FORTINET NSE 6 SPECIALIST

FortiMail
Lab Guide

for FortiMail 7.2

FORTINET®
Training Institute

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)

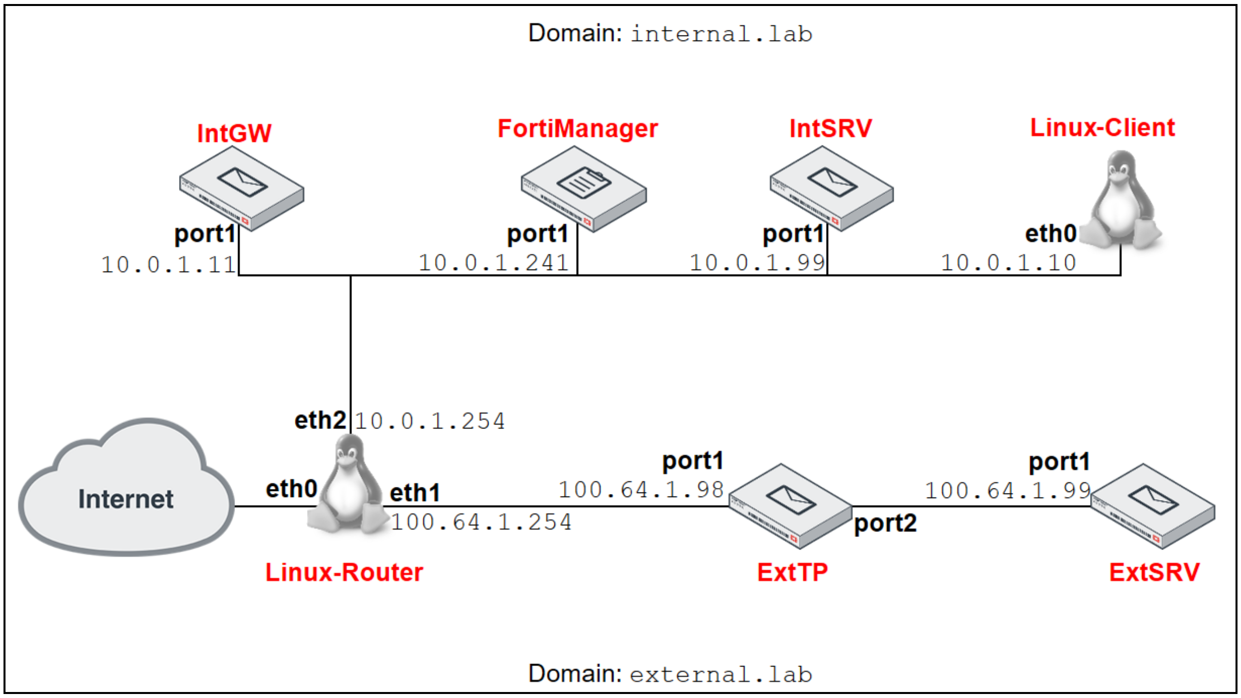
https://helpdesk.training.fortinet.com/support/home

FORTINET

9/13/2022

TABLE OF CONTENTS

Network Topology



Lab 1: Initial Setup

In this lab, you will verify the DNS MX records for both of the lab domains, perform the initial configuration tasks for the FortiMail VMs installed in the `internal.lab` domain for inbound email, and configure an email client to connect to a FortiMail running in server mode. Then, you will issue basic SMTP commands and inspect email headers to understand the flow of SMTP.

Objectives

- Verify DNS MX records for the lab domains
- Configure the initial system and email settings on the FortiMail that is operating in server mode
- Configure the initial system and email settings on the FortiMail that is operating in gateway mode
- Manually send basic SMTP commands to an email server to understand SMTP

Time to Complete

Estimated: 45 minutes

Exercise 1: Verifying DNS Records

DNS is a critical component in routing email messages. In this exercise, you will use the nslookup command-line tool to verify the published DNS mail exchanger (MX) records for both the `internal.lab` and `external.lab` domains, in order to understand how mail routing works in the lab network.

Verify MX Records

The DNS servers in the lab are configured with MX records that are associated with the `internal.lab` and `external.lab` domains. MX records are necessary to route email messages to mail transfer agents (MTAs), which are responsible for accepting email messages.

To verify MX records

1. On the Linux-Client VM, open a terminal window (`Ctrl`+`Alt`+`T`).
2. Enter the following command to display the MX records associated with the `external.lab` domain:

   ```
   nslookup -type=mx external.lab
   ```

   You should receive an output similar to the following example:

   ```
   student@client:~$ nslookup -type=mx external.lab
   Server: 10.0.1.254
   Address: 10.0.1.254#53

   external.lab mail exchanger = 10 extsrv.external.lab.
   ```

   What is the primary MX record for the `external.lab` domain? ______________________________

As indicated in the nslookup query output, there is one MX record associated with the `external.lab` domain:

```
external.lab mail exchanger = 10 extsrv.external.lab.
```

Therefore, all email messages sent to the `external.lab` domain must be sent to the `extsrv.external.lab` host.

3. Enter the following command to display the MX records associated with the `internal.lab` domain:

   ```
   nslookup -type=mx internal.lab
   ```

   You should receive an output similar to the following example:

   ```
   student@client:~$ nslookup -type=mx internal.lab
   Server: 10.0.1.254
   Address: 10.0.1.254#53

   internal.lab mail exchanger = 10 intgw.internal.lab.
   internal.lab mail exchanger = 20 intsrv.internal.lab.
   ```

   What is the primary MX record for the `internal.lab` domain? ______________________________

   What is the secondary MX record for the `internal.lab` domain? ______________________________

As indicated in the nslookup query output, there are two MX records associated with the `internal.lab` domain:

```
internal.lab mail exchanger = 10 intgw.internal.lab.

internal.lab mail exchanger = 20 intsrv.internal.lab.
```

The `intgw.internal.lab` host is the primary MTA for the `internal.lab` domain because it has the lowest preference value. However, at this point in the lab, you haven’t configured the IntGW FortiMail VM to process email messages, so it won’t respond to SMTP sessions. When the TCP connection fails, the remote sender automatically tries to send email messages to the next MX record on the list, which is `intsrv.internal.lab`.

4. Close the terminal window.

In the lab network, the MX records for the `internal.lab` domain are designed for convenience and shouldn't be used as a template for real-world deployments.

Since the back-end mail server might not have the full range of email security features enabled, publishing it as a secondary MX entry is detrimental to security. Spammers can easily use MX records to identify and exploit these servers.

Publishing the back-end mail server as a secondary MX entry also prevents certain FortiMail features, such as greylisting and sender reputation, from working effectively.

Exercise 2: Configuring FortiMail in Server Mode

In the lab network, IntSRV FortiMail is running in server mode, and is intended to be the mail server for the `internal.lab` domain. The mailboxes for end users are located on IntSRV FortiMail, and this is where you will perform all user management tasks, as well as tasks that are specific to a FortiMail that is operating in server mode.

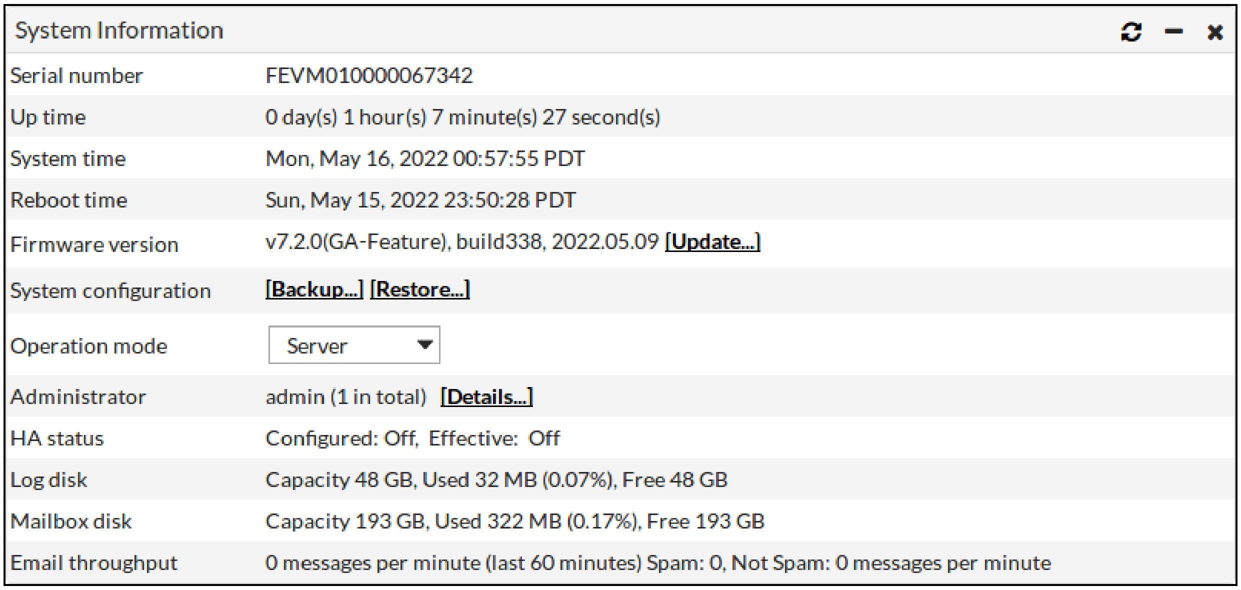
In this exercise, you will perform the basic configuration tasks required to establish inbound email flow on IntSRV FortiMail. You will verify your configuration by sending an email from ExtSRV FortiMail, and then reviewing the logs. Next, you will configure a mail user agent (MUA) to connect to IntSRV FortiMail.

Verify the Operation Mode

You will verify the operation mode of FortiMail on the dashboard of the FortiMail management GUI.

To verify the operation mode

1. On the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
2. On the **Dashboard**, in the **System Information** widget, verify that **Operation mode** is set to **Server**.



System Information

Serial number	FEVM010000067342
Up time	0 day(s) 1 hour(s) 7 minute(s) 27 second(s)
System time	Mon, May 16, 2022 00:57:55 PDT
Reboot time	Sun, May 15, 2022 23:50:28 PDT
Firmware version	v7.2.0(GA-Feature), build338, 2022.05.09 [Update...]
System configuration	[Backup...] [Restore...]
Operation mode	Server
Administrator	admin (1 in total) [Details...]
HA status	Configured: Off, Effective: Off
Log disk	Capacity 48 GB, Used 32 MB (0.07%), Free 48 GB
Mailbox disk	Capacity 193 GB, Used 322 MB (0.17%), Free 193 GB
Email throughput	0 messages per minute (last 60 minutes) Spam: 0, Not Spam: 0 messages per minute

Configure System Settings

You will configure some necessary system settings, such as the IP address of the interface, network routes, and system DNS.

To configure system settings

1. Continuing on the IntSRV FortiMail management GUI, click **System** > **Network** > **Interface**.
2. Select **port1**, and then click **Edit**.
3. Verify the following settings:

Field	Value
Addressing Mode	Manual
IP/Netmask	10.0.1.99/24

4. Expand the **Advanced Setting** section.
5. Verify the following settings:

Field	Value
Access	HTTPS, PING, SSH
Web access	Admin, Webmail
Mail access	SMTP, SMTPS, POP3, IMAP, POP3S, IMAPS
Administrative status	UP

6. Click **OK**.
7. Click **System** > **Network** > **Routing**.
8. Verify the following settings:

Field	Value
Destination IP/netmask	0.0.0.0/0
Interface	port1
Gateway	10.0.1.254

9. Click **System** > **Network** > **DNS**.
10. Configure the following settings:

Field	Value
Primary DNS server	10.0.1.254
Secondary DNS server	10.0.1.10

11. Click **Apply**.

Configure Mail Settings

You will configure a local host name and domain name. You will also configure the protected domain.

To configure mail settings

1. Continuing on the IntSRV FortiMail management GUI, click **System** > **Mail Setting** > **Mail Server Setting**.
2. Configure the following settings:

Field	Value
Host name	IntSRV
Local domain name	internal.lab

3. Click **Apply**.
4. Click **Domain & User** > **Domain** > **Domain.**
5. Click **New**.
6. Configure the following settings:

Field	Value
Domain name	internal.lab

7. Click **Create**.

Configure Server Mode Users

You will configure an email user whose mailbox will be hosted on IntSRV FortiMail.

To configure server mode users

1. Continuing on the IntSRV FortiMail management GUI, click **Domain & User** > **User** > **User**.
2. Click **New**.
3. Configure the following settings:

Field	Value
User name	user1
Display name	Mail User 1
Authentication type	Local
Password	fortinet

4. Click **Create**.

Verify Mail Flow

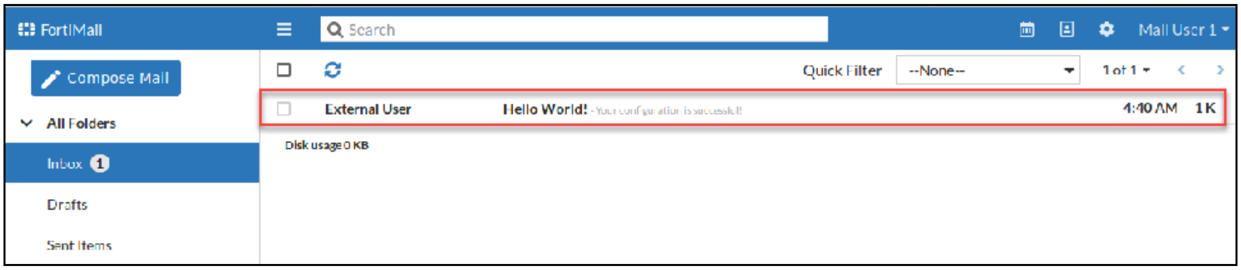
You will send an email message from a user in the `external.lab` domain to a user in the `internal.lab` domain. You will review the logs on IntSRV FortiMail, and confirm that the email message was accepted for delivery.

To send an email message

1. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
2. Click the **Compose Mail** button, and then compose a new email message using the following information:

Field	Value
To	user1@internal.lab
Subject	Hello World!
Message Body	Your configuration is successful!

3. Click **Send**.
4. On the IntSRV FortiMail webmail GUI, log in with the username `user1` and password `fortinet`.
5. If the test email message doesn't appear in the **Inbox**, click the **Refresh** icon.



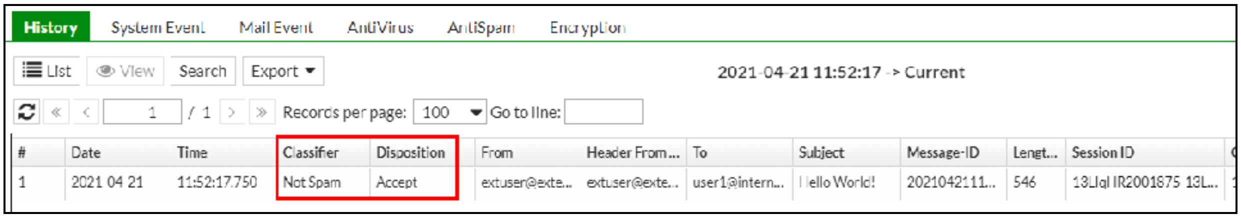
External User Hello World! - Your configuration is successful! 4:40 AM 1K

Disk usage 0 KB

6. Log out of all FortiMail webmail GUIs.

To review the logs

1. Return to the IntSRV FortiMail management GUI, and then click **Monitor** > **Log** > **History**.
2. Review the first log to verify that the system applied the appropriate **Classifier** and **Disposition** to your test email message.



2021-04-21 11:52:17 -> Current

1 / 1

#	Date	Time	Classifier	Disposition	From	Header From...	To	Subject	Message-ID	Lengt...	Session ID
1	2021 04 21	11:52:17.750	Not Spam	Accept	extuser@exte...	extuser@exte...	user1@intern...	Hello World!	2021042111...	546	13LlqI IR2001875 13L...

For the purpose of this lab, most logs are found under **Monitor** > **Log** > **History**, in the **Current** container, since the logs are generated as you test the labs. However, note that you might have to look at the historical logs to view logs that are older than a few days. You can view the historical logs by clicking **Monitor** > **Log** > **History**, and then clicking **List**.

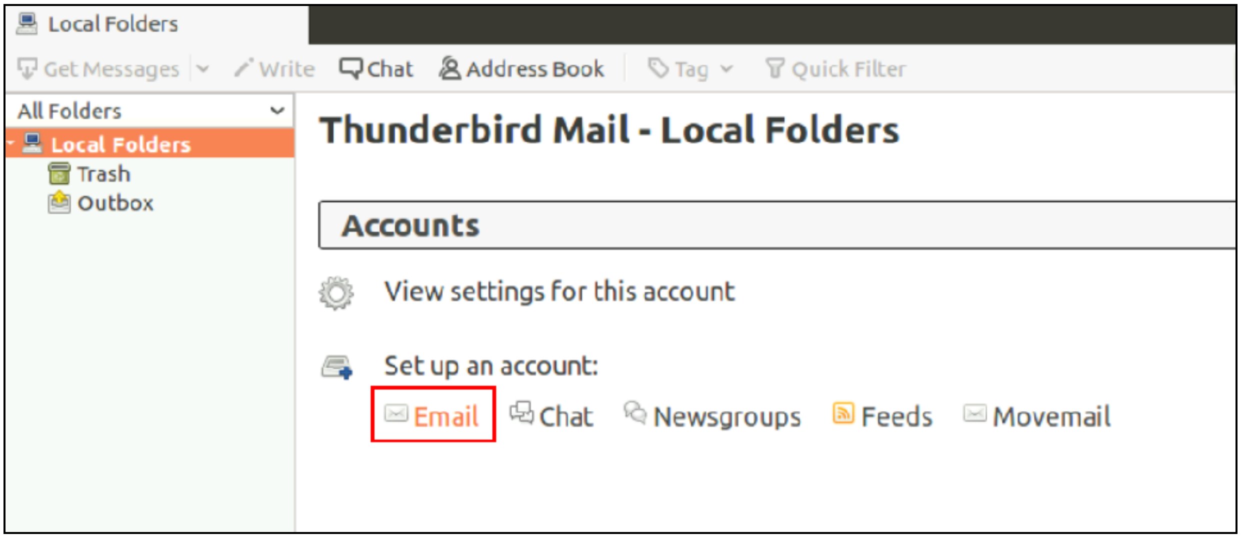
3. Log out of the IntSRV FortiMail management GUI.

Configure the MUA Client

You will configure the Mozilla Thunderbird client to connect to IntSRV FortiMail, so that you can send and receive email messages using the client, instead of using the FortiMail webmail GUI. You will use IMAP to retrieve email messages and SMTP to send email messages.

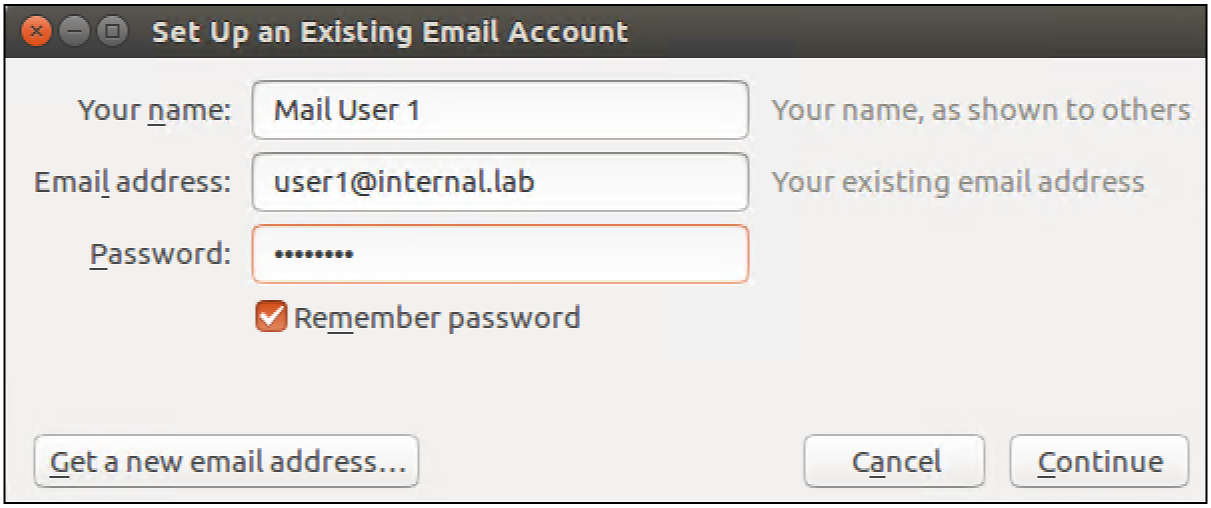
To configure the MUA to connect to the IntSRV FortiMail VM

1. On the Linux-Client VM, open Thunderbird, and then create a new email account.



2. In the **Set Up an Existing Email Account** window, configure the following account information:

Field	Value
Your name	Mail User 1
Email address	user1@internal.lab
Password	fortinet



Set Up an Existing Email Account

Your name: Mail User 1 — Your name, as shown to others

Email address: user1@internal.lab — Your existing email address

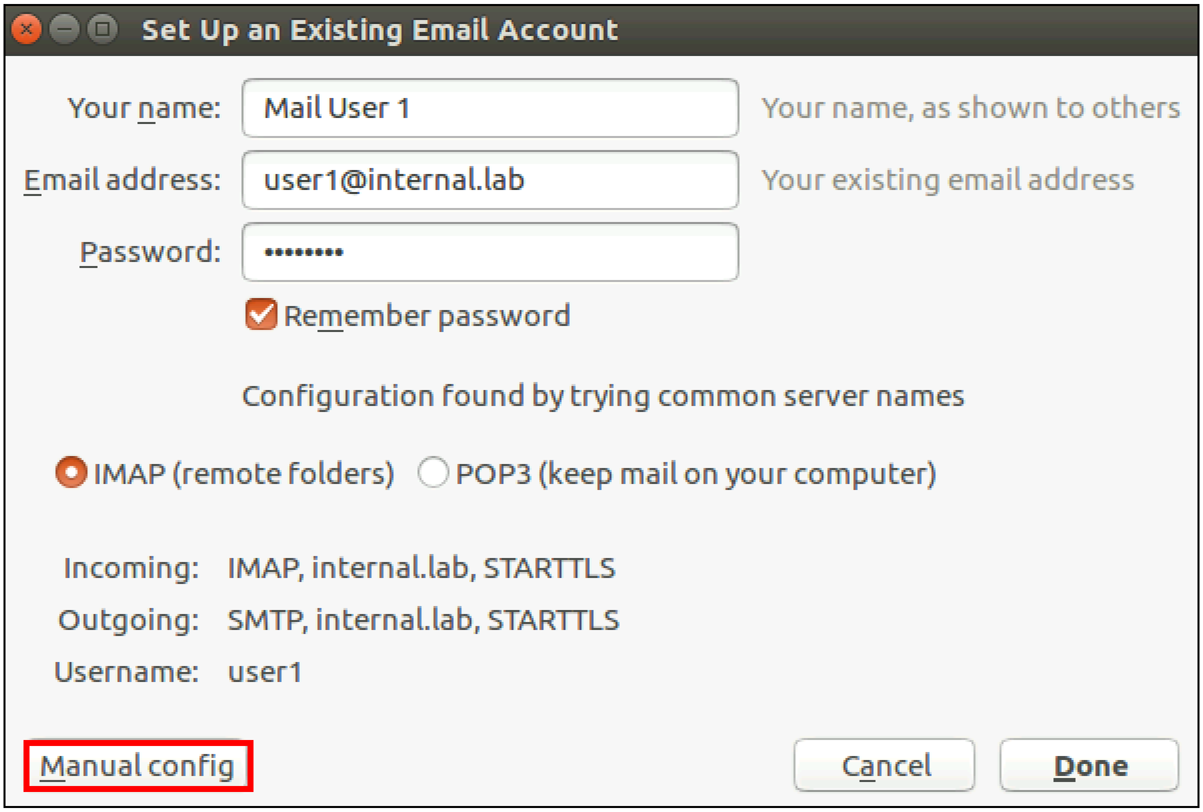
Password: •••••••••

☑ Remember password

3. Click **Continue**.

   Thunderbird attempts to auto-configure the server settings.

4. Click **Manual config**.



Set Up an Existing Email Account

Your name: Mail User 1 — Your name, as shown to others

Email address: user1@internal.lab — Your existing email address

Password: •••••••••

☑ Remember password

Configuration found by trying common server names

● IMAP (remote folders) ○ POP3 (keep mail on your computer)

Incoming: IMAP, internal.lab, STARTTLS

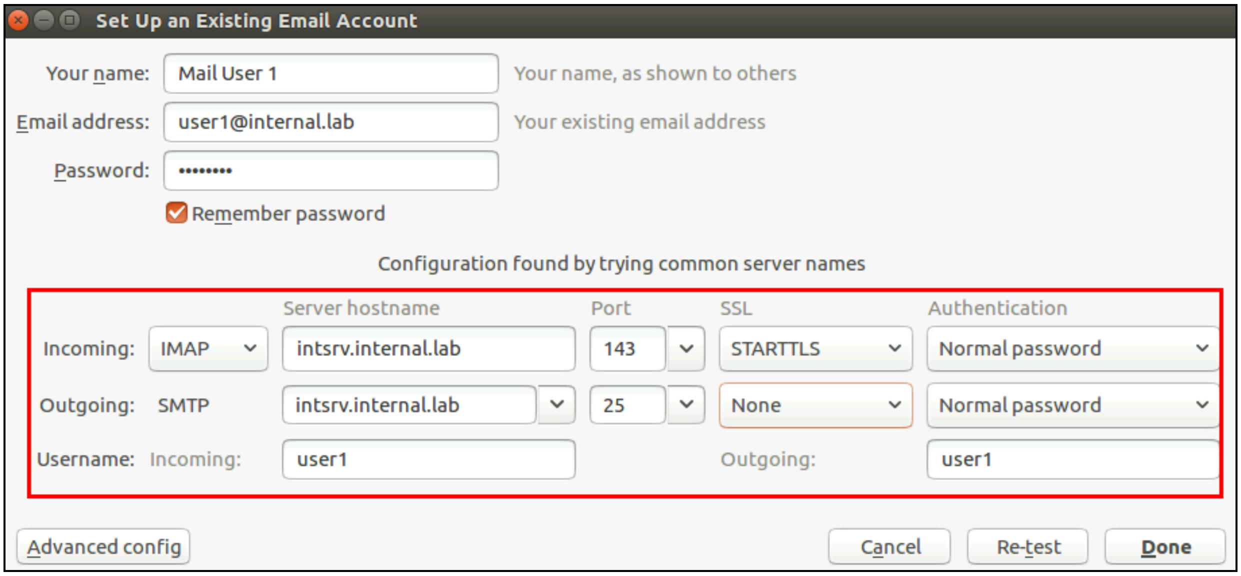
Outgoing: SMTP, internal.lab, STARTTLS

Username: user1

5. Configure the following settings:

Field	Protocol	Server hostname	Port	SSL	Authentication
Incoming	IMAP	intsrv.internal.lab	143	STARTTLS	Normal password
Outgoing	SMTP	intsrv.internal.lab	25	None	Normal password

Your configuration should match the following example:



Set Up an Existing Email Account

Your name: Mail User 1 — Your name, as shown to others

Email address: user1@internal.lab — Your existing email address

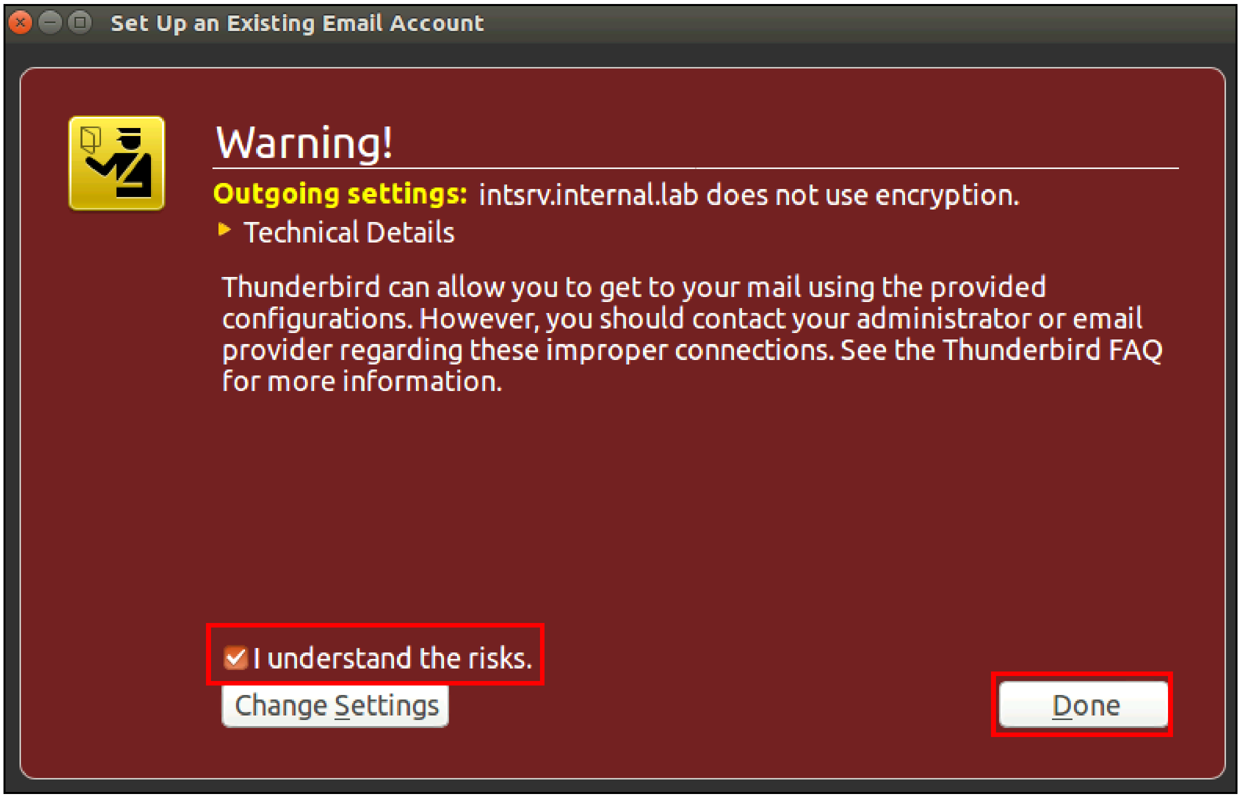
Password: ••••••••

☑ Remember password

Configuration found by trying common server names

		Server hostname	Port	SSL	Authentication
Incoming:	IMAP	intsrv.internal.lab	143	STARTTLS	Normal password
Outgoing:	SMTP	intsrv.internal.lab	25	None	Normal password
Username:	Incoming:	user1		Outgoing:	user1

6. Click **Done**.
7. Select the **I understand the risks** checkbox, and then click **Done**.



Set Up an Existing Email Account

Warning!

Outgoing settings: intsrv.internal.lab does not use encryption.

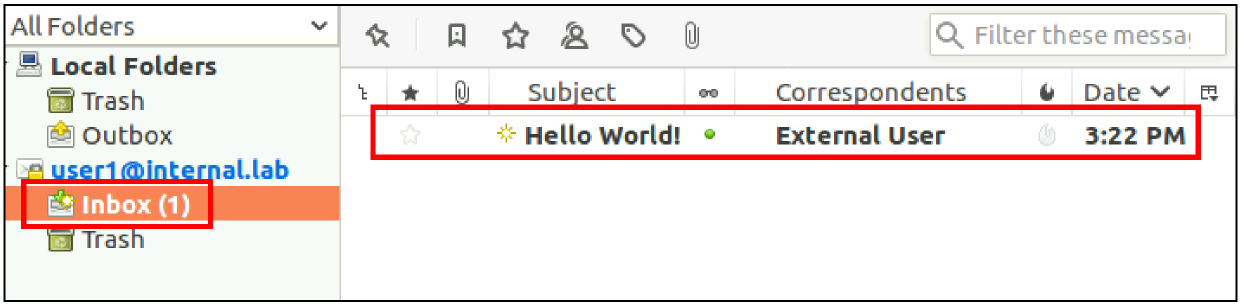
▸ Technical Details

Thunderbird can allow you to get to your mail using the provided configurations. However, you should contact your administrator or email provider regarding these improper connections. See the Thunderbird FAQ for more information.

☑ I understand the risks.

While it is OK to use unencrypted passwords in the lab network, you should avoid using them in real-world deployments.

8. If your configuration is correct, the test email message you sent in the previous exercise appears in your local inbox.



Subject	Correspondents	Date
Hello World!	External User	3:22 PM

9. Close Thunderbird.

Exercise 3: Configuring FortiMail in Gateway Mode

In the lab network, IntGW FortiMail is running in gateway mode and is intended to be the MTA for the `internal.lab` domain. IntGW FortiMail will be the relay server for IntSRV FortiMail, and also where you will perform most of the inspection configuration tasks.

In this exercise, you will perform the configuration tasks required to establish inbound email flow on IntGW FortiMail. You will verify your configuration by sending an email using swaks, and then reviewing the email headers in the Thunderbird mail client.

Remember the DNS verification tasks you performed in the first exercise. As the MX records show, the `intgw.internal.lab` (`10.0.1.11`) host is the primary MTA for the `internal.lab` domain. Therefore, all email messages should be sent to IntGW FortiMail first for processing. IntGW FortiMail will then pass the email messages to IntSRV FortiMail for delivery to the end user.

Configure System Settings

You will configure and verify some necessary system settings, such as the IP address of the interface, network routes, and system DNS.

To configure system settings

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. On the **Dashboard**, in the **System Information** widget, verify that **Operation mode** is set to **Gateway**.
3. Click **System** > **Network** > **Interface**.
4. Select **port1**, and then click **Edit**.
5. Verify the following settings:

Field	Value
Addressing Mode	Manual
IP/Netmask	10.0.1.11/24

6. Expand the **Advanced Setting** section.
7. In the **Mail access** section, enable the **SMTP**and **SMTPS** settings.
8. Verify the following settings:

Field	Value
Access	HTTPS, PING, SSH
Web access	Admin, Webmail

Field	Value
Mail access	SMTP, SMTPS, POP3, IMAP, POP3S, IMAPS
Administrative status	UP

9. Click **OK.**
10. Click **System** > **Network** > **Routing**.
11. Verify that the static route has the following values:

Field	Value
Destination IP/netmask	0.0.0.0/0
Interface	port1
Gateway	10.0.1.254

12. Click **System** > **Network** > **DNS.**
13. Configure the following DNS servers:

Field	Value
Primary DNS server	10.0.1.254
Secondary DNS server	10.0.1.10

14. Click **Apply**.

Configure Mail Settings

You will configure a local host name and domain name. You will also configure the protected domain settings.

Take the Expert Challenge!

Configure the mail server settings on IntGW FortiMail:

- The host name should be `IntGW`.
- The local domain name should be `internal.lab`.

Configure the protected domain settings on IntGW FortiMail:

- IntGW FortiMail should accept all email messages for the `internal.lab` domain.
- After processing, the email message should be delivered to IntSRV FortiMail (`10.0.1.99`).

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Verify Mail Flow on page 22.

To configure mail settings

1. Continuing on the IntGW FortiMail management GUI, click **System** > **Mail Setting** > **Mail Server Setting**.
2. Configure the following settings:

Field	Value
Host name	IntGW
Local domain name	internal.lab

3. Click **Apply**.
4. Click **Domain & User** > **Domain** > **Domain**.
5. Click **New**.
6. Configure the following settings:

Field	Value
Domain name	internal.lab
Relay type	Host
SMTP Server	10.0.1.99

`10.0.1.99` is the IP address of IntSRV FortiMail. This is the FortiMail operating in server mode that you configured in the previous exercise. It contains the user mailboxes for the `internal.lab` domain. Therefore, IntGW FortiMail is configured with `10.0.1.99` as the protected SMTP server for the `internal.lab` domain.

7. Click **Create**.
8. Log out of the IntGW FortiMail management GUI.

Verify Mail Flow

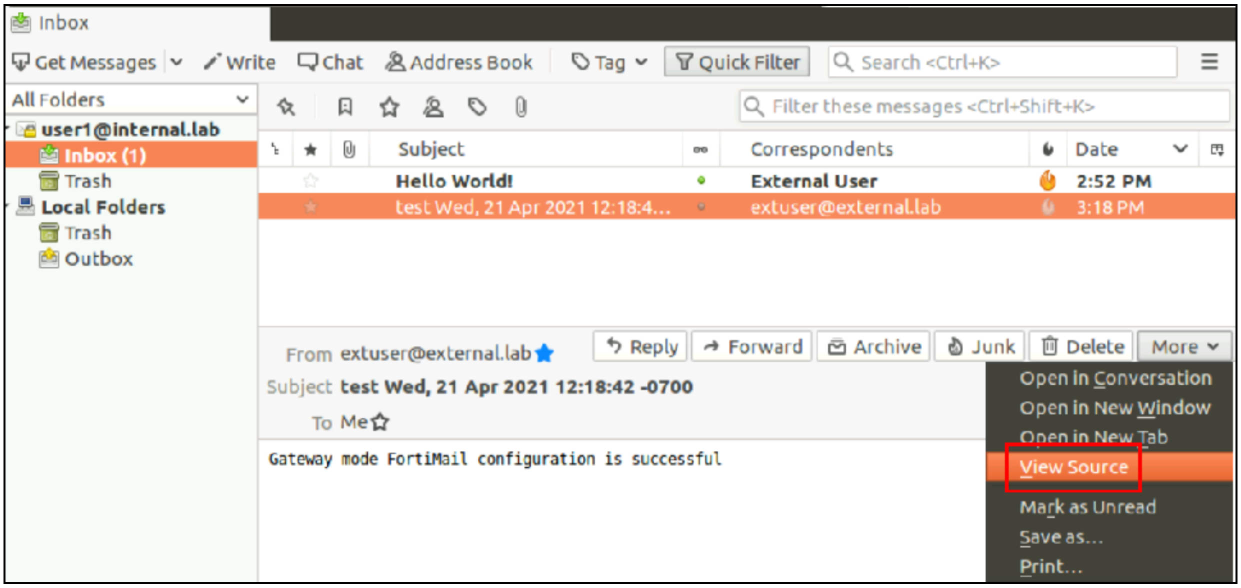
You will send an email message from the Linux-Router VM to a user in the `internal.lab` domain.

To verify mail flow

1. On the Linux-Client VM, open a terminal window (`Ctrl`+`Alt`+`T`).
2. Enter the following command to start an SSH connection to the Linux-Router VM:
   ```
   ssh student@10.0.1.254
   ```
3. Enter the password `password`.
4. Enter `pwd`.
   Verify that your current working directory is `/home/student`.
5. Enter the following swaks command to test the configuration of IntGW FortiMail:
   ```
   swaks -f extuser@external.lab -t user1@internal.lab -s 10.0.1.11 --body 'Gateway mode
       FortiMail configuration is successful'
   ```

A copy of the swaks command is in the `commands.txt` file, which is located in the **Resources** folder on the Linux-Client desktop.

6. After the script finishes, close the terminal window.
7. On the Linux-Client VM, open Thunderbird, and then view the test message that you just sent.
8. In the **More** drop-down list, select **View Source**.



Subject	Correspondents	Date
Hello World!	External User	2:52 PM
test Wed, 21 Apr 2021 12:18:4...	extuser@external.lab	3:18 PM

From extuser@external.lab
Subject test Wed, 21 Apr 2021 12:18:42 -0700
To Me

```
Gateway mode FortiMail configuration is successful
```

9. Compare the `Received` headers in the **test** email with the **Hello World!** email you sent in the previous exercise. What differences do you see?

The `Received` header of the Hello World email shows that IntSRV FortiMail received the email directly from ExtSRV FortiMail.

```
Received: from ExtSRV (extsrv [100.64.1.99]) by
IntSRV.internal.lab
```

The `Received` header of the swaks session email shows that the email was processed first by IntGW FortiMail, and then handed off to IntSRV FortiMail.

```
Received: from IntGW.internal.lab ([10.0.1.11]) by
IntSRV.internal.lab
```

10. Close Thunderbird.

Lab 2: Access Control and Policies

In this lab, you will establish outbound email flow for the `internal.lab` domain, and configure a relay host for the FortiMail that is operating in server mode. You will create IP and recipient policies, and then use logged policy IDs to identify how policies are applied to an email.

Objectives

- Configure access receive rules to allow outbound email
- Configure an external relay host
- Configure IP and recipient policies
- Use logged policy IDs to track messages

Time to Complete

Estimated: 40 minutes

Exercise 1: Establishing Outbound Email Flow

In this exercise, you will configure the necessary access receive rules on both the IntGW and IntSRV FortiMail VMs to allow outbound email.

Verify Authenticated Outbound Relay

You will verify an authenticated outbound email on IntSRV FortiMail.

To verify authenticated outbound relay

1. Go to the Linux-Client VM.
2. Open Mozilla Thunderbird, and then compose a new email to the external user using the following values:

Field	Value
To	extuser@external.lab
Subject	Testing Outbound Email
Message Body	Will this work?

3. Click **Send**.

If Thunderbird displays a security warning, select the **Permanently store this exception** checkbox, and then click **Confirm Security Exception**.

4. Close Thunderbird.
5. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
6. Verify that the `extuser` received the email.

Stop and think!

By default, FortiMail rejects outbound email, so why didn't FortiMail reject this email?

FortiMail rejects outbound email, unless the sender is authenticated. Because you configured Thunderbird to authenticate when sending emails using SMTP, IntSRV FortiMail relays it.

7. Log out of the ExtSRV FortiMail webmail GUI.

Configure Access Receive Rules

You will configure access receive rules based on sender pattern, IP address, and network mask, to allow safe relaying of emails from the `internal.lab` domain.

Take the Expert Challenge!

On IntSRV FortiMail, configure an access control receive rule that will relay emails:

- With the sender pattern containing `internal.lab`
- Originating from the `10.0.1.0/24` subnet

On IntGW FortiMail, configure an access control receive rule that will relay emails:

- With the sender pattern containing `internal.lab`
- Originating from the `10.0.1.99/32` IP address

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Verify Access Receive Rules on page 27.

To configure the IntSRV FortiMail access receive rule

1. On the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Policy** > **Access Control** > **Receiving**.
3. Click **New**, and then configure an access receive rule using the following values:

Field	Value
Sender	*@internal.lab
Source	10.0.1.0/24
Action	Relay

4. Click **Create**.

While the default behavior reduces configuration requirements, it is still a good practice to configure an access receive rule with specific sender patterns and sender IP address and network mask values in a server mode deployment, to restrict outbound sessions.

5. Log out of the IntSRV FortiMail management GUI.

To configure the IntGW FortiMail access receive rule

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Policy** > **Access Control** > **Receiving**.

3. Click **New**.
4. Configure an access receive rule using the following values:

Field	Value
Sender	*@internal.lab
Source	10.0.1.99/32
Action	Relay

On IntGW FortiMail, you are allowing only IntSRV FortiMail to relay emails by using a `/32` subnet mask. No other host can relay emails through IntGW FortiMail.

5. Click **Create**.
6. Log out of the IntGW FortiMail management GUI.

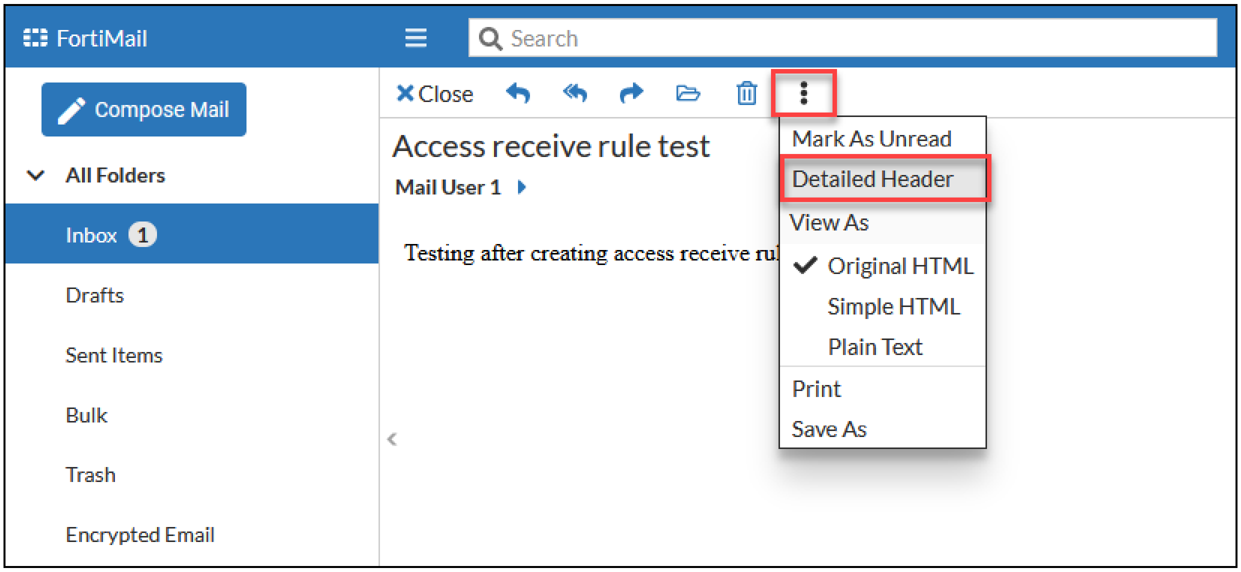
Verify Access Receive Rules

You will send an outbound email to an external user, and then analyze the headers of that email to learn about the hops the email took before arriving at the destination mail server.

To verify the access receive rules

1. Return to the Linux-Client VM, and then open Thunderbird.
2. Compose a new email to `extuser@external.lab`, and then click **Send**.
3. Return to the ExtSRV FortiMail webmail GUI, and then log in with the username `extuser` and password `fortinet`.

   The email should appear in the inbox.
4. Click the email to open it.
5. Click **More** > **Detailed Header**.



6. Review the `Received` headers.

   What hops did the email take to reach the destination inbox?

The email was generated by the Linux-Client VM (`10.0.1.10`) and sent to IntSRV FortiMail (`10.0.1.99`). IntSRV FortiMail then delivered the email to ExtSRV FortiMail (`10.200.1.99`).

```
Received: from IntSRV.internal.lab ([10.0.1.99]) by
ExtSRV.external.lab with ESMTP id 10S02Wot004754-
10S02Wov004754
```

```
Received: from [10.0.1.10] (linuxclient [10.0.1.10])
(user=user1@internal.lab mech=PLAIN bits=0) by
IntSRV.internal.lab with ESMTP id 10S02Ut3004611-
10S02Ut4004611
```

Stop and think!

Was the email relayed by IntGW FortiMail?

According to the headers, the outbound email did not pass through IntGW FortiMail, which is expected. IntSRV FortiMail delivered the email directly to the ExtSRV FortiMail based on MX query results. If you wish to ensure all outbound emails from IntSRV FortiMail relay through IntGW FortiMail, you must configure a relay host on IntSRV FortiMail.

7. Log out of the ExtSRV FortiMail webmail GUI.
8. On the Linux-Client VM, close Thunderbird.

Exercise 2: Configuring a Relay Host

In this exercise, you will configure an external relay host on IntSRV FortiMail, so that all outbound emails are sent to IntGW FortiMail for delivery.

Configure a Relay Host

For outgoing emails, you will configure an SMTP relay host on IntSRV FortiMail. This will force IntSRV FortiMail to always use the defined relay to deliver outbound emails, instead of the built-in MTA. The relay host will be IntGW FortiMail, so all outgoing emails from IntSRV FortiMail will be relayed to IntGW FortiMail.

Take the Expert Challenge!

Configure a relay host on IntSRV FortiMail, and name it `IntGWRelay`.

All outbound emails from the `internal.lab` domain should be sent to IntGW FortiMail (`10.0.1.11`).

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Verify the Relay Host on page 31.

To configure a relay host

1. On the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **System** > **Mail Setting** > **Mail Server Setting**.
3. Expand the **Outgoing Email** subsection.
4. Enable **Deliver to relay host**, and then click **+**.
5. Create a new relay host using the following values:

Field	Value
Name	IntGWRelay
Relay type	Host
Host name/IP	10.0.1.11

6. Click **Create**.
7. Click **Apply**.
8. Log out of the IntSRV FortiMail management GUI.

Verify the Relay Host

You will verify that the relay host is working by sending an email from an `internal.lab` user to an `external.lab` user.

To verify the relay host

1. On the Linux-Client VM, open Thunderbird, and then click **Write**.
2. Compose a new email using the following values:

Field	Value
To	extuser@external.lab
Subject	Testing Relay Host
Message Body	Relay host is working!

3. Click **Send**.
4. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
5. Verify that the `extuser` user received the email.
6. Review the headers.

   Do you see any differences in the `Received` headers? Which hops did the email take this time to reach the destination inbox?

The Linux-Client VM (10.0.1.10) generated the emails and sent it to IntSRV FortiMail (10.0.1.99). IntSRV FortiMail then sent the email to IntGW FortiMail (10.0.1.11). IntGW FortiMail delivered the email to ExtSRV FortiMail (10.200.1.99), which is the final destination.

```
Received: from IntGW.internal.lab ([10.0.1.11]) by
extsrv.external.lab with ESMTP id v1RLvKZS002158-
v1RLvKZU002158
```

```
Received: from IntSRV.internal.lab ([10.0.1.99]) by
IntGW.internal.lab with ESMTP id v1RLvKQj001948-v1RLvKQl001948
```

```
Received: from [10.0.1.10] (linuxclient[10.0.1.10])
(user=user1@internal.lab mech=CRAM-MD5 bits=0) by
IntSRV.internal.lab with ESMTP id v1RLvJ8k002052-
v1RLvJ8m002052
```

You have successfully established bidirectional email flow for the internal.lab domain. All inbound and outbound emails will be relayed by IntGW FortiMail.

7. Log out of the ExtSRV FortiMail webmail GUI.
8. On the Linux-Client VM, close Thunderbird.

Exercise 3: Tracking Policy Usage

As emails flow through FortiMail, it creates log entries that show which policies were used to process the emails. Understanding FortiMail policy tracking will help you to test new policies and troubleshoot existing ones.

In this exercise, you will send two emails, one in each direction, and then review which policies the emails used.

Generate Email Logs

You will send an outbound email from an `internal.lab` user, and then reply to that email from an `external.lab` user.

To generate log entries

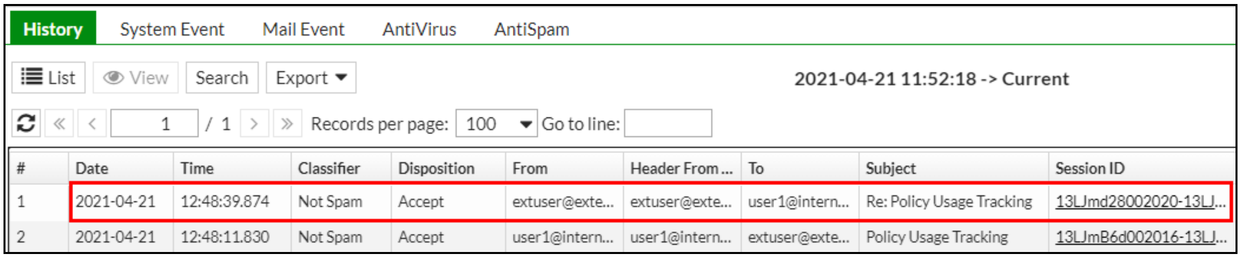
1. On the Linux-Client VM, open Thunderbird, and then send an email to `extuser@external.lab`.
2. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
3. Open the received email, and then click **Reply**.
4. In the message body, type a reply, and then click **Send**.
5. Log out of the ExtSRV FortiMail webmail GUI.
6. Return to the Thunderbird client, and then verify that you received the reply.
7. Close Thunderbird.

Review Log Entries

You will review the log entries for the emails to understand how FortiMail tracks policy usage.

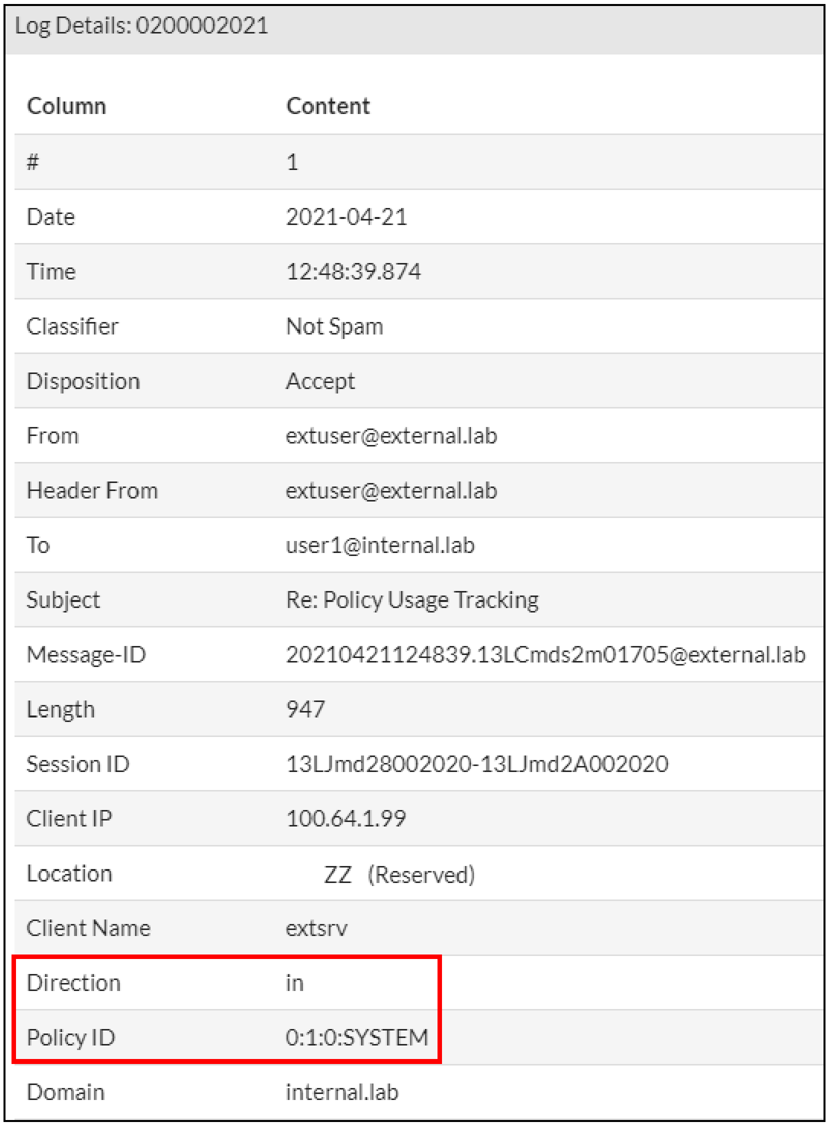
To review log entries

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Monitor** > **Log** > **History**.
   The first two entries in the **History** log should correspond to the two emails that FortiMail just processed.
3. Right-click the entry for the inbound email, and then select **View Details**.



2021-04-21 11:52:18 -> Current

#	Date	Time	Classifier	Disposition	From	Header From ...	To	Subject	Session ID
1	2021-04-21	12:48:39.874	Not Spam	Accept	extuser@exte...	extuser@exte...	user1@intern...	Re: Policy Usage Tracking	13LJmd28002020-13LJ...
2	2021-04-21	12:48:11.830	Not Spam	Accept	user1@intern...	user1@intern...	extuser@exte...	Policy Usage Tracking	13LJmB6d002016-13LJ...



Log Details: 0200002021

Column	Content
#	1
Date	2021-04-21
Time	12:48:39.874
Classifier	Not Spam
Disposition	Accept
From	extuser@external.lab
Header From	extuser@external.lab
To	user1@internal.lab
Subject	Re: Policy Usage Tracking
Message-ID	20210421124839.13LCmds2m01705@external.lab
Length	947
Session ID	13LJmd28002020-13LJmd2A002020
Client IP	100.64.1.99
Location	ZZ (Reserved)
Client Name	extsrv
Direction	in
Policy ID	0:1:0:SYSTEM
Domain	internal.lab

4. Review the **Policy IDs** field, and then answer the following questions:

   The **Policy IDs** field is made up of four fields (X:Y:Z:<recipient policy domain name or SYSTEM>). What does each field correspond to?

   The first policy ID value is **0**. What does this mean?

   The third policy ID value is **0**. What does this mean?

The policy IDs for each email are recorded in the history logs in the format of X:Y:Z:<recipient policy domain name or SYSTEM>, where X is the ID of the access control rule, Y is the ID of the IP-based policy, and Z is the ID of the recipient-based policy. The last field shows the domain name if it matches a recipient policy, and **SYSTEM** if it doesn't match a recipient policy.

If the value in the access control rule field for an 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 a policy or rule couldn’t be matched, or doesn’t exist.

5. Click **Close**.
6. Open the relevant log entry for the outbound email, and then review the **Policy IDs** field.

The policy ID recorded for the outbound email is **1:1:0:SYSTEM**. It was processed using access receive rule ID 1, which you created in the previous exercise. Then, the email was processed using the default IP policy ID 1. Because you didn’t configure an outbound recipient policy, the last field value is 0 and the domain is **SYSTEM**.

7. Log out of the IntGW FortiMail management GUI.

Exercise 4: Creating Policies

In this exercise, you will create IP and recipient policies. Then, you will test your configuration by sending emails back and forth. You will also use logs to observe the changes to the policy usage from the previous exercise.

Create an IP Policy

You will create an IP policy on IntGW FortiMail to process emails specifically from IntSRV FortiMail.

Take the Expert Challenge!

On IntGW FortiMail, create an IP policy that will process all outbound emails from IntSRV FortiMail (`10.0.1.99/32`).

Assign the **Outbound_Session** session profile to this IP policy.

Move this IP policy to the top of the list.

Leave all other settings at the default values.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

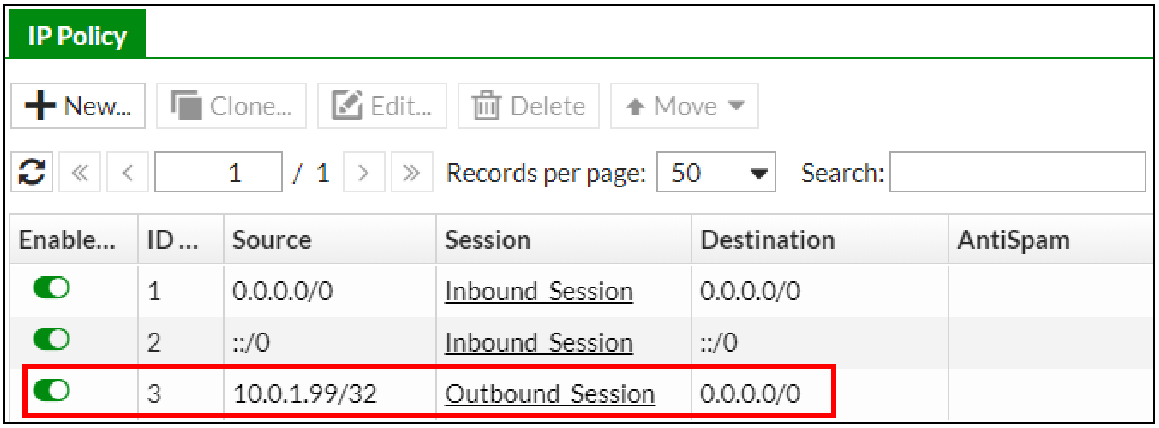
After you complete the challenge, see Create Recipient Policies on page 37.

To create an IP policy

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Policy** > **IP Policy** > **IP Policy**.
3. Click **New**.
4. Configure the following settings:

Field	Value
Source	10.0.1.99/32
Session	Outbound_Session

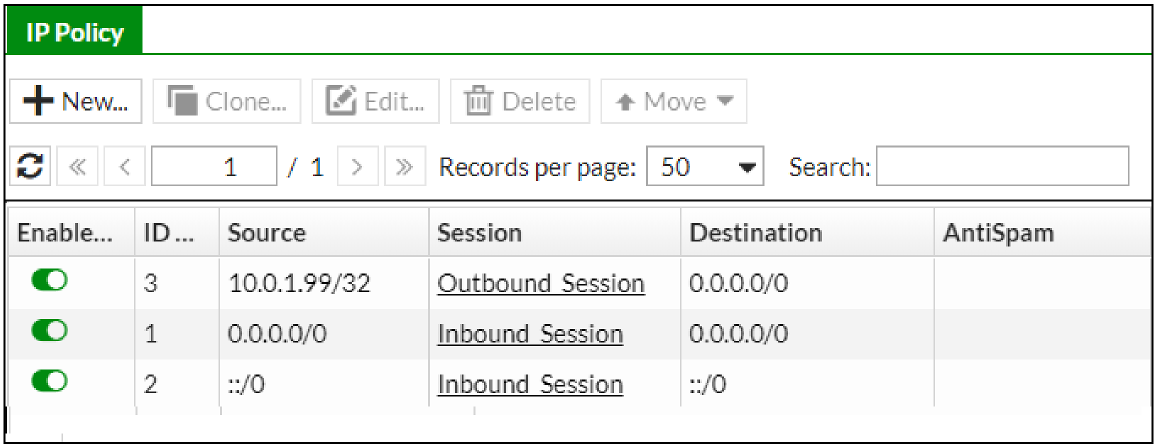
5. Click **Create**.
   The new policy should have an ID value of **3**.



Enable...	ID ...	Source	Session	Destination	AntiSpam
●	1	0.0.0.0/0	Inbound Session	0.0.0.0/0	
●	2	::/0	Inbound Session	::/0	
●	3	10.0.1.99/32	Outbound Session	0.0.0.0/0	

6. Click the policy to select it.
7. In the **Move** drop-down list, select **Before**.
8. In the **Move right before** drop-down list, select **1**.
9. Click **Move**.

   IP policy ID **3** moves to the top of the list. The policies should appear in the following order:



Enable...	ID ...	Source	Session	Destination	AntiSpam
●	3	10.0.1.99/32	Outbound Session	0.0.0.0/0	
●	1	0.0.0.0/0	Inbound Session	0.0.0.0/0	
●	2	::/0	Inbound Session	::/0	

IP policy ID **3** will process all emails sourced from IntSRV FortiMail (outgoing), and IP Policy ID **1** will process all other emails (incoming). IP policy ID **2** is a default IPv6 policy. Since this lab is not configured for IPv6, it is not required. You can delete the policy if you want.

Create Recipient Policies

You will create inbound and outbound recipient policies on IntGW FortiMail.

Take the Expert Challenge!

On IntGW FortiMail, create an inbound recipient policy for the `internal.lab` domain. Do not assign any inspection profiles to this policy.

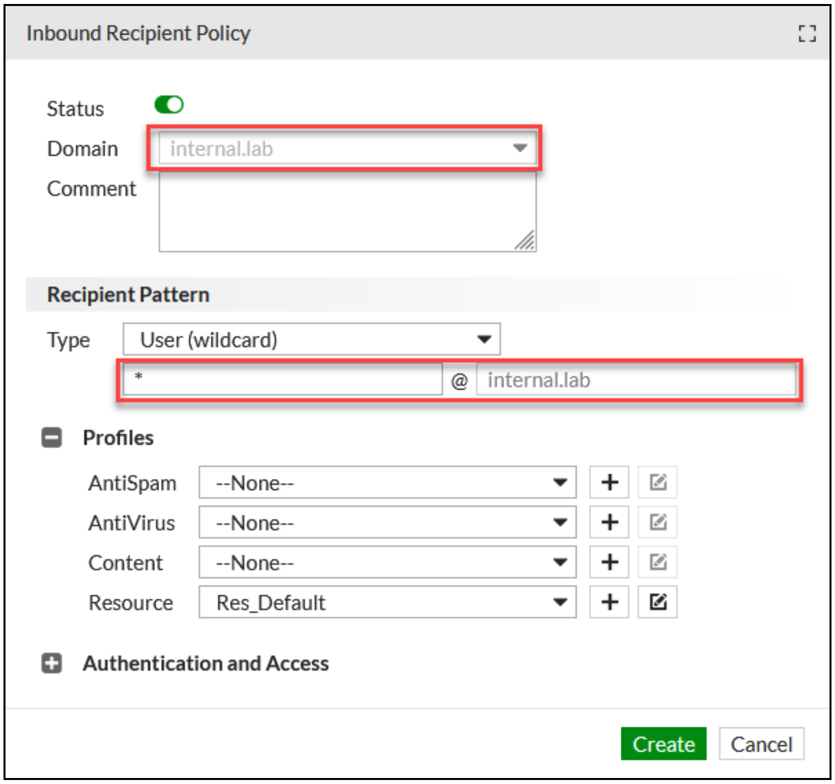
On IntGW FortiMail, create an outbound recipient policy for the `internal.lab` domain. Do not assign any inspection profiles to this policy.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Verify the Policy Configuration on page 39.

To create recipient policies

1. Continuing on the IntGW FortiMail management GUI, click **Policy** > **Recipient Policy** > **Inbound**.
2. In the **Domain** drop-down list, select `internal.lab`.
3. Click **New**.



Inbound Recipient Policy

Status: On
Domain: internal.lab
Comment:

Recipient Pattern

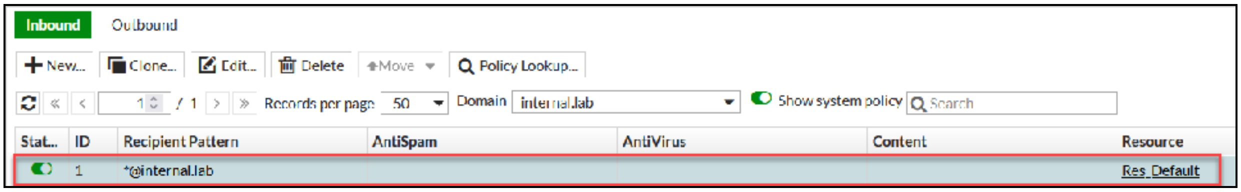
Type: User (wildcard)
* @ internal.lab

Profiles

AntiSpam: --None--
AntiVirus: --None--
Content: --None--
Resource: Res_Default

Authentication and Access

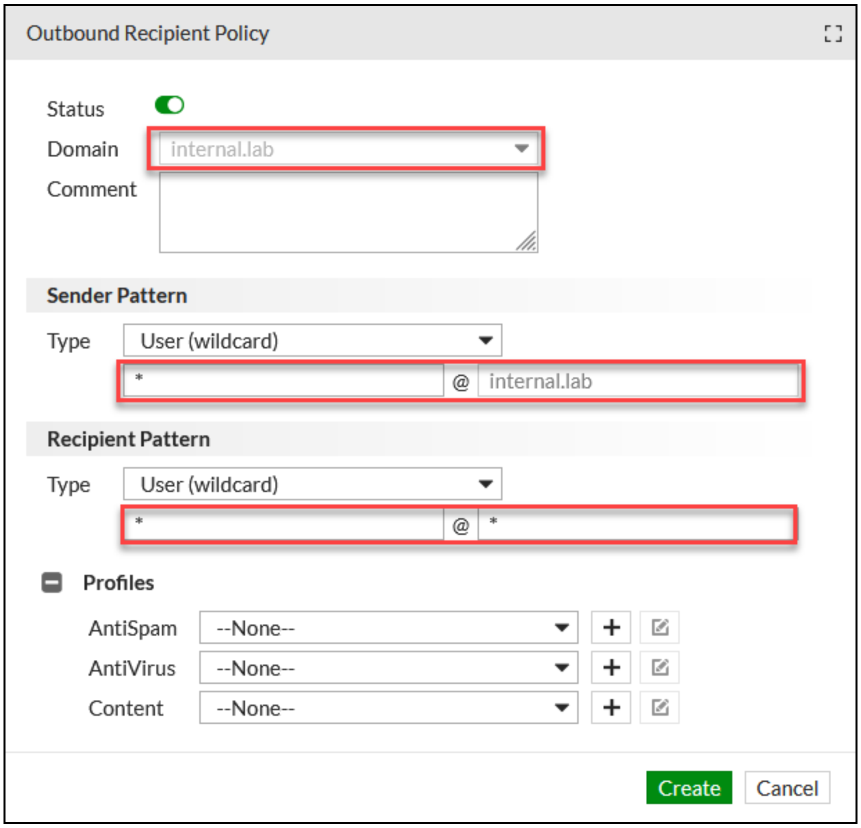
4. Click **Create**.
5. In the **Domain** drop-down list, select `All` or `internal.lab`—otherwise, you may not see the new policy.



Records per page: 50 Domain: internal.lab

Stat...	ID	Recipient Pattern	AntiSpam	AntiVirus	Content	Resource
●	1	*@internal.lab				Res_Default

6. Click **Policy** > **Recipient Policy** > **Outbound**.
7. In the **Domain** drop-down list, select `internal.lab`.
8. Click **New**.



