CIPHERMAIL EMAIL ENCRYPTION

CipherMail Webmail Messenger Quick Setup Guide

October 26, 2017, Rev: 9537

Contents

1 Introduction

This guide briefly explains how to configure the CipherMail gateway and webmail messenger appliance to support sending secure webmail messages. 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 is already installed and configured for sending and receiving email. See the quick setup guide on how to setup the gateway for sending and receiving email.

CipherMail Webmail messenger is a secure pull delivery webmail add-on to the CipherMail encryption gateway. If the rules of the CipherMail encryption gateway determine that a message must be encrypted, and S/MIME, PGP or PDF cannot be used, the email will be sent to the CipherMail Webmail box via an S/MIME secured tunnel. The recipient gets a notification that a new message is available. The first time the user receives a message, the user needs to select a secure password. The user can read and reply to the message using any web browser.

The following steps are taken when sending an email to a recipient via webmail messenger (see figure 1):

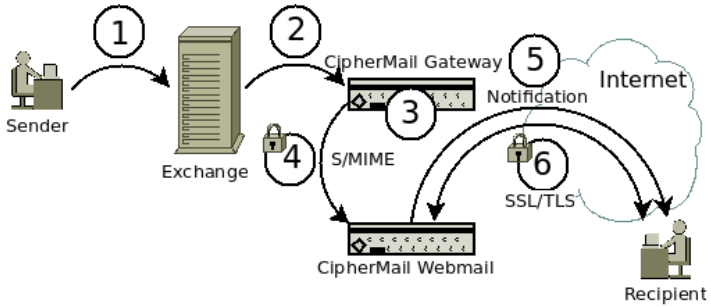

Figure 1: Webmail mail flow

1. User sends email via Exchange (or some other mail server)
2. Exchange forwards the message to the CipherMail gateway.
3. A rule on the CipherMail gateway flags that the email must be sent to webmail.
4. The message gets S/MIME signed with the webmail sender key and encrypted with the webmail recipient certificate and forwarded via email to the webmail appliance. The webmail appliance decrypts the mail, checks the signature and places the email in the mailbox of the recipient(s).

5. A notification message is sent to the recipient that a message is available for pick-up.
6. The user logs-in with a browser via HTTPS and reads the message.

To setup the CipherMail webmail messenger appliance, the gateway has to be configured to forward email to the webmail appliance via an S/MIME protected tunnel. This requires a special webmail sender certificate on the CipherMail gateway and a webmail recipient certificate on the webmail appliance. The rest of this guide will explain how to configure forwarding to the webmail appliance and how to setup the S/MIME tunnel between the CipherMail gateway and webmail appliance.

2 Webmail setup part 1

2.1 Login to admin GUI

The administration GUI can be accessed by opening the following URL in a browser: `https://192.168.1.139:8443` (change the IP address to to match the address of the webmail box).

Use the following default credentials:

username: admin
password: admin

Note: it can take some time to login after a restart because the web application must be initialized upon first login.

2.2 Network config

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

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 2).

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.

2.2.1 IP address

The available network interfaces can be configured by clicking “interfaces”. This opens the interfaces page (see figure 3). A network interface can be configured by clicking the “gear” icon of the interface. The network interface can be

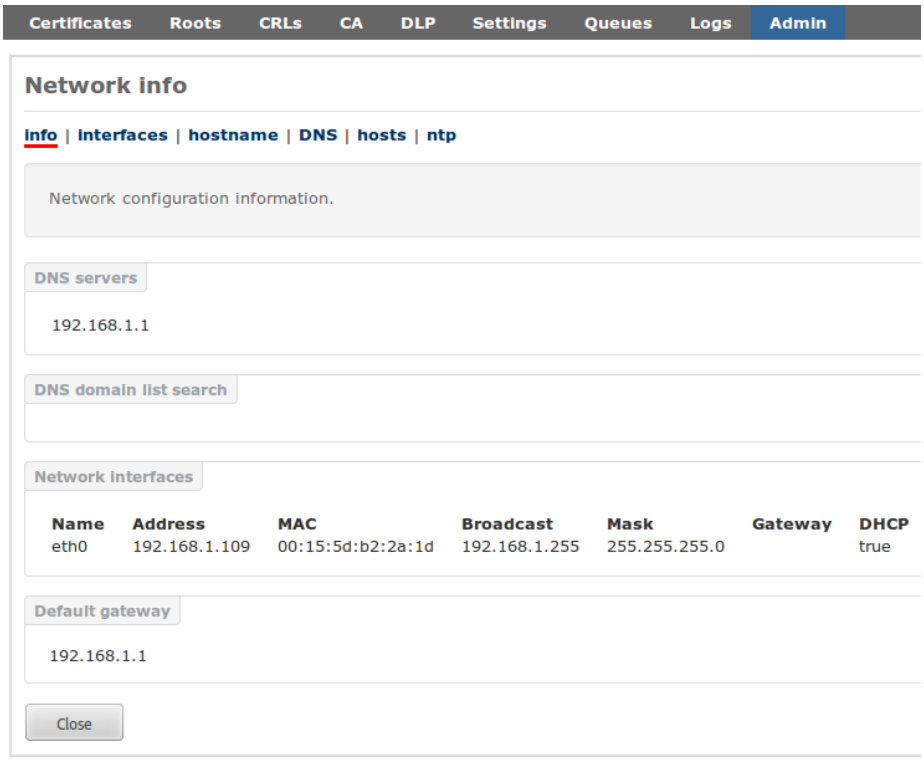

Figure 2: Network info

configured for a dynamic IP address (DHCP) or for a static IP address (see figure 4

Action

Set the IP address of the webmail appliance.

