

Overview

The *passIT* software is a specialized, Java-based web server running a single application for mortgage and loan tracking. Access to the application and its data is restricted to pre-defined users within the application. The *passIT* software is installed as a stand-alone application into a single directory on the server.

In order to support SSL traffic over HTTP (HTTPS), a separate web server, such as Apache, must be installed to terminate the SSL connection with the end-user browser. The web server can then be used as an HTTP proxy for all requests to the *passIT* software. This means all traffic between the end-user browser and the web server is encrypted with the SSL protocol, but all local server traffic is unencrypted HTTP traffic.

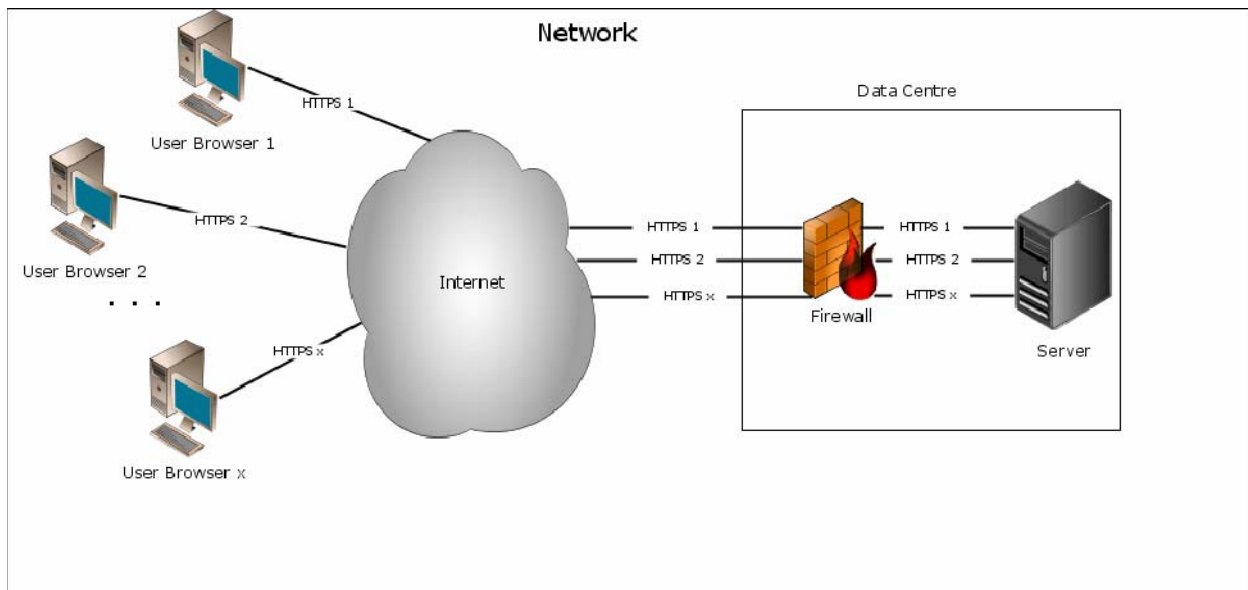


Figure 1

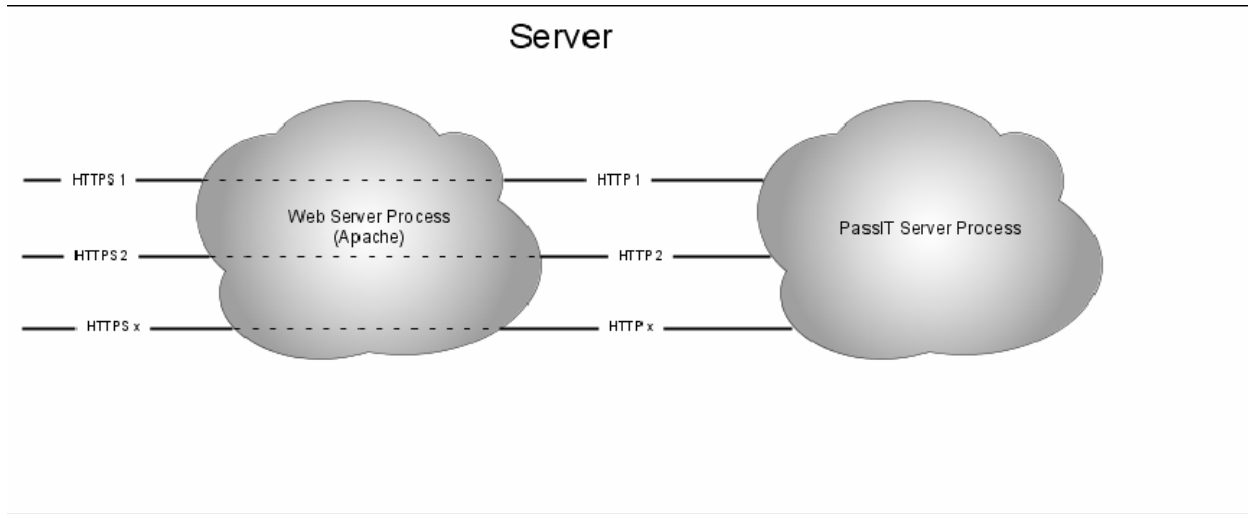


Figure 2

Operations

Hosting Environment

The *passIT* software handles highly sensitive data. Therefore, the configuration of the software and hosting hardware must be extremely secure in order to protect the data. A secure hosting environment is achieved by using the following hardware configuration:

Item	Provided By	Details
Data Centre Space	Hosting Provider	<ul style="list-style-type: none"> • multi-homed with access to Tier 1 backbones • protected against power failure by employing multiple UPS units and generator backup power • 24/7 surveillance by onsite security personnel • 24/7 video camera surveillance • 24/7 server monitoring and technical support • gas fire suppression system • computer grade air conditioning and humidity control systems
Server	Hosting Provider	<ul style="list-style-type: none"> • managed server • Linux running kernel ≥ 2.6 (any distribution) • Sun Java SE Development Kit ≥ 1.5 • ≥ 2 GB memory • ≥ 4 GB swap space

		<ul style="list-style-type: none"> • >= 100 GB disk space • >= 2 CPUs running at >= 2.5 GHz
Firewall	Hosting Provider	<ul style="list-style-type: none"> • allow all outgoing traffic from the server • restrict incoming traffic to the following ports: <ul style="list-style-type: none"> ○ 22 – SSH for encrypted, remote server management and software updates ○ 443 – HTTPS for encrypted SSL based web traffic used by customers to access the software
SSL Certificate	Steward Software or Customer	<ul style="list-style-type: none"> • wildcard SSL certificate shared by all <i>passIT</i> installations on a server • customer can choose to purchase their own SSL certificate, which allows them to use their own, unique domain name in all web-based requests • Steward Software purchases SSL certificates from Entrust. However, customers may purchase an SSL certificate from any authorized SSL certificate authority.

Software Configuration

