



Snorkel-TX

Feature Highlights & Technical Specifications

Odyssey Technologies Ltd.

Snorkel TX - Feature Highlights & Technical Specifications

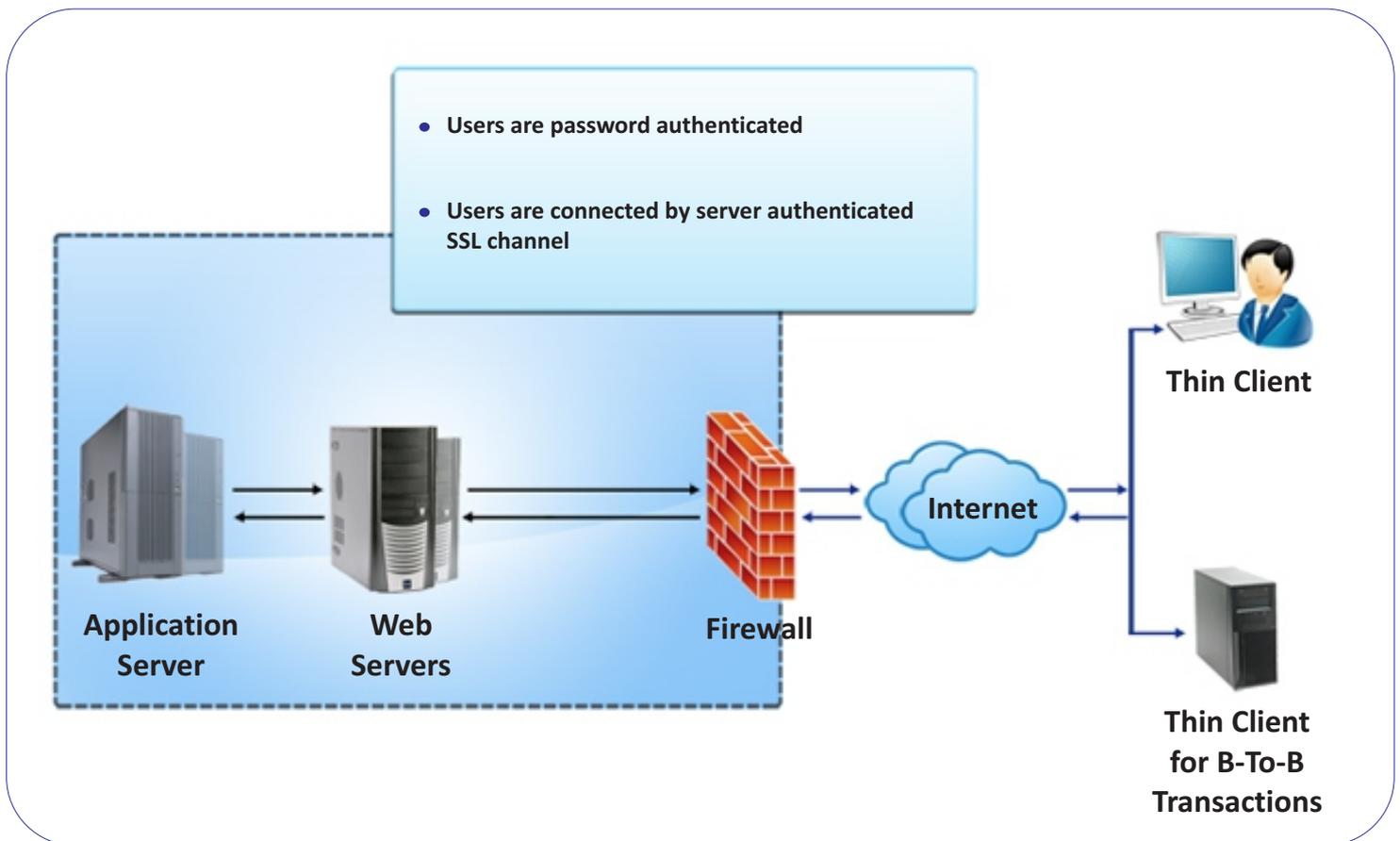


Snorkel-TX is a powerful transaction security server that enables failsafe authentication, access control, non-repudiation and integrity for web applications.

