On the GUI, on the main **System Status**, the **Statistics History** widget shows a bar graph of email history broken down by classifier categories. By default, the widget shows message volume by hour over the previous 24-hour period. You can set the widget to show message volume by minute, by day, by month, and by year.

This display is useful for highlighting out-of-the-ordinary situations, such as a dramatic drop in message volume, or a dramatic rise in a particular type of message classification.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Statistics Summary

Dashboard > Status

Statistics Summary

Messages		Total	This Year	This Month	This Week	Today	This Hour	This Minute
Not Spam Classified By	Not Spam	545	545	545	545	545	545	13
	Subtotal	545	545	545	545	545	545	13
		58.9%	58.9%	58.9%	58.9%	58.9%	58.9%	92.9%
Spam Classified By	Access Control-Relay Denied	33	33	33	33	33	33	0
	Behavior Analysis	26	26	26	26	26	26	0
	DMARC Failure	31	31	31	31	31	31	1
	FortiGuard AntiSpam	135	135	135	135	135	135	0
	FortiGuard AntiSpam-IP	141	141	141	141	141	141	0
	FortiGuard WebFilter	6	6	6	6	6	6	0
	Heuristic	8	8	8	8	8	8	0
	Subtotal	380	380	380	380	380	380	1
		41.1%	41.1%	41.1%	41.1%	41.1%	41.1%	7.1%
Virus Classified By	Subtotal	0	0	0	0	0	0	0
		0%	0%	0%	0%	0%	0%	0%
Total		925	925	925	925	925	925	14

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

The **Statistics Summary** widget displays a summary of all messages processed by FortiMail, divided into three categories: **Not Spam**, **Spam**, and **Virus Infected**.

For each message classification, total counts are displayed for, the current year, month, week, day, hour, and minute.

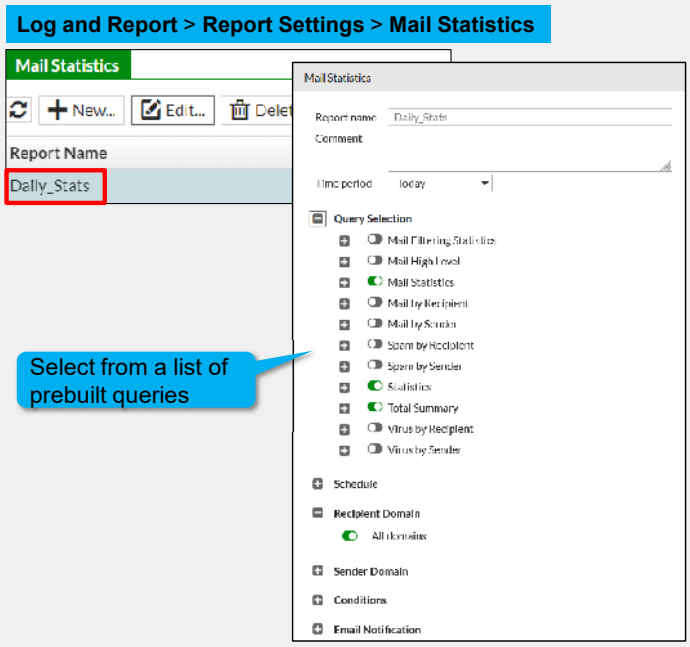
This is extremely useful for understanding which features are effective. You can also use information from this widget to determine which features are allowing potential spam to pass through. For example, a high number for safe lists would mean too many email messages are bypassing antispam scanning, which requires investigation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Reports

- Reports can be scheduled or generated on demand
- Report generation is resource intensive and should be used only during times with low traffic volume



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

FortiMail has a powerful built-in reporting facility that generates both scheduled and on-demand reports. You should use it as a regular monitoring and maintenance tool. You can use the report data to verify or plan improvements to your FortiMail configuration.

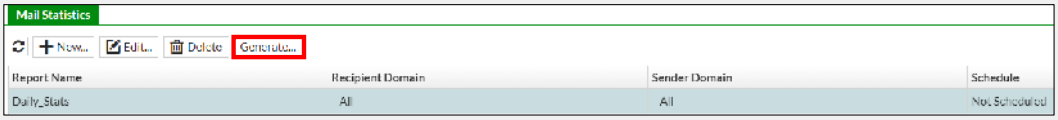
You can configure each report using the prebuilt queries. These queries are hardcoded and can't be modified. You can build each report for a system-wide view, or create a separate report for each protected domain. You can create and schedule new report types for immediate execution, or save them for future use on demand.

Vouchers & Dumps are Available | WhatsApp +201224560923

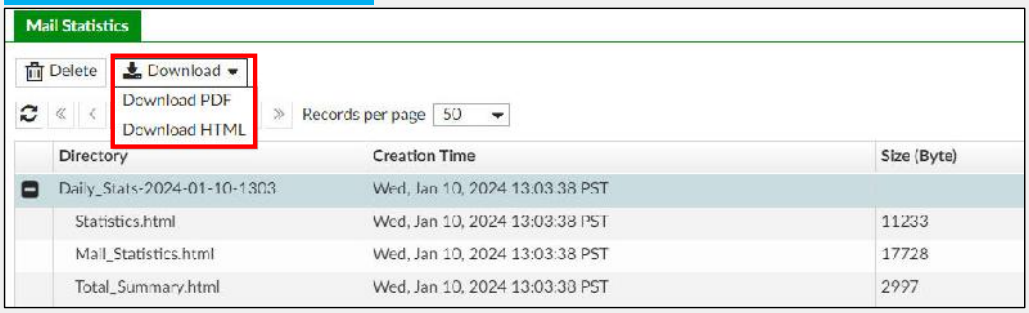
DO NOT REPRINT Brave-dumps.com
© FORTINET

Reports

Log & Report > Report Settings > Mail Statistics



Monitor > Report > Mail Statistics



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

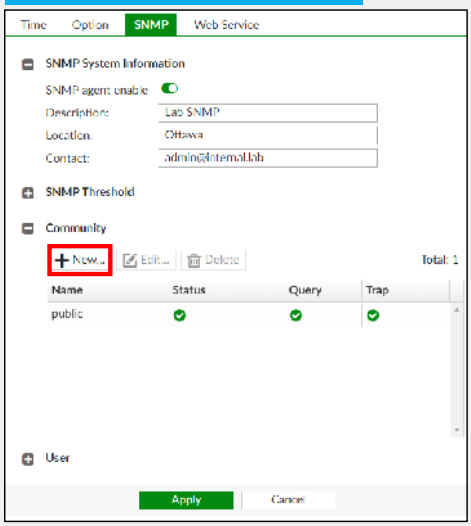
After you generate a report, you can retrieve it on the **Mail Statistics** page on the GUI. You can also choose to have the reports emailed automatically after generation, to one or more recipients. FortiMail can generate reports in either HTML or PDF format.

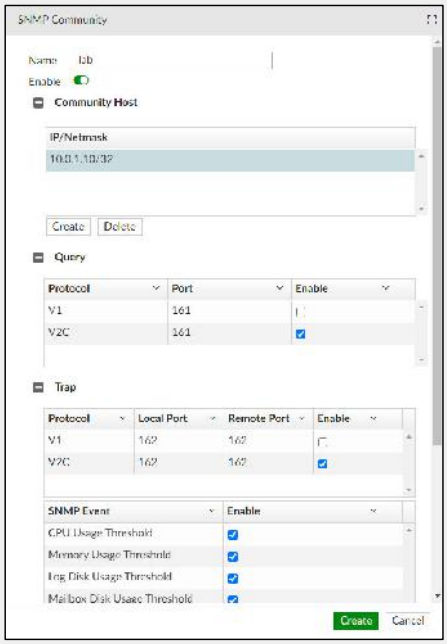
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SNMPv2

System > Configuration > SNMP





FORTINET Training Institute

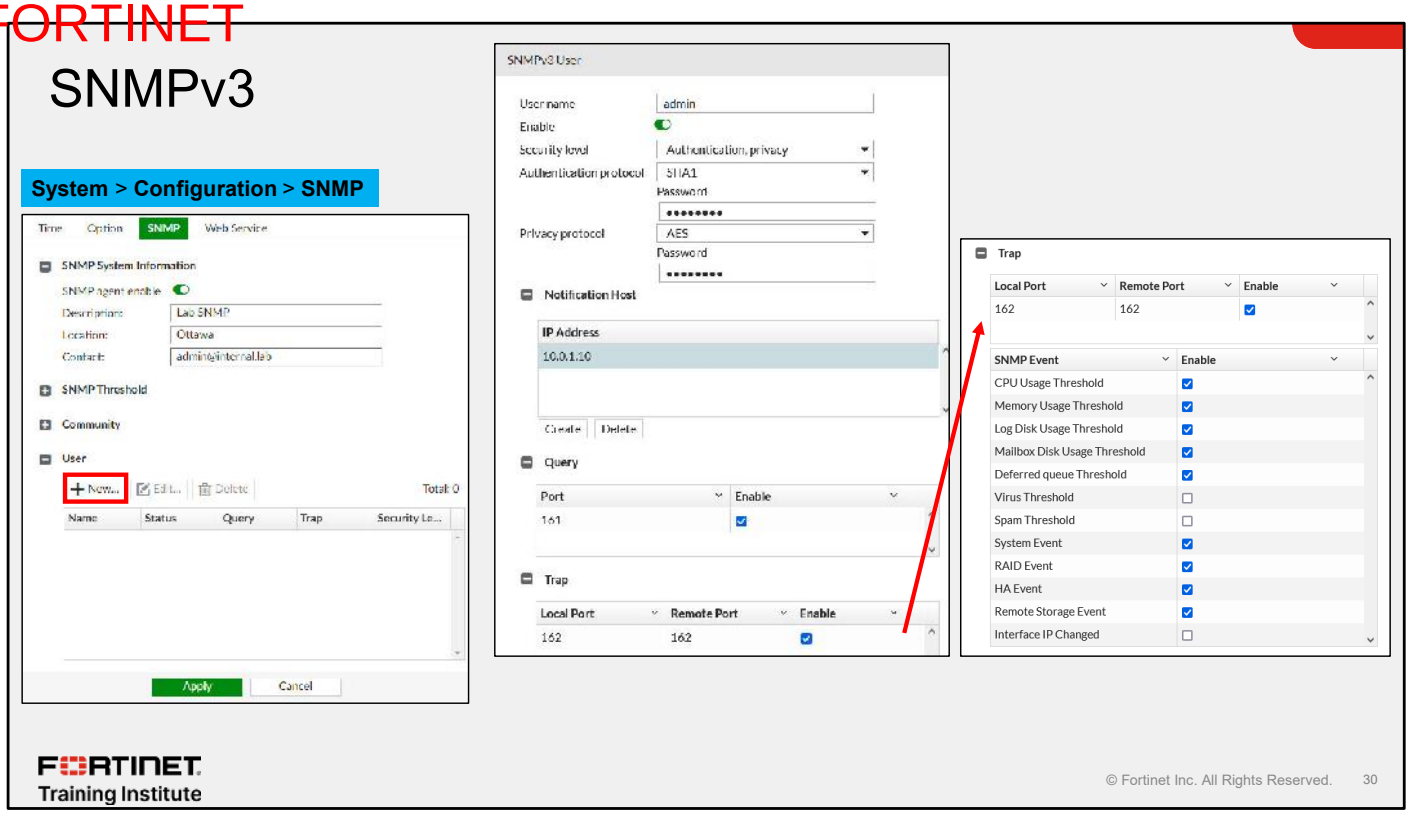
© Fortinet Inc. All Rights Reserved. 29

FortiMail provides read-only support for SNMP v1, v2c, and v3 polling and traps. Integration with third-party SNMP management platforms is provided by the FortiMail vendor MIB, which you can download from the Fortinet support website. For more information, see the *FortiMail Administration Guide*, because the specific FortiMail MIB attributes can change by release.