Outbound Recipient Policy

Status: ●
Domain: internal.lab
Comment:

Sender Pattern

Type: User (wildcard)
* @ internal.lab

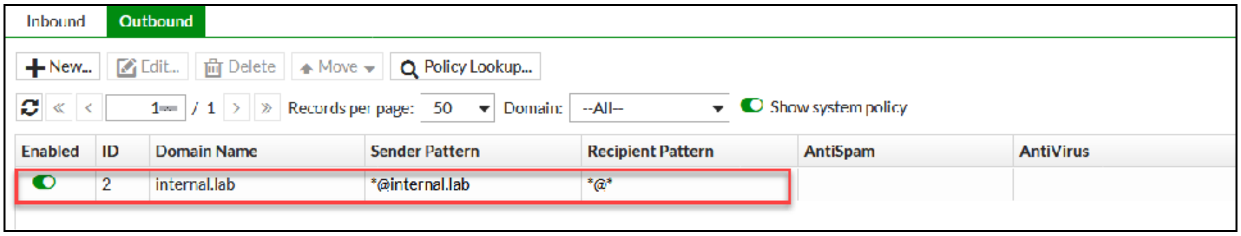
Recipient Pattern

Type: User (wildcard)
* @ *

Profiles

AntiSpam: --None--
AntiVirus: --None--
Content: --None--

9. Click **Create**.
10. In the **Domain** drop-down list, select `All` or `internal.lab`—otherwise, you may not see the new policy.



Records per page: 50 Domain: --All-- Show system policy

Enabled	ID	Domain Name	Sender Pattern	Recipient Pattern	AntiSpam	AntiVirus
●	2	internal.lab	*@internal.lab	*@*		

Verify the Policy Configuration

You will verify your policy configuration by sending an email from an `internal.lab` user, and then replying to that email from an `external.lab` user. After, you will review the generated log entries.

To verify the policy configuration

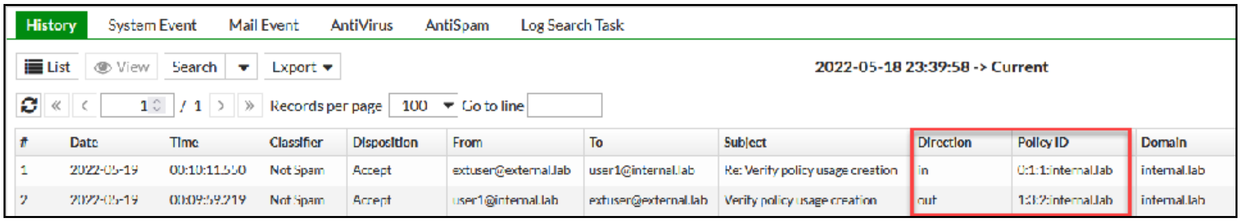
1. On the Linux-Client VM, open Thunderbird, and then compose a new email to `extuser@external.lab`.
2. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
3. Open the new email, and then click **Reply**.

4. In the message body, type a reply, and then click **Send**.
5. Log out of the ExtSRV FortiMail webmail GUI.
6. Return to the Thunderbird client, and then verify that you received the reply.
7. Close Thunderbird.

To review log entries

1. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.
2. Review the first two entries in the **History** logs.

   These two log entries should correspond to the two emails that FortiMail just processed.



2022-05-18 23:39:58 -> Current

#	Date	Time	Classifier	Disposition	From	To	Subject	Direction	Policy ID	Domain
1	2022-05-19	00:10:11.550	Not Spam	Accept	extuser@external.lab	user1@internal.lab	Re: Verify policy usage creation	in	0:1:1:internal.lab	internal.lab
2	2022-05-19	00:09:59.219	Not Spam	Accept	user1@internal.lab	extuser@external.lab	Verify policy usage creation	out	1:3:2:internal.lab	internal.lab

3. Review the **Policy ID** field for each log entry.

   What changes can you see from the previous lab exercise?

The policy usage reflects the new ID values for the policies you created. All outgoing emails are processed by IP policy ID 3 and outgoing recipient policy ID 2. All incoming emails are processed by IP policy ID 1 and incoming recipient policy ID 1.

4. Log out of the IntGW FortiMail management GUI.

Lab 3: Authentication

In this lab, you will configure access receive rules to enforce user SMTP authentication. You will also configure an LDAP profile to enable recipient verification, alias mapping, and user authentication. Finally, you will configure the authentication reputation feature to block an SMTP brute force attack.

Objectives

- Enforce user SMTP authentication using access receive rules
- Configure an LDAP profile
- Enable recipient verification and alias mapping
- Configure LDAP authentication for users
- Block SMTP brute force attacks

Time to Complete

Estimated: 60 minutes

Exercise 1: Enforcing User Authentication

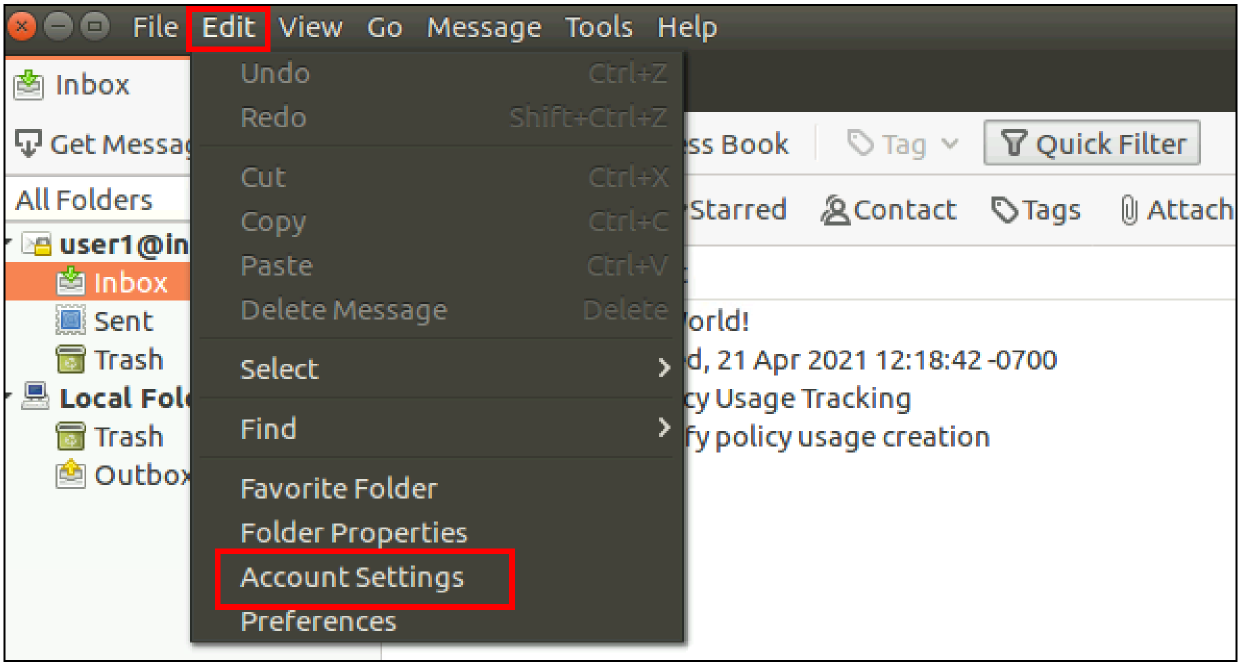
In this exercise, you will explore how FortiMail handles SMTP authentication. You will enforce authentication using access receive rules, and test your configuration using various outgoing server settings in Mozilla Thunderbird.

Disable SMTP Authentication

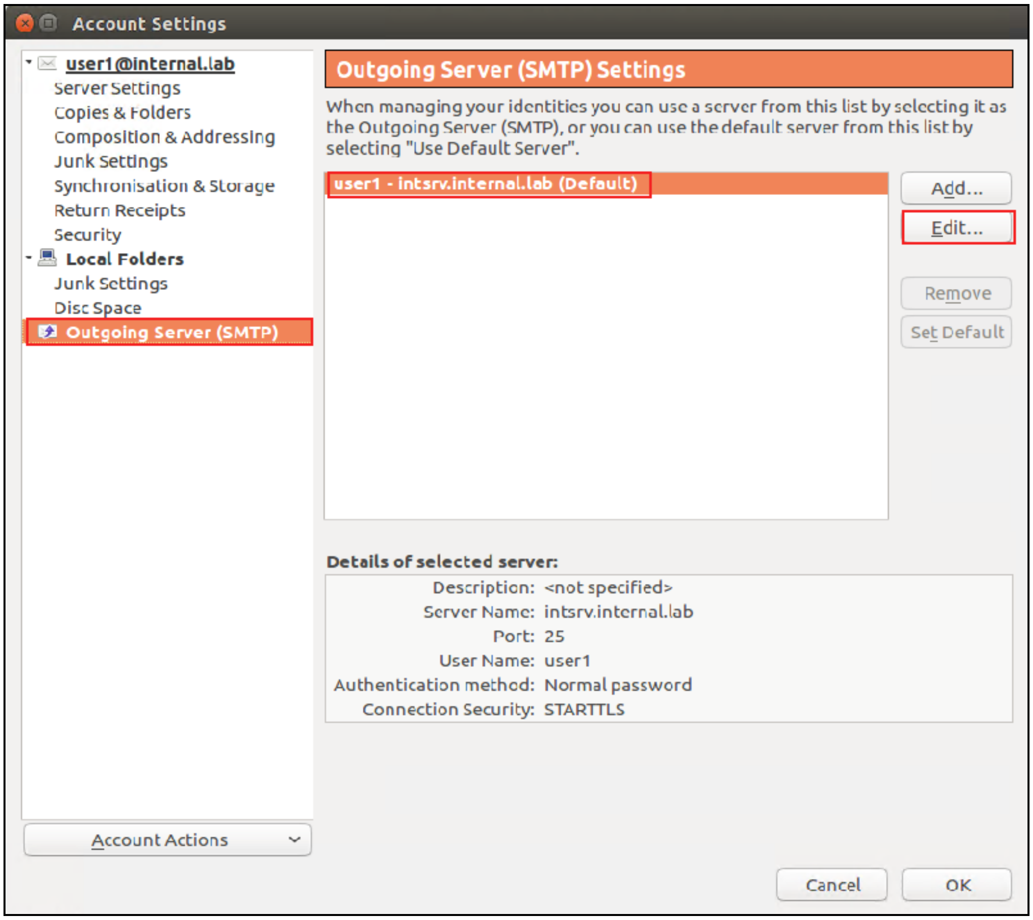
On the Thunderbird client, you previously configured SMTP authentication with a **Normal password**. Now, you will change that authentication method to use no authentication, and then attempt to send an unauthenticated outbound email.

To disable SMTP authentication

1. On the Linux-Client VM, open Thunderbird.
2. Click **Edit** > **Account Settings**.



3. In the **Account Settings** window, in the left pane, click **Outgoing Server (SMTP)**, and then click **Edit**.



Outgoing Server (SMTP) Settings

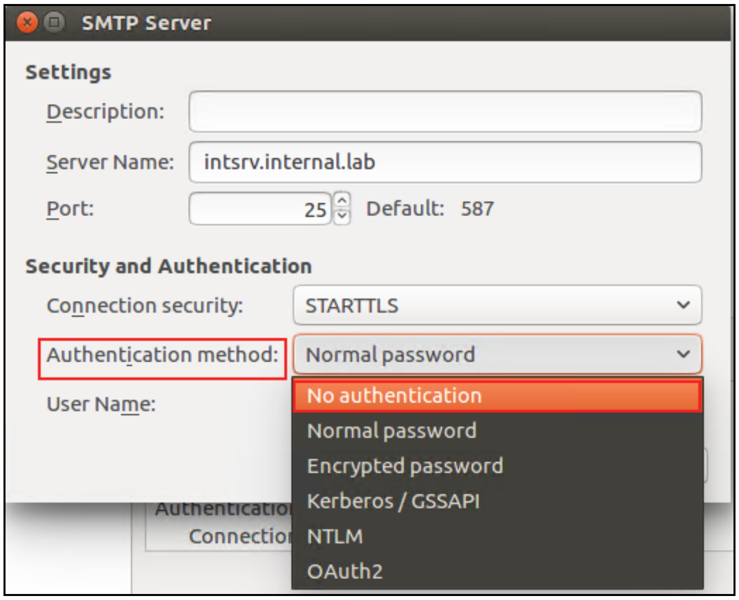
When managing your identities you can use a server from this list by selecting it as the Outgoing Server (SMTP), or you can use the default server from this list by selecting "Use Default Server".

user1 - intsrv.internal.lab (Default)

Details of selected server:

Description: <not specified>
Server Name: intsrv.internal.lab
Port: 25
User Name: user1
Authentication method: Normal password
Connection Security: STARTTLS

4. In the **Authentication method** drop-down list, select **No authentication**.



Settings

Description:
Server Name: intsrv.internal.lab
Port: 25 Default: 587

Security and Authentication

Connection security: STARTTLS
Authentication method: Normal password
User Name:

5. Click **OK**.
6. Click **OK**.

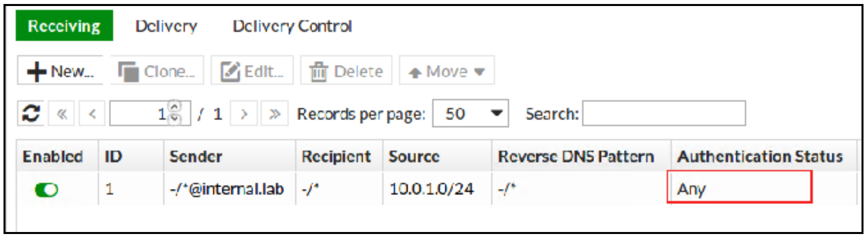
By making these changes, you disabled authentication for SMTP connections. Therefore, when you send an email, Thunderbird won't authenticate to the outgoing SMTP server.

To send an unauthenticated email

1. Continuing on Thunderbird, compose a new email, and then send it to `extuser@external.lab`.
2. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.

   Why was the email delivered to the destination user even though you disabled SMTP authentication in Thunderbird?

The access receive rule that you configured in the previous lab didn't have authentication enforcement enabled.



Enabled	ID	Sender	Recipient	Source	Reverse DNS Pattern	Authentication Status
●	1	-/*@internal.lab	-/*	10.0.1.0/24	-/*	Any

When you set **Authentication Status** to **Any**, FortiMail doesn't verify whether the sender matching the rule is authenticated or not.

Enforce Authentication

You will reconfigure the access control rule on IntSRV FortiMail to enforce authentication.

Take the Expert Challenge!

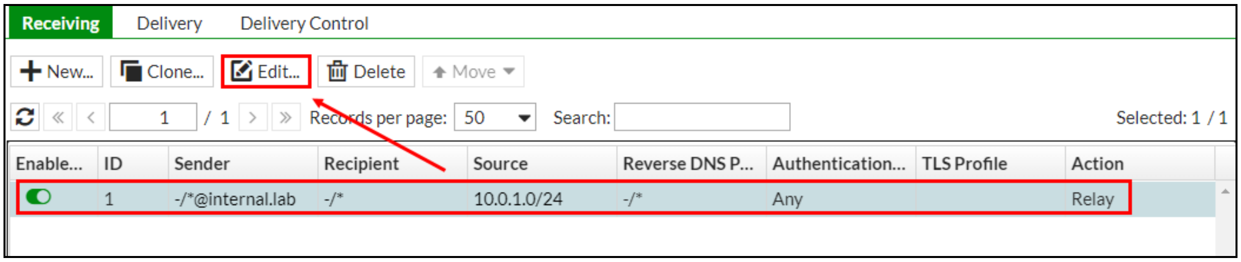
On IntSRV FortiMail, modify the access control receive rule to enforce SMTP authentication for all `internal.lab` users.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Verify Authentication Enforcement on page 45.

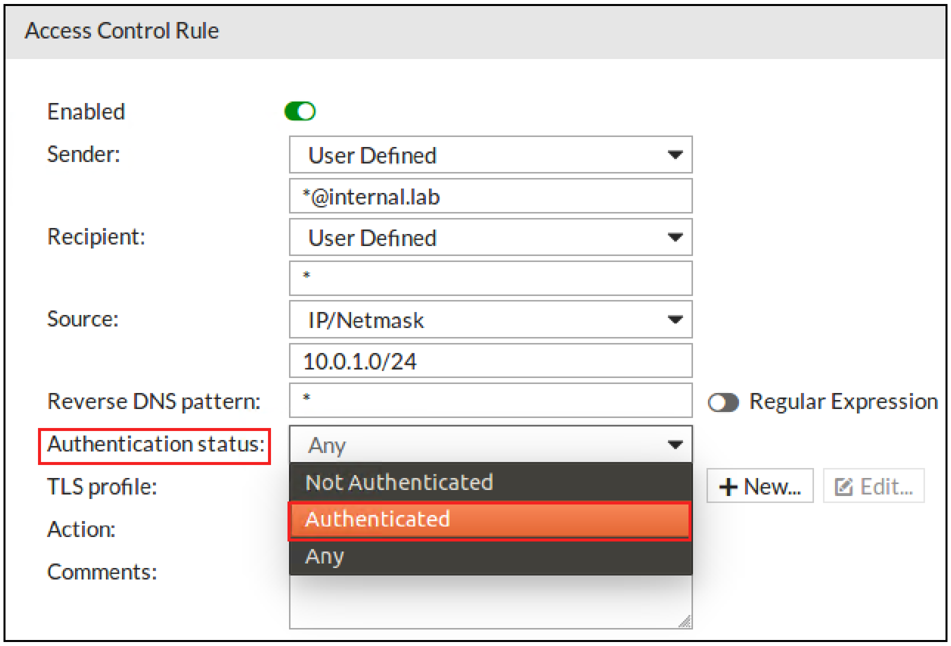
To enforce authentication

1. On the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Policy** > **Access Control** > **Receiving**.
3. Select rule ID **1**, and then click **Edit**.



Enable...	ID	Sender	Recipient	Source	Reverse DNS P...	Authentication...	TLS Profile	Action
●	1	-/*@internal.lab	-/*	10.0.1.0/24	-/*	Any		Relay

4. In the **Authentication status** drop-down list, select **Authenticated**.


Access Control Rule

Enabled	●
Sender:	User Defined *@internal.lab
Recipient:	User Defined *
Source:	IP/Netmask 10.0.1.0/24
Reverse DNS pattern:	* ○ Regular Expression
Authentication status:	Any
TLS profile:	
Action:	
Comments:	

5. Click **OK** to save the changes.

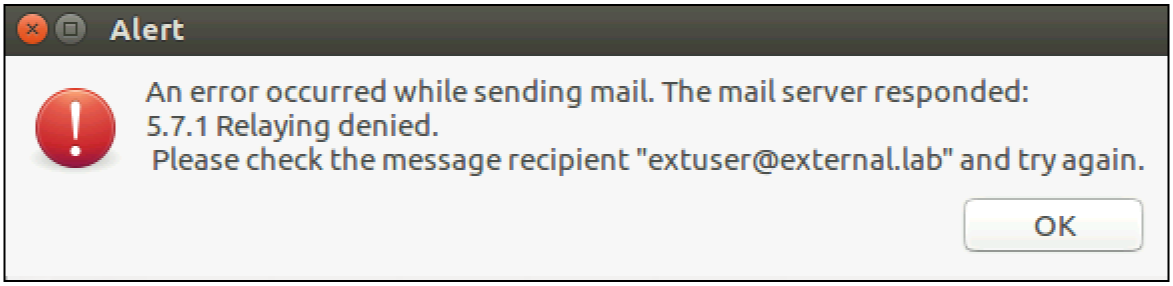
Verify Authentication Enforcement

You will verify authentication enforcement by sending an email from a user in the `internal.lab` domain to a user in the `external.lab` domain.

To verify authentication enforcement

1. Return to the Linux-Client VM, compose a new email, and then send it to `extuser@external.lab`.

   An alert appears indicating that relaying is denied.

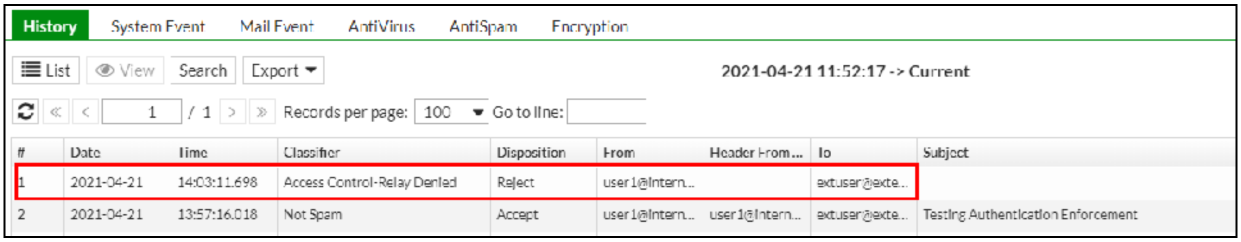


Alert

An error occurred while sending mail. The mail server responded:
5.7.1 Relaying denied.
Please check the message recipient "extuser@external.lab" and try again.

2. Click **OK**.
3. Return to the IntSRV FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

   The first entry in the **History** log should correspond to the rejected email.



2021-04-21 11:52:17 -> Current

Records per page: 100 Go to line:

#	Date	Time	Classifier	Disposition	From	Header From ...	To	Subject
1	2021-04-21	14:03:11.698	Access Control-Relay Denied	Reject	user1@intern...		extuser@exte...	
2	2021-04-21	13:57:16.018	Not Spam	Accept	user1@intern...	user1@intern...	extuser@exte...	Testing Authentication Enforcement

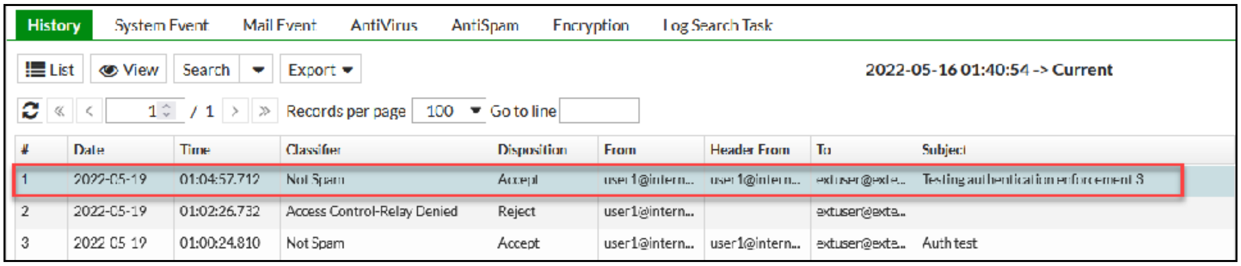
In this log entry, you can see that IntSRV FortiMail has the **Disposition** of **Reject**. By changing the authentication status setting, you successfully enforced authentication for users connecting to IntSRV FortiMail.

Restore SMTP Authentication on Thunderbird

You will restore SMTP authentication on Thunderbird, so you can continue sending emails through FortiMail.

To restore SMTP authentication on Thunderbird

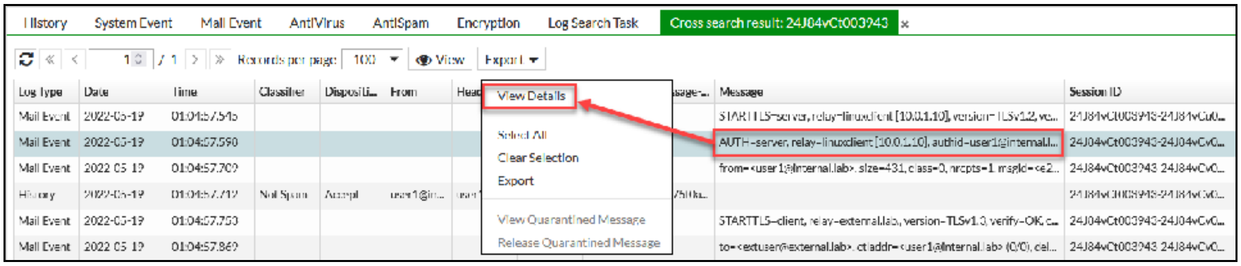
1. Return to the Thunderbird client, and then click **Edit** > **Account Settings**.
2. On the **Account Settings** page, click **Outgoing Server (SMTP)**, and then click **Edit**.
3. In the **Authentication method** drop-down list, select **Normal password**.
4. Click **OK**.
5. Click **OK**.
6. Send another email to `extuser@external.lab`.
7. Close Thunderbird.
8. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
9. Verify that the email was delivered.
10. Log out of the ExtSRV FortiMail webmail GUI.
11. Return to the IntSRV FortiMail management GUI, and then click **Monitor** > **Log** > **History**.
    The first entry in the **History** log should correspond to the email you just sent.



2022-05-16 01:40:54 -> Current

#	Date	Time	Classifier	Disposition	From	Header From	To	Subject
1	2022-05-19	01:04:57.712	Not Spam	Accept	user1@intern...	user1@intern...	extuser@exte...	Testing authentication enforcement 3
2	2022-05-19	01:02:26.732	Access Control-Relay Denied	Reject	user1@intern...		extuser@exte...	
3	2022 05 19	01:00:24.810	Not Spam	Accept	user1@intern...	user1@intern...	extuser@exte...	Auth test

12. Click the **Session ID** link to retrieve the cross-search results.
13. Right-click the event log related to the authentication event to view the details.



Log Type	Date	Time	Classifier	Dispositi...	From	Head...	...sage-...	Message	Session ID
Mail Event	2022-05-19	01:04:57.545						STARTTLS=server, relay=linuxclient [10.0.1.10], version=TLSv1.2, ve...	24J04vCt003943-24J04vCv0...
Mail Event	2022-05-19	01:04:57.590						AUTH=server, relay=linuxclient [10.0.1.10], authid=user1@internal.l...	24J04vCt003943-24J04vCv0...
Mail Event	2022 05 19	01:04:57.709						from=<user1@internal.lab>, size=431, class=0, nrcpts=1 msgid=<e2...	24J04vCt003943 24J04vCv0...
History	2022-05-19	01:04:57.712	Not Spam	Accept	user1@in...	user1	750 ka...		24J04vCt003943-24J04vCv0...
Mail Event	2022-05-19	01:04:57.753						STARTTLS=client, relay=external.lab, version=TLSv1.3, verify=OK, c...	24J04vCt003943-24J04vCv0...
Mail Event	2022 05 19	01:04:57.869						to=<extuser@external.lab>, ctladdr=<user1@internal.lab> (0/0), del...	24J04vCt003943 24J04vCv0...

14. In the **Log Details** window, review the **Message** field.
15. Click **Close**.
16. Log out of the IntSRV FortiMail management GUI.

Exercise 2: Integrating LDAP

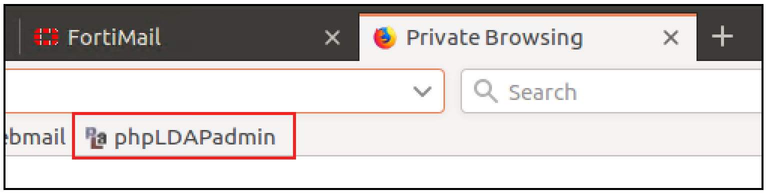
The Linux-Client VM has been preconfigured with OpenLDAP for the `internal.lab` domain. In this exercise, you will review the OpenLDAP configuration and learn how to retrieve LDAP attributes for OpenLDAP objects. Then, you will configure an LDAP profile on both IntSRV FortiMail and IntGW FortiMail for user authentication, alias lookup, and recipient verification.

Review the OpenLDAP Configuration

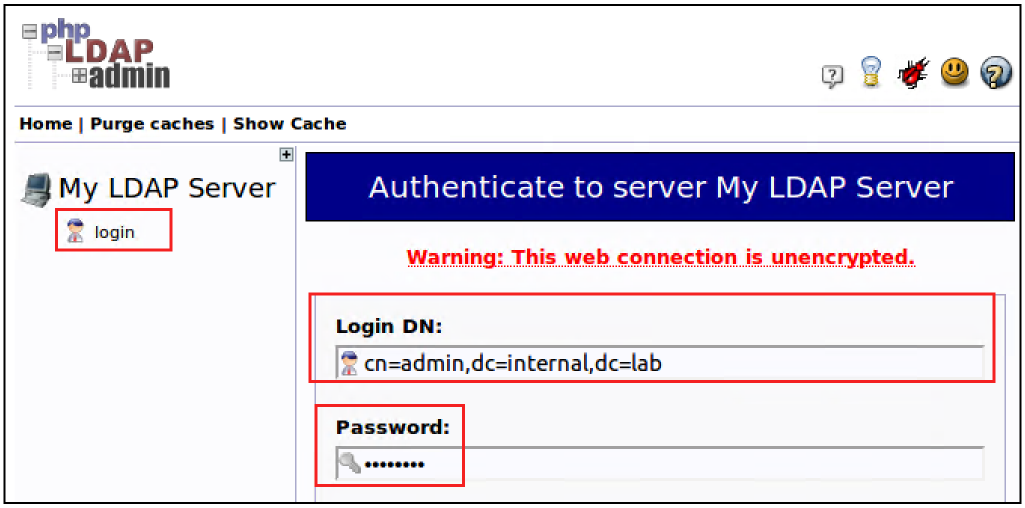
You will review the OpenLDAP configuration and familiarize yourself with the users and groups that have been preconfigured on the Linux-Client VM.

To review the OpenLDAP configuration

1. On the Linux-Client VM, open Mozilla Firefox, and then click the **phpLDAPadmin** bookmark.



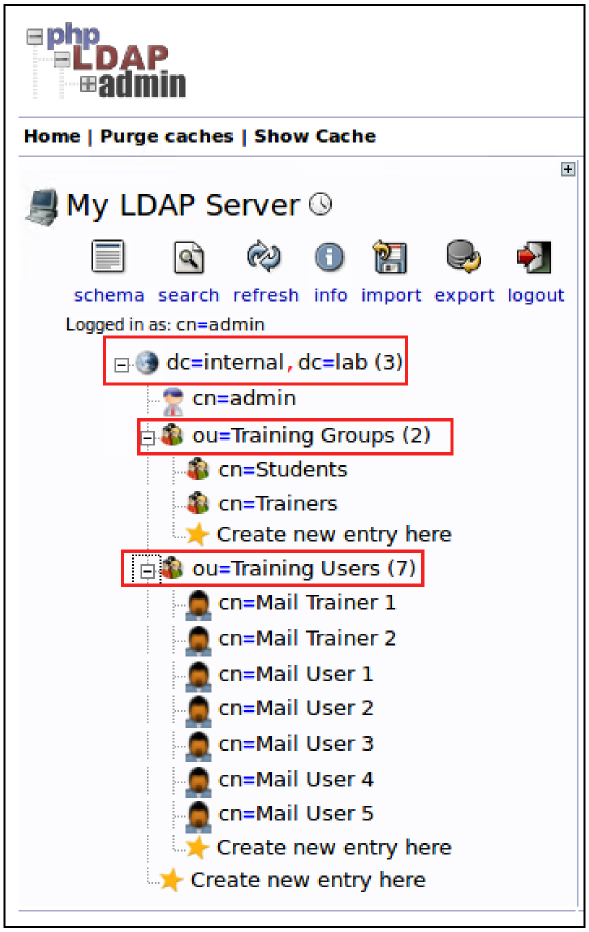
2. Click **login**.
3. Log in using the **Login DN** `cn=admin,dc=internal,dc=lab` and **Password** `password`.


phpLDAPadmin
Home | Purge caches | Show Cache
My LDAP Server
login
Authenticate to server My LDAP Server
Warning: This web connection is unencrypted.

Login DN: cn=admin,dc=internal,dc=lab

Password: ••••••••

4. Click **Authenticate**.
5. Expand the LDAP tree.
6. Expand **Training Groups**.
7. Expand **Training Users**.



Logged in as: cn=admin

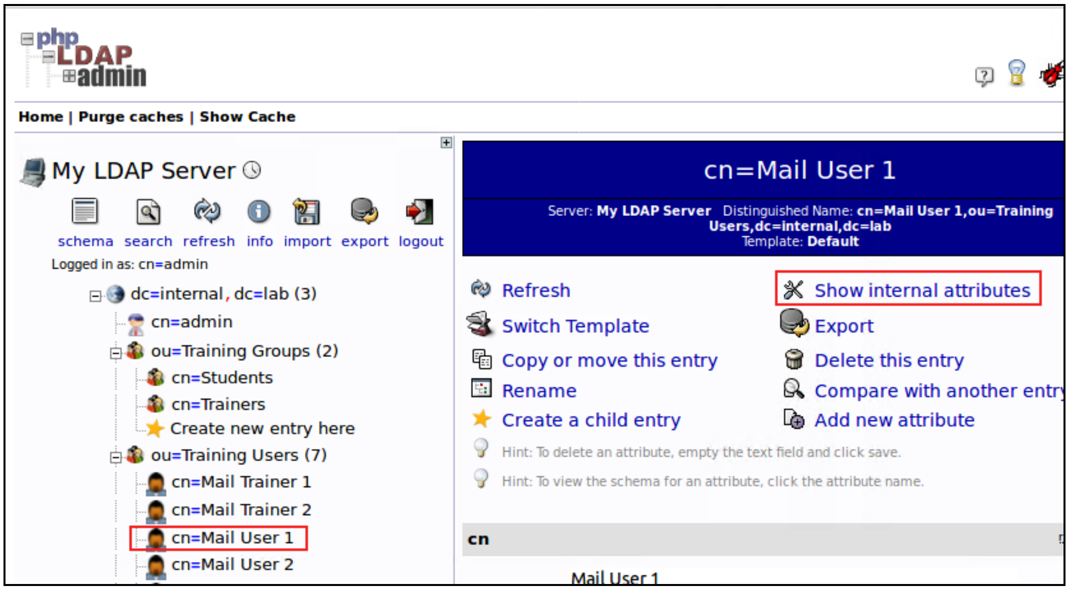
- dc=internal, dc=lab (3)
  - cn=admin
  - ou=Training Groups (2)
    - cn=Students
    - cn=Trainers
    - Create new entry here
  - ou=Training Users (7)
    - cn=Mail Trainer 1
    - cn=Mail Trainer 2
    - cn=Mail User 1
    - cn=Mail User 2
    - cn=Mail User 3
    - cn=Mail User 4
    - cn=Mail User 5
    - Create new entry here
  - Create new entry here

The users and groups are located in the **Training Users** OU and **Training Groups** OU respectively. All account passwords are set to `fortinet`.

To access the LDAP attributes of OpenLDAP objects

1. Click **cn=Mail User 1**.
2. Click **Show internal attributes**.

   You can see the attributes configured for **user1**, such as dn, cn, email, alias, and so on.



Logged in as: cn=admin

- dc=internal, dc=lab (3)
  - cn=admin
  - ou=Training Groups (2)
    - cn=Students
    - cn=Trainers
    - Create new entry here
  - ou=Training Users (7)
    - cn=Mail Trainer 1
    - cn=Mail Trainer 2
    - cn=Mail User 1
    - cn=Mail User 2

cn=Mail User 1

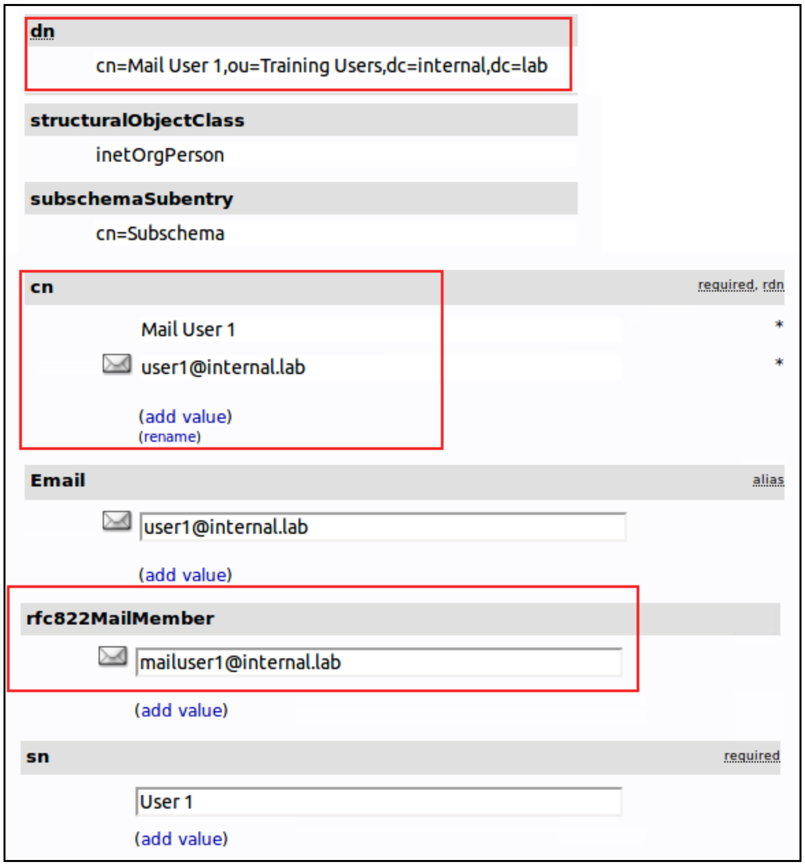
Server: **My LDAP Server** Distinguished Name: **cn=Mail User 1,ou=Training Users,dc=internal,dc=lab**
Template: **Default**

Hint: To delete an attribute, empty the text field and click save.

Hint: To view the schema for an attribute, click the attribute name.

cn

Mail User 1



dn
cn=Mail User 1,ou=Training Users,dc=internal,dc=lab

structuralObjectClass
inetOrgPerson

subschemaSubentry
cn=Subschema

cn required, rdn
Mail User 1 *
user1@internal.lab *
(add value)
(rename)

Email alias
user1@internal.lab
(add value)

rfc822MailMember
mailuser1@internal.lab
(add value)

sn required
User 1
(add value)

Do not make any changes to the OpenLDAP configuration!

3. Close Firefox.

Configure an LDAP Profile on IntGW and IntSRV FortiMail

You will configure an LDAP profile on the IntGW and IntSRV FortiMail. The LDAP profile will contain the necessary queries that FortiMail can use with an OpenLDAP server. You will configure the same LDAP profile on both IntSRV FortiMail and IntGW FortiMail.

To configure an LDAP profile on IntGW FortiMail

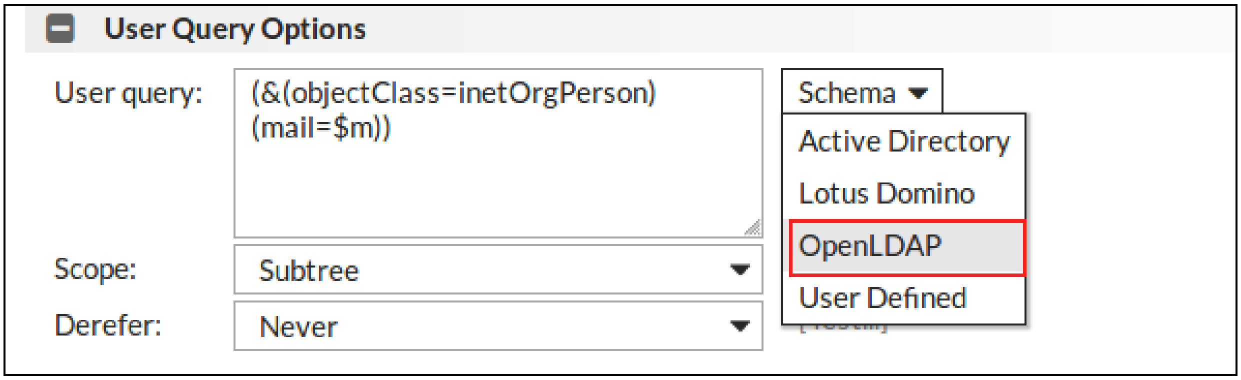
1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Profile** > **LDAP** > **LDAP**.
3. Click **New**.
4. Create an LDAP profile using the following values:

Field	Value
Profile name	InternalLabLDAP
Server name/IP	10.0.1.10

5. Use the following values to configure the **Default Bind Options**:

Field	Value
Base DN	OU=Training Users,DC=internal,DC=lab
Bind DN	CN=admin,DC=internal,DC=lab
Bind password	password

6. Expand the **User Query Options** section, and then in the **Schema** drop-down list, select **OpenLDAP**.



User Query Options

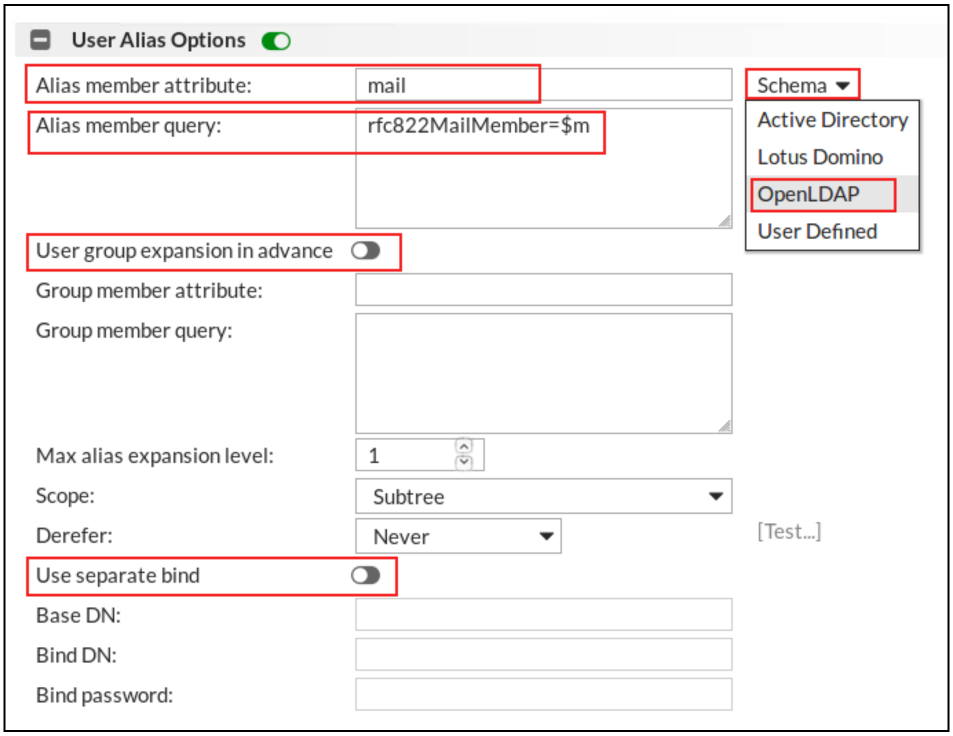
User query: (&(objectClass=inetOrgPerson)(mail=$m))

Scope: Subtree

Derefer: Never

7. Expand the **User Alias Options** section, and then in the **Schema** drop-down list, select **OpenLDAP**.
8. Use the following values to modify the **User Alias Options** settings:

Field	Value
Alias member attribute	mail
Alias member query	rfc822MailMember=$m
User group expansion in advance	Disabled
Use separate bind	Disabled



User Alias Options

Alias member attribute: mail

Alias member query: rfc822MailMember=$m

User group expansion in advance

Group member attribute:

Group member query:

Max alias expansion level: 1

Scope: Subtree

Derefer: Never

Use separate bind

Base DN:

Bind DN:

Bind password:

9. Click **Create**.

To configure an LDAP profile on IntSRV FortiMail

1. On the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Profile** > **LDAP** > **LDAP**.
3. Click **New**.
4. Create an LDAP profile using the following values:

Field	Value
Profile name	InternalLabLDAP
Server name/IP	10.0.1.10

5. Use the following values to configure the **Default Bind Options**:

Field	Value
Base DN	OU=Training Users,DC=internal,DC=lab
Bind DN	CN=admin,DC=internal,DC=lab
Bind password	password

6. In the **User Query Options** section, in the **Schema** drop-down list, select **OpenLDAP**.
7. In the **User Alias Options** section, in the **Schema** drop-down list, select **OpenLDAP**.
8. Use the following values to modify the **User Alias Options**:

Field	Value
Alias member attribute	mail
Alias member query	rfc822MailMember=$m
User group expansion in advance	Disabled
Use separate bind	Disabled

9. Click **Create**.

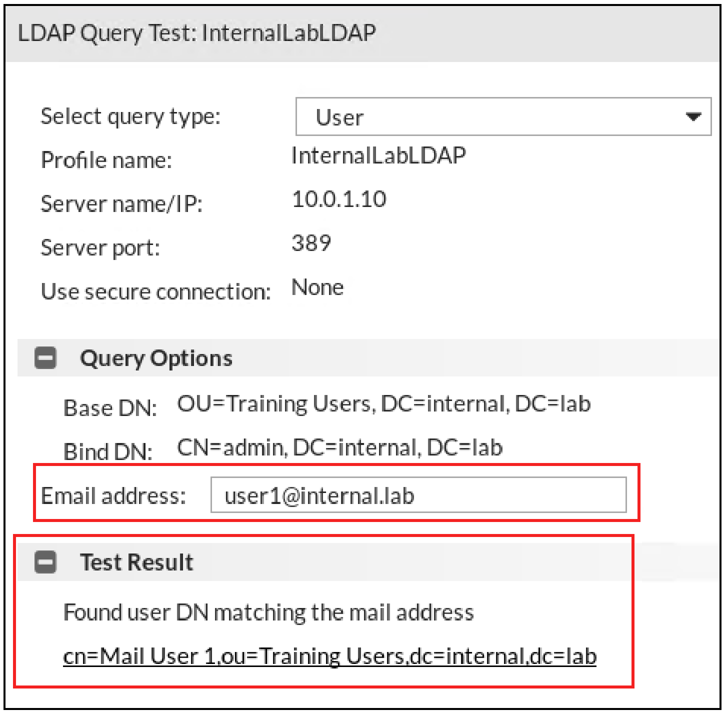
Validate the LDAP Profile Configuration

You will validate the LDAP profile that you created to ensure that the configuration is correct and the OpenLDAP server responds to user queries.

To validate the LDAP profile configuration

1. Continuing on the IntGW FortiMail management GUI, select the **InternalLabLDAP** profile, and then click **Edit**.
2. Click **Test LDAP Query**.
3. Verify that **Select query type** is **User**.
4. In the **Email address** field, type `user1@internal.lab`.
5. Click **Test**.

   If your configuration is correct, you will see the following message in the **Test Result** section:



LDAP Query Test: InternalLabLDAP

Select query type: User

Profile name: InternalLabLDAP

Server name/IP: 10.0.1.10

Server port: 389

Use secure connection: None

Query Options

Base DN: OU=Training Users, DC=internal, DC=lab

Bind DN: CN=admin, DC=internal, DC=lab

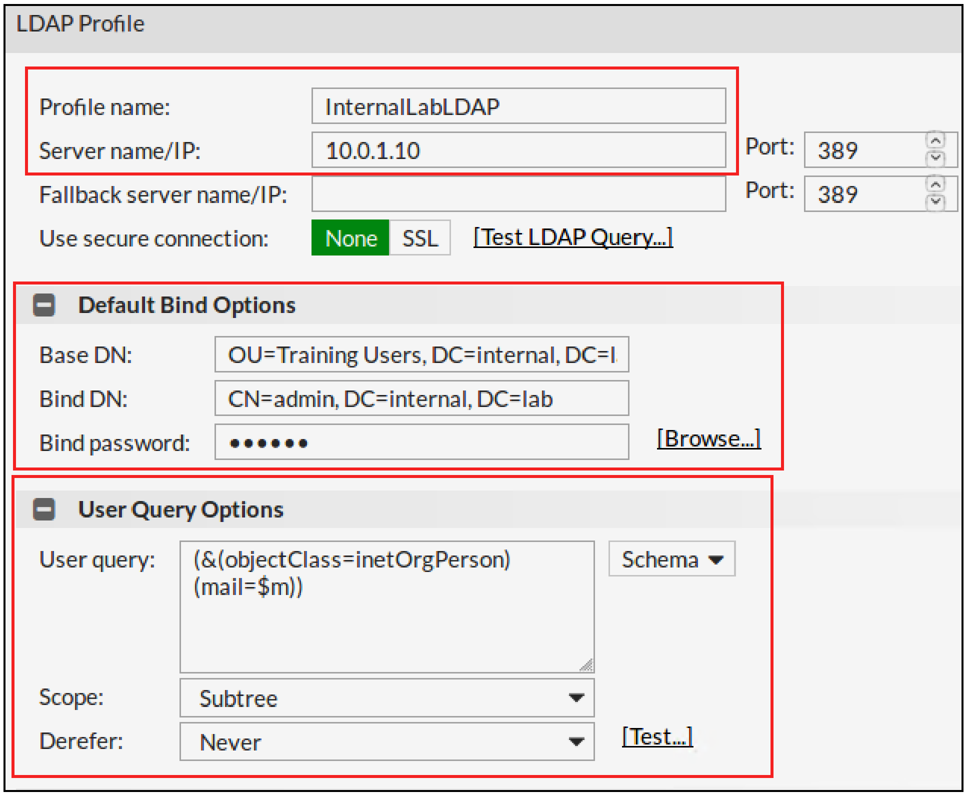
Email address: user1@internal.lab

Test Result

Found user DN matching the mail address

cn=Mail User 1,ou=Training Users,dc=internal,dc=lab

6. If the query fails, make sure that the LDAP profile configuration matches the following example:



LDAP Profile

Profile name: InternalLabLDAP

Server name/IP: 10.0.1.10 Port: 389

Fallback server name/IP: Port: 389

Use secure connection: None SSL [Test LDAP Query...]

Default Bind Options

Base DN: OU=Training Users, DC=internal, DC=l

Bind DN: CN=admin, DC=internal, DC=lab

Bind password: •••••• [Browse...]

User Query Options

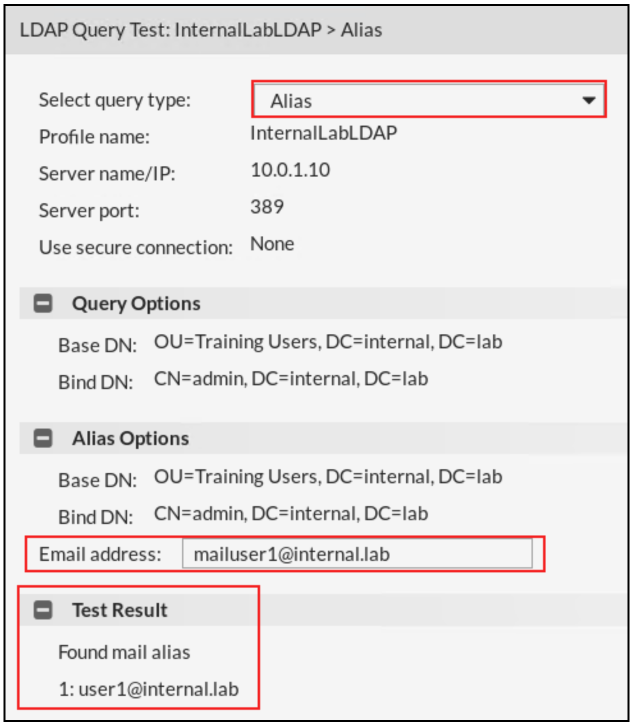
User query: (&(objectClass=inetOrgPerson)(mail=$m)) Schema

Scope: Subtree

Derefer: Never [Test...]

7. In the **Select query type** drop-down list, select **Alias**.
8. In the **Email address** field, type `mailuser1@internal.lab`.
9. Click **Test**.

If your configuration is correct, you will see the following message in the **Test Result** section:



LDAP Query Test: InternalLabLDAP > Alias

Select query type: Alias

Profile name: InternalLabLDAP

Server name/IP: 10.0.1.10

Server port: 389

Use secure connection: None

Query Options

Base DN: OU=Training Users, DC=internal, DC=lab

Bind DN: CN=admin, DC=internal, DC=lab

Alias Options

Base DN: OU=Training Users, DC=internal, DC=lab

Bind DN: CN=admin, DC=internal, DC=lab

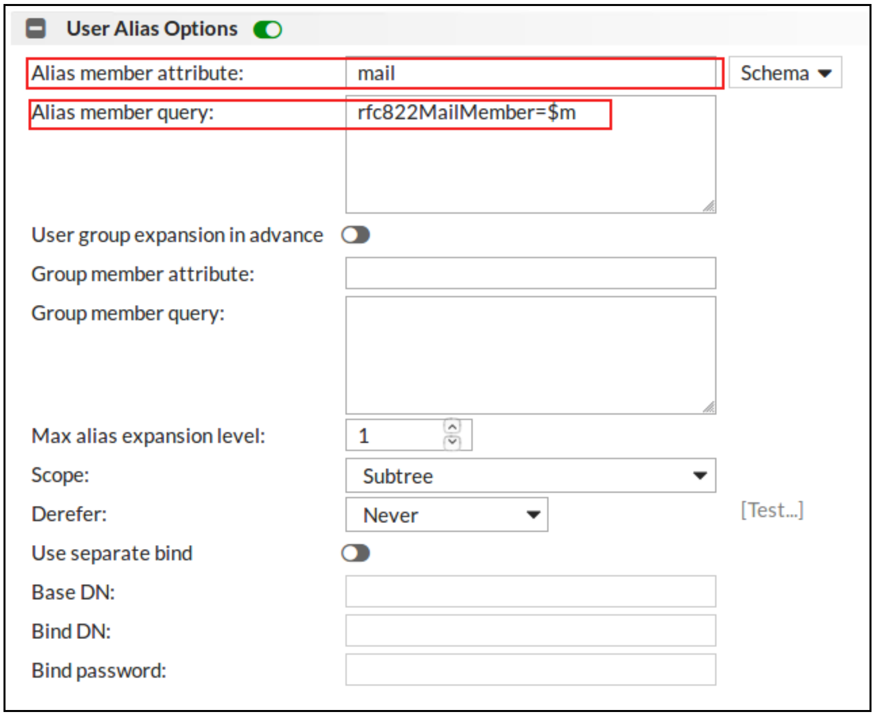
Email address: mailuser1@internal.lab

Test Result

Found mail alias

1: user1@internal.lab

10. If the query fails, make sure that the configuration of the **User Alias Options** LDAP profile matches the following example:



User Alias Options

Alias member attribute: mail

Alias member query: rfc822MailMember=$m

User group expansion in advance

Group member attribute:

Group member query:

Max alias expansion level: 1

Scope: Subtree

Derefer: Never

Use separate bind

Base DN:

Bind DN:

Bind password:

11. Perform the same validation steps on IntSRV FortiMail.

Configure Recipient Address Verification and Alias Mapping

Now that you configured an LDAP profile, you will configure recipient address verification and alias mapping. You will make these configuration changes on IntGW FortiMail because it is the first MTA hop that will process all emails for the `internal.lab` domain.

Take the Expert Challenge!

On IntGW FortiMail, configure recipient address verification and alias mapping using the **InternalLABLDAP** profile.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure LDAP Authentication for Gateway Mode Webmail Access on page 57.

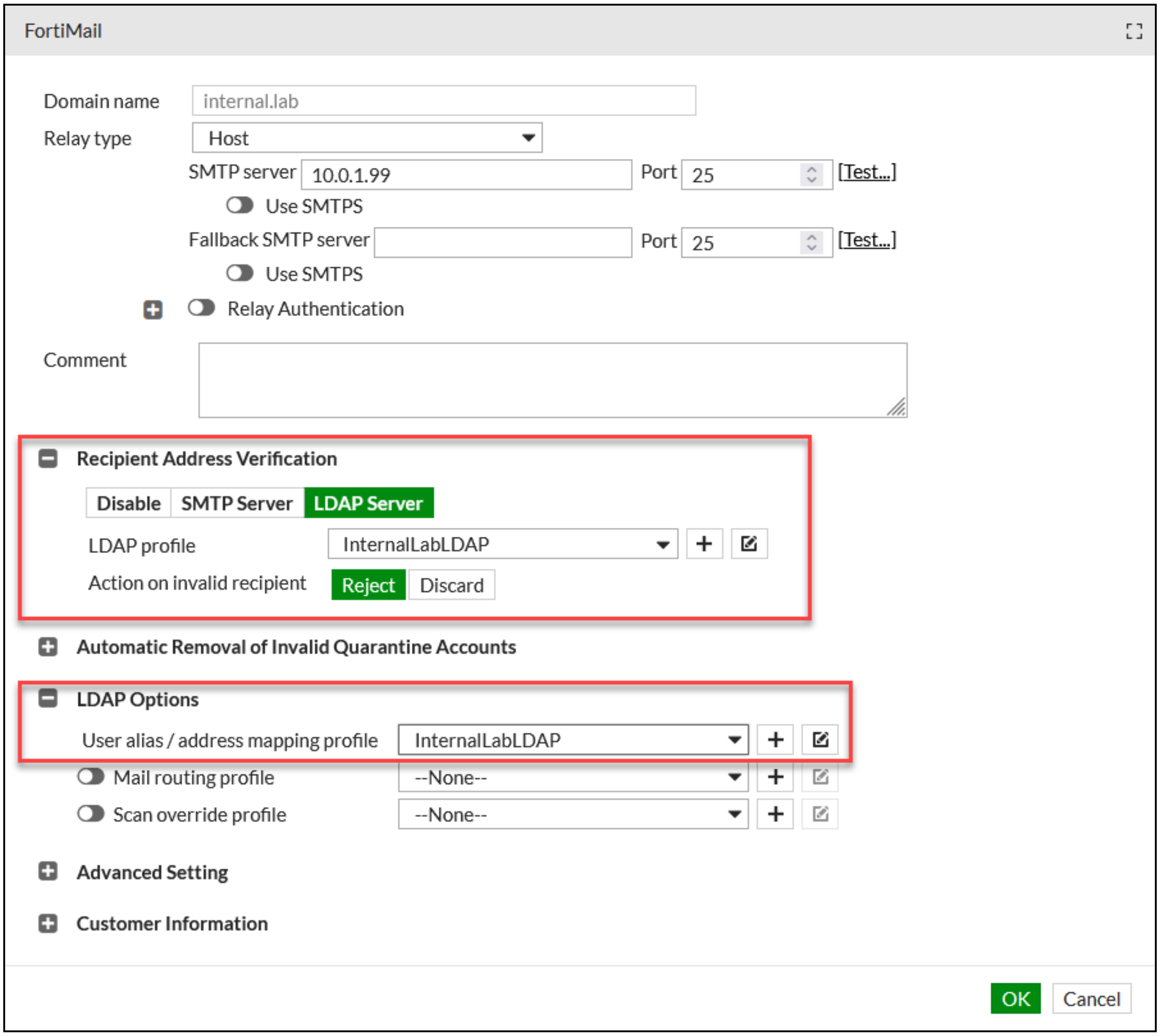
To configure recipient verification and alias mapping for gateway mode

1. Return to the IntGW FortiMail management GUI, and then click **Domain & User** > **Domain** > **Domain.**
2. Select the **internal.lab** domain, and then click **Edit.**
3. In the **Recipient Address Verification** section, click **LDAP Server**.
4. In the **LDAP profile** drop-down list, select **InternalLabLDAP**.
5. Expand the **LDAP Options** section.

If the **LDAP Options** section does not appear in the domain settings, switch to the advanced view in the GUI.

6. In the **User alias / address mapping profile** drop-down list, select **InternalLabLDAP**.

   Your configuration should match the following example:



FortiMail

Domain name: internal.lab
Relay type: Host
SMTP server: 10.0.1.99 Port: 25 [Test...]
Use SMTPS
Fallback SMTP server: Port: 25 [Test...]
Use SMTPS
Relay Authentication
Comment:

Recipient Address Verification
Disable | SMTP Server | LDAP Server
LDAP profile: InternalLabLDAP
Action on invalid recipient: Reject | Discard

Automatic Removal of Invalid Quarantine Accounts

LDAP Options
User alias / address mapping profile: InternalLabLDAP
Mail routing profile: --None--
Scan override profile: --None--

Advanced Setting

Customer Information

7. Click **OK**.

You don’t need to configure recipient verification on IntSRV FortiMail. Recipient verification is enabled implicitly on a FortiMail that is operating in server mode because the user database exists locally.

You also don’t need to configure alias mapping on IntSRV FortiMail because IntGW FortiMail does the mapping before it delivers an email to IntSRV FortiMail.

Configure LDAP Authentication for Gateway Mode Webmail Access

You will configure LDAP authentication on IntGW FortiMail, so that users can authenticate to access their quarantine inbox using the IntGW FortiMail webmail GUI.

Take the Expert Challenge!

On IntGW FortiMail, enable LDAP authentication for gateway mode user quarantine mailbox access using the webmail GUI.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure LDAP Authentication for Server Mode Users on page 58.

To configure LDAP authentication for gateway mode webmail access

1. Continuing on the IntGW FortiMail management GUI, click **Policy** > **Recipient Policy** > **Inbound**.
2. Select recipient policy ID **1**, in the **internal.lab** domain, and then click **Edit**.
3. In the **Authentication and Access** section, configure the following settings:

Field	Value
Authentication type	LDAP
Authentication profile	InternalLabLDAP

4. Click **OK**.

Users will use their OpenLDAP accounts to authenticate and access the IntGW FortiMail webmail GUI for quarantined emails.

Configure LDAP Authentication for Server Mode Users

You will configure LDAP authentication for IntSRV FortiMail users.

To configure LDAP authentication for server mode users

1. Return to the IntSRV FortiMail management GUI, and then click **Domain & User** > **User** > **User**.
2. Select **user1**, and then click **Edit**.
3. In the **Authentication type** drop-down list, select **LDAP**.
4. In the **LDAP profile** drop-down list, select **InternalLabLDAP**.

If the LDAP profile doesn't appear in the drop-down list, then you missed a step. Go back to To configure an LDAP profile on IntSRV FortiMail on page 52, and then follow the steps to configure the same LDAP profile on IntSRV FortiMail.

5. Click **OK**.
6. Click **New**.

7. Configure the following settings:

Field	Value
User name	user2
Display name	Mail User 2
Authentication type	LDAP
LDAP profile	InternalLabLDAP

8. Click **Create**.
9. Log out of the IntSRV FortiMail management GUI.

Validate LDAP Authentication

You will validate LDAP authentication on both FortiMail VMs in the `internal.lab` domain.

To validate server mode LDAP authentication

1. On the IntSRV FortiMail webmail GUI, log in with the username `user2` and password `fortinet`.

   If you configured the server mode user LDAP authentication correctly, the login is successful.
2. Log out of the IntSRV FortiMail webmail GUI.

To validate gateway mode LDAP authentication

1. On the IntGW FortiMail webmail GUI, log in with the username `user2` and password `fortinet`.

   If you configured the gateway mode LDAP authentication correctly, the login is successful.

The webmail GUI in gateway mode gives users access to their bulk folder, which contains only quarantined emails. You will configure email quarantining in a later lab. In this section, you are verifying user access only.

2. Log out of the IntGW FortiMail webmail GUI.

To validate recipient verification

1. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
2. Compose a new email using the following values:

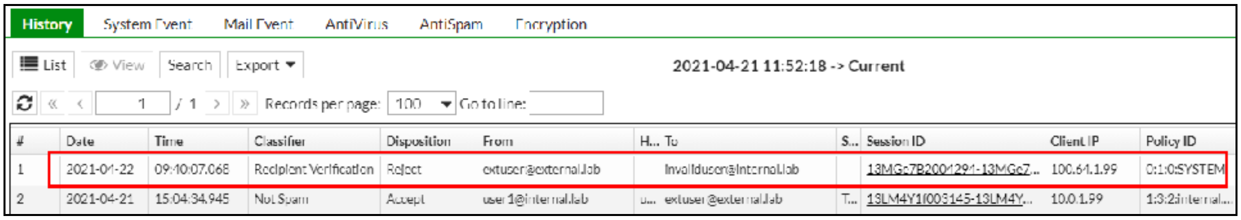
Field	Value
To	invaliduser@internal.lab
Subject	Testing Recipient Verification
Message Body	This should be rejected!

3. Click **Send**.
4. Click **Refresh** to update the inbox.

   You should receive a delivery status notification (DSN) message.

5. Open the DSN message, and then review the transcript details.
6. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.
7. Double-click the active log file.

   The first entry in the **History** log should correspond to the email you just sent.



2021-04-21 11:52:18 -> Current

#	Date	Time	Classifier	Disposition	From	H...	To	S...	Session ID	Client IP	Policy ID
1	2021-04-22	09:10:07.068	Recipient Verification	Reject	extuser@external.lab		invaliduser@internal.lab		13MGc7B2001291-13MGc7...	100.64.1.99	0:1:0:SYSTEM
2	2021-04-21	15:04:34.945	Not Spam	Accept	user1@internal.lab	u...	extuser@external.lab	T...	13LM4Y1I003145-13LM4Y...	10.0.1.99	1:3:2:internal...

8. Review the log details.

   If you configured recipient verification correctly, the log entry shows that the email was rejected with a **Recipient Verification** classifier.

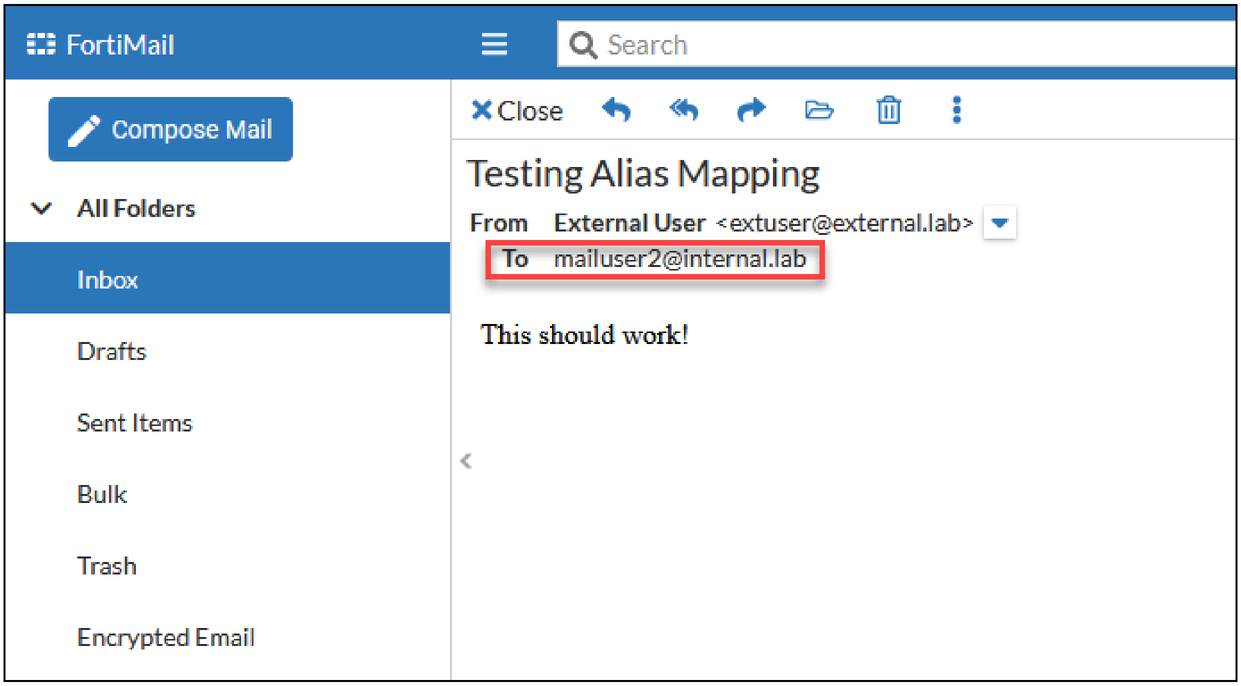
To validate alias mapping

1. Return to the ExtSRV FortiMail webmail GUI, and then compose another email using the following values:

Field	Value
To	mailuser2@internal.lab
Subject	Testing Alias Mapping
Message Body	This should work!

2. Click **Send**.
3. Log out of the ExtSRV FortiMail webmail GUI.
4. On the IntSRV FortiMail webmail GUI, log in with the username `user2` and password `fortinet`.

   The email you sent to `mailuser2@internal.lab` appears in the `user2@internal.lab` inbox.



Testing Alias Mapping

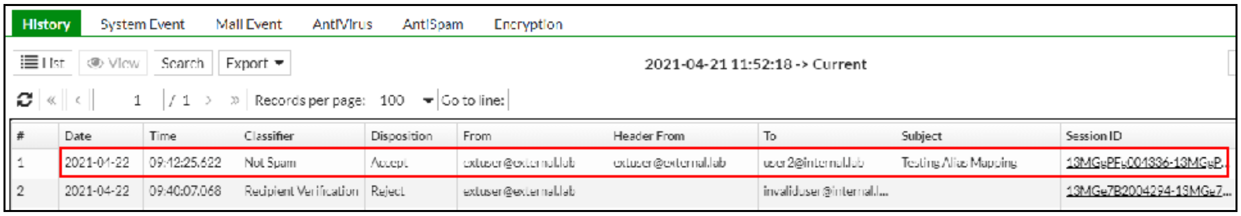
From External User <extuser@external.lab>

To mailuser2@internal.lab

This should work!

5. Log out of the IntSRV FortiMail webmail GUI.
6. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

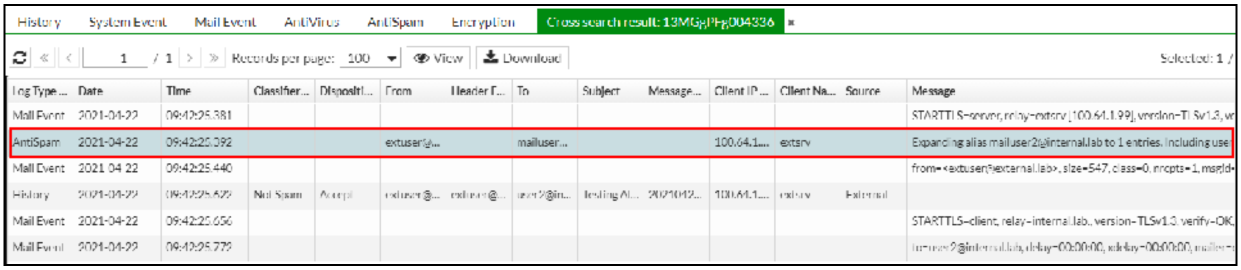
   The first entry in the **History** log should correspond to the email you just sent.