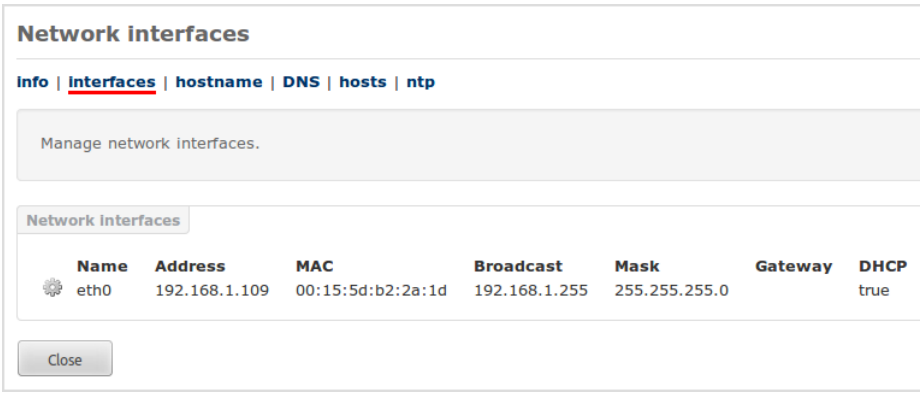

Figure 3: Network interfaces

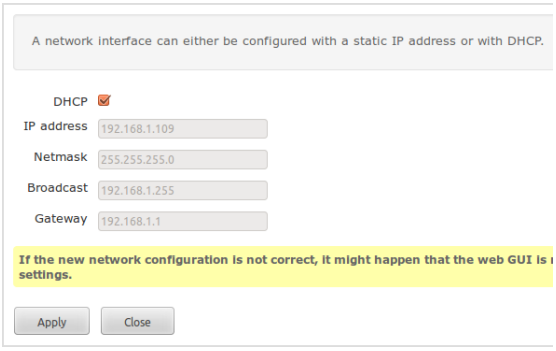

Figure 4: Network interface

2.2.2 Hostname

With the hostname page, the hostname of the gateway can set (see figure 5. The hostname is used by many of the networking programs to identify the machine.

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

Action

Set the hostname of the webmail appliance to the fully qualified hostname.

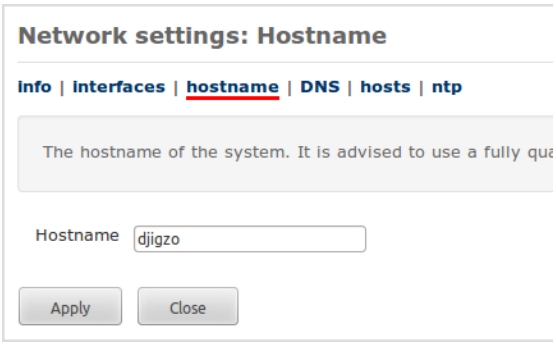

Figure 5: Hostname

2.2.3 DNS

The gateway requires at least one DNS server. The DNS server can be configured with the DNS page (see figure 6)

Action

Configure at least one DNS server entry.

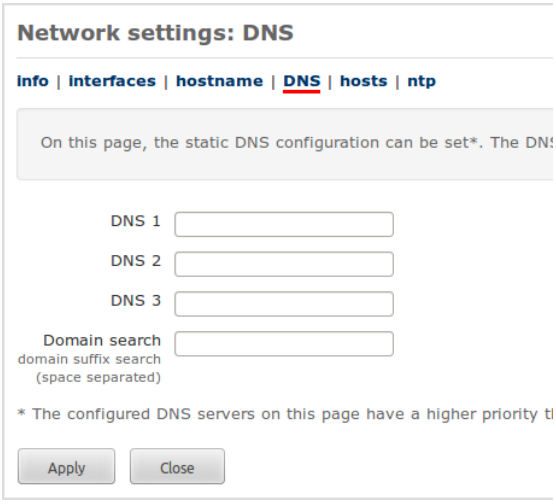

Figure 6: DNS

2.3 Setup

This section explains what changes need to be applied to the default configuration of the webmail appliance.

The following steps will be described:

1. Configure relay domain.
2. Configure MTA hostname.
3. Configure internal relay host.
4. Apply new MTA settings.
5. Test outgoing email.
6. Configure “Relay recipient”.
7. Configure “Portal base URL”.
8. Configure “Notification sender”.
9. Configure “Postmaster”.
10. Apply settings.
11. Create a webmail tunnel certificate.

12. Export webmail tunnel certificate.
13. Configure “Auto mailbox cleanup”.
14. Configure “Authorized recipients”.
15. Finish.

2.3.1 Configure relay domain

Because the webmail appliance will only directly receive email from the CipherMail gateway, we will configure a local private domain for communication between the gateway and webmail. The relay domains can be configured on the MTA settings page (Admin → MTA → config, see figure 7).

Action

Open MTA config page (Admin → MTA → config) and set the field “Add domain” to **webmail.local** and press the “Add” button.

2.3.2 Configure MTA hostname

The MTA hostname can be configured by setting the “My hostname” field (see figure 7). 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

On MTA config page, set hostname to fully qualified domain name.

