

SafeConduct™

Connectivity Security for New and Legacy Systems



A BackOffice Associates, LLC Company

SafeConduct™

SSL Standard

SafeConduct delivers the benefits of Secure Sockets Layer (SSL) v3.0 encryption, including digital certificate authentication and 256-bit data encryption, to your data traffic over VPN or the Internet. The SafeConduct product family transparently works with new and legacy applications. Using SSL, the most widely used protocol for security data transmission on the Internet, SafeConduct eliminates significant risk in information security and privacy.

Secure Channel

SafeConduct builds an invisible, secure channel between two TCP/IP nodes. Before any application data traffic is sent, SafeConduct authenticates the machines, securely negotiates encryption keys, transmits secured user ID/password data, and finally transmits secured application data between the two nodes. SafeConduct prevents unauthorized machines from accessing applications. It also prevents unauthorized access to any application data transmitted over TCP/IP networks.

SafeConduct monitors and intercepts TCP/IP data at pre-configured port addresses. Once secure communication is established between the two TCP/IP nodes, SafeConduct routes application data traffic to the true destination application port address. SafeConduct Server may be installed on a machine other than the one of the server application in order to redirect requirements for SSL encryption processing.

Server and Client for all platforms

The SafeConduct product family includes the SafeConduct Server, SafeConduct Windows Client, and the SafeConduct Java Client. The SafeConduct Windows client runs on client and server platforms as an application or service. The SafeConduct Java Client and the SafeConduct Server can be used on multiple client and server platforms including, but not limited to, Linux, Solaris, Windows, IBM OS/390 and z/OS, IBM i/iSeries/AS400, IBM AIX, Mac OSX, and OS/2.

Key Features

- SSL and TLS standard
- 256-bit SSL data encryption
- NIST FIPS 140-2 validated crypto and SSL functions
- Real-time node-to-node authentication
- Support for corporate digital certificates
- Transparency, no application source code changes necessary
- Broad platform support via Java and Windows components
- Support for any TCP/IP based legacy application architectures including client/server, host-terminal, multi-tier, and multi-cast
- Remote administration server termination control
- Easy configuration and setup

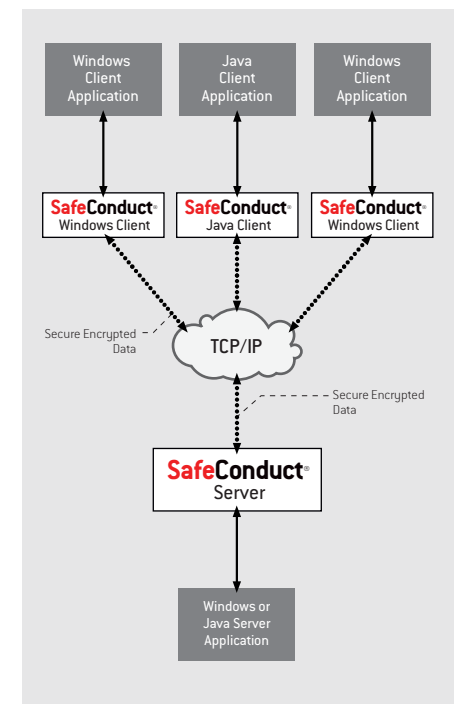
System Requirements

Server

- Any platform with Java Run-time Environment 1.3 and later functions

Client

- Any platform with Java Run-time Environment 1.3 and later functions
- Windows 2008/2003/XP/2000/NT



HiT Software, Inc., A BackOffice Associates, LLC Company

T +1 408.345.4001 F: +1 408.345.4899 info@hitsw.com www.hitsw.com

Copyright © 2012 HiT Software, Inc., A BackOffice Associates, LLC Company. All rights reserved. HiT Software®, HiT Software Logo and SafeConduct are trademarks of HiT Software and BackOffice Associates, LLC in the United States and other countries. All other trademarks are the property of their respective owners. 1002-11500-102_b

BackOffice
ASSOCIATES