You can enable SNMPv2 on FortiMail to generate SNMP traps when certain system events or thresholds have been reached.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



For each SNMPv3 user, define the security level and enable the desired traps. If you enable authentication, privacy, or both, the password values must match those set in the SNMP management platform.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. What extra information does the `get system status` CLI command display, that is not on the **System Information** widget?
   A. Operation mode
   ✓ B. Antivirus database version

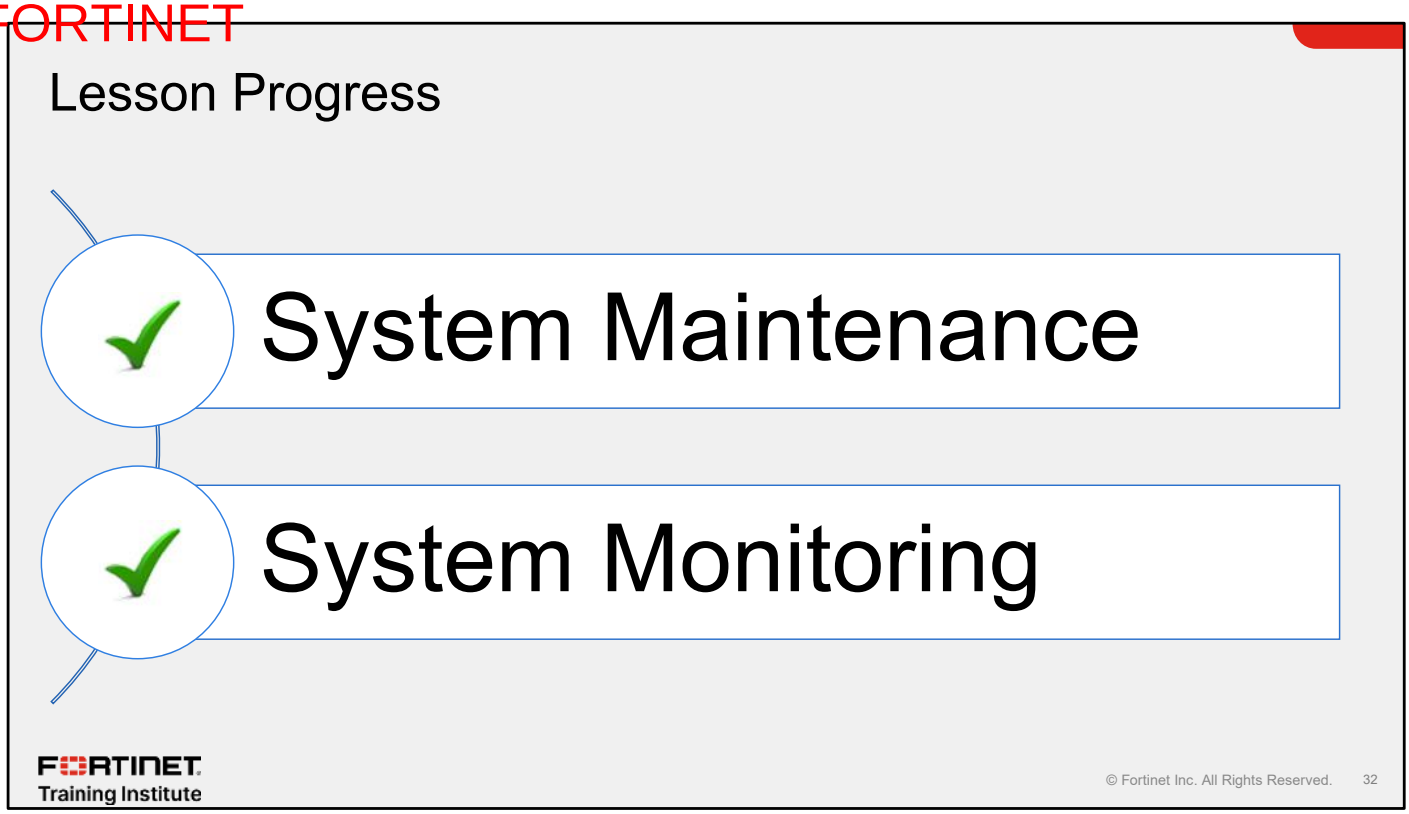
2. Why is it recommended that you run reports during low traffic volume?
   ✓ A. Running reports can be resource intensive.
   B. Reports cannot be generated when CPU usage is over 50%.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Review

- ✓ Perform local storage management tasks
- ✓ Verify FortiGuard service status
- ✓ Monitor system resource use and network interface status
- ✓ Back up and restore system configuration and mail data
- ✓ Use system status, statistics, and reports to maintain optimal system performance
- ✓ Configure SNMP monitoring

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you have learned how to maintain your FortiMail device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FORTINET
Training Institute

FORTINET
CERTIFIED
PROFESSIONAL
Public Cloud
Security

FortiMail Administrator

Troubleshooting

FortiMail 7.4

Last Modified: 25 April 2024

In this lesson, you will learn some useful tips for troubleshooting FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Lesson Overview

- Troubleshooting Tools
- Troubleshooting Methodologies

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 2

In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Troubleshooting Tools

Objectives

- Use connectivity testing tools
- Use the built-in packet capture tool
- Use log searching and log message correlation to find relevant logs
- Decipher SMTP event logs to pinpoint the root cause of SMTP connection issues

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 3

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in using troubleshooting tools, you will be able to use those tools to investigate issues on FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Connectivity Tests

- Ping:

```
# execute ping <IP Address | FQDN>
```

- Traceroute:

```
# execute traceroute <IP Address | FQDN>
```

- Telnet:

```
# execute telnettest <IP Address | FQDN>[:port]
```

- SSH:

```
# execute ssh <user>@<IP Address | FQDN> [port]
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 4

FortiMail includes basic IP connectivity testing tools that can help you diagnose network connectivity issues from the point of view of FortiMail. These include ping, traceroute, SSH, and telnet.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

ARP Table

- Display ARP table:

```
# diagnose netlink neighbor list
Ifindex=4 ifname=port1 192.167.1.254 00:0c:29:d6:2a:12 state=00000004
use=31520477 confirm=63623630 update=23746 ref=0
Ifindex=4 ifname=port1 192.167.1.252 00:09:0f:a5:d5:d4 state=00000004
use=18577243 confirm=18577243 update=23746 ref=0
```

- Flush ARP table:

```
# diagnose netlink neighbor flush <int name>
```

- Remove a specific ARP entry:

```
# diagnose netlink neighbor delete <int name> <IP>
```

- Add a static ARP entry:

```
# diagnose netlink neighbor add <int name> <IP> <MAC>
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 5

When you troubleshoot network issues, displaying the Address Resolution Protocol (ARP) table can help identify any layer 2 problems. You can use the CLI commands shown on this slide to display and manipulate the ARP table in order to address layer 2 problems.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

DNS Connectivity

- NSlookup:

```
# execute nslookup name <fqdn|IP> <type|class|server|port>
```

```
FortiMail # execute nslookup name internal.lab type mx

internal.lab mail exchanger = 10 intGW.internal.lab.
Internal.lab mail exchanger = 20 intSRV.internal.lab.
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 6

You can use the `nslookup` tool to assist you in verifying DNS connectivity issues on FortiMail and resolving them. When you enter the command, you can specify a fully qualified domain name (FQDN) or IP address for the lookup, as well as the type of record, class, server, or even a specific port. This is usually used to verify which mail exchange (MX) record the FortiMail will use when delivering mail when using its mail transfer agent (MTA).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SMTP Connectivity

- To troubleshoot mail server connectivity issues:

```
# execute smtptest < [FQDN | IP]:port>
```

- Can issue full range of SMTP commands

