NAME

tlsproxy − Postfix TLS proxy

SYNOPSIS

tlsproxy [generic Postfix daemon options]

DESCRIPTION

The **tlsproxy**(8) server implements a server−side TLS proxy. It is used by **postscreen**(8) to talk SMTP−over−TLS with remote SMTP clients that are not whitelisted (including clients whose whitelist status has expired), but it should also work for non−SMTP protocols.

Although one **tlsproxy**(8) process can serve multiple sessions at the same time, it is a good idea to allow the number of processes to increase with load, so that the service remains responsive.

PROTOCOL EXAMPLE

The example below concerns **postscreen**(8). However, the **tlsproxy**(8) server is agnostic of the application protocol, and the example is easily adapted to other applications.

After receiving a valid remote SMTP client STARTTLS command, the **postscreen**(8) server sends the remote SMTP client endpoint string, the requested role (server), and the requested timeout to **tlsproxy**(8). **postscreen**(8) then receives a "TLS available" indication from **tlsproxy**(8). If the TLS service is available, **postscreen**(8) sends the remote SMTP client file descriptor to **tlsproxy**(8), and sends the plaintext 220 greeting to the remote SMTP client. This triggers TLS negotiations between the remote SMTP client and **tlsproxy**(8). Upon completion of the TLS−level handshake, **tlsproxy**(8) translates between plaintext from/to **postscreen**(8) and ciphertext to/from the remote SMTP client.

SECURITY

The **tlsproxy**(8) server is moderately security−sensitive. It talks to untrusted clients on the network. The process can be run chrooted at fixed low privilege.

DIAGNOSTICS

Problems and transactions are logged to **syslogd**(8).

CONFIGURATION PARAMETERS

Changes to **main.cf** are not picked up automatically, as **tlsproxy**(8) processes may run for a long time depending on mail server load. Use the command "**postfix reload**" to speed up a change.

The text below provides only a parameter summary. See **postconf**(5) for more details including examples.

STARTTLS SUPPORT CONTROLS

tlsproxy_tls_CAfile ($smtpd_tls_CAfile)

A file containing (PEM format) CA certificates of root CAs trusted to sign either remote SMTP client certificates or intermediate CA certificates.

tlsproxy_tls_CApath ($smtpd_tls_CApath)

A directory containing (PEM format) CA certificates of root CAs trusted to sign either remote SMTP client certificates or intermediate CA certificates.

tlsproxy_tls_always_issue_session_ids ($smtpd_tls_always_issue_session_ids)

Force the Postfix **tlsproxy**(8) server to issue a TLS session id, even when TLS session caching is turned off.

tlsproxy_tls_ask_ccert ($smtpd_tls_ask_ccert)

Ask a remote SMTP client for a client certificate.

tlsproxy_tls_ccert_verifydepth ($smtpd_tls_ccert_verifydepth)

The verification depth for remote SMTP client certificates.

tlsproxy_tls_cert_file ($smtpd_tls_cert_file)

File with the Postfix **tlsproxy**(8) server RSA certificate in PEM format.

tlsproxy_tls_ciphers ($smtpd_tls_ciphers)

The minimum TLS cipher grade that the Postfix **tlsproxy**(8) server will use with opportunistic TLS encryption.

tlsproxy_tls_dcert_file ($smtpd_tls_dcert_file)

File with the Postfix **tlsproxy**(8) server DSA certificate in PEM format.

tlsproxy_tls_dh1024_param_file ($smtpd_tls_dh1024_param_file)

File with DH parameters that the Postfix **tlsproxy**(8) server should use with non−export EDH ciphers.

tlsproxy_tls_dh512_param_file ($smtpd_tls_dh512_param_file)

File with DH parameters that the Postfix **tlsproxy**(8) server should use with export−grade EDH ciphers.

tlsproxy_tls_dkey_file ($smtpd_tls_dkey_file)

File with the Postfix **tlsproxy**(8) server DSA private key in PEM format.

tlsproxy_tls_eccert_file ($smtpd_tls_eccert_file)

File with the Postfix **tlsproxy**(8) server ECDSA certificate in PEM format.