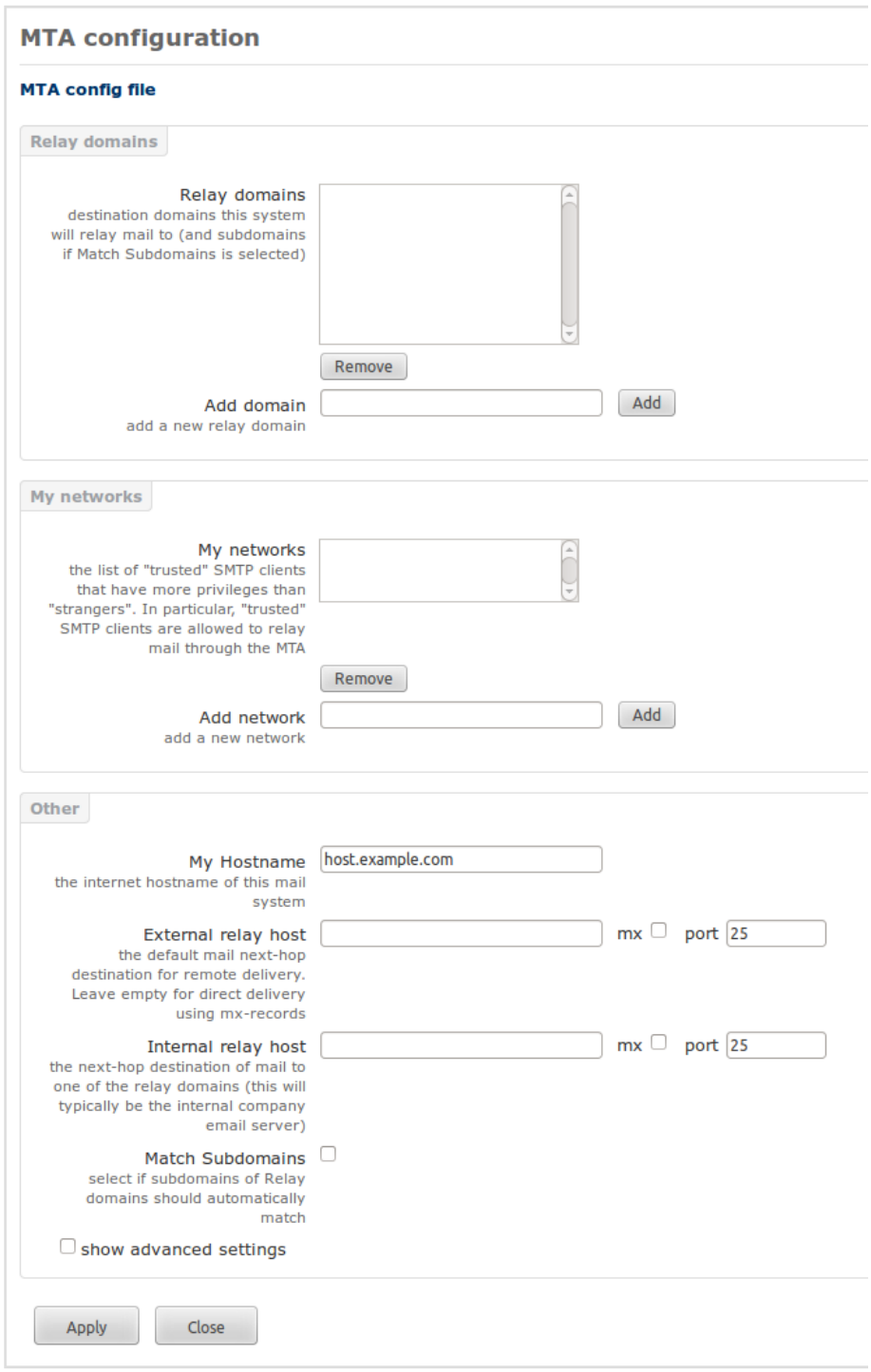

Figure 7: MTA config

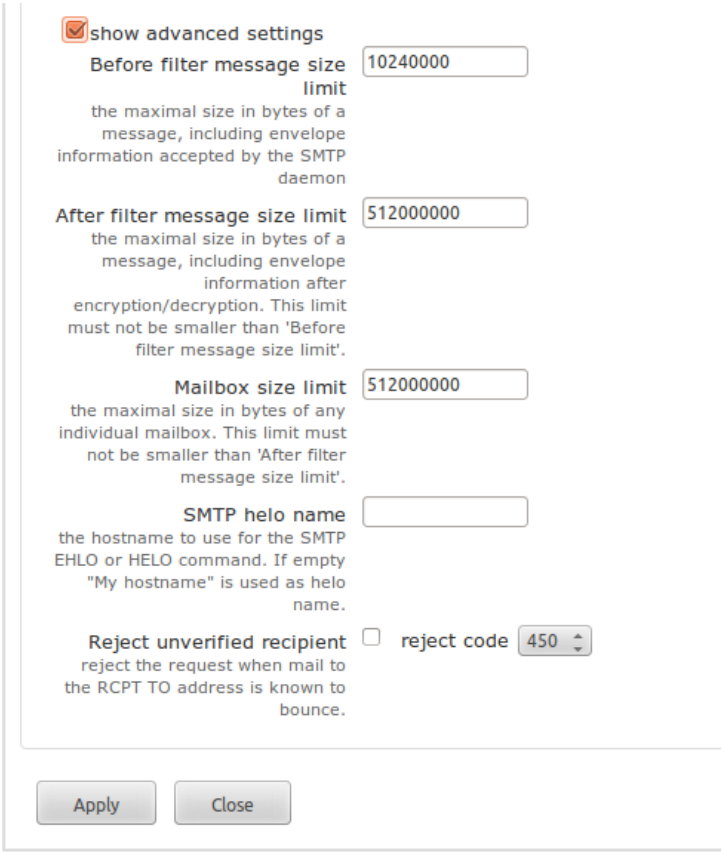

Figure 8: MTA advanced config

2.3.3 Configure internal relay host

Because we will use a local private non-routable domain for webmail (**webmail.local**) we need to set “Internal relay host” to point to localhost on an unused port. This is done to prevent bounces for tunnel messages which are not recognized as valid tunnel messages.