```
IntGW # execute smtptest extsrv.external.lab
Connected

220 ExtSRV.external.lab ESMTP Smtpd; Tue, 13 Feb 2024 06:51:46 -0800

Entering interactive mode. Type CTRL-D to exit.
ehlo mx.internal.lab
250-ExtSRV.external.lab Hello [10.0.1.11], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE 10485760
250-AUTH LOGIN PLAIN DIGEST-MD5 CRAM-MD5
250-STARTTLS
250-DELIVERBY
250 HELP
```

FORTINET Training Institute

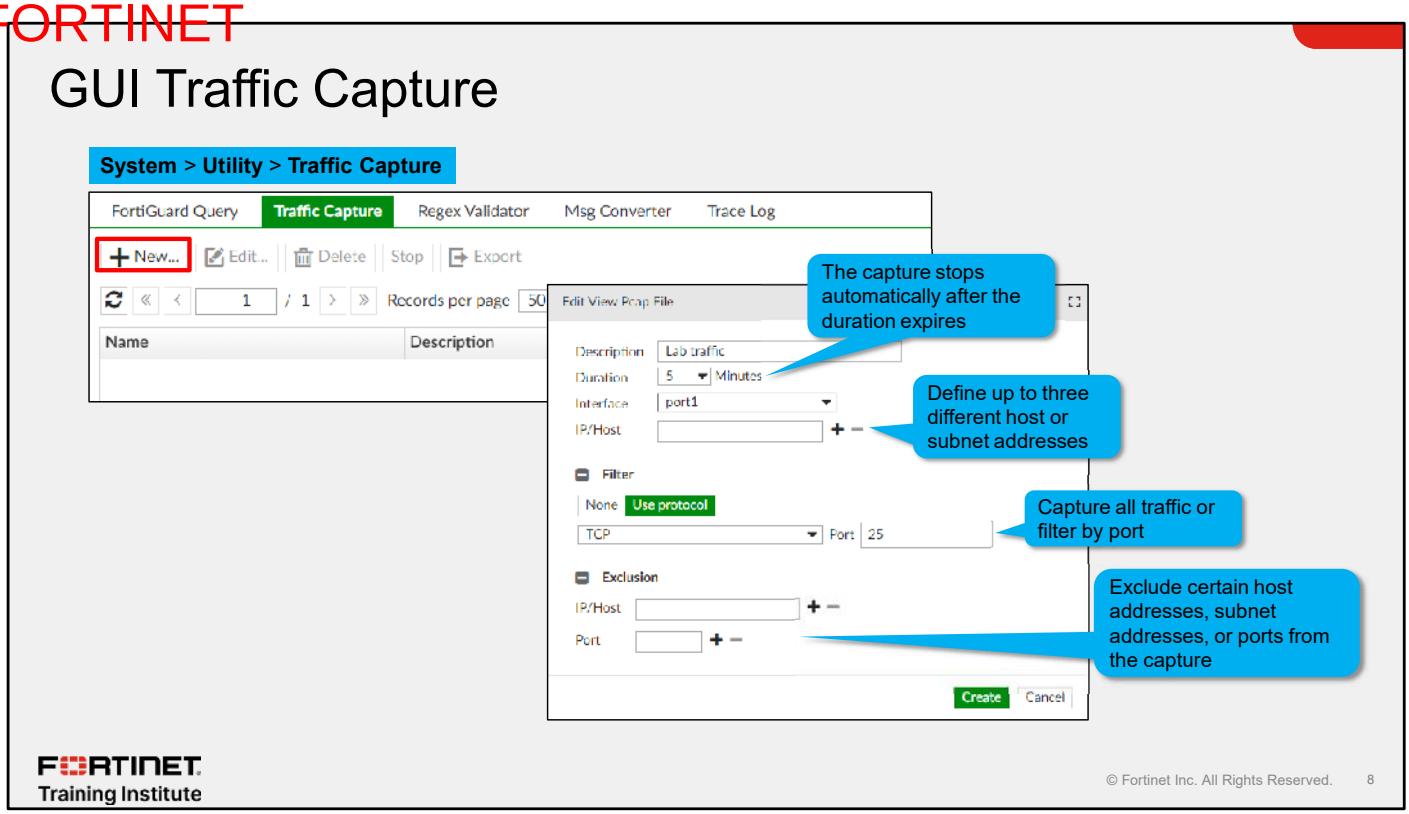
© Fortinet Inc. All Rights Reserved. 7

You can use the `smtptest` command to create an interactive SMTP connection to MTAs. This tool is useful for troubleshooting connectivity issues with other MTAs.

This command initiates an interactive SMTP session with the specified IP or FQDN. If the connection establishes successfully, you can issue the full range of SMTP commands, such as `EHLO`, `MAIL FROM`, `RCTP TO`, `DATA`, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiMail has a built-in GUI based packet capture tool. You can set up a duration to stop the capture without manual intervention. This ensures that the captures don't fill up the log disk partition.

You can define up to three different host or subnet addresses to capture. You can capture all traffic on an interface, or filter by port. You can also exclude certain host addresses, subnet addresses, or ports from the capture, to make sure unnecessary traffic is excluded from the final capture file and make it easier to analyze.

Once the capture runs for its defined duration, it is ready for download. FortiMail generates the capture file in the standard packet capture library (LIBPCAP) format, which you view in WireShark or other traffic analyzers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

CLI Traffic Capture

