

CIPHERMAIL EMAIL ENCRYPTION

---

# CipherMail Gateway Quick Setup Guide

---



April 4, 2016, Rev: 9537



## Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
<b>2</b>	<b>Typical setups</b>	<b>4</b>
2.1	Direct delivery . . . . .	4
2.2	Via relay . . . . .	4
2.3	With virus scanner . . . . .	5
2.4	With virus scanner via relay . . . . .	5
<b>3</b>	<b>Network config</b>	<b>5</b>
3.1	IP address . . . . .	6
3.2	Hostname . . . . .	6
3.3	DNS . . . . .	8
<b>4</b>	<b>Direct delivery setup</b>	<b>8</b>
4.1	Configure relay domains . . . . .	9
4.2	Configure MTA hostname . . . . .	10
4.3	Configure internal relay host . . . . .	10
4.4	Configure external relay host . . . . .	10
4.5	Enable "Reject unverified recipient" . . . . .	13
4.6	Configure "My Networks" . . . . .	13
4.7	Apply new MTA settings . . . . .	14
4.8	Add internal domains . . . . .	14
4.9	Configure internal mail server . . . . .	14
4.10	Test outgoing email . . . . .	15
4.11	Test incoming email . . . . .	15
4.12	Configure firewall (or MX records) . . . . .	16
4.13	Final test . . . . .	16
<b>5</b>	<b>Via relay setup</b>	<b>17</b>
5.1	Configure relay domains . . . . .	17
5.2	Configure MTA hostname . . . . .	18
5.3	Configure internal relay host . . . . .	18
5.4	Configure external relay host . . . . .	18
5.5	Enable "Reject unverified recipient" . . . . .	19
5.6	Configure "My Networks" . . . . .	19
5.7	Apply new MTA settings . . . . .	19
5.8	Add internal domains . . . . .	20
5.9	Configure internal mail server . . . . .	20
5.10	Test incoming email . . . . .	20
5.11	Configure the relay server . . . . .	21
5.12	Final test . . . . .	21
<b>6</b>	<b>With virus scanner setup</b>	<b>21</b>
6.1	Configure relay domains . . . . .	22
6.2	Configure MTA hostname . . . . .	23
6.3	Configure internal relay host . . . . .	23
6.4	Configure external relay host . . . . .	23
6.5	Enable "Reject unverified recipient" . . . . .	24

---

6.6	Configure "My Networks" . . . . .	24
6.7	Apply new MTA settings . . . . .	24
6.8	Add internal domains . . . . .	25
6.9	Configure virus scanner . . . . .	25
6.10	Test outgoing email . . . . .	25
6.11	Test incoming email . . . . .	26
6.12	Configure firewall (or MX records) . . . . .	26
6.13	Final test . . . . .	27
<b>7</b>	<b>With virus scanner via relay setup</b>	<b>27</b>
7.1	Configure relay domains . . . . .	28
7.2	Configure MTA hostname . . . . .	28
7.3	Configure internal relay host . . . . .	28
7.4	Configure external relay host . . . . .	29
7.5	Enable "Reject unverified recipient" . . . . .	29
7.6	Configure "My Networks" . . . . .	30
7.7	Apply new MTA settings . . . . .	30
7.8	Add internal domains . . . . .	30
7.9	Configure virus scanner . . . . .	30
7.10	Test incoming email . . . . .	31
7.11	Configure the relay server . . . . .	31
7.12	Final test . . . . .	31
<b>A</b>	<b>SMTP HELO/EHLO name</b>	<b>33</b>
<b>B</b>	<b>Exchange 2010 send connector</b>	<b>33</b>
<b>C</b>	<b>Simulate a mail client using telnet</b>	<b>34</b>



Figure 1: Direct delivery

## 1 Introduction

This guide briefly explains how to configure a CipherMail gateway for sending and receiving email. This guide does not explain how to configure the gateway for encryption or data leak prevention. For configuring encryption and data leak prevention, see the other guides.

### Note

This guide assumes that the gateway has already been installed but not yet configured, either using the virtual appliance or using the provided installation packages. See the quick install guide or the virtual appliance guide for details on how to install the gateway.

## 2 Typical setups

The CipherMail gateway is an SMTP server which protects email at the gateway level. The gateway should therefore be placed within the existing email infrastructure. The exact placement of the gateway depends on the infrastructure and requirements (for example whether or not there is a centralized virus scanner). The four most typical setups will be handled: “direct delivery” (fig. 1), “via relay” (fig. 2), “with virus scanner” (fig. 3) and “with virus scanner via relay” (fig. 4).

### 2.1 Direct delivery

In this setup (fig. 1), the CipherMail gateway is placed between the internal mail server (for example Exchange) and the Internet. The internal mail server sends email for external recipients to the CipherMail gateway and the CipherMail gateway directly delivers email to the external recipients via MX lookups. The Ciphermail gateway receives email from external senders and forwards the email to the internal mail server.

### 2.2 Via relay

In this setup (fig. 2), the CipherMail gateway is placed between the internal mail server (for example Exchange) and an SMTP relay server (also known as

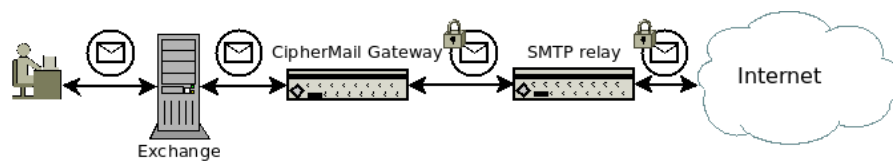


Figure 2: Relay

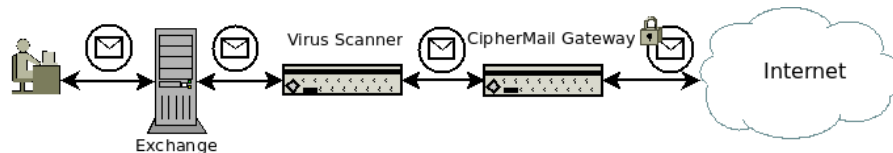


Figure 3: Virus scanner direct

“front-end server”). The internal mail server sends email for external recipients to the CipherMail gateway and the CipherMail gateway forwards the email for external recipients to the SMTP relay server. The SMTP relay server directly delivers email to the external recipients via MX lookups.