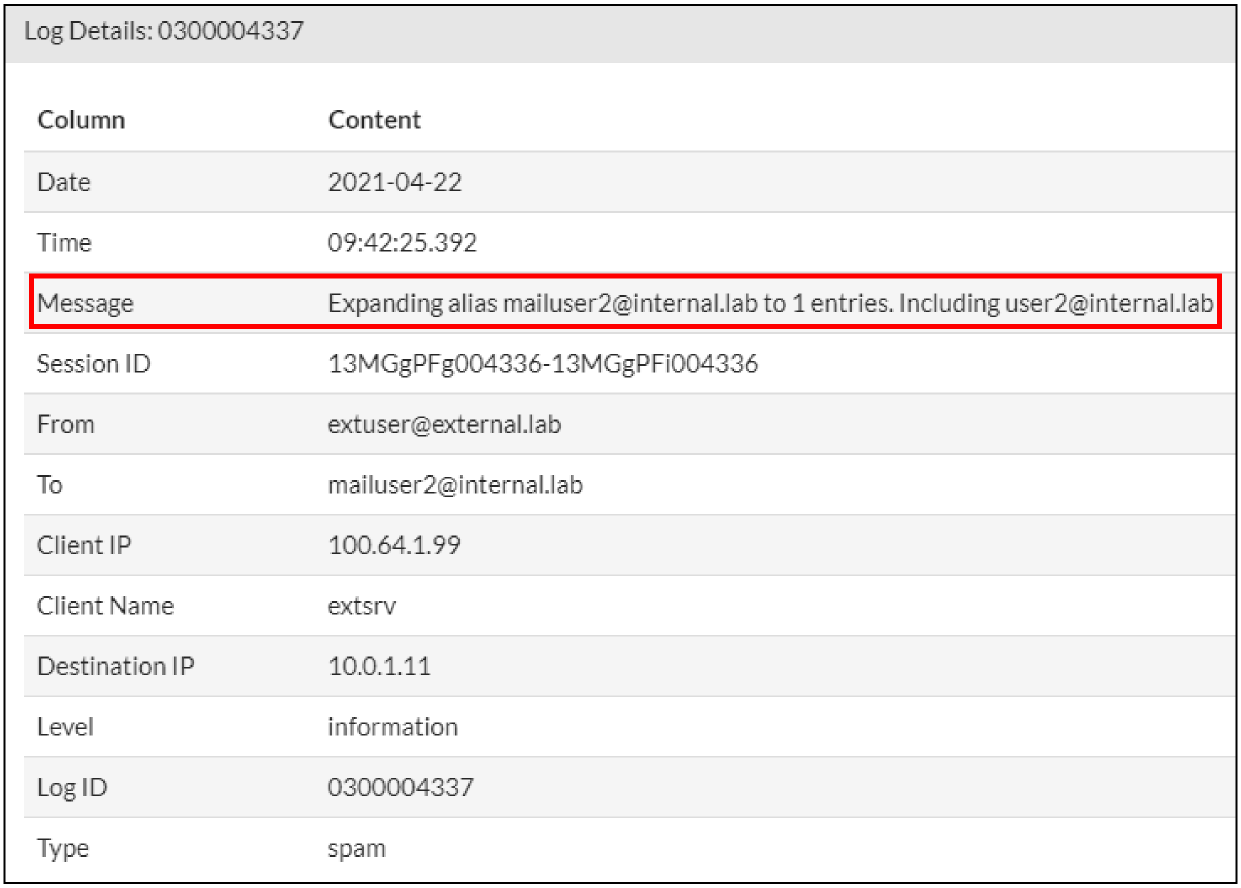
2021-04-21 11:52:18 -> Current

#	Date	Time	Classifier	Disposition	From	Header From	To	Subject	Session ID
1	2021-04-22	09:42:25.622	Not Spam	Accept	extuser@external.lab	extuser@external.lab	user2@internal.lab	Testing Alias Mapping	13MGpPFg004336-13MGpP...
2	2021-04-22	09:40:07.068	Recipient Verification	Reject	extuser@external.lab		invaliduser@internal.l...		13MGe7B2004294-13MGe7...

7. Click the **Session ID** link to retrieve the cross-search result.
8. Review the **AntiSpam** log related to the session.



Log Type ...	Date	Time	Classifier...	Dispositi...	From	Header F...	To	Subject	Message...	Client IP ...	Client Na...	Source	Message
Mail Event	2021-04-22	09:42:25.381											STARTTLS=server, relay=extsrv [100.64.1.99], version=TLSv1.3, ve
AntiSpam	2021-04-22	09:42:25.392			extuser@...		mailuser...			100.64.1....	extsrv		Expanding alias mailuser2@internal.lab to 1 entries. Including use
Mail Event	2021 04 22	09:42:25.440											from=<extuser@external.lab>, size=547, class=0, nrcpts=1, msgid=
History	2021-04-22	09:42:25.622	Not Spam	Accept	extuser@...	extuser@...	user2@in...	Testing Al...	2021042...	100.64.1....	extsrv	External	
Mail Event	2021-04-22	09:42:25.656											STARTTLS=client, relay=internal.lab., version=TLSv1.3, verify=OK,
Mail Event	2021-04-22	09:42:25.772											to=user2@internal.lab, delay=00:00:00, xdelay=00:00:00, mailer=



Log Details: 0300004337

Column	Content
Date	2021-04-22
Time	09:42:25.392
Message	Expanding alias mailuser2@internal.lab to 1 entries. Including user2@internal.lab
Session ID	13MGgPFg004336-13MGgPFi004336
From	extuser@external.lab
To	mailuser2@internal.lab
Client IP	100.64.1.99
Client Name	extsrv
Destination IP	10.0.1.11
Level	information
Log ID	0300004337
Type	spam

Alias mapping is useful to consolidate multiple emails for different aliases in a single email account, using the user's primary email address as the identifier. This reduces account management overhead for the user and the administrator. For example, if a user has five aliases in addition to a primary email address, FortiMail can use alias mapping to maintain a single user quarantine mailbox. Otherwise, the user would have to manage six separate quarantine accounts, as well as the quarantine reports for each account.

9. Click **Close**.
10. Log out of the IntGW FortiMail management GUI.

Exercise 3: Blocking SMTP Brute Force Attacks

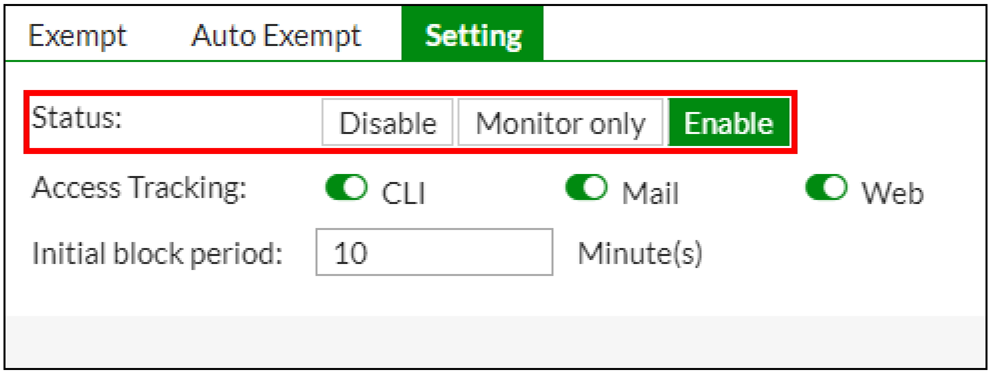
In this exercise, you will explore how FortiMail handles failed SMTP authentication. You will generate an SMTP brute force attack and block the offending IP address.

Configure Authentication Reputation

You will configure authentication reputation on IntGW FortiMail.

To configure authentication reputation

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Security** > **Authentication Reputation** > **Setting**.
3. Click **Enable**.



Status: Disable | Monitor only | [✓ Enable]

Access Tracking: CLI Mail Web

Initial block period: 10 Minute(s)

The default block period for an offending IP address is 10 minutes. You can set the block period to a maximum of 60 minutes and minimum of 5 minutes.

4. Click **Apply**.

Generate an SMTP Brute Force Attack

You will execute an SMTP brute force attack on IntGW FortiMail, and then review the logs to validate that the authentication reputation feature is working correctly.

To generate an SMTP brute force attack

1. On the Linux-Client VM, open a terminal window (`Ctrl`+`Alt`+`T`).
2. Enter the following command to start an SSH connection to the Linux-Router VM:

```
ssh student@10.0.1.254
```

3. Enter the password `password`.
4. Enter `pwd`.

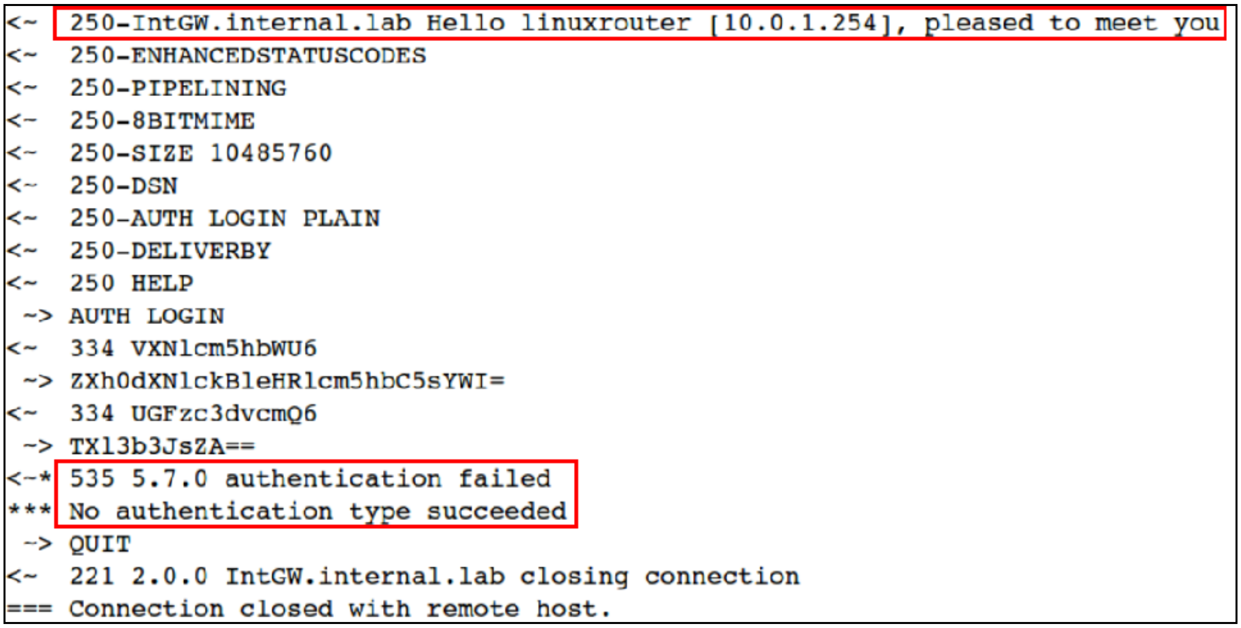
   Verify that your current working directory is `/home/student`.

5. Enter the following swaks command to generate an SMTP brute force attack:

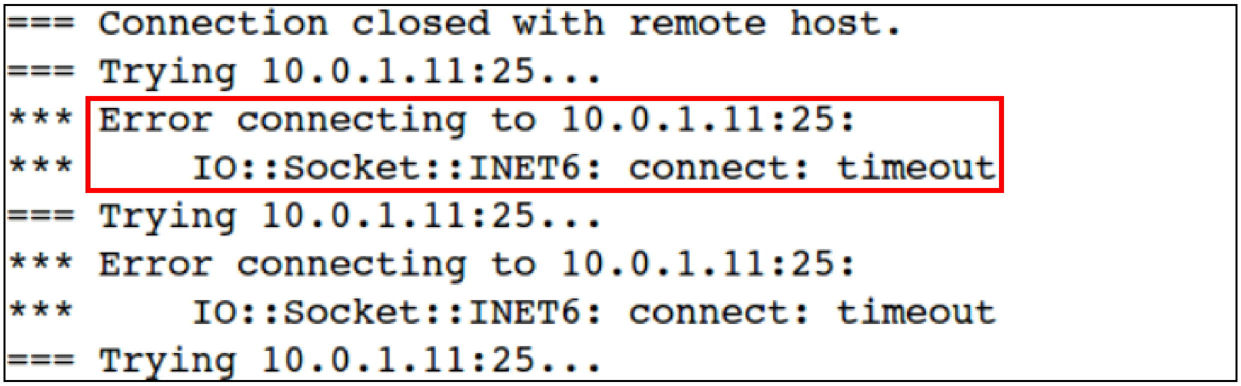
```
while sleep 1; do swaks --to user1@internal.lab --from "extuser@external.lab" --
    header "Subject: Test mail" --body "This is a test mail" --server 10.0.1.11 --
    port 25 --timeout 40s --auth LOGIN --auth-user "extuser@external.lab" --auth-
    password "Myworld" -tls; done
```

A copy of the swaks command is in the `commands.txt` file, which is located in the **Resources** folder on the Linux-Client desktop.

After a few successful SMTP connections, subsequent connections time out.



```
<~  250-IntGW.internal.lab Hello linuxrouter [10.0.1.254], pleased to meet you
<~  250-ENHANCEDSTATUSCODES
<~  250-PIPELINING
<~  250-8BITMIME
<~  250-SIZE 10485760
<~  250-DSN
<~  250-AUTH LOGIN PLAIN
<~  250-DELIVERBY
<~  250 HELP
 ~> AUTH LOGIN
<~  334 VXNlcm5hbWU6
 ~> ZXh0dXNlckBleHRlcm5hbC5sYWI=
<~  334 UGFzc3dvcmQ6
 ~> TXl3b3JsZA==
<~* 535 5.7.0 authentication failed
*** No authentication type succeeded
 ~> QUIT
<~  221 2.0.0 IntGW.internal.lab closing connection
=== Connection closed with remote host.
```



```
=== Connection closed with remote host.
=== Trying 10.0.1.11:25...
*** Error connecting to 10.0.1.11:25:
***     IO::Socket::INET6: connect: timeout
=== Trying 10.0.1.11:25...
*** Error connecting to 10.0.1.11:25:
***     IO::Socket::INET6: connect: timeout
=== Trying 10.0.1.11:25...
```

6. Press `Ctrl+C` to stop the script.

Stop and think!

Why are the SMTP connections failing?

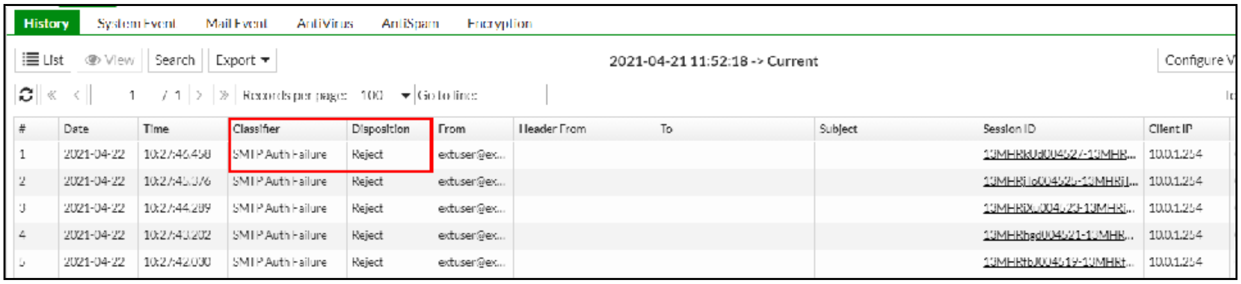
FortiMail uses a variety of adaptive factors to detect and block brute forcing (not only consecutive failures) and they temporarily lock out the user. FortiMail detected a brute force attack and blocked that IP address. New TCP connections from that attacker were denied.

7. Close the terminal window.

To review the logs

1. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

   The first few log entries should correspond to the failed SMTP authentication, with **SMTP Auth Failure** showing in the **Classifier** column, and **Reject** showing in the **Disposition** column.



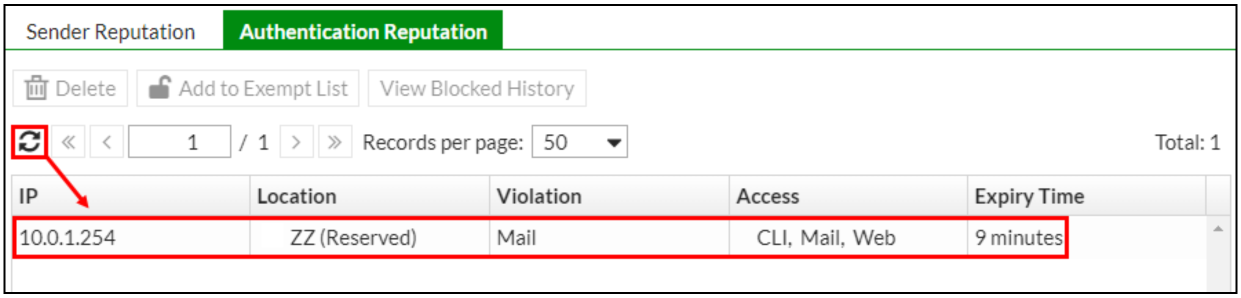
2021-04-21 11:52:18 -> Current

#	Date	Time	Classifier	Disposition	From	Header From	To	Subject	Session ID	Client IP
1	2021-04-22	10:27:46.458	SMTP Auth Failure	Reject	extuser@ex...				13MHRk0d004527-13MHR...	10.0.1.254
2	2021-04-22	10:27:45.376	SMTP Auth Failure	Reject	extuser@ex...				13MHRjIo004526-13MHRjI...	10.0.1.254
3	2021-04-22	10:27:44.289	SMTP Auth Failure	Reject	extuser@ex...				13MHRiX004523-13MHRi...	10.0.1.254
4	2021-04-22	10:27:43.202	SMTP Auth Failure	Reject	extuser@ex...				13MHRhad004521-13MHR...	10.0.1.254
5	2021-04-22	10:27:42.030	SMTP Auth Failure	Reject	extuser@ex...				13MHRfbJ004519-13MHRf...	10.0.1.254

2. Click **Monitor** > **Reputation** > **Authentication Reputation**.

   The blocked IP address of the attacker is displayed.

3. Refresh to view the current expiry time.



Total: 1

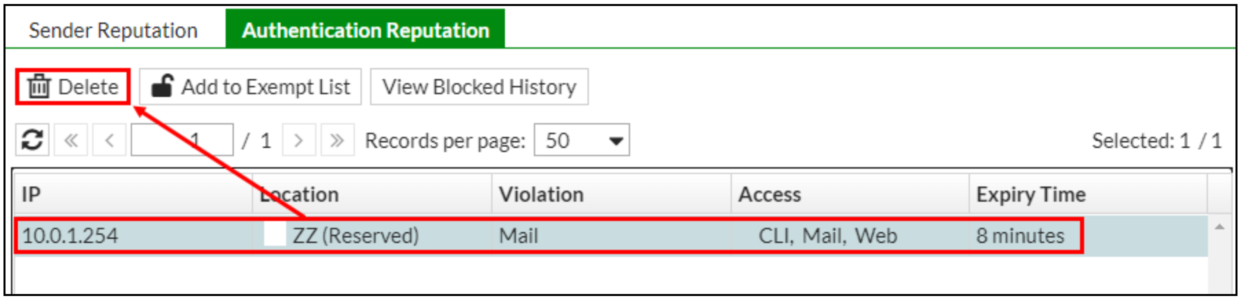
IP	Location	Violation	Access	Expiry Time
10.0.1.254	ZZ (Reserved)	Mail	CLI, Mail, Web	9 minutes

If you do not see the IP address on the **Authentication Reputation** tab, enter the following command on the IntGW FortiMail CLI. To access the CLI console, click **Dashboard** > **Console**.

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

To remove the blocked IP address

1. Continuing on the IntGW FortiMail management GUI, select the blocked IP address (**10.0.1.254**), and then click **Delete**.



IP	Location	Violation	Access	Expiry Time
10.0.1.254	ZZ (Reserved)	Mail	CLI, Mail, Web	8 minutes

2. Click **Delete**.
3. Log out of the IntGW FortiMail management GUI.

Lab 4: Session Management

In this lab, you will configure session profiles to inspect the envelope of emails. You will also use session profiles to hide internal network information from email headers.

Objectives

- Configure session profile connection settings to limit inbound connections to IntGW FortiMail
- Configure sender address rate control to limit outbound connections on IntSRV FortiMail
- Configure session profile header manipulation to hide your internal network information

Time to Complete

Estimated: 45 minutes

Prerequisites

Before beginning this lab, you must restore a configuration file on IntSRV FortiMail.

To restore a configuration file on IntSRV FortiMail

1. Go to the Linux-Client VM.
2. Open a new browser, and then on the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
3. Click **System** > **Maintenance** > **Configuration**.
4. Click **Restore Configuration**.
5. Click **Desktop** > **Resources** > **Starting Configs** > **Lab 4** > `04_Initial_IntSRV.tgz`, and then click **Open**.
6. Click **OK**.
7. Wait for IntSRV FortiMail to finish rebooting before you proceed with the exercise.
8. Close the browser tab.

The configuration file adds a new IP policy that causes all email delivery attempts from ExtSRV FortiMail to IntSRV FortiMail to fail temporarily. This ensures that when the session limits are triggered on IntGW FortiMail, ExtSRV FortiMail can't deliver to IntSRV FortiMail directly. This change prevents confusion when testing the session profile settings you will be configuring on the IntGW FortiMail later in this lab.

Exercise 1: Limiting SMTP Connections

In this exercise, you will limit the number of SMTP sessions that each client can establish within a 30-minute period. Spammers usually send as many emails as they can in a short period of time before legitimate email servers begin to block their delivery. If blocked, the spammers won't spend the time to retry. Legitimate email servers *will* retry delivery if it fails the first time.

Configure Connection Limits

You will configure a session profile on IntGW FortiMail to limit the number of connections that ExtSRV FortiMail can establish over a 30-minute period.

Take the Expert Challenge!

On IntGW FortiMail, configure a new session profile to limit client connections to 4 per 30 minutes.

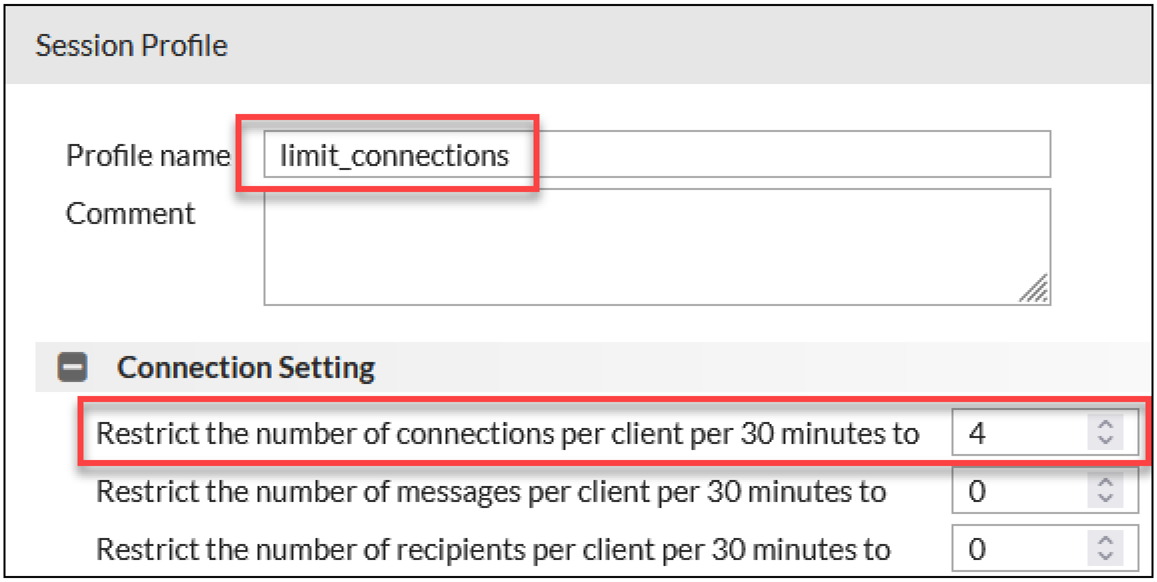
Apply the new session profile to the correct policy, so that IntGW FortiMail applies the connection limits to all inbound connections.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Validate Connection Limits on page 69.

To configure connection limits

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Profile** > **Session** > **Session**.
3. Click **New**.
4. In the **Profile name** field, type `limit_connections`.
5. In the **Restrict the number of connections per client per 30 minutes to** field, type `4`.



Session Profile

Profile name: limit_connections

Comment:

Connection Setting

Restrict the number of connections per client per 30 minutes to: 4

Restrict the number of messages per client per 30 minutes to: 0

Restrict the number of recipients per client per 30 minutes to: 0

6. Click **Create**.

4 connections every 30 minutes is too few to be realistic for real-world deployments. Email servers usually send many emails to or through FortiMail each minute. In this lab, however, you will use the 30-minute restriction to make your rate limit easy to trigger.

To apply the session profile to inbound connections

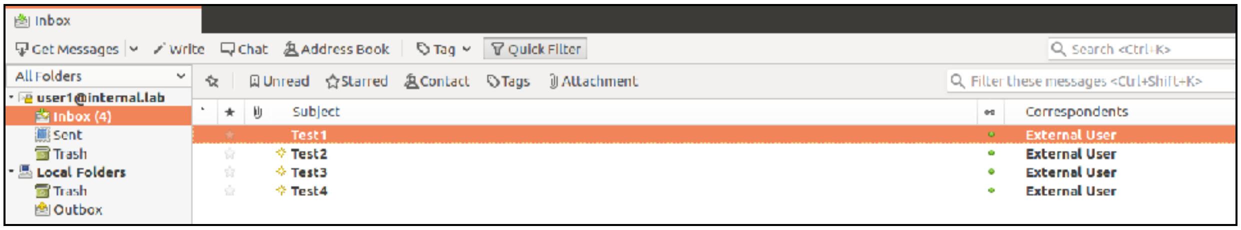
1. Continuing on the IntGW FortiMail management GUI, click **Policy** > **IP Policy** > **IP Policy**.
2. Edit IP policy ID **1**.
3. In the **Profiles** section, in the **Session** drop-down list, select **limit_connections**.
4. Click **OK**.

Validate Connection Limits

You will test the connection limitation by sending consecutive emails to trigger a violation. You will also verify your configuration by reviewing the logs.

To validate connection limits

1. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
2. Send five emails to `user1@internal.lab` to trigger the session limit.
3. Log out of the ExtSRV FortiMail webmail GUI.
4. On the Linux-Client VM, open Mozilla Thunderbird, and then verify how many emails were delivered to the `user1@internal.lab` inbox.

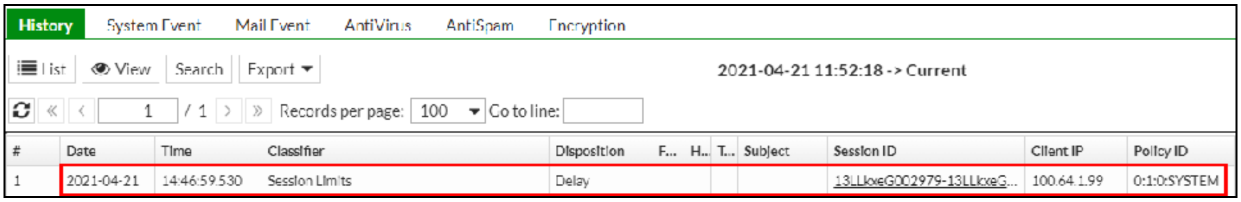


Subject	Correspondents
Test1	External User
Test2	External User
Test3	External User
Test4	External User

There will be one email sent per TCP connection. Therefore, IntGW FortiMail should allow the first four but block the fifth, which exceeds your configured connection limit.

5. Close Thunderbird.
6. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

   The first entry in the **History** log should correspond to the rejected email.



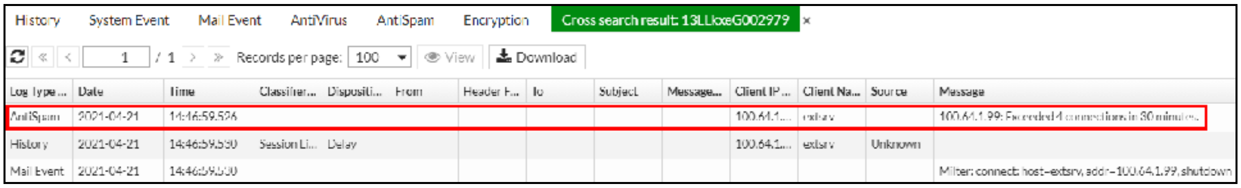
2021-04-21 11:52:18 -> Current

#	Date	Time	Classifier	Disposition	F...	H...	T...	Subject	Session ID	Client IP	Policy ID
1	2021-04-21	14:46:59.530	Session Limits	Delay					13LLkxeG002979-13LLkxeG...	100.64.1.99	0:1:0:SYSTEM

Why are the **From**, **To**, and **Subject** fields in this log entry empty?

FortiMail blocked the client's attempt when it scanned the IP layer of the initial packets *before* the SMTP session could be established. The SMTP session contains the SMTP envelope—the sender's email address, the recipient's email address, and the subject. So, those parts of the email were never received.

7. Click the **Session ID** to retrieve the cross-search results.
8. Review the related **AntiSpam** log.



Log Type...	Date	Time	Classifier...	Dispositi...	From	Header F...	To	Subject	Message...	Client IP...	Client Na...	Source	Message
AntiSpam	2021-04-21	14:46:59.526								100.64.1....	extsrv		100.64.1.99: Exceeded 4 connections in 30 minutes.
History	2021-04-21	14:46:59.530	Session Li...	Delay						100.64.1....	extsrv	Unknown	
Mail Event	2021-04-21	14:46:59.530											Milter: connect: host=extsrv, addr=100.64.1.99, shutdown

Disable Connection Limits

To continue with the lab exercises, you must disable connection limits in the session profile, so that it does not interfere with the other labs.

To disable connection limits

1. Continuing on the IntGW FortiMail management GUI, click **Policy** > **IP Policy** > **IP Policy**.
2. Edit IP policy ID **1**.
3. In the **Session** drop-down list, select **None**.
4. Click **OK**.
5. Log out of the IntGW FortiMail management GUI.

Exercise 2: Configuring Sender Address Rate Control

In this exercise, you will configure sender address rate control to control the volume of outbound emails your internal users can send. While it is important to protect your email users from spammers sending large volumes of email, it is also important to protect your own mail server IP reputation by controlling the volume of email received from internal users.

Configure Sender Address Rate Control

You will configure sender address rate control on IntSRV FortiMail.

Take the Expert Challenge!

On IntSRV FortiMail, configure sender address rate control to limit outbound emails to 4 per 30 minutes.

If any user exceeds any of the sender address rate control settings, IntSRV FortiMail should send a notification email to `user1@internal.lab`.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Validate Sender Address Rate Control on page 74.

To configure sender address rate control

1. On the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Domain & User** > **Domain** > **Domain**.
3. Select the **internal.lab** domain, and then click **Edit**.
4. In the **Advanced Settings** section, click **Sender Address Rate Control**.
5. Enable **Status**.
6. Configure the following values:

Field	Value
Action	Reject
Maximum number of messages per half hour	4
Send email notification upon rate control violations	Enable

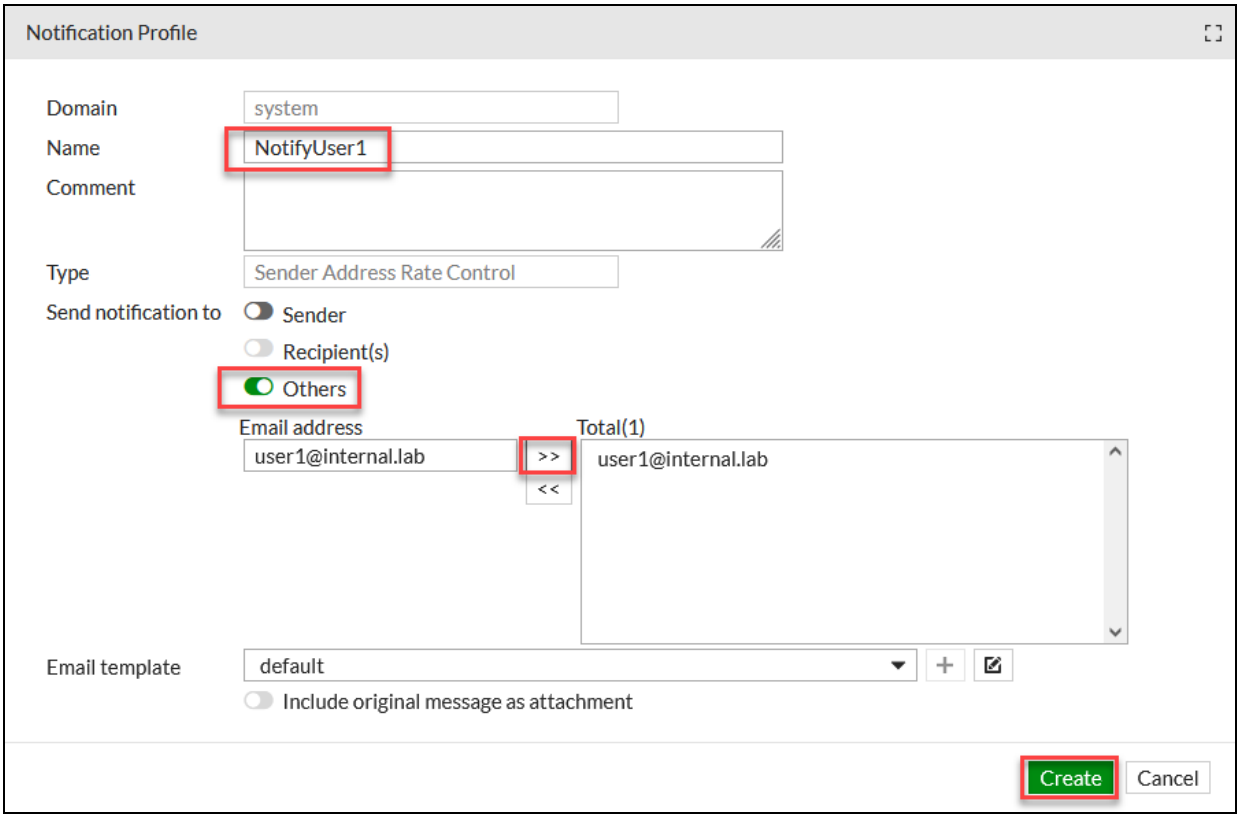
7. In the **Send email notification upon rate control violations** field, click **+** to add a new notification setting.
8. Configure the following values:

Field	Value
Name	NotifyUser1

Field	Value
Send notification to	Others

9. In the **Email address** field, type `user1@internal.lab`.
10. Click **>>**.

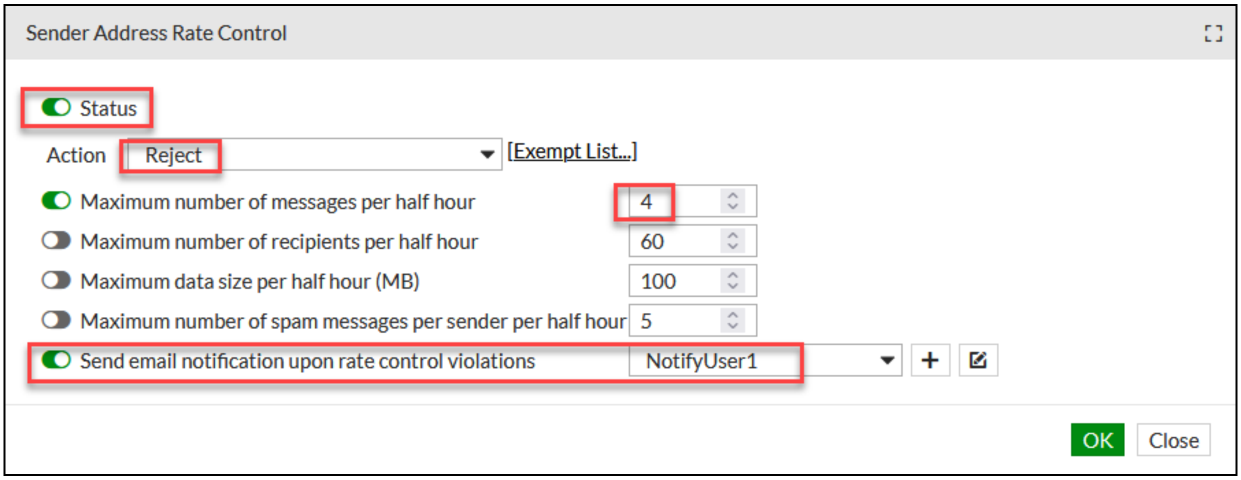
    Your configuration should match the following example:



Notification Profile

Domain	system
Name	NotifyUser1
Comment	
Type	Sender Address Rate Control
Send notification to	○ Sender ○ Recipient(s) ● Others
Email address	user1@internal.lab
Total(1)	user1@internal.lab
Email template	default
	○ Include original message as attachment

11. Click **Create**.



Sender Address Rate Control

● Status

Action Reject [Exempt List...]

● Maximum number of messages per half hour	4
○ Maximum number of recipients per half hour	60
○ Maximum data size per half hour (MB)	100
○ Maximum number of spam messages per sender per half hour	5
● Send email notification upon rate control violations	NotifyUser1

12. Verify the settings, and then click **OK**.
13. Click **OK**.

Validate Sender Address Rate Control

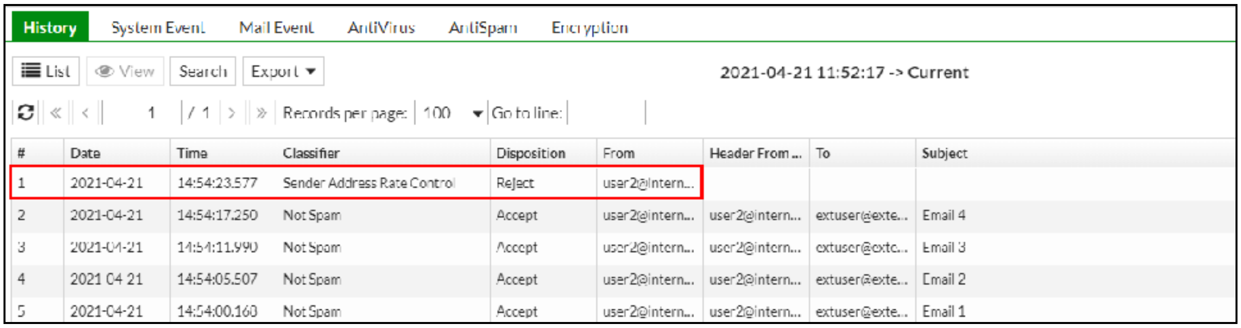
You will validate sender address rate control by sending five emails from a user in the `internal.lab` domain. Since you configured the limit to 4 emails within a 30-minute period, the fifth message will be rejected.

To validate sender address rate control

1. On the IntSRV FortiMail webmail GUI, log in with the username `user2` and password `fortinet`.
2. Send five emails to `extuser@external.lab` to trigger the rate control limit.
3. Log out of the IntSRV FortiMail webmail GUI.
4. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
5. Check how many emails were delivered to the `extuser@external.lab` inbox.
6. Log out of the ExtSRV FortiMail webmail GUI.

   By now, `user1@internal.lab` should have received the notification email for the rate control violation.
7. On the Linux-Client VM, open Thunderbird, and then view the details in the notification email with the subject **Sender Rate Exceeded**.
8. Close Thunderbird.
9. Return to the IntSRV FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

   The first entry in the **History** log should correspond to the rate control violation.



2021-04-21 11:52:17 -> Current

#	Date	Time	Classifier	Disposition	From	Header From ...	To	Subject
1	2021-04-21	14:54:23.577	Sender Address Rate Control	Reject	user2@intern...			
2	2021-04-21	14:54:17.250	Not Spam	Accept	user2@intern...	user2@intern...	extuser@exte...	Email 4
3	2021-04-21	14:54:11.990	Not Spam	Accept	user2@intern...	user2@intern...	extuser@exte...	Email 3
4	2021 04 21	14:54:05.507	Not Spam	Accept	user2@intern...	user2@intern...	extuser@exte...	Email 2
5	2021-04-21	14:54:00.160	Not Spam	Accept	user2@intern...	user2@intern...	extuser@exte...	Email 1

While session profile connection limits and sender address rate control appear to function very similarly, FortiMail applies them very differently.

As you observed in the previous exercise, FortiMail applies the session profile connection limits at the IP layer. The sender address rate control feature limits connections based on the sender's address, which is derived from the `Mail From:` field of the SMTP envelope. So, for sender address rate control, FortiMail must process at least a portion of the SMTP envelope. This is also why **user2@internal.lab** appears in the **From** field of the log entry, but the log entries from the session profile connection limits are empty.

10. Click the **Session ID** to retrieve the cross-search results.
11. Review the related event and antispam logs.

Disable Sender Address Rate Control

You will disable sender address rate control. In the lab environment, it can interfere with other lab exercises, but in a real-world environment, it is a good practice to enable sender address rate control.

To disable sender address rate control

1. Continuing on the IntSRV FortiMail management GUI, click **Domain & User** > **Domain** > **Domain**.
2. Select the **internal.lab** domain, and then click **Edit**.
3. In the **Advanced Settings** section, select **Sender address rate control**, and then disable it.
4. Click **OK**.
5. Click **OK**.
6. Log out of the IntSRV FortiMail management GUI.

Exercise 3: Hiding Internal Headers

In this exercise, you will remove internal headers. It is a good security practice to hide your internal network information and it also reduces the size of messages.

Configure Header Manipulation

You will observe the effects of header manipulation settings by configuring a session profile on IntGW FortiMail to hide internal headers.

To review headers

1. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
2. Open any email message sent by an `internal.lab` user.

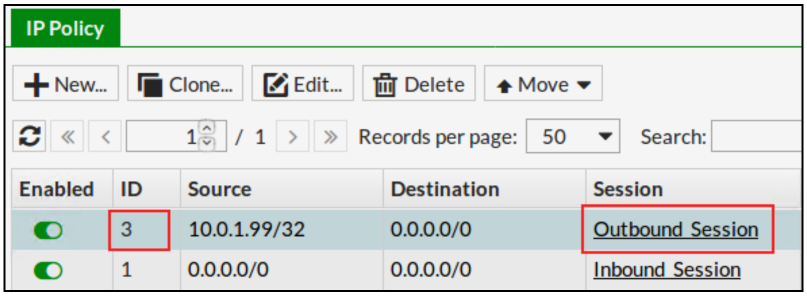
If you deleted all previous email messages, on the Linux-Client VM, open Thunderbird, and then send a new email message to `extuser@external.lab`.

3. Click **More** > **Detailed Header**.
4. Select and copy (`Ctrl+C`) the header contents.
5. Open a text editor application, and then paste (`Ctrl+V`) the header details.
6. Save the file on the desktop as `Header_Before.txt`.

To configure header manipulation

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Policy** > **IP Policy** > **IP Policy**.
3. Click the **Outbound_Session** link.

   This is the session profile currently applied to IP policy ID 3, which processes all outbound email for the `internal.lab` domain.



Enabled	ID	Source	Destination	Session
●	3	10.0.1.99/32	0.0.0.0/0	Outbound Session
●	1	0.0.0.0/0	0.0.0.0/0	Inbound Session

4. Expand **Header Manipulation**, and then enable **Remove received headers**.
5. Click **OK**.
6. Log out of the IntGW FortiMail management GUI.

Validate Header Manipulation

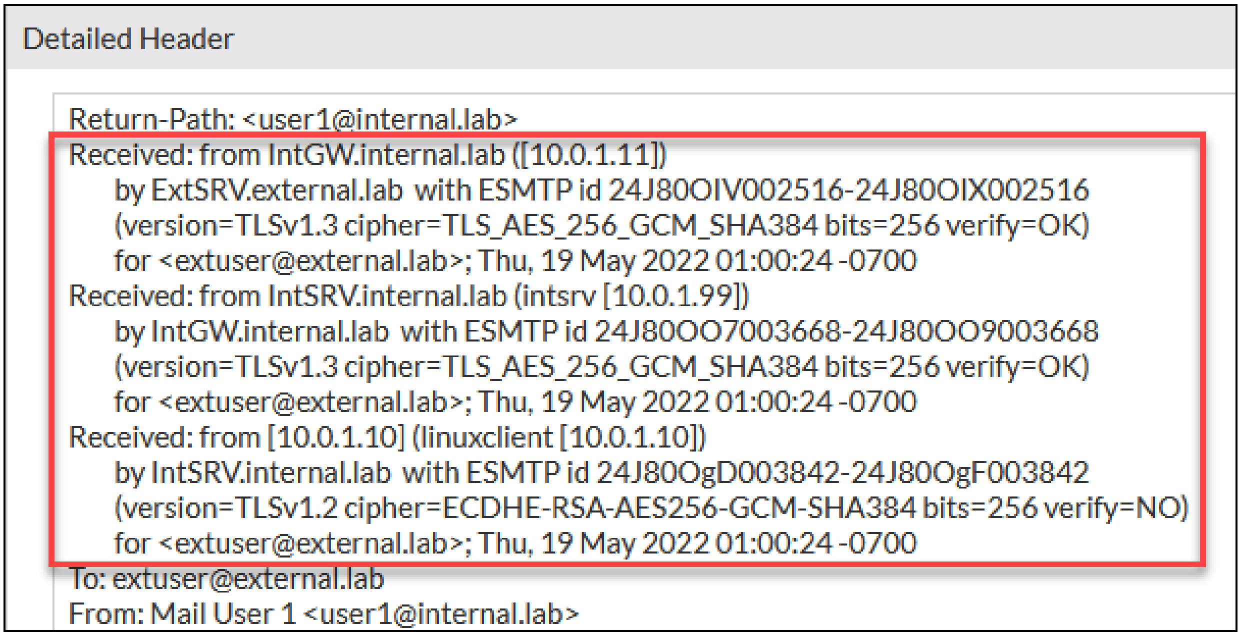
You will validate header manipulation by comparing the headers of an email before and after you configure header manipulation.

To validate header manipulation settings

1. On the Linux-Client VM, open Thunderbird, and then send a new email to `extuser@external.lab`.
2. Close Thunderbird.
3. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
4. Open the email you just sent from `user1@internal.lab`.
5. Review the detailed headers of the email.

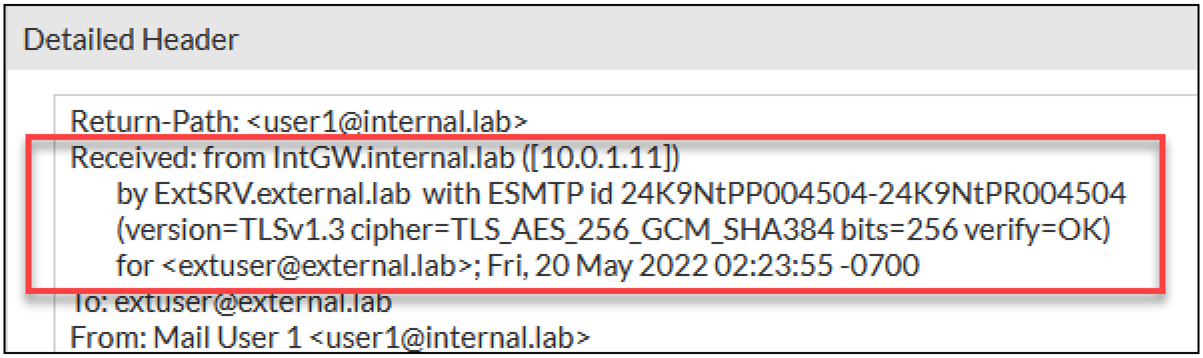
In the `Received:` header, you should see only details about IntGW FortiMail and ExtSRV FortiMail, and no information about Linux-Client (`10.0.1.10`) or IntSRV FortiMail (`10.0.1.99`).

6. Open the `Header_Before.txt` file you saved earlier.
7. Compare the differences.



Detailed Header

```
Return-Path: <user1@internal.lab>
Received: from IntGW.internal.lab ([10.0.1.11])
    by ExtSRV.external.lab  with ESMTP id 24J80OIV002516-24J80OIX002516
    (version=TLSv1.3 cipher=TLS_AES_256_GCM_SHA384 bits=256 verify=OK)
    for <extuser@external.lab>; Thu, 19 May 2022 01:00:24 -0700
Received: from IntSRV.internal.lab (intsrv [10.0.1.99])
    by IntGW.internal.lab  with ESMTP id 24J80OO7003668-24J80OO9003668
    (version=TLSv1.3 cipher=TLS_AES_256_GCM_SHA384 bits=256 verify=OK)
    for <extuser@external.lab>; Thu, 19 May 2022 01:00:24 -0700
Received: from [10.0.1.10] (linuxclient [10.0.1.10])
    by IntSRV.internal.lab  with ESMTP id 24J80OgD003842-24J80OgF003842
    (version=TLSv1.2 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=NO)
    for <extuser@external.lab>; Thu, 19 May 2022 01:00:24 -0700
To: extuser@external.lab
From: Mail User 1 <user1@internal.lab>
```



Detailed Header

```
Return-Path: <user1@internal.lab>
Received: from IntGW.internal.lab ([10.0.1.11])
    by ExtSRV.external.lab  with ESMTP id 24K9NtPP004504-24K9NtPR004504
    (version=TLSv1.3 cipher=TLS_AES_256_GCM_SHA384 bits=256 verify=OK)
    for <extuser@external.lab>; Fri, 20 May 2022 02:23:55 -0700
To: extuser@external.lab
From: Mail User 1 <user1@internal.lab>
```

8. Return to the ExtSRV FortiMail webmail GUI, and then click **OK**.
9. Log out of the ExtSRV FortiMail webmail GUI.

Lab 5: Antivirus

In this lab, you will configure FortiMail local malware detection techniques to scan for viruses in inbound email.

Objectives

- Configure an antivirus action profile to enable local malware detection
- Configure an antivirus profile to replace infected content from an email
- Apply antivirus scanning to inbound email
- Test antivirus functionality

Time to Complete

Estimated: 15 minutes

Exercise 1: Configuring Antivirus Scanning

In this exercise, you will configure an antivirus action profile and an antivirus profile on IntGW FortiMail. Then, you will apply the antivirus profile to a recipient-based policy in order to scan all inbound emails sent to the `internal.lab` domain.

Configure an Antivirus Action Profile

You will configure an antivirus action profile.

Take the Expert Challenge!

On IntGW FortiMail, configure an antivirus action profile and name it `AV_Tag_Replace`.

The antivirus action profile should be available for the `internal.lab` domain only.

The antivirus action profile should remove all malicious attachments from emails and tag the email subject line with the string `[VIRUS DETECTED]`.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

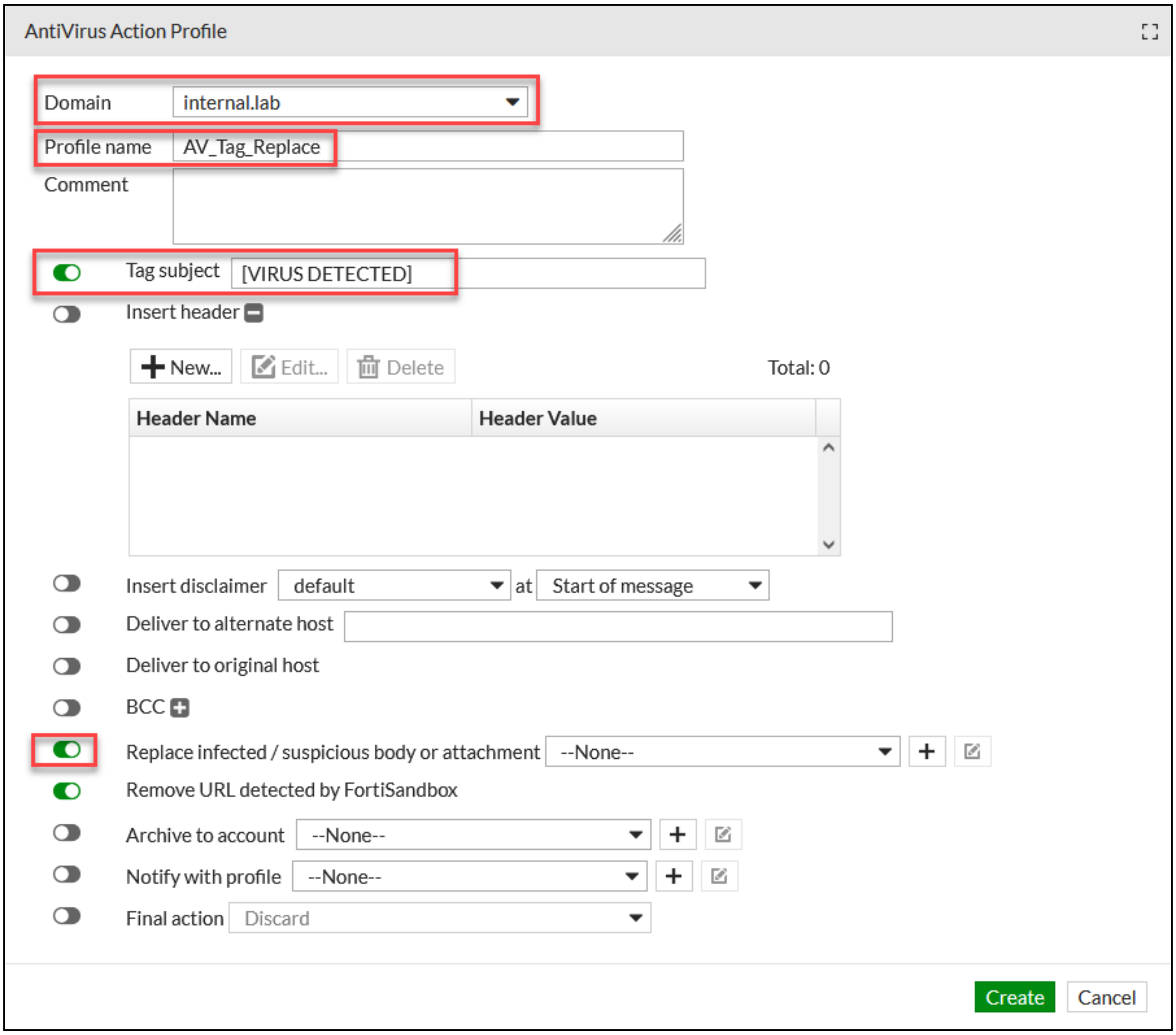
After you complete the challenge, see Configure an Antivirus Profile on page 81.

To configure an antivirus action profile

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Profile** > **AntiVirus** > **Action**.
3. Click **New**.
4. Configure the following settings:

Field	Value
Domain	internal.lab
Profile name	AV_Tag_Replace
Tag subject	enabled
Replace infected/suspicious body or attachment	enabled

5. In the **Tag subject** field, type `[VIRUS DETECTED]`.



AntiVirus Action Profile

Domain: internal.lab
Profile name: AV_Tag_Replace
Comment:

● Tag subject: [VIRUS DETECTED]
○ Insert header

Header Name	Header Value

Total: 0

○ Insert disclaimer: default at Start of message
○ Deliver to alternate host:
○ Deliver to original host
○ BCC
● Replace infected / suspicious body or attachment: --None--
● Remove URL detected by FortiSandbox
○ Archive to account: --None--
○ Notify with profile: --None--
○ Final action: Discard

6. Click **Create**.

Stop and think!

The action profile that you created doesn't appear in the list. Why?

The list view is filtered by domain. If you want to see the new profile, change the selection in the **Domain** drop-down list. Select **internal.lab** to view the action profiles for that specific domain, or select **All** to view the action profiles for all domains.

Configure an Antivirus Profile

You will create an antivirus profile and specify the default action that FortiMail takes when it detects a virus. If FortiMail detects a virus, it takes the actions that you define in the antivirus action profiles.

Take the Expert Challenge!

On IntGW FortiMail, configure an antivirus profile and name it `AV_In`.

The antivirus profile should be available for the `internal.lab` domain only.

The antivirus profile should use the **AV_Tag_Replace** antivirus action profile.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Apply Antivirus to Inbound Emails on page 82.

To configure an antivirus profile for local malware detection

1. Continuing on the IntGW FortiMail management GUI, click **Profile** > **AntiVirus** > **AntiVirus**.
2. Click **New**.
3. Configure the following settings:

Field	Value
Domain	internal.lab
Profile name	AV_In
Default action	AV_Tag_Replace

4. Click **Create**.
5. In the **Domain** drop-down list, select **internal.lab**.

   The **AV_In** antivirus profile is displayed.

Apply Antivirus to Inbound Emails

You will apply the antivirus profile to the inbound recipient policy for the `internal.lab` domain.

To apply antivirus to inbound emails

1. Continuing on the IntGW FortiMail management GUI, click **Policy** > **Recipient Policy** > **Inbound**.
2. Select recipient policy ID **1**, and then click **Edit**.
3. In the **Profiles** section, in the **Antivirus** drop-down list, select **AV_In**.
4. Click **OK**.

Validate Antivirus Functionality

You will test antivirus functionality using an EICAR file. An EICAR file does not contain a real virus. It is a harmless, industry-standard test file that is designed to trigger antivirus engines for testing purposes. So, if your antivirus configuration is correct, FortiMail should detect the EICAR file as a virus.

You shouldn’t test your antivirus configuration using a live virus. By doing so, you risk infecting your network hosts if your configuration is incorrect.

To send an infected email

1. On the Linux-Client VM, open a new browser tab, and then on the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
2. Compose a new email message using the following values:

Field	Value
To	user1@internal.lab
Subject	AV EICAR Test
Message Body	This contains a virus!

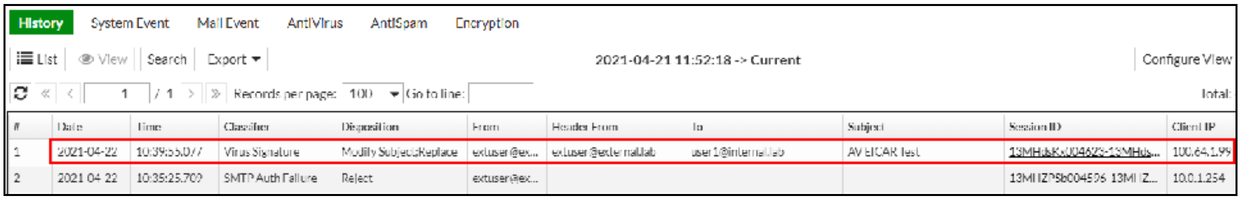
3. Click the **Attach** icon (the paperclip on the lower-left).
4. Click **Desktop** > **Resources** > **Files** > `eicar.com`, and then click **Open**.
5. Wait for the file upload to finish, and then click **Send**.
6. Log out of the ExtSRV FortiMail webmail GUI.

To validate antivirus functionality

1. Continuing on the Linux-Client VM, open Mozilla Thunderbird.
2. Confirm that you received the email message sent from `extuser@external.lab`.
3. Note that the following actions have been applied to the email message:
   - The subject line contains the **[VIRUS DETECTED]** tag.
   - IntGW FortiMail replaced the `eicar.com` file, and inserted a replacement message.
4. Close Thunderbird.

To monitor the logs

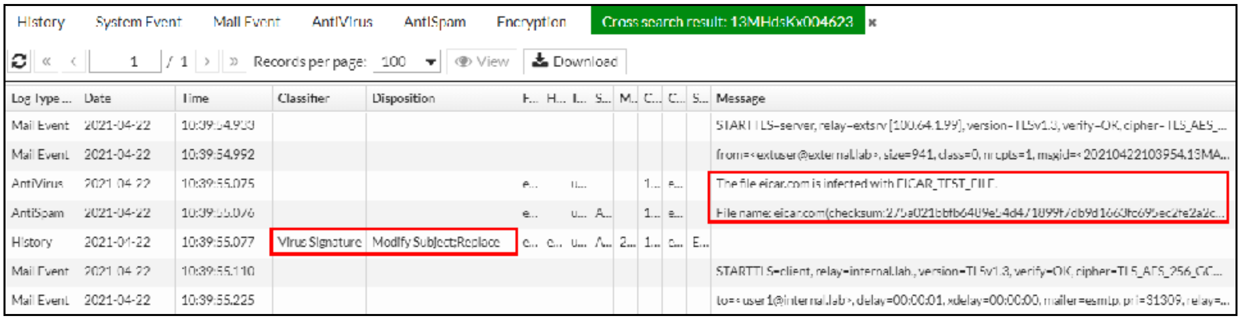
1. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.
2. The first entry in the **History** log should correspond to the virus email.



2021-04-21 11:52:18 -> Current

#	Date	Time	Classifier	Disposition	From	Header From	To	Subject	Session ID	Client IP
1	2021-04-22	10:39:55.077	Virus Signature	Modify Subject,Replace	extuser@ex...	extuser@external.lab	user1@internal.lab	AV EICAR Test	13MHdsKx004623-13MHds...	100.64.1.99
2	2021-04-22	10:35:25.709	SMTP Auth Failure	Reject	extuser@ex...				13MHZP5b004596-13MHZ...	10.0.1.254

3. Click the **Session ID** link to review the cross-search result for more details.



Log Type...	Date	Time	Classifier	Disposition	F...	H...	I...	S...	M...	C...	C...	S...	Message
Mail Event	2021-04-22	10:39:54.933											STARTTLS=server, relay=extsrv [100.64.1.99], version=TLSv1.3, verify=OK, cipher=TLS_AES_...
Mail Event	2021-04-22	10:39:54.992											from=<extuser@external.lab>, size=941, class=0, nrcpts=1, msgid=<20210422103954.13MA...
AntiVirus	2021-04-22	10:39:55.075			e...		u...			1...	e...		The file eicar.com is infected with EICAR_TEST_FILE.
AntiSpam	2021-04-22	10:39:55.076			e...		u...	A...		1...	e...		File name: eicar.com(checksum:275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c...
History	2021-04-22	10:39:55.077	Virus Signature	Modify Subject:Replace	c...	c...	u...	A...	2...	1...	c...	E...	
Mail Event	2021-04-22	10:39:55.110											STARTTLS=client, relay=internal.lab., version=TLSv1.3, verify=OK, cipher=TLS_AES_256_GC...
Mail Event	2021-04-22	10:39:55.225											to=<user1@internal.lab>, delay=00:00:01, xdelay=00:00:00, mailer=esmtp, pri=31309, relay=...

4. Log out of the IntGW FortiMail management GUI.

Lab 6: Antispam

In this lab, you will configure antispam scanning for both inbound and outbound email. Then, you will verify your configuration by sending spam through IntGW FortiMail. You will also configure quarantine report settings and manage user quarantine mailboxes.

Objectives

- Scan both incoming and outgoing emails for spam
- Send spam emails to user quarantine
- Manage quarantine report configuration
- Access and explore the user quarantine mailbox

Time to Complete

Estimated: 70 minutes

Prerequisites

Before beginning this lab, you must restore a configuration file on the `internal.lab` FortiMail VMs.

To restore a configuration file on IntSRV FortiMail

1. On the Linux-Client VM, open a new browser tab, and then on the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **System** > **Maintenance** > **Configuration**.
3. Click **Restore Configuration**.
4. Click **Desktop** > **Resources** > **Starting Configs** > **Lab 6** > `06_Initial_IntSRV.tgz`, and then click **Open**.
5. Click **OK**.

To restore a configuration file on IntGW FortiMail

1. Open a new browser tab, and then on the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **System** > **Maintenance** > **Configuration**.
3. Click **Restore Configuration**.
4. Click **Desktop** > **Resources** > **Starting Configs** > **Lab 6** > `06_Initial_IntGW.tgz`, and then click **Open**.
5. Click **OK**.
6. Wait for the FortiMail VMs to finish rebooting before proceeding with the first exercise.
7. Close the browser.

The configuration files disable all session profile inspection features, which can potentially interfere with the antispam testing you will do in this lab.

Exercise 1: Scanning Incoming Email for Spam

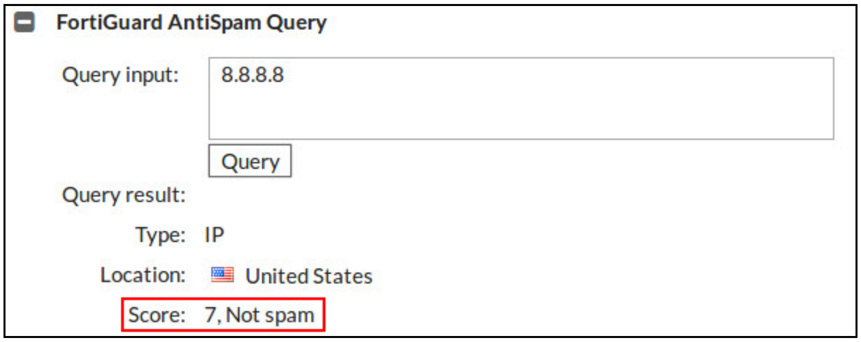
In this exercise, you will verify the FortiGuard configuration. Then, you will configure an antispam profile to scan all incoming email and send all spam email to the users' personal quarantine accounts.

Verify FortiGuard Configuration

You will configure FortiGuard settings. FortiMail devices receive antispam and antivirus updates from the FortiGuard Distribution Network (FDN), as long as there is a support contract attached to the device serial number.

To verify FortiGuard configuration

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **System** > **FortiGuard** > **Antispam**.
3. Enable **Enable cache**.
4. Click **Apply**.
5. Click **System** > **FortiGuard** > **License**.
6. Expand **FortiGuard Antispam Query**.
7. In the **Query input** field, type `8.8.8.8`.
8. Click **Query**.
9. Confirm that the **Score** field displays a query score value.



FortiGuard AntiSpam Query

Query input: 8.8.8.8

Query

Query result:

Type: IP

Location: United States

Score: 7, Not spam

If the **Query result** is **No response**, check the **License Information** widget on the FortiMail dashboard (**Dashboard** > **Status**). If the status is **Trial**, force a license update on the FortiMail GUI.

1. Click **Dashboard** > **Console**.
2. Type `execute update now`, and then press `Enter`.
3. Wait two minutes, and then click **Dashboard** > **Status**.
4. Review the **License Information** widget, and verify that the status is **Registered**.

Configure an Antispam Action Profile

You will configure an antispam action profile.

Take the Expert Challenge!

On IntGW FortiMail, create a new antispam action profile and name it `AS_In_User_Quar`.

The antispam action profile should be available for the `internal.lab` domain only.

The antispam action profile should send all detected spam messages to user quarantine.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure a Resource Profile on page 87.

To configure an antispam action profile

1. Continuing on the IntGW FortiMail management GUI, click **Profile** > **AntiSpam** > **Action**.
2. Click **New**.
3. Configure a new action profile using the following values:

Field	Value
Domain	internal.lab
Profile name	AS_In_User_Quar
Final action	Enabled

4. In the **Final action** drop-down list, select **Personal quarantine**.
5. Click **Create**.

Configure a Resource Profile

You will configure a resource profile, which allows you to control user accounts at the policy level. You will enable web and email release so that the recipient can use either email actions or web actions to release or delete quarantined messages.

Take the Expert Challenge!

On IntGW FortiMail, create a new resource profile and name it `Resource_AS_In_User_Quar`.

The resource profile should be available for the `internal.lab` domain only.

Configure the resource profile so that users will receive quarantine reports, and can use both web and email release functions.

Disable the automatic safelisting of senders of released messages.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure an Antispam Profile on page 88.

To configure a resource profile

1. Continuing on the IntGW FortiMail management GUI, click **Profile** > **Resource** > **Resource**.
2. Click **New**.
3. Configure a new resource profile using the following values:

Field	Value
Domain	internal.lab
Profile name	Resource_AS_In_User_Quar
Send quarantine report	Enabled
Web release	Enabled
Email release	Enabled
Safelist sender of released message	Disabled

4. Click **Create**.

Configure an Antispam Profile

You will create an antispam profile, enable various antispam techniques, and select the antispam action profile that you created before, as the default action.

