Inviare la Posta Elettronica in Modo Sicuro

Uno dei principali problemi pratici attuali nella gestioni delle reti informatiche, è quello della posta elettronica. Ormai la posta elettronica è un fattore essenziale nella quotidianità aziendale, e deve essere possibile per i dipendenti accedere alla propria posta in qualunque momento da qualunque postazione. Una soluzione adottata molto spesso è quella di fornire l'accesso alla posta elettronica via *Webmail*, questo permette di accedere alla propria posta, sia in ricezione che invio, via internet tramite un qualunque web-browser. In questo caso però, tutti i messaggi rimangono sul server Webmail e non è possibile accedere alla posta off-line. Molti perciò preferiscono avere la posta a disposizione in qualunque momento, tenendola ad esempio sul proprio portatile. Questa soluzione comporta delle problematiche per chi a livello aziendale deve gestire il servizio. Possiamo considerare i problemi indipendentemente per l'invio e la ricezione della posta ed a secondo che l'accesso avvenga dall'interno o dall'esterno della rete aziendale.

Per la ricezione della posta è prassi utilizzare un server POP3/IMAP4. In pratica la posta in arrivo viene depositata dal server SMTP aziendale nella casella dell'utente sul server POP3/IMAP4. Il programma client di posta, detto anche *Mail User Agent* (MUA), sul PC dell'utente accede alla casella di posta e scarica i nuovi messaggi arrivati. L'accesso è autenticato, usualmente con username e password. Questa procedura funziona anche se l'utente, con il suo PC portatile, è all'esterno dell'azienda e si collega via internet al server POP3/IMAP4. Ovviamente il server POP3/IMAP4 deve offrire il servizio in internet, il che comporta ben chiari rischi, ma in linea di principio richiedendo che la connessione tra l'MUA ed il server sia protetta con SSL/TLS e la presenza dell'autenticazione del servizio, è possibile configurare il servizio in modo da mitigare parzialmente i rischi associati.

Se per la ricezione della posta il problema è abbastanza semplice, per l'invio è un poco più complicato. Per inviare un messaggio di posta, un MUA si connette al server SMTP aziendale. Se il PC è all'interno della rete aziendale, il server SMTP riceve il messaggio e lo invia a destinazione. I

server SMTP **devono** però essere configurati a non accettare messaggi da inviare ad altri da macchine all'esterno della propria rete aziendale. Questo è il famoso problema degli *Open Relay*, server SMTP che permettono a chiunque in internet di inviare posta a chiunque altro, usati principalmente da chi invia spam e virus. La soluzione a questo problema è simile alla precedente, anche se meno nota. In pratica quando un MUA deve inviare un messaggio di posta, crea un canale sicuro di comunicazione con il server SMTP via SSL/TLS, si autentica presso il server come per i servizi POP3/IMAP4, ed invia il messaggio. Il server SMTP agisce da relay aperto solo per i client che si sono autenticati con successo presso di lui.

Postfix con SASL e TLS

Poiché questa configurazione è meno standard, la illustriamo con l'esempio a nostro parere più semplice, postfix con SASL e TLS. Il fatto è che i server SMTP non supportano nativamente né TLS né l'autenticazione dei client, pertanto alcune modifiche vanno fatte. In realtà postfix, sendmail, qmail ecc. ormai hanno tutti integrato sia TLS, spesso tramite *openssl*, che *Simple Authentication and Security Layer* (SASL). SASL è un programma (demone), indipendente dalla piattaforma/sistema operativo, che permette di aggiungere facilmente ad altri programmi l'autenticazione degli utenti. In pratica un programma che ha necessità di verificare le credenziali di autenticazione ma che non è in grado di farlo direttamente, passa a SASL le credenziali dell'utente e SASL le verifica presso l'opportuna base dati, dal file di password, a PAM, ad un server LDAP ecc. Il programma non ha idea di come debbano essere verificate le credenziali, cosa che invece deve essere fatta da SASL. Vediamo ora come implementare in pratica tutto ciò.