**Note:** The relay server can be internally and externally hosted. For example the relay server can be provided by your ISP.

### 2.3 With virus scanner

In this setup (fig. 3), the CipherMail gateway is placed between the centralized email virus scanner and the Internet. The internal mail server sends email for external recipients to the virus scanner, the virus scanner forwards the email to the CipherMail gateway and the CipherMail gateway directly delivers email to the external recipients via MX lookups.

### 2.4 With virus scanner via relay

In this setup (fig. 4), the CipherMail gateway is placed between the centralized email virus scanner and an SMTP relay server (also known as “front-end server”). The internal mail server sends email for external recipients to the virus scanner, the virus scanner forwards the email to the CipherMail gateway and the CipherMail gateway forwards the email for external recipients to the SMTP relay server. The SMTP relay server directly delivers email to the external recipients via MX lookups.

## 3 Network config

The following network settings must be configured for a functional gateway: IP address, hostname and DNS.

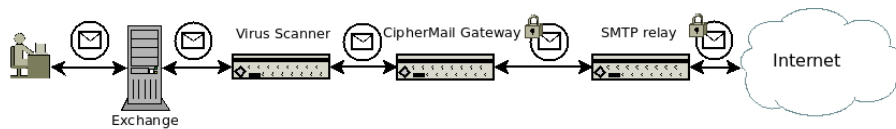


Figure 4: Virus scanner via relay

**Note**

The network settings page is only available for the Ciphermail Virtual Appliance. If the gateway has been manually installed, the network should be configured with the tools provided by the operating system. This part can be skipped if the network is already configured.

The network settings can be configured from the WEB GUI. The network info page can be opened by clicking Admin → network. The “Network info” page will be opened which provides all the relevant network information like DNS servers, network interfaces etc. (see figure 5).

**Note:** Since most network settings should be configured from the WEB GUI, the WEB GUI should have a valid IP before the WEB GUI can be accessed. The IP address can be configured with the console system application by logging into the console. See the “Virtual Appliance Guide” for more information.

### 3.1 IP address

The available network interfaces can be configured by clicking “interfaces”. This opens the interfaces page (see figure 6). A network interface can be configured by clicking the “gear” icon of the interface. The network interface can be configured for a dynamic IP address (DHCP) or for a static IP address (see figure 7).

**Action**

Set the IP address of the gateway appliance.

### 3.2 Hostname

With the hostname page, the hostname of the gateway can be set (see figure 8). The hostname is used by many of the networking programs to identify the machine.

**Note:** It’s advised to use a fully qualified hostname.

Certificates Roots CRLs CA DLP Settings Queues Logs Admin

### Network info

[Info](#) | [Interfaces](#) | [hostname](#) | [DNS](#) | [hosts](#) | [ntp](#)

Network configuration information.

**DNS servers**

192.168.1.1

**DNS domain list search**

**Network interfaces**

Name	Address	MAC	Broadcast	Mask	Gateway	DHCP
eth0	192.168.1.109	00:15:5d:b2:2a:1d	192.168.1.255	255.255.255.0		true

**Default gateway**

192.168.1.1

Close


Figure 5: Network info

### Network interfaces

[Info](#) | [Interfaces](#) | [hostname](#) | [DNS](#) | [hosts](#) | [ntp](#)

Manage network interfaces.

**Network interfaces**

Name	Address	MAC	Broadcast	Mask	Gateway	DHCP
 eth0	192.168.1.109	00:15:5d:b2:2a:1d	192.168.1.255	255.255.255.0		true

Close

Figure 6: Network interfaces

**Action**

Set the hostname of the gateway appliance to the fully qualified host-name.



A network interface can either be configured with a static IP address or with DHCP.

DHCP

IP address

Netmask

Broadcast

Gateway

If the new network configuration is not correct, it might happen that the web GUI is not working.

Figure 7: Network interface

**Network settings: Hostname**

[info](#) | [interfaces](#) | [hostname](#) | [DNS](#) | [hosts](#) | [ntp](#)

The hostname of the system. It is advised to use a fully qualified domain name.

Hostname

Figure 8: Hostname

### 3.3 DNS

The gateway requires at least one DNS server. The DNS server can be configured with the DNS page (see figure 9)

Action
Configure at least one DNS server entry.

## 4 Direct delivery setup

This section explains the “Direct” setup where the CipherMail gateway is placed between the internal mail server (for example Exchange) and the Internet. (see figure 1).

The following steps will be described:

1. Configure relay domains.
2. Configure MTA hostname.

**Network settings: DNS**

[Info](#) | [Interfaces](#) | [hostname](#) | [DNS](#) | [hosts](#) | [ntp](#)

On this page, the static DNS configuration can be set\*. The DNS:

DNS 1

DNS 2

DNS 3

Domain search   
domain suffix search  
(space separated)

\* The configured DNS servers on this page have a higher priority than the system default.

