Software Product Description

PMDF-TLS

Overview

PMDF-TLS implements the Transport Layer Security (TLS) protocol of RFC- 2246 for PMDF's servers and clients. Transport Layer Security is currently supported for:

- SMTP
- IMAP
- POP3
- HTTP
- LDAP

PMDF-TLS provides a secure data stream between the client and the server ensuring the data that is exchanged between your system and a remote system using TLS will be protected from others on the network. PMDF-TLS is compatible with SSL (Secure Socket Layer) and PMDF-TLS is fully compatible with SSL-enabled clients.

Since the encryption is negotiated between the SMTP client and server at each session, no prior agreements need to be entered in order for an SMTP session to be secured cryptographically. PMDF-TLS-enhanced SMTP servers can "discover" other SMTP servers supporting TLS and automatically create secure message paths. This implements an MTA-to-MTA level security environment that ensures the message path between end point messaging servers is secured from attack even if the message path is subject to a potentially hostile environment.

You can configure PMDF to require that clients use encrypted connections to the servers. This requirement can be restricted to the external network, if desired. You can allow external users to connect to internal messaging servers and maintain overall system security. This allows you to use the services of an Internet Service Provider for dial-in connections to messaging servers.

Description

There are two modes of operation that PMDF-TLS supports:

1. Connecting to a TLS-enabled port where TLS negotiation happens immediately once the TCP connection has been established.
2. Connecting to a "regular" port and then issuing a STARTTLS command to begin TLS negotiation.

The only difference between these two modes is when the TLS negotiation happens. In both cases, once the TLS negotiation is complete, all subsequent data sent across the TCP connection will be secure. Connecting to a special port number is the more commonly used way to connect to a TLS-enabled server. SMTP, IMAP, HTTP, and POP3 all have established ports for use with TLS (port numbers 465, 993, 443, and 995, respectively). When a client connects to one of these special ports (as configured in the Dispatcher configuration file), PMDF- TLS begins TLS negotiations immediately.

Once the negotiation is complete, the connection will be given to the service as usual.

In the case that a STARTTLS command is used, the TCP connection is established on the usual port number (or an alternate port number if configured in the Dispatcher) and given to the service in the usual way. If TLS is available to the client, the server advertises STARTTLS as one of its available extensions. The client then issues the STARTTLS command, the server acknowledges receipt of the command and instructs the client to begin TLS negotiation. Again, once the negotiation is complete, the connection continues normally.

In addition to the added support for the SMTP, POP, HTTP, IMAP, and LDAP use of TLS services, PMDF-TLS comes with a set of utilities that support PMDF secure messaging services:

- `tls_certreq` - is used to generate a public key pair and a certificate request.
- `tls_certdump` - decodes the binary files that contain certificates used by PMDF.
- `tls_ciphers` - lists the ciphers avail-able for use with PMDF-TLS.

RFC Support

Title	RFC Number
The TLS Protocol Version 1.0	2246
SMTP Service Extension for Secure SMTP over TLS	2487
Internet X.509 Public Key Infrastructure	2459
Using TLS with IMAP, POP3, and ACAP	2595

Encryption Strength

PMDF-TLS supports all modern encryption algorithms, with a key strength up to 1024 bits.

Hardware Requirements

PMDF-TLS supports any valid OpenVMS or Linux configuration.

Software Requirements

One of the following operating system environments is required:

- RedHat Enterprise Linux 6 or higher
- OpenVMS Alpha 7.3 or higher
- OpenVMS Integrity 8.2 or higher

Services, Documentation, and Ordering Information

Technical Services

Process Software's Technical Services Program has a well-deserved reputation for excellence. Services include consulting, training, software maintenance, support, online resources, and 24-hour support - in short, everything you need to keep your Process Software products and your network operating at peak efficiency.

Consulting

A comprehensive suite of programs is available on a host of topics, including PMDF installation and configuration, network security, troubleshooting, and others.

Hot Line Support

Networking experts are available by telephone and e-mail. Optional 24-hour support is also available.

Updates

All maintenance customers with current service contracts receive automatic software and documentation updates of major releases.

Training

A wide range of educational services can be provided at your site, at regional training locations throughout North America, or at our own training facility in Framingham, MA.

Documentation

Comprehensive documentation for all PMDF products includes user guides, installation and configuration information, management functions and utilities, programming facilities, and network security. Documentation in HTML and PDF format is included on your product CD, and is also available on Process Software's web site, www.process.com.

You can find Frequently Asked Questions (FAQs) in the Support section of the Process Software web site.

Ordering Information

PMDF is shipped on CD-ROM and available for download from Process Software. Contact sales@process.com or request a free evaluation on the Process Software web site at www.process.com.

About Process Software

Process Software is a premier supplier of infrastructure software solutions to mission critical environments. We deliver customer-centric and innovative IP-based technologies to our customers worldwide, and provide them with superior customer support and service.

Process Software
959 Concord Street
Framingham, Massachusetts 01701-4682

Telephone:	
U.S./Canada	1- (800) 722-7770
International	1- (508) 879-6994
FAX:	1- (508) 879-0042
Web:	http://www.process.com
E-mail:	info@process.com

The information contained in this document is subject to change without notice. Process Software assumes no responsibility for any errors that may appear in this document.