Postfix mit TLS und PFS

Postfix ist ein MTA[1)]. Mit TLS[2)] werden Daten verschlüsselt übertragen. Und PFS[3)] verhindert, dass trotzdem aufgezeichnete Kommunikation im Nachhinein entschlüsselt werden kann.

Dieser Beitrag beruht im Wesentlichen auf http://www.heinlein-support.de/blog/security/perfect-forward-secrecy-pfs-fur-postfix-und-dovecot/. Um Postfix grundsätzlich TLS-fähig zu machen, wurden die Schritte von http://blog.alonso.ch/tech/sicherheit/postfix-mit-tls-erweitern/ herangezogen.

Was ist zu tun? Auf der Maschine muss natürlich Postfix installiert sein, openssl ist meist ohnehin vorhanden. Postfix muss mindestens in Version 2.6, besser 2.8, vorliegen. Openssl ab Version 0.9 ist für das Diffie-Hellman-Verfahren (DHE) auch Voraussetzung, aber ältere Versionen dürften ohnehin schon ausgestorben sein (außer vielleicht auf Debian Stable 😬). Ab Version 1.0 von openssl wird die optimierte Version (Elliptic Curve Diffie Hellman, ECDHE) benutzt.

Postfix mit TLS

Diverse Howtos finden sich z. B. auf http://www.postfix.org/docs.html ebenso wie unter http://www.postfix.org/TLS_README.html.

Zunächst muss sichergestellt werden, dass Postfix überhaupt mit TLS umgehen kann. Dazu sind mehrere Voraussetzungen zu erfüllen:

- in der Datei /etc/postfix/master.cf muss der Eintrag für tlsmgr aktiv sein (ggf. Kommentarzeichen am Zeilenanfang entfernen, so dass „tlsmgr“ am Zeilenanfang beginnt)
- Postfix muss mit existierenden Dateien zu den Parametern[4)] smtp_tls_cert_file, smtpd_tls_cert_file, smtp_tls_key_file, smtpd_tls_key_file konfiguriert sein
- etliche weitere Parameter sollten TLS ermöglichen, aber nicht erzwingen: smtpd_tls_auth_only, smtpd_enforce_tls, smtpd_tls_security_level, smtp_tls_note_starttls_offer, smtpd_tls_loglevel, smtpd_tls_received_header, smtpd_tls_session_cache_timeout, tls_random_source

Wenn die Parameter smtp[,d]_tls_*_file nicht gesetzt oder die Dateien nicht vorhanden sind, kann man sie relativ schnell erstellen. Allerdings sind es dann selbsterstellte Zertifikate und Schlüssel...

```
mkdir /etc/postfix/ssl
cd /etc/postfix/ssl
openssl genrsa -out smtp.key 2048
openssl req -new -key smtp.key -out smtp.csr
openssl x509 -req -days 3650 -in smtp.csr -out smtp.cert -signkey smtp.key
```

Nachdem die Schüssel vorhanden sind, kann Postfix die entsprechenden Einträge in der Konfigurationsdatei erhalten:

```
postconf -e "smtp_tls_note_starttls_offer = yes"
postconf -e "smtp_tls_CApath = /etc/ssl/certs"                    # dort stehen
vertrauenswuerdige CA-Zertifikate
```

```
postconf -e "smtp_tls_security_level = may"
postconf -e "smtpd_tls_CApath  = /etc/ssl/certs"
postconf -e "smtpd_tls_security_level = may"
postconf -e "smtpd_tls_auth_only = no"
postconf -e "smtpd_enforce_tls = no"
postconf -e "smtpd_tls_cert_file = /etc/postfix/ssl/smtp.cert" # wenn noch
nicht (oder falsch) gesetzt
postconf -e "smtpd_tls_key_file = /etc/postfix/ssl/smtp.key"   # wenn noch
nicht (oder falsch) gesetzt
postconf -e "smtpd_tls_loglevel = 1"
postconf -e "smtpd_tls_received_header = yes"
postconf -e "smtpd_tls_session_cache_timeout = 3600s"
postconf -e "tls_random_source = dev:/dev/urandom"
```

Wer fertige Schlüssel hat, sollte natürlich die entsprechenden Pfade hier angeben (oder die Schlüssel an die angegebenen Orte kopieren). Beispiel:

```
postconf -e "smtpd_tls_key_file = /etc/postfix/ssl/1234.key.op.pem"
# bei neuen Zertifikaten: privatekey_without_password.pem
postconf -e "smtpd_tls_cert_file =
/etc/postfix/ssl/hostname.intranet.my.corp"  # bei neuen Zertifikaten:
cert_chain.txt
postconf -e "smtp_tls_key_file = /etc/postfix/ssl/1234.key.op.pem"
# bei neuen Zertifikaten: privatekey_without_password.pem
postconf -e "smtp_tls_cert_file =
/etc/postfix/ssl/hostname.intranet.my.corp"   # bei neuen Zertifikaten:
cert_chain.txt
```

Anmerkung smtp_*-Parameter sind für den Versand, smtpd_*-Parameter für den Mailempfang.