Figure 9: DNS

3. Configure CipherMail to deliver email for the relay domains to the internal mail server.
4. Configure CipherMail to directly deliver email for external recipients.
5. Enable “Reject unverified recipient”.
6. Allow internal mail server to relay to external recipients.
7. Apply new MTA settings.
8. Add internal domains.
9. Configure the internal mail server to relay email for external recipients via the CipherMail gateway.
10. Test outgoing email.
11. Test incoming email.
12. Configure firewall (or MX records) to deliver incoming email to CipherMail gateway.
13. Final test.

## 4.1 Configure relay domains

The relay domains are the domains of the gateway for which the internal mail server handles email. The relay domains should match all the domains of the internal mail server. The relay domains can be configured on the MTA settings page (see figure 10).

**Action**

For each domain, fill-in the “Add domain” field and press the “Add” button

## 4.2 Configure MTA hostname

The MTA hostname can be configured by setting the “My hostname” field (see figure 10). It is advised that the MTA hostname be set to the fully qualified domain name of the external IP address and that the reverse lookup of the external IP address (i.e., PTR record) is equal to the MTA hostname. If for whatever reason the MTA hostname cannot be set to the fully qualified domain name of the external IP address, or the reverse lookup does not match the MTA hostname, the “SMTP helo name” should be manually set to the reverse lookup of the external IP address (see appendix A for more information about HELO/EHLO name).

**Note:** The MTA hostame should be different from the name of the virus scanner and the external relay server. If the MTA (Postfix) detects that the hostname of the server it connects to is the same as it’s own hostname, the email will be bounced and a the following message will appear in the MTA log:

```
status=bounced (mail for [x.x.x.x] loops back to myself).
```

This check was added to prevent mail loops.

**Action**

Set hostname to fully qualified domain name.

## 4.3 Configure internal relay host

After email has been handled by the gateway, email sent to any of the relay domains should be forwarded to the internal mail server.

**Action**

Set “Internal relay host” to the hostname or IP address of the internal server. For most setups, port should be set to 25 and “mx” should not be selected.

## 4.4 Configure external relay host

With the “Direct delivery setup”, email sent to external recipients will be delivered directly to the mail servers of the recipients using MX records. By leaving

### MTA configuration

---

#### MTA config file

---

##### Relay domains

**Relay domains**  
destination domains this system will relay mail to (and subdomains if Match Subdomains is selected)

**Add domain**  
add a new relay domain

---

##### My networks

**My networks**  
the list of "trusted" SMTP clients that have more privileges than "strangers". In particular, "trusted" SMTP clients are allowed to relay mail through the MTA

**Add network**  
add a new network

---

##### Other

**My Hostname**   
the internet hostname of this mail system

**External relay host**  mx  port   
the default mail next-hop destination for remote delivery. Leave empty for direct delivery using mx-records

**Internal relay host**  mx  port   
the next-hop destination of mail to one of the relay domains (this will typically be the internal company email server)

**Match Subdomains**   
select if subdomains of Relay domains should automatically match

show advanced settings

Figure 10: MTA config

show advanced settings

**Before filter message size limit**   
the maximal size in bytes of a message, including envelope information accepted by the SMTP daemon

**After filter message size limit**   
the maximal size in bytes of a message, including envelope information after encryption/decryption. This limit must not be smaller than 'Before filter message size limit'.

**Mailbox size limit**   
the maximal size in bytes of any individual mailbox. This limit must not be smaller than 'After filter message size limit'.

**SMTP helo name**   
the hostname to use for the SMTP EHLO or HELO command. If empty "My hostname" is used as helo name.

**Reject unverified recipient**  reject code   
reject the request when mail to the RCPT TO address is known to bounce.

Figure 11: MTA advanced config

“External relay host” empty, CipherMail will deliver email to external recipients using MX records.

**Action**

Set “External relay host” to an empty (i.e., blank) value.

## 4.5 Enable “Reject unverified recipient”

A mail server should know which recipients are valid recipients for a relay domain before accepting the message (i.e., the mail server should know whether there is a valid inbox for the recipient). If an email is accepted for relay but the next server (i.e., the internal mail server) does not accept the message because the recipient is not valid, the email should be bounced by the receiving server. Bouncing an email after accepting the message is called “backscatter”. Systems that generate email backscatter can end up being listed on a mail blacklist (RBL).

By enabling “Reject unverified recipient” the gateway “learns” which recipient addresses are valid or not by querying the server it relays to. When an email is received for an unknown recipient, the server “asks” the server it relays to whether the recipient is a valid recipient or not. The message is only accepted when the next email server reports that the recipient is a valid. The result of this verification process is cached.

The “reject code” is the SMTP result code used when the email is not accepted. This should initially be set to “450” (which tells the connecting SMTP server that the message is not accepted because of a temporary error). It should be changed to “550” (permanent error) when the verification procedure works correctly. See the Postfix documentation for more information on address verification<sup>1</sup>.

**Action**

Select “Reject unverified recipient”

## 4.6 Configure “My Networks”

To encrypt outgoing email, the internal mail server should send all outgoing email via the CipherMail gateway. The internal mail server should therefore be allowed to send email to all external recipient via the CipherMail gateway.

**Action**

Add the IP address of the internal mail server to “My Networks”.

<sup>1</sup>See [http://www.postfix.org/ADDRESS\\_VERIFICATION\\_README.html](http://www.postfix.org/ADDRESS_VERIFICATION_README.html)

**Edit domain: example.com**

S/MIME ▾ PGP ▾ | portal | templates | DLP | sms | PDF | cert req | we

**General**

Comment   inherit

Locality   inherit

Encrypt Mode   inherit

Figure 12: Locality

## 4.7 Apply new MTA settings

Now all the required MTA configuration changes are done, the new MTA settings should be applied.