```
# diagnose sniffer packet <interface> <filter> <verbose> [count] [a]
```

- `<interface>`: Interface name; to capture on all interfaces use any
- `<filter>`: Filter the capture using the Berkeley Packet Filtering (BPF) syntax
- `<verbose>`: Verbose levels control the level of detail displayed from the captured data
  1. Print header from the IP header
  2. Print header and data from the IP header
  3. Print header and data from the Ethernet header
  4. Print header from the IP header with interface name
  5. Print header and data from the IP header with the interface name
  6. Print header and data from the Ethernet header with interface name
- `[count]`: the number of packets to capture before stopping
- `[a]`: print the absolute timestamp instead of the relative one

- Captured data can be converted to PCAP format using WireShark's text2pcap tool

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 9

There is a similar CLI traffic capture tool, identical to the one on FortiGate. You can limit the CLI capture to network traffic on a particular interface and filter it with Berkeley Packet Filter (BPF) formatted filter expressions.

The output of this command is displayed on the CLI terminal session for real-time analysis. To capture the output to a file, use a terminal program such as PuTTY that allows session logging.

For further protocol analysis with Wireshark, you can convert the captured output to packet capture (PCAP) format using the WireShark text2pcap tool.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiMail Log Types

- History
  - General overview of the email handled by FortiMail
  - Allows log message correlation using session ID link
- Event
  - System event logs
  - Email event logs
- Antivirus
  - Virus detection details
- Antispam
  - Spam detection details
- Encryption
  - IBE and SMIME-related details

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 10

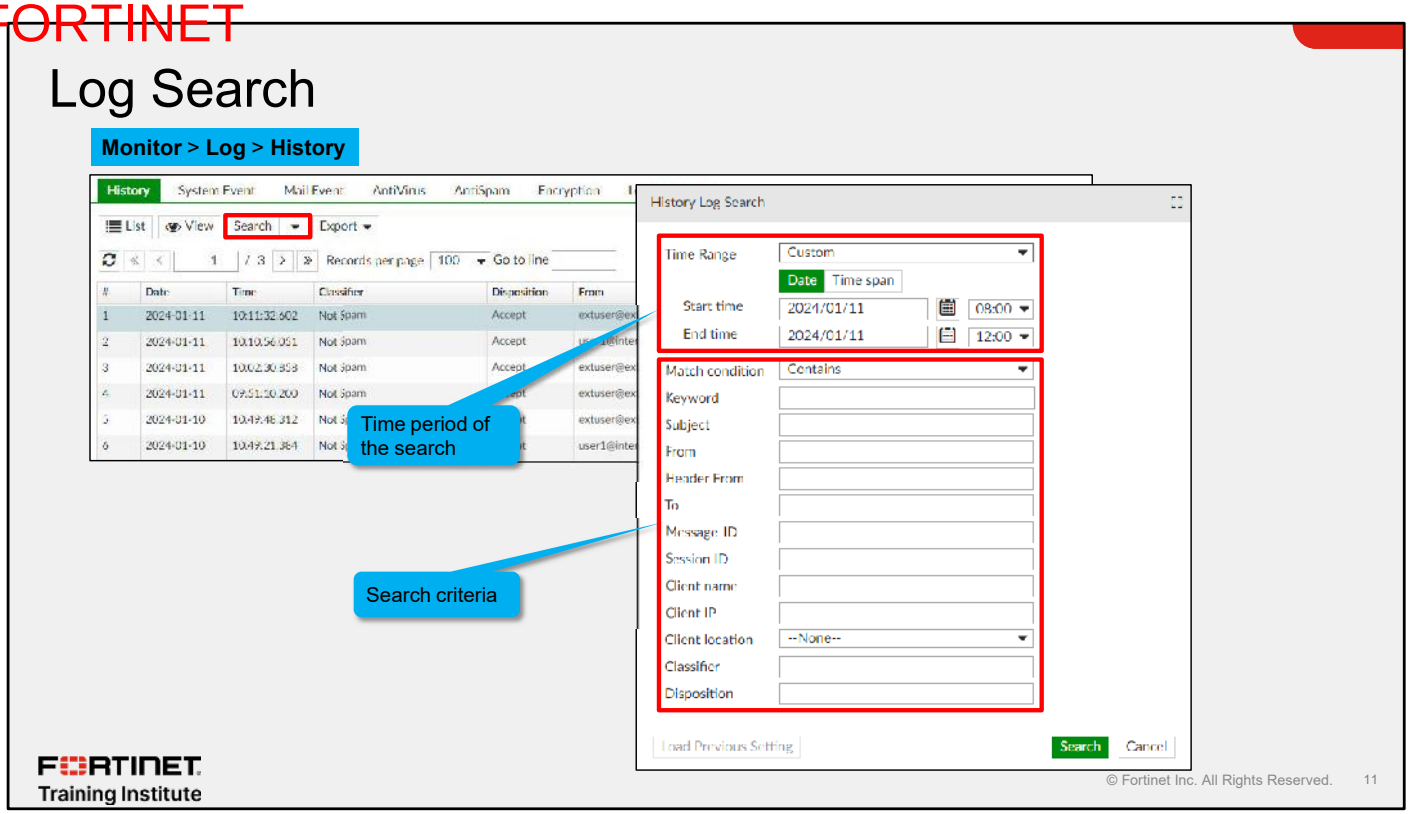
There are five different log types on FortiMail. Each of the five log types holds the details for different FortiMail activities.

The history log contains a high-level abstract of each email processed by FortiMail, and its final disposition. Event log entries provide the details of SMTP connections as well as system events. Antivirus log entries are generated for any virus detection event. Antispam logs contain entries for each email that the antispam scans detect as spam, along with which scan type detected it, and the elements in the email that triggered the hit. And finally, the encryption log entries are created when an email message triggers identity-based encryption (IBE) or secure/multipurpose internet mail extensions (S/MIME) encryption.

A single email can potentially generate four to five different log types, depending on which inspection profiles are triggered. This allows a deep look into each single email event.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Use the built-in search function to find what you are looking for. The search form allows you to search the logs using different search criteria and time periods. The search functions exist for each of the log types, with different criteria available for each.

When performing searches, try to narrow down your scope using short time periods; otherwise, the search can potentially use enough FortiMail resources to affect performance.

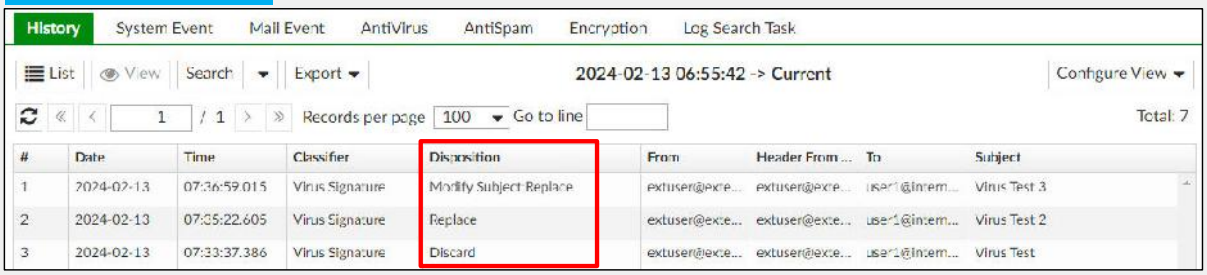
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

History Logs

- Use the **Classifier** and **Disposition** columns to provide extra information about email processing
  - **Disposition** defines the action taken by FortiMail
  - **Classifier** explains why such action was taken

Monitor > Log > History



- For a complete list of classifiers and dispositions, see the *FortiMail Administration Guide*

FORTINET Training Institute

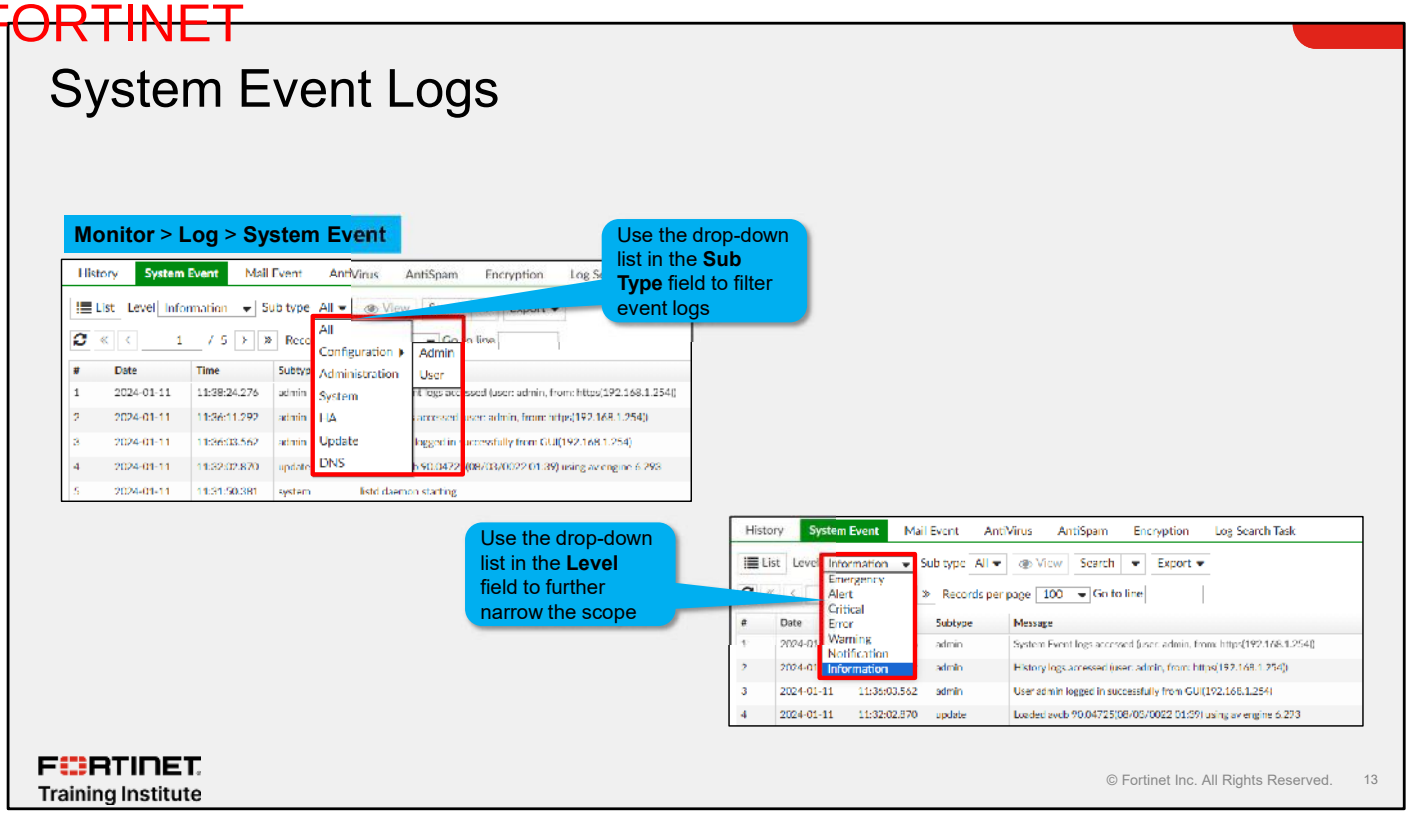
© Fortinet Inc. All Rights Reserved. 12

History log entries have two attributes: classifier and disposition. These attributes provide more information about actions related to a specific email message. The disposition attribute shows the action taken by FortiMail on the email message, and the classifier attribute shows the reason the action was taken. Classifier values tend to be the names of particular FortiMail subsystems, but can also be generic terms such as **Not Spam**.

For a complete list of classifiers and dispositions, see the *FortiMail Administration Guide*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

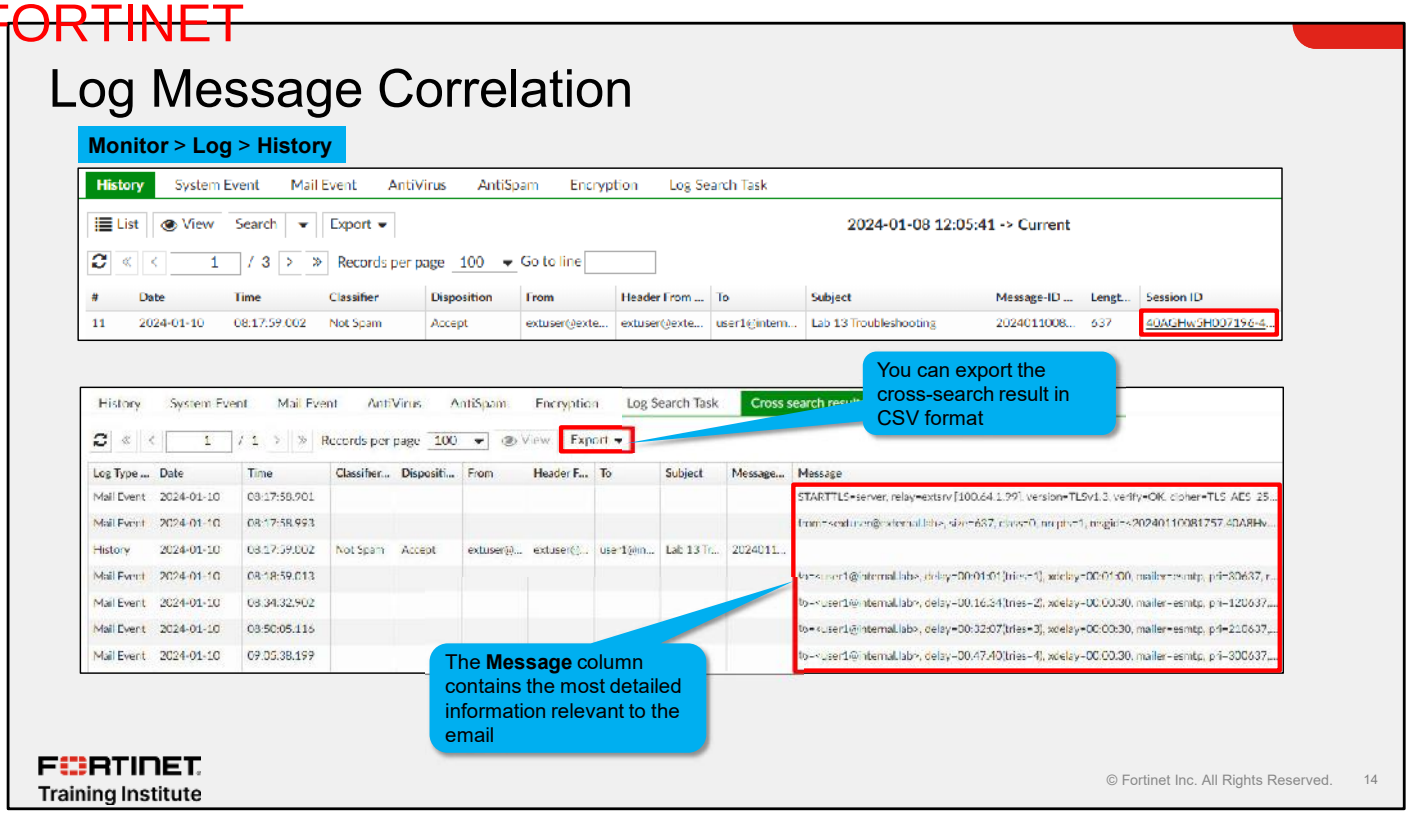


In addition to SMTP sessions, the event log can contain entries related to other FortiMail subsystems, such as IMAP and POP client connections, HA, internal system activities, configuration changes, problems with FortiMail processes, and DNS failures.

If you are searching for logs related to a particular system event, it is always a good practice to filter the logs using the drop-down list in the **Sub type** field. Otherwise, the sheer volume of logs in this section makes investigation very difficult. You can narrow the scope even further by selecting the appropriate severity level using the drop-down list in the **Level** field.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Clicking the **Session ID** link will open the cross-search result showing all relevant log entries—of all log types—that are associated with the same TCP session.

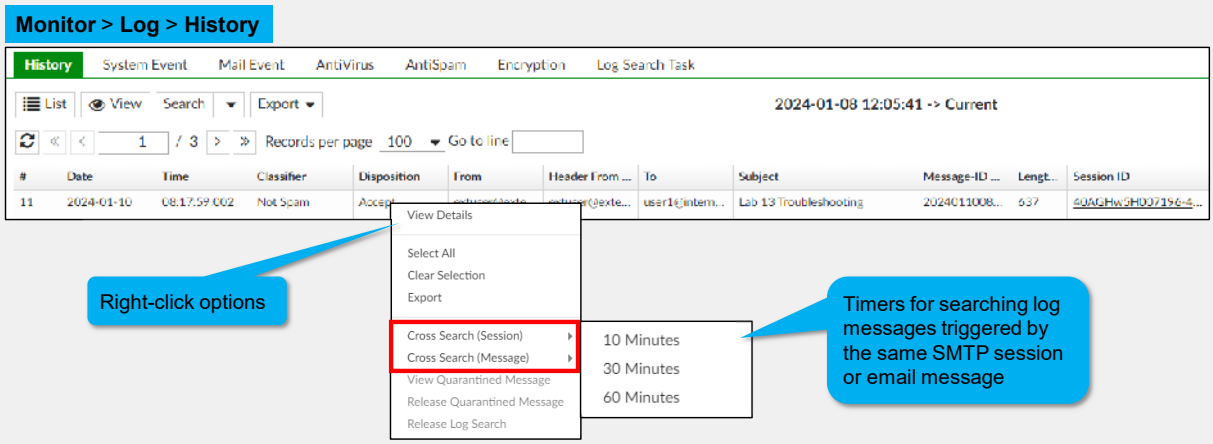
This is an extremely powerful and convenient way to see the sequence of events and FortiMail actions that took place for a given session. In the cross-search result, the **Message** column contains the most detailed information relevant to the email event.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Log Message Correlation (Contd)

- Timers
  - **Cross Search (Session)**: Displays log messages triggered by the same SMTP session
  - **Cross Search (Message)**: Displays log messages triggered by the same email message



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 15

The cross search is time based, and the default period is 5 minutes. Remote MTA security implementations can occasionally introduce delays within email sessions. When these delays exceed 5 minutes, the standard log correlation search may not capture and present all relevant logs associated with the affected session.

To retrieve logs for sessions that experience delays exceeding 5 minutes, use the right-click context menu options: **Cross Search (Session)** and **Cross Search (Message)**.

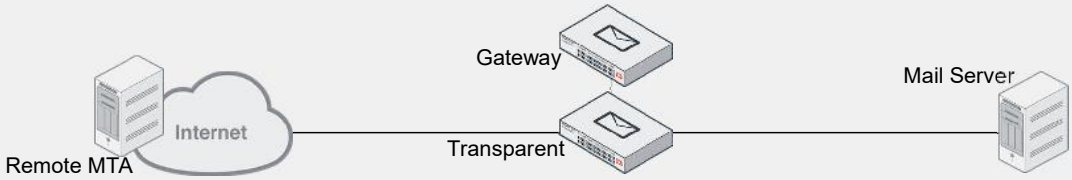
The session-based cross-search function retrieves email messages associated with a specific session ID. This is equivalent to clicking the session ID link in a history log entry. In certain cases, a session-based cross search retrieves multiple email messages, if multiple email messages are sent over the same SMTP session. Use this option to focus on a specific SMTP session.