tlsproxy_tls_eckey_file ($smtpd_tls_eckey_file)

File with the Postfix **tlsproxy**(8) server ECDSA private key in PEM format.

tlsproxy_tls_eecdh_grade ($smtpd_tls_eecdh_grade)

The Postfix **tlsproxy**(8) server security grade for ephemeral elliptic−curve Diffie−Hellman (EECDH) key exchange.

tlsproxy_tls_exclude_ciphers ($smtpd_tls_exclude_ciphers)

List of ciphers or cipher types to exclude from the **tlsproxy**(8) server cipher list at all TLS security levels.

tlsproxy_tls_fingerprint_digest ($smtpd_tls_fingerprint_digest)

The message digest algorithm to construct remote SMTP client−certificate fingerprints.

tlsproxy_tls_key_file ($smtpd_tls_key_file)

File with the Postfix **tlsproxy**(8) server RSA private key in PEM format.

tlsproxy_tls_loglevel ($smtpd_tls_loglevel)

Enable additional Postfix **tlsproxy**(8) server logging of TLS activity.

tlsproxy_tls_mandatory_ciphers ($smtpd_tls_mandatory_ciphers)

The minimum TLS cipher grade that the Postfix **tlsproxy**(8) server will use with mandatory TLS encryption.

tlsproxy_tls_mandatory_exclude_ciphers ($smtpd_tls_mandatory_exclude_ciphers)

Additional list of ciphers or cipher types to exclude from the **tlsproxy**(8) server cipher list at mandatory TLS security levels.

tlsproxy_tls_mandatory_protocols ($smtpd_tls_mandatory_protocols)

The SSL/TLS protocols accepted by the Postfix **tlsproxy**(8) server with mandatory TLS encryption.

tlsproxy_tls_protocols ($smtpd_tls_protocols)

List of TLS protocols that the Postfix **tlsproxy**(8) server will exclude or include with opportunistic TLS encryption.

tlsproxy_tls_req_ccert ($smtpd_tls_req_ccert)

With mandatory TLS encryption, require a trusted remote SMTP client certificate in order to allow TLS connections to proceed.

tlsproxy_tls_security_level ($smtpd_tls_security_level)

The SMTP TLS security level for the Postfix **tlsproxy**(8) server; when a non−empty value is specified, this overrides the obsolete parameters smtpd_use_tls and smtpd_enforce_tls.

Available in Postfix version 2.11 and later:

tlsmgr_service_name (tlsmgr)

The name of the **tlsmgr**(8) service entry in master.cf.

OBSOLETE STARTTLS SUPPORT CONTROLS

These parameters are supported for compatibility with **smtpd**(8) legacy parameters.

tlsproxy_use_tls ($smtpd_use_tls)

Opportunistic TLS: announce STARTTLS support to remote SMTP clients, but do not require that clients use TLS encryption.

tlsproxy_enforce_tls ($smtpd_enforce_tls)

Mandatory TLS: announce STARTTLS support to remote SMTP clients, and require that clients use TLS encryption.

RESOURCE CONTROLS

tlsproxy_watchdog_timeout (10s)

How much time a **tlsproxy**(8) process may take to process local or remote I/O before it is terminated by a built−in watchdog timer.

MISCELLANEOUS CONTROLS

config_directory (see 'postconf -d' output)

The default location of the Postfix main.cf and master.cf configuration files.

process_id (read−only)

The process ID of a Postfix command or daemon process.

process_name (read−only)

The process name of a Postfix command or daemon process.

syslog_facility (mail)

The syslog facility of Postfix logging.

syslog_name (see 'postconf -d' output)

The mail system name that is prepended to the process name in syslog records, so that "smtpd" becomes, for example, "postfix/smtpd".

SEE ALSO

postscreen(8), Postfix zombie blocker
smtpd(8), Postfix SMTP server
postconf(5), configuration parameters
syslogd(5), system logging

LICENSE

The Secure Mailer license must be distributed with this software.

HISTORY

This service was introduced with Postfix version 2.8.

AUTHOR(S)

Wietse Venema
IBM T.J. Watson Research
P.O. Box 704
Yorktown Heights, NY 10598, USA