CIPHERMAIL EMAIL ENCRYPTION

CipherMail Email Encryption Gateway Office 365 Integration Guide

April 26, 2017, Rev: 6852

Contents

1 Introduction

This guide explains how to configure CipherMail Email Encryption Gateway as a smarthost for Office 365 Exchange Online. It is assumed that CipherMail Email Encryption Gateway is already installed and fully functional.

This guide assumes that CipherMail Gateway will be configured for incoming and outgoing email, i.e., email received by the CipherMail Gateway for internal domains will be relayed to Exchange Online and email sent with Exchange Online will be relayed via CipherMail Gateway which will then deliver it to the final recipient or to the next hop.

> **Note**
>
> Part of the configuration requires that some commands are executed on the command line. Basic Linux experience is therefore required.

Requirements

- A functional CipherMail Email Encryption Gateway (Community or Enterprise Edition).
- Office 365 account with Exchange Online.
- Admin access to Office 365

> **Note**
>
> Instead of typing all required data and commands, it's better to copy-paste all data and commands. Copy-paste from PDF does not always preserve white-space. A text attachment containing the data and commands is therefore added to this PDF. The text attachment can be opened from the attachment pane of the PDF reader or by clicking this link

2 CipherMail configuration

Configuring the CipherMail Gateway requires the following steps

1. Configure "relay domains"
2. Configure "mynetworks"
3. Configure "internal relay host"
4. Configure relay restrictions

2.1 Configure “relay domains”

“Relay domains” (Admin → MTA) should be configured to contain all the domains hosted by Exchange Online. For example if Exchange Online is configured to handle email for domain *exchange.example.com*, you need to set “relay domains” to *exchange.example.com*. Repeat this for all domains hosted by Exchange Online.

2.2 Configure “mynetworks”

Because email sent from Exchange Online will be relayed via the CipherMail Gateway, the CipherMail Gateway should be configured to allow relaying of email from the IP addresses used by Exchange Online. The list of IP addresses used by Exchange Online can be found online https://technet.microsoft.com/en-us/library/dn163583(v=exchg.150).aspx.

The IP ranges used by Exchange Online should be added to “mynetworks”. Paste the following lines to the MTA config file (Admin → MTA → MTA config file). Replace the line `djigzo_mynetworks =` with the following lines:

```
djigzo_mynetworks = 23.103.132.0/22,
  23.103.136.0/21,
  23.103.144.0/20,
  23.103.156.0/22,
  23.103.191.0/24,
  23.103.198.0/23,
  23.103.198.0/24,
  23.103.199.0/24,
  23.103.200.0/22,
  23.103.212.0/22,
  40.92.0.0/14,
  40.107.0.0/17,
  40.107.128.0/18,
  52.100.0.0/14,
  65.55.88.0/24,
  65.55.169.0/24,
  94.245.120.64/26,
  104.47.0.0/17,
  104.212.58.0/23,
  134.170.132.0/24,
  134.170.140.0/24,
  157.55.234.0/24,
  157.56.110.0/23,
  157.56.112.0/24,
  207.46.51.64/26,
  207.46.100.0/24,
  207.46.163.0/24,
  213.199.154.0/24,
  213.199.180.128/26,
  216.32.180.0/23
```

Warning

Copying the above list from the PDF removes the spaces at the beginning of the lines. The spaces at the beginning of the lines are important. You are strongly advised to copy-paste directly from the attached txt file *ciphermail-o365-intergration-guide.txt*

Alternatively, the IP ranges can also be added using the Web GUI.

2.3 Configure “internal relay host”

Email received by the CipherMail Gateway should be delivered to Exchange Online. The MTA “internal relay host” (Admin → MTA) should be set to the Exchange Online hostname responsible for handling your email (see domains in Office 365 Admin center).

2.4 Configure relay restrictions

Exchange Online does not support authentication when relaying via a smarthost. Relaying to external domains should therefore only be allowed if the SMTP connection comes from the Exchange Online IP range and only if the sender is from one of your own domains. This requires a number of configuration steps.

1. Configure MTA main config
2. Create authorized domains file

Configure MTA main config

The following lines should be added to the MTA main config file (Admin → MTA → MTA config file).

```
indexed = ${default_database_type}:${config_directory}/
smtpd_relay_restrictions =
  check_sender_access ${indexed}o365_authorized_senders
  defer_unauth_destination
```

Note: You can add the lines at the end of the config file.

Create authorized senders domains file

Email sent from Exchange Online should only be relayed if the sender domain is from one of your domains hosted by Exchange Online.

The file `/etc/postfix/o365_authorized_senders` should be created containing the list of the allowed sending domains (this should be the same list of domains configured as “relay domains”).

```
$ sudo vi /etc/postfix/o365_authorized_senders
```

The `o365_authorized_senders` file should contain the mappings from your domains to the `permit_mynetworks` action.

```
<>                      permit_mynetworks
exchange.example.com    permit_mynetworks
other.example.com       permit_mynetworks
```

Note: Add all your domains which are hosted by Exchange Online (this should be the same list of domains configured as "relay domains").

Note: <> is required for connector validation and bounce mail.

Create indexed version The `o365_authorized_senders` file should be indexed:

```
$ sudo postmap hash://etc/postfix/o365_authorized_senders
```

3 Add Exchange Online smarthost connector

A connector should be added to the Exchange Online configuration which will send all outgoing email via the CipherMail Gateway. Adding a connector requires a number steps.

1. Log into the Office 365 Admin center.
2. Open Exchange Admin center ("Admin Centers" → "Exchange").
3. In Exchange admin center click on "mail flow" → "connector".
4. In connectors overview click on "New" (click the + sign).
5. In "Select your mail flow scenario" set from to "Office 365" and to 'Partner organization'. Click Next.
6. Set a name for the connector (for example "Relay via CipherMail"). Click Next.
7. Select "Only when email messages are sent to these domains"
8. Add a domain (click the + sign)
9. Set domain to "*" (* means use for all domains). Click OK. Click Next.
10. On "How do you want to route email messages" select "Route email through these smart hosts"
11. Add smart host (click the + sign)
12. Select the hostname (or IP address) of the CipherMail Gateway. Click Save. Click Next.

13. In “How should Office 365 connect to your partner organization’s email server” select the preferred TLS level [1]. Click Next.
14. Confirm new connector settings. Click Next.
15. On “Validate this connector” page, add a recipient used for validation (click the + sign).
16. Select a valid recipient. Click OK. Click Validate.
17. Check whether the validation was successful (a message should have been sent via the CipherMail Gateway).
18. If validation was successful click Save.

4 Test outgoing email

Test whether email sent from Exchange Online is relayed via the CipherMail Gateway.

5 Test incoming email

Send a message from the CipherMail Gateway to an Office 365 recipient and check whether the message is received. This can be done for example from the Web GUI of CipherMail Gateway, with telnet connecting to port 25 or using an SMTP application connecting directly to the CipherMail Gateway on port 25.

6 Change or add MX record

If all incoming email should first be handled by the CipherMail Gateway, to make sure that S/MIME or PGP encrypted email is decrypted, the MX records for your domains should point to the hostname of the CipherMail Gateway. The existing MX record can be modified or an additional MX record pointing to the CipherMail Gateway can be added (in which case the new MX record should have a higher priority).

7 Finished

All incoming and outgoing email should now be relayed via the CipherMail Gateway.

[1] Selecting TLS requires that the CipherMail Gateway is configured for TLS