The message-based cross-search function retrieves logs related to a single email message. Use this option to focus on a specific email message.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Gateway and Transparent Mode SMTP Event Logs



#	Message
1	STARTTLS=server, relay=extsrv [100.64.1.99], version=TLSv1.3, verify=OK, cipher=TLS_AES_256_GCM_SHA384, bits=256/256
2	from=<extuser@external.lab>, size=550, class=0, nrcpts=1, msgid=<20240313062536.42D6PaWk004692@external.lab>, proto=ESMTPS, daemon=SMTP_MTA, relay=extsrv [100.64.1.99]
3	SMTPS=client, relay=10.0.1.99, version=TLSv1.3, verify=OK, cipher=TLS_AES_256_GCM_SHA384, bits=256/256
4	to=<user1@internal.lab>, delay=00:00:01(tries=1), xdelay=00:00:00, mailer=esmtp, pri=30550, relay=[10.0.1.99] [10.0.1.99], dsn=2.0.0, stat=Sent (42DDQg3t010612-42DDQg3u010612 Message accepted for delivery)

TLS and email session details between the remote MTA and FortiMail

SMTPS and email session details between FortiMail and the back-end mail server

Acknowledgement from the back-end mail server

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 16

The **Message** column contains the most detailed information about the email session. Specifically, the SMTP event logs are divided in a way that can assist in identifying issues in email transmission.

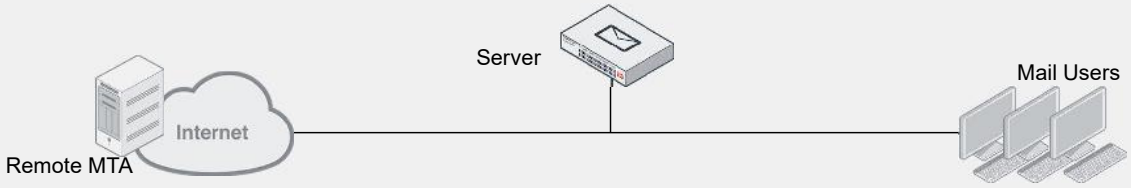
The first pair of event logs are always related to details of the TLS and email transmissions between the sending MTA and FortiMail. The second pair of event logs are related to details of SMTPS, and email transmissions between FortiMail and the back-end mail sever. FortiMail records the acknowledgement message from the back-end mail server in the section of the logs.

The presence, or absence, of certain information in the logs can help you identify the root cause of email transmission issues. For example, a lack of STARTTLS messages might mean that transport layer security (TLS) is either not enabled, or not supported, by either MTA. Or, if FortiMail recorded a delivery acknowledgment, but the message never reached the end user, then there might be an issue with the path between the mail server and the end user.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Server Mode SMTP Event Logs



#	Message
1	STARTTLS=server, relay=extsrv [100.64.1.99], version=TLSv1.3, verify=OK, cipher=TLS_AES_256_GCM_SHA384, bits=256/256
2	from=<extuser@external.lab>, size=551, class=0, nrcpts=1, msgid=<20240213071011.41D7ABS4002246@external.lab>, proto=ESMTPS, daemon=SMTP_MTA, relay=extsrv [100.64.1.99]
3	to=user1@internal.lab, mailer=local, stat=sent

TLS and email session details between the remote MTA and FortiMail

Acknowledgement of mail delivery to user mailbox

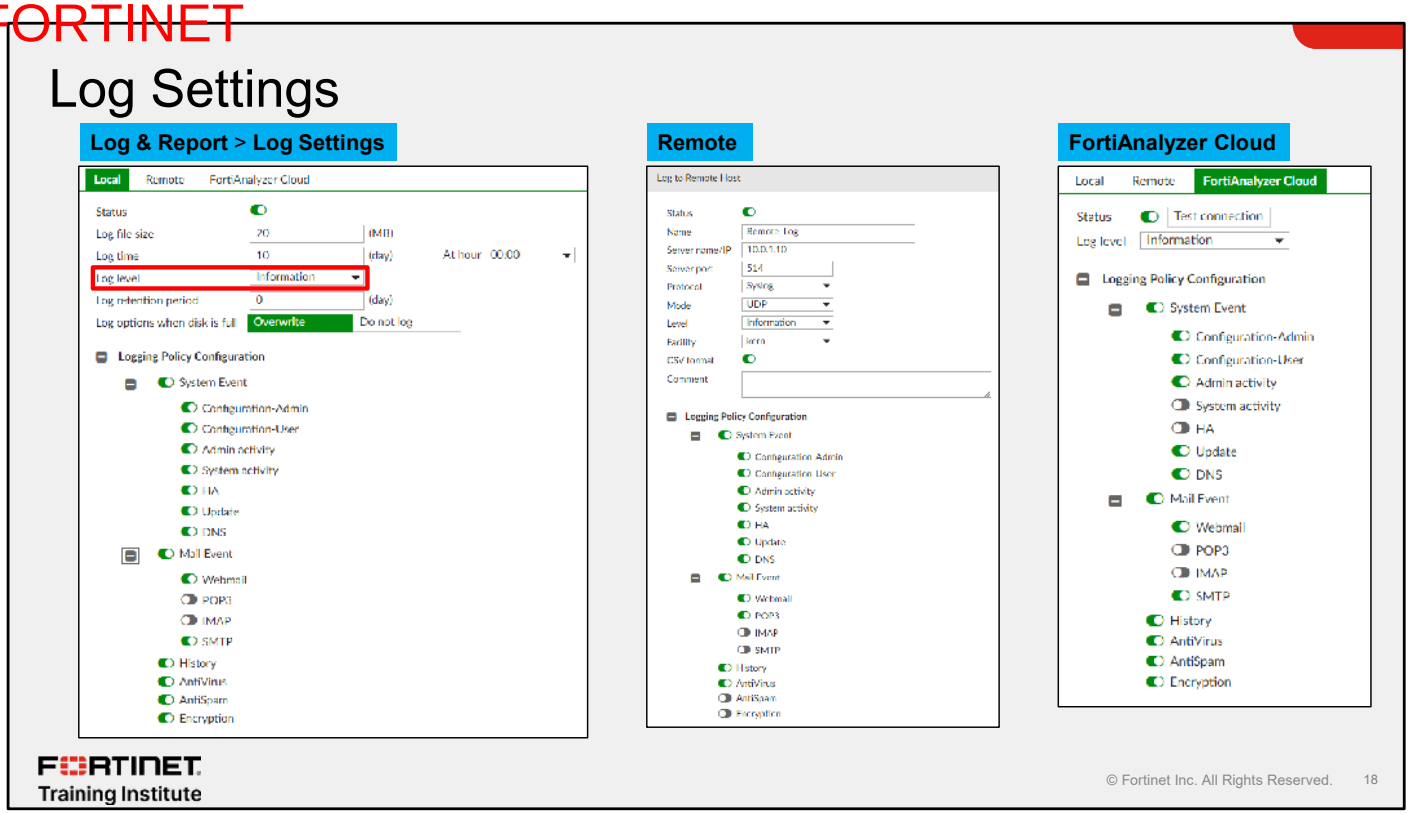
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 17

Server mode deployments involve fewer sessions and, therefore, fewer logs are recorded. The first part of the session still generates TLS and email session details between the sending MTA and FortiMail. The second part of the session doesn't contain the same number of details because the email is simply delivered to a local mailbox.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



By default, FortiMail logs are set at the most verbose level: **Information**. This results in the most detailed logs, but also the largest volume of log data. The log viewer in the FortiMail GUI allows you to filter the logs by severity level, which allows you to quickly locate log entries of a particular level.

You can also configure FortiMail to send all logs to remote storage in syslog in OFTPS format, or to FortiAnalyzer cloud (cloud storage subscription license required). Just remember, if you disable local logging and rely solely on remote logging, the log correlation feature will be lost. You will have to manually find all related logs for a single email using the session ID on the remote logging server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which command is used for testing network connectivity on FortiMail?
   - ✓ A. `execute ping <ip address>`
   - B. `execute nslookup name <fqdn|IP> <type|class|server|port>`

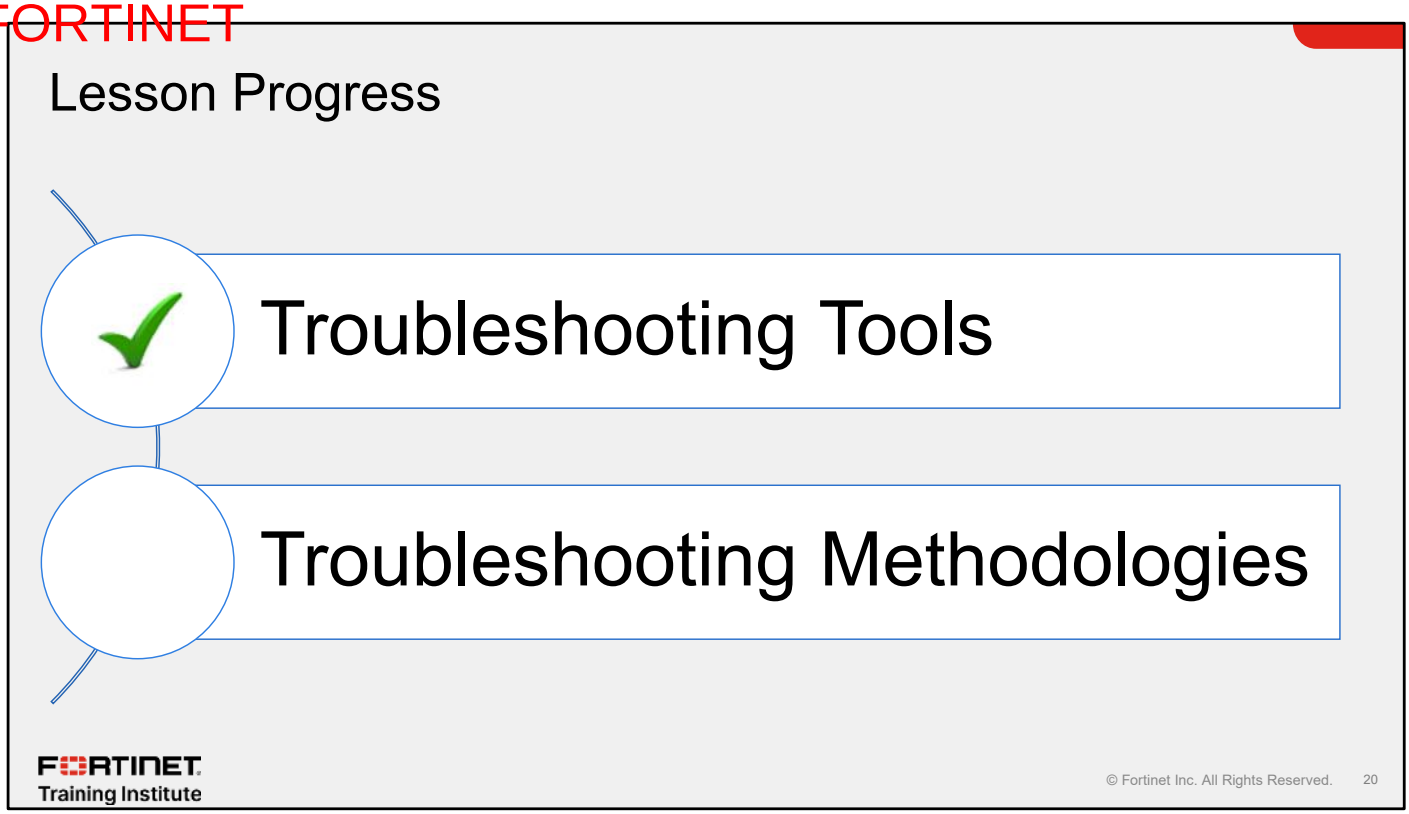
2. Which history log column shows the action FortiMail took on an email?
   - A. **Classifier**
   - ✓ B. **Disposition**

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 19

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Good job! You now understand FortiMail troubleshooting tools.

Now, you will learn about troubleshooting methodologies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Troubleshooting Methodologies

Objectives

- Use the built-in troubleshooting tools to address common issues

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 21

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in using the built-in troubleshooting tools, you will be able to effectively manage issues that arise on FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Troubleshooting Basics—Where Do You Start?

- Look at the logs first!
  - For email events, start with the history logs
    - Use the session ID to view the correlated logs
  - If no history logs exist, or if looking for system events, search the event logs
    - Narrow the search scope using the **Level** and **type** drop-down lists
  - If no history or event logs exist, check network connectivity
    - Use `execute ping` and packet capture tools to check connectivity
- Be mindful of time
  - Not all MTAs exist in the same time zone
- An MTA can send *more than one* email through a *single* TCP session

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 22

To address most email-related issues that occur on FortiMail, you should start by looking at the logs. By far, FortiMail logs provide the most information about the activities and behaviors of the system. The default settings produce verbose logs full of detail.

Start with the history logs. If you can find the event in question, use the session ID to view the correlated logs. At this point, you can be sure that a successful transmission control protocol (TCP) session was established, and any issues were caused by higher-layer inspections.

If no history logs exist, it means no TCP session was established. This is the time to search the event logs. Try to narrow down your search scope using filters. When searching event logs, always be aware of time and shifting time zones.

Not all MTAs exist in the same time zone, so pinpointing the exact time period of the event will help in finding the logs related to the event.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGuard Antivirus and Antispam Updates

- Ensure FortiMail is registered with a proper support contract to receive updates from the FDN
- Use network test commands to check connectivity with the `update.fortiguard.net` server on port 443