The *passIT* software is a Java-based web server which runs a single application for mortgage and loan tracking. Every installation of the software is specific to an individual customer.

Installation

- The *passIT* software is installed into a unique directory on the file system for each customer.
- The software is configured to run on a unique port per installation.
- Each installation directory is owned by a unique userid dedicated to the customer and the permissions on the installation directory are restricted to the userid and its group, which is also unique to the customer. The *passIT* software is executed using the permissions of the customer userid and group. This ensures each installation of the *passIT* software has no ability to access or alter any other installation of the *passIT* software on the file system.

Web Server

- Apache is installed on the server, with the `mod_ssl` module enabled. The `mod_ssl` module enables Apache to communicate using SSL encrypted data, using the HTTPS protocol.

- Apache is configured to load up the SSL certificate associated with every *passIT* software installation on the server.
- Apache examines all incoming HTTPS web-based requests and applies the appropriate SSL certificate. The web request will contain a fully qualified hostname. Apache uses the full qualified hostname to determine the SSL certificate. Apache then forwards, or proxies, the web request as unencrypted HTTP traffic to the correct port for the customer's *passIT* installation. This is not a security issue because the traffic is contained on the server, and customers do not have login access to the server. The *passIT* software is able to accept the incoming HTTP requests as if it is communicating directly with the end-user. Apache sends all responses back to the customer over the initial HTTPS encrypted connection. Therefore, all web-based traffic between the end-user and the Apache web server process is encrypted using SSL.

Security

- The *passIT* software restricts access to the software by only allowing users in its user database to log into the application. When the end-user initially accesses the software using a web browser, they are presented with a login screen, asking for a userid and password. The user must type in a userid and password from the user database in order to be logged into the *passIT* application.
- Every *passIT* installation must contain at least one userid with administration privileges. The administrative userid has the ability to create and delete users in the user database. The administrative userid has the ability to grant and revoke access to various elements of the software to each userid. It is also possible to set up "groups" of users, which allows users to share access rights within the software.