Server Positioning

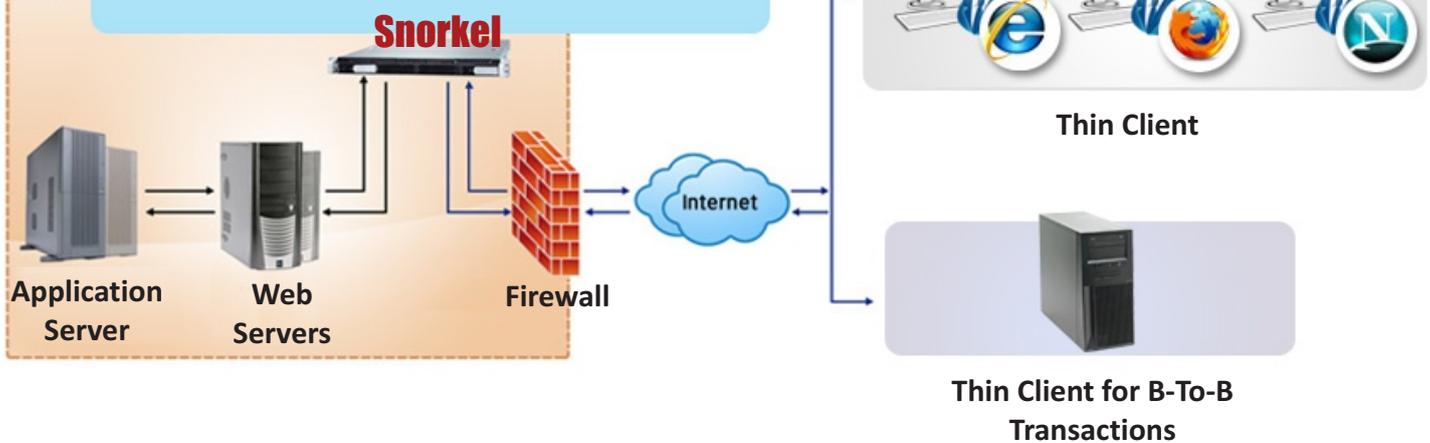
Snorkel-TX server is logically positioned between the web application and Internet so that all requests to the backend application pass through Snorkel. The solution requires no integration with the application server, and therefore requires no change to the application code-base, web server, or database. This allows the application and rest of the IT infrastructure to be upgraded or changed in the future without affecting the security of the web service.

Web application before Snorkel placement



Web application after Snorkel placement

- Users protected by two levels of authentication (Password and digital certificates/one time passwords).
- Users are connected to application by server and client authenticated SSL channel
- Digital Signatures are enforced for individual URLs, forms and file uploads to provide accountability
- Users have varying levels of access to backend applications based on policy and configuration



Two-factor Authentication

Certificate-based authentication

- *Support for all X.509 digital certificates*
 - Snorkel issued digital certificate
 - Third Party issued digital certificate
 - Self-signed digital certificate
- *Multiple end-user registration options*
 - End-users can register themselves with Snorkel by clicking a link on the website
 - Administrators can add individual users
 - Administrators can add users in bulk from a csv file

Snorkel TX - Feature Highlights & Technical Specifications



- **Multiple authentication mechanisms supported simultaneously**

- End-users can move to certificate-based authentication at their convenience
- Password-based users, and certificate-based users can co-exist.

- **Multiple key carriage options**

- Browser Stores
- Crypto Smart Cards
- USB Crypto Tokens
- PKCS #12 files

One Time Password Solutions

- **Multiple OTP options**

- SMS based OTP
- Token based OTP
- Software based OTP
- Mobile based OTP

Access Control

- Access to specific applications based on username/user group
- Access to specific application URLs based on username/user group

Channel Security

- Easily shift between secure and non-secure connection, based on URL
- Choose between client-authenticated and non-client authenticated SSL

Snorkel TX - Feature Highlights & Technical Specifications



- Protocols supported include:
 - **SSL V2**
 - **SSL V3**
 - **TLS**

Accountability

- Enforce digital signatures for user transactions, forms submissions and file uploads.
- Enforce digital signature for all administrator activities.
- Enable users to transact securely even on the move. Key carriage options include:
 - **Browser Stores**
 - **Crypt Smart Cards**
 - **USB Crypto Tokens**
 - **PKCS #12 files**

Digital Signatures

- Digital signing and verification of submitted forms, and file uploads.
- Archival of digital signatures with context preservation, for offline verification and retrieval.
- Signatures stored in PKCS #7 format.

Encryption

- Secure communication using SSL V3/TLS, with server and client authentication.

Administration

- Policy driven, multi-tiered administration.
- Secure web-based administration with strong two factor authentication.
 - Password-based
 - Digital certificate based

Snorkel TX - Feature Highlights & Technical Specifications



- Encrypted communication channel (SSL V3)
- Signing and archival of all administrator activities for accountability.
- Administrator dashboards for real-time administration
 - Monitor system performance
 - Monitor user activity
- Comprehensive reports of all successful logins, failed logins, administrator activity, user activity, transactions, and digital signatures.
- High availability with options for hot and cold standby.

Comprehensive web-based reporting system

- Reports accessible from anywhere on the web
- Tamper evident logs
- Easy filter-based logs retrieval
- Offline reports available in XML and CSV formats for downstream processing
Online and offline verification of stored signatures

Report Format

Online	HTML
Offline	XML, CSV

Report Filters

Time-wise	Signatures	User-wise	Administrator-wise
<ul style="list-style-type: none">Administrator loginsAdministrator activitiesUser loginsUser activities and transactions	<ul style="list-style-type: none">Administrator loginsAdministrator activitiesUser loginsUser transactions	<ul style="list-style-type: none">User loginsUser transactionsUser key historyUser track record	<ul style="list-style-type: none">Administrator loginsAdministrator activitiesAdministrator key history and track record

• Backup

- Option to move signatures to long-term storage
- Scheduled back-ups
- Hot standby for high availability



• Purging

- Scheduled purging
- Low-level purging mechanism to prevent data restoration



ODYSSEY TECHNOLOGIES LTD.

5th Floor, Dowlath Towers, 63, Taylors Road, Kilpauk,
Chennai - 600 010, India.
Tel : +91 44 26450082, 26450083, 43084070, 43084080
e-mail: info@odysseytec.com