Prima di tutto bisogna installare openssl, SASL e postfix con supporto per TLS e SASL. Per la maggior parte delle piattaforme UNIX/Linux esistono pacchetti già pronti di questi programmi. Bisogna però sempre verificare la validità della fonte tramite firma digitale od almeno l'impronta originale SHA1. Qui perciò descriviamo solo le configurazioni necessarie.

Postfix e TLS

Innanzitutto abbiamo bisogno di un certificato digitale per postfix.[1] In realtà dobbiamo avere 3 file: il certificato digitale della CA, il certificato digitale per postfix, ed il file contenente la relativa chiave privata non cifrata (altrimenti dobbiamo digitare la passphrase ad ogni attivazione di postfix). Mettiamo questi 3 file nella directory di configurazione di postfix, `/etc/postfix/`, ed aggiungiamo le relative configurazioni al file /etc/postfix/main.cf come indicato in Tabella 1.

SASL

La configurazione di SASL è molto semplice, basta modificare il file `/usr/lib/sasl2/smtpd.conf` ad esempio come indicato in Tabella 2, e lanciare il programma indicando quale base dati usare per l'autenticazione: ad esempio si può lanciare `saslauthd` con l'opzione `-a shadow`, oppure `-a pam`, oppure `-a ldap` eccetera. Per il nostro esempio semplicissimo utilizziamo il file di password locale (`-a shadow`) ed i metodi di autenticazione PLAIN o LOGIN. Di solito si usa la stessa base dati ove sono le credenziali degli utenti usate per l'accesso ai servizi POP3/IMAP4.

Postfix e SASL

Dobbiamo a questo punto configurare postfix per utilizzare SASL per l'autenticazione degli utenti, le istruzioni necessarie sono indicate in Tabella 3. La regola importante è la `smtpd_recipient_restrictions` che indica che postfix può inviare posta (fare il relay) per tutte le macchine interne (`permit_mynetworks`) e per tutti i client MUA autenticati con SASL (`permit_sasl_authenticated`) anche se si connettono da una rete esterna. Inoltre l'autenticazione è accettata solo se protetta da TLS (`smtpd_tls_auth_only = yes`). Un'alternativa all'uso della porta 25 per l'invio autenticato della posta, è quello dell'uso della porta `submission`=587 oppure `smtps`=465. Invece di aggiungere

1 Si veda ad esempio *Gestire Certificati Digitali con openssl*, ICTSecurity 18, Novembre 2003.

`permit_sasl_authenticated` ad `smtpd_recipient_restrictions`, si può modificare il file `/etc/postfix/master.cf` come indicato in Tabella 4. In questo modo postfix accetterà la posta autenticata solo sulle porte 587 e 465, mentre sulla porta 25 fa relay solo per i clienti MUA interni. Si noti che sulla porta 465 è attivato un TLS-wrapping usato da Outlook Express.

Configurazione del client

Infine consideriamo la configurazione del client MUA. In realtà in questo caso c'è ben poco da fare, se il client supporta l'invio tramite TLS e autenticato, basta inserire gli opportuni parametri nella pagina di configurazione, si veda la Fig. 1 per un esempio con Evolution, e caricare il certificato della CA che ha firmato il certificato del server SMTP se questo non fosse già presente, si veda la Fig. 2.

Andrea Pasquinucci
pasquinucci@ucci.it

Riferimenti Bibliografici

[1] SSLv3.0: http://wp.netscape.com/eng/ssl3/
[2] TLSv1.0 descritto in RFC-2246
[3] openssl: http://www.openssl.org/
[4] SASL: descritto in RFC-2222, RFC-2444
[5] RFC-2554 smtp-auth, RFC-2487 smtp-starttls, RFC-2476 smtp-submission
[6] postfix: http://www.postfix.org/
[7] una implementazione di SASL: http://asg.web.cmu.edu/sasl/sasl-library.html
[8] evolution: http://www.novell.com/products/desktop/features/evolution.html,
http://gnome.org/projects/evolution/

```
#TLS
smtpd_tls_key_file = /etc/postfix/postfix-server.key
smtpd_tls_cert_file = /etc/postfix/postfix-cert.pem
smtpd_tls_CAfile = /etc/postfix/CA.pem
smtpd_use_tls = yes
smtpd_tls_loglevel = 2
smtpd_tls_received_header = yes
```