Action

On MTA config page, set “Internal relay host” to **127.0.0.1** and port **26**.

2.3.4 Apply new MTA settings

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

Action

On MTA config page, click “Apply” to apply the new MTA settings.

2.3.5 Test outgoing email

To test whether the webmail appliance 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 (Admin → other → send email)

2.3.6 Configure “Relay recipient”

The “Relay recipient” is the special recipient email address for the tunnel messages sent by the CipherMail gateway to the webmail appliance (see step 4 of figure 1. The “Relay recipient” should be configured on the global settings page (see figure 9).

Action

On global settings page, set “Relay recipient” to **webmail@webmail.local**

2.3.7 Configure “Portal base URL”

The base URL for the user sign-up and password reset pages. This should normally be set to the fully qualified domain name (or external IP address) of the server. Example: **https://webmail.ciphermail.com**.

Action

On global settings page, set “Portal base URL” to to the fully qualified domain name (or external IP address) of the server.

2.3.8 Configure “Notification sender”

The from address used for notification messages (sign-up and email notification messages). This should be a valid email address. It’s advised to use an email address which is monitored by an administrator.

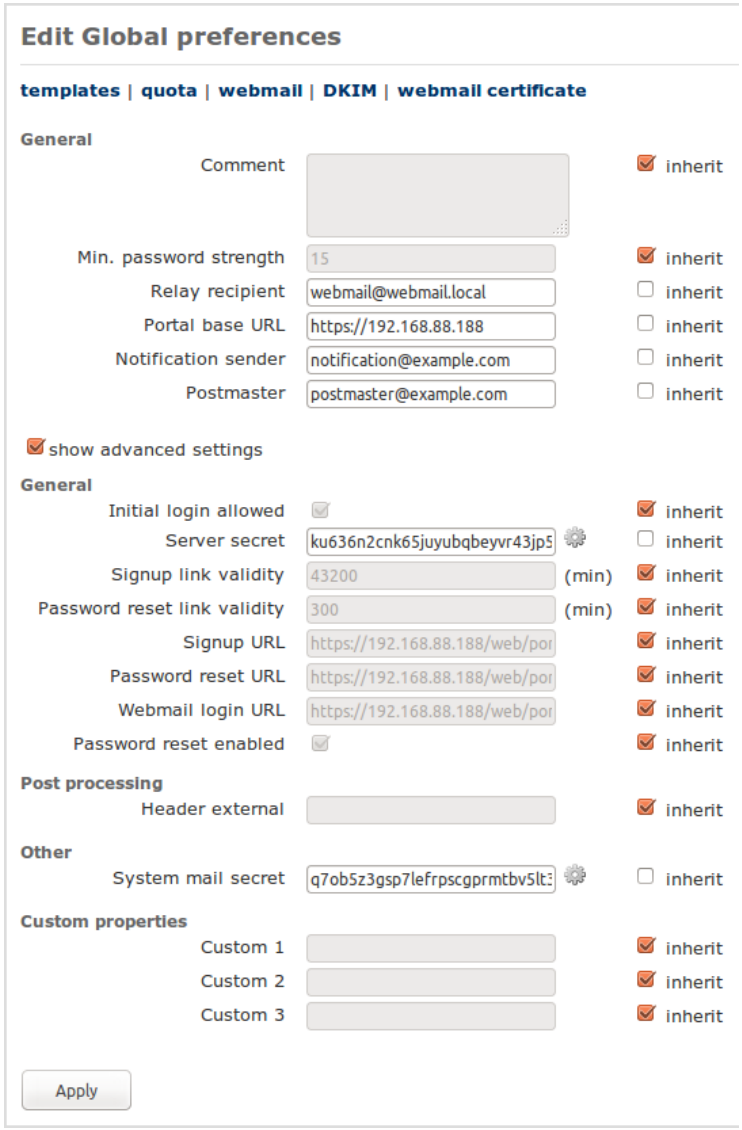

Figure 9: Webmail global settings

Action

On global settings page, set “Notification sender” to a valid email address.

2.3.9 Configure “Postmaster”

If there is some error with the S/MIME tunnelled message, for example the message was signed with an untrusted certificate, the email will be forwarded to the “Postmaster”. This should be a valid email address. It’s advised to use

an email address which is monitored by an administrator.

Action

On global settings page, set “Postmaster” to a valid email address.

2.3.10 Apply settings

Now all required global changes are done, the new settings must be applied.

Action

On global settings page, click “Apply”.

2.3.11 Create a webmail tunnel certificate

The special message sent from the CipherMail gateway to the webmail appliance (step 4 in figure 1) is signed and encrypted with S/MIME. The webmail appliance therefore requires a certificate with an associated private key.

A webmail tunnel certificate can be created with the “Create webmail relay recipient certificate” page which can be opened by clicking the “webmail certificate” link on the “Edit Global preferences page” (see figure 9). This will open the page on which the certificate and key can be created (see figure 10).

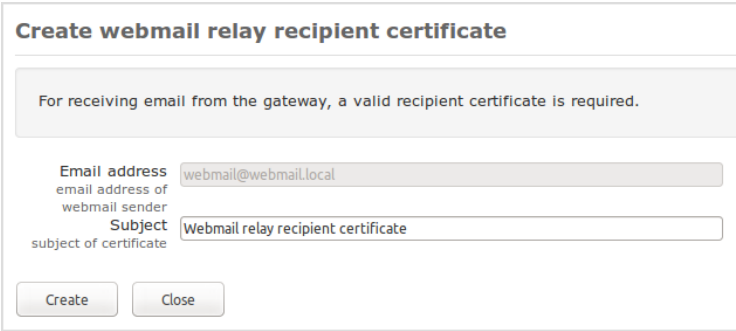

Figure 10: Create tunnel certificate

Action

On global settings page, click the “webmail certificate” link. On the “Create webmail relay recipient certificate” page, click the “Create” button.