### Action

Click “Apply” on the MTA config page to apply the new MTA settings.

## 4.8 Add internal domains

The CipherMail gateway needs to encrypt email for external recipients and decrypt email for internal recipients. The gateway therefore has to know which recipients are internal and which recipients are external. The user property “Locality” determines whether a recipient is internal or external. In most setups, all domains from the “relay domains” should be internal because the gateway is configured to handle incoming email for this domains.

### Action

For every domain configured as a “relay domain” take the following steps:

1. Add a new domain (“Domains” → “add domain”)
2. For “Locality”, deselect “inherit” and set “Locality” to “Internal” (see figure 12)
3. Apply settings

## 4.9 Configure internal mail server

To allow the CipherMail gateway to encrypt outgoing email, all outgoing email should be handled by the CipherMail gateway. The internal mail server should

therefore be configured to relay via the CipherMail gateway.

Because every mail server is configured differently, we refer you to the documentation of the internal mail server on how to configure the mail server to relay via an external server. For a brief overview on how to configure Exchange 2010, see appendix B.

#### Action

Configure the internal mail server to relay email via the CipherMail gateway.

### 4.10 Test outgoing email

To test whether the CipherMail gateway can send email to external recipients, use the built-in “Send email” tool (Admin → other → send email). This test tool will directly send an email from the CipherMail gateway to the external recipients.

#### Action

Send a test email to an external recipient using the “Send email” tool.

To test whether the internal mail server can send email to external recipients via the CipherMail gateway, send an email from a mail client connected to the internal mail server and check the MTA logs of CipherMail to see whether the email is actually relayed via the CipherMail gateway.

#### Action

Send a test email to an external recipient with a mail client and check the MTA logs of CipherMail whether it was relayed via CipherMail.

### 4.11 Test incoming email

It should be tested whether the CipherMail gateway can deliver email to the internal mail server. To test this, email should be sent to a valid recipient. The best way to test this is by sending an email with an email client configured to connect to the CipherMail gateway on the SMTP port (25). Alternatively, telnet can be used to “simulate” and email client by directly connecting to port 25 of the CipherMail gateway (see appendix C) for more information on how to send an email using telnet.



**Action**

Send a test email to a valid internal recipient with a mail client directly connected to the CipherMail gateway or using telnet and check whether it was delivered.

### 4.12 **Configure firewall (or MX records)**

The complete mail flow has been configured. However mail sent by external senders is still delivered to the internal mail server and not to the CipherMail gateway. The best way to make sure that incoming email is delivered to the CipherMail gateway and not to the internal mail server is by changing NAT rules on the firewall (i.e., tell the firewall to translate the external IP address to the internal IP address of the CipherMail gateway on port 25). Alternatively if the firewall does not support this, the external DNS MX records can be modified to point to the CipherMail gateway.

**Note:** Changing DNS records might take some time before all DNS servers are updated. It's therefore advised to first try to use a firewall rule to redirect mail to the CipherMail gateway.

**Action**

Set a firewall rule to redirect incoming external mail to the CipherMail gateway.

### 4.13 **Final test**

Now the complete mail flow has been setup, incoming and outgoing mail should be tested.

**Action**

Test outgoing email by sending a message from an internal mail client to an external recipient.

**Action**

Test incoming email by sending a message from an external email account to an internal recipient.

## 5 Via relay setup

In this setup (figure 2), the CipherMail gateway is placed between the internal mail server (for example Exchange) and an SMTP relay server (also known as “front-end server”). The internal mail server sends email for external recipients to the CipherMail gateway and the CipherMail gateway forwards the email for external recipients to the SMTP relay server.

The following steps will be described:

1. Configure relay domains.
2. Configure MTA hostname.
3. Configure CipherMail to deliver email for the relay domains to the internal mail server.
4. Configure CipherMail to deliver email for external recipients to the relay server.
5. Enable “Reject unverified recipient”.
6. Allow internal mail server to relay to external recipients.
7. Apply new MTA settings.
8. Add internal domains.
9. Configure the internal mail server to relay email for external recipients via the CipherMail gateway.
10. Test incoming email.
11. Configure the relay mail server to deliver email for internal recipients to the CipherMail gateway.
12. Final test.

### 5.1 Configure relay domains

The relay domains are the domains of the gateway for which the internal mail server handles email. The relay domains should match all the domains of the internal mail server. To relay domains can be configured on the MTA settings page (see figure 10).

#### Action

For each domain, fill-in the “Add domain” field and press the “Add” button

## 5.2 Configure MTA hostname

The MTA hostname can be configured by setting the “My hostname” field (see figure 10).

**Note:** The MTA hostname should be different from the name of the virus scanner and the external relay server. If the MTA (Postfix) detects that the hostname of the server it connects to is the same as its own hostname, the email will be bounced and the following message will appear in the MTA log:

```
status=bounced (mail for [x.x.x.x] loops back to myself).
```

This check was added to prevent mail loops.

### Action

Set hostname.

## 5.3 Configure internal relay host

After email has been handled by the gateway, email sent to any of the relay domains should be forwarded to the internal mail server.

### Action

Set “Internal relay host” to the hostname or IP address of the internal server. For most setups, port should be set to 25 and “mx” should not be selected.

## 5.4 Configure external relay host

With the “Via relay setup”, email sent to external recipients will be relayed via the relay server. The CipherMail gateway therefore has to be configured to relay email for external recipient via the relay server.

### Action

Set “External relay host” to the hostname or IP address of the relay server. For most setups, port should be set to 25 and “mx” should not be selected.

**Note:** If the relay server requires username/password authentication, add the credentials for the relay to the SASL settings (see MTA → sasl).