To configure an antispam profile

1. Continuing on the IntGW FortiMail management GUI, click **Profile** > **AntiSpam** > **AntiSpam**.
2. Click **New**.
3. Configure a new antispam profile using the following values:

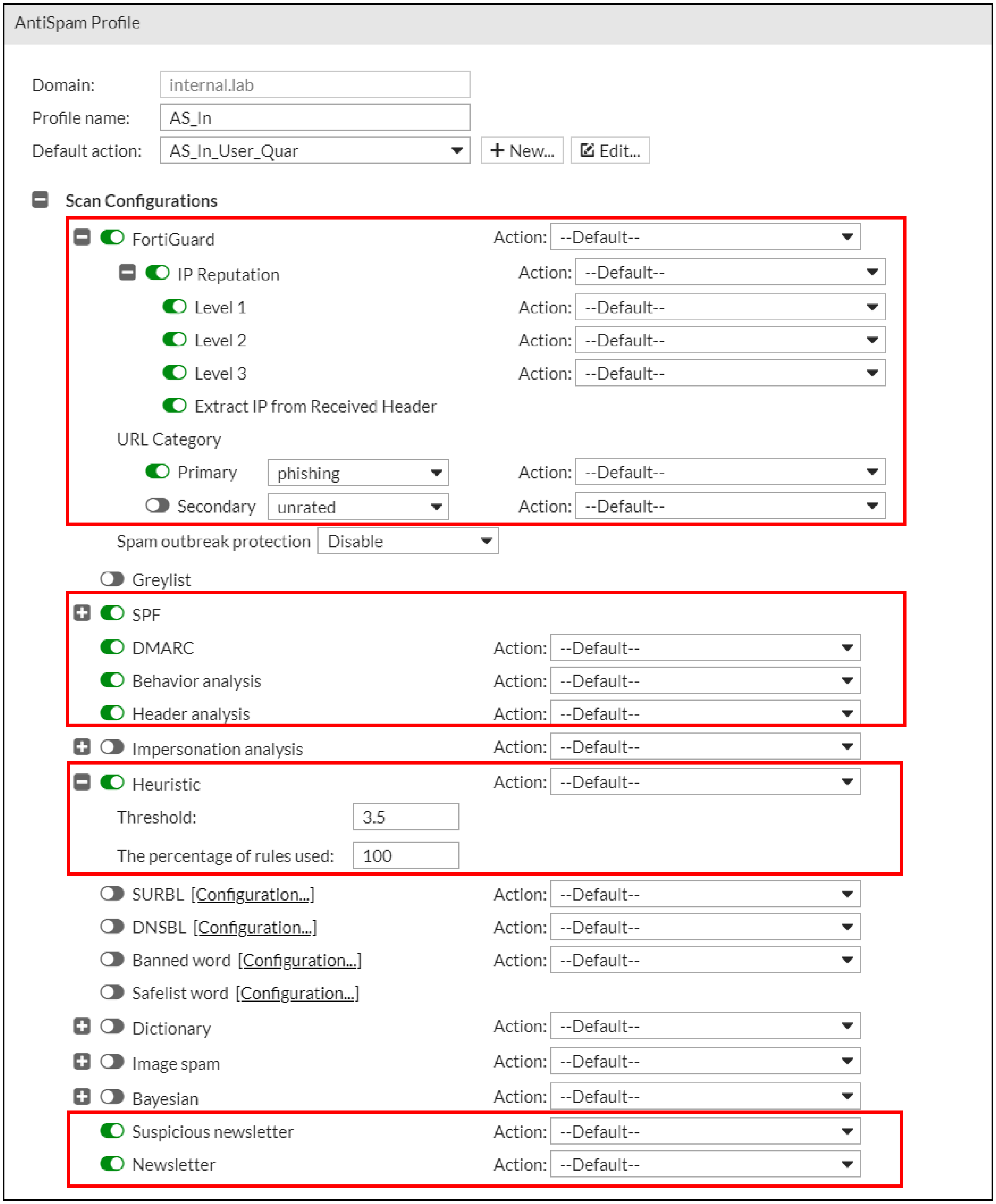
Field	Value
Domain	internal.lab
Profile name	AS_In
Default action	AS_In_User_Quar

4. Click **Create**.
5. In the **Domain** drop-down list, select **internal.lab**.
6. Select the **AS_In** antispam profile, and then click **Edit.**
7. Review the default settings.

   The following antispam techniques should already be enabled:

   - **FortiGuard**
   - **SPF**
8. Expand **FortiGuard**.
9. Expand **IP Reputation**, and then enable **Extract IP from Received Header**.
10. In the **URL Category** section, enable **Primary**, and then in the drop-down list, select **phishing**.
11. Enable the following antispam techniques:
    - **DMARC**
    - **Behavior analysis**
    - **Header analysis**
    - **Heuristic**
12. Expand **Heuristic**, and then in the **The percentage of rules used** field, type `100`.
13. Enable the following antispam techniques:
    - **Suspicious newsletter**
    - **Newsletter**

    Your configuration should match the following example:



AntiSpam Profile

Domain: internal.lab

Profile name: AS_In

Default action: AS_In_User_Quar

Scan Configurations

● FortiGuard		Action: --Default--
● IP Reputation		Action: --Default--
● Level 1		Action: --Default--
● Level 2		Action: --Default--
● Level 3		Action: --Default--
● Extract IP from Received Header		
URL Category		
● Primary	phishing	Action: --Default--
○ Secondary	unrated	Action: --Default--
Spam outbreak protection	Disable	
○ Greylist		
● SPF		
● DMARC		Action: --Default--
● Behavior analysis		Action: --Default--
● Header analysis		Action: --Default--
○ Impersonation analysis		Action: --Default--
● Heuristic		Action: --Default--
Threshold:	3.5	
The percentage of rules used:	100	
○ SURBL [Configuration...]		Action: --Default--
○ DNSBL [Configuration...]		Action: --Default--
○ Banned word [Configuration...]		Action: --Default--
○ Safelist word [Configuration...]		
○ Dictionary		Action: --Default--
○ Image spam		Action: --Default--
○ Bayesian		Action: --Default--
● Suspicious newsletter		Action: --Default--
● Newsletter		Action: --Default--

14. Click **OK** to save the changes.

Apply Antispam Scanning to Inbound Emails

You will apply the antispam profile to the inbound recipient policy for the `internal.lab` domain.

Take the Expert Challenge!

On IntGW FortiMail, apply the **AS_In** antispam profile and the **Resources_AS_In_User_Quar** resource profile to the inbound recipient policy for the `internal.lab` domain.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Validate the Antispam Configuration on page 91.

To apply antispam scanning to all inbound email

1. Continuing on the IntGW FortiMail management GUI, click **Policy** > **Recipient Policy** > **Inbound**.
2. In the **Domain** drop-down list, select **internal.lab**.
3. Select the recipient policy ID **1**, and then click **Edit**.
4. In the **AntiSpam** profile drop-down list, select **AS_In**.
5. In the **Resource** profile drop-down list, select **Resources_AS_In_User_Quar**.
6. Click **OK**.

Validate the Antispam Configuration

To validate your antispam settings, you will use the swaks tool on the Linux-Router VM to send spam messages to the user mailboxes in the `internal.lab` domain.

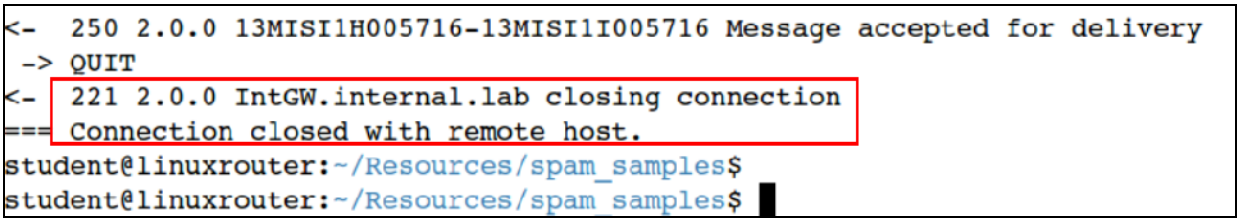
To test the antispam configuration

1. On the Linux-Client VM, open a terminal window (`Ctrl`+`Alt`+`T`).
2. Enter the following command to start an SSH connection to the Linux-Router VM:
   ```
   ssh student@10.0.1.254
   ```
3. Enter the password `password`.
4. Enter `pwd`.

   Verify that your current working directory is `/home/student`.
5. Enter the following command to change your current directory:
   ```
   cd Resources/spam_samples
   ```
6. Enter the following swaks command to generate the spam emails:
   ```
   for ii in `ls`; do swaks -s 10.0.1.11 -f spam@external.lab -t user1@internal.lab -d
       $ii; done
   ```

A copy of the swaks command is in the `commands.txt` file, which is located in the **Resources** folder on the Linux-Client desktop.

Wait until all the spam emails are sent. This could take up to 5 minutes.

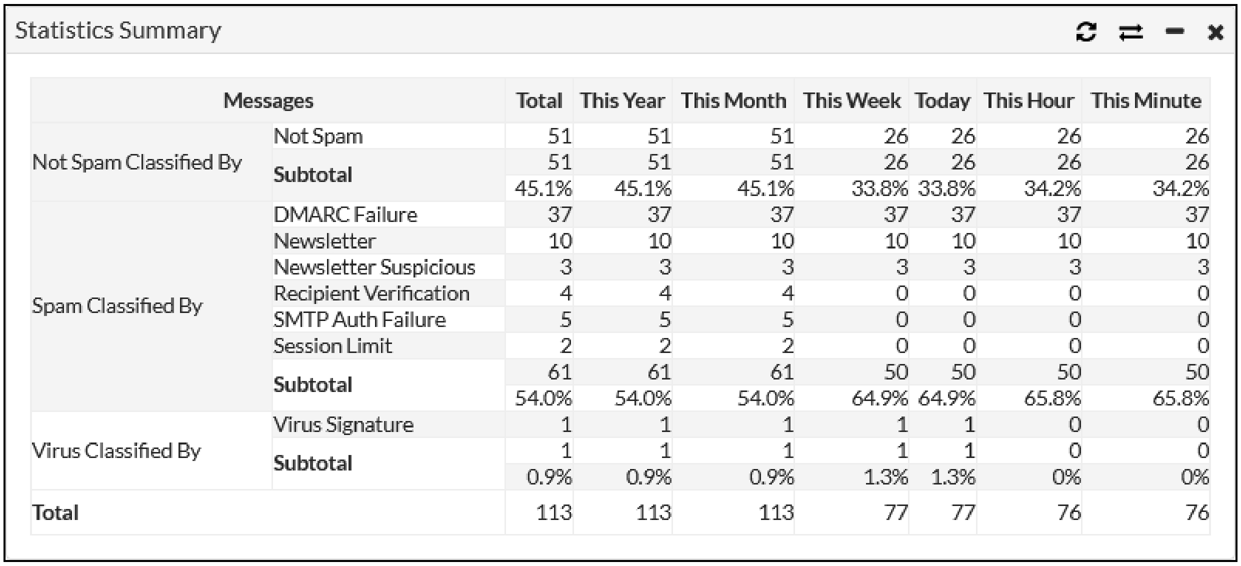


```
<-  250 2.0.0 13MISI1H005716-13MISI1I005716 Message accepted for delivery
 -> QUIT
<-  221 2.0.0 IntGW.internal.lab closing connection
=== Connection closed with remote host.
student@linuxrouter:~/Resources/spam_samples$
student@linuxrouter:~/Resources/spam_samples$ █
```

7. Close the terminal window.

To monitor the logs

1. Return to the IntGW FortiMail management GUI, and then click **Dashboard** > **Status**.
2. Review the **Statistics Summary** widget.



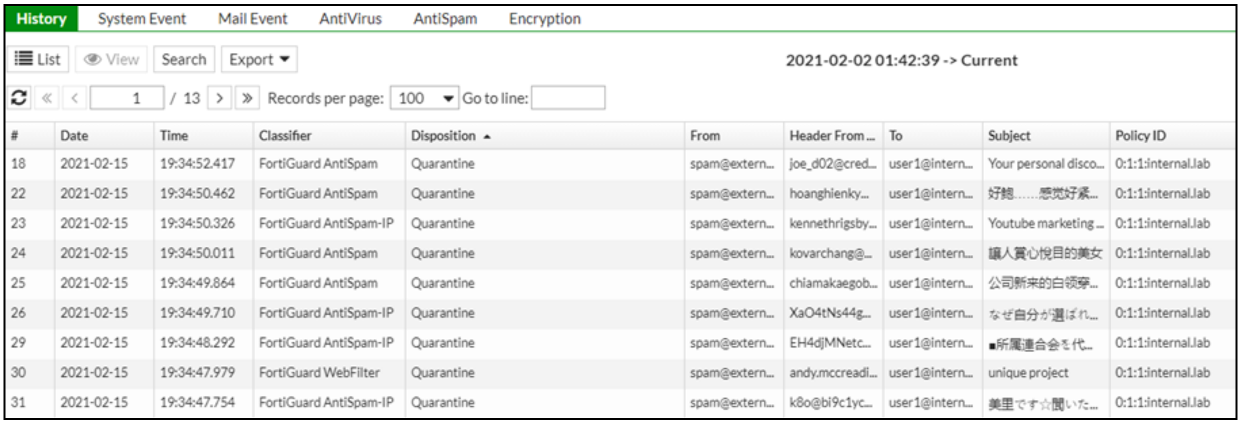
Statistics Summary

Messages		Total	This Year	This Month	This Week	Today	This Hour	This Minute
Not Spam Classified By	Not Spam	51	51	51	26	26	26	26
	Subtotal	51	51	51	26	26	26	26
		45.1%	45.1%	45.1%	33.8%	33.8%	34.2%	34.2%
Spam Classified By	DMARC Failure	37	37	37	37	37	37	37
	Newsletter	10	10	10	10	10	10	10
	Newsletter Suspicious	3	3	3	3	3	3	3
	Recipient Verification	4	4	4	0	0	0	0
	SMTP Auth Failure	5	5	5	0	0	0	0
	Session Limit	2	2	2	0	0	0	0
	Subtotal	61	61	61	50	50	50	50
		54.0%	54.0%	54.0%	64.9%	64.9%	65.8%	65.8%
Virus Classified By	Virus Signature	1	1	1	1	1	0	0
	Subtotal	1	1	1	1	1	0	0
		0.9%	0.9%	0.9%	1.3%	1.3%	0%	0%
Total		113	113	113	77	77	76	76

You can see current information about the total number of emails received, the percentage of spam detected, and the type of antispam technique used to detect most of the spam.

3. Click **Monitor** > **Log** > **History**.

   You should see all the history logs associated with the recently caught spam email messages.



2021-02-02 01:42:39 -> Current

#	Date	Time	Classifier	Disposition	From	Header From ...	To	Subject	Policy ID
18	2021-02-15	19:34:52.417	FortiGuard AntiSpam	Quarantine	spam@extern...	joe_d02@cred...	user1@intern...	Your personal disco...	0:1:1:internal.lab
22	2021-02-15	19:34:50.462	FortiGuard AntiSpam	Quarantine	spam@extern...	hoanghienky...	user1@intern...	好鲍……感觉好紧...	0:1:1:internal.lab
23	2021-02-15	19:34:50.326	FortiGuard AntiSpam-IP	Quarantine	spam@extern...	kennethrigsby...	user1@intern...	Youtube marketing ...	0:1:1:internal.lab
24	2021-02-15	19:34:50.011	FortiGuard AntiSpam	Quarantine	spam@extern...	kovarchang@...	user1@intern...	讓人賞心悅目的美女	0:1:1:internal.lab
25	2021-02-15	19:34:49.864	FortiGuard AntiSpam	Quarantine	spam@extern...	chiamakaegob...	user1@intern...	公司新来的白领穿...	0:1:1:internal.lab
26	2021-02-15	19:34:49.710	FortiGuard AntiSpam-IP	Quarantine	spam@extern...	XaO4tNs44g...	user1@intern...	なぜ自分が選ばれ...	0:1:1:internal.lab
29	2021-02-15	19:34:48.292	FortiGuard AntiSpam-IP	Quarantine	spam@extern...	EH4djMNetc...	user1@intern...	■所属連合会を代...	0:1:1:internal.lab
30	2021-02-15	19:34:47.979	FortiGuard WebFilter	Quarantine	spam@extern...	andy.mccreadi...	user1@intern...	unique project	0:1:1:internal.lab
31	2021-02-15	19:34:47.754	FortiGuard AntiSpam-IP	Quarantine	spam@extern...	k8o@bi9c1yc...	user1@intern...	美里です☆聞いた...	0:1:1:internal.lab

4. Click the **Session ID** link of a history log entry, and then review the related antispam log for the session.
5. Log out of the IntGW FortiMail management GUI.

Exercise 2: Scanning Outgoing Email for Spam

In this exercise, you will configure outbound antispam scanning on IntGW FortiMail. Then, you will test the configuration by sending an outbound email containing a banned word.

Configure an Outbound Antispam Profile

You will configure an antispam profile, and then apply that profile to an outbound recipient policy. In this profile configuration, you will enable banned words for FortiMail to scan for in outbound emails.

Take the Expert Challenge!

On IntGW FortiMail, create a new antispam profile and name it `AS_Out`.

The antispam profile should be available for the `internal.lab` domain only.

The antispam profile should use the **Reject_Outbound** action profile.

In the antispam profile, configure banned word scanning. Choose your own words and email locations (body, subject, or both).

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

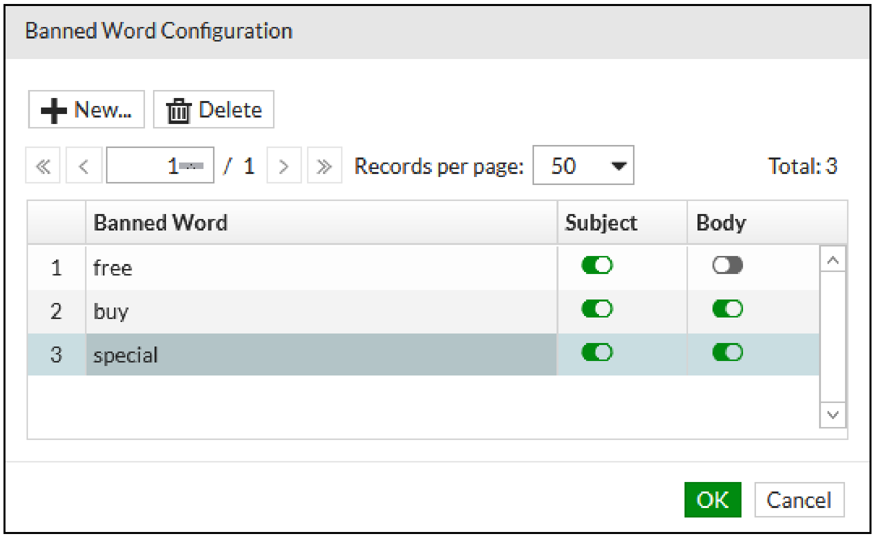
After you complete the challenge, see Apply Antispam Scanning to Outbound Emails on page 95.

To configure an outbound antispam profile

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Profile** > **AntiSpam** > **AntiSpam**.
3. Click **New**.
4. Configure a new antispam profile using the following values:

Field	Value
Domain	internal.lab
Profile name	AS_Out
Default action	Reject_Outbound

5. Enable **Banned word**.
6. Click **Configuration**.
7. Add some words to include in your banned word list—for each word, select whether FortiMail will scan the subject, body, or both, as shown in the following example:



Banned Word Configuration

	Banned Word	Subject	Body
1	free	●	○
2	buy	●	●
3	special	●	●

8. Click **OK**.
9. Click **Create**.

Apply Antispam Scanning to Outbound Emails

You will apply antispam scanning to all outbound email from the `internal.lab` domain.

To apply antispam scanning to outbound email

1. Continuing on the IntGW FortiMail management GUI, click **Policy** > **Recipient Policy** > **Outbound**.
2. Select policy ID **2**, and then click **Edit**.
3. In the **Profiles** section, in the **AntiSpam** drop-down list, select **AS_Out**.
4. Click **OK**.

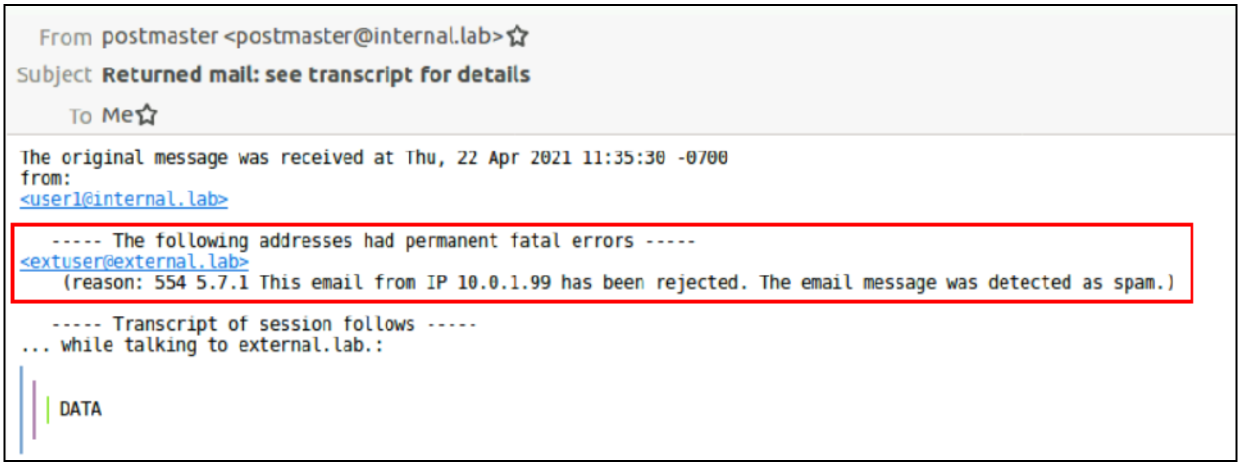
Validate the Antispam Configuration

You will validate the antispam configuration by sending an outbound email, containing one of the banned words you configured in the previous task, from the `internal.lab` domain. You will also monitor the logs on IntGW FortiMail.

To verify the antispam configuration

1. On the Linux-Client VM, open the Mozilla Thunderbird client.
2. Compose a new email message to `extuser@external.lab` containing one of the banned words you configured in the previous task.

   You should receive a delivery status notification (DSN) message.
3. Open the DSN message, and then review the transcript details.



From postmaster <postmaster@internal.lab>

Subject **Returned mail: see transcript for details**

To Me

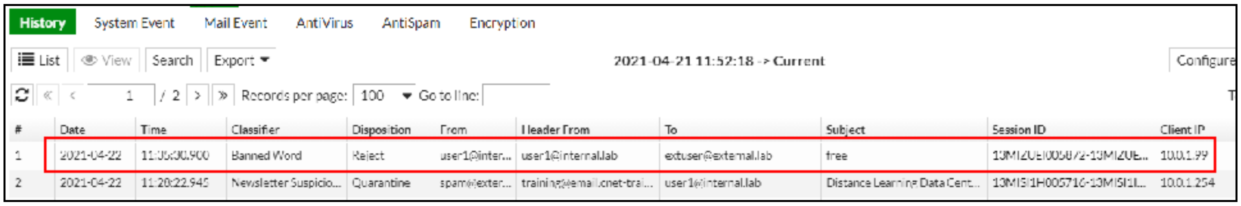
```
The original message was received at Thu, 22 Apr 2021 11:35:30 -0700
from:
<user1@internal.lab>

   ----- The following addresses had permanent fatal errors -----
<extuser@external.lab>
    (reason: 554 5.7.1 This email from IP 10.0.1.99 has been rejected. The email message was detected as spam.)

   ----- Transcript of session follows -----
... while talking to external.lab.:

DATA
```

4. Close Thunderbird.

To monitor the logs

1. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

   The first entry in the **History** log should correspond to the rejected email message.



#	Date	Time	Classifier	Disposition	From	Header From	To	Subject	Session ID	Client IP
1	2021-04-22	11:35:30.900	Banned Word	Reject	user1@inter...	user1@internal.lab	extuser@external.lab	free	13MI2UE1005872-13MI2UE...	10.0.1.99
2	2021-04-22	11:20:22.945	Newsletter Suspicio...	Quarantine	spam@exter...	training@email.cnet-trai...	user1@internal.lab	Distance Learning Data Cent...	13MI3I1H005716-13MI3I1I...	10.0.1.254

2. Review the log, and verify that the appropriate action was applied to the outbound email message.
3. Click the **Session ID** link to review the cross-search results for more details.
4. Log out of the IntGW FortiMail management GUI.

Exercise 3: Managing User Quarantine

An email user can access their list of quarantined emails using either POP3 or webmail. In this exercise, you will access the `user1@internal.lab` quarantine mailbox on the IntGW FortiMail webmail GUI. You will also configure quarantine report scheduling and generate an on-demand quarantine report. Then, you will explore the options available in a quarantine report.

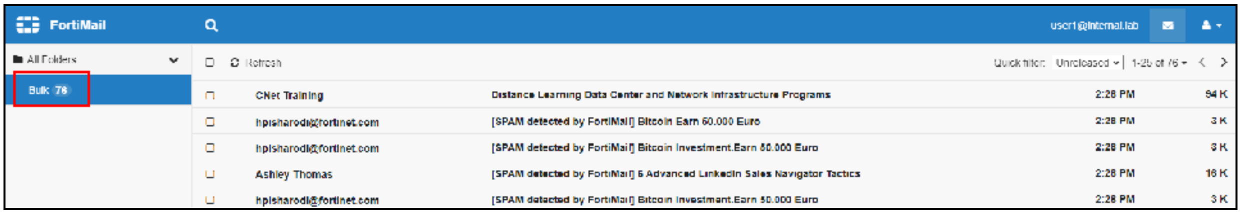
Access a Personal Quarantine

In the previous lab exercise, you selected user quarantine as an action in the antispam action profiles. All the spam emails from the previous exercise were redirected to their personal quarantine. Now, you will access the personal quarantine mailbox of user1.

To access a personal quarantine

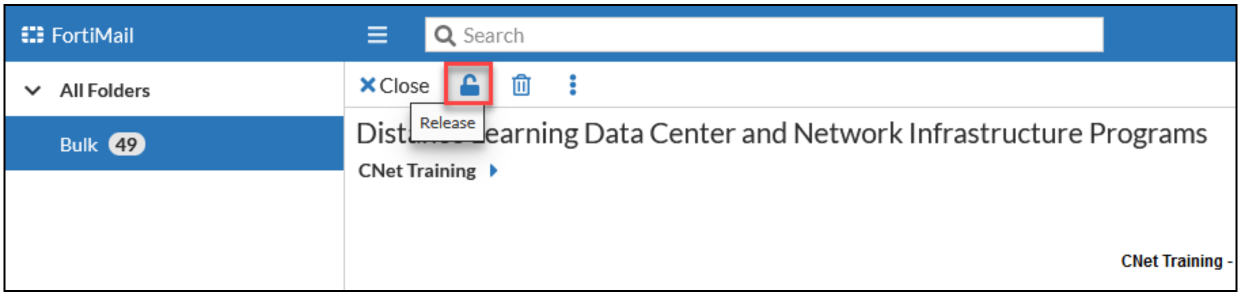
1. On the IntGW FortiMail webmail GUI, log in with the username `user1` and password `fortinet`.

   You should see all the quarantined spam messages in the **Bulk** folder.



CNet Training	Distance Learning Data Center and Network Infrastructure Programs	2:28 PM	94 K
hpisharodi@fortinet.com	[SPAM detected by FortiMail] Bitcoin Earn 60.000 Euro	2:28 PM	3 K
hpisharodi@fortinet.com	[SPAM detected by FortiMail] Bitcoin Investment.Earn 80.000 Euro	2:28 PM	3 K
Ashley Thomas	[SPAM detected by FortiMail] 6 Advanced LinkedIn Sales Navigator Tactics	2:28 PM	16 K
hpisharodi@fortinet.com	[SPAM detected by FortiMail] Bitcoin Investment.Earn 50.000 Euro	2:28 PM	3 K

2. Open one of the quarantined emails, and then click **Release**.



Dist... Learning Data Center and Network Infrastructure Programs
CNet Training
CNet Training -

   Once released, the message is delivered to the user's inbox. To verify this, you can view the message in the Thunderbird client.

3. Delete a quarantined email message.
4. Log out of the IntGW FortiMail webmail GUI.

Configure Quarantine Reports

You will configure quarantine reports, which will allow recipients to delete or release quarantined email messages.

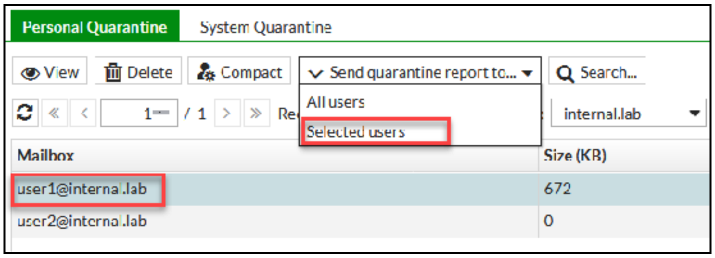
To configure quarantine reports

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Security** > **Quarantine** > **Quarantine Report**.
3. In the **Schedule** section, enable the following days and times only:
   - **These hours: 9:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00**
   - **These days: Mon Tue Wed Thu Fri**
4. In the **Quarantine report template** drop-down list, select **default-with-icons**.
5. Click **Apply** to save the changes.

FortiMail automatically generates quarantine reports on schedule only for accounts that have quarantined email. If a user's quarantine account is empty, a report is not generated for that account.

To generate quarantine reports on demand

1. Continuing on the IntGW FortiMail management GUI, click **Monitor** > **Quarantine** > **Personal Quarantine**.
2. Select the **user1@internal.lab** mailbox.
3. In the **Send quarantine report to** drop-down list, select **Selected users**.



Mailbox	Size (KB)
user1@internal.lab	672
user2@internal.lab	0

4. In the **For the past hours** field, type `120`.
5. Click **OK**.
6. Log out of the IntGW FortiMail management GUI.

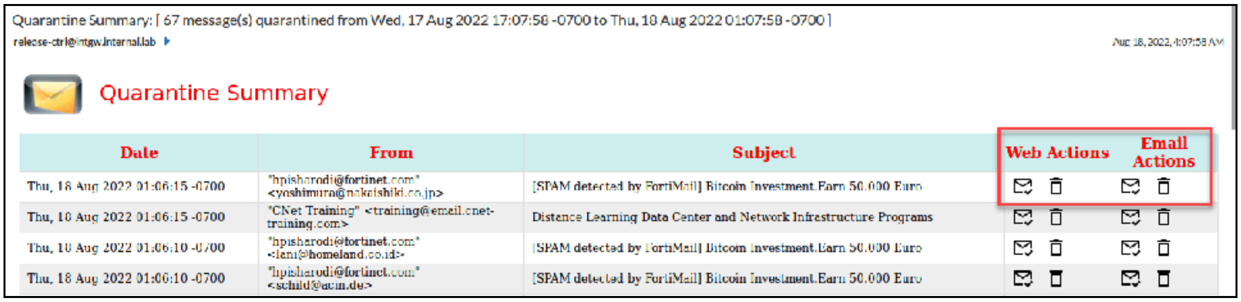
To view the quarantine report

1. On the IntSRV FortiMail webmail GUI, log in with the username `user1` and password `fortinet`.
2. Open the quarantine report.

   The subject should contain the words **Quarantine Summary**.

3. Review the **Web Actions** and **Email Actions** columns.

   You can release or delete each quarantined email using these actions.



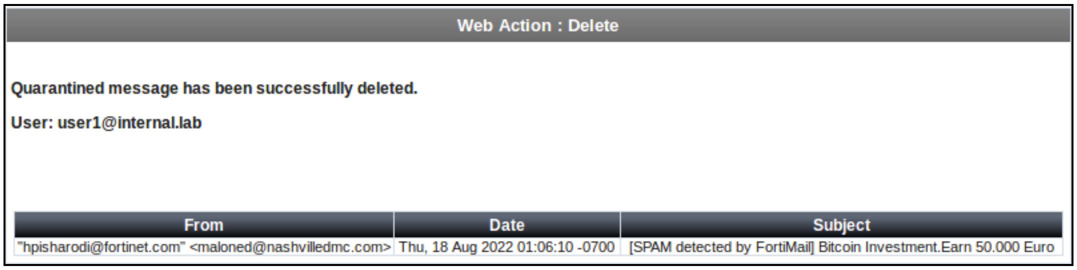
Quarantine Summary: [67 message(s) quarantined from Wed, 17 Aug 2022 17:07:58 -0700 to Thu, 18 Aug 2022 01:07:58 -0700]
release-ctrl@intgw.internal.lab
Aug 18, 2022, 4:07:58 AM

Quarantine Summary

Date	From	Subject	Web Actions	Email Actions
Thu, 18 Aug 2022 01:06:15 -0700	"hpisharodi@fortinet.com" <yoshimura@nakaishiki.co.jp>	[SPAM detected by FortiMail] Bitcoin Investment.Earn 50.000 Euro	✉ 🗑	✉ 🗑
Thu, 18 Aug 2022 01:06:15 -0700	"CNet Training" <training@email.cnet-training.com>	Distance Learning Data Center and Network Infrastructure Programs	✉ 🗑	✉ 🗑
Thu, 18 Aug 2022 01:06:10 -0700	"hpisharodi@fortinet.com" <lani@homeland.co.id>	[SPAM detected by FortiMail] Bitcoin Investment.Earn 50.000 Euro	✉ 🗑	✉ 🗑
Thu, 18 Aug 2022 01:06:10 -0700	"hpisharodi@fortinet.com" <schild@acin.de>	[SPAM detected by FortiMail] Bitcoin Investment.Earn 50.000 Euro	✉ 🗑	✉ 🗑

4. Click the web delete action for one of the spam emails.

   You are redirected to the deletion confirmation page.



Web Action : Delete

Quarantined message has been successfully deleted.

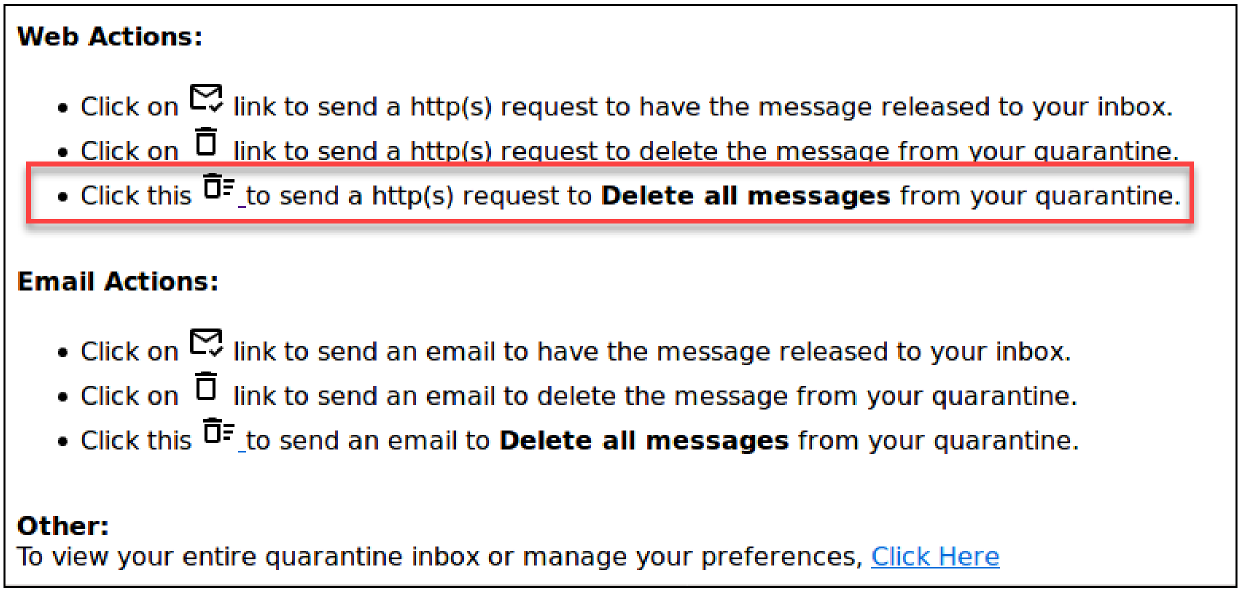
User: user1@internal.lab

From	Date	Subject
"hpisharodi@fortinet.com" <maloned@nashvilledmc.com>	Thu, 18 Aug 2022 01:06:10 -0700	[SPAM detected by FortiMail] Bitcoin Investment.Earn 50.000 Euro

You can perform the web actions using most email clients as long as they support the clicking of web links in emails. This is disabled in the lab so if you use Thunderbird you must copy and paste the links from the quarantine report into a browser tab.

5. Return to the FortiMail webmail GUI, and then scroll down to the end of the quarantine report.

   The end of the quarantine report contains options to delete all quarantined emails using either an email or a web action.



Web Actions:

- Click on ✉ link to send a http(s) request to have the message released to your inbox.
- Click on 🗑 link to send a http(s) request to delete the message from your quarantine.
- Click this 🗑≡ to send a http(s) request to **Delete all messages** from your quarantine.

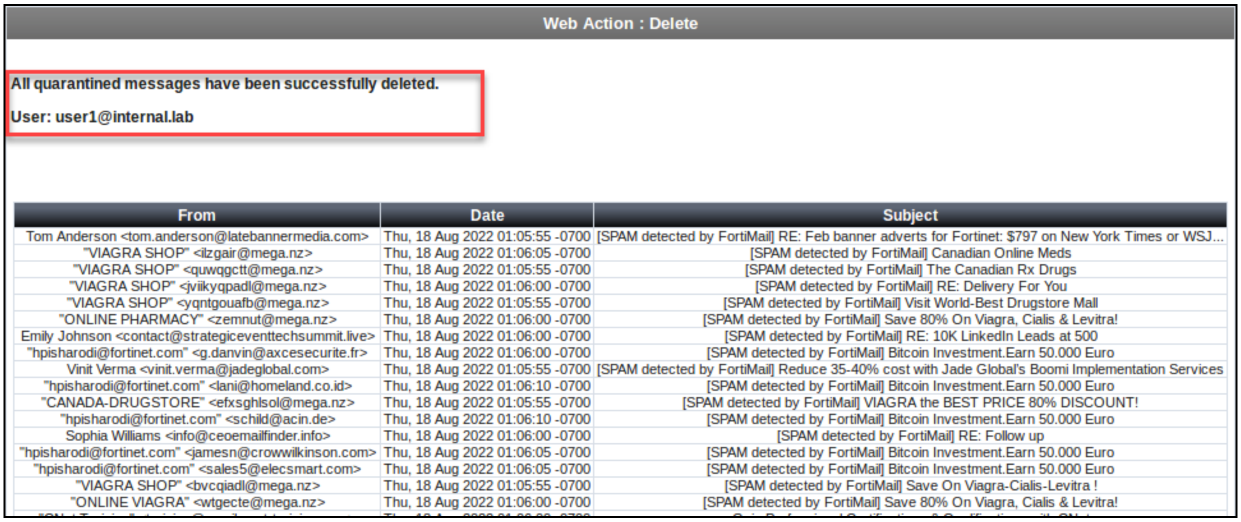
Email Actions:

- Click on ✉ link to send an email to have the message released to your inbox.
- Click on 🗑 link to send an email to delete the message from your quarantine.
- Click this 🗑≡ to send an email to **Delete all messages** from your quarantine.

Other:
To view your entire quarantine inbox or manage your preferences, Click Here

6. Select the web action to delete all the quarantined email messages for `user1@internal.lab`.

   You are redirected to the deletion confirmation page.



All quarantined messages have been successfully deleted.

User: user1@internal.lab

From	Date	Subject
Tom Anderson <tom.anderson@latebannermedia.com>	Thu, 18 Aug 2022 01:05:55 -0700	[SPAM detected by FortiMail] RE: Feb banner adverts for Fortinet: $797 on New York Times or WSJ...
"VIAGRA SHOP" <ilzgair@mega.nz>	Thu, 18 Aug 2022 01:06:05 -0700	[SPAM detected by FortiMail] Canadian Online Meds
"VIAGRA SHOP" <quwqgctt@mega.nz>	Thu, 18 Aug 2022 01:05:55 -0700	[SPAM detected by FortiMail] The Canadian Rx Drugs
"VIAGRA SHOP" <jviikyqpadl@mega.nz>	Thu, 18 Aug 2022 01:06:00 -0700	[SPAM detected by FortiMail] RE: Delivery For You
"VIAGRA SHOP" <yqntgouafb@mega.nz>	Thu, 18 Aug 2022 01:05:55 -0700	[SPAM detected by FortiMail] Visit World-Best Drugstore Mall
"ONLINE PHARMACY" <zemnut@mega.nz>	Thu, 18 Aug 2022 01:06:00 -0700	[SPAM detected by FortiMail] Save 80% On Viagra, Cialis & Levitra!
Emily Johnson <contact@strategiceventtechsummit.live>	Thu, 18 Aug 2022 01:06:00 -0700	[SPAM detected by FortiMail] RE: 10K LinkedIn Leads at 500
"hpisharodi@fortinet.com" <g.danvin@axcesecurite.fr>	Thu, 18 Aug 2022 01:06:00 -0700	[SPAM detected by FortiMail] Bitcoin Investment.Earn 50.000 Euro
Vinit Verma <vinit.verma@jadeglobal.com>	Thu, 18 Aug 2022 01:05:55 -0700	[SPAM detected by FortiMail] Reduce 35-40% cost with Jade Global's Boomi Implementation Services
"hpisharodi@fortinet.com" <lani@homeland.co.id>	Thu, 18 Aug 2022 01:06:10 -0700	[SPAM detected by FortiMail] Bitcoin Investment.Earn 50.000 Euro
"CANADA-DRUGSTORE" <efxsghlsol@mega.nz>	Thu, 18 Aug 2022 01:05:55 -0700	[SPAM detected by FortiMail] VIAGRA the BEST PRICE 80% DISCOUNT!
"hpisharodi@fortinet.com" <schild@acin.de>	Thu, 18 Aug 2022 01:06:10 -0700	[SPAM detected by FortiMail] Bitcoin Investment.Earn 50.000 Euro
Sophia Williams <info@ceoemailfinder.info>	Thu, 18 Aug 2022 01:06:00 -0700	[SPAM detected by FortiMail] RE: Follow up
"hpisharodi@fortinet.com" <jamesn@crowwilkinson.com>	Thu, 18 Aug 2022 01:06:05 -0700	[SPAM detected by FortiMail] Bitcoin Investment.Earn 50.000 Euro
"hpisharodi@fortinet.com" <sales5@elecsmart.com>	Thu, 18 Aug 2022 01:06:05 -0700	[SPAM detected by FortiMail] Bitcoin Investment.Earn 50.000 Euro
"VIAGRA SHOP" <bvcqiadl@mega.nz>	Thu, 18 Aug 2022 01:05:55 -0700	[SPAM detected by FortiMail] Save On Viagra-Cialis-Levitra !
"ONLINE VIAGRA" <wtgecte@mega.nz>	Thu, 18 Aug 2022 01:06:00 -0700	[SPAM detected by FortiMail] Save 80% On Viagra, Cialis & Levitra!

7. Close the browser on the FortiMail webmail GUI.

Exercise 4: Configuring Impersonation Analysis

In this exercise, you will configure FortiMail to inspect all emails designed to impersonate critical personnel and take appropriate action on these types of messages.

Configure an Impersonation Analysis Profile

You will configure an impersonation analysis profile with a display name mapped to an email address, and then apply that profile to an inbound antispam profile that you configured in a previous lab exercise.

Take the Expert Challenge!

On IntGW FortiMail, create a new impersonation analysis profile, and name it `Impersonation`.

The profile should be available for the `internal.lab` domain only.

Configure a wildcard match rule for the `Corporate CEO` display name and `ceo@internal.lab` email address.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Apply Impersonation Analysis to an Antispam Profile on page 102.

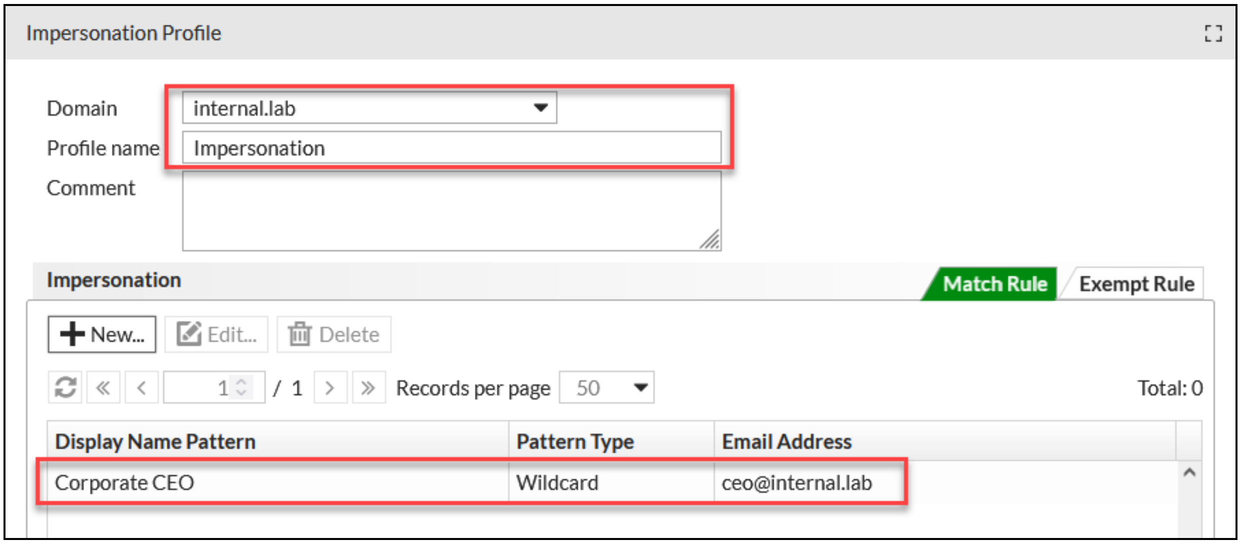
To configure an impersonation analysis profile

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Profile** > **Antispam** > **Impersonation**.
3. Click **New** to create a new impersonation profile.
4. In the **Profile Name** field, type `Impersonation`.
5. In the **Domain** drop-down list, select **internal.lab**.
6. Select **Match Rule**.
7. In the **Impersonation** section, click **New**.
8. Configure a new entry using the following values:

Field	Value
Display name pattern	Corporate CEO
Pattern type	Wildcard
Email address	ceo@internal.lab

9. Click **Create**.

   Your configuration should match the following example:



Impersonation Profile

Domain: internal.lab

Profile name: Impersonation

Comment:

Impersonation

Display Name Pattern	Pattern Type	Email Address
Corporate CEO	Wildcard	ceo@internal.lab

10. Click **Create**.

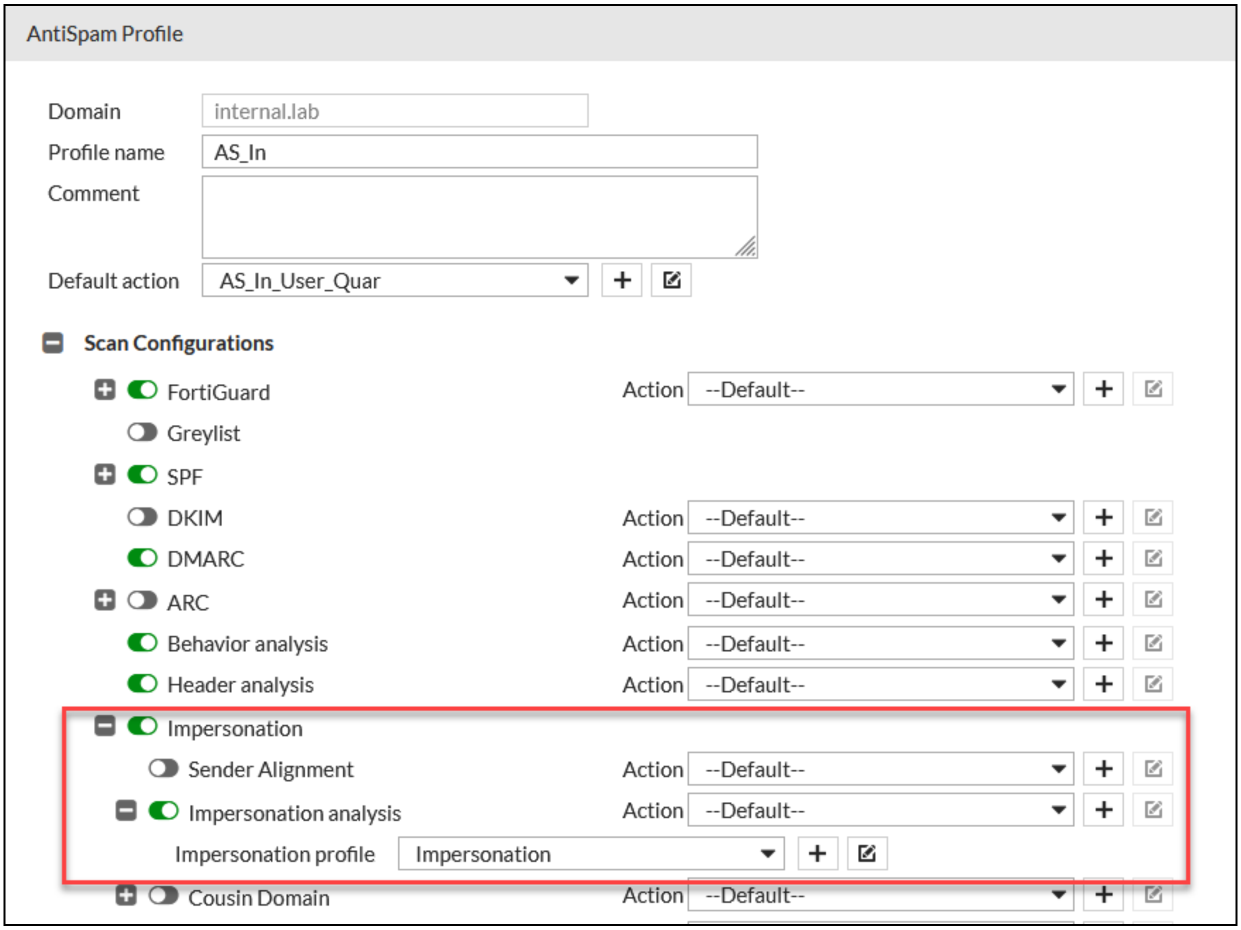
Apply Impersonation Analysis to an Antispam Profile

You will enable impersonation analysis in an inbound antispam profile.

To apply impersonation to an antispam profile

1. Continuing on the IntGW FortiMail management GUI, click **Profile** > **Antispam** > **Antispam**.
2. In the **Domain** drop-down list, select **internal.lab**.
3. Edit the **AS_In** profile.
4. Enable, and then expand **Impersonation**.
5. Enable, and then expand **Impersonation analysis**.
6. In the **Impersonation profile** drop-down list, select **Impersonation**.

   Your configuration should match the following example:



AntiSpam Profile

Domain	internal.lab
Profile name	AS_In
Comment	
Default action	AS_In_User_Quar

Scan Configurations

● FortiGuard	Action --Default--
○ Greylist	
● SPF	
○ DKIM	Action --Default--
● DMARC	Action --Default--
○ ARC	Action --Default--
● Behavior analysis	Action --Default--
● Header analysis	Action --Default--
● Impersonation	
○ Sender Alignment	Action --Default--
● Impersonation analysis	Action --Default--
Impersonation profile	Impersonation
○ Cousin Domain	Action --Default--

7. Click **OK**.

The **AS_In** antispam profile is already applied to the inbound recipient policy ID 1 for the `internal.lab` domain.

Validate Impersonation Analysis

You will validate your configuration by sending an impersonation email from the Linux-Router VM.

To test impersonation

1. On the Linux-Client VM, open a terminal window (`Ctrl+Alt+T`).
2. Enter the following command to start an SSH connection to the Linux-Router VM:

```
ssh student@10.0.1.254
```

3. Enter the password `password`.
4. Enter `pwd`.

   Verify that your current working directory is `/home/student`.

5. Enter the following swaks command to impersonate a high-target user:

```
swaks -f extuser@external.lab -t user1@internal.lab -s 10.0.1.11 --header-From
    "Corporate CEO <extuser@external.lab>"
```

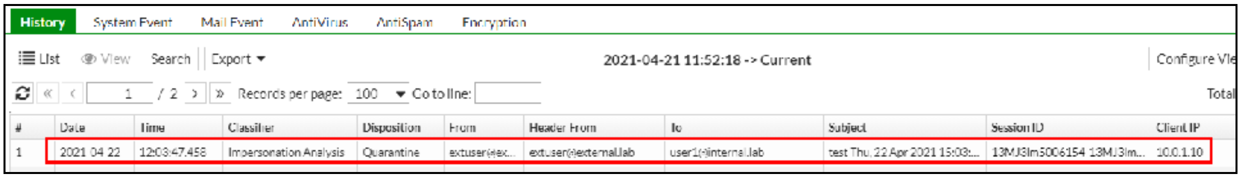
A copy of the swaks command is in the `commands.txt` file, which is located in the **Resources** folder on the Linux-Client desktop.

6. Close the terminal window.

To review the logs

1. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

   The first entry in the **History** log should correspond to the email that was sent. Notice the values in the **Classifier** and **Disposition** columns.



1 / 2

2021-04-21 11:52:18 -> Current

#	Date	Time	Classifier	Disposition	From	Header From	To	Subject	Session ID	Client IP
1	2021 04 22	12:03:47.458	Impersonation Analysis	Quarantine	extuser@ex...	extuser@external.lab	user1@internal.lab	test Thu, 22 Apr 2021 15:03:...	13MJ3Im5006154 13MJ3Im...	10.0.1.10

2. Click the **Session ID** link to retrieve the cross-search results.
3. Review the antispam logs related to the session.
4. Log out of the IntGW FortiMail management GUI.

Exercise 5: Configuring Bounce Verification

In this exercise, you will configure bounce verification to block backscatter spam.

Disable Recipient Address Verification

You will disable recipient address verification on IntGW FortiMail so that you can test backscatter spam.

To disable recipient address verification

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Domain & User** > **Domain** > **Domain**.
3. Edit **internal.lab**.
4. Expand **Recipient Address Verification**.
5. Select **Disable**.
6. Click **OK**.
7. Log out of the IntGW FortiMail management GUI.

Send Backscatter Spam

You will send a backscatter spam email from the Linux-Router VM. You will use the backscatter target email address in the `MAIL FROM:` field, and use an invalid recipient address in the `RCPT TO:` field. Then, you will review the spam email and identify the spam content in the DSN message.

To send backscatter spam

1. On the Linux-Client VM, open a terminal window (`Ctrl`+`Alt`+`T`).
2. Enter the following command to start an SSH connection to the Linux-Router VM:
   ```
   ssh student@10.0.1.254
   ```
3. Enter the password `password`.
4. Enter `pwd`.

   Verify that your current working directory is `/home/student`.
5. Enter the following swaks command to send an email to an invalid user:
   ```
   swaks -f user1@internal.lab -t nonexistent@internal.lab -s intgw.internal.lab --ehlo
       linux.internal.lab --body 'buy while supplies last'
   ```

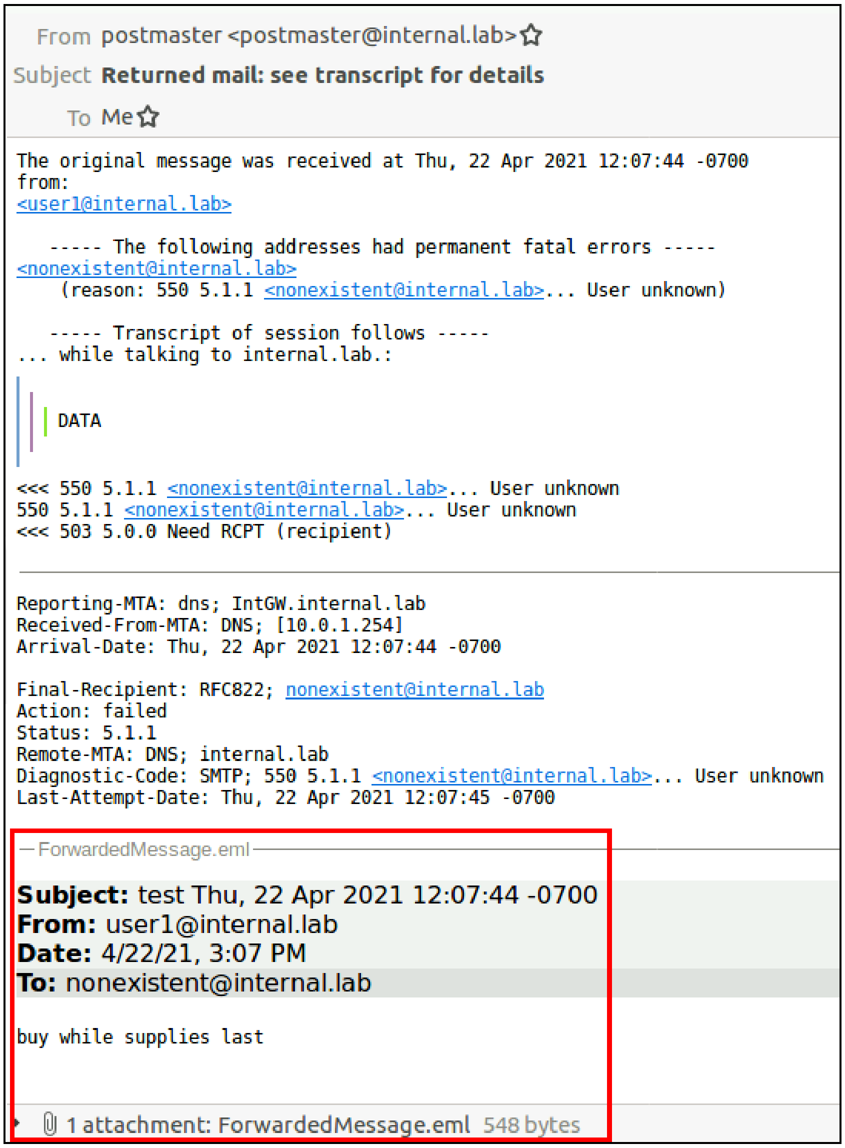
A copy of the swaks command is in the `commands.txt` file, which is located in the **Resources** folder on the Linux-Client desktop.

6. Close the terminal window.

To verify the DSN email

1. Continuing on the Linux-Client VM, open Thunderbird.
2. Open the email with **Returned mail: see transcript for details** in the subject line.

   The spam is attached to the DSN email.



```
From postmaster <postmaster@internal.lab>
Subject Returned mail: see transcript for details
To Me

The original message was received at Thu, 22 Apr 2021 12:07:44 -0700
from:
<user1@internal.lab>

   ----- The following addresses had permanent fatal errors -----
<nonexistent@internal.lab>
    (reason: 550 5.1.1 <nonexistent@internal.lab>... User unknown)

   ----- Transcript of session follows -----
... while talking to internal.lab.:

DATA

<<< 550 5.1.1 <nonexistent@internal.lab>... User unknown
550 5.1.1 <nonexistent@internal.lab>... User unknown
<<< 503 5.0.0 Need RCPT (recipient)

Reporting-MTA: dns; IntGW.internal.lab
Received-From-MTA: DNS; [10.0.1.254]
Arrival-Date: Thu, 22 Apr 2021 12:07:44 -0700

Final-Recipient: RFC822; nonexistent@internal.lab
Action: failed
Status: 5.1.1
Remote-MTA: DNS; internal.lab
Diagnostic-Code: SMTP; 550 5.1.1 <nonexistent@internal.lab>... User unknown
Last-Attempt-Date: Thu, 22 Apr 2021 12:07:45 -0700

ForwardedMessage.eml
Subject: test Thu, 22 Apr 2021 12:07:44 -0700
From: user1@internal.lab
Date: 4/22/21, 3:07 PM
To: nonexistent@internal.lab

buy while supplies last

1 attachment: ForwardedMessage.eml 548 bytes
```

3. Close Thunderbird.

Configure Bounce Verification

You will configure bounce verification to detect backscatter spam and discard it.

Take the Expert Challenge!

On IntSRV FortiMail, configure bounce verification to discard all backscatter spam. You can use `internal` as a key.

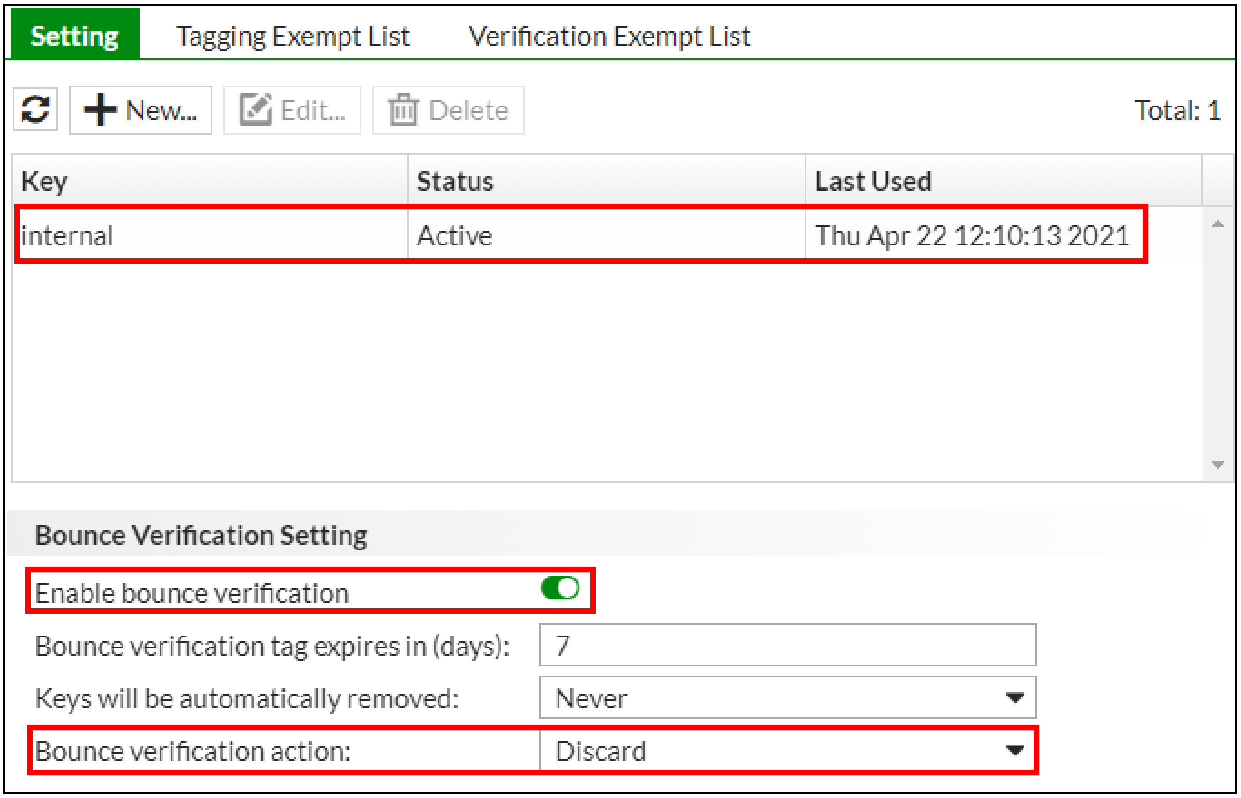
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Validate Bounce Verification on page 108.

To configure bounce verification

1. On the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Security** > **Bounce Verification** > **Setting**.
3. Click **New**.
4. In the **Key name** field, type `internal`.
5. In the **Status** drop-down list, select **Active**.
6. Click **Create**.
7. Click **Enable bounce verification**.
8. In the **Bounce verification action** drop-down list, select **Discard**.

   Your configuration should match the following example:



Key	Status	Last Used
internal	Active	Thu Apr 22 12:10:13 2021

Bounce Verification Setting

Enable bounce verification: enabled

Bounce verification tag expires in (days): 7

Keys will be automatically removed: Never

Bounce verification action: Discard

9. Click **Apply**.

Validate Bounce Verification

You will send a backscatter spam email to validate your bounce verification configuration, and then review the logs on IntSRV FortiMail.

To send backscatter spam

1. Return to the Linux-Client VM, and then open a terminal window (`Ctrl+Alt+T`).
2. Enter the following command to start an SSH connection to the Linux-Router VM:

```
ssh student@10.0.1.254
```

3. Enter the password `password`.
4. Enter `pwd`.

   Verify that your current working directory is `/home/student`.

5. Enter the following swaks command to send the backscatter email:

```
swaks -f user1@internal.lab -t nonexistent@internal.lab -s intgw.internal.lab --ehlo
    linux.internal.lab --body 'buy while supplies last'
```

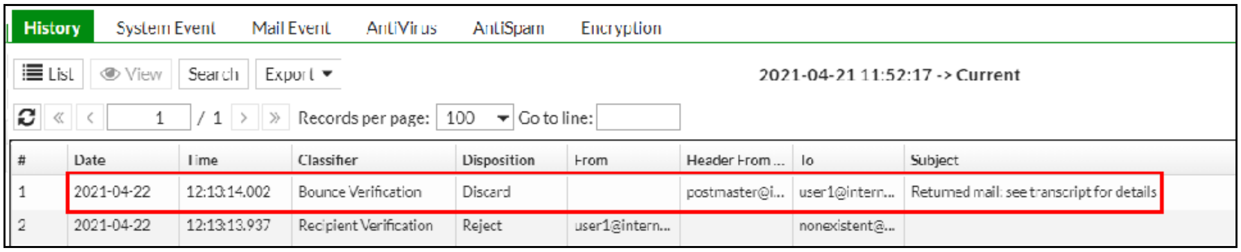
A copy of the swaks command is in the `commands.txt` file, which is located in the **Resources** folder on the Linux-Client desktop.

6. Close the terminal window.

To monitor the logs

1. Return to the IntSRV FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

   The first log should correspond to the email you just sent.



2021-04-21 11:52:17 -> Current

1 / 1

#	Date	Time	Classifier	Disposition	From	Header From ...	To	Subject
1	2021-04-22	12:13:14.002	Bounce Verification	Discard		postmaster@i...	user1@intern...	Returned mail: see transcript for details
2	2021-04-22	12:13:13.937	Recipient Verification	Reject	user1@intern...		nonexistent@...	

2. Verify the **Classifier** and **Disposition**.
3. Log out of the IntSRV FortiMail management GUI.

Lab 7: Content Inspection

In this lab, you will configure a content filter to monitor email based on dictionary word scores. You will also configure the data loss prevention (DLP) feature to detect and block any outbound email that contains credit card numbers. Finally, you will configure and verify the content disarm and reconstruction (CDR) feature on FortiMail.

Objectives

- Configure a dictionary profile to monitor words using scores
- Configure a content profile to use the dictionary profile
- Apply content filtering on all inbound email
- Configure DLP to detect credit card numbers in an email body and attachments
- Apply DLP on all outbound email
- Configure CDR to detect HTML tags and URIs in an email body and attachments
- Apply CDR to all inbound email

Time to Complete

Estimated: 60 minutes

Prerequisites

Before beginning this lab, you must restore a configuration file on the `internal.lab` FortiMail VMs.

To restore a configuration file on IntSRV FortiMail

1. On the Linux-Client VM, open a new browser, and then on the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **System** > **Maintenance** > **Configuration**.
3. Click **Restore Configuration**.
4. Click **Desktop** > **Resources** > **Starting Configs** > **Lab 7** > `07_Initial_IntSRV.tgz`, and then click **Open**.
5. Click **OK**.

To restore a configuration file on IntGW FortiMail

1. On the Linux-Client VM, open a new browser tab, and then on the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **System** > **Maintenance** > **Configuration**.
3. Click **Restore Configuration**.
4. Click **Desktop** > **Resources** > **Starting Configs** > **Lab 7** > `07_Initial_IntGW.tgz`, and then click **Open**.
5. Click **OK**.
6. Wait for the VMs to finish restarting before proceeding with the exercise.

The configuration files disable bounce verification on IntSRV FortiMail and the antispam profile on IntGW FortiMail, which can potentially interfere with the content inspection testing you will do in this lab.

7. Close the browser tabs.

Exercise 1: Configuring Content Inspection

In this exercise, you will configure the content monitoring and filtering options of a content profile to scan for specific pattern occurrences in inbound emails. Then, you will configure the action to be applied after the same word occurs three times in an email.

Configure a Dictionary Profile

You will create a new dictionary profile with pattern scores. This allows FortiMail to inspect email content for multiple occurrences of a word and, if a specific number of matches are found, take appropriate action.

Take the Expert Challenge!

On IntGW FortiMail, create a new dictionary profile and name it `WordScores`.

Create a new wildcard pattern, and use the word `fortimail`.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure a Content Profile and Action on page 111.

To configure a dictionary profile

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Profile** > **Dictionary** > **Dictionary**.
3. Select the **WordScores** dictionary.
4. Click **Edit**.
5. In the **Dictionary Entries** section, click **New**.
6. Configure a dictionary entry using the following values:

Field	Value
Pattern	fortimail
Pattern type	Wildcard

7. Click **Create**.
8. Click **OK**.

Configure a Content Profile and Action

You will create a new content profile to use the dictionary profile you just created.

Take the Expert Challenge!

On IntGW FortiMail, create a new content profile and name it `CF_Dictionary`.

The profile should be available for the `internal.lab` domain only.

The profile should use the **SysQuarantine_Inbound** action profile and be set to send system quarantine emails to the **Content** folder.

The profile should use the **WordScores** dictionary profile, and trigger only after at least three occurrences of the configured pattern in an email.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Apply Content Inspection to Inbound Emails on page 113.

To configure a content profile

1. Continuing on the IntGW FortiMail management GUI, click **Profile** > **Content** > **Content.**
2. Click **New**.
3. Configure a new content profile using the following values:

Field	Value
Domain	internal.lab
Profile name	CF_Dictionary
Action	SysQuarantine_Inbound

4. Scroll down to the **Content Monitor and Filtering** section.
5. Click **New**.
6. Configure the content monitor profile using the following values:

Field	Value
Dictionary	profile
	WordScores
Minimum score	3

7. Click **Create**.
8. Click **Create**.

Configuring a **Minimum score** of 3 ensures that the action profile is applied only after **fortimail** has found three occurrences of the pattern in a single email.

To configure a content action

1. Continuing on the IntGW FortiMail management GUI, click **Profile** > **Content** > **Action**.
2. Double-click **SysQuarantine_Inbound**.
3. Configure a new content profile using the following values:

Field	Value
Final action	Enable
Final action name	System quarantine
Folder name	Content

4. Click **OK**.

Apply Content Inspection to Inbound Emails

You will apply the content profile to the inbound recipient policy ID 1 for the `internal.lab`.

