port25
A Message Systems Company

WHITE PAPER

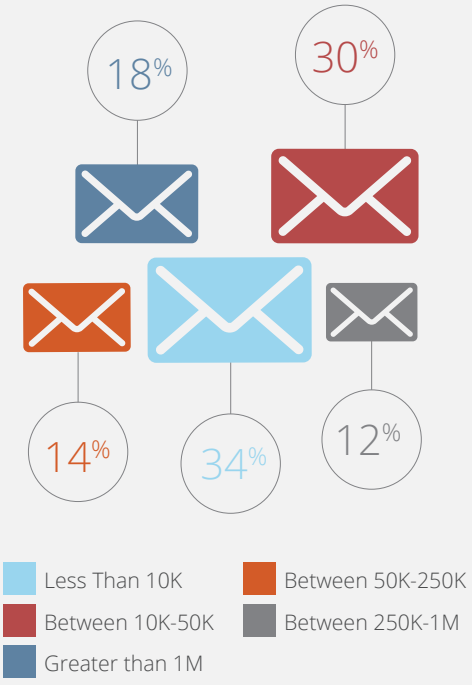
Encrypting Connections in PowerMTA

port25
A Message Systems Company

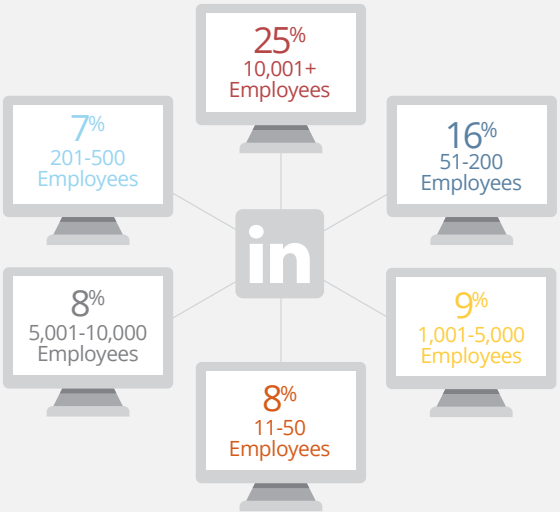
WHITE PAPER

Encrypting Connections in PowerMTA

Port25 **Evaluation Requests**
By Hourly Email Volume



Port25 **LinkedIn Engagement Data**
By Company Size



Encryption is becoming increasingly necessary when transferring data across the internet, and email is no different. In PowerMTA 4.5 and later there are several methods to encrypt both inbound and outbound connections. Keep in mind, this document only deals with encrypting the channel, not the content.

Outbound Opportunistic Encryption

To use outbound opportunistic encryption in PowerMTA simply add the following to your configuration file:

```
<domain *>
    use-starttls yes
    require-starttls no
</domain>
```

With this PowerMTA will check to see if the remote mail server supports encryption. If it does, an attempt will be made to create an encrypted channel over which to send mail. If the encryption fails, or if no encryption is offered, then the mail sent using no encryption.

To verify if the mail was sent over an encrypted channel, it is necessary to add additional fields to the CSV accounting file. This can be done with the following configuration:

```
<acct-file log\acct.csv>
    records d, b
    record-fields d *, dlvTlsProtocol, dlvTlsCipher
    record-fields b *, dlvTlsProtocol, dlvTlsCipher
</acct-file>
```

If encryption is used the above configuration will record the protocol and cipher used to deliver the message over an encrypted channel.

Outbound Opportunistic Encryption

While the vast majority of outbound connections do not require a local certificate, there may be some B2B cases in which the remote mail server requires PowerMTA to use a given certificate for encrypting the channel between the two servers. This can be facilitated in PowerMTA with a setup similar to the following:

<domain super-secure-server.com>
smtp-client-certificate /path/to/certificate.pem password
use-starttls yes
require-starttls yes
</domain>

In the above example, any messages sent to super-secure-server.com will sent over an encrypted channel using the certificate /path/to/certificate.pem (in most cases supplied by the administrator of the remote mail server). If the encryption fails, the messages will not be sent.

Inbound Encryption

Of course, outbound traffic is only half of the traffic on a PowerMTA server. It may be required to encrypt the traffic coming into a PowerMTA server as well. This can be done in PowerMTA on a per <source> basis. The setup would look similar to the following:

#
smtp-listener 1.2.3.4:465 tls=yes
smtp-server-tls-certificate /etc/pmta/smtp-cert.pem "YourPasswordHere"
smtp-server-tls-ciphers "HIGH:MEDIUM:!ADH:@STRENGTH"

<source 0/0> # matches all
allow-starttls yes
require-starttls-before-auth yes
allow-unencrypted-plain-auth no
</source>
#

Creation of the certificate /etc/pmta/smtp-cert.pem follows standard OpenSSL practices, and if assistance is needed in getting the certificate created, please contact support@port25.com. An example of the contents of the certificate is as follows:

-----BEGIN CERTIFICATE-----

YOUR CERT HERE

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,EBA505536010547C

YOUR PRIVATE KEY HERE

-----END RSA PRIVATE KEY-----

With this configuration all traffic connecting to 1.2.3.4 on port 465 can attempt to use encryption for transmitting email into PowerMTA.

Inbound Certificate Chain Validation

PowerMTA 4.5 and later supports the ability to validate certificate chains.