## 5.5 Enable “Reject unverified recipient”

A mail server should know which recipients are valid recipients for a relay domain before accepting the message (i.e., the mail server should know whether there is a valid inbox for the recipient). If an email is accepted for relay but the next server (i.e., the internal mail server) does not accept the message because the recipient is not valid, the email should be bounced by the receiving server. Bouncing an email after accepting the message is called “backscatter”. Systems that generate email backscatter can end up being listed on a mail blacklist (RBL).

By enabling “Reject unverified recipient” the gateway “learns” which recipient addresses are valid or not by querying the server it relays to. When an email is received for an unknown recipient, the server “asks” the server it relays to whether the recipient is a valid recipient or not. The message is only accepted when the next email server reports that the recipient is a valid. The result of this verification process is cached.

The “reject code” is the SMTP result code used when the email is not accepted. This should initially be set to “450” (which tells the connecting SMTP server that the message is not accepted because of a temporary error). It should be changed to “550” (permanent error) when the verification procedure works correctly. See the Postfix documentation for more information on address verification<sup>2</sup>.

**Note:** If the relay server already knows which recipients are valid recipients or not, for example using LDAP, there is not need to enable “Reject unverified recipient”.

### Action

Select “Reject unverified recipient”

## 5.6 Configure “My Networks”

To encrypt outgoing email, the internal mail server should send all outgoing email via the CipherMail gateway. The internal mail server should therefore be allowed to send email to all external recipient via the CipherMail gateway.

### Action

Add the IP address of the internal mail server to “My Networks”.

## 5.7 Apply new MTA settings

Now all the required MTA configuration changes are done, the new MTA settings should be applied.

<sup>2</sup>See [http://www.postfix.org/ADDRESS\\_VERIFICATION\\_README.html](http://www.postfix.org/ADDRESS_VERIFICATION_README.html)

**Action**

Click “Apply” on the MTA config page to apply the new MTA settings.

## 5.8 Add internal domains

The CipherMail gateway needs to encrypt email for external recipients and decrypt email for internal recipients. The gateway therefore has to know which recipients are internal and which recipients are external. The user property “Locality” determines whether a recipient is internal or external. In most setups, all domains from the “relay domains” should be internal because the gateway is configured to handle incoming email for this domains.

**Action**

For every domain configured as a “relay domain” take the following steps:

1. Add a new domain (“Domains” → “add domain”)
2. For “Locality”, deselect “inherit” and set “Locality” to “Internal” (see figure 12)
3. Apply settings

## 5.9 Configure internal mail server

To allow the CipherMail gateway to encrypt outgoing email, all outgoing email should be handled by the CipherMail gateway. The internal mail server should therefore be configured to relay via the CipherMail gateway.

Because every mail server is configured differently, we refer you to the documentation of the internal mail server on how to configure the mail server to relay via an external server. For a brief overview on how to configure Exchange 2010, see appendix B.

**Action**

Configure the internal mail server to relay email via the CipherMail gateway.

## 5.10 Test incoming email

It should be tested whether the CipherMail gateway can deliver email to the internal mail server. To test this, email should be sent to a valid recipient. The best way to test this is by sending an email with an email client configured to

connect to the CipherMail gateway on the SMTP port (25). Alternatively, telnet can be used to “simulate” and email client by directly connecting to port 25 of the CipherMail gateway (see appendix C) for more information on how to send an email using telnet.

**Action**

Send a test email to a valid internal recipient with a mail client directly connected to the CipherMail gateway or using telnet and check whether it was delivered.

### 5.11 Configure the relay server

The relay server should be configured to relay all incoming email for the relay domains to the CipherMail gateway. Because every mail server is configured differently, we refer you to the documentation of the relay server server on how to configure the relay server.

**Action**

Configure the relay server to relay incoming email for the relay domains via the CipherMail gateway.

### 5.12 Final test

Now the complete mail flow has been setup, incoming and outgoing mail should be tested.

**Action**

Test outgoing email by sending a message from an internal mail client to an external recipient.

**Action**

Test incoming email by sending a message from an external email account to an internal recipient.

## 6 With virus scanner setup

In this setup (figure 3), the CipherMail gateway is placed between the centralized email virus scanner and the Internet. The internal mail server sends email for external recipients to the virus scanner, the virus scanner forwards the email

to the CipherMail gateway and the CipherMail gateway directly delivers email to the external recipients via MX lookups.

The following steps will be described:

1. Configure relay domains.
2. Configure MTA hostname.
3. Configure CipherMail to deliver email for the relay domains to the virus scanner.
4. Configure CipherMail to directly deliver email for external recipients.
5. Enable “Reject unverified recipient”.
6. Allow virus scanner to relay to external recipients.
7. Apply new MTA settings.
8. Add internal domains.
9. Configure the virus scanner to relay email for external recipients via the CipherMail gateway.
10. Test outgoing email.
11. Test incoming email.
12. Configure firewall (or MX records) to deliver incoming email to CipherMail gateway.
13. Final test.

## 6.1 **Configure relay domains**

The relay domains are the domains of the gateway for which the internal mail server handles email. The relay domains should match all the domains of the internal mail server. To relay domains can be configured on the MTA settings page (see figure 10).

### Action

For each domain, fill-in the “Add domain” field and press the “Add” button

## 6.2 Configure MTA hostname

The MTA hostname can be configured by setting the “My hostname” field (see figure 10). It is advised that the MTA hostname be set to the fully qualified domain name of the external IP address and that the reverse lookup of the external IP address (i.e., PTR record) is equal to the MTA hostname. If for whatever reason the MTA hostname cannot be set to the fully qualified domain name of the external IP address, or the reverse lookup does not match the MTA hostname, the “SMTP helo name” should be manually set to the reverse lookup of the external IP address (see appendix A for more information about HELO/EHLO name).