```
#execute ping update.fortiguard.net
```

  - Is DNS resolution working? Are there ping responses?

```
#execute telnet update.fortiguard.net:443
```

  - Can FortiMail establish an outbound connection on port 443?
- Alternatively, use the built-in sniffer to verify traffic flow
  - Are the update requests leaving FortiMail?
  - Are the responses arriving at FortiMail?

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 23

FortiMail receives antispam and antivirus updates from the Fortinet Distribution Network (FDN), as long as there is a support contract attached to the device serial number. If the FortiMail device is registered and isn't receiving updates, there are a few things you can check to verify whether or not FortiMail is set up correctly to receive updates.

All update requests are sent to update.fortiguard.net using port 443. You can use the `execute ping` command to test DNS resolution and verify connectivity. You can also use the `execute telnet` command to verify whether or not FortiMail can establish an outbound TCP connection on port 443. If either of these tests fail, you must address the root causes accordingly. For example, if the DNS resolution fails, ensure you have the correct DNS servers configured on Fortimail. If there are no ping responses, or if the telnet connection fails on port 443, ensure the default gateway is configured correctly on FortiMail. You may also need to investigate the issue on your network firewall to ensure the proper firewall rules are in place for FortiMail to allow outbound connections on port 443.

Alternatively, you can use the built-in packet sniffer to verify traffic flow. If DNS or the default gateway is not configured correctly, you won't see any update requests leaving FortiMail. If there is an issue with firewall rules, you would see the requests leave FortiMail; however, you wouldn't see any response traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGuard Update Real-Time Debug

```
diagnose debug application update 7
diagnose debug enable
execute update now

01.03-10:15:19 upd_daemon.c[1005] upd_daemon-Received update now request
01.03-10:15:19 upd_daemon.c[378] do_update-Starting now UPDATE (final try)
01.03-10:15:19 upd_act.c[381] upd_act_update-Trying FDS 96.45.33.89:443 with AcceptDelta=1
01.03-10:15:19 upd_comm.c[229] tcp_connect_fds-Proxy tunneling is disabled
01.03-10:16:19 upd_comm.c[252] tcp_connect_fds-select() timed out
01.03-10:16:19 upd_comm.c[546] upd_comm_connect_fds-Failed TCP connect
01.03-10:16:19 upd_vm.c[209] upd_vm_cfg_set_status-Saved status code 502
...

diagnose debug application update 7
diagnose debug enable
execute update now

01.03-12:58:08 upd_daemon.c[1005] upd_daemon-Received update now request
01.03-12:58:08 upd_daemon.c[378] do_update-Starting now UPDATE (final try)
01.03-12:58:08 upd_cfg.c[69] upd_cfg_get_host_by_name-Failed to gethostbyname for
update.fortiguard.net
...

diagnose debug disable
diagnose debug application update 0
```

TCP connection failure

DNS failure

Disable debugging after you are done.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 24

You can also see the update process status message in real time using the CLI commands shown on this slide. After you have collected the required output, disable debugging.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGuard Rating Queries

- Use the ping command to check connectivity with `service.fortiguard.net`