To apply content inspection to inbound emails

1. Continuing on the IntGW FortiMail management GUI, click **Policy** > **Recipient Policy** > **Inbound**.
2. Under the **Domain** pull-down, select **All**.
3. Select policy ID **1**, and then click **Edit**.
4. In the **Profiles** section, in the **Content** drop-down list, select **CF_Dictionary**.
5. Click **OK**.

Validate Content Inspection

You will send an email from an `external.lab` user to an `internal.lab` user. The email will contain several instances of the configured dictionary pattern. FortiMail should detect the email because it exceeds the minimum threshold score. Then, you will review the logs generated by content inspection.

To validate content inspection

1. On the Linux-Client VM, open a new browser tab, and then on the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
2. Compose a new email to `user1@internal.lab`.

   Do not send the email yet.
3. Return to the Linux-Client VM desktop, and then browse to the folder **Resources** > **Files**.
4. Double-click the `messagebody.txt` file to open it.
5. Copy the contents of the file, return to the ExtSRV FortiMail webmail GUI, and then paste it into the body of the email.
6. Click **Send**.

The `messagebody.txt` file contains the following text:

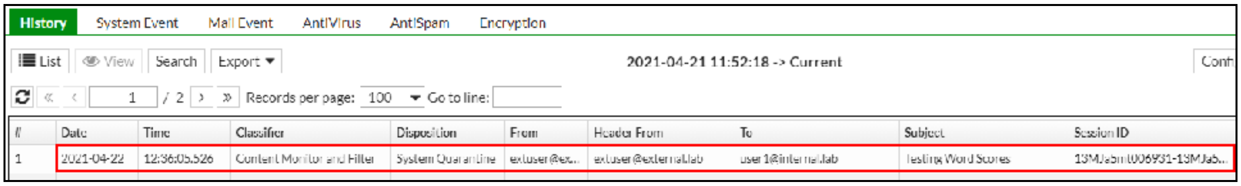
FortiMail appliances provide high-performance email routing and security by utilizing multiple high-accuracy antispam filters. As part of the Fortinet Security Fabric, FortiMail prevents your email systems from becoming threat delivery systems. FortiMail can be deployed in the cloud or on premises and gateway, inline and server modes in a range of appliance or virtual machine form factors.

To review the logs

1. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

   The first entry in the **History** logs should correspond to the email that you sent.

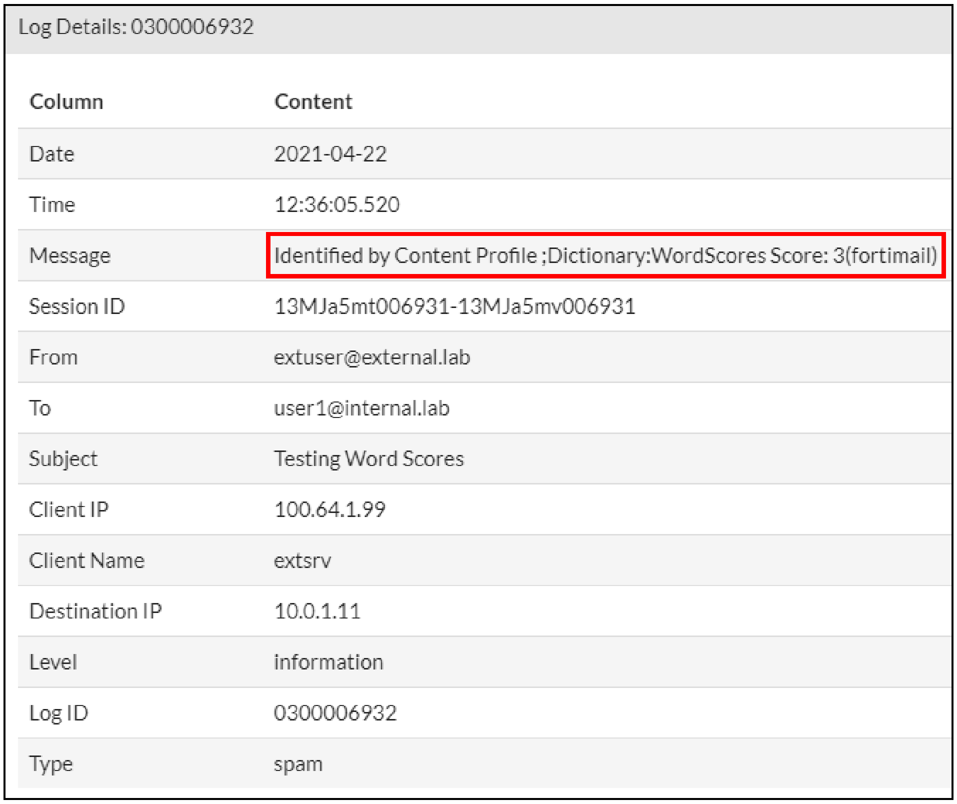
2. Verify the values in the **Classifier** and **Disposition** columns.



2021-04-21 11:52:18 -> Current

#	Date	Time	Classifier	Disposition	From	Header From	To	Subject	Session ID
1	2021-04-22	12:36:05.526	Content Monitor and Filter	System Quarantine	extuser@ex...	extuser@external.lab	user1@internal.lab	Testing Word Scores	13MJa5mt006931-13MJa5...

3. Click the **Session ID** link to retrieve the cross-search results.
4. Review the antispam log related to the session.



Log Details: 0300006932

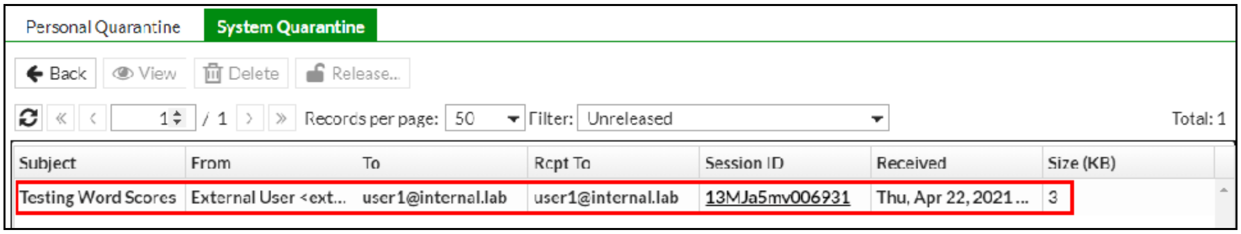
Column	Content
Date	2021-04-22
Time	12:36:05.520
Message	Identified by Content Profile ;Dictionary:WordScores Score: 3(fortimail)
Session ID	13MJa5mt006931-13MJa5mv006931
From	extuser@external.lab
To	user1@internal.lab
Subject	Testing Word Scores
Client IP	100.64.1.99
Client Name	extsrv
Destination IP	10.0.1.11
Level	information
Log ID	0300006932
Type	spam

5. Click **Close**.

To access the system quarantine

1. Continuing on the IntGW FortiMail management GUI, click **Monitor** > **Quarantine** > **System Quarantine**.
2. Double-click **Content/current**.

   Verify that the email was sent to the system quarantine folder.



1 / 1 Records per page: 50 Filter: Unreleased Total: 1

Subject	From	To	Rcpt To	Session ID	Received	Size (KB)
Testing Word Scores	External User <ext...	user1@internal.lab	user1@internal.lab	13MJa5mv006931	Thu, Apr 22, 2021 ...	3

To perform a sanity check

1. Return to the Linux-Client VM.
2. On the ExtSRV FortiMail webmail GUI, compose a new email to `user1@internal.lab`.
3. Copy and paste the contents from the `messagebody.txt` file, but remove two occurrences of the word `FortiMail`, and then send the email.
4. Log out of the ExtSRV FortiMail webmail GUI.
5. Continuing on the Linux-Client VM, open Mozilla Thunderbird.
6. Verify that the email was delivered to the `user1@internal.lab` inbox.
7. Close Thunderbird.

Exercise 2: Configuring DLP

In this exercise, you will configure a DLP profile on IntGW FortiMail. Then, you will apply the DLP profile to a recipient-based policy, to scan all outbound email sent from the `internal.lab` domain.

Configure a DLP Scan Rule

You will configure a DLP scan rule. This rule scans the body and attachments in an email for credit card numbers.

Take the Expert Challenge!

On IntGW FortiMail, create a new DLP profile and name it `ScanCreditCards`.

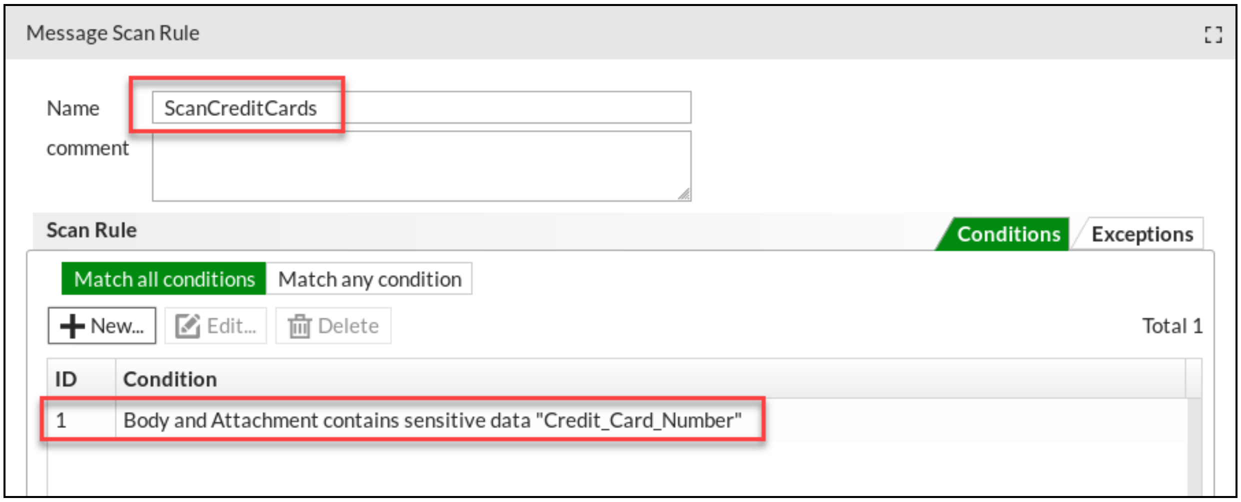
Configure a new DLP scan rule to scan for credit card numbers in an email message body and attachments.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure a DLP Profile on page 117.

To configure a DLP scan rule

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Data Loss Prevention** > **Rule & Profile** > **Rule**.
3. Click **New**.
4. In the **Name** field, type `ScanCreditCards`.
5. In the **Scan Rule** section, click **New**.
6. In the first **Condition** drop-down list, select **Body and Attachment**.
7. In the second **Condition** drop-down list, select **contains sensitive data**.
8. Click **Edit**.
9. Enable the radio button beside **Credit_Card_Number**.
10. Click **OK**.
11. Click **Create**.
12. Verify that your **Message Scan Rule** matches the following example:



Message Scan Rule

Name ScanCreditCards

comment

Scan Rule

Total 1

ID	Condition
1	Body and Attachment contains sensitive data "Credit_Card_Number"

13. Click **Create**.

Configure a DLP Profile

You will configure a DLP profile to use the DLP rule you just created. You will also create a new action profile, which sends the identified emails to the DLP system quarantine folder.

Take the Expert Challenge!

On IntGW FortiMail, create a new DLP action profile and name it `DLP_Out_Sys_Quar`.

Configure the action profile to send identified emails to the DLP system quarantine folder.

Create a new DLP profile and name it `DLP_Out`.

The profile should use the DLP action profile and the DLP scan rule you just created.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

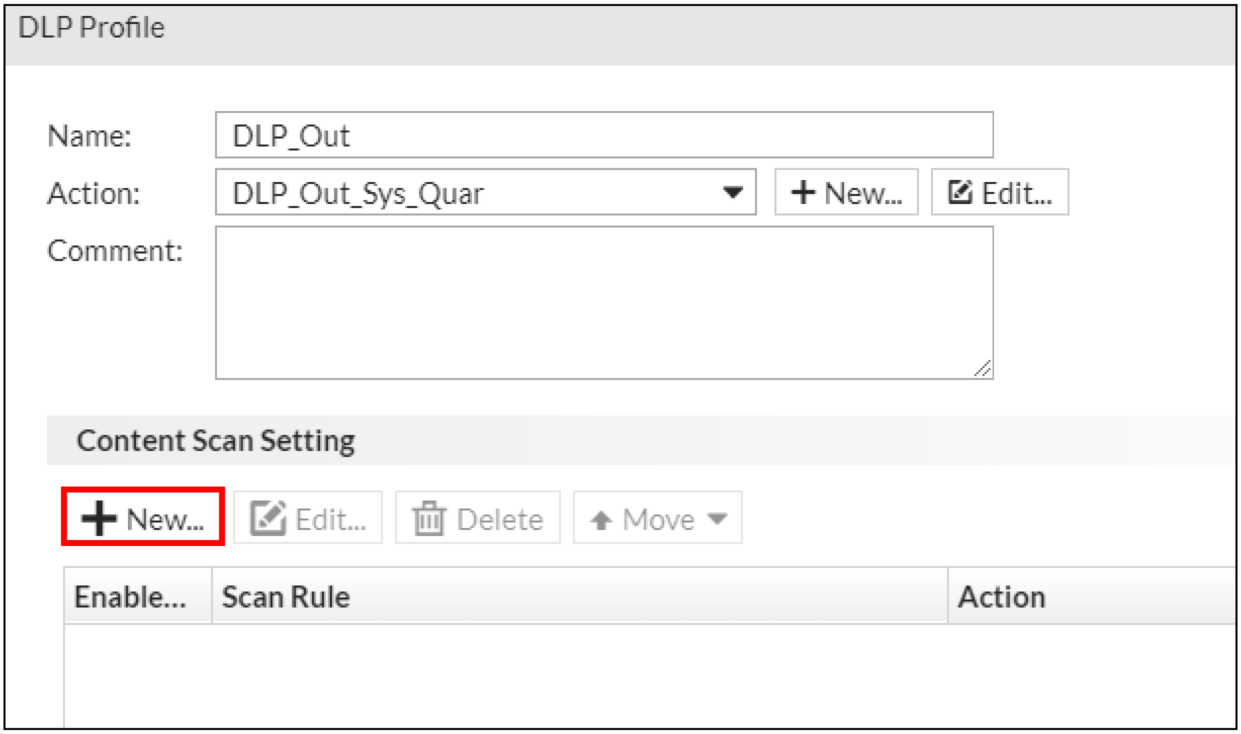
After you complete the challenge, see Apply DLP Scanning to Outbound Emails on page 119.

To configure a DLP profile

1. Continuing on the IntGW FortiMail management GUI, click **Data Loss Prevention** > **Rule & Profile** > **Profile**.
2. Click **New**.
3. In the **Name** field, type `DLP_Out`.
4. Beside the **Action** drop-down list, click **+**.
5. Configure the following settings:

Field	Value
Profile name	DLP_Out_Sys_Quar
Final action	Enable

6. In the **Final action** drop-down list, select **System quarantine**.
7. In the **Folder name** drop-down list, select **Dlp**.
8. Click **Create**.
9. In the **Content Scan Setting** section, click **New**.



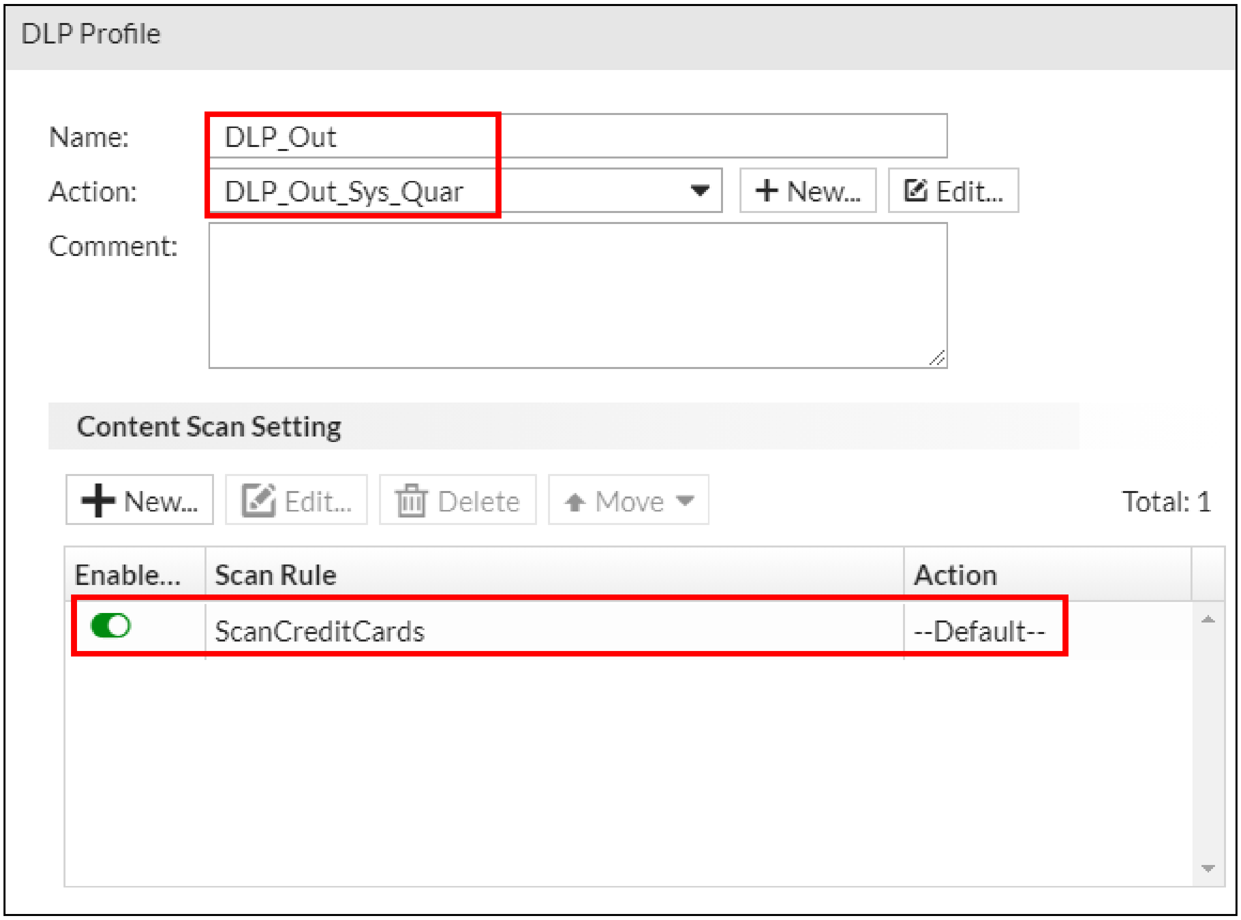
DLP Profile

Name: DLP_Out

Action: DLP_Out_Sys_Quar

Comment:

10. In the **Scan rule** drop-down list, select **ScanCreditCards**.
11. Leave the action as **Default**.
12. Click **Create**.
13. Verify that your DLP profile matches the following example:



DLP Profile

Name: DLP_Out

Action: DLP_Out_Sys_Quar

Comment:

Content Scan Setting

Enable...	Scan Rule	Action
●	ScanCreditCards	--Default--

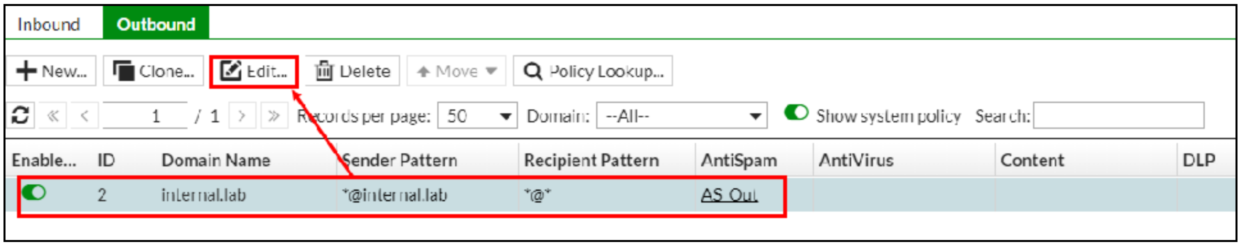
14. Click **Create**.

Apply DLP Scanning to Outbound Emails

You will apply the DLP profile to an outbound recipient policy so that any outgoing emails that contain credit card numbers are quarantined.

To apply DLP scanning to outbound emails

1. Continuing on the IntGW FortiMail management GUI, click **Policy** > **Recipient Policy** > **Outbound**.
2. Under the **Domain** drop-down list, select **All** to see all the policies.
3. Edit the outbound recipient policy.



Enable...	ID	Domain Name	Sender Pattern	Recipient Pattern	AntiSpam	AntiVirus	Content	DLP
●	2	internal.lab	*@internal.lab	*@*	AS Out			

4. In the **Profiles** section, in the **DLP** drop-down list, select **DLP_Out**.
5. Click **OK**.

Validate DLP Scanning

You will test your DLP configuration by sending an email to an external user with an attachment that contains credit card numbers. You will also review the logs to verify your configuration.

To validate DLP scanning

1. On the Linux-Client VM, open Thunderbird.
2. Click **Write**.
3. Compose a new email using the following values:

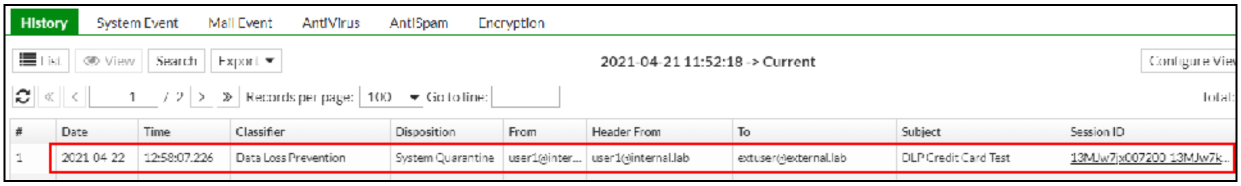
Field	Value
To	extuser@external.lab
Subject	DLP Credit Card Test
Message Body	DLP test email

4. Click **Attach**.
5. Click **Desktop** > **Resources** > **Files** > `sample.pdf`, and then click **Open**.
6. Click **Send**.
7. Close Thunderbird.

To review the logs

1. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.
2. Double-click the active log file.

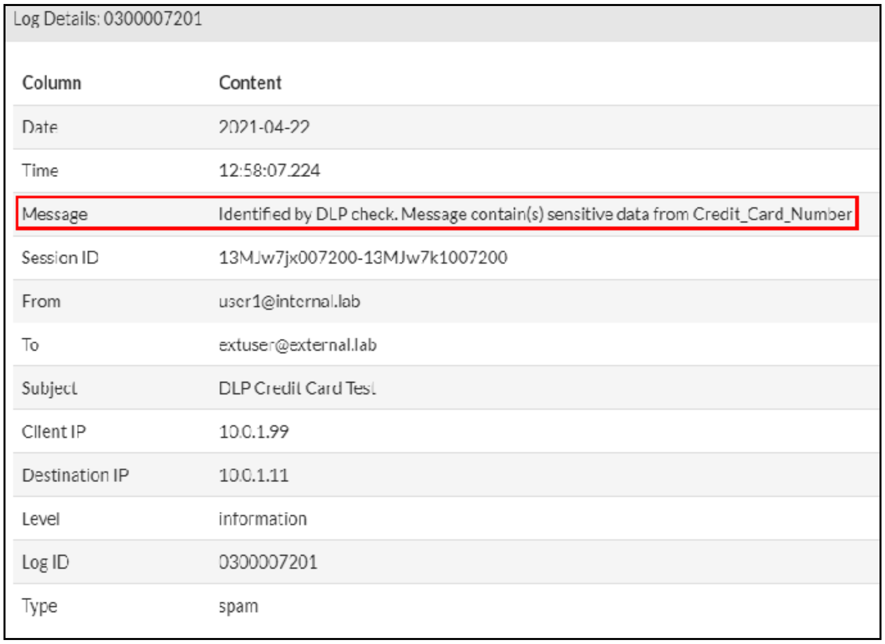
   The first entry in the **History** logs should correspond to the email you just sent.



2021-04-21 11:52:18 -> Current

#	Date	Time	Classifier	Disposition	From	Header From	To	Subject	Session ID
1	2021 04 22	12:58:07.226	Data Loss Prevention	System Quarantine	user1@inter...	user1@internal.lab	extuser@external.lab	DLP Credit Card Test	13MJw7jx007200 13MJw7k...

3. Click the **Session ID** link to retrieve the cross-search results.
4. Review the antispam log related to the session.



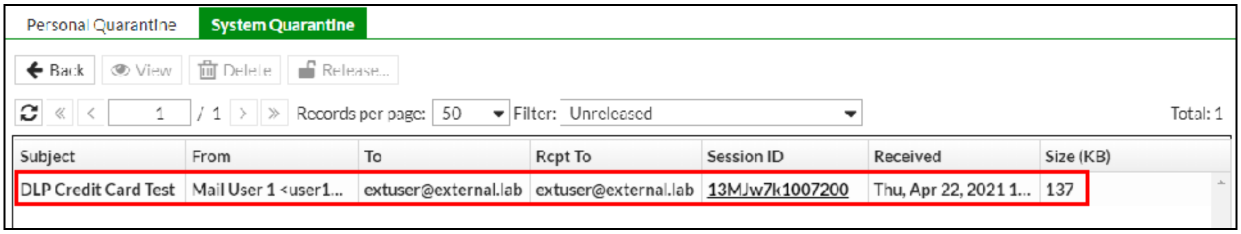
Log Details: 0300007201

Column	Content
Date	2021-04-22
Time	12:58:07.224
Message	Identified by DLP check. Message contain(s) sensitive data from Credit_Card_Number
Session ID	13MJw7jx007200-13MJw7k1007200
From	user1@internal.lab
To	extuser@external.lab
Subject	DLP Credit Card Test
Client IP	10.0.1.99
Destination IP	10.0.1.11
Level	information
Log ID	0300007201
Type	spam

5. Click **Close**.

To view the system quarantine

1. Continuing on the IntGW FortiMail management GUI, click **Monitor** > **Quarantine** > **System Quarantine**.
2. Double-click **Dlp/current**.
3. Verify that the email you sent was quarantined.



Subject	From	To	Rcpt To	Session ID	Received	Size (KB)
DLP Credit Card Test	Mail User 1 <user1...	extuser@external.lab	extuser@external.lab	13MJw7k1007200	Thu, Apr 22, 2021 1...	137

4. Log out of the IntGW FortiMail management GUI.

Exercise 3: Configuring CDR

In this exercise, you will configure CDR in a content profile to scan the HTML content in an email body and attachments that may contain potentially hazardous tags and attributes, such as hyperlinks and scripts.

Configure a Content Action Profile for CDR

You will configure a content action profile that will be used specifically for CDR, so that any inbound emails that trigger CDR will be sanitized. The sanitized email will be delivered to the end user mailbox, but the original email will be sent to the user's personal quarantine mailbox.

You will also configure the action profile settings to quarantine unmodified copies of emails. This means that the original email will be preserved in the personal quarantine, while the end user will receive an email with sanitized contents.

To configure an action profile for sanitized email

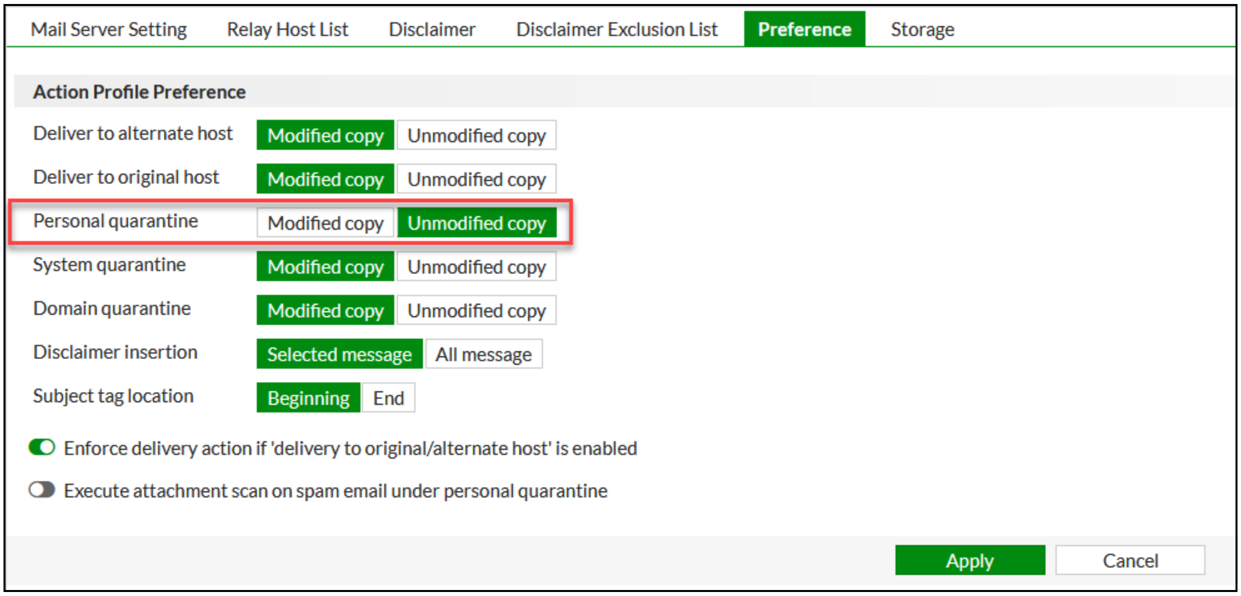
1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Profile** > **Content** > **Action**.
3. Click **New**.
4. Configure the following settings:

Field	Value
Domain	internal.lab
Profile name	CDR_User_Quar
Tag subject	Enabled
Deliver to original host	Enabled
Final action	Enabled

5. In the **Tag subject** field, type `[Sanitized Content]`.
6. In the **Final action** drop-down list, select **Personal Quarantine**.
7. Click **Create**.

To configure quarantine behavior

1. Continuing on the IntGW FortiMail management GUI, click **System** > **Mail Setting** > **Preference**.
2. In the **Personal quarantine** section, click **Unmodified copy**.



Action Profile Preference

Deliver to alternate host: [✓ Modified copy] Unmodified copy

Deliver to original host: [✓ Modified copy] Unmodified copy

Personal quarantine: Modified copy [✓ Unmodified copy]

System quarantine: [✓ Modified copy] Unmodified copy

Domain quarantine: [✓ Modified copy] Unmodified copy

Disclaimer insertion: [✓ Selected message] All message

Subject tag location: [✓ Beginning] End

● Enforce delivery action if 'delivery to original/alternate host' is enabled

○ Execute attachment scan on spam email under personal quarantine

3. Click **Apply**.

Configure CDR

You will configure CDR for HTML content, text content, and PDF files.

Take the Expert Challenge!

On IntGW FortiMail, create a new content profile and name it `CDR`.

The profile should be available for the `internal.lab` domain only, and use the **CDR_User_Quar** action profile.

In the profile, configure CDR to sanitize HTML content, remove URIs, and inspect PDF files.

The CDR action should be the default action profile for the content profile.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Apply CDR to Inbound Emails on page 124.

To configure CDR

1. Continuing on the IntGW FortiMail management GUI, click **Profile** > **Content** > **Content**.
2. Click **New**.
3. Configure a new content profile using the following values:

Field	Value
Domain	internal.lab

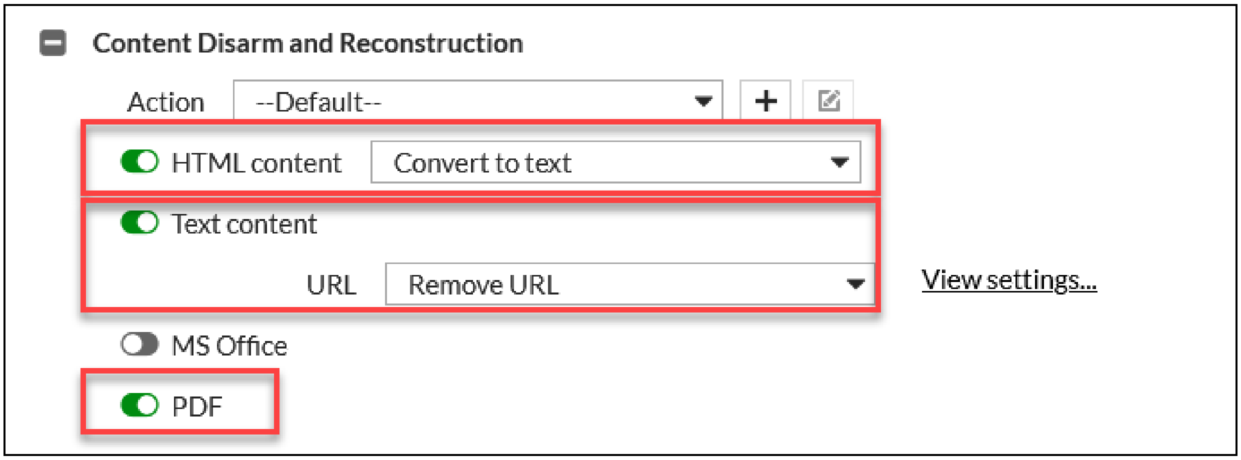
Field	Value
Profile name	CDR
Action	CDR_User_Quar

4. Expand the **Content Disarm and Reconstruction** section.
5. In the **Action** drop-down list, select **Default**.
6. Configure the following settings:

Field	Value
HTML content	Enable
Text content	Enable
PDF	Enable

7. In the **HTML content** drop-down list, select **Convert to text**.
8. In the **URL** drop-down list, select **Remove URL**.

Your configuration should match the following example:



Content Disarm and Reconstruction

Action: --Default--

HTML content: Convert to text

Text content

URL: Remove URL

MS Office

PDF

9. Click **Create**.

Apply CDR to Inbound Emails

You will apply the content profile to an inbound recipient policy.

To apply CDR to inbound emails

1. Continuing on the IntGW FortiMail management GUI, click **Policy** > **Recipient Policy** > **Inbound**.
2. Edit policy ID **1**.
3. In the **Profiles** section, in the **Content** drop-down list, select **CDR**.
4. Click **OK**.

Validate PDF Sanitization

You will validate your CDR configuration by sending an email with a PDF attachment from a user in the `external.lab` domain. You will review the logs on IntGW FortiMail. You will also compare the original PDF attachment with the sanitized PDF attachment.

To validate PDF sanitization

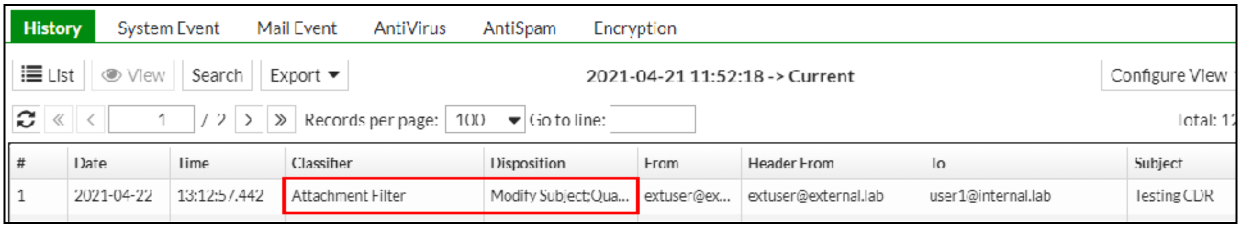
1. On the Linux-Client VM, open a new browser, and then on theExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
2. Compose a new email to `user1@internal.lab`.
3. Click **Attach** (the paperclip icon on the bottom-left of the screen).
4. Click **Resources** > **Files** > `labdoc.pdf`, and then click **Open**.

   Wait for the file to upload.
5. Click **Send**.
6. Log out of the ExtSRV FortiMail webmail GUI.

To review the logs

1. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

   The first entry in the **History** logs should correspond to the email that was sent.
2. Review the values for **Classifier** and **Disposition**.

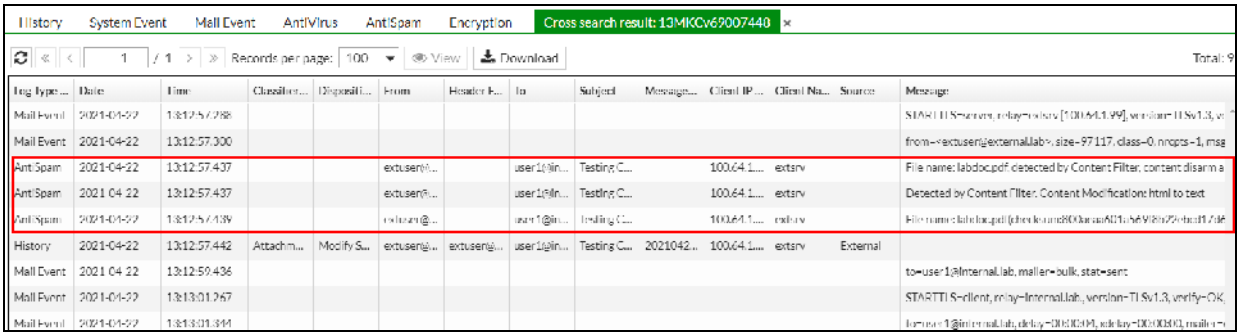


2021-04-21 11:52:18 -> Current

1 / 2 · 100 · Total: 1

#	Date	Time	Classifier	Disposition	From	Header From	To	Subject
1	2021-04-22	13:12:57.442	Attachment Filter	Modify Subject,Qua...	extuser@ex...	extuser@external.lab	user1@internal.lab	Testing CDR

3. Click the **Session ID** link to retrieve the cross-search results.
4. Review the antispam log messages related to the session.



1 / 1 · 100 · Total: 9

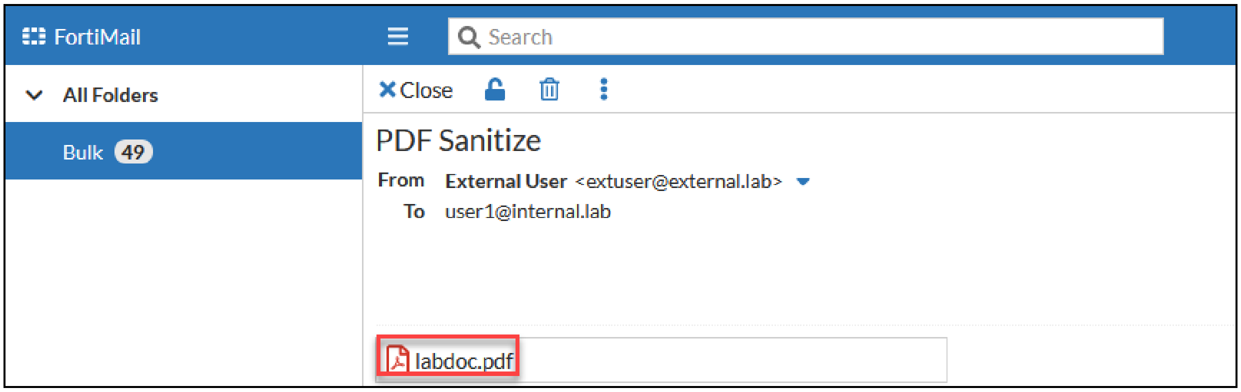
Log Type...	Date	Time	Classifier...	Dispositi...	From	Header F...	To	Subject	Message...	Client IP ...	Client Na...	Source	Message
Mail Event	2021-04-22	13:12:57.288											STARTTLS=server, relay=extsrv [100.64.1.99], version=TLSv1.3, v
Mail Event	2021-04-22	13:12:57.300											from=<extuser@external.lab>, size=97117, class=0, nrcpts=1, msg
AntiSpam	2021-04-22	13:12:57.437			extuser@...		user1@in...	Testing C...		100.64.1....	extsrv		File name: labdoc.pdf detected by Content Filter, content disarm a
AntiSpam	2021 04 22	13:12:57.437			extuser@...		user1@in...	Testing C...		100.64.1....	extsrv		Detected by Content Filter. Content Modification: html to text
AntiSpam	2021-04-22	13:12:57.439			extuser@...		user1@in...	Testing C...		100.64.1....	extsrv		File name: labdoc.pdf (checksum:800aeaa601a56918a79ebcd17d6
History	2021-04-22	13:12:57.442	Attachm...	Modify S...	extuser@...	extuser@...	user1@in...	Testing C...	2021042...	100.64.1....	extsrv	External	
Mail Event	2021 04 22	13:12:59.436											to=user1@internal.lab, mailer=bulk, stat=sent
Mail Event	2021-04-22	13:13:01.267											STARTTLS=client, relay=internal.lab., version=TLSv1.3, verify=OK,
Mail Event	2021-04-22	13:13:01.344											to=user1@internal.lab, delay=00:00:04, xdelay=00:00:00, mailer=

To compare the PDF files

1. Return to the Linux-Client VM, and then open Thunderbird .

   Verify that the email was delivered to the user mailbox.

2. Open the PDF attachment.
3. Verify that the URIs in the PDF file were neutralized.
4. Close the PDF reader.
5. Open a new browser tab, and then on the IntGW FortiMail webmail GUI, log in with the username `user1` and password `fortinet`.
6. Open the quarantined email, and then view the attached, unmodified PDF file.



PDF Sanitize

From External User <extuser@external.lab>

To user1@internal.lab

labdoc.pdf

7. Compare the quarantined PDF file with the sanitized PDF file that was delivered to the user's mailbox.

In the sanitized PDF file , the links were neutralized by CDR. You cannot click the links to visit the websites.

In the quarantined PDF, the links are still active. You can click the links to visit the websites.

Validate URI Removal

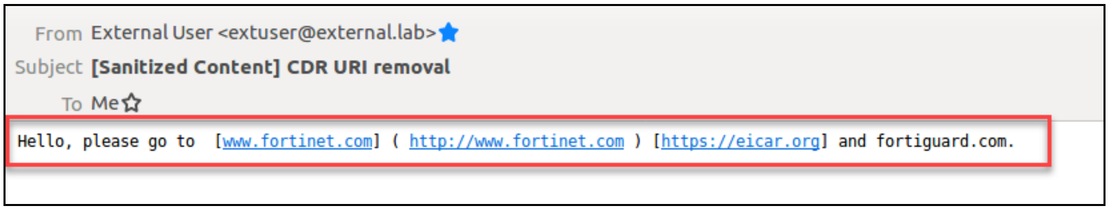
You will validate CDR URI removal by sending an email with different URIs. FortiMail will remove any URI to display only the website name and no underlying links that can be misleading or malicious.

To validate URI removal

1. On the Linux-Client VM, open a new browser, and then on the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
2. Compose a new email to `user1@internal.lab`.
3. Give the email a subject.
4. Type the following in the body of the message or write a short note that includes some URLs. They will turn blue if the email client automatically adds associated links. Feel free to modify the links to make then different from the display text.

```
Hello, please go to www.fortinet.com https://eicar.org and fortiguard.com.
```

5. Send email.
6. Return to the Linux-Client VM, and then open Thunderbird.
7. Verify that the email were flagged and the URIs are listed separately from the display name. In the following example, the Thunderbird email client attempts to recognize the strings as URLs and highlights them in blue.



From External User <extuser@external.lab>
Subject **[Sanitized Content] CDR URI removal**
To Me

```
Hello, please go to  [www.fortinet.com] ( http://www.fortinet.com ) [https://eicar.org] and fortiguard.com.
```

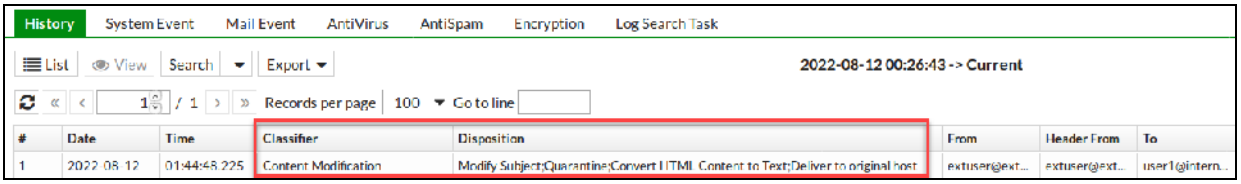
Notice that FortiMail expands what URL was associated with a link in the email. (http://www.fortinet.com for www.fortinet.com), https://eicar.org is exactly as listed, and fortiguard.com did not have an associated web link and is treated as basic text.

To review the logs

1. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

   The first entry in the **History** logs should correspond to the email that you sent.

2. Review the values in the **Classifier** and **Disposition** columns.



#	Date	Time	Classifier	Disposition	From	Header From	To
1	2022-08-12	01:44:48.225	Content Modification	Modify Subject;Quarantine;Convert HTML Content to Text;Deliver to original host	extuser@ext...	extuser@ext...	user1@intern...

Validate HTML Content Sanitization

You will send an email with HTML content. CDR should neutralize all potentially hazardous tags and attributes, such as hyperlinks and scripts. Then, you will release the original email from quarantine and compare the original email with the sanitized email.

To validate HTML sanitization

1. Return to the Linux-Client VM, and then open a terminal window (`Ctrl`+`Alt`+`T`).
2. Enter the following command to start an SSH connection to the Linux-Router VM:

   ```
   ssh student@10.0.1.254
   ```

3. Enter the password `password`.
4. Enter `pwd`.

   Verify that the current working directory is `/home/student`.

5. Enter the following swaks command to send the email with HTML content:

   ```
   cat Resources/tosanitize.dat | swaks -f extuser@external.lab -t user1@internal.lab -s
       intgw.internal.lab --ehlo linux.internal.lab --data -
   ```

Swaks takes the contents of the `tosanitize.dat` file, which contains HTML content, and includes it in the body of the email.

A copy of the swaks command is in the `commands.txt` file, which is located in the **Resources** folder on the Linux-Client VM desktop.

6. Close the terminal window.
7. In Thunderbird, review the email that you just sent.
8. Verify that it has been converted to text and all URIs in the email body have been neutralized and displayed in parentheses.

To compare the emails

1. Return to the IntGW FortiMail webmail GUI, and then click **Refresh**.

   An unmodified copy of the email is available in the **Bulk** folder.

2. Compare the original to what is sent to the user's inbox.
3. Log out of the IntGW FortiMail webmail GUI.

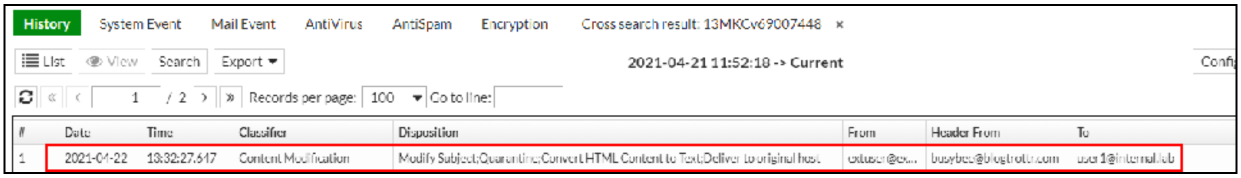
HTML links in the body of the email will redirect the user to various websites.

To review the logs

1. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

   The first log corresponds to the email that you just sent.

2. Review the values in the **Classifier** and **Disposition** columns.



2021-04-21 11:52:18 -> Current

#	Date	Time	Classifier	Disposition	From	Header From	To
1	2021-04-22	13:32:27.617	Content Modification	Modify Subject;Quarantine;Convert HTML Content to Text;Deliver to original host	extuser@ex...	busybee@blogtrotr.com	user1@internal.lab

3. Log out of the IntGW FortiMail management GUI.

Lab 8: Secure Communications

In this lab, you will implement SMTPS between IntGW FortiMail and IntSRV FortiMail. You will also configure content inspection-based identity-based encryption (IBE), and verify your configuration by sending a secure email.

Objectives

- Implement SMTPS between IntGW FortiMail and IntSRV FortiMail
- Implement content inspection-based IBE
  - Configure the dictionary profile with the trigger word
  - Configure an encryption profile
  - Configure a content action profile to apply the encryption profile
  - Apply the dictionary profile and content action profile to a content profile
  - Apply the content profile to an outbound recipient-based policy
- Register an IBE user and access the IBE email

Time to Complete

Estimated: 40 minutes

Prerequisites

Before beginning this lab, you must disable CDR on IntGW FortiMail.

To disable CDR on IntGW FortiMail

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Policy** > **Recipient Policy** > **Inbound**.
3. In the **Domain** drop-down list, select **All**.
4. Edit policy ID **1**.
5. In the **Profiles** section, in the **Content** drop-down list, select **None**.
6. Click **OK**.
7. Log out of the IntGW FortiMail management GUI.

Exercise 1: Implementing SMTPS

In this exercise, you will configure SMTPS between IntGW FortiMail and IntSRV FortiMail. You will also compare logged details before and after implementing SMTPS.

Verify STARTTLS Usage

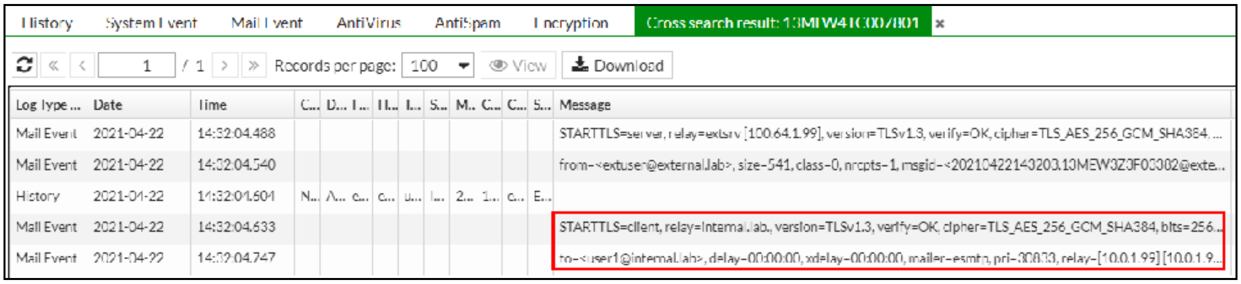
You will send an email from an external MTA, and then review the logs on IntGW FortiMail to validate the type of connection that was established between the external MTA and IntGW FortiMail.

To review logs

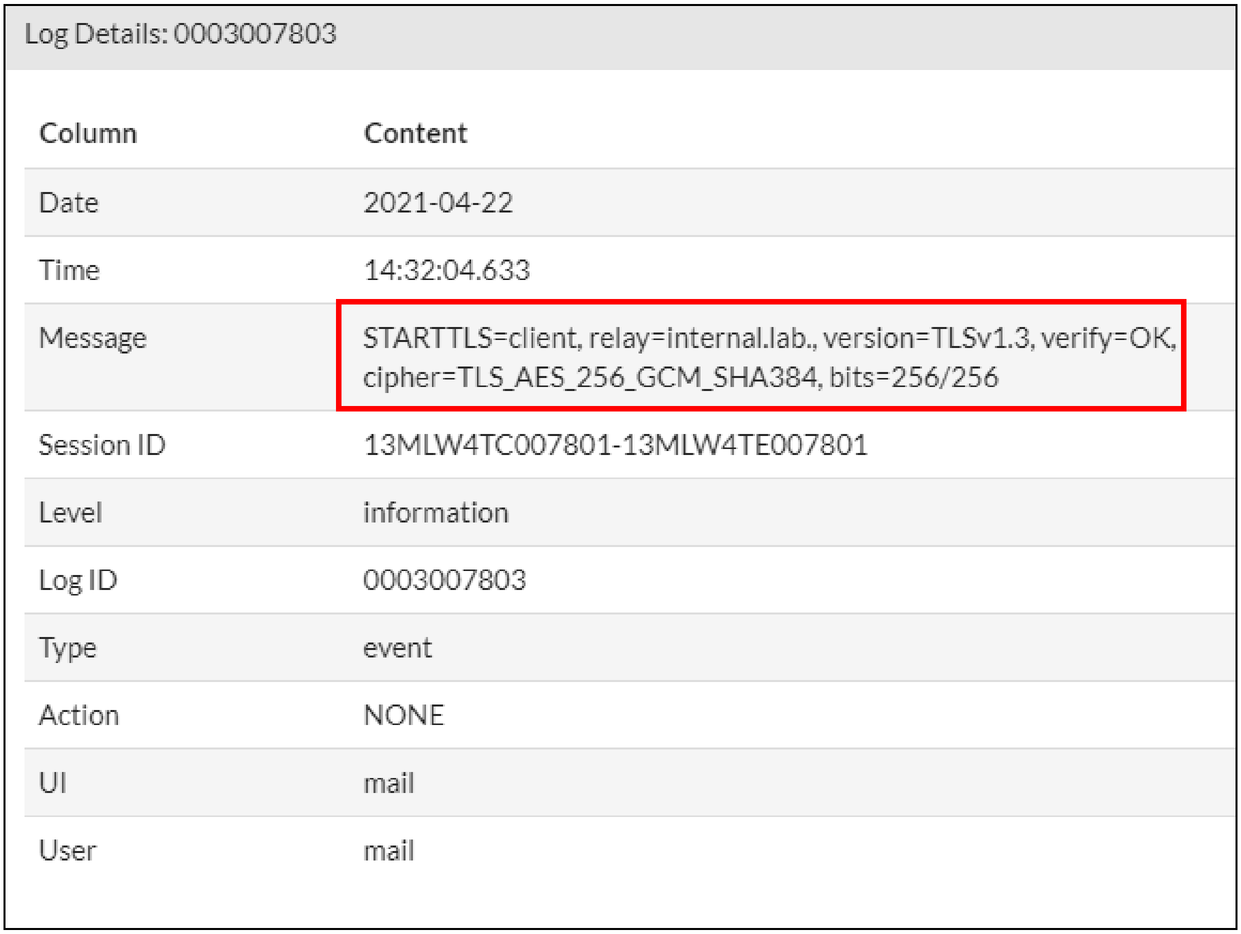
1. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
2. Send an email message to `user1@internal.lab`.
3. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
4. Click **Monitor** > **Log** > **History**.

   The first entry in the **History** logs should correspond to the email you just sent.

5. Click the **Session ID** link to retrieve the cross-search results, and then review the last two entries, which contain details about the session between IntGW FortiMail and IntSRV FortiMail.

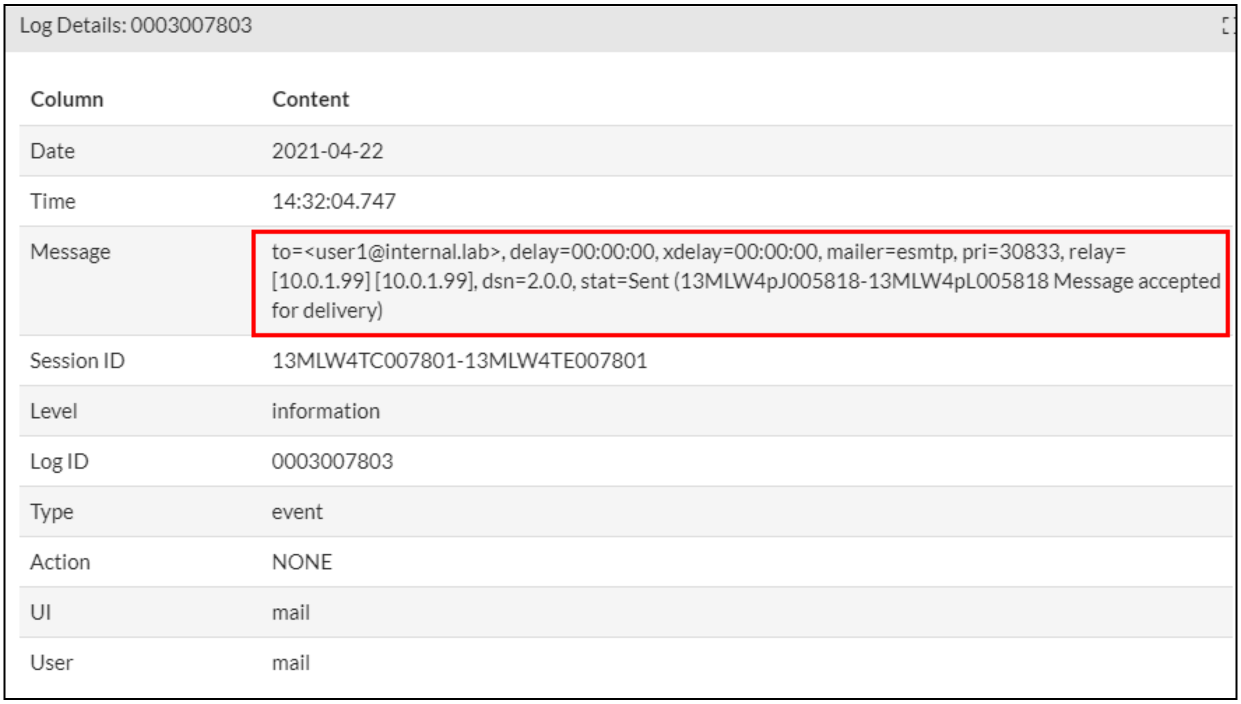


Log Type ...	Date	Time	C...	D...	I...	H...	I...	S...	M...	C...	C...	S...	Message
Mail Event	2021-04-22	14:32:04.488											STARTTLS=server, relay=extsrv [100.64.1.99], version=TLSv1.3, verify=OK, cipher=TLS_AES_256_GCM_SHA384, ...
Mail Event	2021-04-22	14:32:04.540											from=<extuser@external.lab>, size=541, class=0, nrcpts=1, msgid=<20210422143203.13MEW3Z3F03302@exte...
History	2021-04-22	14:32:04.604	N...	A...	c...	c...	u...	l...	2...	1...	c...	E...	
Mail Event	2021-04-22	14:32:04.633											STARTTLS=client, relay=internal.lab., version=TLSv1.3, verify=OK, cipher=TLS_AES_256_GCM_SHA384, bits=256...
Mail Event	2021-04-22	14:32:04.747											to=<user1@internal.lab>, delay=00:00:00, xdelay=00:00:00, mailer=esmtp, pri=30833, relay=[10.0.1.99] [10.0.1.9...



Log Details: 0003007803

Column	Content
Date	2021-04-22
Time	14:32:04.633
Message	STARTTLS=client, relay=internal.lab., version=TLSv1.3, verify=OK, cipher=TLS_AES_256_GCM_SHA384, bits=256/256
Session ID	13MLW4TC007801-13MLW4TE007801
Level	information
Log ID	0003007803
Type	event
Action	NONE
UI	mail
User	mail

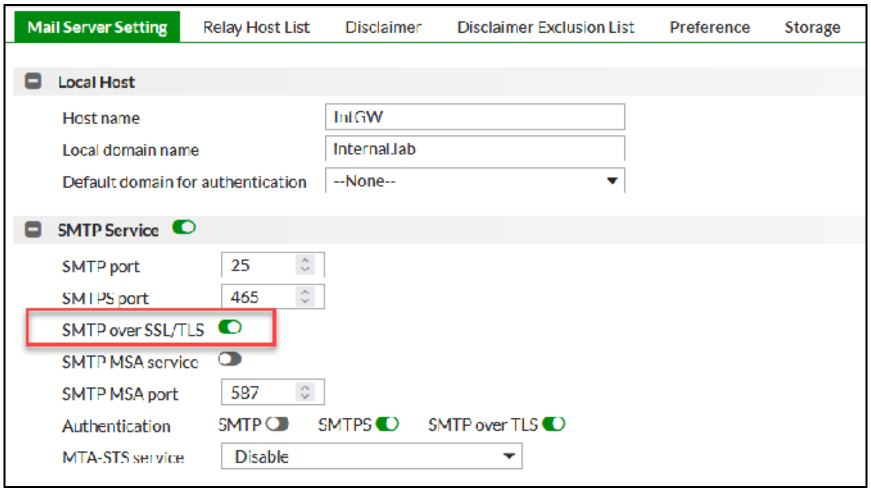


Log Details: 0003007803

Column	Content
Date	2021-04-22
Time	14:32:04.747
Message	to=<user1@internal.lab>, delay=00:00:00, xdelay=00:00:00, mailer=esmtp, pri=30833, relay=[10.0.1.99] [10.0.1.99], dsn=2.0.0, stat=Sent (13MLW4pJ005818-13MLW4pL005818 Message accepted for delivery)
Session ID	13MLW4TC007801-13MLW4TE007801
Level	information
Log ID	0003007803
Type	event
Action	NONE
UI	mail
User	mail

By default, FortiMail uses SMTP over TLS if the recipient MTA supports it. In this session, IntSRV FortiMail is the recipient MTA.

By default, SMTP over TLS is enabled on FortiMail.



Local Host

Host name: IntGW

Local domain name: Internal.lab

Default domain for authentication: --None--

SMTP Service: ●

SMTP port: 25

SMTPS port: 465

SMTP over SSL/TLS: ●

SMTP MSA service: ○

SMTP MSA port: 587

Authentication: SMTP ○ SMTPS ● SMTP over TLS ●

MTA-STS service: Disable

Configure SMTPS

On IntGW FortiMail, you will enable SMTPS for back-end connectivity with IntSRV FortiMail.

Take the Expert Challenge!

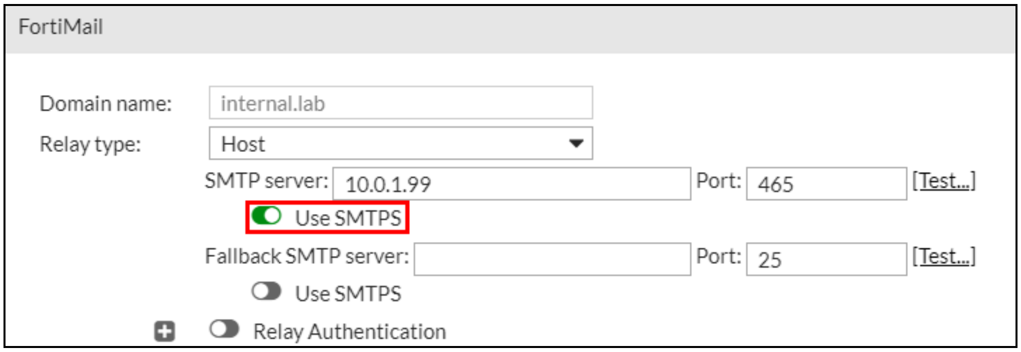
On IntGW FortiMail, enable SMTPS for back-end connectivity with IntSRV FortiMail.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Verify SMTPS on page 133.

To configure SMTPS

1. Continuing on the IntGW FortiMail management GUI, click **Domain & User** > **Domain** > **Domain**.
2. Select **internal.lab**, and then click **Edit**.
3. Enable **Use SMTPS**.



Domain name: internal.lab

Relay type: Host

SMTP server: 10.0.1.99 Port: 465

● Use SMTPS

Fallback SMTP server: Port: 25

○ Use SMTPS

○ Relay Authentication

4. Click **OK**.

Verify SMTPS

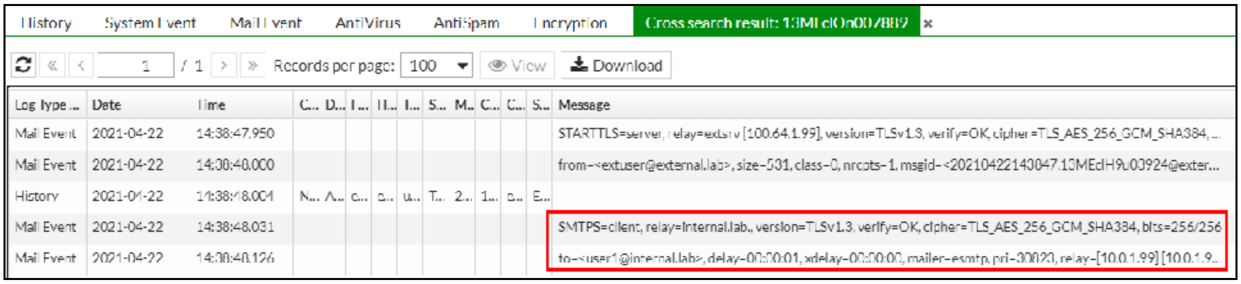
You will send an email from a user in the `external.lab` domain, and then review the logs on IntGW FortiMail, to validate that SMTPS is being used.

To verify SMTPS

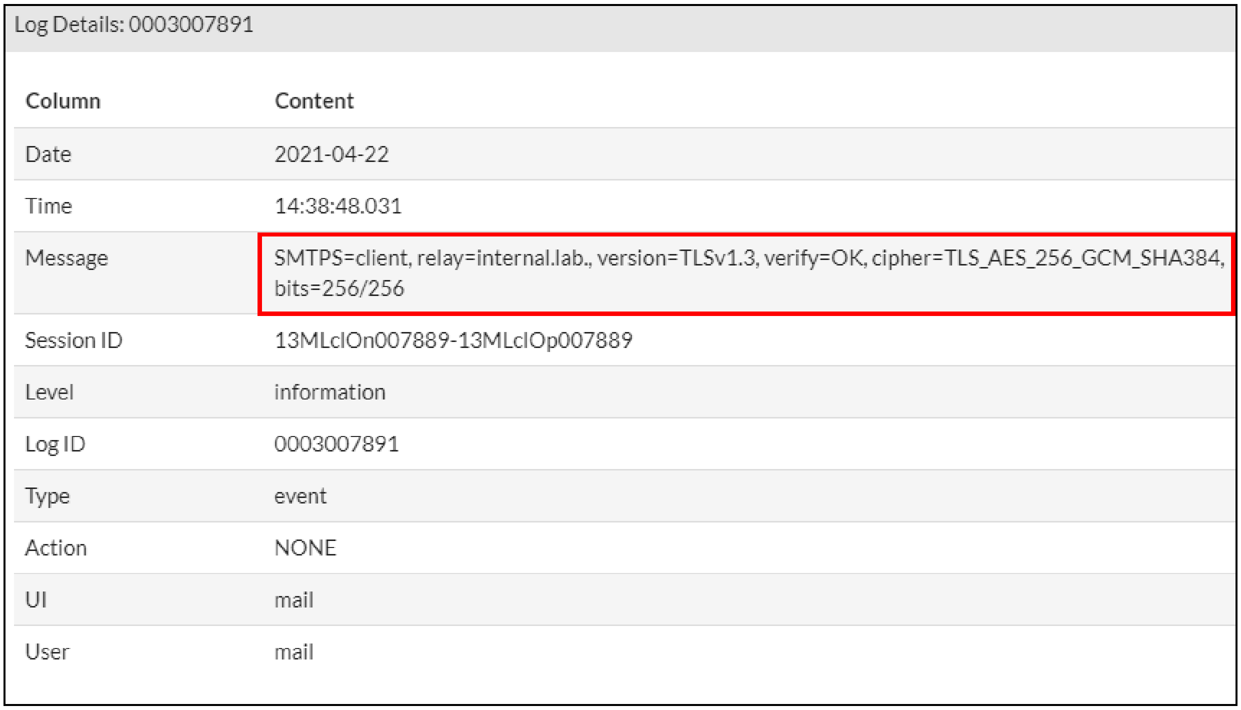
1. Return to the ExtSRV FortiMail webmail GUI, and then send another email to `user1@internal.lab`.
2. Log out of the ExtSRV FortiMail webmail GUI.
3. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

   The first entry in the **History** logs should correspond to the email message you just sent.

4. Click the **Session ID** link to retrieve the cross-search results.
5. Review the last two entries, which should indicate the switchover to SMTPS from STARTTLS.

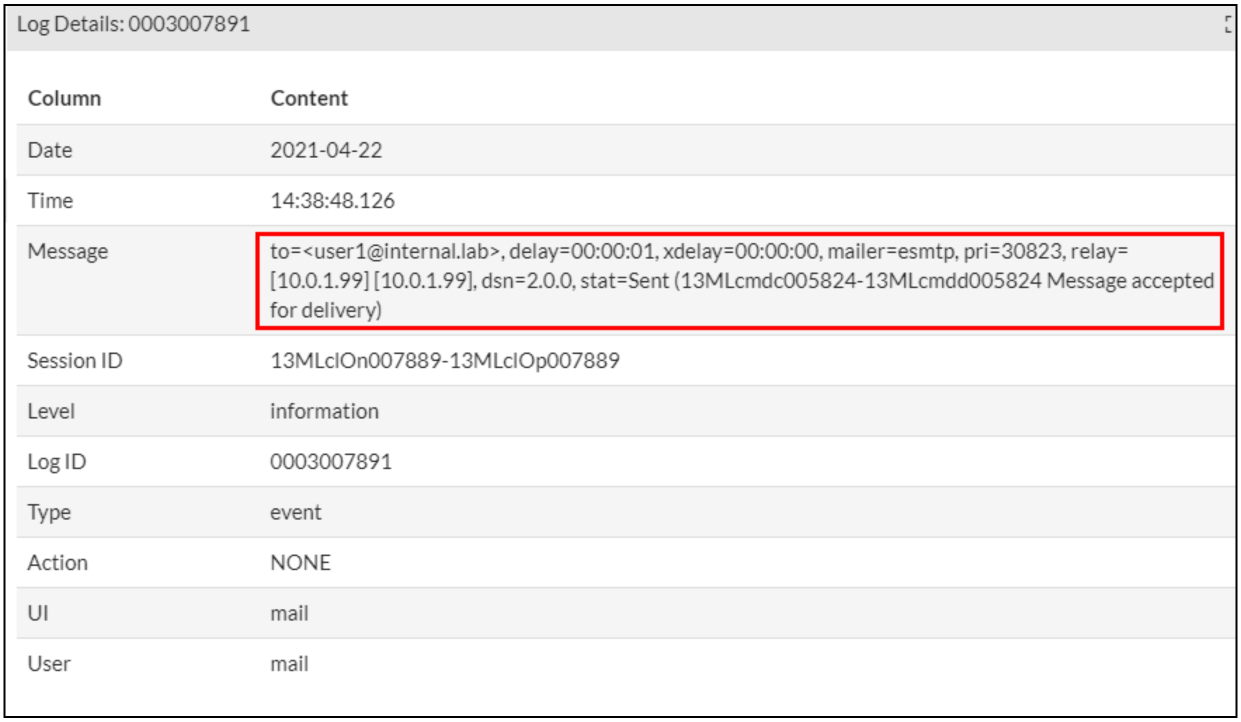


Log Type ...	Date	Time	C...	D...	I...	H...	I...	S...	M...	C...	C...	S...	Message
Mail Event	2021-04-22	14:38:47.950											STARTTLS=server, relay=extsrv [100.64.1.99], version=TLSv1.3, verify=OK, cipher=TLS_AES_256_GCM_SHA384, ...
Mail Event	2021-04-22	14:38:48.000											from=<extuser@external.lab>, size=531, class=0, nrcpts=1, msgid=<20210422143047.13MEdH9u03924@exter...
History	2021-04-22	14:38:48.004	N...	A...	c...	a...	u...	T...	2...	1...	a...	E...	
Mail Event	2021-04-22	14:38:48.031											SMTPS=client, relay=internal.lab., version=TLSv1.3, verify=OK, cipher=TLS_AES_256_GCM_SHA384, bits=256/256
Mail Event	2021-04-22	14:38:48.126											to=<user1@internal.lab>, delay=00:00:01, xdelay=00:00:00, mailer=esmtp, pri=30020, relay=[10.0.1.99] [10.0.1.9...