TLS mit PFS

Auch hier kann man anderswo nachlesen, z. B. auf http://www.postfix.org/FORWARD_SECRECY_README.html.

Hier sind einige Postfix-Einstellungen vorzunehmen sowie – falls noch nicht vorhanden – zwei Dateien mit Diffie-Hellman-Parametern anzulegen.

Analog zu den Zertifikaten sollte man zunächst prüfen, welchen Inhalt die Parameter smtpd_tls_dh1024_param_file und smtpd_tls_dh512_param_file haben und dann sicherstellen, dass die Dateien auch existieren. Ist das nicht der Fall, können sie mit

```
  openssl gendh -out /etc/postfix/dh_512.pem -2 512
  openssl gendh -out /etc/postfix/dh_1024.pem -2 1024
```

schnell und schmerzlos erstellt werden.

Der Rest besteht dann wieder aus dem Eintragen von Parametern:

```
postconf -e "smtpd_tls_dh1024_param_file = /etc/postfix/dh_1024.pem"
postconf -e "smtpd_tls_dh512_param_file = /etc/postfix/dh_512.pem"
postconf -e "smtpd_tls_eecdh_grade = strong"
postconf -e "tls_preempt_cipherlist = yes"
postconf -e "smtpd_tls_loglevel = 1"
postconf -e "smtp_tls_loglevel = 1"
```

als Script

Das folgende Script erledigt beide Teilaufgaben (Aktivieren von TLS, Aktivieren von PFS) und läuft auf SLES 11. Für andere Linux-Varianten (und andere Speicherorte der Zertifikate) sind ggf. die Pfade anzupassen – und zum Schluss der Befehl, um Postfix durchzustarten.

