# Postfix-Mailversand über SSL

Mailversand über SSL ist ja kein Problem. Man stellt im Mailclient ein, dass man SSL benutzen will, der Port wird dann auf 465 eingestellt[1)], und alles klappt.

Und was ist, wenn ein Server seine Mail so versenden soll? Wenn der Server – wie das aktuell meist der Fall ist – mit Postfix läuft, kann man vorgehen wie unter http://www.postfix.org/TLS_README.html#client_smtps beschrieben.

Bei einem SLES 11 sieht das so aus, dass man zunächst mit

```
zypper in stunnel
```

die Software `stunnel` installiert. Abhängigkeiten würden dabei gleich mitinstalliert, aber es gibt keine 🙂

Dann konfiguriert man stunnel, indem man die große mitgelieferte Datei `/etc/stunnel/stunnel.conf` durch eine kleinere ersetzt[2)]:

```
mv /etc/stunnel/stunnel.conf /etc/stunnel/stunnel.conf.original
mkdir /var/run/stunnel/
chown stunnel /var/run/stunnel/
cat > /etc/stunnel/stunnel.conf<<EOT
[smtp-tls-wrapper]
accept = 11125
client = yes
connect = imap.example.net:465
EOT
```

Nun kann man via

```
rcstunnel start
```

den SSL-Tunnel zum Mailserver aufbauen. Den kann man gleich mit telnet testen:

```
telnet localhost 11125
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 imap.example.net -- Server ESMTP (Oracle Communications Messaging
Exchange Server 7u4-22.01 64bit (built Apr 21 2011))
```

Erfolgreich! Nun hat man eine verschlüsselte Verbindung. Jetzt muss Postfix sie noch zur Nachrichtenübermittlung benutzen. Das erreicht man, indem man in die Datei `/etc/postfix/main.cf` die Zeile

```
relayhost = [127.0.0.1]:11125
```

aufnimmt. Auf diese Weise spricht Postfix bei jedem Mailversand mit dem Server, der unter [127.0.0.1]:11125 erreicht wird, und das ist dank `stunnel` der interne IMAP-Server. Damit die Einstellung wirksam wird, muss Postfix durchgestartet werden:

```
rcpostfix restart
```

Nun wäre es schön, wenn man sich auf den Tunnel verlassen könnte. Da es ja passieren kann, dass `stunnel` abstürzt, installieren wir gleich noch `monit` und lassen dadurch sicherstellen, dass `stunnel` immer läuft.

Die Schritte sind

```
zypper in monit
mv /etc/monitrc /etc/monitrc.original
cat > /etc/monitrc <<EOT
set daemon 120
set logfile /var/log/monit
set idfile /var/run/monit/monit.id
set statefile /var/run/monit/monit.state
set mailserver localhost
set alert root@localhost
set httpd port 2812 and
    allow 192.168.0.0/24
    allow localhost
include /etc/monit.d/*
EOT
chmod 0700 /etc/monitrc
cat > /etc/monit.d/stunnel<<EOT
check process stunnel with pidfile /var/run/stunnel/stunnel.pid
    start program = "/etc/init.d/stunnel start"
    stop program  = "/etc/init.d/stunnel stop"
    if failed host 127.0.0.1 port 11125 protocol smtp then restart
EOT
rcmonit start
```

Also eigentlich wie oben: Software installieren, Konfigurationsdatei anpassen bzw. erstellen, Software starten. Und wohlfühlen nicht vergessen 

Und um sicherzustellen, dass `monit` und `stunnel` beim nächsten Systemstart auch brav mitstarten, gibt man noch ein:

```
insserv monit
insserv stunnel
```

## Sicherheitsgewinn

Und welchen Sicherheitsgewinn haben wir erreicht, wenn wir jetzt über Port 465 kommunizieren? Richtig, keinen[3)]. Denn eine verschlüsselte Verbindung bekommt man auch anders hin, nämlich

schlicht und ergreifend über Port 25 und eine Konfigurationszeile in Postfix. Die Voraussetzungen sind ja gegeben:

```
telnet imap.example.net 25
Trying 192.168.0.166...
Connected to imap.example.net.
Escape character is '^]'.
220 imap.example.net -- Server ESMTP (Oracle Communications Messaging
Exchange Server 7u4-22.01 64bit (built Apr 21 2011))
EHLO ruebennase.example.net
250-imap.example.net
250-8BITMIME
250-PIPELINING
250-CHUNKING
250-DSN
250-ENHANCEDSTATUSCODES
250-EXPN
250-HELP
250-XADR
250-XSTA
250-XCIR
250-XGEN
250-XLOOP 084A42ABFB7696DCD5C12F59399F94C9
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=LOGIN PLAIN
250-ETRN
250-NO-SOLICITING
250 SIZE 0
```

Wenn man Postfix mit dem Parameter `smtp_tls_security_level = may` oder `smtp_tls_security_level = encrypt` versieht (Quelle: http://www.postfix.org/TLS_README.html#client_tls), wird Postfix bei Kommunikation über Port 25 das Verfahren STARTTLS benutzen, was der Mailserver ja anbietet. Damit ist auch die Verbindung über Port 25 verschlüsselt, und zwar in mindestens demselben Maße, wie `stunnel` verschlüsselt.

Aber egal, in der Dokumentation steht, dass ein „sicherer“ Port benutzt wird (der übrigens von der IANA für „URL Rendezvous Directory for SSM“ reserviert ist), und nicht der pöse, unsichere Port 25.

Könnte ja jeder kommen… 😕

1)

nein, natürlich nicht. Port 465 wurde damals von Outlook eingeführt, den benutzt heutzutage kein Mensch mehr, aber…

2)

das `mkdir` dabei sollte eigentlich von der Post-Installationsroutine des rpms ausgeführt werden, denn die mitgelieferte Konfiguration setzt die Existenz des Verzeichnisses voraus

3)

strenggenommen ist es unsicherer geworden, weil zwei zusätzliche Softwarepakete auf dem Host installiert wurden