Log Details: 0003007891

Column	Content
Date	2021-04-22
Time	14:38:48.031
Message	SMTPS=client, relay=internal.lab., version=TLSv1.3, verify=OK, cipher=TLS_AES_256_GCM_SHA384, bits=256/256
Session ID	13MLclOn007889-13MLclOp007889
Level	information
Log ID	0003007891
Type	event
Action	NONE
UI	mail
User	mail



Log Details: 0003007891

Column	Content
Date	2021-04-22
Time	14:38:48.126
Message	to=<user1@internal.lab>, delay=00:00:01, xdelay=00:00:00, mailer=esmtp, pri=30823, relay=[10.0.1.99] [10.0.1.99], dsn=2.0.0, stat=Sent (13MLcmdc005824-13MLcmdd005824 Message accepted for delivery)
Session ID	13MLclOn007889-13MLclOp007889
Level	information
Log ID	0003007891
Type	event
Action	NONE
UI	mail
User	mail

The underlying encryption mechanism for SMTPS and SMTP over TLS is the same. Both protocols use TLS. In this case, the FortiMail VMs negotiate TLSv1.3. The difference is in how and when TLS encryption is applied.

When SMTP over TLS is used, the connection is made on the standard SMTP port—TCP port 25. If the recipient MTA supports the STARTTLS extension, the sender chooses whether SMTP over TLS is used, by transmitting the `STARTTLS` message. This STARTTLS request happens after the envelope exchange, and so, in SMTP over TLS, only a portion of the session is encrypted.

When SMTPS is used, the client initiates the SMTP session with the server over a fully-encrypted tunnel, using a separate port—TCP port 465. SMTPS encrypts the full session.

6. Log out of the IntGW FortiMail management GUI.

Exercise 2: Implementing Content Inspection-Based IBE

In this exercise, you will configure content inspection-based IBE. You will also verify your configuration by sending an IBE email message and reviewing the logs.

Configure the IBE Service

You will enable the IBE service on IntGW FortiMail. You will enable replying, forwarding, and composing of email messages for IBE users in the secure webmail portal.

Take the Expert Challenge!

On IntGW FortiMail, enable the IBE service, and configure the service name `Internal Lab Secure Portal`.

In the IBE settings, enable secure replying, forwarding, and composing.

Use the IntGW FortiMail FQDN for the base URL.

Enable read message notifications for the sender.

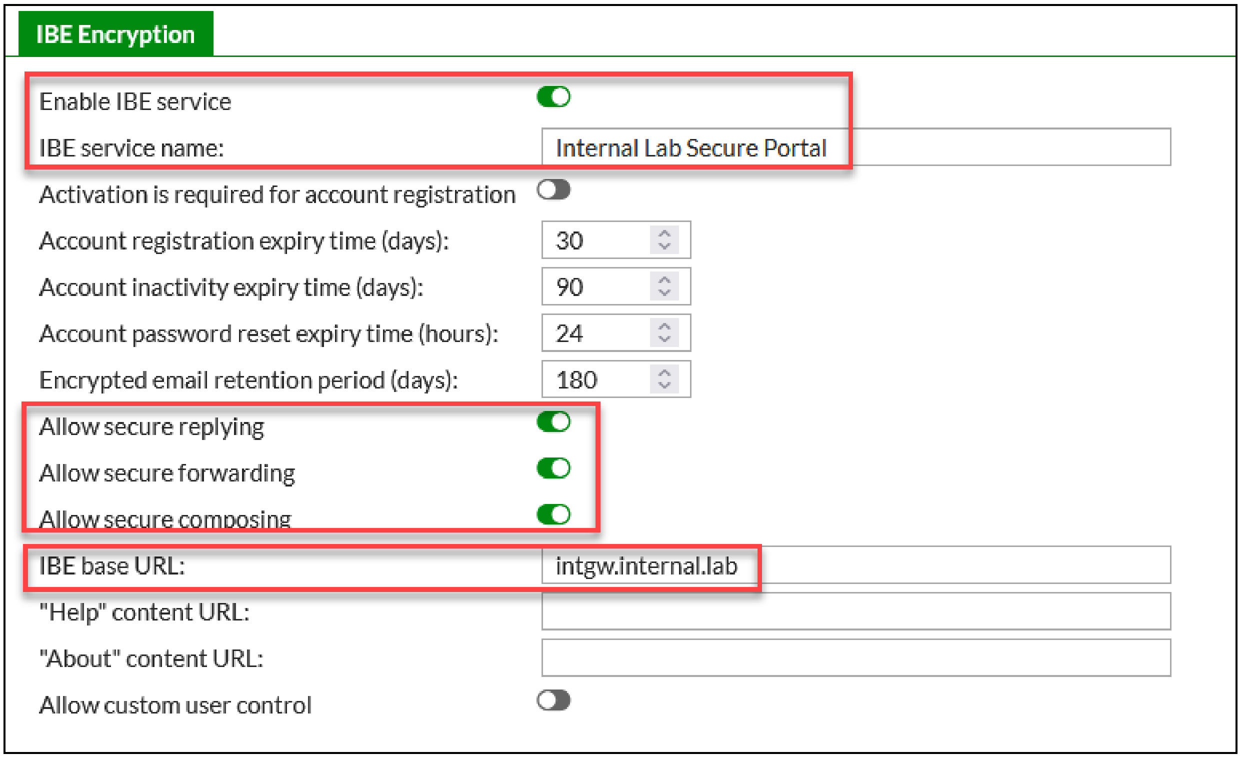
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure the IBE Trigger Word on page 136.

To configure the IBE service

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Encryption** > **IBE** > **IBE Encryption**.
3. Configure the following settings:

Field	Value
Enable IBE service	Enabled
IBE service name	Internal Lab Secure Portal
Activation is required for account registration	Disabled
Allow secure replying	Enabled
Allow secure forwarding	Enabled
Allow secure composing	Enabled
IBE base URL	intgw.internal.lab



IBE Encryption

Enable IBE service	●
IBE service name:	Internal Lab Secure Portal
Activation is required for account registration	○
Account registration expiry time (days):	30
Account inactivity expiry time (days):	90
Account password reset expiry time (hours):	24
Encrypted email retention period (days):	180
Allow secure replying	●
Allow secure forwarding	●
Allow secure composing	●
IBE base URL:	intgw.internal.lab
"Help" content URL:	
"About" content URL:	
Allow custom user control	○

4. In the **Email Status Notification** section, enable **Message is read (notify sender)**.
5. Click **Apply**.

Configure the IBE Trigger Word

You will configure a dictionary profile to define the IBE trigger word.

Take the Expert Challenge!

On IntGW FortiMail, create a new dictionary profile and name it `IBEDictionary`.

Create a wildcard dictionary entry. Use the string `[CONFIDENTIAL]`. Remember to use the correct escape character.

The dictionary profile should search for the trigger word in email headers only.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure an Encryption Profile on page 137.

To configure the IBE trigger word

1. Continuing on the IntGW FortiMail management GUI, click **Profile** > **Dictionary** > **Dictionary**.
2. Edit the dictionary profile **IBEDictionary**.
3. In the **Dictionary Entries** section, click **New**.
4. Configure a dictionary entry using the following values:

Field	Value
Pattern	\[CONFIDENTIAL]
Pattern type	Wildcard
Search header	Enabled
Search body	Disabled

5. Click **Create**.
6. Click **OK**.

Configure an Encryption Profile

You will verify a system default encryption profile.

To configure an encryption profile

1. Continuing on the IntGW FortiMail management GUI, click **Profile** > **Security** > **Encryption**.
2. Select the **IBE_Pull** profile, and then click **Edit**.
3. Verify the **Encryption algorithm** is **AES 256**, otherwise select it in the drop-down list.
4. Click **OK** to save the changes.

Configure a Content Action Profile to Trigger IBE

You will create a new content action profile that will trigger IBE.

Take the Expert Challenge!

On IntGW FortiMail, create a new content action profile and name it `CF_IBE_Pull`.

The content profile should use the **IBE_Pull** encryption profile.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure a Content Profile for IBE on page 138.

To configure a content action profile to trigger IBE

1. Continuing on the IntGW FortiMail management GUI, click **Profile** > **Content** > **Action**.
2. Click **New**.
3. Configure the following settings:

Field	Value
Domain	--System--
Profile name	CF_IBE_Pull
Final action	Enable

4. In the **Final action** drop-down list, select **Encrypt with profile**.
5. In the **Profile name** drop-down list, select **IBE_Pull**.
6. Click **Create**.

Configure a Content Profile for IBE

You will configure a content profile for IBE, and then apply it to the outbound recipient policy for the `internal.lab` domain.

Take the Expert Challenge!

On IntGW FortiMail, create a new content profile and name it `CF_Out`.

The content profile should use the **CF_IBE_Pull** content action profile.

Apply the **IBEDictionary** dictionary profile to the content profile.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Validate IBE on page 139.

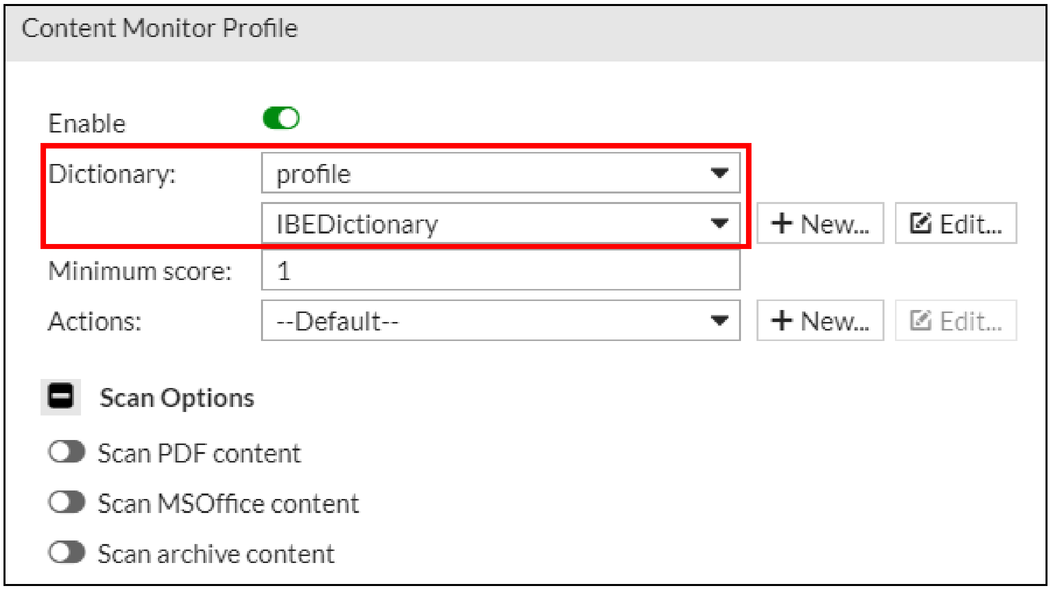
To configure a content profile for IBE

1. Continuing on the IntGW FortiMail management GUI, click **Profile** > **Content** > **Content**.
2. Click **New**.
3. Configure the following settings:

Field	Value
Domain	--System--
Profile name	CF_Out
Action	CF_IBE_Pull

4. In the **Content Monitor and Filtering** section, click **New**.
5. In the first **Dictionary** drop-down list, select **profile**.
6. In the second **Dictionary** drop-down list, select **IBEDictionary**.

   Your configuration should match the following example:



Content Monitor Profile

Enable: ●

Dictionary: profile

IBEDictionary

Minimum score: 1

Actions: --Default--

Scan Options

○ Scan PDF content

○ Scan MSOffice content

○ Scan archive content

7. Click **Create**.
8. Click **Create**.

To apply the content profile to outbound email messages

1. Continuing on the IntGW FortiMail management GUI, click **Policy** > **Recipient Policy** > **Outbound**.
2. Edit the outgoing recipient policy.
3. In the **Content** drop-down list, select **CF_Out**.
4. Click **OK**.

Validate IBE

You will send an email with the IBE trigger word to a user in the `external.lab` domain. You will verify that IBE is working by viewing the logs on IntGW FortiMail.

To send an IBE email

1. On the Linux-Client VM, open Mozilla Thunderbird.
2. Compose a new email message using the following values:

Field	Value
To	extuser@external.lab
Subject	[CONFIDENTIAL] Requires immediate attention
Message body	Did you leave the stove on?

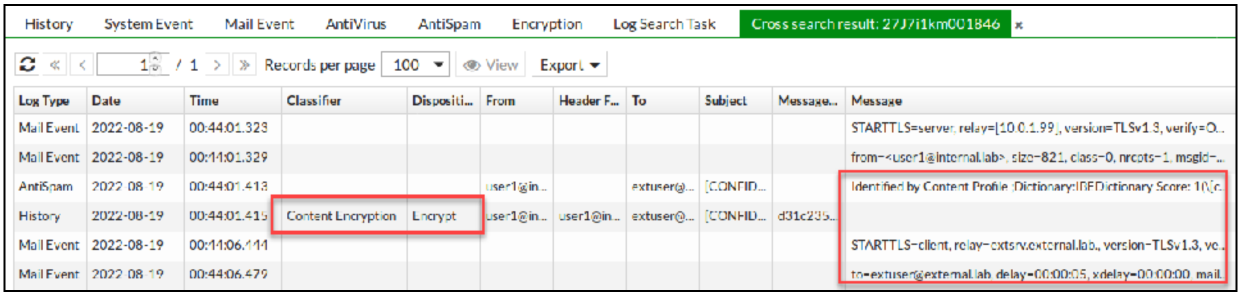
3. Click **Send**.
4. Close Thunderbird.

To verify IBE operations using logs

1. Return to the IntGW FortiMail management GUI, and then click **Monitor** > **Log** > **History**.

   The first entry in the **History** logs should correspond to the email you just sent.

2. Click the **Session ID** link to retrieve the cross-search results.
3. Review the antispam and encryption logs related to the session.



Log Type	Date	Time	Classifier	Dispositi...	From	Header F...	To	Subject	Message...	Message
Mail Event	2022-08-19	00:44:01.323								STARTTLS=server, relay=[10.0.1.99], version=TLSv1.3, verify=O...
Mail Event	2022-08-19	00:44:01.329								from=<user1@internal.lab>, size=821, class=0, nrcpts=1, msgid=...
AntiSpam	2022-08-19	00:44:01.413			user1@in...		extuser@...	[CONFID...		Identified by Content Profile :Dictionary:IBEDictionary Score: 10(c...
History	2022-08-19	00:44:01.415	Content Encryption	Encrypt	user1@in...	user1@in...	extuser@...	[CONFID...	d31c235...	
Mail Event	2022-08-19	00:44:06.444								STARTTLS=client, relay=extsrv.external.lab., version=TLSv1.3, ve...
Mail Event	2022-08-19	00:44:06.479								to=extuser@external.lab, delay=00:00:05, xdelay=00:00:00, mail...

4. You will retrieve this email in the next lab lesson.
5. Log out of the IntGW FortiMail management GUI.

Exercise 3: Accessing IBE Emails

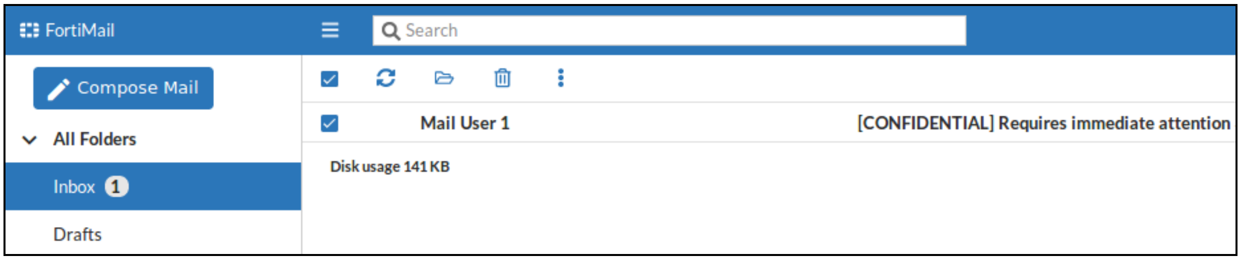
In this exercise, you will register a new IBE user. Then, you will log in to the secure portal to retrieve the IBE email. You will also see the message read notification that the sender receives after the IBE user has read the IBE email.

Register an IBE User

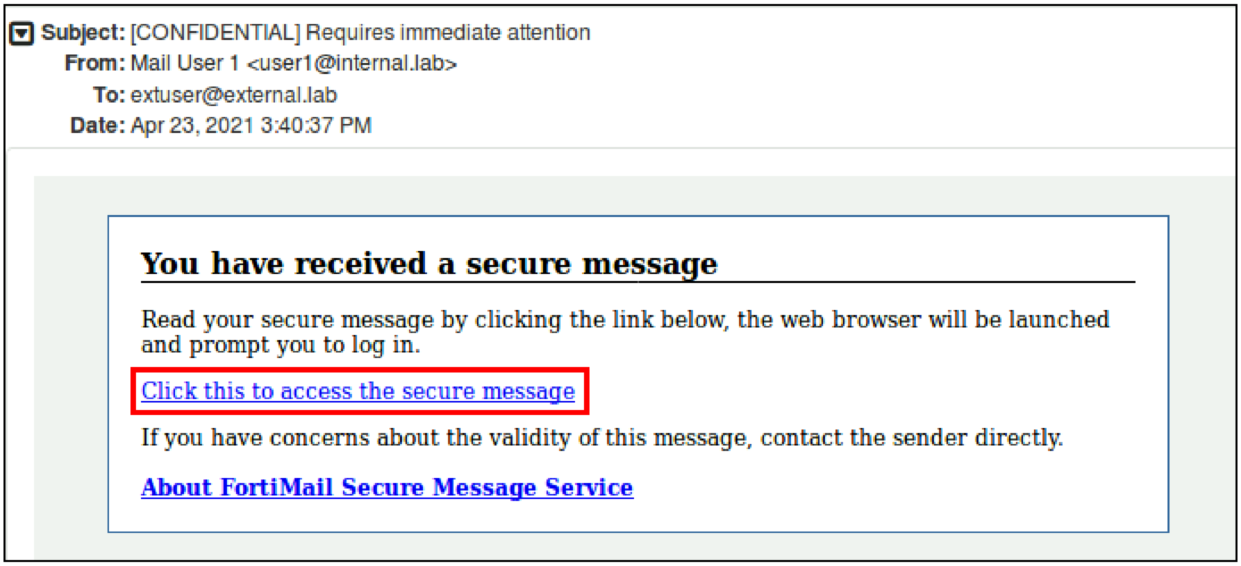
You will register an IBE user. To register, you must submit your name, create a password, and answer three password recovery questions.

To register an IBE user

1. Go to the Linux-Client VM.
2. Open a browser, and then on the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
3. Open the IBE notification email.



4. Click the link in the notification email.



Subject: [CONFIDENTIAL] Requires immediate attention
From: Mail User 1 <user1@internal.lab>
To: extuser@external.lab
Date: Apr 23, 2021 3:40:37 PM

You have received a secure message

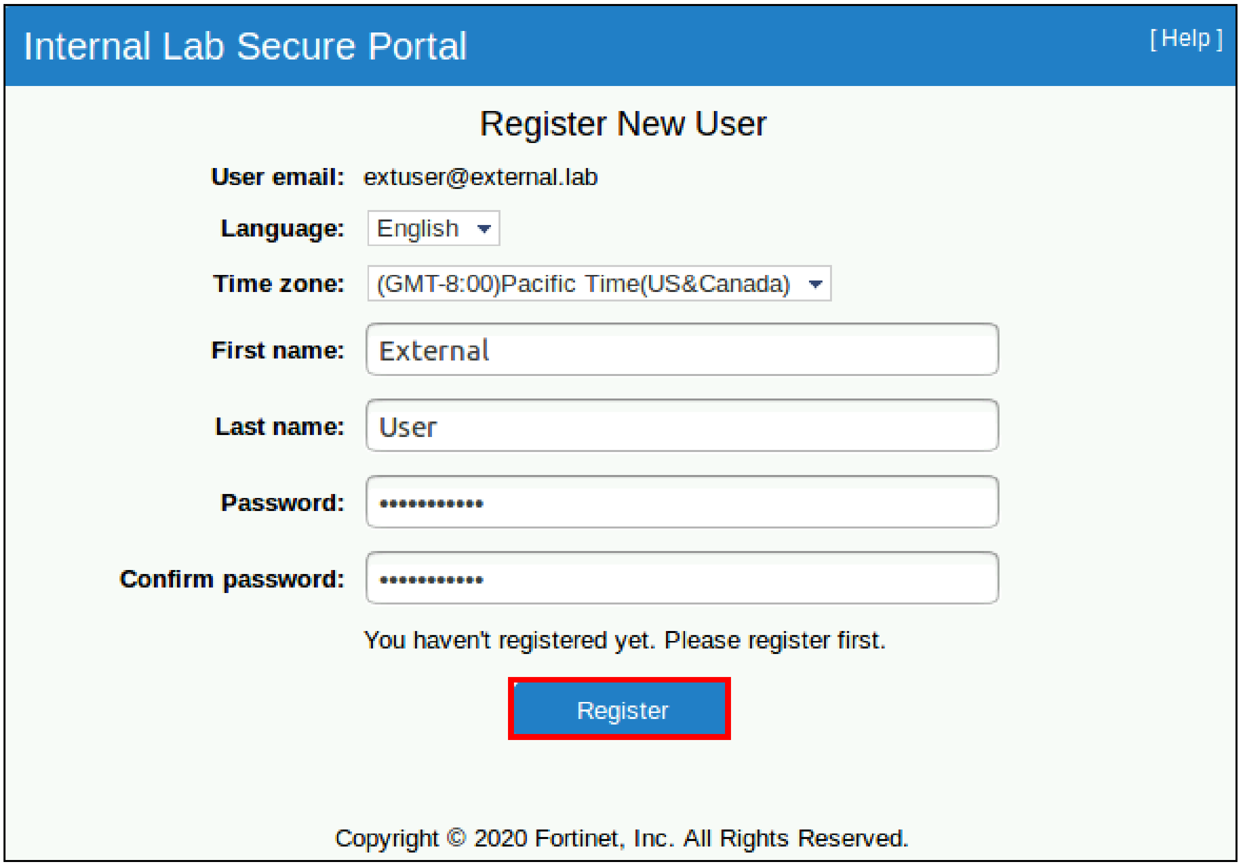
Read your secure message by clicking the link below, the web browser will be launched and prompt you to log in.

Click this to access the secure message

If you have concerns about the validity of this message, contact the sender directly.

About FortiMail Secure Message Service

5. Complete the registration form, and then click **Register**.



Internal Lab Secure Portal [Help]

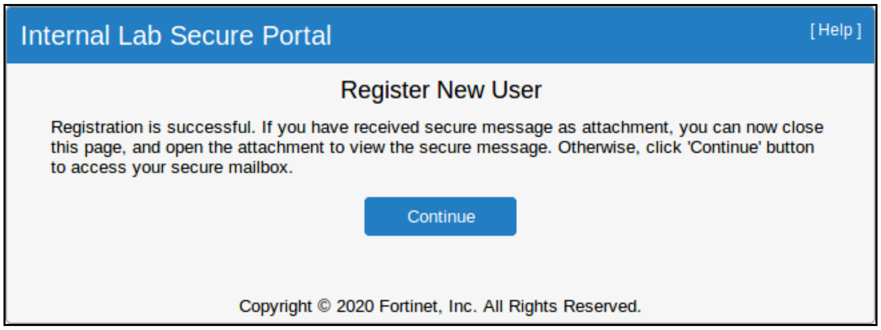
Register New User

User email:	extuser@external.lab
Language:	English
Time zone:	(GMT-8:00)Pacific Time(US&Canada)
First name:	External
Last name:	User
Password:	••••••••••••
Confirm password:	••••••••••••

You haven't registered yet. Please register first.

Copyright © 2020 Fortinet, Inc. All Rights Reserved.

The FortiMail IBE webmail GUI displays a notification that the registration was successful.



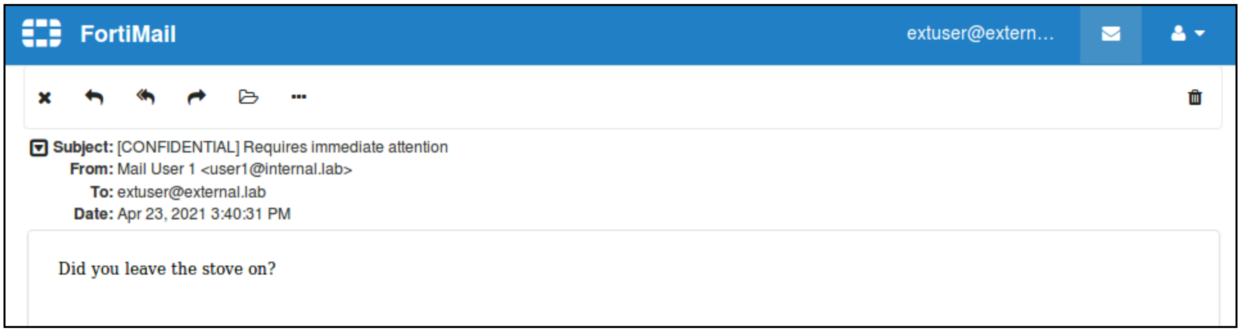
Internal Lab Secure Portal [Help]

Register New User

Registration is successful. If you have received secure message as attachment, you can now close this page, and open the attachment to view the secure message. Otherwise, click 'Continue' button to access your secure mailbox.

Copyright © 2020 Fortinet, Inc. All Rights Reserved.

Then, you are redirected to the contents of the IBE email.



Subject: [CONFIDENTIAL] Requires immediate attention
From: Mail User 1 <user1@internal.lab>
To: extuser@external.lab
Date: Apr 23, 2021 3:40:31 PM

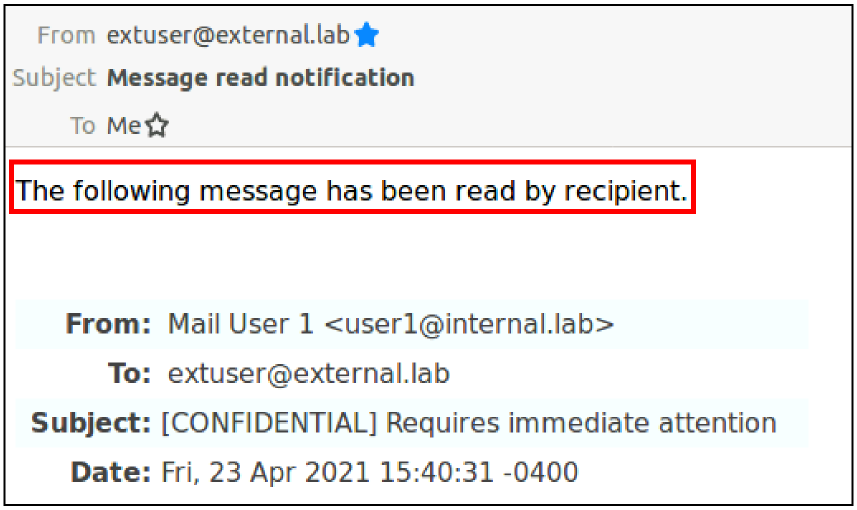
Did you leave the stove on?

6. Reply to the IBE email message.
7. Log out of the IBE webmail GUI.
8. Log out of the ExtSRV FortiMail webmail GUI.

To access the message read notification

1. On the Linux-Client VM, open Thunderbird.
2. View the email with the subject **Message read notification**.

   This notification email is generated when `extuser@external.lab` opens the IBE email.



From extuser@external.lab
Subject **Message read notification**
To Me

The following message has been read by recipient.

From: Mail User 1 <user1@internal.lab>
To: extuser@external.lab
Subject: [CONFIDENTIAL] Requires immediate attention
Date: Fri, 23 Apr 2021 15:40:31 -0400

3. Close Thunderbird.

Lab 9: High Availability

In this lab, you will build an active-passive FortiMail high availability (HA) cluster with two FortiMail VMs. The cluster will operate in server mode.

You will configure IntSRV FortiMail (`10.0.1.99`) as the primary device and IntGW FortiMail (`10.0.1.11`) as the secondary device. You will verify the HA and configuration synchronization status, configure a virtual IP, and use the HA service monitor to detect when the SMTP service connectivity fails on the primary FortiMail device.

The DNS server in the lab network has the following CNAME records to help identify the two clustered devices:

- `primary CNAME intsrv.internal.lab`
- `secondary CNAME intgw.internal.lab`

Objectives

- Configure an active-passive HA cluster
- Verify the health of the cluster
- Configure a virtual IP for the HA cluster
- Configure remote service monitoring

Time to Complete

Estimated: 40 minutes

Prerequisites

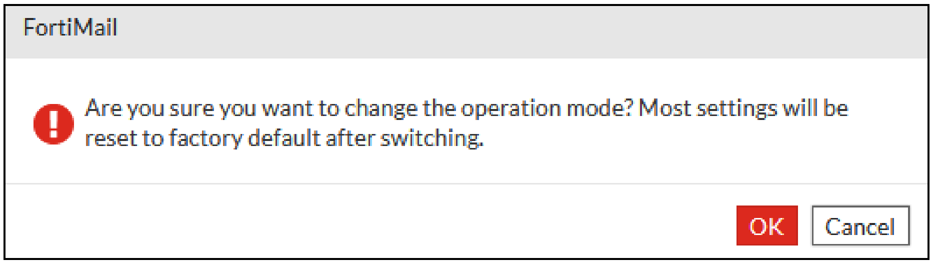
Before beginning this lab, you must change the operation mode of IntGW FortiMail.

To change the operation mode of IntGW FortiMail

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Dashboard** > **Status**.
3. On the **System information** widget, in the **Operation mode** drop-down list, select **Server**.

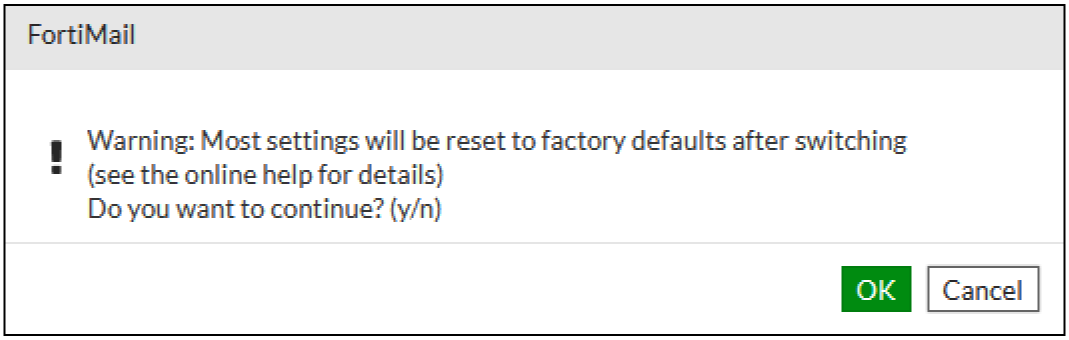
   The system prompts you twice to confirm that you want to proceed.

4. Click **OK** in both windows.



FortiMail

Are you sure you want to change the operation mode? Most settings will be reset to factory default after switching.



FortiMail

Warning: Most settings will be reset to factory defaults after switching (see the online help for details)
Do you want to continue? (y/n)

5. Wait for IntGW FortiMail to restart.

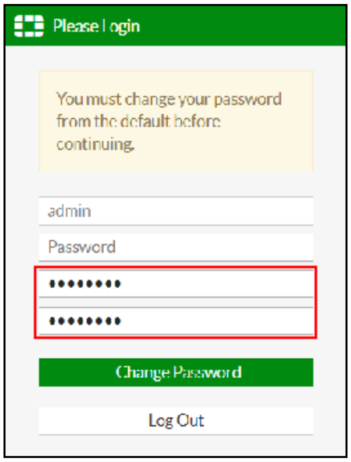
The IP address for port1 on IntGW FortiMail persists after changing the operation mode. After the restart, you will be able to access the IntGW FortiMail management GUI again.

To verify the IntGW FortiMail configuration

1. Log in to the IntGW FortiMail management GUI with the username `admin` and leave the **password** field empty.

   You are presented with a password change prompt.

2. In both **Choose a new password** fields, type `password`.



Please Login

You must change your password from the default before continuing.

admin

Password

••••••••

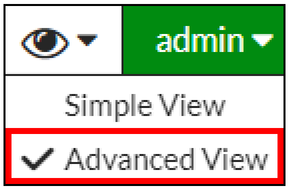
••••••••

3. Click **Change Password**.

   The login page is displayed.

4. Log in with the username `admin` and password `password`.

5. In the upper-right corner of the screen, click the view icon (👁), and then click **Advanced View**.



6. Verify that the following system settings have not been reset:

- Interface (**System** > **Network** > **Interface**)
- Route (**System** > **Network** > **Routing**)
- DNS (**System** > **Network** > **DNS**)

7. Verify the status of the following mail settings—the settings should be reset to factory default values:

- Mail server settings (**System** > **Mail Setting** > **Mail Server Setting**)
- Domains (**Domain & User** > **Domain** > **Domain**)

IntGW FortiMail is ready to be configured as a secondary device in the cluster.

Caution: When doing the lab exercises, ensure you apply the configuration changes to the correct FortiMail VM.

If, at any point, you want to reset the configuration state for the FortiMail VMs, you can restore the following configuration files:

IntSRV FortiMail (primary):

```
Desktop\Resources\Starting Configs\Lab 9\09_Reset_InSRV.tgz
```

IntGW FortiMail (secondary):

```
Desktop\Resources\Starting Configs\Lab 9\09_Reset_IntGW.tgz
```

Always restore the secondary FortiMail first, and then the primary FortiMail. The configuration files restore the VMs to the standalone states they were in after you completed Secure Communications on page 129.

8. Log out of the IntGW FortiMail management GUI.

Exercise 1: stConfiguring HA

In this exercise, you will configure an active-passive cluster with two FortiMail VMs.

Configure the Mail Server Settings on the Primary FortiMail

You will configure the mail server settings on the primary FortiMail.

Take the Expert Challenge!

Configure the host name of the primary FortiMail (IntSRV `10.0.1.99`) as `primary`.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure the HA Settings on the Primary FortiMail on page 147.

To configure the mail server settings on the primary FortiMail

1. On the primary FortiMail (IntSRV) management GUI, log in with the username `admin` and password `password`.
2. Click **System** > **Mail Setting** > **Mail Server Setting**.
3. In the **Host name** field, type `primary`.
4. Click **Apply**.

Configure the HA Settings on the Primary FortiMail

You will configure the HA settings on the primary FortiMail.

Take the Expert Challenge!

On the primary FortiMail (IntSRV `10.0.1.99`), configure the HA role of master.

On failure, the primary FortiMail (IntSRV) should wait for recovery, and then restore to the original role.

Configure authentication for the cluster. Use the string `fortinet`.

Enable the backing up of mail data and MTA queues.

Configure port1 as a primary heartbeat port, enable port monitoring, and peer with the secondary FortiMail (IntGW `10.0.1.11`).

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure the Mail Server Settings on the Secondary FortiMail on page 148.

To configure the HA settings on the primary FortiMail

1. Continuing on the primary FortiMail (IntSRV) management GUI, click **System** > **High Availability** > **Configuration**.
2. Configure the following settings:

Field	Value
HA mode	Primary
On failure	wait for recovery then restore secondary role
Shared password	fortinet

3. Expand the **Advanced options** section.
4. Configure the following settings:

Field	Value
Synchronize mail data directory	Enabled
Synchronize MTA queue directory	Enabled

5. Click **Apply**.
6. In the **Interface** section, double-click **port1**.
7. Configure the following settings:

Field	Value
Enable port monitor	Enabled
Heartbeat status	Primary
Peer IP address	10.0.1.11

8. Click **OK**.
9. Click **Apply**.
10. Log out of the primary FortiMail (IntSRV) management GUI.

Configure the Mail Server Settings on the Secondary FortiMail

You will configure the mail server settings on the secondary FortiMail.

Take the Expert Challenge!

Configure the host name of the secondary FortiMail (IntGW, `10.0.1.11`) as `secondary`.

Configure the local domain name as `internal.lab`.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure the HA Settings on the Secondary FortiMail on page 149.

To configure mail server settings on the secondary FortiMail

1. On the secondary FortiMail (IntGW) management GUI, log in with the username `admin` and password `password`.
2. Click **System** > **Mail Setting** > **Mail Server Setting**.
3. Configure the following settings:

Field	Value
Host name	secondary
Local domain name	internal.lab

4. Click **Apply**.

Configure the HA Settings on the Secondary FortiMail

You will configure the HA settings on the secondary FortiMail.

Take the Expert Challenge!

On the secondary FortiMail (IntGW `10.0.1.11`), configure it to be the secondary FortiMail in a cluster.

On failure, the secondary FortiMail (IntGW) should wait for recovery, and then restore to the original role.

The authentication string for the cluster should be `fortinet`.

Enable the backing up of mail data and MTA queues.

On the secondary FortiMail (IntGW), configure port1 as a primary heartbeat port, enable port monitoring, and configure the peer as the primary FortiMail (IntSRV `10.0.1.99`).

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Verify the HA Status on page 150.

To configure HA on the secondary FortiMail

1. Continuing on the secondary FortiMail (IntGW) management GUI, click **System** > **High Availability** > **Configuration**.
2. Configure the following settings:

Field	Value
HA mode	Secondary
On failure	wait for recovery then restore secondary role
Shared password	fortinet

3. Expand the **Advanced options** section.
4. Configure the following settings:

Field	Value
Synchronize mail data directory	Enabled
Synchronize MTA queue directory	Enabled

5. Click **Apply**.
6. In the **Interface** section, double-click **port1**.
7. Configure the following settings:

Field	Value
Enable port monitor	Enabled
Heartbeat status	Primary
Peer IP address	10.0.1.99

8. Click **OK**.
9. Click **Apply**.

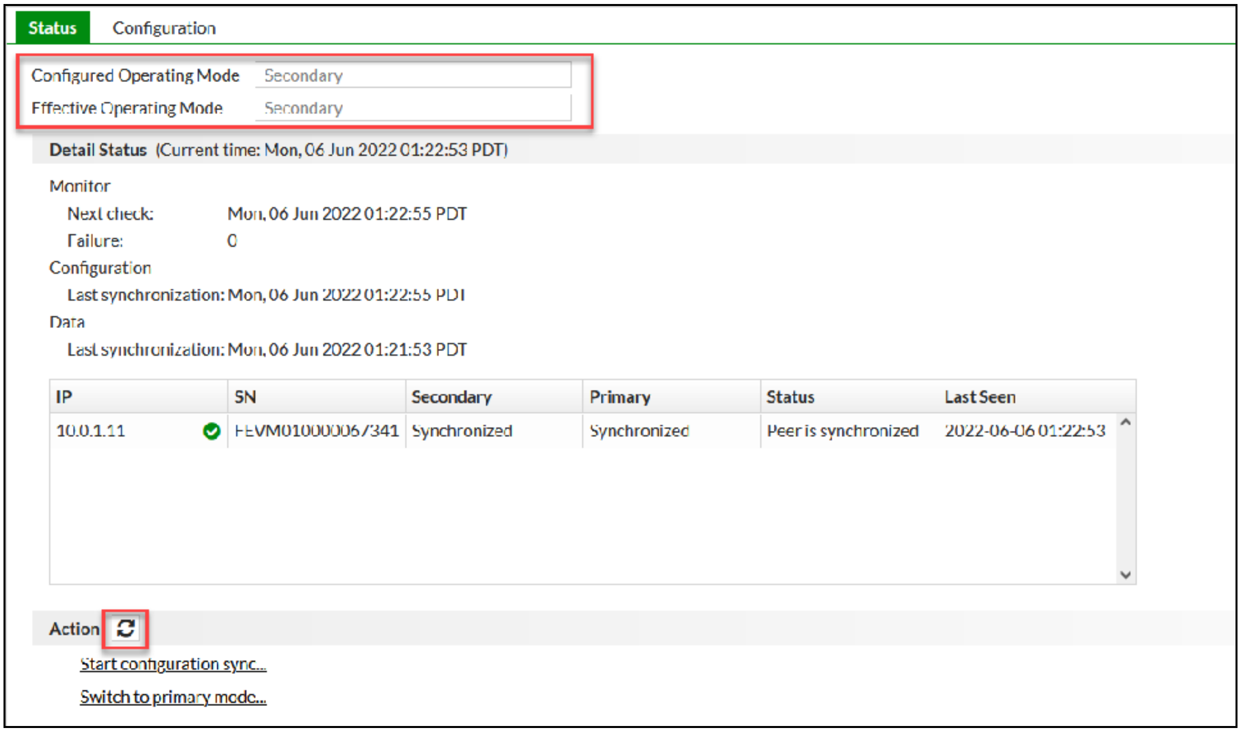
As soon as the two devices join in a cluster and complete synchronization, the secondary FortiMail (IntGW) management GUI session times out and returns to the login prompt. This process may take a few minutes.

Verify the HA Status

You will check the status of the HA cluster.

To verify the HA status

1. Continuing on the secondary FortiMail (IntGW) management GUI, click **System** > **High Availability** > **Status**.
2. Click the refresh icon beside **Action** to update the daemon status.



Configured Operating Mode	Secondary
Effective Operating Mode	Secondary

Detail Status (Current time: Mon, 06 Jun 2022 01:22:53 PDT)

Monitor
Next check: Mon, 06 Jun 2022 01:22:55 PDT
Failure: 0

Configuration
Last synchronization: Mon, 06 Jun 2022 01:22:55 PDT

Data
Last synchronization: Mon, 06 Jun 2022 01:21:53 PDT

IP	SN	Secondary	Primary	Status	Last Seen
10.0.1.11 ✓	FEVM010000067341	Synchronized	Synchronized	Peer is synchronized	2022-06-06 01:22:53

3. Log out of the secondary FortiMail (IntGW) management GUI.

Exercise 2: Verifying the Health of the Cluster

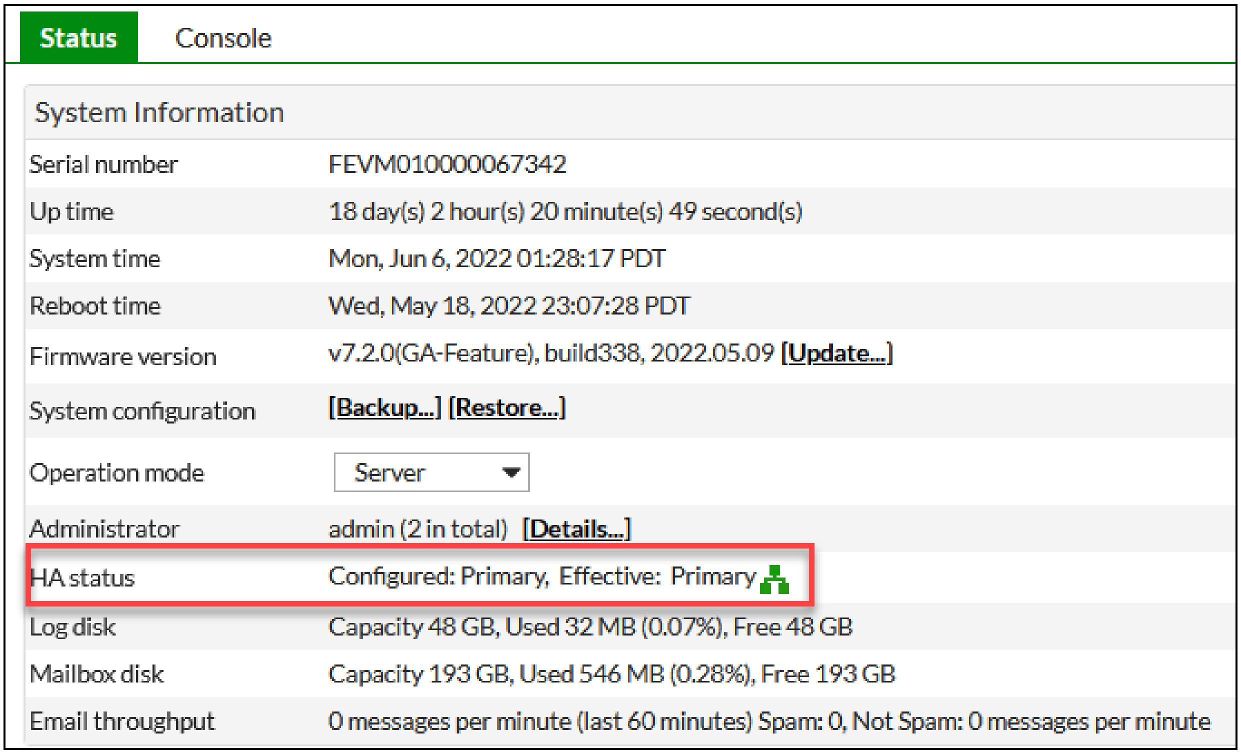
In this exercise, you will verify the status of both HA and the configuration synchronization for the FortiMail cluster.

Verify the HA Status

You will verify the status of the HA cluster and configuration synchronization between the cluster members.

To verify the HA status of the primary FortiMail

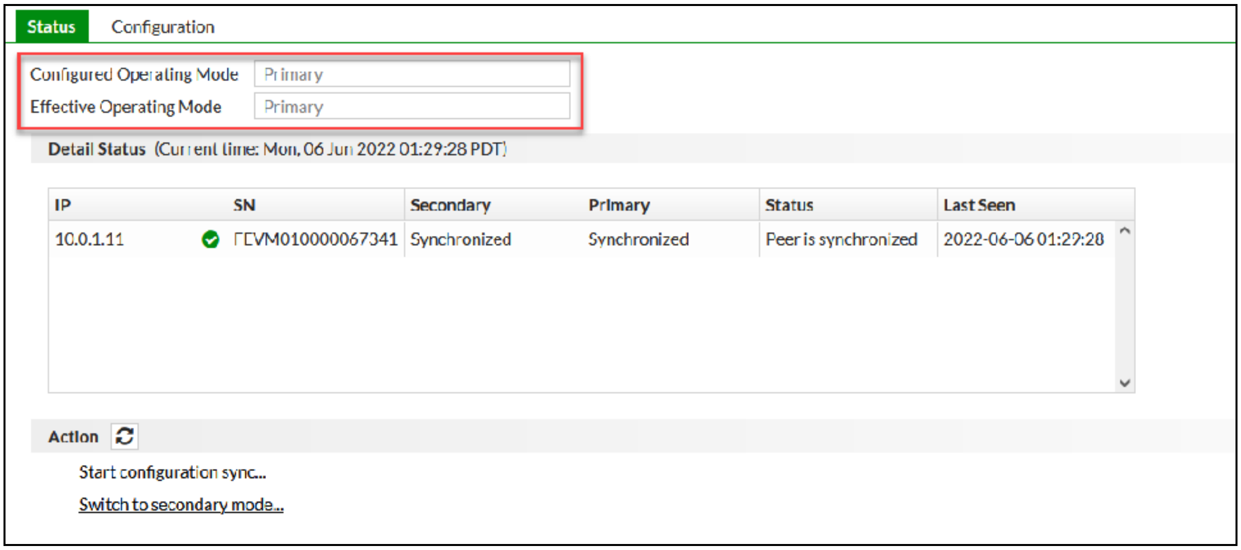
1. On the primary FortiMail (IntSRV) management GUI, log in with the username `admin` and password `password`.
2. On the **System Information** widget, verify that the **HA status** values are **Configured: Primary, Effective: Primary**.



System Information

Serial number	FEVM010000067342
Up time	18 day(s) 2 hour(s) 20 minute(s) 49 second(s)
System time	Mon, Jun 6, 2022 01:28:17 PDT
Reboot time	Wed, May 18, 2022 23:07:28 PDT
Firmware version	v7.2.0(GA-Feature), build338, 2022.05.09 [Update...]
System configuration	[Backup...] [Restore...]
Operation mode	Server
Administrator	admin (2 in total) [Details...]
HA status	Configured: Primary, Effective: Primary
Log disk	Capacity 48 GB, Used 32 MB (0.07%), Free 48 GB
Mailbox disk	Capacity 193 GB, Used 546 MB (0.28%), Free 193 GB
Email throughput	0 messages per minute (last 60 minutes) Spam: 0, Not Spam: 0 messages per minute

3. Click **System** > **High Availability** > **Status** to find the same information.



Configured Operating Mode: Primary
Effective Operating Mode: Primary

Detail Status (Current time: Mon, 06 Jun 2022 01:29:28 PDT)

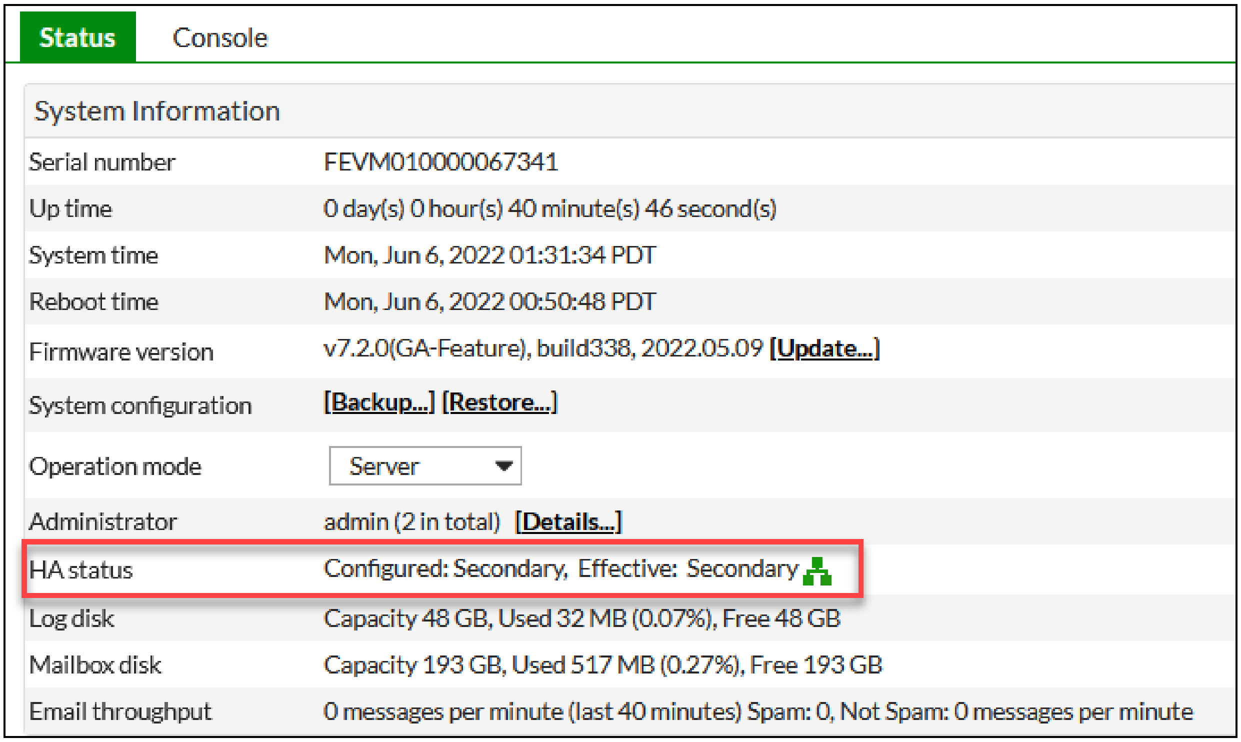
IP	SN	Secondary	Primary	Status	Last Seen
10.0.1.11	✓ FEVM010000067341	Synchronized	Synchronized	Peer is synchronized	2022-06-06 01:29:28

Start configuration sync...

Switch to secondary mode...

To verify the HA status of the secondary FortiMail

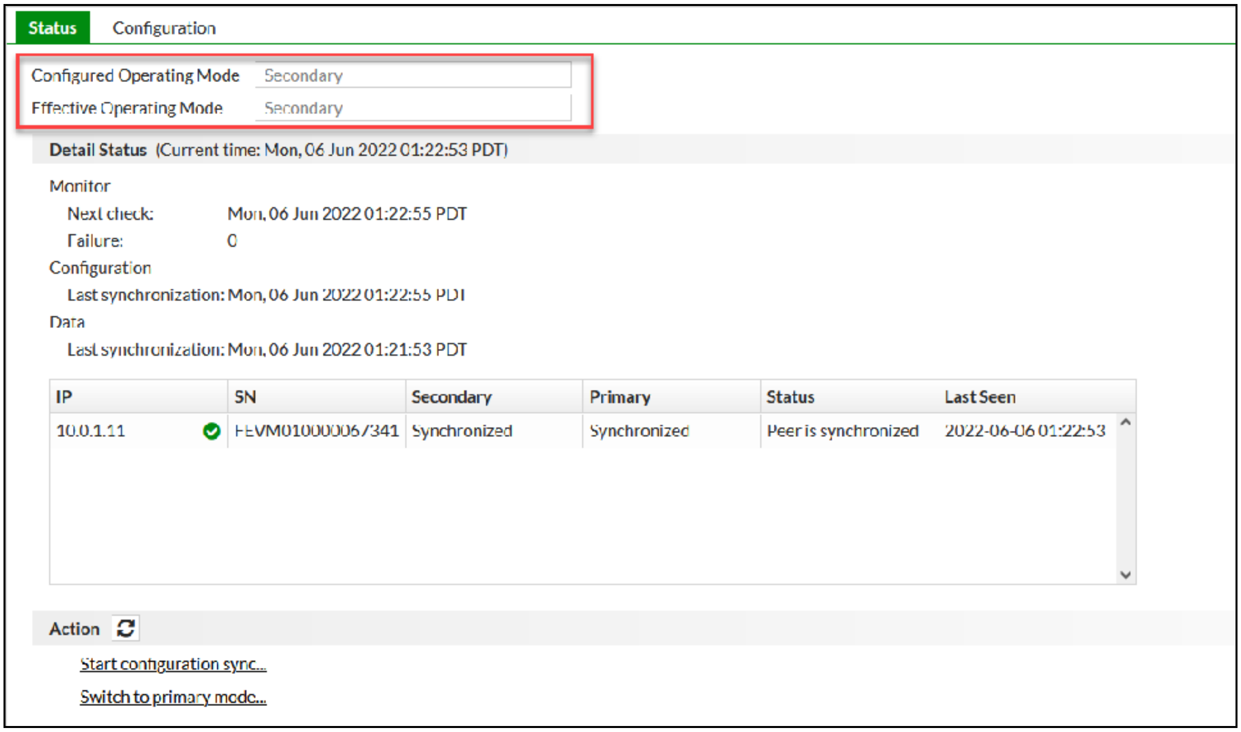
1. On the secondary FortiMail (IntGW) management GUI, log in with the username `admin` and password `password`.
2. On the **System Information** widget, verify that the **HA status** values are **Configured: Secondary, Effective: Secondary**.



System Information

Serial number	FEVM010000067341
Up time	0 day(s) 0 hour(s) 40 minute(s) 46 second(s)
System time	Mon, Jun 6, 2022 01:31:34 PDT
Reboot time	Mon, Jun 6, 2022 00:50:48 PDT
Firmware version	v7.2.0(GA-Feature), build338, 2022.05.09 [Update...]
System configuration	[Backup...] [Restore...]
Operation mode	Server
Administrator	admin (2 in total) [Details...]
HA status	Configured: Secondary, Effective: Secondary
Log disk	Capacity 48 GB, Used 32 MB (0.07%), Free 48 GB
Mailbox disk	Capacity 193 GB, Used 517 MB (0.27%), Free 193 GB
Email throughput	0 messages per minute (last 40 minutes) Spam: 0, Not Spam: 0 messages per minute

3. Click **System** > **High Availability** > **Status** to find the same information.



Configured Operating Mode: Secondary
Effective Operating Mode: Secondary

Detail Status (Current time: Mon, 06 Jun 2022 01:22:53 PDT)

Monitor
Next check: Mon, 06 Jun 2022 01:22:55 PDT
Failure: 0
Configuration
Last synchronization: Mon, 06 Jun 2022 01:22:55 PDT
Data
Last synchronization: Mon, 06 Jun 2022 01:21:53 PDT

IP	SN	Secondary	Primary	Status	Last Seen
10.0.1.11 ✓	FEVM01000067341	Synchronized	Synchronized	Peer is synchronized	2022-06-06 01:22:53

To verify the configuration synchronization

1. Continuing on the secondary FortiMail (IntGW) management GUI, click **Domain & User** > **Domain** > **Domain**.
2. Verify that the **internal.lab** domain configuration has been synchronized from the primary FortiMail (IntSRV).
3. Click **Domain & User** > **User** > **User**.
4. Verify that the `internal.lab` domain user configuration has been synchronized from the primary FortiMail (IntSRV).
5. Click **Profile** > **LDAP** > **LDAP**.
6. Verify that the LDAP profile configuration has been synchronized from the primary FortiMail (IntSRV).
7. Return to the primary FortiMail (IntSRV) management GUI, and then click **Policy** > **Recipient Policy** > **Inbound**.
8. Click **New**.
9. Click **Create**.
10. Return to the secondary FortiMail (IntGW) management GUI, and then click **Policy** > **Recipient Policy** > **Inbound**.
11. Verify that the new recipient policy has been synchronized from the primary FortiMail (IntSRV).

Verify the HA Synchronization Status on the CLI

You will use CLI commands to verify the status of HA synchronization. The checksum for both FortiMail VMs should match, indicating that the cluster is in sync.

To verify the HA synchronization status on the CLI

1. Open an SSH connection to the primary FortiMail (IntSRV).
2. Enter the following command to display the configuration checksum for the primary FortiMail (IntSRV):

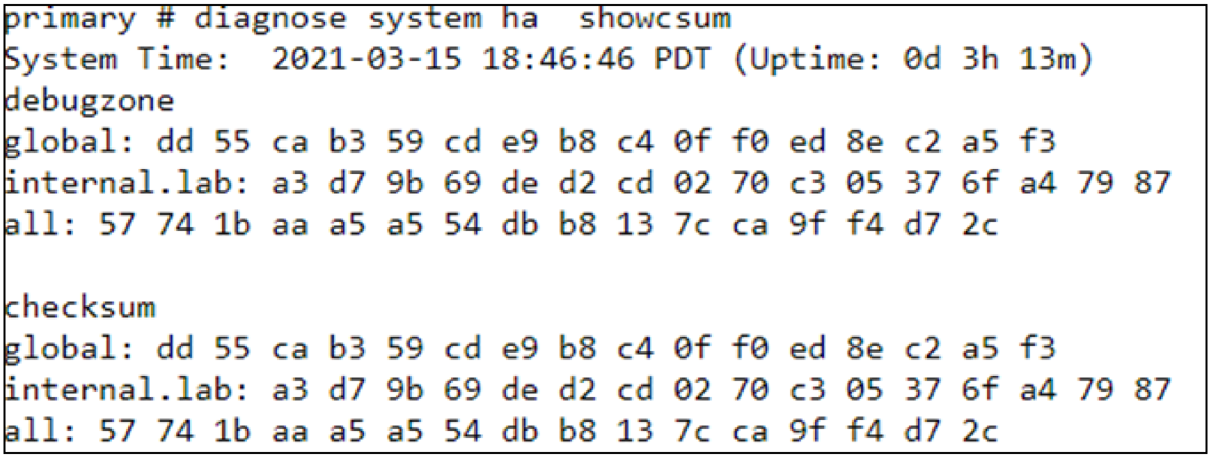
```
diagnose system ha showcsum
```

3. Open an SSH connection to the secondary FortiMail (IntGW).
4. Enter the following command to display the configuration checksum for the secondary FortiMail (IntGW):

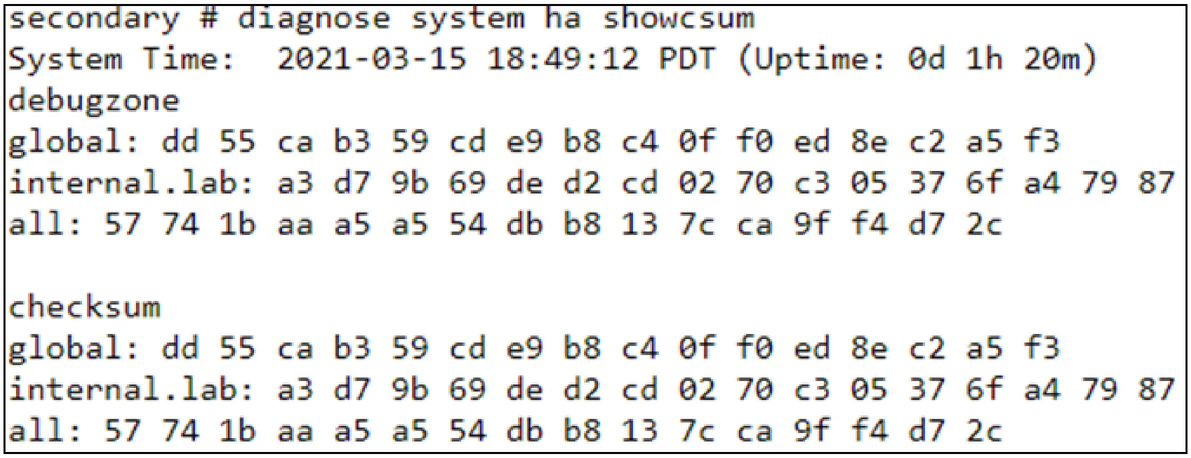
```
diagnose system ha showcsum
```

5. Compare the checksum values of the two FortiMail VMs.

   If they match, their configurations are in sync.



```
primary # diagnose system ha  showcsum
System Time:  2021-03-15 18:46:46 PDT (Uptime: 0d 3h 13m)
debugzone
global: dd 55 ca b3 59 cd e9 b8 c4 0f f0 ed 8e c2 a5 f3
internal.lab: a3 d7 9b 69 de d2 cd 02 70 c3 05 37 6f a4 79 87
all: 57 74 1b aa a5 a5 54 db b8 13 7c ca 9f f4 d7 2c

checksum
global: dd 55 ca b3 59 cd e9 b8 c4 0f f0 ed 8e c2 a5 f3
internal.lab: a3 d7 9b 69 de d2 cd 02 70 c3 05 37 6f a4 79 87
all: 57 74 1b aa a5 a5 54 db b8 13 7c ca 9f f4 d7 2c
```



```
secondary # diagnose system ha showcsum
System Time:  2021-03-15 18:49:12 PDT (Uptime: 0d 1h 20m)
debugzone
global: dd 55 ca b3 59 cd e9 b8 c4 0f f0 ed 8e c2 a5 f3
internal.lab: a3 d7 9b 69 de d2 cd 02 70 c3 05 37 6f a4 79 87
all: 57 74 1b aa a5 a5 54 db b8 13 7c ca 9f f4 d7 2c

checksum
global: dd 55 ca b3 59 cd e9 b8 c4 0f f0 ed 8e c2 a5 f3
internal.lab: a3 d7 9b 69 de d2 cd 02 70 c3 05 37 6f a4 79 87
all: 57 74 1b aa a5 a5 54 db b8 13 7c ca 9f f4 d7 2c
```

6. Close both SSH sessions.
7. Log out of the primary FortiMail (IntSRV) management GUI.
8. Log out of the secondary FortiMail (IntGW) management GUI.

Exercise 3: Configuring a Virtual IP for the HA Cluster

In this exercise, you will configure a virtual IP for the HA cluster. You will also verify the virtual IP function by forcing a failover.

Configure a Virtual IP on the Primary FortiMail

You will configure a virtual IP for the FortiMail cluster.

Take the Expert Challenge!

Configure a virtual IP for the FortiMail cluster. Use the IP address `10.0.1.100`.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Verify the Virtual IP Configuration on page 157.

To configure a virtual IP on the primary FortiMail

1. On the primary FortiMail (IntSRV) management GUI, log in with the username `admin` and password `password`.
2. Click **System** > **High Availability** > **Configuration**.
3. In the **Interface** section, double-click **port1**.
4. Configure the following settings:

Field	Value
Virtual IP action	Use
Virtual IP address	10.0.1.100/24

5. Click **OK**.
6. Click **Apply**.
7. Log out of the primary FortiMail (IntSRV) management GUI.

To configure a virtual IP on the secondary FortiMail

1. On the secondary FortiMail (IntGW) management GUI, log in with the username `admin` and password `password`.
2. Click **System** > **High Availability** > **Configuration**.
3. In the **Interface** section, double-click **port1**.
4. Configure the following settings:

Field	Value
Virtual IP action	Use
Virtual IP address	10.0.1.100/24

5. Click **OK**.
6. Click **Apply**.
7. Log out of the secondary FortiMail (IntGW) management GUI.

Verify the Virtual IP Configuration

You will verify the virtual IP configuration for the cluster by accessing the FortiMail management GUI.

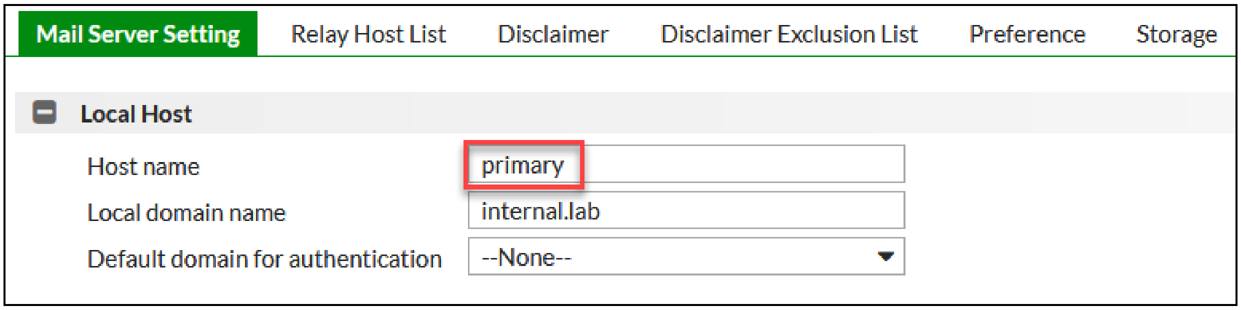
To verify the virtual IP configuration

1. On the Linux-Client VM, open a new browser, and then go to the virtual IP to access the FortiMail management GUI:

```
https://10.0.1.100/admin
```

Ignore any security warnings generated by your browser. These relate to the CN field and the signer of the self-signed FortiMail certificate.

2. Log in with the username `admin` and password `password`.
3. Click **System** > **Mail Setting** > **Mail Server Setting**.
4. Verify the **Host name** of the current FortiMail that owns the virtual IP.



Host name: primary
Local domain name: internal.lab
Default domain for authentication: --None--

Trigger a Cluster Failover

You will trigger a cluster failover and verify that the failover was successful.

To trigger a cluster failover

1. Continuing on the FortiMail cluster management GUI, click **System** > **High Availability** > **Status**.
2. In the **Actions** section, click **Switch to secondary mode**.

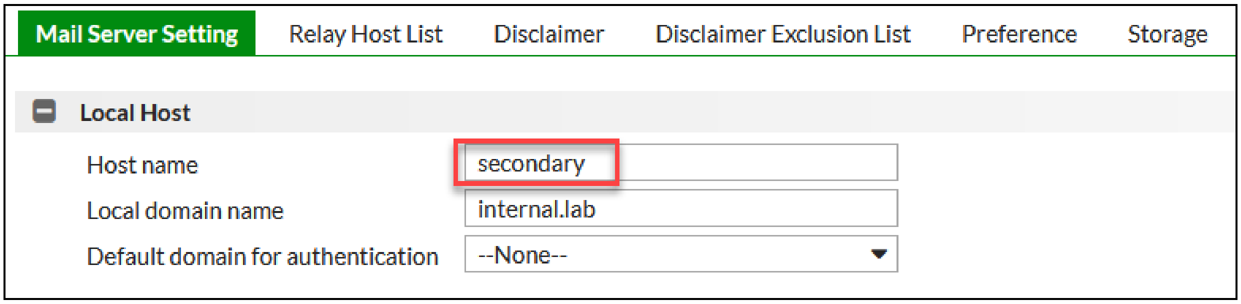
3. Click **OK**.
4. Click **OK**.