/usr/local/bin/postfix_pfs.sh

/usr/local/bin/postfix_pfs.sh

```
#!/bin/bash
#
# enable TLS in postfix
# and make sure that PFS can be used

[ -z "$PATH" ] && PATH=/bin:/usr/bin:/usr/local/bin:/sbin:/usr/sbin

# first: care about the TLS certificates and keys

# get the current config of postfix
TLSCERT1=$(postconf -h smtp_tls_cert_file)
TLSCERT2=$(postconf -h smtpd_tls_cert_file)
TLSKEY1=$(postconf -h smtp_tls_key_file)
TLSKEY2=$(postconf -h smtpd_tls_key_file)

# make sure both TLS CERT variables are set and the files exist
[ -n "$TLSCERT1" -a -f "$TLSCERT1" ] || TLSCERT1=''
[ -n "$TLSCERT2" -a -f "$TLSCERT2" ] || TLSCERT2=''
[ -n "$TLSKEY1"  -a -f "$TLSKEY1"  ] || TLSKEY1=''
[ -n "$TLSKEY2"  -a -f "$TLSKEY2"  ] || TLSKEY2=''

# maybe we got other certificates?
if [ -z "$TLSKEY1" ]; then
    ERSATZ=$(ls /home/*/cert/my.corp/*key.op.pem)
    if [ -n "$ERSATZ" -a -f "$ERSATZ" ] ; then
        TLSKEY1="$ERSATZ"
        [ -z "$TLSKEY2" ] && TLSKEY2="$TLSKEY1"
    fi
fi
[ -z "$TLSKEY2" -a -n "$TLSKEY1" ] && TLSKEY2="$TLSKEY1"
```

```
if [ -z "$TLSCERT1" ]; then
    ERSATZ=$(ls /home/*/cert/von_2013/*.intranet.my.corp.pem)
    if [ -n "$ERSATZ" -a -f "$ERSATZ" ] ; then
        TLSCERT1="$ERSATZ"
        [ -z "$TLSCERT2" ] && TLSCERT2="$TLSCERT1"
    fi
fi
[ -z "$TLSCERT2" -a -n "$TLSCERT1" ] && TLSCERT2="$TLSCERT1"

# now make sure the CERT/KEY files really exist
if [ -z "$TLSCERT1" -o -z "$TLSKEY1" ]; then
    # no TLS cert/key for smtp
    if [ -z "$TLSCERT2" -o -z "$TLSKEY2" ]; then
        # no TLS cert/key available at all, we'll create them
        TLSCERT1='/etc/postfix/ssl/smtp.cert'
        TLSKEY1='/etc/postfix/ssl/smtp.key'
        TLSCERT2="$TLSCERT1"
        TLSKEY2="$TLSKEY1"
        mkdir -p /etc/postfix/ssl
        openssl genrsa -out "$TLSKEY1" 2048
        # next command ist interactive
        # make it as comfortable as possible
        sed -i 's|^countryName_default.*$|countryName_default        =
DE|' /etc/ssl/openssl.cnf
        sed -i
's|^stateOrProvinceName_default.*$|stateOrProvinceName_default   =
Sachsen|' /etc/ssl/openssl.cnf
        sed -i
's|^0.organizationName_default.*$|0.organizationName_default   =
Pferdebadeanstalt|' /etc/ssl/openssl.cnf
        openssl req -new -key "$TLSKEY1" -out /etc/postfix/ssl/smtp.csr
        openssl x509 -req -days 3650 -in /etc/postfix/ssl/smtp.csr -out
"$TLSCERT1" -signkey "$TLSKEY1"
    else
        # we can use the smtpd TLS cert/key as smtp cert/key
        TLSCERT1="$TLSCERT2"
        TLSKEY1="$TLSKEY2"
    fi
else
    if [ -z "$TLSCERT2" -o -z "$TLSKEY2" ]; then
        # we can use the smtp TLS cert/key as smtpd cert/key
        TLSCERT2="$TLSCERT1"
        TLSKEY2="$TLSKEY1"
    # else
        # all files exist, nothing to repair here
    fi
fi

# second: for PFS, we need the Diffie-Hellman files
PFS1=$(postconf -h smtpd_tls_dh1024_param_file)
PFS5=$(postconf -h smtpd_tls_dh512_param_file)
```

```
[ -n "$PFS1" -a -f "$PFS1" ] || PFS1=''
[ -n "$PFS5" -a -f "$PFS5" ] || PFS5=''
if [ -z "$PFS1" ] ; then
    PFS1='/etc/postfix/dh_1024.pem'
    openssl gendh -out "$PFS1" -2 1024
    postconf -e "smtpd_tls_dh1024_param_file = $PFS1"
fi
if [ -z "$PFS5" ] ; then
    PFS5='/etc/postfix/dh_0512.pem'
    openssl gendh -out "$PFS5" -2 512
    postconf -e "smtpd_tls_dh512_param_file = $PFS5"
fi

# third: we set the postfix config to use the certs and enable PFS
postconf -e "smtp_tls_cert_file = $TLSCERT1"
postconf -e "smtp_tls_key_file = $TLSKEY1"
postconf -e "smtp_tls_loglevel = 1"
postconf -e "smtp_tls_note_starttls_offer = yes"
postconf -e "smtp_tls_security_level = may"
postconf -e "smtp_use_tls = yes"
postconf -e "smtpd_enforce_tls = no"
postconf -e "smtpd_tls_auth_only = no"
postconf -e "smtpd_tls_CApath = /etc/ssl/certs"
postconf -e "smtpd_tls_cert_file = $TLSCERT2"
postconf -e "smtpd_tls_eecdh_grade = strong"
postconf -e "smtpd_tls_key_file = $TLSKEY2"
postconf -e "smtpd_tls_loglevel = 1"
postconf -e "smtpd_tls_received_header = yes"
postconf -e "smtpd_tls_security_level = may"
postconf -e "smtpd_tls_session_cache_timeout = 3600s"
postconf -e "smtpd_use_tls = yes"
postconf -e "tls_random_source = dev:/dev/urandom"
postconf -e "tls_preempt_cipherlist = yes"

egrep -q '^tlsmgr' /etc/postfix/master.cf || sed -i.tls
's|#tlsmgr|tlsmgr|' /etc/postfix/master.cf

rcpostfix restart
rcpostfix status
```

Hat's geklappt?