2.3.12 Export webmail tunnel certificate

Because the CipherMail gateway need to encrypt the special tunnel message with the webmail tunnel certificate, the webmail tunnel certificate must be available on the CipherMail gateway. The webmail tunnel certificate must therefore be exported to a file so it can later be imported into the CipherMail gateway. The webmail tunnel certificate can be exported from the certificates page (Admin → PKI → certificates) by selecting the certificate and clicking "download certificates" (see figure 11). Save the the certificate to disk. The certificate is required when configuring the CipherMail gateway.

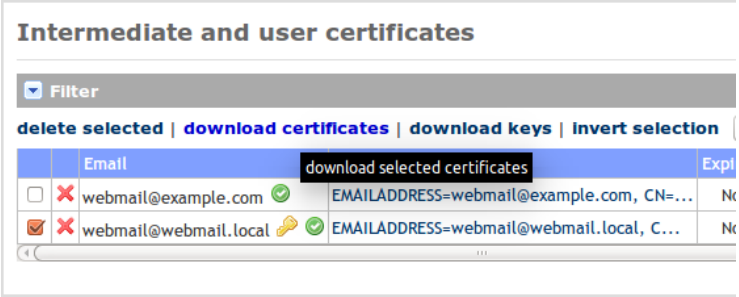

Figure 11: Export certificate

Action

Open the certificates pages (Admin → PKI → certificates), select the webmail certificate and click "download certificates". Save the certificate to disk.

2.3.13 Configure "Auto mailbox cleanup"

The webmail appliance can be configured to automatically delete emails older than a configured number of days. This makes managing the gateway easier because it's less likely to run out of disk space if emails are not kept indefinitely. Removing old email is also advised for security reasons because emails which are deleted cannot be leaked.

The "Auto mailbox cleanup" functionality can be enabled by opening the "Auto cleanup settings" page (Settings → auto cleanup). To enable auto cleanup, select the checkbox "Auto cleanup enabled" and set the cleanup interval (see figure 12).

Action

On the auto cleanup settings page (Settings → auto cleanup), select the checkbox "Auto cleanup enabled", set the cleanup interval and apply settings.

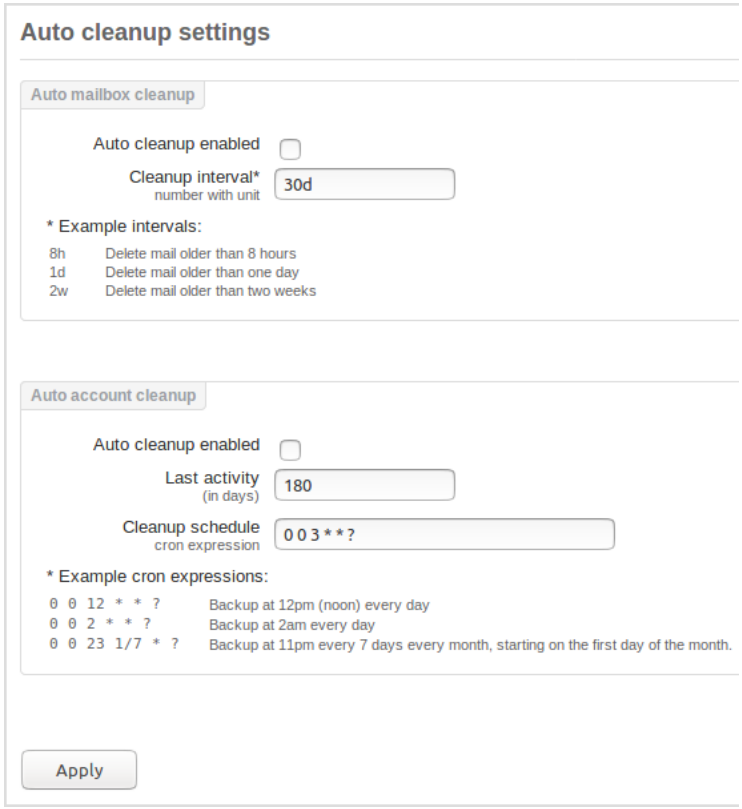

Figure 12: Auto cleanup

2.3.14 Configure “Authorized recipients”

Recipients of a webmail messenger message are only allowed to send messages to the list of “Authorized recipients”. The “Authorized recipients” list can contain domains or individual email addresses. Typically the authorized recipients are set to all the domains handled by the gateway. By default the authorized recipients list is empty which mean that a webmail recipient cannot reply to an email. The authorized recipients can be set on the “Authorized recipients” page (Admin → MTA → authorized recipients).

Action

Open the authorized recipients page (Admin → MTA → authorized recipients) and add all the gateway relay domains to the list of “Authorized recipients”.

2.3.15 Finish

The webmail appliance configuration is now almost done. The only thing that is missing is the import of the gateway certificate. However, before the gateway

certificate can be imported, it must be created first. The next part will outline the required steps to configure the CipherMail gateway for webmail.

3 CipherMail gateway setup

The next part will explain how to configure the CipherMail gateway for webmail.

Note: This part assumes that the gateway is already installed and configured for sending and receiving email. See the quick setup guide on how to setup the gateway for sending and receiving email.

The following steps will be described:

1. Login to admin GUI.
2. Import webmail tunnel certificate.
3. Trust webmail tunnel certificate.
4. Enable webmail.
5. Configure webmail recipient.
6. Configure webmail sender.
7. Apply webmail settings.
8. Create gateway tunnel certificate.
9. Export gateway tunnel certificate.
10. Add SMTP transport.
11. Finish.