   After a few seconds, you are redirected to the login prompt.

5. Log in with the username `admin` and password `password`.

To verify the virtual IP after failover

1. Continuing on the FortiMail cluster management GUI, click **System** > **Mail Setting** > **Mail Server Setting**.
2. Verify the **Host name** of the current FortiMail that owns the virtual IP.



Host name: secondary

Local domain name: internal.lab

Default domain for authentication: --None--

Restore the Cluster

You will restore the cluster to its original state.

To restore the cluster

1. Continuing on the FortiMail cluster management GUI, click **System** > **High Availability** > **Status**.
2. In the **Actions** section, click **Restore to configured operating mode**.
3. Click **OK**.
4. Click **OK**.

   After a few seconds, you are redirected to the primary FortiMail (IntSRV) management GUI session.

5. Click **System** > **Mail Setting** > **Mail Server Setting**.
6. Verify that the primary FortiMail now owns the cluster virtual IP.
7. Close the browser on Linux-Client.

Exercise 4: Monitoring Remote Services

In this exercise, you will configure remote SMTP service monitoring on both devices in the cluster. Then, you will trigger a service-based failover to verify the configuration, and then verify the failover using event logs.

Configure SMTP Service Monitoring on the Primary FortiMail

You will configure remote SMTP service monitoring on the primary FortiMail.

Take the Expert Challenge!

On the primary FortiMail (IntSRV), configure SMTP service monitoring of the secondary FortiMail (IntGW `10.0.1.11`).

The SMTP connectivity test should occur every 30 seconds.

If the connection attempt times out for 10 seconds, it should be considered a failure.

After two retries, the cluster should trigger a failover.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure SMTP Service Monitoring on the Secondary FortiMail on page 160.

To configure SMTP service monitoring on the primary FortiMail

1. On the primary FortiMail (IntSRV) management GUI, log in with the username `admin` and password `password`.
2. Click **System** > **High Availability** > **Configuration**.
3. In the **Service Monitor** section, double-click **Remote SMTP**.
4. Configure the following settings:

Field	Value
Enable	Enabled
Remote IP	10.0.1.11
Timeout	10
Interval	30
Retries	2

For the purposes of this lab, you are reducing the time values to their lowest configurable value to speed things up. In a live production environment, the default values are a good place to start. You can fine-tune them as you discover what kind of outage your email network can tolerate.

5. Click **OK**.
6. Click **Apply**.

Configure SMTP Service Monitoring on the Secondary FortiMail

You will configure SMTP service monitoring on the secondary FortiMail.

Take the Expert Challenge!

On the secondary FortiMail (IntGW), configure SMTP service monitoring of the primary FortiMail (IntSRV, `10.0.1.99`).

The SMTP connectivity test should occur every 30 seconds.

If the connection attempt times out for 10 seconds, it should be considered a failure.

After two retries, the cluster should trigger a failover.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Trigger a Service-Based Failover on page 161.

To configure SMTP service monitoring on the secondary FortiMail

1. On the secondary FortiMail (IntGW) management GUI, log in with the username `admin` and password `password`.
2. Click **System** > **High Availability** > **Configuration**.
3. In the **Service Monitor** section, double-click **Remote SMTP**.
4. Configure the following settings:

Field	Value
Enable	Enabled
Remote IP	10.0.1.99
Timeout	10
Interval	30
Retries	2

5. Click **OK**.
6. Click **Apply**.

Trigger a Service-Based Failover

You will trigger a service-based failover by changing the SMTP service port on the primary FortiMail (IntSRV). The secondary FortiMail (IntGW) will fail to connect to the standard SMTP port (TCP port 25), which should trigger a failover. You will verify the failover using the system event logs.

To trigger a service-based failover

1. Return to the primary FortiMail (IntSRV) management GUI, and then click **System** > **Mail Setting** > **Mail Server Setting**.
2. In the **SMTP port** field, type `125`.
3. Click **Apply**.

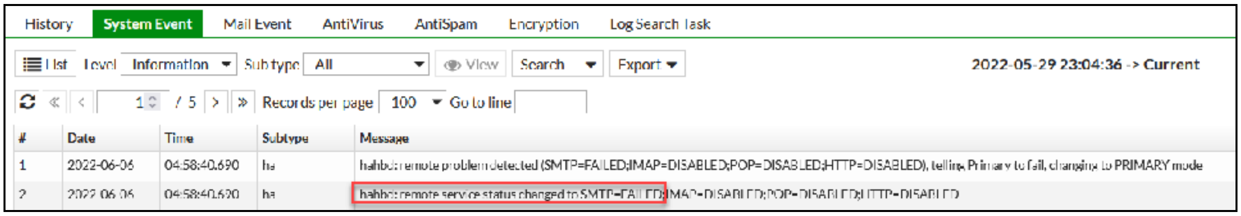
You changed the SMTP service port on the primary FortiMail (IntSRV) to port 125. Because of this change, the secondary FortiMail (IntGW) can no longer detect SMTP services on port 25. This will trigger a failover based on a remote service failure.

You must wait a few minutes for the secondary FortiMail (IntGW) to go through the service monitoring check schedule before a failover is triggered.

To verify the service-based failover

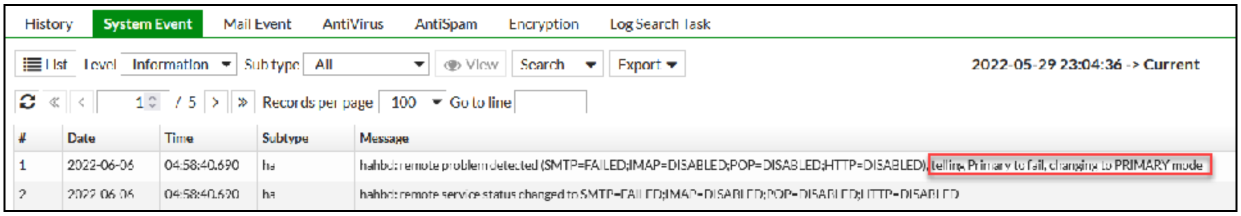
1. Return to the secondary FortiMail (IntGW) management GUI, and then click **Monitor** > **Log** > **System Event**.
2. In the **Sub Type** drop-down list, select **HA**, and then keep clicking the refresh icon to see the latest logs related to HA events.

   Event logs related to the remote SMTP service should appear when the secondary FortiMail (IntGW) detects a failure for the first time.



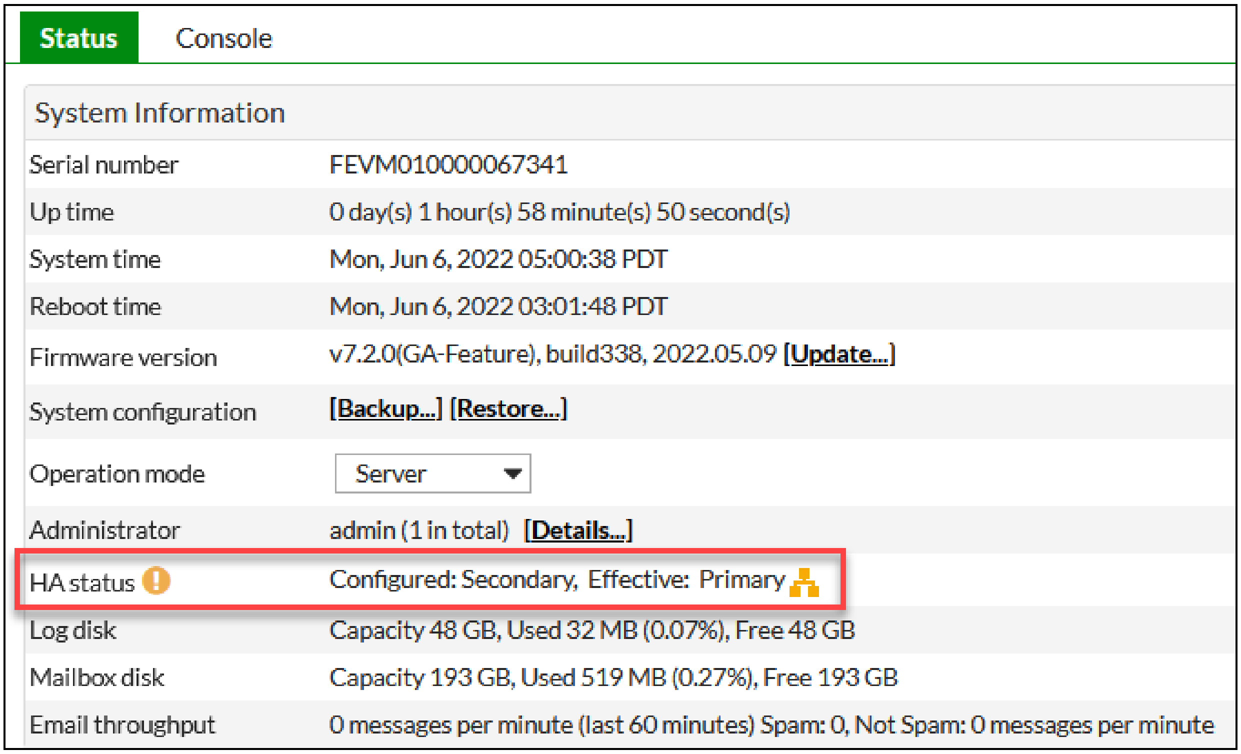
#	Date	Time	Subtype	Message
1	2022-06-06	04:58:40.690	ha	hahbd: remote problem detected (SMTP=FAILED;IMAP=DISABLED;POP=DISABLED;HTTP=DISABLED), telling Primary to fail, changing to PRIMARY mode
2	2022-06-06	04:58:40.620	ha	hahbd: remote service status changed to SMTP=FAILED;IMAP=DISABLED;POP=DISABLED;HTTP=DISABLED

   After the second detection, the secondary FortiMail takes over as the active member.



#	Date	Time	Subtype	Message
1	2022-06-06	04:58:40.690	ha	hahbd: remote problem detected (SMTP=FAILED;IMAP=DISABLED;POP=DISABLED;HTTP=DISABLED), telling Primary to fail, changing to PRIMARY mode
2	2022-06-06	04:58:40.620	ha	hahbd: remote service status changed to SMTP=FAILED;IMAP=DISABLED;POP=DISABLED;HTTP=DISABLED

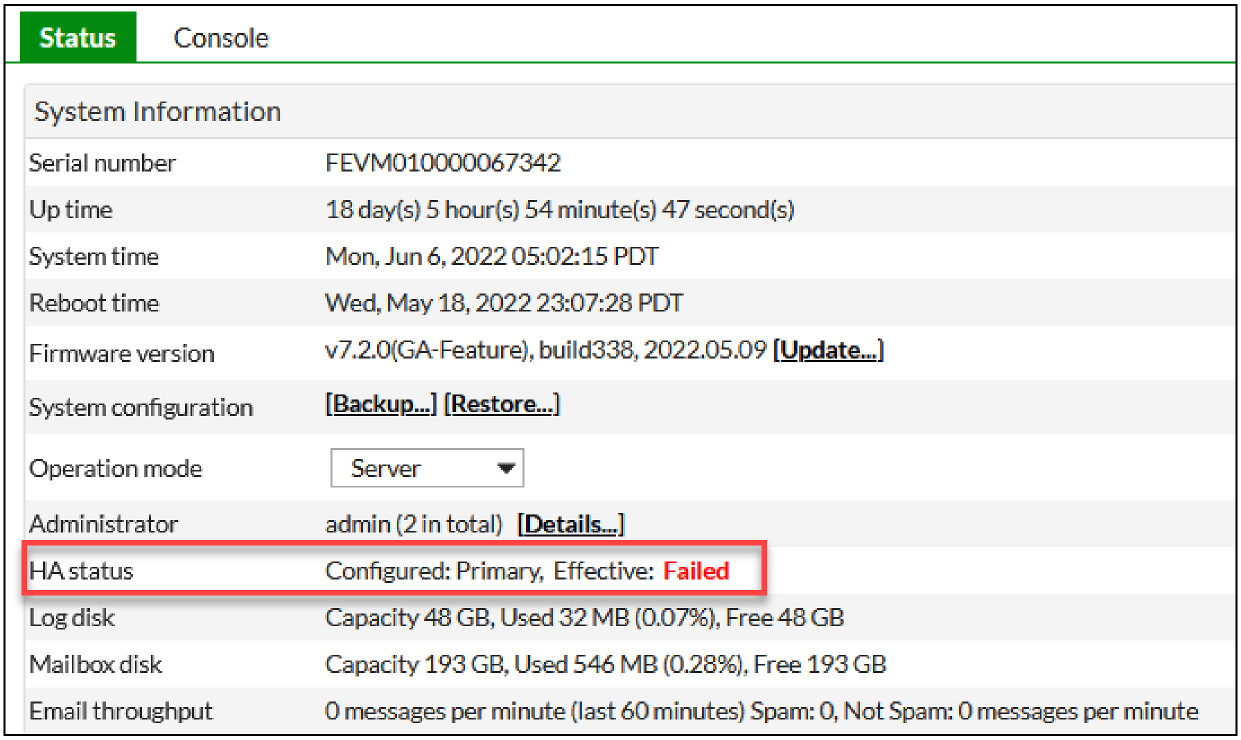
3. Click **Dashboard** > **Status**.
4. On the **System Information** widget, verify that the **HA status** values are **Configured: Secondary, Effective: Primary**.



System Information

Serial number	FEVM010000067341
Up time	0 day(s) 1 hour(s) 58 minute(s) 50 second(s)
System time	Mon, Jun 6, 2022 05:00:38 PDT
Reboot time	Mon, Jun 6, 2022 03:01:48 PDT
Firmware version	v7.2.0(GA-Feature), build338, 2022.05.09 [Update...]
System configuration	[Backup...] [Restore...]
Operation mode	Server
Administrator	admin (1 in total) [Details...]
HA status	Configured: Secondary, Effective: Primary
Log disk	Capacity 48 GB, Used 32 MB (0.07%), Free 48 GB
Mailbox disk	Capacity 193 GB, Used 519 MB (0.27%), Free 193 GB
Email throughput	0 messages per minute (last 60 minutes) Spam: 0, Not Spam: 0 messages per minute

5. Return to the primary FortiMail (IntSRV) management GUI, and then click **Dashboard** > **Status**.
6. On the **System Information** widget, verify that the **HA status** values are **Configured: Primary, Effective: Failed**.



System Information

Serial number	FEVM010000067342
Up time	18 day(s) 5 hour(s) 54 minute(s) 47 second(s)
System time	Mon, Jun 6, 2022 05:02:15 PDT
Reboot time	Wed, May 18, 2022 23:07:28 PDT
Firmware version	v7.2.0(GA-Feature), build338, 2022.05.09 [Update...]
System configuration	[Backup...] [Restore...]
Operation mode	Server
Administrator	admin (2 in total) [Details...]
HA status	Configured: Primary, Effective: Failed
Log disk	Capacity 48 GB, Used 32 MB (0.07%), Free 48 GB
Mailbox disk	Capacity 193 GB, Used 546 MB (0.28%), Free 193 GB
Email throughput	0 messages per minute (last 60 minutes) Spam: 0, Not Spam: 0 messages per minute

This means that the primary FortiMail (IntSRV) has had a failure.

Restore the Cluster

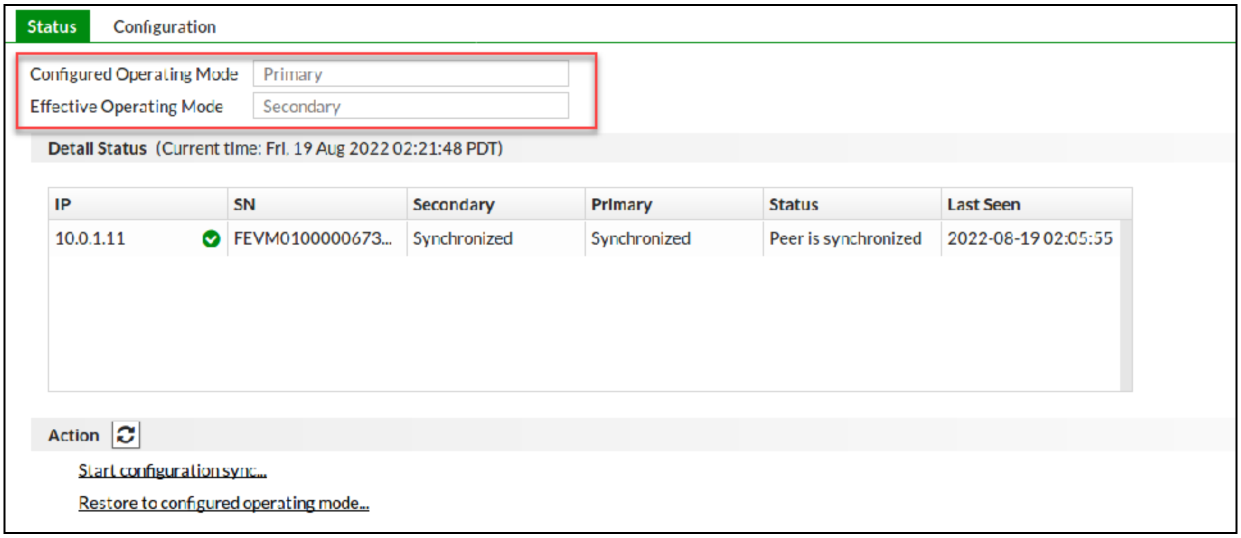
You will restore the SMTP services on the primary FortiMail (IntSRV), which will restore the cluster.

To restore the cluster

1. On the secondary FortiMail (IntGW) management GUI, click **System** > **Mail Setting** > **Mail Server Setting**.
2. In the **SMTP port** field, type `25`.
3. Click **Apply**.

   This setting was synchronized from the primary before failure.

4. Continuing on the primary FortiMail (IntSRV) management GUI, click **System** > **High Availability** > **Status**.
5. In the **Actions** section, click **Restart the HA system**.
6. Click **OK**.
7. Click the **Refresh** button.

Configured Operating Mode	Primary
Effective Operating Mode	Secondary

   Detail Status (Current time: Fri, 19 Aug 2022 02:21:48 PDT)

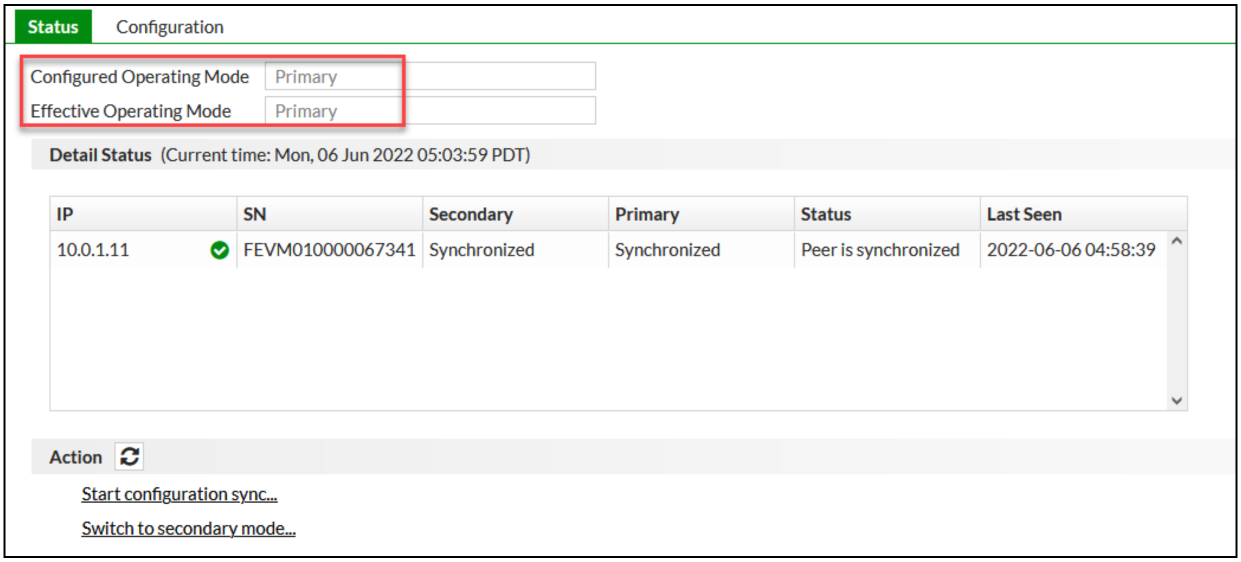
IP	SN	Secondary	Primary	Status	Last Seen
10.0.1.11 ✓	FEVM0100000673...	Synchronized	Synchronized	Peer is synchronized	2022-08-19 02:05:55

   Action
   Start configuration sync...
   Restore to configured operating mode...

   The primary FortiMail (IntSRV) joins the cluster as **Secondary** because that was how it was configured.

8. Click **Restore to configured operating mode**.
9. Click **OK**.
10. Click **OK**.

The primary FortiMail (IntSRV)is now the **Primary** HA member.



Configured Operating Mode: Primary

Effective Operating Mode: Primary

Detail Status (Current time: Mon, 06 Jun 2022 05:03:59 PDT)

IP	SN	Secondary	Primary	Status	Last Seen
10.0.1.11 ✓	FEVM010000067341	Synchronized	Synchronized	Peer is synchronized	2022-06-06 04:58:39

11. Log out of the primary FortiMail (IntSRV) management GUI.

12. Log out of the secondary FortiMail (IntGW) management GUI.

Lab 10: Server Mode

In this lab, you will configure server mode resource profiles, and see their effect on user resource allocation. You will also populate the global address book from the LDAP server.

Objectives

- Configure resource profiles
- Configure LDAP mapping to import a domain address book

Time to Complete

Estimated: 35 minutes

Prerequisites

Before beginning this lab, you must restore a configuration file on the `internal.lab` FortiMail VMs.

To restore a configuration file on IntGW FortiMail

1. On the Linux-Client VM, open a new browser, and then go to the IntGW FortiMail management GUI.
2. Log in with the username `admin` and password `password`.
3. Click **System** > **Maintenance** > **Configuration**.
4. Click **Restore Configuration**.
5. Click **Desktop** > **Resources** > **Starting Configs** > **Lab 10** > `10_Initial_IntGW.tgz`, and then click **Open**.
6. Click **OK**.

To restore a configuration file on IntSRV FortiMail

1. Continuing on the Linux-Client VM, open a new browser tab, and then go to the IntSRV FortiMail management GUI.
2. Log in with the username `admin` and password `password`.
3. Click **System** > **Maintenance** > **Configuration**.
4. Click **Restore Configuration**.
5. Click **Desktop** > **Resources** > **Starting Configs** > **Lab 10** > `10_Initial_IntSRV.tgz`, and then click **Open**.
6. Click **OK**.
7. Wait for the VMs to finish restarting before proceeding with the exercise.

The configuration files will restore the FortiMail VMs to a similar state they were in before you completed High Availability on page 144.

Exercise 1: Configuring Resource Profiles

In this exercise, you will review the IntSRV FortiMail configuration. Then, you will configure resource profiles and observe their effects on resource allocation for email users.

Review the Server Mode Configuration

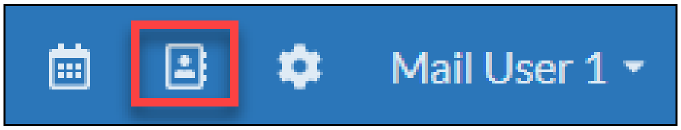
You will review the server mode webmail interface, which comes with all the standard mailbox features. You will also verify the default disk limit for users.

To review the server mode configuration

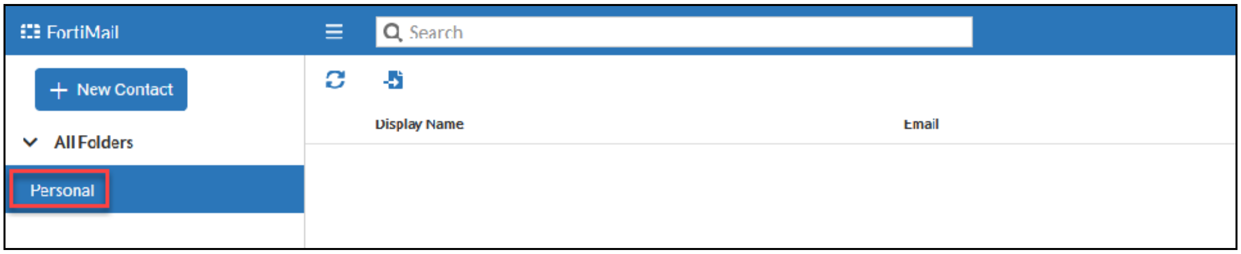
1. On the IntSRV FortiMail webmail GUI, log in with the username `user1` and password `fortinet`.
2. View the **Disk Usage** value.

If there are no resource profiles or domain-level service settings configured, there is a system default disk limit of 500 MB for each user mailbox.

3. Click the address book icon.



The address books are displayed.



If there are no resource profiles configured, server mode users have access to their personal address book only.

4. Log out of the `user1@internal.lab` account.

Configure Resource Profiles

You will configure new resource profiles on IntSRV FortiMail.

Take the Expert Challenge!

On IntSRV FortiMail, create two new resource profiles, and name them `PowerUsers` and `RegularUsers` respectively.

The profiles should be available for the `internal.lab` domain only.

The `PowerUsers` resource profile should allow users access to 2000 MB of disk space and the domain address book.

The `RegularUsers` resource profile should allow users access to 1000 MB of disk space.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Apply the Resource Profiles to a Recipient Policy on page 168.

To configure resource profiles

1. On the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Profile** > **Resource** > **Resource**.
3. Click **New**.
4. Configure the following settings:

Field	Value
Domain	internal.lab
Profile name	PowerUsers
Disk quota (MB)	2000

5. Expand **Webmail access**, and then enable **Domain** under **Address book access**.
6. Click **Create**.
7. Click **New**.
8. Configure the following settings:

Field	Value
Domain	internal.lab
Profile name	RegularUsers

9. Click **Create**.

Apply the Resource Profiles to a Recipient Policy

You will create two new inbound recipient policies, and apply resource profiles to specific users.

Take the Expert Challenge!

On IntSRV FortiMail, configure a new recipient policy to apply the **PowerUsers** resource profile to `user1@internal.lab`.

Configure a second recipient policy to apply the **RegularUsers** resource profile to `user2@internal.lab`.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Validate the Resource Profile Configuration on page 169.

To apply the resource profiles to a recipient policy

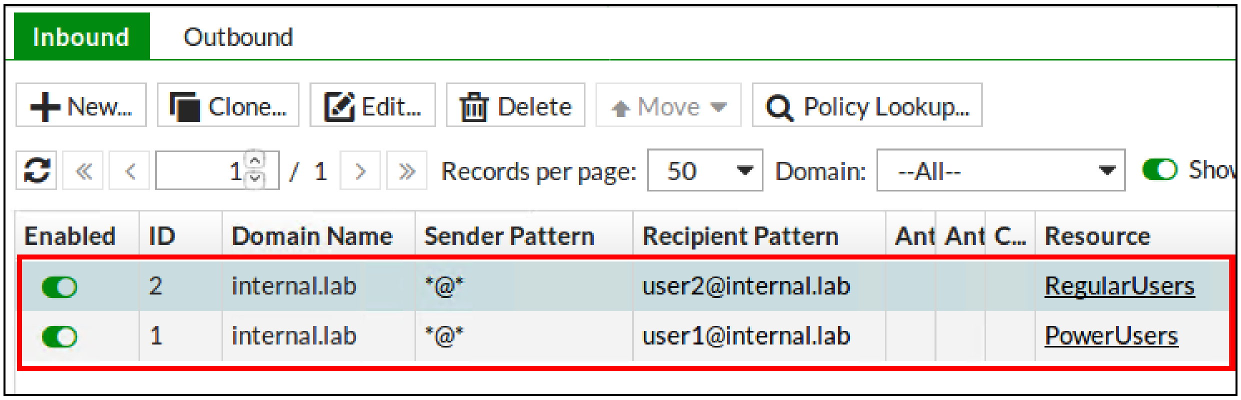
1. Continuing on the IntSRV FortiMail management GUI, click **Policy** > **Recipient Policy** > **Inbound**.
2. Click **New**.
3. Configure the following values:

Field	Value
Domain	internal.lab
Recipient Pattern	user1
Resource	PowerUsers

4. Click **Create**.
5. Click **New**.
6. Configure the following values:

Field	Value
Domain	internal.lab
Recipient Pattern	user2
Resource	RegularUsers

7. Click **Create**.
   Your recipient policy configuration should match the following example:



Enabled	ID	Domain Name	Sender Pattern	Recipient Pattern	Ant	Ant	C...	Resource
●	2	internal.lab	*@*	user2@internal.lab				RegularUsers
●	1	internal.lab	*@*	user1@internal.lab				PowerUsers

For larger deployments that have different levels of resource allocation requirements, you can create recipient policies for local or LDAP groups, and assign resource profiles using separate recipient policies.

8. Log out of the IntSRV FortiMail management GUI.

Validate the Resource Profile Configuration

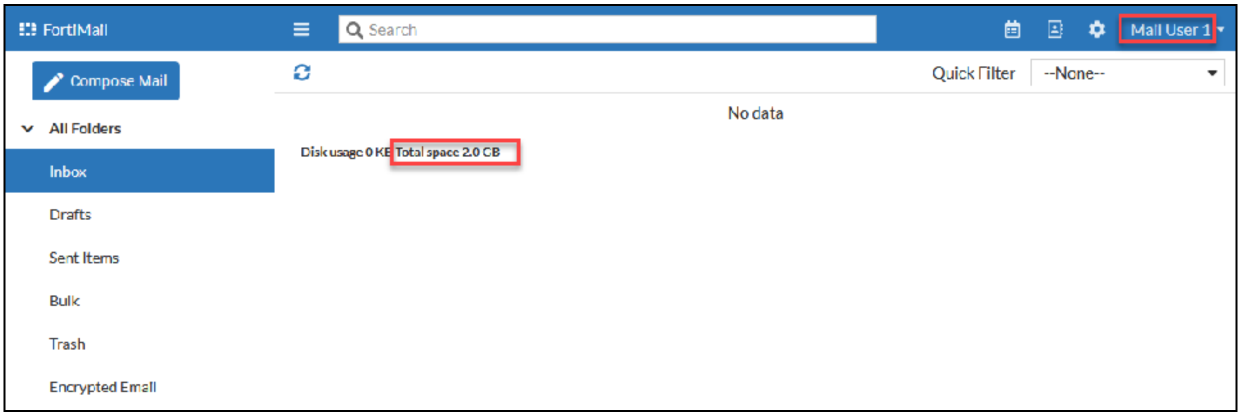
You will verify the resource profile configuration by comparing the disk quota and address book access for user1 and user2.

To verify the resource profile configuration

1. Return to the IntSRV FortiMail webmail GUI, and then log in with the username `user1` and password `fortinet`.

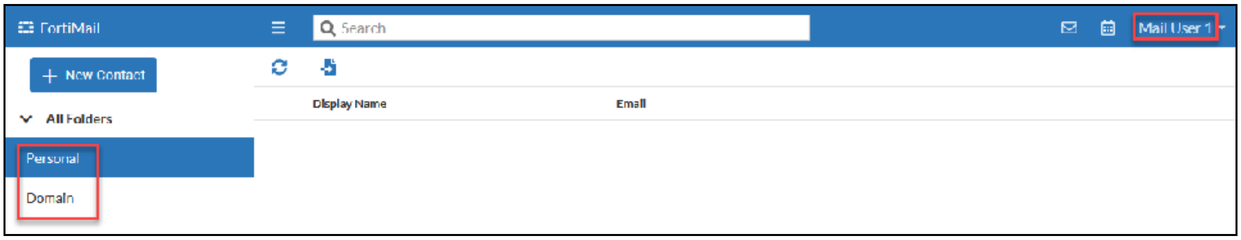
If you were already logged in, you must log out and log back in for the resource profile changes to apply.

2. Verify that `user1@internal.lab` has the correct disk quota and address book access.

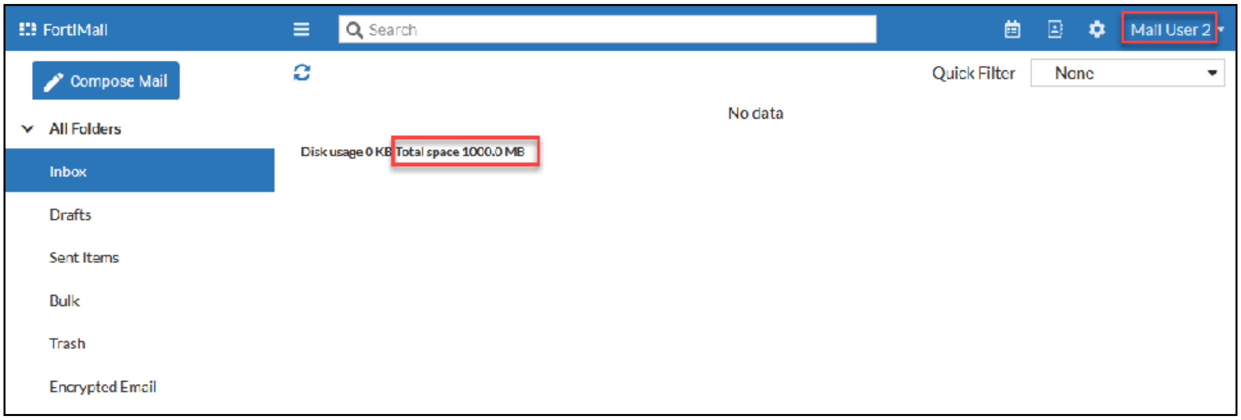


No data

Disk usage 0 KB Total space 2.0 GB

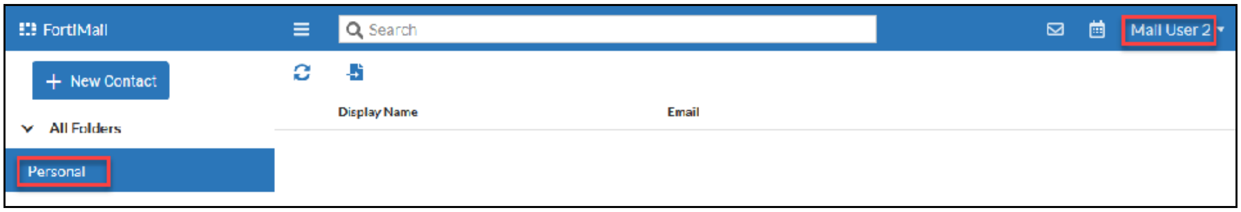


3. Log out of the `user1@internal.lab` account.
4. Log in with the username `user2` and password `fortinet`.
5. Verify that `user2@internal.lab` has the correct disk quota and address book access.



No data

Disk usage 0 KB Total space 1000.0 MB



6. Log out of the IntSRV FortiMail webmail GUI.

Exercise 2: Importing Contacts From LDAP

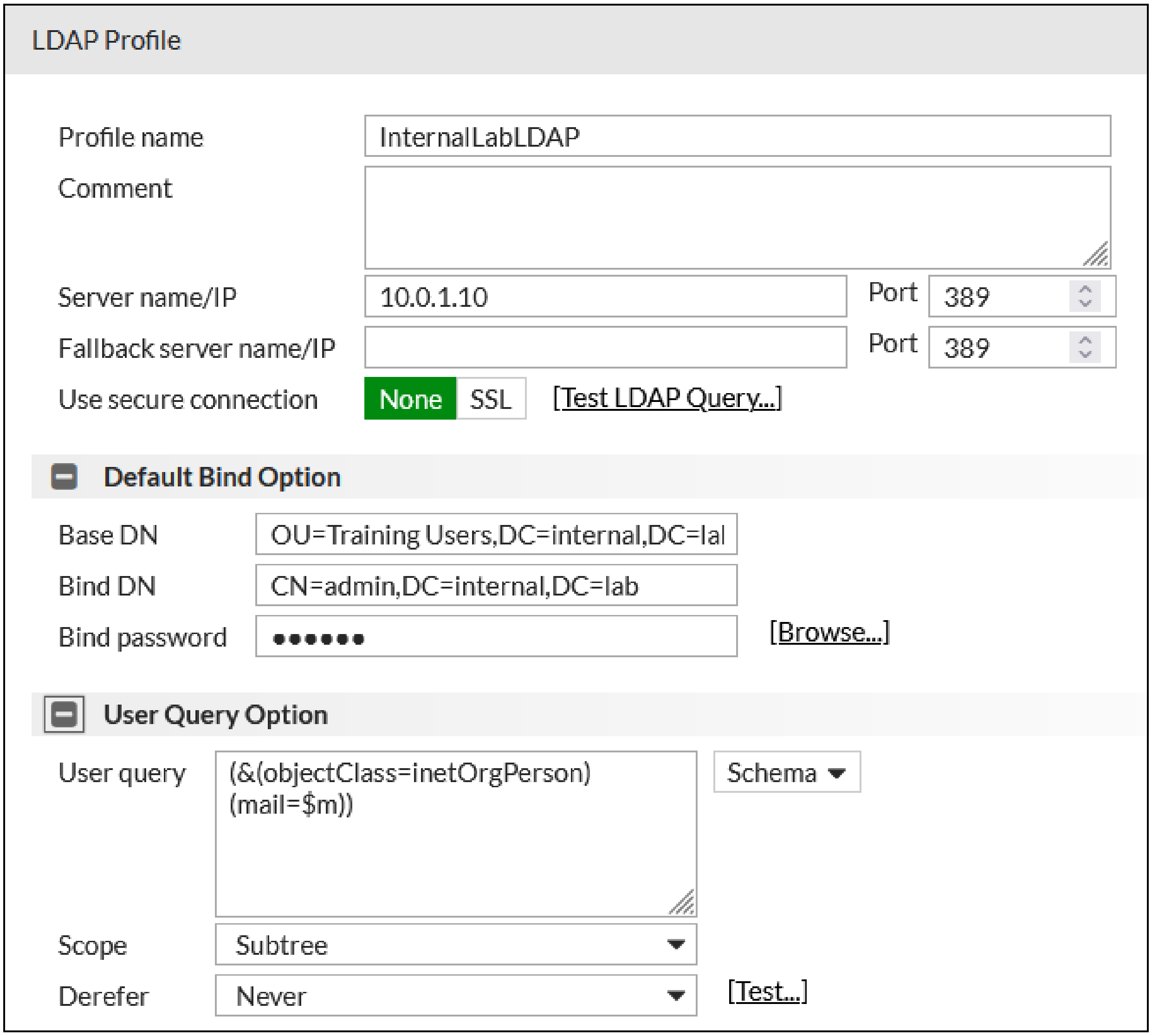
In this exercise, you will review the existing LDAP profile you configured in Authentication on page 41. Then, you will configure an LDAP mapping profile and use the LDAP profile to import contacts into the domain address book.

Review the Existing LDAP Profile

You will review the existing LDAP profile on IntSRV FortiMail.

To review the existing LDAP profile

1. On the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Profile** > **LDAP** > **LDAP**.
3. Double-click **InternalLabLDAP**.
4. Verify that the profile configuration matches the following example:



LDAP Profile

Profile name	InternalLabLDAP
Comment	
Server name/IP	10.0.1.10 Port 389
Fallback server name/IP	Port 389
Use secure connection	[✓ None] SSL [Test LDAP Query...]

Default Bind Option

Base DN	OU=Training Users,DC=internal,DC=lal
Bind DN	CN=admin,DC=internal,DC=lab
Bind password	•••••• [Browse...]

User Query Option

User query	(&(objectClass=inetOrgPerson) (mail=$m)) Schema
Scope	Subtree
Derefer	Never [Test...]

5. Click **Cancel**.

Configure an LDAP Mapping Profile

You will configure a new LDAP mapping profile. You will use attributes from the OpenLDAP server.

Take the Expert Challenge!

On IntSRV FortiMail, create a new LDAP mapping profile and name it `InternalLabMapping`.

Map the following address book fields to their matching LDAP attributes:

- **Email (Work)** → `mail`
- **Display name** → `cn`
- **First name** → `givenName`
- **Last name** → `sn`

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Import Contacts From LDAP on page 174.

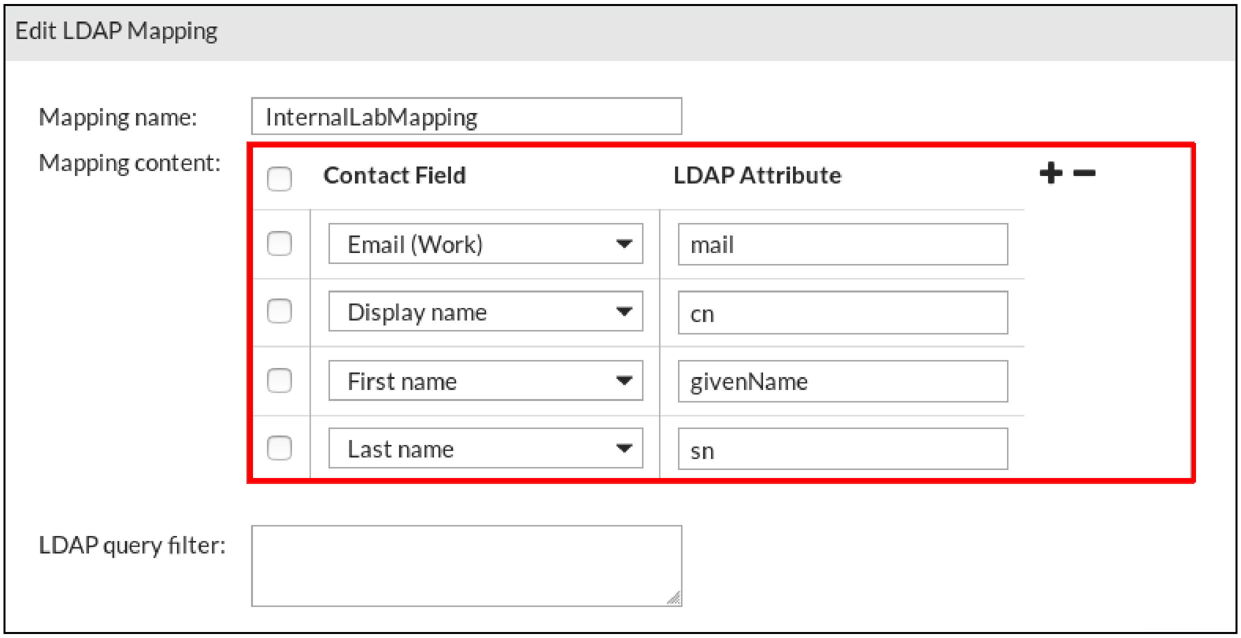
To configure an LDAP mapping profile

1. Continuing on the IntSRV FortiMail management GUI, click **Domain & User** > **Address Book** > **LDAP Mapping**.
2. Click **New**.
3. Create a new mapping profile using the values in the following table—to add new contact fields, click **+**.

Field	Value
Mapping name	InternalLabMapping
Email (Work)	mail
Display name	cn
First name	givenName
Last name	sn

To review how to find the LDAP attributes of OpenLDAP objects, see Authentication on page 41.

Your configuration should match the following example:



Edit LDAP Mapping

Mapping name: InternalLabMapping

Mapping content:

□	Contact Field	LDAP Attribute
□	Email (Work)	mail
□	Display name	cn
□	First name	givenName
□	Last name	sn

LDAP query filter:

4. Click **Create**.

Import Contacts From LDAP

You will import all LDAP contacts from the `internal.lab` LDAP database.

Take the Expert Challenge!

Import all LDAP contacts from the `internal.lab` LDAP database to the `internal.lab` domain address book on IntSRV FortiMail.

The import should overwrite existing contacts and delete any nonexistent contacts.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Verify the Domain Address Book From Webmail on page 175.

To import contacts from LDAP

1. Continuing on the IntSRV FortiMail management GUI, click **Domain & User** > **Address Book** > **Contact**.
2. In the **Domain** drop-down list, select **internal.lab**.
3. In the **More** drop-down list, select **Import**, and then select **LDAP**.
4. Configure the following values:

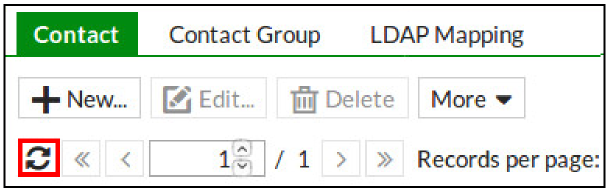
Field	Value
Select LDAP profile	InternalLabLDAP

Field	Value
Select LDAP mapping	InternalLabMapping
Overwrite existing contacts	Enabled
Delete nonexistent contacts	Enabled

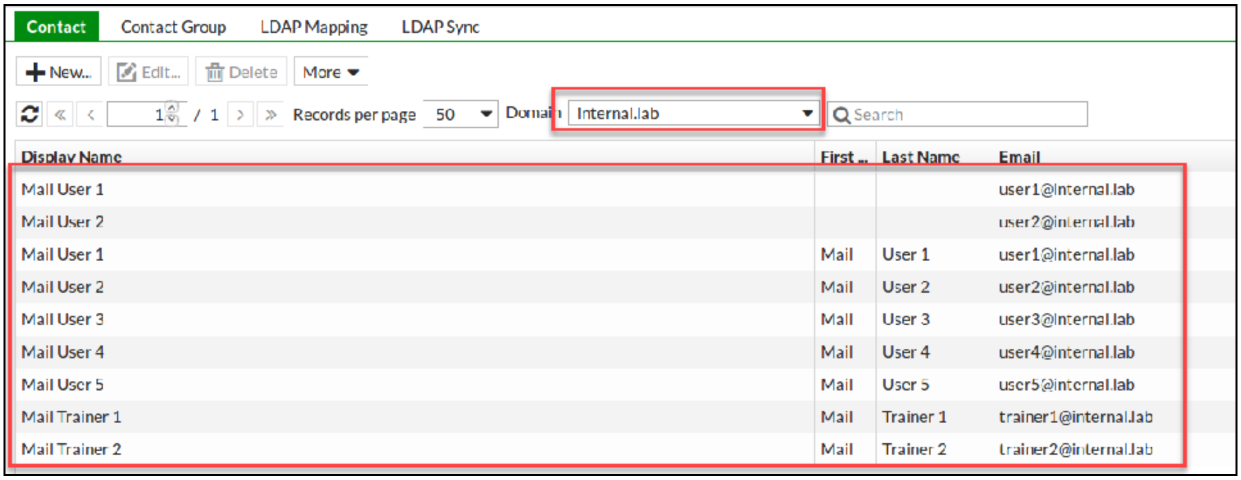
5. Click **OK**.

   The system notifies you that LDAP synchronization is running.

6. Click **OK**.
7. Click the refresh icon.



After the import, your `internal.lab` address book should match the following example:



Display Name	First ...	Last Name	Email
Mail User 1			user1@internal.lab
Mail User 2			user2@internal.lab
Mail User 1	Mail	User 1	user1@internal.lab
Mail User 2	Mail	User 2	user2@internal.lab
Mail User 3	Mail	User 3	user3@internal.lab
Mail User 4	Mail	User 4	user4@internal.lab
Mail User 5	Mail	User 5	user5@internal.lab
Mail Trainer 1	Mail	Trainer 1	trainer1@internal.lab
Mail Trainer 2	Mail	Trainer 2	trainer2@internal.lab

There are extra contact entries for Mail User 1 and Mail User 2 because they were added automatically when these users were created on the FortiMail as local domain users. If you want, you can delete them from the contact list.

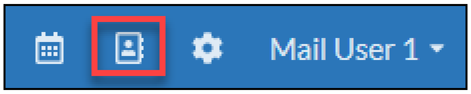
8. Log out of the IntSRV FortiMail management GUI.

Verify the Domain Address Book From Webmail

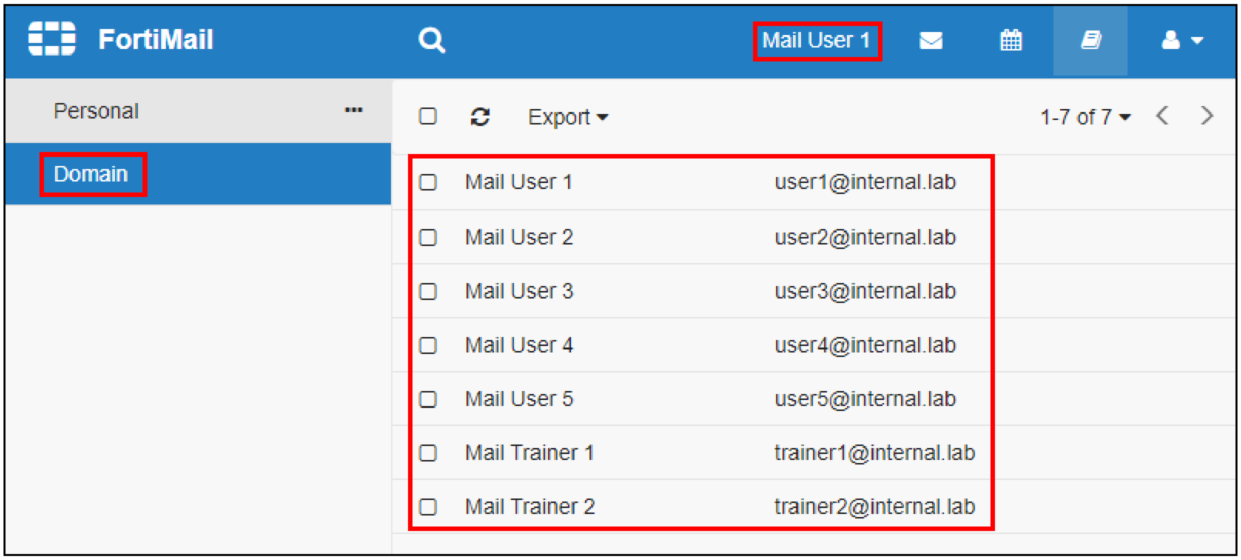
You will verify the domain address book from the IntSRV FortiMail webmail interface.

To verify the domain address book from webmail

1. Return to the IntSRV FortiMail webmail GUI, and then log in with the username `user1` and password `fortinet`.
2. Click the address book icon.



3. Click **Domain**.
4. Verify that the contacts imported from LDAP are now in the **Domain** address book for `user1@internal.lab`.



☐ Mail User 1	user1@internal.lab
☐ Mail User 2	user2@internal.lab
☐ Mail User 3	user3@internal.lab
☐ Mail User 4	user4@internal.lab
☐ Mail User 5	user5@internal.lab
☐ Mail Trainer 1	trainer1@internal.lab
☐ Mail Trainer 2	trainer2@internal.lab

5. Log out of the IntSRV FortiMail webmail GUI.

Lab 11: Transparent Mode

In this lab, you will configure a transparent mode FortiMail to process bidirectional email for the `external.lab` domain, using the built-in MTA. You will also configure and verify bidirectional transparency.

Objectives

- Configure a transparent mode FortiMail to process bidirectional email
- Verify built-in MTA functionality
- Configure bidirectional transparency

Time to Complete

Estimated: 50 minutes

Exercise 1: Configuring a Transparent Mode FortiMail

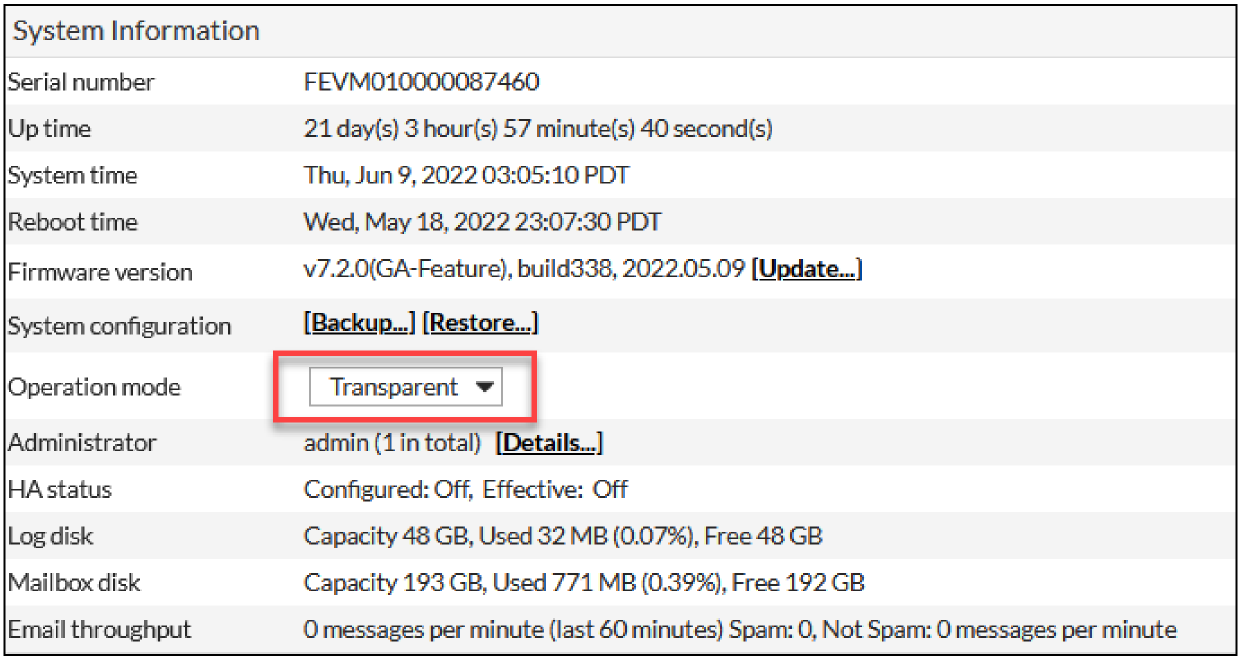
In this exercise, you will review the initial system configuration and deployment topology of ExtTP FortiMail running in transparent mode. Then, you will perform the rest of the basic configuration tasks required to establish bidirectional email flow. You will also verify built-in MTA functionality using logs.

Verify the ExtTP FortiMail System Configuration and Topology

You will verify the initial system configuration of ExtTP FortiMail. You will verify the operation mode, network interface, and routing. You will also configure the DNS settings, and review the deployment topology.

To verify and configure the ExtTP FortiMail system configuration

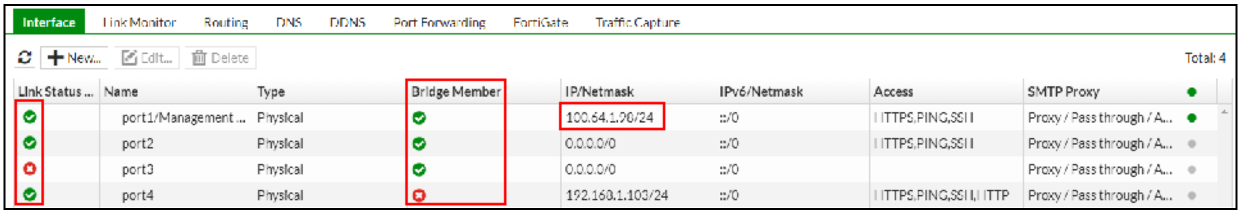
1. On the ExtTP FortiMail management GUI, log in with the username `admin` and password `password`.
2. On the **System Information** widget, beside **Operation mode**, verify that **Transparent** is selected.



System Information

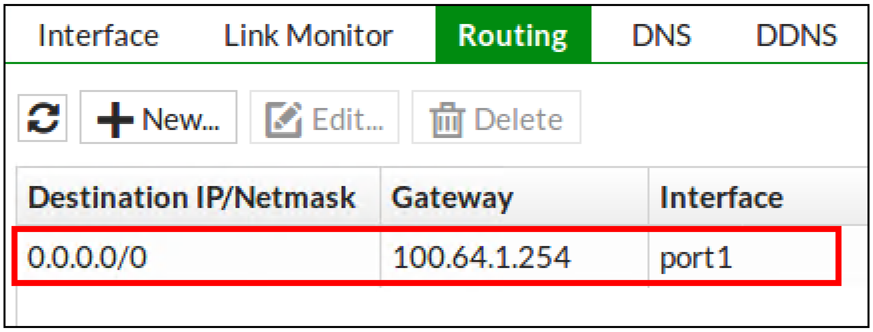
Serial number	FEVM010000087460
Up time	21 day(s) 3 hour(s) 57 minute(s) 40 second(s)
System time	Thu, Jun 9, 2022 03:05:10 PDT
Reboot time	Wed, May 18, 2022 23:07:30 PDT
Firmware version	v7.2.0(GA-Feature), build338, 2022.05.09 [Update...]
System configuration	[Backup...] [Restore...]
Operation mode	Transparent
Administrator	admin (1 in total) [Details...]
HA status	Configured: Off, Effective: Off
Log disk	Capacity 48 GB, Used 32 MB (0.07%), Free 48 GB
Mailbox disk	Capacity 193 GB, Used 771 MB (0.39%), Free 192 GB
Email throughput	0 messages per minute (last 60 minutes) Spam: 0, Not Spam: 0 messages per minute

3. Click **System** > **Network** > **Interface**.
4. Verify the following:
   - **port1/Management IP** is configured with the IP address `100.64.1.98/24`.
   - All interfaces are members of the built-in bridge except **port4**.
   - **port3** is administratively down.



Link Status ...	Name	Type	Bridge Member	IP/Netmask	IPv6/Netmask	Access	SMTP Proxy
✓	port1/Management ...	Physical	✓	100.64.1.98/24	::/0	HTTPS,PING,SSH	Proxy / Pass through / A... ●
✓	port2	Physical	✓	0.0.0.0/0	::/0	HTTPS,PING,SSH	Proxy / Pass through / A... ●
✗	port3	Physical	✓	0.0.0.0/0	::/0		Proxy / Pass through / A... ●
✓	port4	Physical	✗	192.168.1.103/24	::/0	HTTPS,PING,SSH,HTTP	Proxy / Pass through / A... ●

5. Click **System** > **Network** > **Routing**.
6. Verify that there is a default route configured through **port1**.



Destination IP/Netmask	Gateway	Interface
0.0.0.0/0	100.64.1.254	port1

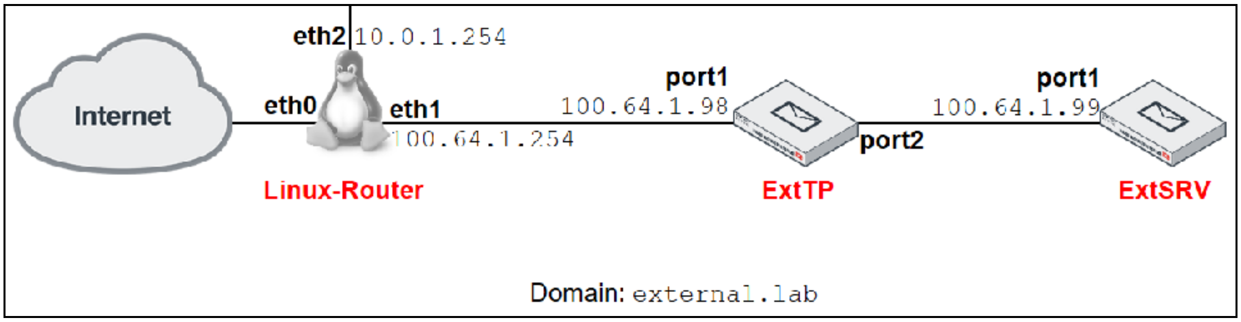
7. Click **System** > **Network** > **DNS**.
8. Configure the following settings:

Field	Value
Primary DNS server	10.0.1.254
Secondary DNS server	10.0.1.10

9. Click **Apply**.

To verify the ExtTP FortiMail deployment topology

1. Review the following topology:



ExtSRV FortiMail is directly connected to port2 of ExtTP FortiMail, which is a bridge-member interface. The ExtTP FortiMail port1 and port2 are in the same Layer 2 broadcast domain.

Configure Connection Pickup

You will verify and configure connection pickup settings on ExtTP FortiMail.

Take the Expert Challenge!

On ExtTP FortiMail, verify that port1 is configured to proxy incoming connections, pass through outgoing connections, and accept local connections.

Configure port2 to proxy outgoing connections, pass through incoming connections, and drop local connections.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure the Mail Server Settings on page 181.

To configure connection pickup

1. Continuing on the ExtTP FortiMail management GUI, click **System** > **Network** > **Interface**.
2. Double-click **port1/Management IP**.
3. Expand the **SMTP proxy** section.
4. Configure the following settings:

Field	Value
Incoming connections	Proxy
Outgoing connections	Pass through
Local connections	Enabled

5. Click **OK**.
6. Double-click **port2**.
7. Expand the **SMTP proxy** section.
8. Configure the following settings:

Field	Value
Incoming connections	Pass through
Outgoing connections	Proxy
Local connections	Disabled

9. Click **OK**.

Since port1 is the closest interface to the source for all incoming email, port1 proxies all incoming connections. Since port2 is the closest interface to the source for all outgoing email, port2 proxies all outgoing connections.

Configure the Mail Server Settings

You will configure the mail server settings.

Take the Expert Challenge!

Configure the mail server settings so that the FQDN for ExtTP FortiMail is `ExtTP.external.lab`.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure a Protected Domain on page 181.

To configure the mail server settings

1. Continuing on the ExtTP FortiMail management GUI, click **System** > **Mail Setting** > **Mail Server Setting**.
2. Configure the following settings:

Field	Value
Host name	ExtTP
Local domain name	external.lab

3. Click **Apply**.

Configure a Protected Domain

You will configure a protected domain on ExtTP FortiMail, and configure the transparent mode settings to identify which interface will connect to the back-end mail server (ExtSRV FortiMail).

Take the Expert Challenge!

ExtTP FortiMail should accept all emails for the `external.lab` domain.

After processing, the emails should be delivered to ExtSRV FortiMail (`100.64.1.99`), using port2.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

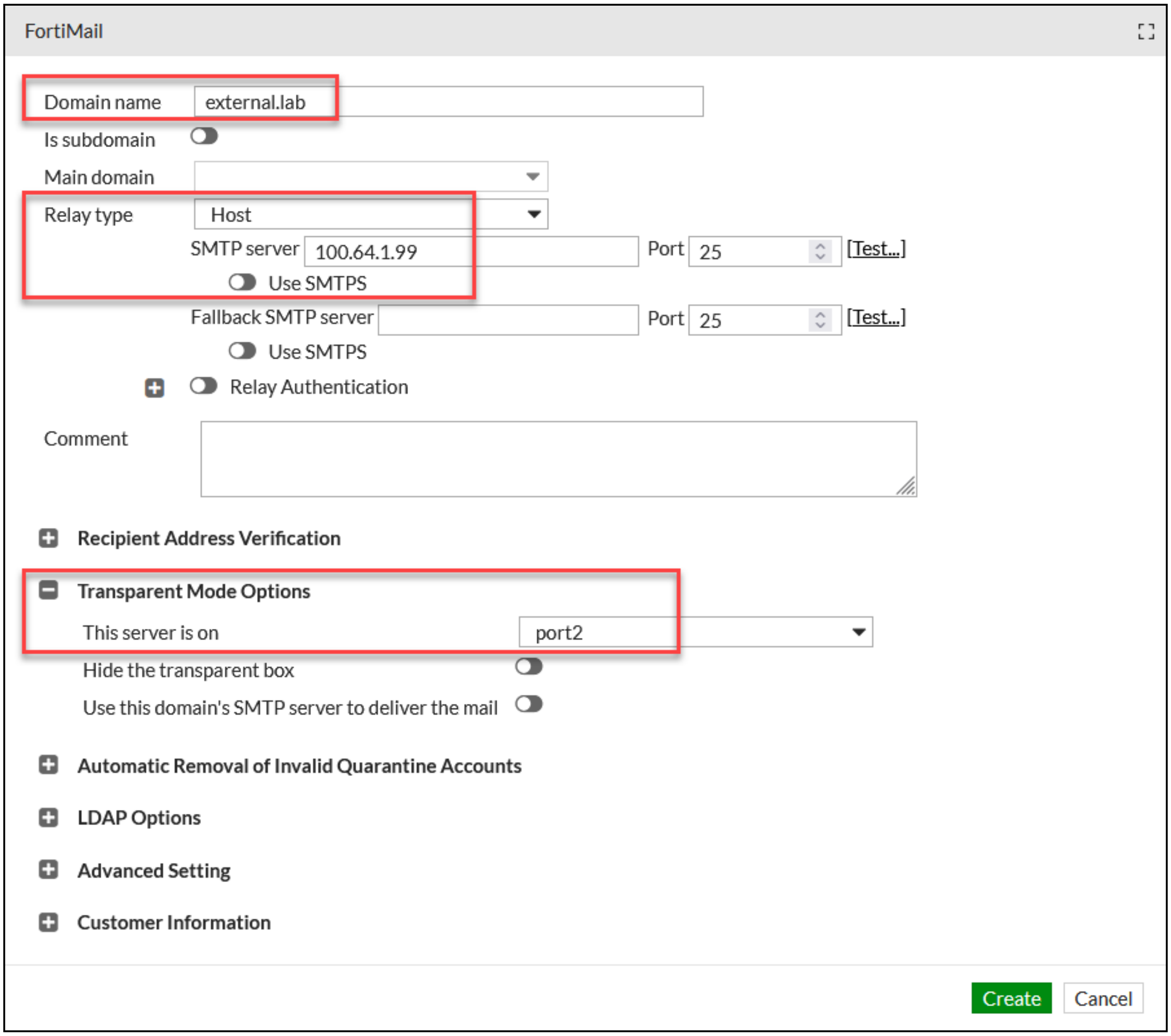
After you complete the challenge, see Configure an Access Control Rule for Outbound Emails on page 183.

To configure a protected domain

1. Continuing on the ExtTP FortiMail management GUI, click **Domain & User** > **Domain** > **Domain**.
2. Click **New**.
3. Configure the following settings:

Field	Value
Domain name	external.lab
SMTP server	100.64.1.99

4. Expand **Transparent Mode Options**.
5. In the **This server is on** drop-down list, select **port2**.



FortiMail

Domain name	external.lab
Is subdomain	○
Main domain	
Relay type	Host
SMTP server	100.64.1.99 Port 25 [Test...]
	○ Use SMTPS
Fallback SMTP server	Port 25 [Test...]
	○ Use SMTPS
	○ Relay Authentication
Comment	

Recipient Address Verification

Transparent Mode Options

This server is on	port2
Hide the transparent box	○
Use this domain's SMTP server to deliver the mail	○

6. Click **Create**.

Configure an Access Control Rule for Outbound Emails

You will create an access receive rule to allow outbound emails from the `external.lab` users.

Take the Expert Challenge!

On ExtTP FortiMail, configure an access control rule that will relay emails:

- With the sender pattern containing `external.lab`
- Originating from the `100.64.1.99/32` IP address

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Validate Transparent Mode Functionality on page 183.

To configure an access control rule

1. Continuing on the ExtTP FortiMail management GUI, click **Policy** > **Access Control** > **Receiving**.
2. Click **New**.
3. Configure the following settings:

Field	Value
Sender	*@external.lab
Source	100.64.1.99/32
Action	Relay

4. Click **Create**.

Validate Transparent Mode Functionality

You will validate your configuration by sending emails back and forth between the `internal.lab` and `external.lab` domains. The email should be routed in both directions, and you will verify that from the logs on ExtTP FortiMail.

To validate transparent mode functionality

1. On the Linux-Client VM, open the Thunderbird client.
2. Compose a new email, using the following values:

Field	Value
To	extuser@external.lab

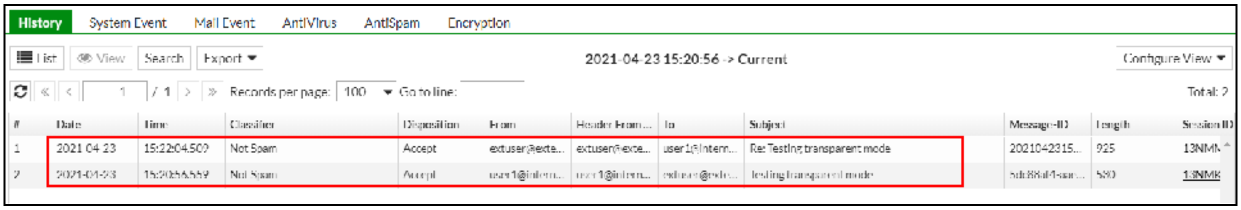
Field	Value
Subject	Testing Transparent Mode
Message Body	Will this work?

3. Click **Send**.
4. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
5. Verify that the email was delivered.
6. Reply to the email.
7. Log out of the ExtSRV FortiMail webmail GUI.
8. Return to the Thunderbird client, and then verify that the reply was received.
9. Close Thunderbird.

To view the logs on ExtTP FortiMail

1. Return to the ExtTP FortiMail management GUI, and then click **Monitor** > **Log** > **History**.
2. Double-click the active log file.

   The first two entries in the **History** logs should correspond to the two emails.