Vor dem Testen muss Postfix seine Konfiguration neu laden. Wenn der „tlsmgr“-Eintrag in der Datei „master.cf“ geändert oder neu angelegt wurde, muss Postfix durchgestartet werden, sonst reicht ein „reload“. Prüfen lässt sich der Erfolg anschließend mit

```
openssl s_client -starttls smtp -connect localhost:25
```

bzw. bei SUSE mit

```
openssl s_client -starttls smtp -connect localhost:25 -CApath
/etc/ssl/certs/
```

Der ausgegebene Text sollte einen der beiden folgenden Textblöcke enthalten:

```
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
```

(mit openssl vor 1.0) oder (mit openssl ab 1.0):

```
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
```

main.cf komplett (Beispiel)

Als Beispiel hier eine Konfiguration mit den Pfaden, wie sie auf einem SLES 11 typischerweise existieren (und in der ausgelieferten main.cf auch eingetragen werden). Die Datei wurde durch `mv /etc/postfix/main.cf /etc/postfix/main.cf.full && grep ^[^#] /etc/postfix/main.cf.full > /etc/postfix/main.cf` erstellt, dann umsortiert, feingeschliffen und mit `rcpostfix reload` angewendet.

Datei /etc/postfix/main.cf

/etc/postfix/main.cf

```
# Pfade und Verzeichnisse
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/lib/postfix
data_directory = /var/lib/postfix
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/packages/postfix-doc/samples
readme_directory = /usr/share/doc/packages/postfix-doc/README_FILES
html_directory = /usr/share/doc/packages/postfix-doc/html
mail_spool_directory = /var/mail
sendmail_path = /usr/sbin/sendmail
newaliases_path = /usr/bin/newaliases
mailq_path = /usr/bin/mailq

# allgemeine Einstellungen
mail_owner = postfix
setgid_group = maildrop
debug_peer_level = 2
debugger_command =
```

```
        PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
        ddd $daemon_directory/$process_name $process_id & sleep 5
unknown_local_recipient_reject_code = 550
mailbox_command =
mailbox_transport =
strict_8bitmime = no
disable_mime_output_conversion = no
strict_rfc821_envelopes = no
mailbox_size_limit = 0
message_size_limit = 10240000

# Netzwerkeinstellungen
inet_interfaces = localhost
inet_protocols = all
myhostname = beispiel.intranet.my.corp
mydomain = intranet.my.corp
mydestination = $myhostname, localhost.$mydomain, localhost, beispiel
mynetworks_style = subnet
disable_dns_lookups = no
relayhost = [imap.intranet.my.corp]
defer_transports =
biff = no

# diverse Mappings
alias_maps = hash:/etc/aliases, ldap:/etc/postfix/my-ldap-aliases.cf
virtual_alias_maps = hash:/etc/postfix/virtual
virtual_alias_domains = hash:/etc/postfix/virtual
canonical_maps = hash:/etc/postfix/canonical
relocated_maps = hash:/etc/postfix/relocated
transport_maps = hash:/etc/postfix/transport
sender_canonical_maps = hash:/etc/postfix/sender_canonical
masquerade_exceptions = root
masquerade_classes = envelope_sender, header_sender, header_recipient
masquerade_domains =

# SMTP-Parameter (Mailversand)
smtp_dns_resolver_options = res_defnames
smtp_sasl_auth_enable = no
smtp_tls_CApath = /etc/ssl/certs
smtp_tls_cert_file = /etc/postfix/ssl/smtp.cert
smtp_tls_key_file = /etc/postfix/ssl/smtp.key
smtp_tls_loglevel = 1
smtp_tls_note_starttls_offer = yes
smtp_tls_security_level = may
smtp_use_tls = yes

# SMTP-Parameter (Maileingang)
smtpd_banner = $myhostname
smtpd_client_restrictions =
smtpd_enforce_tls = no
smtpd_helo_required = no
```

```
smtpd_helo_restrictions =
smtpd_recipient_restrictions =
permit_mynetworks,reject_unauth_destination
smtpd_sasl_auth_enable = no
smtpd_sender_restrictions = hash:/etc/postfix/access
smtpd_tls_auth_only = no
smtpd_tls_CApath = /etc/ssl/certs
smtpd_tls_cert_file = /etc/postfix/ssl/smtp.cert
smtpd_tls_dh1024_param_file = /etc/postfix/dh_1024.pem
smtpd_tls_dh512_param_file = /etc/postfix/dh_0512.pem
smtpd_tls_eecdh_grade = strong
smtpd_tls_key_file = /etc/postfix/ssl/smtp.key
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_security_level = may
smtpd_tls_session_cache_timeout = 3600s
smtpd_use_tls = yes

# TLS-Parameter
tls_random_source = dev:/dev/urandom
tls_preempt_cipherlist = yes
```

1)
Mail Transport Agent
2)
Transport Layer Security
3)
Perfect Forward Secrecy
4)
alle erklärt z. B. auf http://www.postfix.org/postconf.5.html oder per `man 5 postconf`