3.1 Login to admin GUI

Action

Login to the WEB GUI of the CipherMail gateway with the configured credentials.

3.2 Import webmail tunnel certificate

Email sent to the webmail appliance must be encrypted with the webmail tunnel certificate. The webmail certificate which was exported in step 2.3.12 should therefore be imported into the certificates store of the CipherMail gateway. The certificate can be imported from the certificates store by clicking “Import certificates” on the left-hand side menu. Because the webmail tunnel certificate is a self-signed certificate, “skip self-signed” should not be selected.

Action

Import the webmail tunnel certificate (Certificates → Import certificates) from step 2.3.12 into the certificates store of the CipherMail gateway (**uncheck “skip self-signed” on import page)**

3.3 Trust webmail tunnel certificate

The imported webmail tunnel certificate is a self-signed certificate. It should therefore be trusted by placing it on the certificate trust list (CTL) white-list.

The imported webmail tunnel certificate can be placed on the CTL white-list with the following steps:

1. Open the certificate details page of the imported webmail tunnel certificate.
2. On the certificate details page click “Add to CTL” (see figure 13).
3. On the “Add new Certificate Trust List entry” page, select “Whitelisted” and click “Add”.

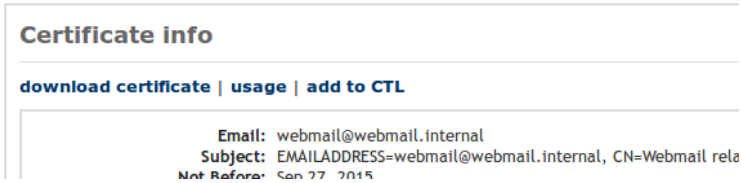

Figure 13: Add to CTL

Action

Add the imported webmail tunnel certificate to the CTL white-list.

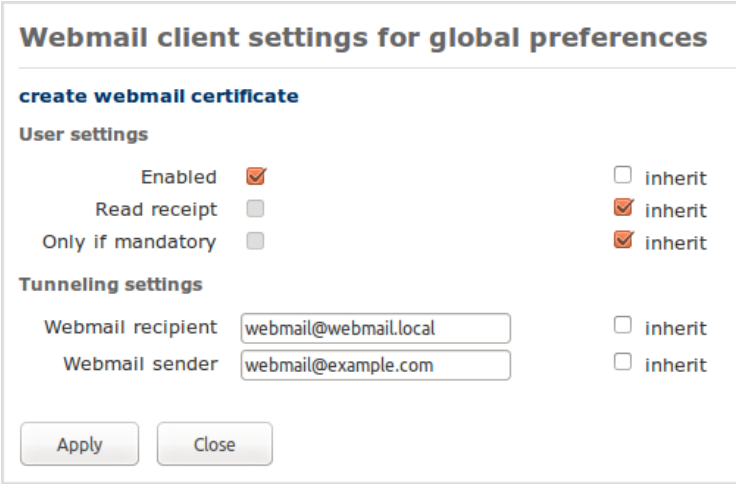

Figure 14: Gateway webmail settings

3.4 Enable webmail

Webmail is not enabled by default and should therefore be enabled. To enable webmail, open the global webmail settings and select the “enabled” checkbox (see figure 14).

Action

Open the global webmail settings (Settings → webmail) and select the “enabled” checkbox.

3.5 Configure webmail recipient

The webmail recipient is the email address on which the webmail appliance listens for incoming mail from the gateway. The webmail recipient should be set to the email address configured for “Relay recipient” in section 2.3.6.

Action

Set “Webmail recipient” to **webmail@webmail.local**.

3.6 Configure webmail sender

The special tunnel message sent from the gateway to the webmail appliance will be sent by the “webmail sender” address. It’s advised to use an email address which is exclusively used for webmail and that there is a valid mailbox for this email address.

Action

Set “Webmail sender” to a valid email address.

3.7 Apply webmail settings

After changing the webmail settings, the new settings must be applied.

Action

Apply new webmail settings

3.8 Create gateway tunnel certificate

The special tunnel message sent from the gateway to the webmail appliance must be S/MIME digitally signed (step 4 in figure 1). A certificate with associated private key must therefore be available on the gateway for the “webmail sender” address. A gateway tunnel certificate can be created with the “Create webmail tunnel certificate” page (see figure 15) which can be opend by clicking “create webmail certificate” on the webmail settings page.

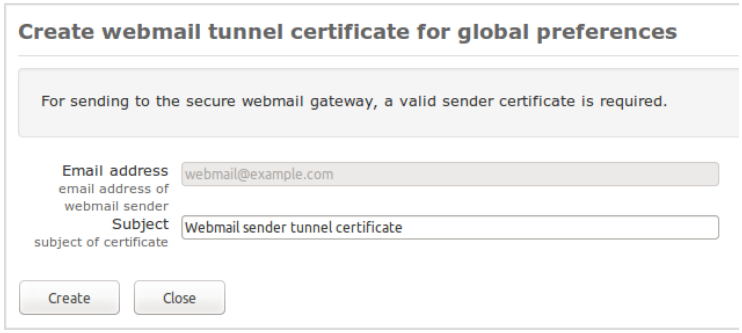

Figure 15: Create gateway tunnel certificate

Action

Click “create webmail certificate” on the webmail settings page (Settings → webmail) and then click the “Create” button.

3.9 Export gateway tunnel certificate

The newly generated gateway tunnel certificate must be exported to a file because it later steps it need to be imported into the webmail appliance. The webmail appliance requires the gateway tunnel certificate in order to validate

the email sent by the gateway.