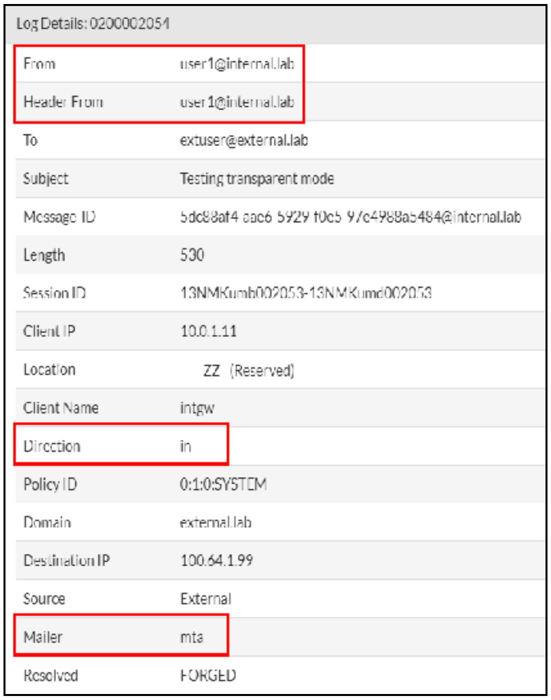


2021-04-23 15:20:56 -> Current

Total: 2

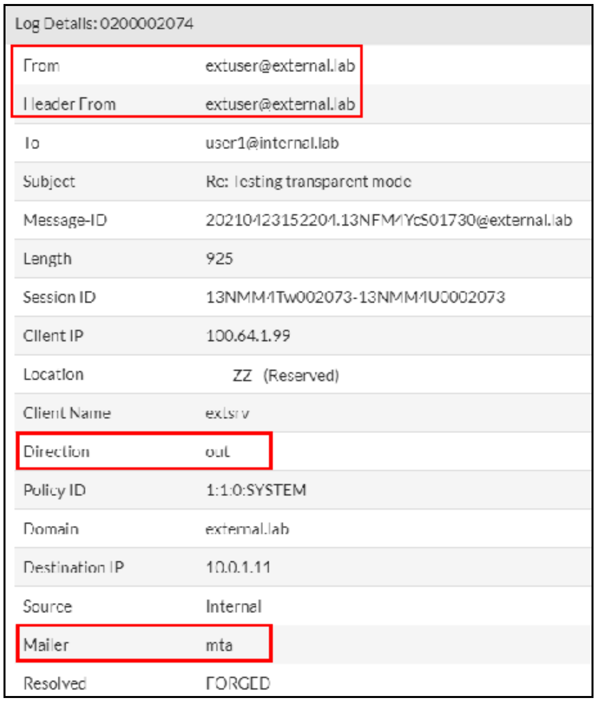
#	Date	Time	Classifier	Disposition	From	Header From ...	To	Subject	Message-ID	Length	Session ID
1	2021-04-23	15:22:04.509	Not Spam	Accept	extuser@exte...	extuser@exte...	user1@intern...	Re: Testing transparent mode	2021042315...	925	13NMN
2	2021-04-23	15:20:56.559	Not Spam	Accept	user1@intern...	user1@intern...	extuser@exte...	Testing transparent mode	5dc88af4-aac...	530	13NMK

3. View the details for each log, and review the values in the **Direction** and **Mailer** fields.



Log Details: 0200002054

From	user1@internal.lab
Header From	user1@internal.lab
To	extuser@external.lab
Subject	Testing transparent mode
Message ID	5dc88af4-aac6-5929-f0c5-97c4988ab484@internal.lab
Length	530
Session ID	13NMKumb002053-13NMKumd002053
Client IP	10.0.1.11
Location	ZZ (Reserved)
Client Name	intgw
Direction	in
Policy ID	0:1:0:SYSTEM
Domain	external.lab
Destination IP	100.64.1.99
Source	External
Mailer	mta
Resolved	FORGED



Log Details: 0200002074

From	extuser@external.lab
Header From	extuser@external.lab
To	user1@internal.lab
Subject	Re: Testing transparent mode
Message-ID	20210423152201.13NFM4YcS01730@external.lab
Length	925
Session ID	13NMM4Tw002073-13NMM4U0002073
Client IP	100.64.1.99
Location	ZZ (Reserved)
Client Name	extsrv
Direction	out
Policy ID	1:1:0:SYSTEM
Domain	external.lab
Destination IP	10.0.1.11
Source	Internal
Mailer	mta
Resolved	FORGED

The **mta** value in the **Mailer** field shows that ExtTP FortiMail is using its built-in MTA to route emails in both directions.

4. Log out of the ExtTP FortiMail management GUI.

Exercise 2: Configuring Bidirectional Transparency

You verified that ExtTP FortiMail is picking up emails in both directions, and using the built-in MTA to route emails to their destination successfully.

In this exercise, you will examine email message headers to investigate the transparency of ExtTP FortiMail. Then, you will configure transparency for both incoming and outgoing emails.

Review Outbound and Inbound Message Headers

You will examine the message headers of emails to determine the transparency of ExtTP FortiMail.

To review outbound message headers

1. On the Linux-Client VM, open the Thunderbird client.
2. Open the latest email message received from `extuser@external.lab`.
3. Click **More** > **View Source**.
4. Review the `Received` headers:

```
Received: from IntGW.internal.lab ([10.0.1.11] by IntSRV.internal.lab with ESMTP id
    v29HESsx001946-v29HESt0001946
Received: from ExtTP.external.lab ([100.64.1.98] by IntGW.internal.lab with ESMTP id
    v29HESm1001931-v29HESm3001931
Received: from ExtSRV.external.lab ([100.64.1.99])by ExtTP.external.lab with ESMTP id
    v29HERuL002360-v29HERuN002360
Received: from [10.0.1.10] ([127.0.0.1])by ExtSRV.external.lab with ESMTP id
    v29HER6G001960-v29HER6H001960
```

To review inbound message headers

1. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `password`.
2. Open the latest email message received from `user1@internal.lab`.
3. Click **More** > **Detailed Header**.
4. Review the `Received` headers:

```
Received: from ExtTP.external.lab ([100.64.1.98])by extsrv.external.lab with ESMTP id
    v29HEDnS001931-v29HEDnU00193
Received: from IntGW.internal.lab ([10.0.1.11])by ExtTP.external.lab with ESMTP id
    v29HEDhs002345-v29HEDhu002345
```

ExtTP FortiMail appears in the `Received` headers. It is not yet fully transparent.

Configure Bidirectional Transparency

You will configure inbound and outbound transparency on ExtTP FortiMail.

Take the Expert Challenge!

Configure bidirectional transparency on ExtTP FortiMail.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Verify Inbound Transparency on page 187.

To configure inbound transparency

1. On the ExtTP FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Domain & User** > **Domain** > **Domain**.
3. Double-click **external.lab**.
4. Expand the **Transparent Mode Options** section.
5. Enable **Hide the transparent box**.
6. Click **OK**.

To configure outbound transparency

1. Continuing on the ExtTP FortiMail management GUI, click **Policy** > **IP Policy** > **IP Policy**.
2. In the **IP Policies** section, click the **Inbound_Session** link for policy ID **1**.
3. In the **Connection Settings** section, enable **Hide this box from the mail server**.
4. Click **OK**.

Verify Inbound Transparency

You will verify inbound transparency by sending an email from a user in the `internal.lab` domain to a user in the `external.lab` domain. You will review the message headers of that email to verify that ExtTP FortiMail does not appear in the `Received` headers.

To verify inbound transparency

1. Return to the Thunderbird client on the Linux-Client VM, and then send a new email to `extuser@external.lab`.
2. Return to the ExtSRV FortiMail webmail GUI, and open the email you just sent.
3. Click **More** > **Detailed Header**.
4. Review the `Received` headers.

```
Received: from IntGW.internal.lab ([10.0.1.11] by extsrv.external.lab with ESMTP id
    v29IUVNd002175-v29IUVNf002175
```

ExtTP FortiMail no longer appears in the inbound message headers.

Verify Outbound Transparency

You will send an email from a user in the `external.lab` domain to a user in the `internal.lab` domain. You will review the message headers of that email to verify outbound transparency.

To verify outbound transparency

1. Continuing on the ExtSRV FortiMail webmail GUI, send a new email to `user1@internal.lab`.
2. Return to the Thunderbird client, and then open the email you just sent.
3. Click **More** > **View Source**.
4. Review the `Received` headers:

```
Received: from IntGW.internal.lab ([10.0.1.11])by IntSRV.internal.lab with ESMTP id
    v29IgrVu001966-XXXXXXX
Received: from ExtTP.external.lab ([100.64.1.99])by IntGW.internal.lab with ESMTP id
    v29IgrJV001947-XXXXXXX
Received: from [10.0.1.10] ([127.0.0.1])by ExtSRV.external.lab with ESMTP id
    v29IgqvA00221-XXXXXXX
```

While the header is now showing the IP address of ExtSRV FortiMail (`100.64.1.99`), the host name still shows `ExtTP.external.lab`. This is because ExtTP FortiMail uses its own host name in the SMTP greeting. There is one more configuration change you must make to prevent this.

Configure SMTP Greeting Rewrite

You will configure SMTP greeting rewrite so that ExtTP FortiMail does not use its own host name in the SMTP greeting. To replicate the ExtSRV SMTP greeting, you will use the host name `ExtSRV.external.lab`.

Take the Expert Challenge!

Configure SMTP greeting rewrite on ExtTP FortiMail. Use the FQDN `ExtSRV.external.lab`.

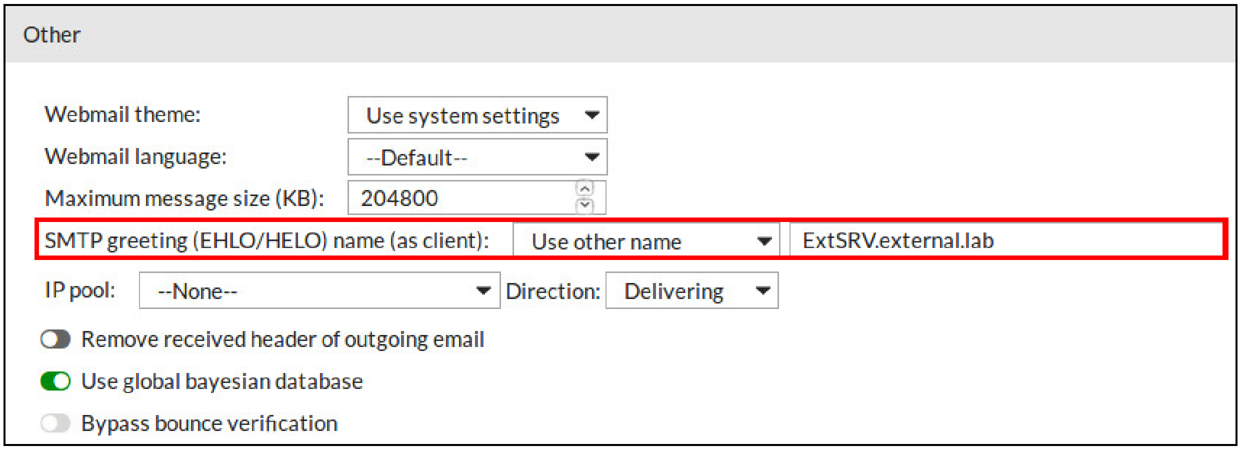
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Validate SMTP Greeting Rewrite on page 189.

To configure SMTP greeting rewrite

1. Return to the ExtTP FortiMail management GUI, and then click **Domain & User** > **Domain** > **Domain**.
2. Double-click **external.lab**.
3. Expand **Advanced Settings**, and then click **Other**.

4. In the **SMTP greeting (EHLO/HELO) name (as client)** drop-down list, select **Use other name**, and then in the field, type `ExtSRV.external.lab`.



Other

Webmail theme: Use system settings
Webmail language: --Default--
Maximum message size (KB): 204800
SMTP greeting (EHLO/HELO) name (as client): Use other name ExtSRV.external.lab
IP pool: --None-- Direction: Delivering
○ Remove received header of outgoing email
● Use global bayesian database
○ Bypass bounce verification

5. Click **OK**.
6. Click **OK**.
7. Log out of the ExtTP FortiMail management GUI.

Validate SMTP Greeting Rewrite

You will send another email from a user in the `external.lab` domain, and then verify the message headers.

To validate SMTP greeting rewrite

1. Return to the ExtSRV FortiMail webmail GUI, and then send a new email to `user1@internal.lab`.
2. Log out of the ExtSRV FortiMail webmail GUI.
3. Return to the Thunderbird client, and open the email you just sent.
4. Click **More** > **View Source**.
5. Review the `Received` headers.

```
Received: from IntGW.internal.lab ([10.0.1.11]) by IntSRV.internal.lab with ESMTP id
    v29MUF0s001921-v29MUF0t001921
Received: from ExtSRV.external.lab ([10.200.1.99]) by IntGW.internal.lab with ESMTP
    id v29MUEdn001911-v29MUEdp001911
Received: from [10.0.1.10] ([127.0.0.1]) by ExtSRV.external.lab with ESMTP id
    v29MUExs002184-v29MUExt002184
```

ExtTP FortiMail no longer appears in the message headers.

6. Close Thunderbird.

Lab 12: Maintenance

In this lab, you will configure and generate a local report, and monitor system resource use.

Objectives

- Configure and generate a local report
- Monitor historical and real-time system resource use

Time to Complete

Estimated: 20 minutes

Exercise 1: Configuring and Generating Local Reports

In this exercise, you will configure a local report on IntGW FortiMail for mail filtering statistics. Then, you will generate an on-demand report and review the statistics.

Configure a Local Report

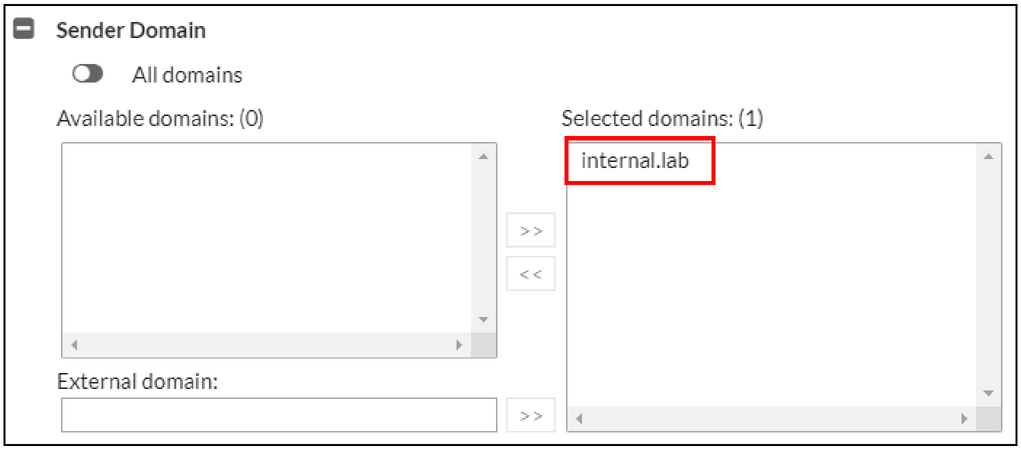
You will configure the local report settings on IntGW FortiMail.

To configure a local report

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Log and Report** > **Report Settings** > **Mail Statistics**.
3. Click **New**.
4. Configure the following settings:

Field	Value
Report name	IntGWReport
Time Period	This week

5. Expand the **Query Selection** section.
6. Expand the **Mail Filtering Statistics** category, and then enable the following queries:
   - **Mail Category by Date**
   - **Non-Spam Classifier by Date**
   - **Spam Classifier by Date**
   - **Virus Classifier by Date**
7. Expand the **Sender Domain** section, and then disable **All domains**.
8. From the **Available domains** list, move the **internal.lab** domain to the **Selected domains** list.



9. Click **Create**.

On a production FortiMail, you should also configure scheduling, and add a notification email address so that the report is automatically generated and emailed to you. The scheduled reporting helps keep you up-to-date on the email trends of your network.

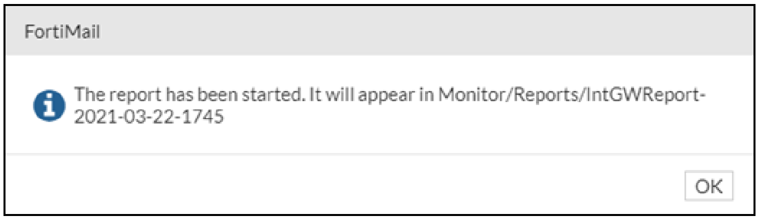
Generate an On-Demand Report

You will generate an on-demand report.

To generate an on-demand report

1. Continuing on the IntGW FortiMail management GUI, select the **IntGWReport** entry, and then click **Generate**.

   A notification is displayed.



FortiMail

The report has been started. It will appear in Monitor/Reports/IntGWReport-2021-03-22-1745

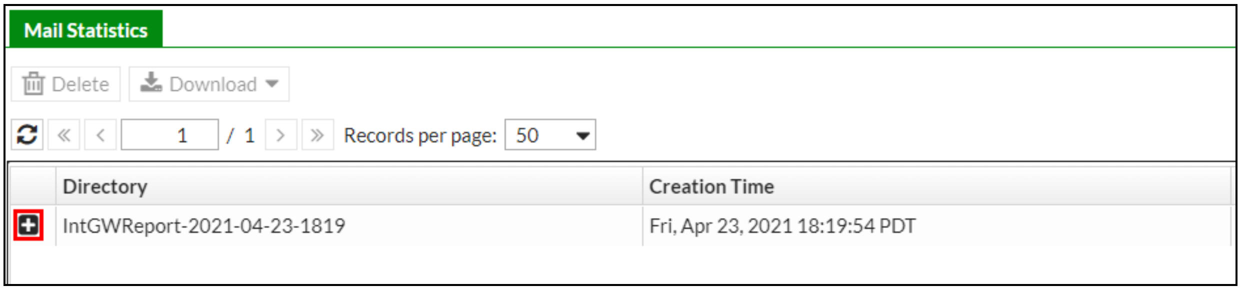
2. Click **OK**.

Review a Local Report

You will review the on-demand report.

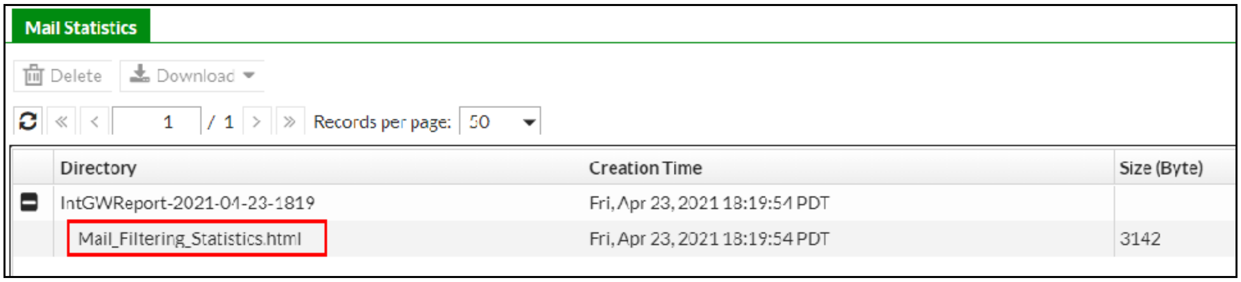
To review a local report

1. Continuing on the IntGW FortiMail management GUI, click **Monitor** > **Report** > **Mail Statistics**.
2. Expand the report file entry.



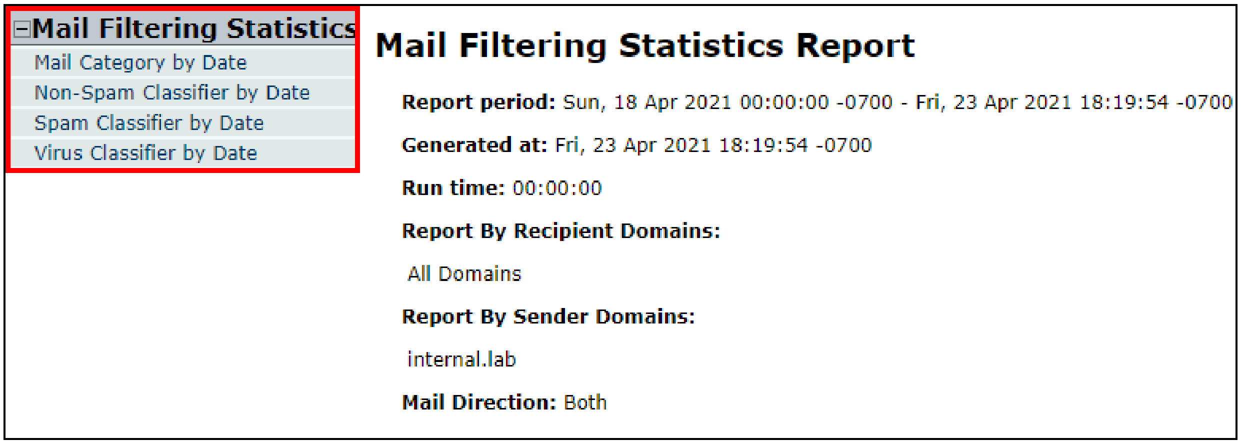
Directory	Creation Time
IntGWReport-2021-04-23-1819	Fri, Apr 23, 2021 18:19:54 PDT

3. Double-click the HTML file.



	Directory	Creation Time	Size (Byte)
⊟	IntGWReport-2021-04-23-1819	Fri, Apr 23, 2021 18:19:54 PDT	
	Mail_Filtering_Statistics.html	Fri, Apr 23, 2021 18:19:54 PDT	3142

4. Use the menu on the left to navigate and review the data.



Mail Filtering Statistics Report

Report period: Sun, 18 Apr 2021 00:00:00 -0700 - Fri, 23 Apr 2021 18:19:54 -0700

Generated at: Fri, 23 Apr 2021 18:19:54 -0700

Run time: 00:00:00

Report By Recipient Domains:

All Domains

Report By Sender Domains:

internal.lab

Mail Direction: Both

5. Close the report tab.
6. Log out of the IntGW FortiMail management GUI.

Exercise 2: Monitoring System Resources

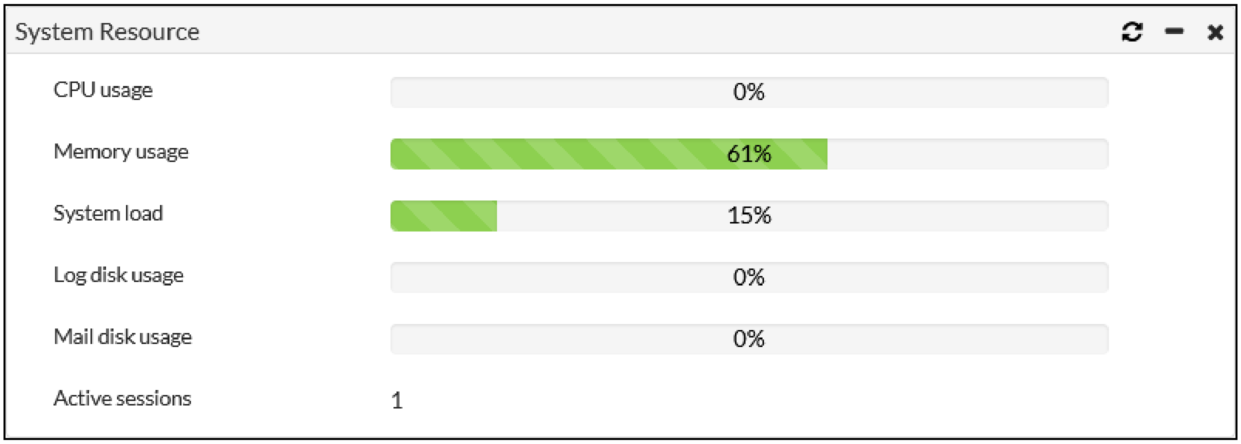
In this exercise, you will view the historical and real-time resource usage on IntGW FortiMail.

Review the Resource Usage History

You will review the resource usage history on IntGW FortiMail.

To review the resource usage history

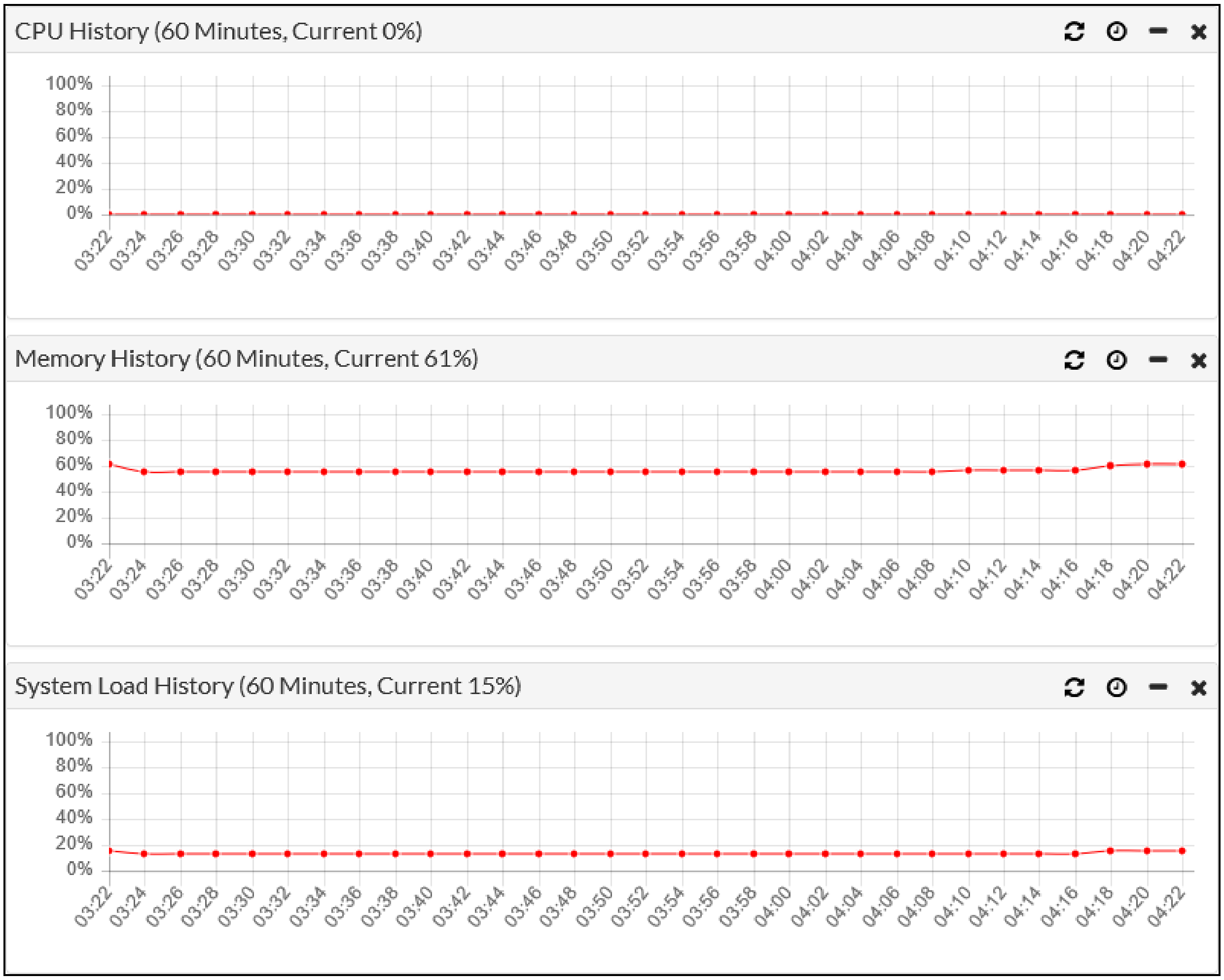
1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. In the **System Resource** widget, make a note of the following values:
   - **CPU usage**
   - **Memory usage**
   - **System load**
   - **Active sessions**



System Resource

CPU usage	0%
Memory usage	61%
System load	15%
Log disk usage	0%
Mail disk usage	0%
Active sessions	1

3. Make a note of the trends in resource usage below the **System Resource** widget.



View Resource Usage in Real Time

You will use a script to generate continuous emails at a high rate, and then you will view the resource usage trends during the period the script is running.

To view resource usage in real time

1. Open an SSH connection to IntGW FortiMail.
2. Enter the following command to view the list of processes that are consuming the most CPU cycles or RAM:

```
diagnose system top delay 1
```

A list of system processes is displayed. The processes consuming the most CPU are at the top of the list. The list refreshes every second, which gives you a real-time view of the system resource usage.

3. Press Q to stop the output.

To generate traffic

1. On the Linux-Client VM, open a terminal window (`Ctrl+Alt+T`).
2. Enter the following command to open an SSH connection to the Linux-Router VM:

```
ssh student@10.0.1.254
```

3. Enter the password `password`.
4. Enter `pwd`.
5. Verify that your current working directory is `/home/student`.
6. Enter the following swaks command to send emails continuously:

```
while sleep 1; do swaks --to user1@internal.lab --from "extuser@external.lab" --
    header "Subject: Testing live system resources" --body "This is a test mail" --
    server IntGW.internal.lab --port 25 --timeout 40s; done
```

7. Leave the terminal window open.

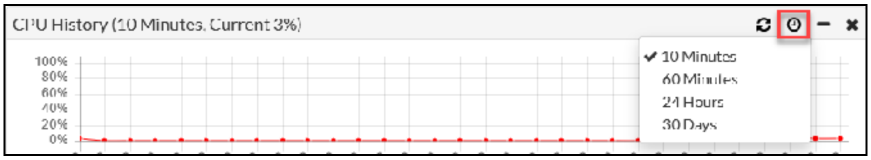
A copy of the swaks command is in the `commands.txt` file, which is located in the **Resources** folder on the Linux-Client desktop.

To view system resource usage during live traffic

1. Return to the IntGW FortiMail management GUI, and then in the **System Resource** widget, click the **Refresh** icon (↻).

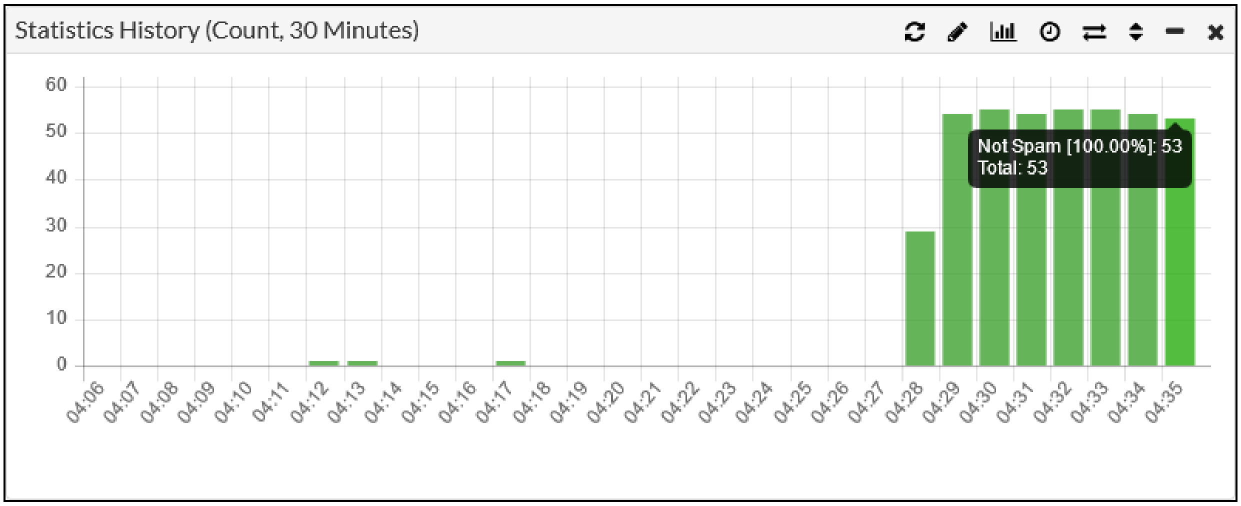
You must wait a few minutes before the charts refresh with new data.

Using the **Period** icon, you can select a different period time or specify how much history you want to see for a particular resource.



CPU History (10 Minutes, Current 3%)

2. Review the change in resource utilization across **CPU**, **System Load**, and **Statistics History**.



Statistics History (Count, 30 Minutes)

3. Log out of the IntGW FortiMail management GUI.
4. Return to the Linux-Client VM, and then stop the swaks script (`Ctrl+C`).
5. Close the terminal window.

Lab 13: Troubleshooting

The `internal.lab` users are complaining that they cannot send or receive emails. In this lab, you will use SMTP event logs and the built-in packet capture tool to investigate and fix the mail flow issues.

Objectives

- Investigate user complaints
- Use SMTP event logs and packet capturing to determine where the issue is occurring
- Fix the email flow issues

Time to Complete

Estimated: 45 minutes

Prerequisites

Before beginning this lab, you must restore a configuration file on the `internal.lab` FortiMail VMs.

To restore a configuration file on IntGW FortiMail

1. On the Linux-Client VM, open a browser, and then go to the IntGW FortiMail management GUI.
2. Log in with the username `admin` and password `password`.
3. Click **System** > **Maintenance** > **Configuration**.
4. Click **Restore Configuration**.
5. Click **Desktop** > **Resources** > **Starting Configs** > **Lab 13** > `13_Initial_IntGW.tgz`, and then click **Open**.
6. Click **OK**.

To restore a configuration file on IntSRV FortiMail

1. Continuing on the Linux-Client VM, open a new browser tab, and then go to the IntSRV FortiMail management GUI.
2. Log in with the username `admin` and password `password`.
3. Click **System** > **Maintenance** > **Configuration**.
4. Click **Restore Configuration**.
5. Click **Desktop** > **Resources** > **Starting Configs** > **Lab 13** > `13_Initial_IntSRV.tgz`, and then click **Open**.
6. Click **OK**.
7. Wait for the FortiMail VMs to finish rebooting before proceeding with the exercise.
8. Close the browser.

Exercise 1: Troubleshooting the Problem

In this exercise, you will verify the problem. Then, you will use SMTP event logs and packet capture tools to determine where the issue is.

Investigate Inbound Mail Flow

You will send an email from a user in the `external.lab` domain to a user in the `internal.lab` domain. You will view the logs on IntGW FortiMail and try to identify any potential issues.

To investigate inbound mail flow

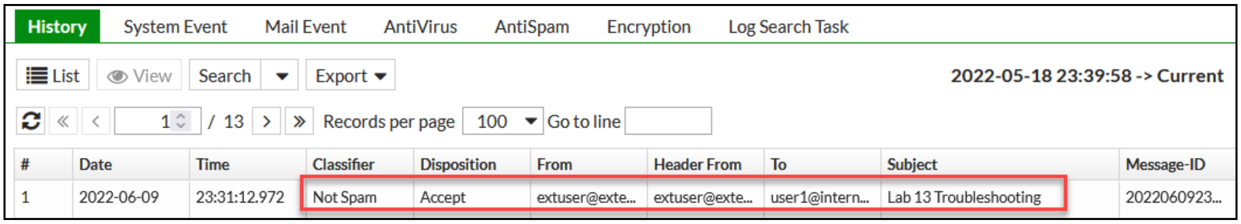
1. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
2. Send an email to `user1@internal.lab`.
3. On the Linux-Client VM, open the Thunderbird client, and then check if the email arrived.

   Hint: It won't arrive.

To view the logs on IntGW FortiMail

1. On the IntGW FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Monitor** > **Log** > **History**.
3. Double-click the active log file.

   The first entry in the **History** logs should correspond to the email you just sent.

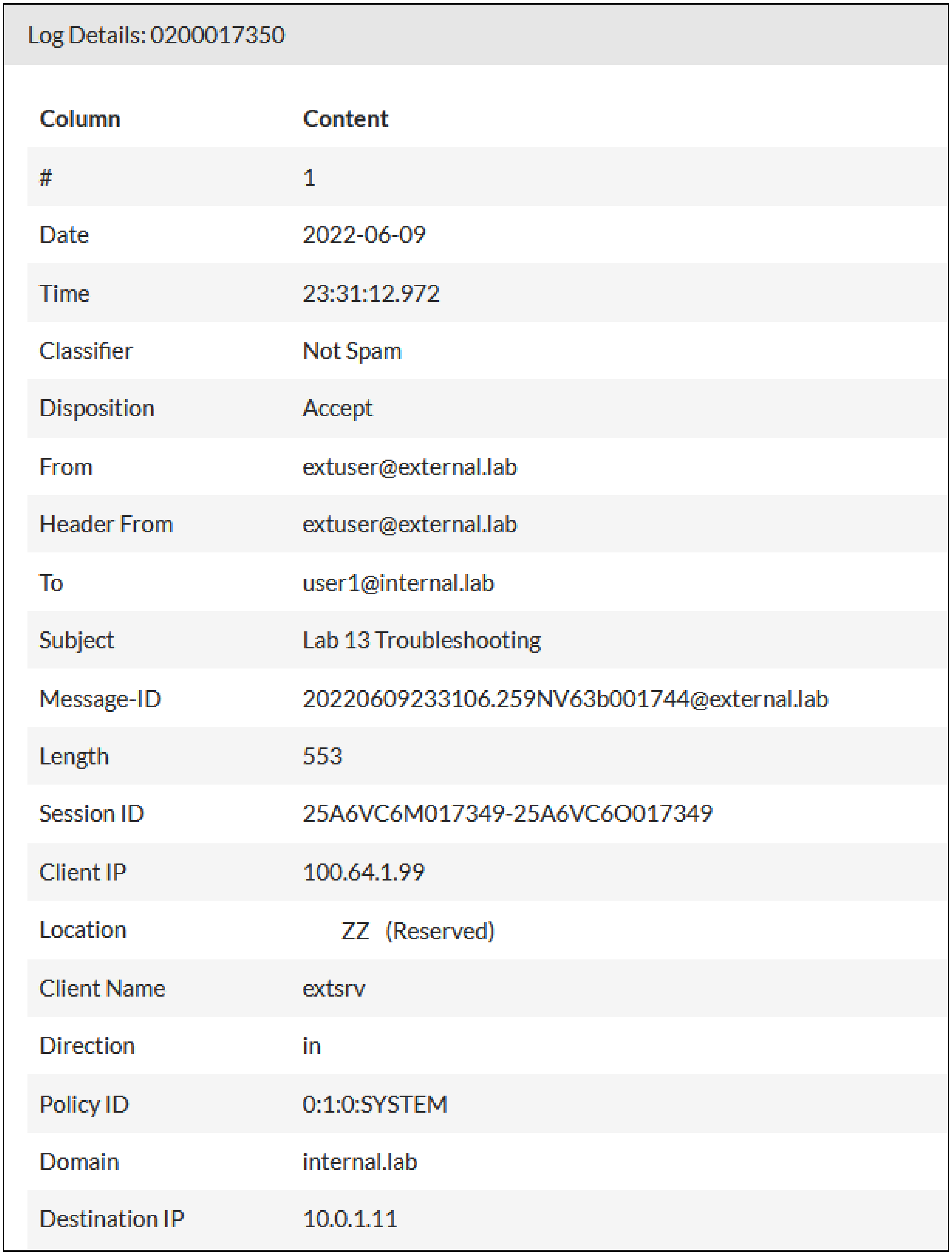


2022-05-18 23:39:58 -> Current

#	Date	Time	Classifier	Disposition	From	Header From	To	Subject	Message-ID
1	2022-06-09	23:31:12.972	Not Spam	Accept	extuser@exte...	extuser@exte...	user1@intern...	Lab 13 Troubleshooting	2022060923...

4. Right-click the log entry, and then select **View Details**.

   Do the details indicate that there is a problem?

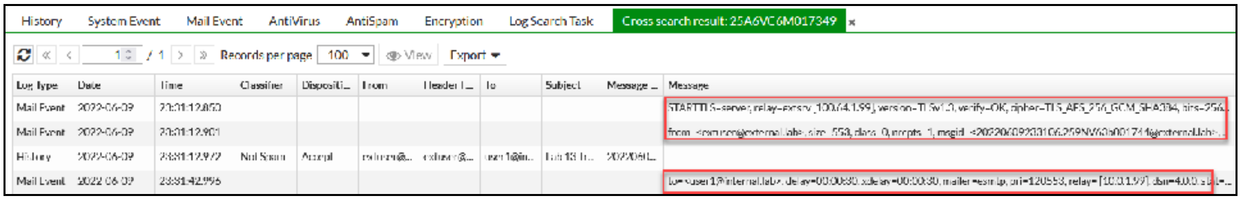


Log Details: 0200017350

Column	Content
#	1
Date	2022-06-09
Time	23:31:12.972
Classifier	Not Spam
Disposition	Accept
From	extuser@external.lab
Header From	extuser@external.lab
To	user1@internal.lab
Subject	Lab 13 Troubleshooting
Message-ID	20220609233106.259NV63b001744@external.lab
Length	553
Session ID	25A6VC6M017349-25A6VC6O017349
Client IP	100.64.1.99
Location	ZZ (Reserved)
Client Name	extsrv
Direction	in
Policy ID	0:1:0:SYSTEM
Domain	internal.lab
Destination IP	10.0.1.11

In this instance, the **History** log details don't provide much information. You must dig deeper.

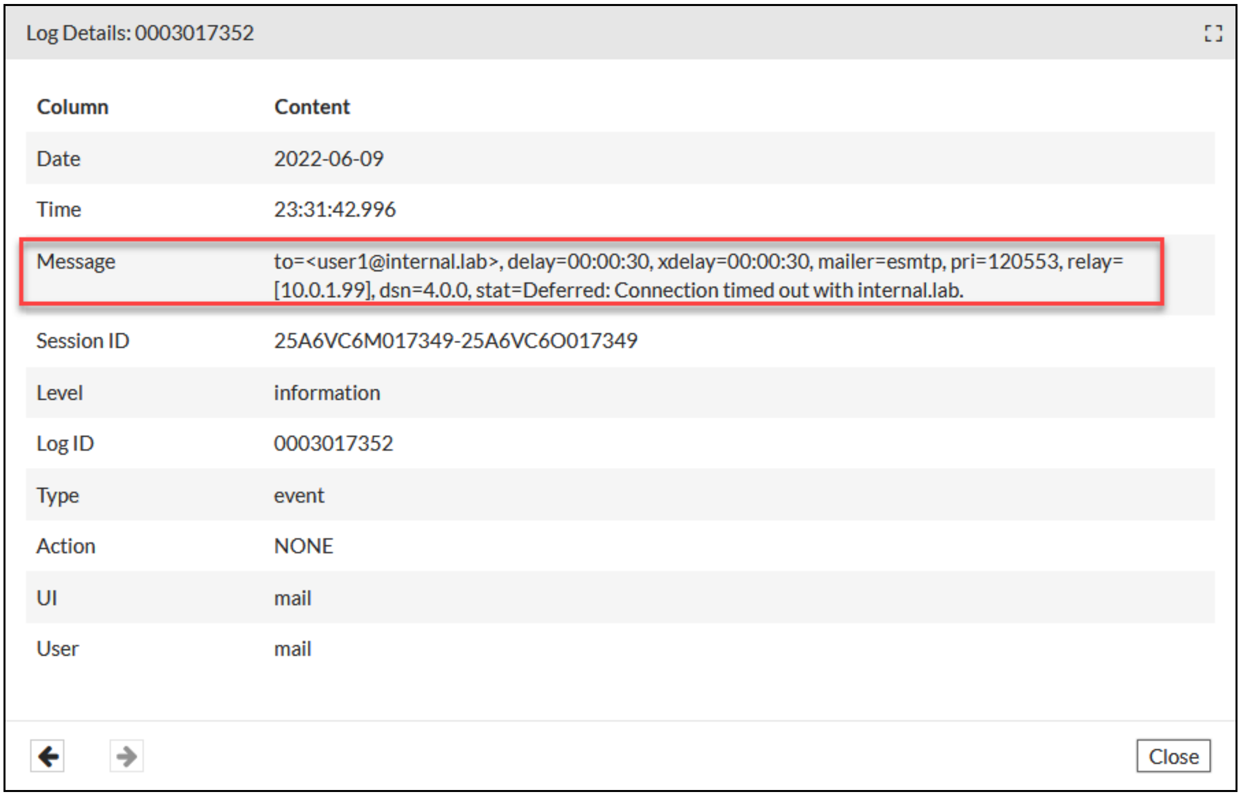
5. Click **Close**.
6. Click the **Session ID** link to retrieve the cross-search results.
7. Review the **Mail Event** logs related to the session.



Log Type	Date	Time	Classifier	Dispositi...	From	Header F...	To	Subject	Message ...	Message
Mail Event	2022-06-09	23:31:12.850								STARTTLS=server, relay=extsrv [100.64.1.99], version=TLSv1.3, verify=OK, cipher=TLS_AES_256_GCM_SHA384, bits=256...
Mail Event	2022-06-09	23:31:12.901								from=<extuser@external.lab>, size=553, class=0, nrcpts=1, msgid=<20220609233106.259NV63b001714@external.lab>, ...
History	2022-06-09	23:31:12.972	Not Spam	Accept	extuser@...	extuser@...	user1@in...	Lab 13 T...	2022060...	
Mail Event	2022-06-09	23:31:42.996								to=<user1@internal.lab>, delay=00:00:30, xdelay=00:00:30, mailer=esmtp, pri=120553, relay=[10.0.1.99], dsn=4.0.0, stat=...

The first two event logs are for the external part of the session—from ExtSRV FortiMail to IntGW FortiMail. The third event log is for the internal part of the session—from IntGW FortiMail to IntSRV FortiMail.

Do the event logs indicate that there is a problem?


Log Details: 0003017352

Column	Content
Date	2022-06-09
Time	23:31:42.996
Message	to=<user1@internal.lab>, delay=00:00:30, xdelay=00:00:30, mailer=esmtp, pri=120553, relay=[10.0.1.99], dsn=4.0.0, stat=Deferred: Connection timed out with internal.lab.
Session ID	25A6VC6M017349-25A6VC6O017349
Level	information
Log ID	0003017352
Type	event
Action	NONE
UI	mail
User	mail

The external part of the session appears to be without issues. The internal part of the session appears to be experiencing problems. Specifically, the connection from IntGW FortiMail to 10.0.1.99 is not connecting. However, the reason for the timeout is not listed.

8. Click **Close**.
9. Log out of the IntGW FortiMail management GUI.

Investigate Outbound Mail Flow

You will send an email from a user in the `internal.lab` domain to a user in the `external.lab` domain. You will view the logs on IntSRV FortiMail and try to identify any potential issues.

To investigate outbound mail flow

1. Return to the Linux-Client VM, and then using Thunderbird, try to send an email to `extuser@external.lab`.

   Hint: It won't work.

2. Click **Cancel**.
3. Click **OK**.

To view the logs on IntSRV FortiMail

1. On the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Monitor** > **Log** > **History**.
3. Double-click the active log file.

   Try to find an entry in the **History** logs for the outbound email you just tried to send.

   Hint: There won't be any.

4. Click **Monitor** > **Log** > **Mail Event**.
5. In the **Sub type** drop-down list, select **SMTP**.

   Try to find a related SMTP event log entry for the outbound email you just tried to send.

   Hint: There won't be any.

If you can't find an entry in the history or event logs for a specific session, it means there is an issue at either the IP or TCP layer. In these types of scenarios, only a traffic capture might show you what the problem is.

6. Log out of the IntSRV FortiMail management GUI.

Capture Inbound Email Traffic

You will send an email from a user in the `external.lab` domain to a user in the `internal.lab` domain, and capture that email traffic on IntGW FortiMail.

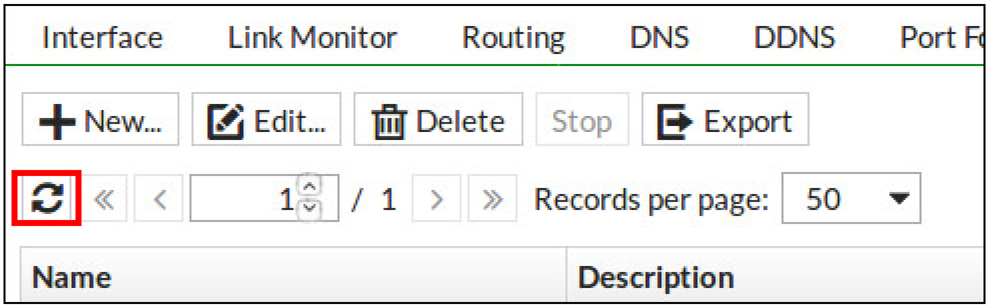
To capture inbound email traffic

1. Return to the Linux-Client VM, open a new browser, and then go to the IntGW FortiMail management GUI.
2. Click **System** > **Utility** > **Traffic Capture**.
3. Click **New**.
4. Configure the following settings:

Field	Value
Description	InboundCapture
Duration	10 minutes
Interface	port1
IP/Host	10.0.1.99
Filter	None

> After investigating the inbound email flow, you established that the issue appears to be with the internal portion of the email session. Therefore, you are only interested in seeing traffic for IntSRV FortiMail (`10.0.1.99`).

5. Click **Create**.
6. Return to the ExtSRV FortiMail webmail GUI, and then send a new email to `user1@internal.lab`.
7. Log out of the ExtSRV FortiMail webmail GUI.
8. Return to the Linux-Client VM, and then on the **Traffic Capture** tab, click the **Refresh** icon (🔄).



9. Verify that the **Size(Byte)** column is populated.
10. Select the capture, and then click **Stop**.
11. Select the capture again, and then click **Export**.

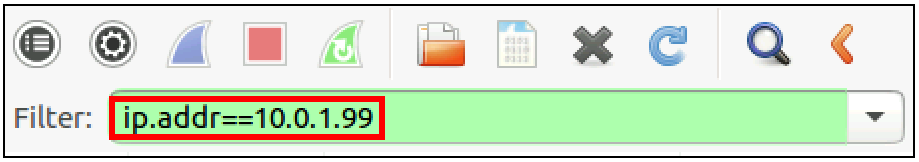
12. Save the capture file to the **Downloads** folder.
13. Log out of the IntGW FortiMail management GUI.

Review the Traffic Capture

You will review the traffic capture file and try to identify any potential issues.

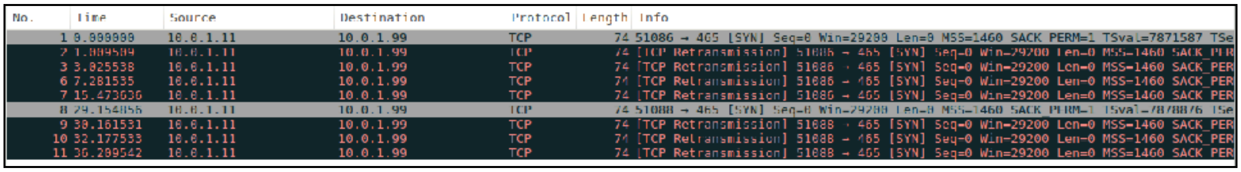
To review the traffic capture

1. Continuing on the Linux-Client VM, browse to the **Downloads** folder, and then open the traffic capture file.
2. In the **Filter** field, type `ip.addr==10.0.1.99`, and then press `Enter`.



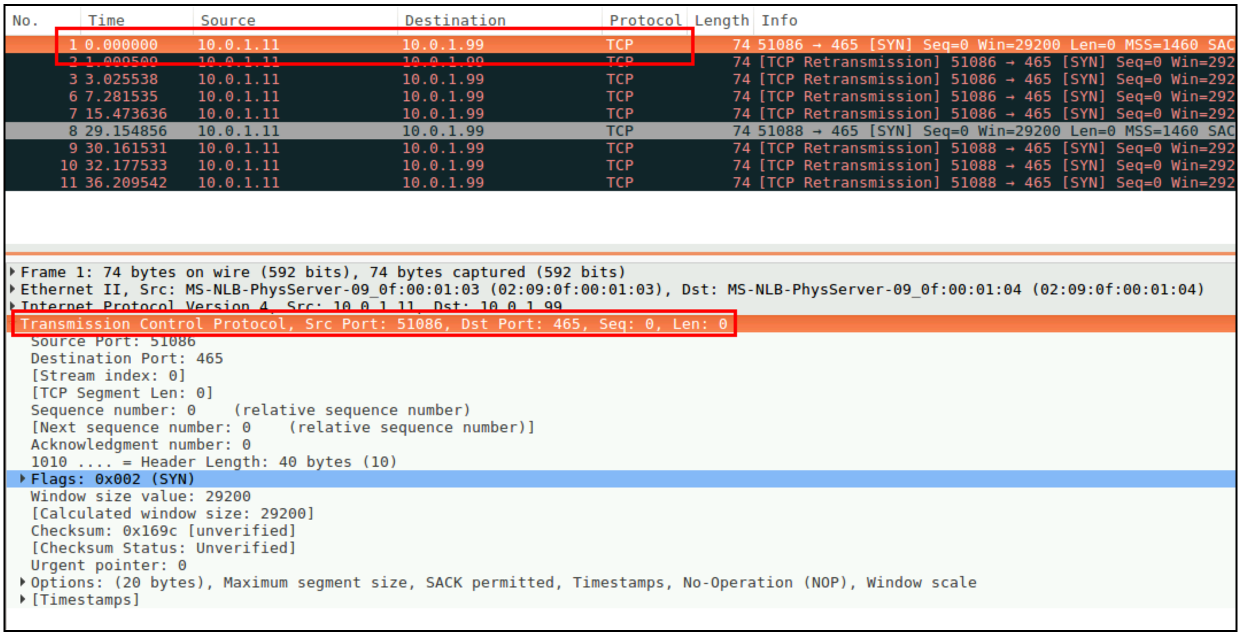
Filter: ip.addr==10.0.1.99

You should see the following packets:



```
No.  Time          Source       Destination   Protocol Length Info
   1 0.000000      10.0.1.11    10.0.1.99     TCP          74 51086 → 465 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=7871587 TSe
   2 1.000500      10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51086 → 465 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
   3 3.025538      10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51086 → 465 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
   6 7.281535      10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51086 → 465 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
   7 15.473636     10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51086 → 465 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
   8 29.154856     10.0.1.11    10.0.1.99     TCP          74 51088 → 465 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=7878876 TSe
   9 30.161531     10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51088 → 465 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
  10 32.177533     10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51088 → 465 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
  11 36.209542     10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51088 → 465 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PER
```

3. Select the first packet (**Source**: `10.0.1.11` **Destination** `10.0.1.99`), and then expand the **Transmission Control Protocol** header.

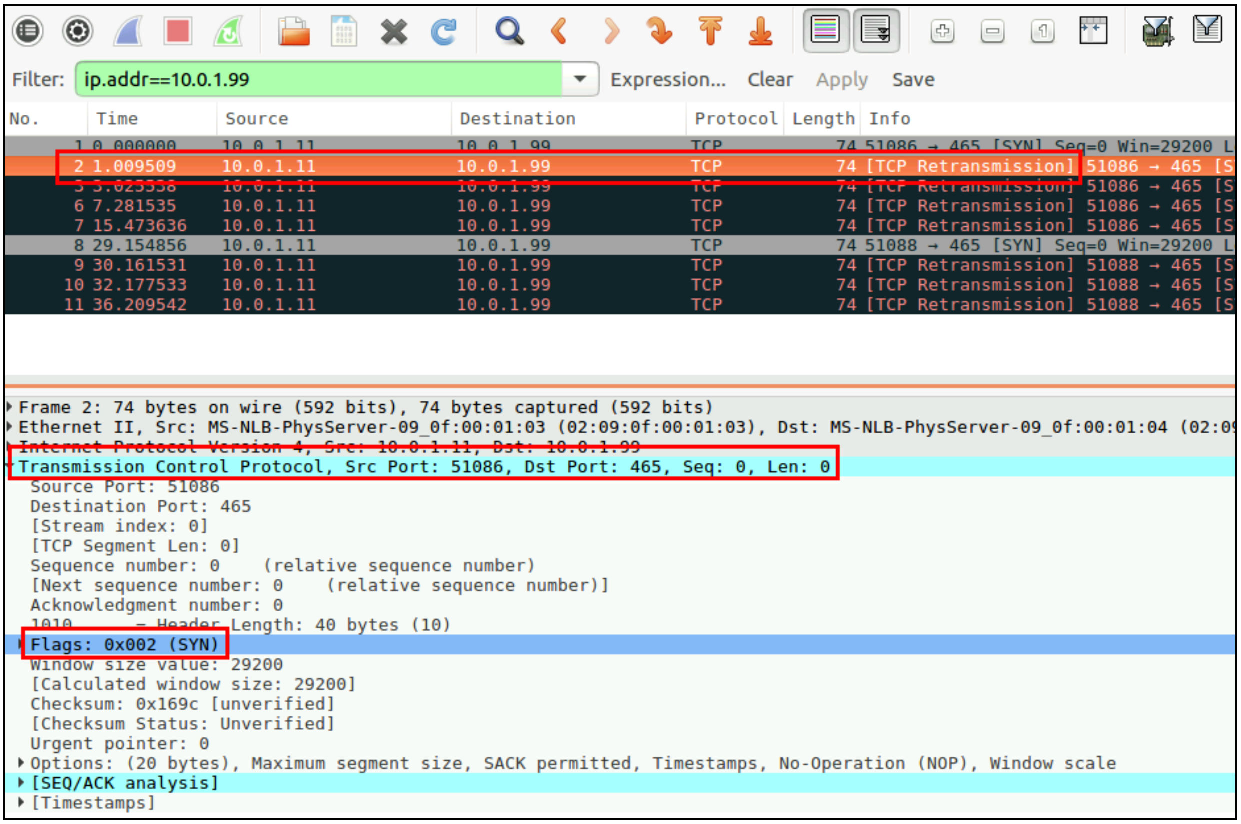


```
No.  Time        Source       Destination   Protocol Length Info
   1 0.000000    10.0.1.11    10.0.1.99     TCP          74 51086 → 465 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SAC
   2 1.000500    10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51086 → 465 [SYN] Seq=0 Win=292
   3 3.025538    10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51086 → 465 [SYN] Seq=0 Win=292
   6 7.281535    10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51086 → 465 [SYN] Seq=0 Win=292
   7 15.473636   10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51086 → 465 [SYN] Seq=0 Win=292
   8 29.154856   10.0.1.11    10.0.1.99     TCP          74 51088 → 465 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SAC
   9 30.161531   10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51088 → 465 [SYN] Seq=0 Win=292
  10 32.177533   10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51088 → 465 [SYN] Seq=0 Win=292
  11 36.209542   10.0.1.11    10.0.1.99     TCP          74 [TCP Retransmission] 51088 → 465 [SYN] Seq=0 Win=292

▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▸ Ethernet II, Src: MS-NLB-PhysServer-09_0f:00:01:03 (02:09:0f:00:01:03), Dst: MS-NLB-PhysServer-09_0f:00:01:04 (02:09:0f:00:01:04)
▸ Internet Protocol Version 4, Src: 10.0.1.11, Dst: 10.0.1.99
▾ Transmission Control Protocol, Src Port: 51086, Dst Port: 465, Seq: 0, Len: 0
    Source Port: 51086
    Destination Port: 465
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x002 (SYN)
    Window size value: 29200
    [Calculated window size: 29200]
    Checksum: 0x169c [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  ▸ [Timestamps]
```

4. Review the details.

This is the first packet of the session between IntGW FortiMail (`10.0.1.11`) and IntSRV FortiMail (`10.0.1.99`) on destination port `465`. This packet has a sequence number of `0` and is flagged as the `SYN` packet. This packet is expected, since all TCP sessions start with a `SYN` packet.

5. Select the second packet (**Source**: `10.0.1.99` **Destination**: `10.0.1.11`).
6. Review the details.



```
No.   Time         Source       Destination   Protocol Length Info
    1 0.000000     10.0.1.11    10.0.1.99     TCP      74 51086 → 465 [SYN] Seq=0 Win=29200 L
    2 1.009509     10.0.1.11    10.0.1.99     TCP      74 [TCP Retransmission] 51086 → 465 [S
    3 3.023338     10.0.1.11    10.0.1.99     TCP      74 [TCP Retransmission] 51086 → 465 [S
    6 7.281535     10.0.1.11    10.0.1.99     TCP      74 [TCP Retransmission] 51086 → 465 [S
    7 15.473636    10.0.1.11    10.0.1.99     TCP      74 [TCP Retransmission] 51086 → 465 [S
    8 29.154856    10.0.1.11    10.0.1.99     TCP      74 51088 → 465 [SYN] Seq=0 Win=29200 L
    9 30.161531    10.0.1.11    10.0.1.99     TCP      74 [TCP Retransmission] 51088 → 465 [S
   10 32.177533    10.0.1.11    10.0.1.99     TCP      74 [TCP Retransmission] 51088 → 465 [S
   11 36.209542    10.0.1.11    10.0.1.99     TCP      74 [TCP Retransmission] 51088 → 465 [S
```

```
▸ Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▸ Ethernet II, Src: MS-NLB-PhysServer-09_0f:00:01:03 (02:09:0f:00:01:03), Dst: MS-NLB-PhysServer-09_0f:00:01:04 (02:09
▸ Internet Protocol Version 4, Src: 10.0.1.11, Dst: 10.0.1.99
▾ Transmission Control Protocol, Src Port: 51086, Dst Port: 465, Seq: 0, Len: 0
    Source Port: 51086
    Destination Port: 465
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x002 (SYN)
    Window size value: 29200
    [Calculated window size: 29200]
    Checksum: 0x169c [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
```

This second packet is not expected. It is a `TCP Retransmission` packet with a `SYN` flag. IntSRV FortiMail (`10.0.1.99`) is not sending a reply back to IntGW FortiMail (`10.0.1.11`) when it attempts to connect on port `465`. The expected packet is a `SYN/ACK` packet, but this is not the case.

From this analysis, you can start to form an idea about the root cause. IntGW FortiMail (`10.0.1.11`) is sending a `SYN` packet for port `465`—however, the connection to IntSRV FortiMail (`10.0.1.99`) is timing out. So, it must be related to the remote side not replying to the traffic. However, before you try to fix this issue, look at the outbound session using another packet capture.

7. Close Wireshark.

Capture Outbound Email Traffic

You will capture outbound email traffic using the packet capture tool on the IntSRV FortiMail CLI. You will review the packet capture output and try to identify any potential issues.

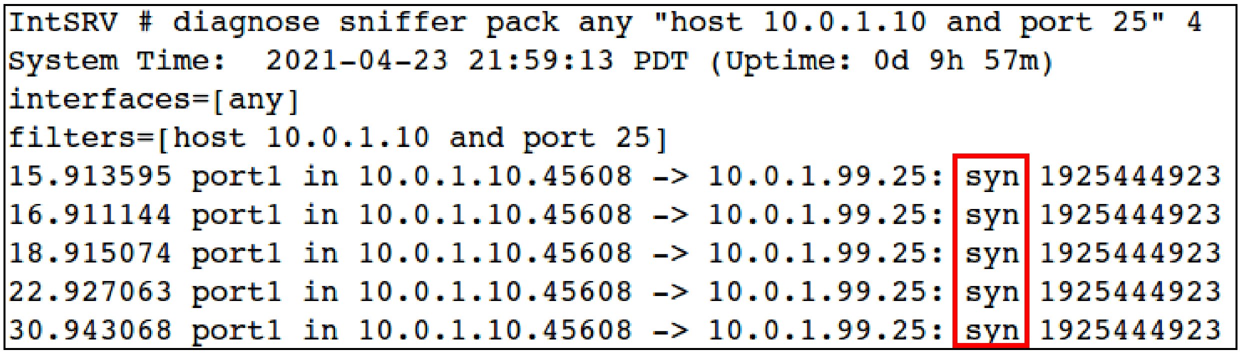
To capture outbound email traffic

1. Open an SSH connection to IntSRV FortiMail.
2. Enter the following command to start a packet capture:

```
diagnose sniffer packet any “host 10.0.1.10 and port 25” 4
```

The sniffer filter captures SMTP (`port 25`) traffic from the Linux-Client VM (`10.0.1.10`).

3. Return to the Linux-Client VM, and then using Thunderbird, try to resend the email to `extuser@external.lab`.
4. Click **Cancel**.
5. Click **OK**.
6. Return to the IntSRV FortiMail SSH session, and then review the capture output.



```
IntSRV # diagnose sniffer pack any "host 10.0.1.10 and port 25" 4
System Time:  2021-04-23 21:59:13 PDT (Uptime: 0d 9h 57m)
interfaces=[any]
filters=[host 10.0.1.10 and port 25]
15.913595 port1 in 10.0.1.10.45608 -> 10.0.1.99.25: syn 1925444923
16.911144 port1 in 10.0.1.10.45608 -> 10.0.1.99.25: syn 1925444923
18.915074 port1 in 10.0.1.10.45608 -> 10.0.1.99.25: syn 1925444923
22.927063 port1 in 10.0.1.10.45608 -> 10.0.1.99.25: syn 1925444923
30.943068 port1 in 10.0.1.10.45608 -> 10.0.1.99.25: syn 1925444923
```

IntSRV FortiMail is showing similar behavior for outbound traffic. The Linux-Client VM (`10.0.1.10`) is initiating the session on port `25` with a `SYN` packet. However, IntSRV FortiMail (`10.0.1.99`) is not replying to the session.

7. Press `Ctrl`+`C` to stop the capture.
8. Close the terminal window.
9. Close Thunderbird.

Exercise 2: Fixing the Problem

In this exercise, you will review the configuration and fix any errors. Then, you will verify your changes by sending email in both directions.

Review the Configuration

You will review the configuration on IntSRV FortiMail, and fix any potential configuration issues.

Take the Expert Challenge!

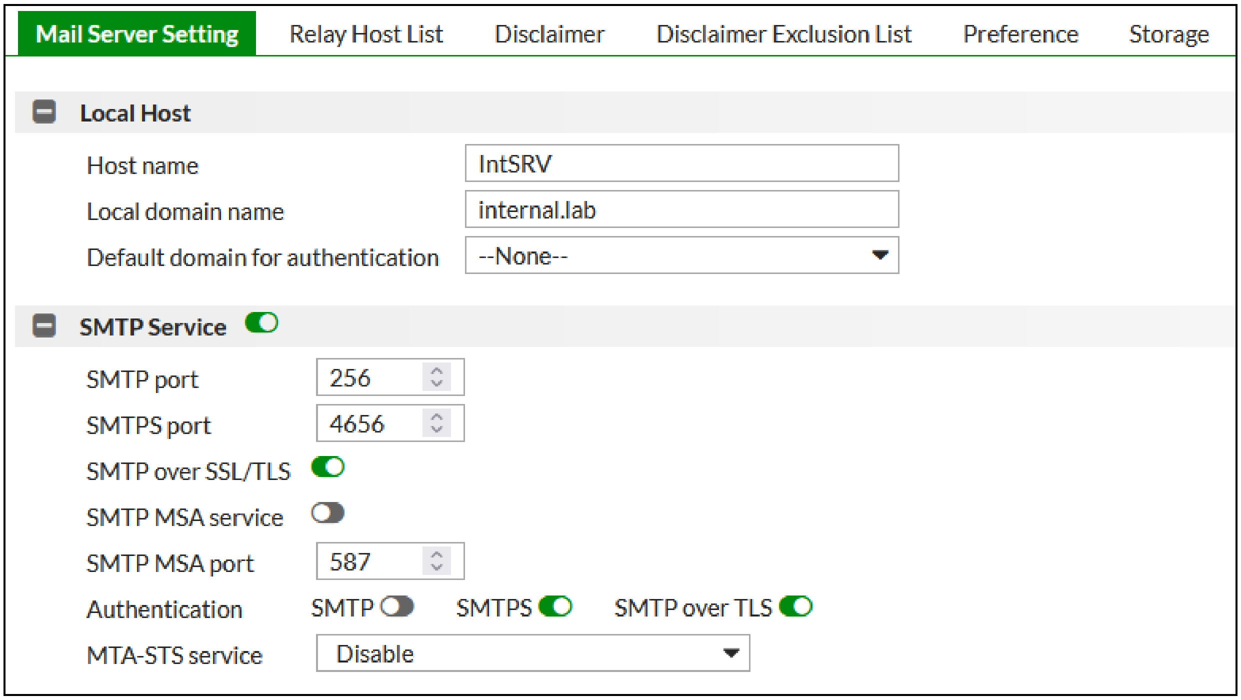
Based on your observations in the previous exercise, fix all configuration issues on IntSRV FortiMail.

Validate your fixes by sending email messages back and forth between the `internal.lab` domain and `external.lab` domain.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

To review the configuration

1. On the IntSRV FortiMail management GUI, log in with the username `admin` and password `password`.
2. Log in with the username `admin` and password `password`.
3. Click **System** > **Mail Setting** > **Mail Server Setting**.



Local Host

Host name: IntSRV
Local domain name: internal.lab
Default domain for authentication: --None--

SMTP Service ●

SMTP port: 256
SMTPS port: 4656
SMTP over SSL/TLS: ●
SMTP MSA service: ○
SMTP MSA port: 587
Authentication: SMTP ○ SMTPS ● SMTP over TLS ●
MTA-STS service: Disable

4. Review the configuration—do you notice any issues?

The **SMTP server port number** and **SMTPS server port number** values have been modified.

5. In the **SMTP server port number** field, type `25`.
6. In the **SMTPS server port number** field, type `465`.
7. Click **Apply**.
8. Log out of the IntSRV FortiMail management GUI.

To validate the fixes

1. On the Linux-Client VM, open the Thunderbird client, and then send an email message to `extuser@external.lab`.
2. On the ExtSRV FortiMail webmail GUI, log in with the username `extuser` and password `fortinet`.
3. Verify that the email was received.
4. Open the email you just sent, and then reply to it.
5. Log out of the ExtSRV FortiMail webmail GUI.
6. Return to the Linux-Client VM, and then in Thunderbird, verify that the reply is received.
7. Close Thunderbird.