**Note:** The MTA hostname should be different from the name of the virus scanner and the external relay server. If the MTA (Postfix) detects that the hostname of the server it connects to is the same as its own hostname, the email will be bounced and the following message will appear in the MTA log:

```
status=bounced (mail for [x.x.x.x] loops back to myself).
```

This check was added to prevent mail loops.

### Action

Set hostname to fully qualified domain name.

## 6.3 Configure internal relay host

After email has been handled by the gateway, email sent to any of the relay domains should be forwarded to the virus scanner.

### Action

Set “Internal relay host” to the hostname or IP address of the virus scanner. For most setups, port should be set to 25 and “mx” should not be selected.

## 6.4 Configure external relay host

With the “virus scanner setup”, email sent to external recipients will be delivered directly to the mail servers of the recipients using MX records. By leaving “External relay host” empty, CipherMail will deliver email to external recipients using MX records.

### Action

Set “External relay host” to an empty (i.e., blank) value.



## 6.5 Enable “Reject unverified recipient”

A mail server should know which recipients are valid recipients for a relay domain before accepting the message (i.e., the mail server should know whether there is a valid inbox for the recipient). If an email is accepted for relay but the next server (i.e., the internal mail server) does not accept the message because the recipient is not valid, the email should be bounced by the receiving server. Bouncing an email after accepting the message is called “backscatter”. Systems that generate email backscatter can end up being listed on a mail blacklist (RBL).

By enabling “Reject unverified recipient” the gateway “learns” which recipient addresses are valid or not by querying the server it relays to. When an email is received for an unknown recipient, the server “asks” the server it relays to whether the recipient is a valid recipient or not. The message is only accepted when the next email server reports that the recipient is a valid. The result of this verification process is cached.

The “reject code” is the SMTP result code used when the email is not accepted. This should initially be set to “450” (which tells the connecting SMTP server that the message is not accepted because of a temporary error). It should be changed to “550” (permanent error) when the verification procedure works correctly. See the Postfix documentation for more information on address verification<sup>3</sup>.

### Action

Select “Reject unverified recipient”

## 6.6 Configure “My Networks”

To encrypt outgoing email, the virus scanner should send all outgoing email via the CipherMail gateway. The virus scanner should therefore be allowed to send email to all external recipient via the CipherMail gateway.

### Action

Add the IP address of the virus scanner to “My Networks”.

## 6.7 Apply new MTA settings

Now all the required MTA configuration changes are done, the new MTA settings should be applied.

### Action

Click “Apply” on the MTA config page to apply the new MTA settings.

<sup>3</sup>See [http://www.postfix.org/ADDRESS\\_VERIFICATION\\_README.html](http://www.postfix.org/ADDRESS_VERIFICATION_README.html)

## 6.8 Add internal domains

The CipherMail gateway needs to encrypt email for external recipients and decrypt email for internal recipients. The gateway therefore has to know which recipients are internal and which recipients are external. The user property “Locality” determines whether a recipient is internal or external. In most setups, all domains from the “relay domains” should be internal because the gateway is configured to handle incoming email for this domains.

### Action

For every domain configured as a “relay domain” take the following steps:

1. Add a new domain (“Domains” → “add domain”)
2. For “Locality”, deselect “inherit” and set “Locality” to “Internal” (see figure 12)
3. Apply settings

## 6.9 Configure virus scanner

To allow the CipherMail gateway to encrypt outgoing email, all outgoing email should be handled by the CipherMail gateway. The virus scanner should therefore be configured to relay via the CipherMail gateway.

Because every mail server is configured differently, we refer you to the documentation of the virus scanner on how to configure the mail server to relay via an external server.

### Action

Configure the virus scanner to relay email via the CipherMail gateway.

## 6.10 Test outgoing email

To test whether the CipherMail gateway can send email to external recipients, use the built-in “Send email” tool (Admin → other → send email). This test tool will directly send an email from the CipherMail gateway to the external recipients.

### Action

Send a test email to an external recipient using the “Send email” tool.

To test whether the virus scanner mail server can send email to external recipients via the CipherMail gateway, send an email from a mail client connected to the internal mail server and check the MTA logs of CipherMail to see whether the email is actually relayed via the CipherMail gateway.

**Action**

Send a test email to an external recipient with a mail client and check the MTA logs of CipherMail whether it was relayed via CipherMail.

### 6.11 Test incoming email

It should be tested whether the CipherMail gateway can deliver email to the virus scanner. To test this, email should be sent to a valid recipient. The best way to test this is by sending an email with an email client configured to connect to the CipherMail gateway on the SMTP port (25). Alternatively, telnet can be used to “simulate” and email client by directly connecting to port 25 of the CipherMail gateway (see appendix C) for more information on how to send an email using telnet.

**Action**

Send a test email to a valid internal recipient with a mail client directly connected to the CipherMail gateway or using telnet and check whether it was delivered.

### 6.12 Configure firewall (or MX records)

The complete mail flow has been configured. However mail sent by external senders is still delivered to the virus scanner and not to the CipherMail gateway. The best way to make sure that incoming email is delivered to the CipherMail gateway and not to the virus scanner is by changing NAT rules on the firewall (i.e., tell the firewall to translate the external IP address to the internal IP address of the CipherMail gateway on port 25). Alternatively if the firewall does not support this, the external DNS MX records can be modified to point to the CipherMail gateway.

**Note:** Changing DNS records might take some time before all DNS servers are updated. It’s therefore advised to first try to use a firewall rule to redirect mail to the CipherMail gateway.