The gateway tunnel certificate can be exported with the following steps:

1. Click the “available” link on the create webmail tunnel certificate page (see figure 16).
2. On the “Select signing certificate” page for the webmail sender, click the “Subject’ field of the certificate. This opens the certificate info page.
3. On the certificate info page, click “download certificate” and save the certificate to disk.

Action

Export newly generated gateway tunnel certificate.

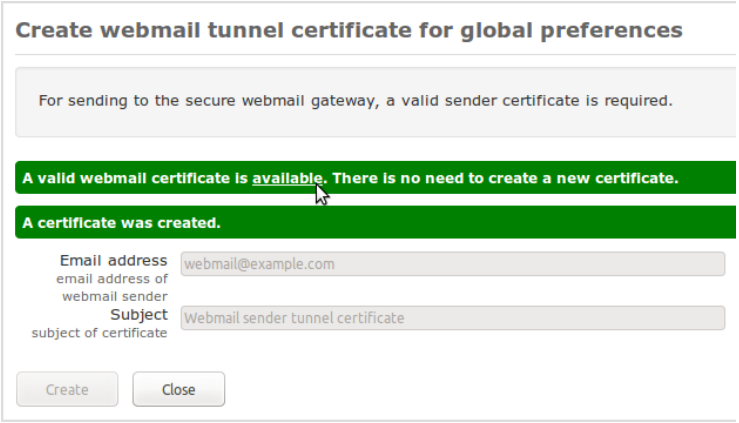

Figure 16: Gateway tunnel certificate created

3.10 Add SMTP transport

Because the webmail appliance was configured for a private local domain (**webmail.local**), routing via DNS will not work. An explicit routing rule should therefore be added. An explicit routing rule for the webmail appliance can be added with the following steps:

1. Open SMTP transports page (Admin → MTA → transports).
2. On the SMTP transports page, click “add transport”.
3. On the Add SMTP transport page, set “Recipients domain” to **webmail.local** and “Relay Host” to the domain name or IP address of the webmail appliance.

4. Click Add to add the new transport. The SMTP transports page should now look like figure 17 (the relay host IP address should match the IP or domain name of your webmail appliance).

Action

On the SMTP transport page (Admin → MTA → transports) add an SMTP transport to route email for **webmail.local** to the webmail appliance.

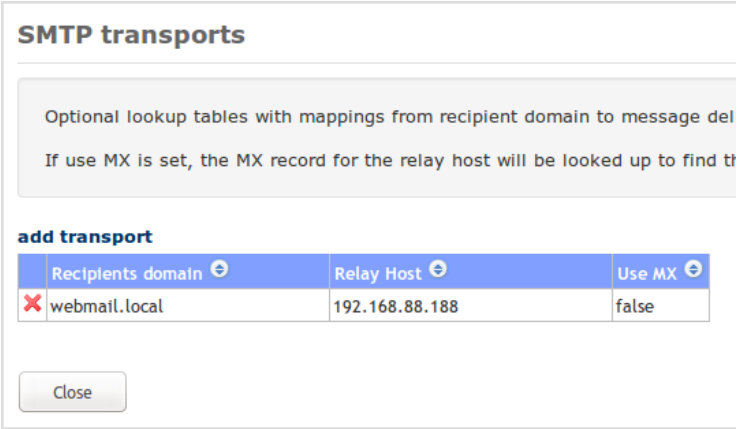

Figure 17: SMTP transports

3.11 Finish

The CipherMail gateway is now configured for webmail. In the next section the final configuration steps for the webmail appliance will be explained.

4 Webmail setup part 2

The webmail appliance still requires a couple of configuration changes.

The following steps will be described:

1. Import gateway tunnel certificate.
2. Trust the gateway tunnel certificate.

4.1 Import gateway tunnel certificate

The gateway tunnel certificate exported in section 3.9 should be imported into the webmail appliance. This is required to validate email sent by the CipherMail

gateway to the webmail appliance.

The gateway tunnel certificate can be imported with the following steps:

1. Login to the webmail appliance web GUI.
2. Open the certificates store (Admin → PKI → certificates).
3. On the intermediate and user certificates page, click “Import certificates” on the left hand side menu.
4. On the “Import certificates” page, select the exported gateway tunnel certificate, deselect “skip self-signed” and press the Import button.
5. Click the Close button. The intermediate and user certificates page should now view the newly imported certificate.

The certificate should be shown with a gray background to indicate that the certificate is not yet valid. The next section, will explain how to trust the certificate.

Action

On the certificates page (Admin → PKI → certificates) import the gateway tunnel certificate into the certificates store.

4.2 Trust the gateway tunnel certificate

The imported gateway tunnel certificate is not yet finished. This is because it’s a self-signed certificate. The certificate should be explicitly trusted by placing it on the white-list of the certificate trust list (CTL).

The gateway tunnel certificate can be placed on the white-list of the CTL with the following steps:

1. Open the certificates store (Admin → PKI → certificates).
2. On the intermediate and user certificates page, click on the subject of the gateway tunnel certificate to open the certificate info page.
3. On the certificate info page, click “add to CTL”.
4. On the “Add new Certificate Trust List entry” page, select “Whitelisted” and click “Add”.

The certificates store should now contain two certificates, one webmail tunnel certificate with a private key attached and one gateway tunnel certificate without private key (see figure 18). Both certificates should contain a green icon on the right side of the email address to indicate that the certificates are white-listed.

Action

Add the gateway tunnel certificate to the CTL white-list.