```
#execute ping service.fortiguard.net
```

  - Is DNS resolution working? Are there ping responses?
  - If the perimeter firewall is configured to do DNS traffic inspection, try one of the alternate service ports - 8888, or 8889
    - Ensure any applicable firewall rules are in place to allow the traffic
- Use the built-in sniffer to verify traffic flow
  - Are the rating queries leaving FortiMail?
  - Are the responses arriving back at FortiMail?

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 25

Rating queries are an important function of FortiMail inspection tasks. Failed queries can result in spam being delivered to end users. Use the FortiGuard query tool to test whether FortiMail can perform successful queries.

All rating requests are sent to the service.fortiguard.net FQDN. By default, FortiMail is configured to use port 53. If your network firewall is configured to perform DNS inspection, it will interfere with the rating query traffic. In such cases, you should use one of the alternate service ports: 8888 or 8889.

Similar to FortiGuard update troubleshooting, you can use the built-in packet sniffer to verify traffic flow. If DNS or default gateway are not configured correctly, you would not see any rating requests leaving FortiMail. If there is an issue with firewall rules, you would see the requests leave FortiMail; however, you wouldn't see any response traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

False Positives

- Check the logs to find out which antispam technique triggered the false positive
- The major causes of false positives are DMARC, heuristics, and Bayesian
  - Enable DMARC for specific domains only
    - DMARC is still new, and may not yet have been adopted by the majority of organizations
  - Increase the heuristics threshold or reduce the percentage of rules used
  - Disable the bayesian database if users are not participating in training the databases
- Content profile can also cause false positives, and is immune to the safelist

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 26

When you encounter false positives, check the logs first. Identify which FortiMail feature detected the email message as spam.

The most common sources of false positives are Domain-based Message Authentication, Reporting and Conformance (DMARC), heuristics, and Bayesian detection.

DMARC relies on the presence of a Sender Policy Framework (SPF) record, or a DomainKeys Identified Mail (DKIM) signature. While SPF has been around longer, it's still not adopted by everyone, and DKIM even less so. To prevent false positives by DMARC, you can enable it only for domains known to use SPF records or DKIM signing.

If heuristics are causing false positives, try increasing the thresholds or reducing the percentage of rules used.

If the bayesian databases are not continuously trained, or worse, not trained at all, filtering becomes far less accurate. Since the other FortiMail scan methods are more accurate without needing continuous maintenance, you should disable bayesian filtering in most cases.

Content profiles can cause false positives if they match unintended messages. This can be especially problematic, since content profiles are immune to safelist entries. If content profiles are causing false positives, check the profile configuration and see if you can configure it to be more selective.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

False Negatives

- Check the logs to find out which access control rule, IP policy, and recipient policy processed the email
- Ensure antispam profiles have at least the following features enabled:
  - FortiGuard
    - IP reputation, deep header inspection, URI filter, and spam outbreak protection
  - Behavior analysis
  - Header analysis
  - SURBL and DNSBL
    - Use well-known third-party rating servers
  - Image spam
    - Use the aggressive option to scan image attachments
  - Suspicious newsletter

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 27

When spam makes it through the FortiMail antispam scans, the first place you should look is the logs. Verify which access control rule, IP policy, and recipient policy processed the emails. Then, check the configuration of the policies and profiles, and ensure the proper antispam features are enabled.

As a baseline, your inbound antispam profiles should have at least the following features enabled:
- FortiGuard IP reputation, deep header inspection, URI filter, and spam outbreak protection
- Behavior analysis
- Header analysis
- Spam URI real-time block Lists (SURBL) and domain name system block lists (DNSBL)
- Image spam
- Suspicious newsletter

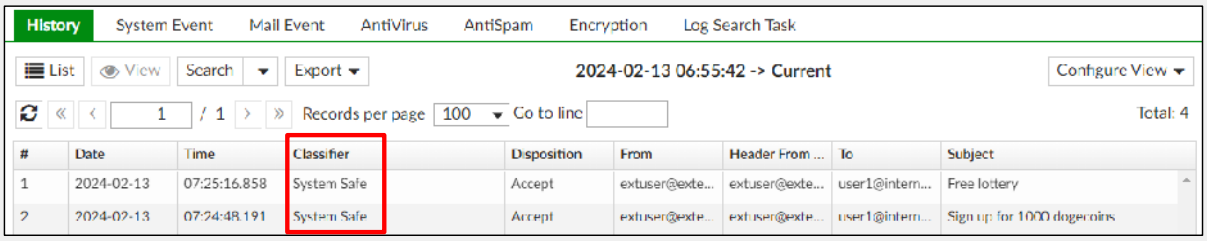
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

False Negatives (Contd)

- Make sure that spam is not slipping through any safelists
  - Use caution when using wildcards in a safelist entry
  - If possible, avoid safelisting entire domains

Monitor > Log > History



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 28

The FortiMail safelists can be another source of false negatives. There are four safelists: system, session, domain, and personal. A matching entry in any safelist causes the email to bypass antispam. Use caution when using wildcards in safelist entries, because they can cause false negative issues as well.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

False Negatives (Contd)

- Enable antispam features specifically intended to proactively combat zero-day outbreaks
  - FortiGuard spam outbreak protection
  - Behavior analysis
  - Header analysis

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 29

FortiMail has antispam features specifically designed to combat zero-day outbreaks. These include FortiGuard spam outbreak protection, behavior analysis, and header analysis.

For more information about these features, see the *Antivirus and Antispam* lesson.

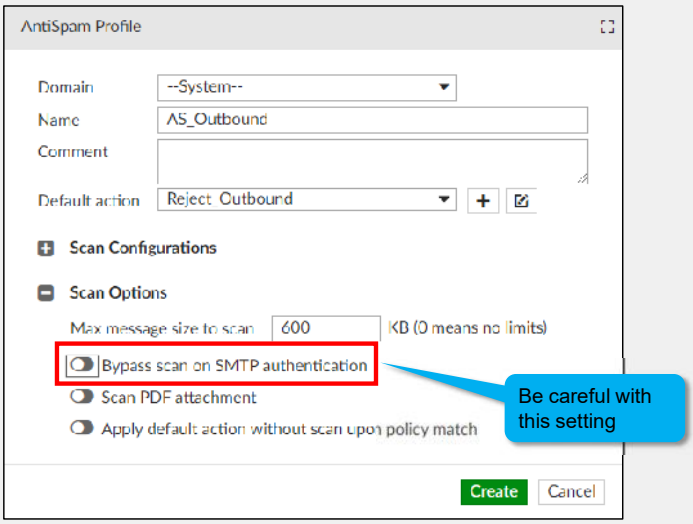
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

False Negatives (Contd)

- Trust no one!
- If spam is coming from an authenticated user, it may be coming from a compromised device

Profile > Antispam > Antispam



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 30

When configuring the FortiMail antispam settings, a common mistake is to consider only incoming email as potential spam threats. With the rise of spam bots, internal devices are now sources of spam traffic, and you should treat their outbound email with the same level of suspicion as incoming messages.

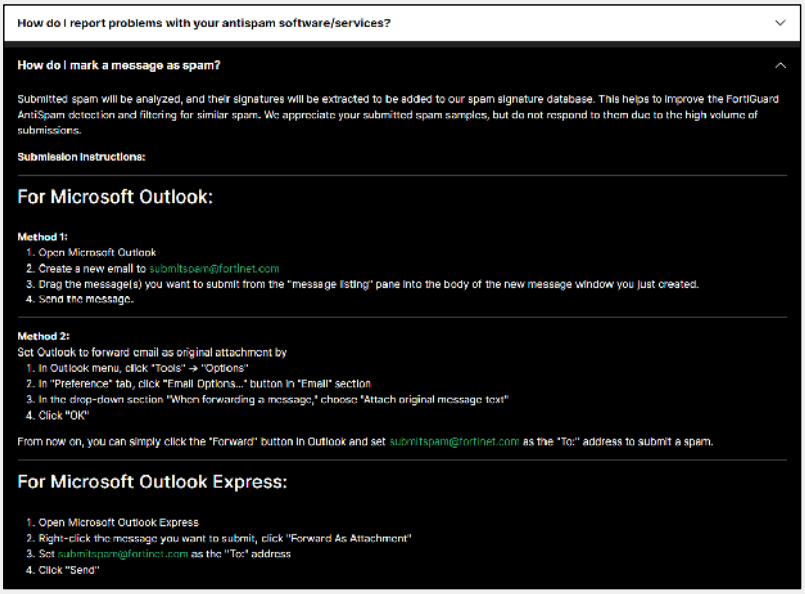
Each FortiMail antispam profile contains the **Bypass scan on SMTP authentication** setting, which, as its name implies, skips antispam scanning if the SMTP session is coming from an authenticated user. If this setting is enabled in the active antispam profile used by a compromised device, then FortiMail delivers all its outbound messages. This not only leads to false negatives, but could also adversely affect the IP reputation of the domain. Use this setting with caution!

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

False Negatives (Contd)

- Sometimes, spam just gets through
- Submit spam to FortiGuard so that it is added to the spam signature database
- Visit the FortiGuard website (www.fortiguard.com) for more information and scroll down to *Frequently Asked Questions*



How do I report problems with your antispam software/services?

How do I mark a message as spam?

Submitted spam will be analyzed, and their signatures will be extracted to be added to our spam signature database. This helps to improve the FortiGuard AntiSpam detection and filtering for similar spam. We appreciate your submitted spam samples, but do not respond to them due to the high volume of submissions.

Submission Instructions:

For Microsoft Outlook:

Method 1:

1. Open Microsoft Outlook
2. Create a new email to submitspam@fortinet.com
3. Drag the message(s) you want to submit from the "message listing" pane into the body of the new message window you just created.
4. Send the message.

Method 2:

Set Outlook to forward email as original attachment by

1. In Outlook menu, click "Tools" → "Options"
2. In "Preference" tab, click "Email Options..." button in "Email" section
3. In the drop-down section "When forwarding a message," choose "Attach original message text"
4. Click "OK"

From now on, you can simply click the "Forward" button in Outlook and set submitspam@fortinet.com as the "To:" address to submit a spam.

For Microsoft Outlook Express:

1. Open Microsoft Outlook Express
2. Right-click the message you want to submit, click "Forward As Attachment"
3. Set submitspam@fortinet.com as the "To:" address
4. Click "Send"

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 31

Even when FortiMail is properly configured, false negatives and false positives can sometimes happen. When this happens, you can submit the messages to FortiGuard for evaluation and inclusion in the FortiGuard databases. To view the instructions for submitting the offending email, visit the FortiGuard website.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

No Incoming Email

- Check that SMTP traffic is arriving at FortiMail
  - Send an email from an external source while running a packet capture on the arriving interface
- Verify that you can telnet to the MX record on port 25 from an outside machine
- Check the logs
  - Use the SMTP event logs to determine where the issue lies
- For gateway and transparent mode, check the deferred queue
  - If there is a connection issue between FortiMail and the back-end server, email starts queuing up
  - Test the connectivity between FortiMail and the back-end server

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 32

A lack of incoming email can be caused by several issues. You should verify that incoming email is arriving at FortiMail by sending a message from an outside source while running a packet capture.

If no traffic is arriving at FortiMail, try the following:

- Check that the DNS MX record resolves to the correct IP address. If your organization's MX record doesn't resolve correctly to an IP address, no MTA will be able to find your FortiMail.
- From the outside, use telnet to connect to the MX record's IP address on port 25 and verify that the normal SMTP session conversation is happening. If this test fails, it is most likely either a firewall rule, or a destination network address translation (DNAT) issue.
- Check the SMTP event logs to determine where the issue lies. Depending on the deployment mode, the presence, or absence, of certain event logs will identify if the issue is a FortiMail issue.
- For gateway and transparent mode, check the deferred queue. If there is a connection issue between FortiMail and the back-end server, email starts to fill the queue. Test the connectivity between FortiMail and the back-end server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

No Outbound Email

- Check the logs
  - Ensure proper access receive rules are in place
- Check that the SMTP traffic is leaving FortiMail
  - Send an outbound email while running a packet capture to verify
- Test the DNS resolution on FortiMail
  - DNS is a critical service for email operations, especially for outbound email
- Use the `smtptest` command to connect to an outside MTA
  - Determine if it's a global issue, or only certain MTAs
- Check the deferred queue
- Check the outbound session profile configuration

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 33

If outbound email messages are not being delivered by FortiMail, check the logs first. Ensure proper access control rules are in place. See the *Access Control and Policies* lesson.

If that doesn't expose the cause of the problem, try the following:

- Test the DNS resolution on FortiMail; DNS is a critical service for email operations.
- Use the `smtptest` command to connect to an outside MTA. Determine if it's a global issue, or only affecting certain MTAs. Your MX IP just might be blocklisted.
- Check the deferred queue; deferred messages include the reason for their deferral.
- Verify that the outbound session profile isn't interfering with email delivery by being too restrictive. It's a recommended practice to create specific IP policies with less restrictive session profiles, for outbound email.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Blocklisted MX IP Address

- Is FortiMail configured correctly?
  - Ensure access receive rules are not configured to allow open relay
- Is outbound traffic passing through FortiMail?
  - Redirect all outbound email through FortiMail to allow antispam scanning
- Block any outbound SMTP traffic from your organization that isn't coming from the FortiMail IP address

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 34

Since IP blocklists are an important and widely-used tool to limit spam, maintaining your public IP reputation is critical. If spam email is being sent using your public MX IP address or addresses, you could quickly find that your outbound email is being rejected because of a poor IP reputation.

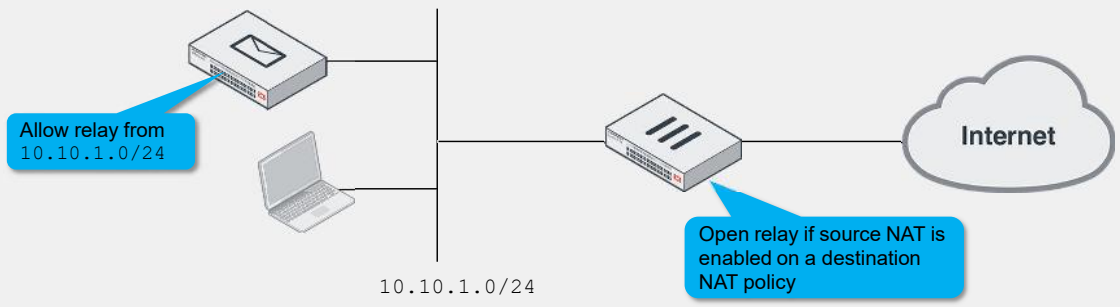
If this happens, ensure that FortiMail is not improperly configured to act as an open relay, and that outbound email is passing through antispam scans. Another potential cause of a poor IP reputation is that outbound SMTP sessions are bypassing FortiMail entirely. This can happen with client devices that are compromised with spambot malware. To prohibit SMTP traffic from bypassing FortiMail, block all SMTP traffic at the firewall, except for SMTP sessions originating from the FortiMail IP address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Open Relay

- Check the logs to see if the relay is being done by an authenticated user
- Check for any wide-open access rules (`x.x.x.x/0`)
- Check for subnet-wide access receive rules combined with inbound NAT



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 35

As a rule, you should never configure FortiMail to operate as an open relay, a MTA that forwards email from any arbitrary external senders. By default, FortiMail without any access rules prohibits the system from acting as an open relay. When configuring access receive rules, take great care to make sure that the access rule doesn't create an unintentional open relay situation, such as specifying a sender IP address value with a `/0` subnet mask and an action of relay.

You can also create an open relay situation when combining a subnet-wide access control receive rule with a misconfigured NAT policy on a firewall. For example, if source NAT (SNAT) is enabled on a destination NAT (DNAT) policy, all inbound traffic through that policy will have its source IP address NATed to an internal IP. This will inadvertently satisfy the access receive rule constraints and allow relaying.

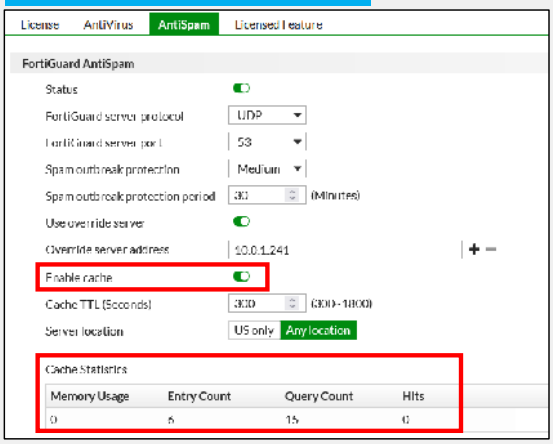
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

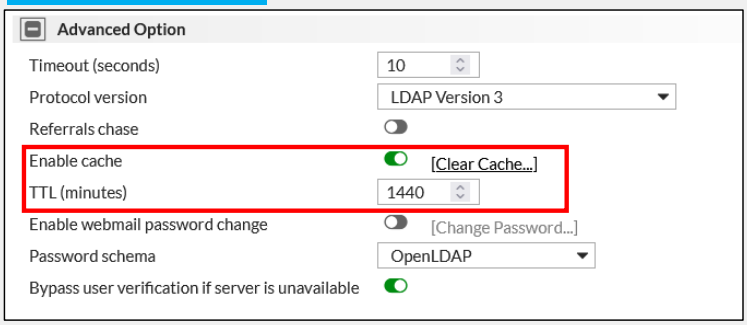
High CPU or Memory Utilization

- Make sure there are no significant delays in DNS resolution
- Enable antispam rating cache
- Enable LDAP caching

System > FortiGuard > AntiSpam



Profile > LDAP > LDAP



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 36

High CPU or memory utilization is often caused by DNS resolution or slow LDAP responses. These things are often indicated by frequent DNS or LDAP errors being reported in the event logs under the system type.

By default, DNS caching is enabled on FortiMail. This can alleviate some of the problems related to slow DNS resolution. You can also enable antispam rating caching to alleviate it further. However, you must still address the root cause of the problem, which is most likely an overtaxed DNS server.

LDAP query results can also be cached, to temporarily alleviate some of the symptoms caused by slow responses. However, you should address the root cause as soon as possible.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

SMTP Disconnections or Timeouts

- Event logs show timeout messages
  `Milter (mailfilterd): timeout before data read, where=rcpt`
- Check CPU and memory utilization
  - High resource utilization causes delays and premature session termination
  - Use the `diagnose system top` command to determine if a particular process is responsible
- Use packet capturing to determine if there is packet loss in the network
- Verify that no other device is performing inspection on the SMTP traffic
  - If another device is performing SMTP inspection, it will introduce delays, which cause timeouts

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 37

If the logs show frequent SMTP disconnects or timeouts, first review the CPU and memory utilization to check that the system is not critically overloaded. Another possible cause is an intervening firewall device configured to perform security inspection on SMTP traffic destined for FortiMail. This can cause the SMTP session to be significantly delayed and can cause the remote MTA to prematurely terminate the session. Since FortiMail is a dedicated device for SMTP inspections, disable SMTP inspections at the firewall level.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Delayed Emails

- Check the logs to see if delays are caused by greylisting
  - Don’t enable greylisting on outbound email
- Check the SMTP event logs