**Action**

Set a firewall rule to redirect incoming external mail to the CipherMail gateway.

### 6.13 Final test

Now the complete mail flow has been setup, incoming and outgoing mail should be tested.

#### Action

Test outgoing email by sending a message from an internal mail client to an external recipient.

#### Action

Test incoming email by sending a message from an external email account to an internal recipient.

## 7 With virus scanner via relay setup

In this setup (figure 4), the CipherMail gateway is placed between the centralized email virus scanner and an SMTP relay server (also known as “front-end server”). The internal mail server sends email for external recipients to the virus scanner, the virus scanner forwards the email to the CipherMail gateway and the CipherMail gateway forwards the email for external recipients to the SMTP relay server.

The following steps will be described:

1. Configure relay domains.
2. Configure MTA hostname.
3. Configure CipherMail to deliver email for the relay domains to the virus scanner.
4. Configure CipherMail to deliver email for external recipients to the relay server.
5. Enable “Reject unverified recipient”.
6. Allow virus scanner to relay to external recipients.
7. Apply new MTA settings.
8. Add internal domains.
9. Configure the virus scanner to relay email for external recipients via the CipherMail gateway.
10. Test incoming email.
11. Configure the relay mail server to deliver email for internal recipients to the CipherMail gateway.
12. Final test.

## 7.1 Configure relay domains

The relay domains are the domains of the gateway for which the internal mail server handles email. The relay domains should match all the domains of the internal mail server. To relay domains can be configured on the MTA settings page (see figure 10).

### Action

For each domain, fill-in the “Add domain” field and press the “Add” button

## 7.2 Configure MTA hostname

The MTA hostname can be configured by setting the “My hostname” field (see figure 10).

**Note:** The MTA hostame should be different from the name of the virus scanner and the external relay server. If the MTA (Postfix) detects that the hostname of the server it connects to is the same as it’s own hostname, the email will be bounced and a the following message will appear in the MTA log:

```
status=bounced (mail for [x.x.x.x] loops back to myself).
```

This check was added to prevent mail loops.

### Action

Set hostname.

## 7.3 Configure internal relay host

After email has been handled by the gateway, email sent to any of the relay domains should be forwarded to the virus scanner.

### Action

Set “Internal relay host” to the hostname or IP address of the virus scanner. For most setups, port should be set to 25 and “mx” should not be selected.

## 7.4 Configure external relay host

With the “virus scanner via relay setup”, email sent to external recipients will be relayed via the relay server. The CipherMail gateway therefore has to be configured to relay email for external recipient via the relay server.

### Action

Set “External relay host” to the hostname or IP address of the relay server. For most setups, port should be set to 25 and “mx” should not be selected.

**Note:** If the relay server requires username/password authentication, add the credentials for the relay to the SASL settings (see MTA → sasl).

## 7.5 Enable “Reject unverified recipient”

A mail server should know which recipients are valid recipients for a relay domain before accepting the message (i.e., the mail server should know whether there is a valid inbox for the recipient). If an email is accepted for relay but the next server (i.e., the internal mail server) does not accept the message because the recipient is not valid, the email should be bounced by the receiving server. Bouncing an email after accepting the message is called “backscatter”. Systems that generate email backscatter can end up being listed on a mail blacklist (RBL).

By enabling “Reject unverified recipient” the gateway “learns” which recipient addresses are valid or not by querying the server it relays to. When an email is received for an unknown recipient, the server “asks” the server it relays to whether the recipient is a valid recipient or not. The message is only accepted when the next email server reports that the recipient is a valid. The result of this verification process is cached.

The “reject code” is the SMTP result code used when the email is not accepted. This should initially be set to “450” (which tells the connecting SMTP server that the message is not accepted because of a temporary error). It should be changed to “550” (permanent error) when the verification procedure works correctly. See the Postfix documentation for more information on address verification<sup>4</sup>.

**Note:** If the relay server already knows which recipients are valid recipients or not, for example using LDAP, there is not need to enable “Reject unverified recipient”.

### Action

Select “Reject unverified recipient”

<sup>4</sup>See [http://www.postfix.org/ADDRESS\\_VERIFICATION\\_README.html](http://www.postfix.org/ADDRESS_VERIFICATION_README.html)

## 7.6 Configure “My Networks”

To encrypt outgoing email, the virus scanner should send all outgoing email via the CipherMail gateway. The virus scanner should therefore be allowed to send email to all external recipient via the CipherMail gateway.

### Action

Add the IP address of the virus scanner to “My Networks”.

## 7.7 Apply new MTA settings

Now all the required MTA configuration changes are done, the new MTA settings should be applied.

### Action

Click “Apply” on the MTA config page to apply the new MTA settings.

## 7.8 Add internal domains

The CipherMail gateway needs to encrypt email for external recipients and decrypt email for internal recipients. The gateway therefore has to know which recipients are internal and which recipients are external. The user property “Locality” determines whether a recipient is internal or external. In most setups, all domains from the “relay domains” should be internal because the gateway is configured to handle incoming email for this domains.

### Action

For every domain configured as a “relay domain” take the following steps:

1. Add a new domain (“Domains” → “add domain”)
2. For “Locality”, deselect “inherit” and set “Locality” to “Internal” (see figure 12)
3. Apply settings

## 7.9 Configure virus scanner

To allow the CipherMail gateway to encrypt outgoing email, all outgoing email should be handled by the CipherMail gateway. The virus scanner should therefore be configured to relay via the CipherMail gateway.

## 7.10 Test incoming email 7 WITH VIRUS SCANNER VIA RELAY SETUP

Because every mail server is configured differently, we refer you to the documentation of the virus scanner on how to configure the mail server to relay via an external server.