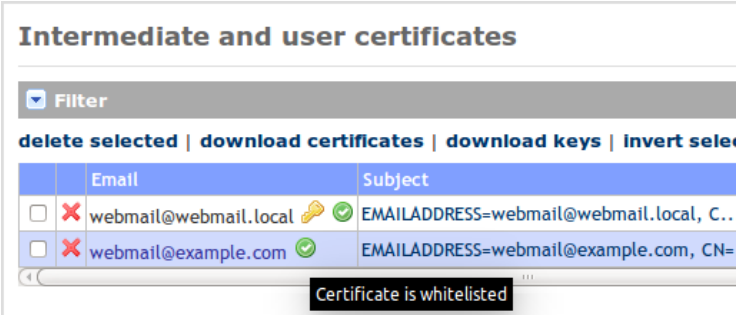

Figure 18: Webmail white-listed certificates

4.3 Finish

The gateway and webmail appliance are now correctly configured. Email sent by the CipherMail gateway which should be encrypted and cannot be encrypted with S/MIME, PGP or PDF, should now be delivered to the webmail gateway. In the next section the most common webmail related configuration problems will be discussed.

5 Troubleshooting

In this section we will discuss the most common webmail related configuration problems.

Webmail is disabled

Symptoms: The MPA logs of the gateway shows any of the following lines:

```
INFO Webmail is disabled for the sender....
INFO Webmail is disabled for the recipient....
```

Solution: enable webmail (settings → webmail) for sender and/or recipient.

The tunnel message could not be signed

Symptoms: The MPA logs of the gateway shows the following line:

```
WARN The tunneled message should have been signed...
```

The sender gets the following bounce message:

```
The message with Subject

CipherMail Secure Webmail message

has not been sent to the following recipients because the message could
not be encrypted.
```

```
webmail@webmail.local

The tunneled message should have been signed.
```

Solution: There is no valid S/MIME certificate with private key for the webmail sender address. Create a gateway tunnel certificate (see section 3.8).

The tunnel message could not be encrypted

Symptoms: The MPA log of the gateway shows the following line:

```
WARN There are no valid S/MIME certificates for the webmail recipient...
```

The sender gets the following bounce message:

```
The message with Subject

CipherMail Secure Webmail message

has not been sent to the following recipients because the message could
not be encrypted.

webmail@webmail.local

There are no valid S/MIME certificates for the webmail recipient.
```

Solution: There is no valid S/MIME certificate for the webmail recipient address. Import the webmail certificate and make sure the webmail certificate is trusted (see section 3.2 and 3.3).

The tunnel message was bounced by the gateway

Symptoms: The MTA log of the gateway shows the following line:

```
to=<webmail@webmail.local>, relay=none, delay=0.06, delays=0/0/0.06/0, dsn=5.4.4,
status=bounced (Host or domain name not found. Name service error for
name=webmail.local type=AAAA: Host not found)
```

The webmail sender address gets the following bounce message:

```
This is the mail system at host gateway.example.com.

I'm sorry to have to inform you that your message could not
be delivered to one or more recipients. It's attached below.

For further assistance, please send mail to postmaster.

If you do so, please include this problem report. You can
delete your own text from the attached returned message.
```

```
                    The mail system

<webmail@webmail.local>: Host or domain name not found. Name service
error for name=webmail.local type=AAAA: Host not found
```

Solution: Configure the SMTP transport (see section 3.10).

The tunnel message gets stuck in the MTA queue of the gateway

Symptoms: The MTA log of the gateway shows the following line:

```
3E808D2: to=<webmail@webmail.local> ... status=deferred (connect to
192.168.88.254[192.168.88.254]:25: No route to host)
```

Solution: Check whether the SMTP transport is correctly configured (see section 3.10). If the SMTP transport is correctly configured, check whether there is a firewall that blocks access to the webmail appliance.

The tunnel message gets stuck in the MTA queue of the gateway

Symptoms: The MTA log of the gateway shows the following line:

```
3E808D2: to=<webmail@webmail.local> ... status=deferred
(host 192.168.88.188[192.168.88.188] said: 454 4.7.1
<webmail@webmail.local>: Relay access denied (in reply to
RCPT TO command))
```

Solution: Add the domain **webmail.local** to the webmail relay domains (see section 2.3.1).

The tunnel message gets stuck in the MTA queue of the webmail appliance

Symptoms: The MPA log of the webmail appliance shows the following line:

```
INFO Email is not a relay email; ... Recipients: [webmail@webmail.local]
```

Solution: The “Relay recipient ” of the webmail appliance is not configured or does not match the “Webmail recipient” of the gateway (see section 2.3.6 and 3.5).

The tunnel message gets forwarded to the postmaster address of the webmail appliance

Symptoms: The MPA log of the webmail appliance shows the following line:

```
WARN S/MIME decryption key not found; ... Message: A suitable
decryption key could not be found..
```

The postmaster receives the following message:

```
The webmail relay message could not be handled. The message
is attached to this message.

Additional information:

The web relay message was not properly signed.
...
```

Solution: The tunnel message was encrypted with a certificate for which there is no private key available on the webmail appliance. Check whether a valid webmail tunnel certificate was generated (see section 2.3.11). If there is a valid webmail tunnel certificate (with associated private key), check whether the webmail recipient certificate on the gateway matches the certificate on the webmail appliance.

The tunnel message gets forwarded to the postmaster address of the webmail appliance

Symptoms: The MPA log of the webmail appliance shows the following line:

```
WARN S/MIME signature was not valid; Signer IDs:
EMAILADDRESS=webmail@example.com ...
```

The postmaster receives the following message:

```
The webmail relay message could not be handled. The message
is attached to this message.

Additional information:

The web relay message was not properly signed.
...
```

Solution: The gateway tunnel certificate was not imported or not trusted. Import the gateway tunnel certificate and add the gateway tunnel certificate to the white-list of the certificate trust list (see section 4.1 and 4.2).

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.