Tabella 1. Configurazione TLS per postfix in /etc/postfix/main.cf

```
pwcheck_method: saslauthd
# this limits announced AUTH mechanisms to only these
mech_list: plain login
```

Tabella 2. Configurazione di SASL in /usr/lib/sasl2/smtpd.conf

```
# SASL
smtpd_sasl_auth_enable = yes
broken_sasl_auth_clients = yes
# do AUTH only if protected by TLS
smtpd_tls_auth_only = yes
# Relay internal clients and AUTH clients
smtpd_recipient_restrictions = permit_mynetworks,
    permit_sasl_authenticated,
    reject_unauth_destination
```

Tabella 3. Configurazione SASL per postfix in /etc/postfix/main.cf

```
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (50)
# ==========================================================================
smtps     inet  n       -       y       -       -       smtpd -o\
                      smtpd_tls_wrappermode=yes -o smtpd_sasl_auth_enable=yes
submission inet n       -       y       -       -       smtpd -o\
                      smtpd_enforce_tls=yes -o smtpd_sasl_auth_enable=yes
```

Tabella 4. Configurazione porte di relay sicuro in /etc/postfix/master.cf

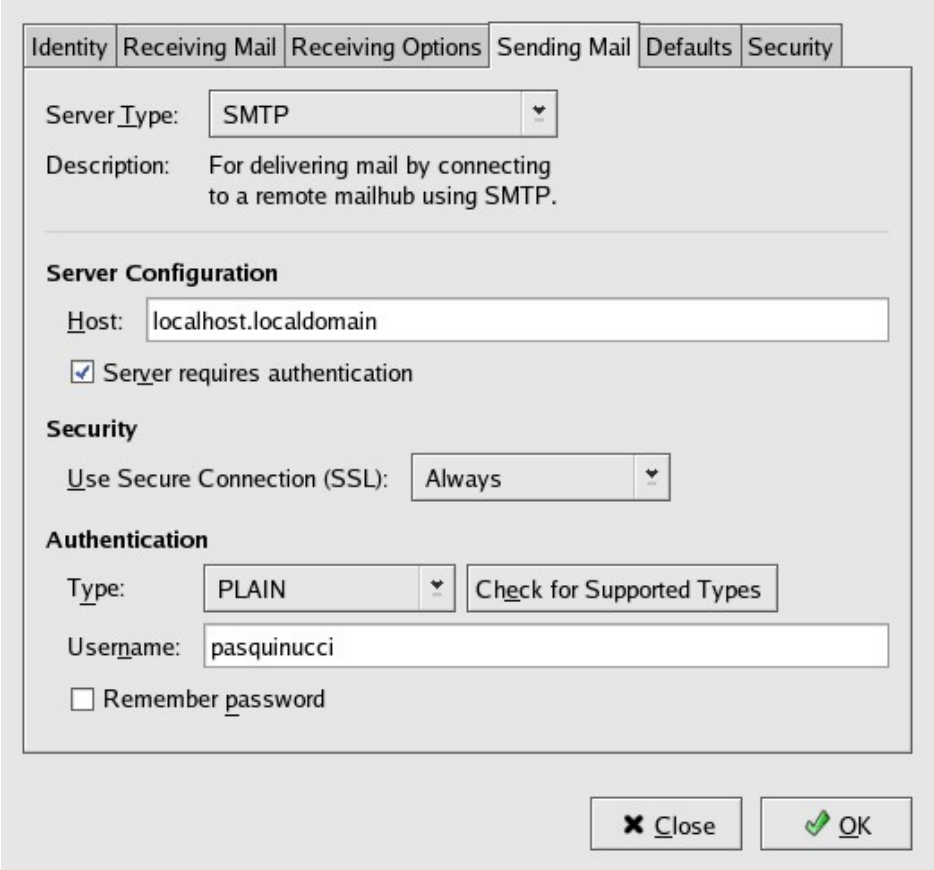

Figura 1. Configurazione dell'autenticazione in invio in Evolution

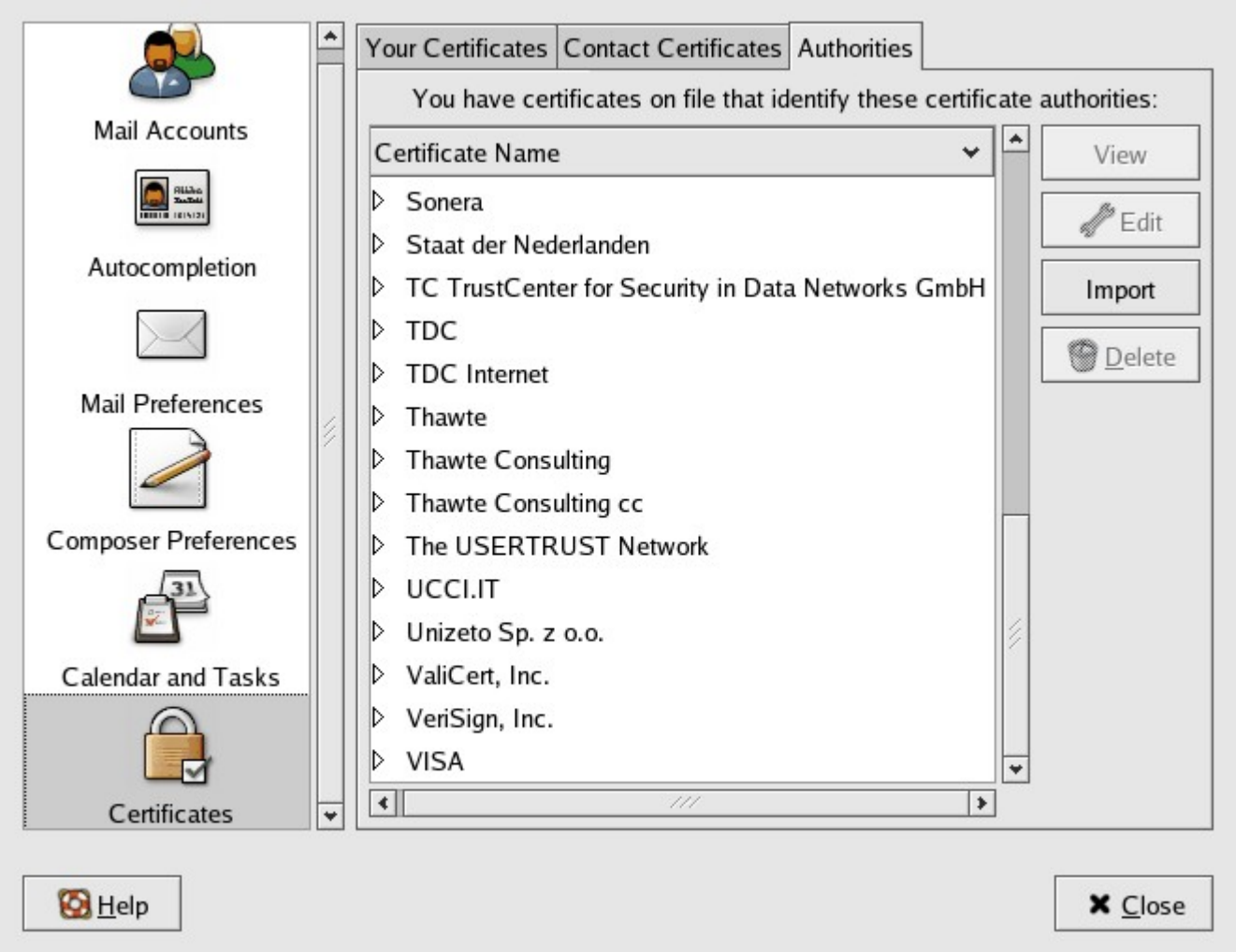

Figura 2. Inserimento di una nuova CA in Evolution