```
2021-06-11 - 12:18:41 - to=<user@test.com>, delay=00:00:01, xdelay=00:00:01,
mailer=esmtp, pri=30690, relay=smtp.test.com. [10.10.10.1], dsn=2.0.0,
stat=Sent (r1BKIfaB028780-r1BKIfaD028780 Message accepted for delivery)
```

Time between FortiMail receiving the email and being able to deliver it

- Check deferred mail queue

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 38

Email may be delayed if the greylisting feature is enabled, if it’s the first attempt for a triplet. Ensure greylisting is not enabled on outbound email. For delay issues not caused by greylisting, the SMTP event logs will show whether the delay occurred due to FortiMail processing. The delay field shows the time it took FortiMail to process an email and send it out. Outbound email may also be delayed if the next MTA hop is experiencing issues or is not responding. Check the deferred queue, which will indicate the reason for deferral.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Hard Disk Issues

```
# execute formatmaildisk
```

- This operation erases all mail data and rebuilds the mail disk partition

```
# execute formatmaildisk_backup
```

- This operation backs up the mail data to the log disk, if there is sufficient space, and then formats the mail disk partition
- This is done as a best-effort process and doesn't guarantee data retention

```
# execute formatlogdisk
```

- This operation erases all log data and rebuilds the log disk partition

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 39

In the rare event that there are unrecoverable disk issues, you may need to format the drives. You can use the format commands to rebuild either the mail or log partitions. Formatting erases all data, so perform any necessary backups prior to executing the commands.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Knowledge Check

1. Which troubleshooting step should you take when investigating FortiGuard antispam and antivirus update issues?
   - ✓ A. Confirm that FortiMail can establish outbound connections on TCP port 443.
   - B. Use the `execute ping` command to check connectivity with fgd.fortiguard.net.

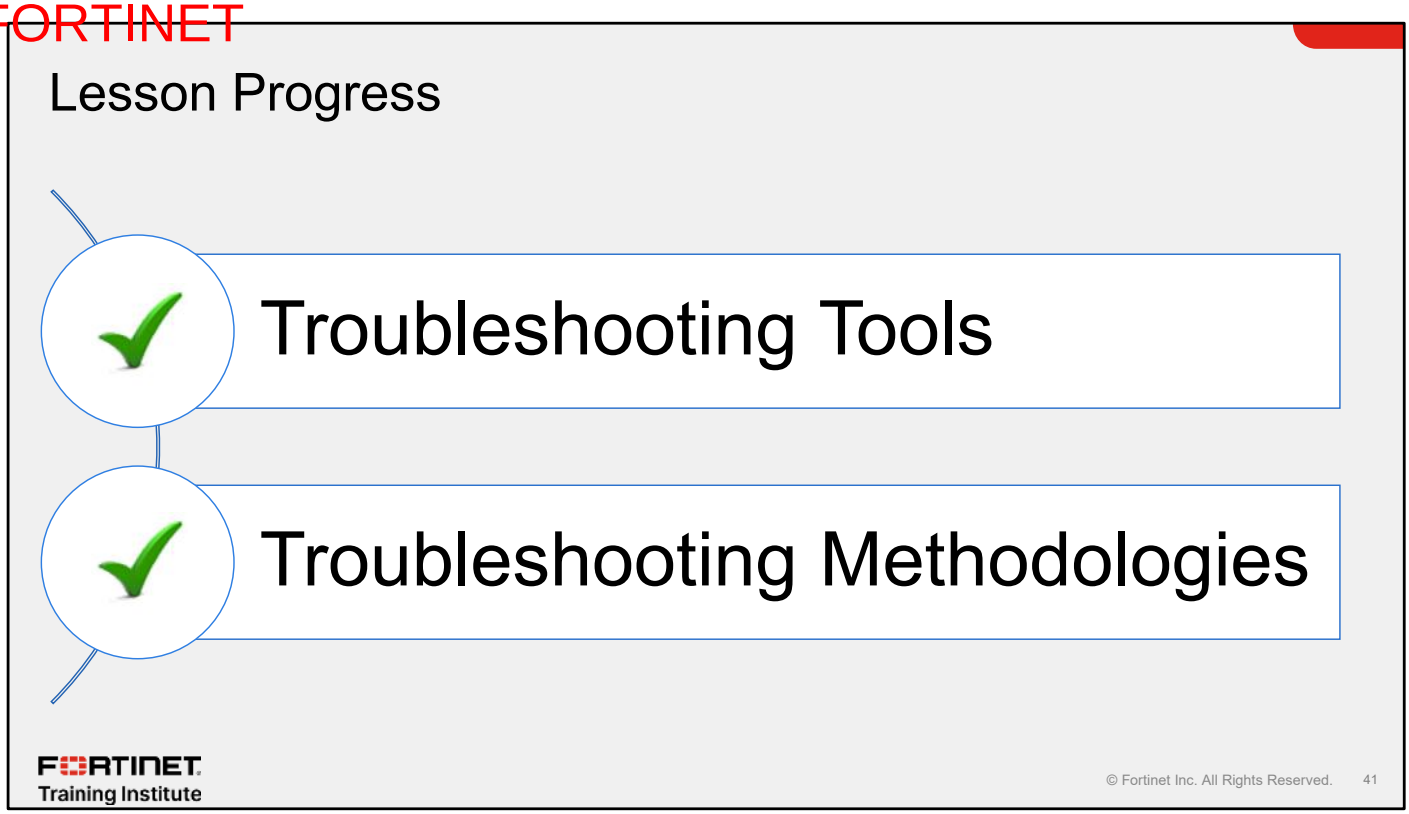
2. If the heuristics antispam technique is causing many false positive detections, what action can you take to reduce the catch rate?
   - A. Retrain the local heuristic database.
   - ✓ B. Reduce the percentage of rules used.

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 40

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Review

- ✓ Use connectivity testing tools
- ✓ Use the built-in packet capture tools
- ✓ Use log searching and log message correlation to find relevant logs
- ✓ Decipher SMTP event logs to pinpoint the root cause of SMTP connection issues
- ✓ Use the built-in troubleshooting tools to address common issues

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved. 42

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned some useful tips for troubleshooting FortiMail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Vouchers & Dumps are Available | WhatsApp +201224560923