### Action

Configure the virus scanner to relay email via the CipherMail gateway.

## 7.10 Test incoming email

It should be tested whether the CipherMail gateway can deliver email to the virus scanner. To test this, email should be sent to a valid recipient. The best way to test this is by sending an email with an email client configured to connect to the CipherMail gateway on the SMTP port (25). Alternatively, telnet can be used to “simulate” and email client by directly connecting to port 25 of the CipherMail gateway (see appendix C) for more information on how to send an email using telnet.

### Action

Send a test email to a valid internal recipient with a mail client directly connected to the CipherMail gateway or using telnet and check whether it was delivered.

## 7.11 Configure the relay server

The relay server should be configured to relay all incoming email for the relay domains to the CipherMail gateway. Because every mail server is configured differently, we refer you to the documentation of the relay server server on how to configure the relay server.

### Action

Configure the relay server to relay incoming email for the relay domains via the CipherMail gateway.

## 7.12 Final test

Now the complete mail flow has been setup, incoming and outgoing mail should be tested.

### Action

Test outgoing email by sending a message from an internal mail client to an external recipient.



Action

Test incoming email by sending a message from an external email account to an internal recipient.

## A SMTP HELO/EHLO name

The SMTP HELO/EHLO name is the name the SMTP server identifies itself with when connecting to another SMTP server. Some email servers check whether the HELO/EHLO name is equal to the reverse lookup of the IP address (i.e., querying the PTR record). If the reverse IP lookup and HELO/EHLO name do not match, some mail servers might flag the mail as spam.

If the CipherMail gateway is used to directly send email to external recipients (i.e., outgoing email is not relayed through an external relay host) the gateway should be setup with the correct HELO/EHLO. The SMTP helo name should be equal to the reverse lookup of the external IP address.

If the SMTP hostname of the Ciphermail gateway is set to the external hostname and the reverse IP lookup matches the hostname, the SMTP helo name can be left empty because the SMTP helo name defaults to the hostname.

**Checking the HELO/EHLO name** whether the HELO/EHLO name is correctly setup can be checked using the helo check services from <http://cbl.abuseat.org/helocheck.html> by sending an email to "helocheck@cbl.abuseat.org". The email will be immediately bounced. The bounce message contains the HELO name used by the gateway.

```
<helocheck@cbl.abuseat.org>: host mail-in.cbl.abuseat.org said:
  550 HELO for IP 82.94.189.170 was "secure.djigzo.com"
  (in reply to RCPT TO command)
```

Where 82.94.189.170 is the external IP address of the gateway (IP address will be different for every server) and "secure.djigzo.com" was the HELO name used by the gateway.

## B Exchange 2010 send connector

To configure Exchange 2010 to direct all outbound email via an external SMTP server, an "SMTP connector" should be added.

To create the SMTP Connector, follow the steps below:

1. In the Exchange Admin Console select "Microsoft Exchange" → "Organization Configuration" → "Hub Transport"
2. Right click and select "New Send Connector" or on the right hand side in "Actions" select "New Send Connector"
3. In the Name field, type a meaningful name for this connector
4. In the Select the intended use for this connector field, select "Custom"
5. On the Address space page click the "Add" button and select "SMTP Address Space"
6. Set address space to "Address =\*" and cost to 1 and click Next

7. On the Network settings page, select “Route mail through the following smart host” and then click the Add button
8. Specify the IP address or the Fully qualified domain name of the Cipher-Mail gateway. Click Next.
9. On the Configure smart host authentication settings page, leave the smart host authentication setting as None and click Next
10. Add the Source Sever and click Next
11. The New Send Connector page, check that everything is correct and then click New
12. On the Completion page, check that the wizard completed successfully, and then click Finish to close the wizard

For more information on managing connectors see <https://technet.microsoft.com/en-us/library/bb125128%28v=exchg.141%29.aspx>

## C Simulate a mail client using telnet

By directly connecting to port 25 of the CipherMail gateway with telnet, a mail client can be simulated. This can be used for example to directly send a test email. To send a test email, use the following steps:

### connect with telnet

```
$ telnet 192.168.88.196 25

Trying 192.168.88.196...
Connected to 192.168.88.196.
Escape character is '^]'.
220 ciphermail.example.com ESMTP CipherMail
```

**Note:** Replace 192.168.88.196 with the IP address of the CipherMail gateway.

Issue the EHLO command:

```
ehlo test.example.com
```

The SMTP server should respond with all the supported enhanced SMTP commands:

```
250-ciphermail.example.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-STARTTLS
250-ENHANCEDSTATUSCODES
250 8BITMIME
```

Issue the MAIL command:

```
mail from:<test@example.com>
```

The SMTP server should respond with Ok:

```
250 2.1.0 Ok
```

Specify the recipient(s) (repeat for multiple recipients):

```
rcpt to:<test@ciphermail.com>
```

The SMTP server should respond with Ok:

```
250 2.1.5 Ok
```

Or with an error if the recipient is not allowed:

```
454 4.7.1 <test@ciphermail.com>: Relay access denied
```

A “Relay access denied” error is issued if the recipient is not in a relay domain or, if the IP address of the machine from which the telnet command is issued is not added to “My Networks”.

Issue the DATA command:

```
data
```

The SMTP server should respond with:

```
354 End data with <CR><LF>.<CR><LF>
```

Type the mail content (including headers) and end with “.”:

```
Subject: test
```

```
test
```

```
.
```

The SMTP server should respond with:

```
250 2.0.0 Ok: queued as ***
```

Issue the QUIT command:

```
quit
```