



SafeConduct™

Application access security for new and legacy systems

SSL Standard

SafeConduct brings benefits of the **Secure Sockets Layer (SSL) v3.0** standard, including digital certificate authentication and 128-bit data encryption, to any point-to-point Internet or VPN application data traffic. 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 information security and privacy risks.

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. Since the SafeConduct Server also offers proxy support, it may be installed on a machine other than the actual application server 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 can be used on multiple client and server platforms including, but not limited to, Linux, Solaris, Windows, IBM OS390 and zOS, IBM iSeries/AS400, IBM AIX, Mac OSX, and OS/2. The SafeConduct Server can similarly be used on multiple client and server platforms.

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

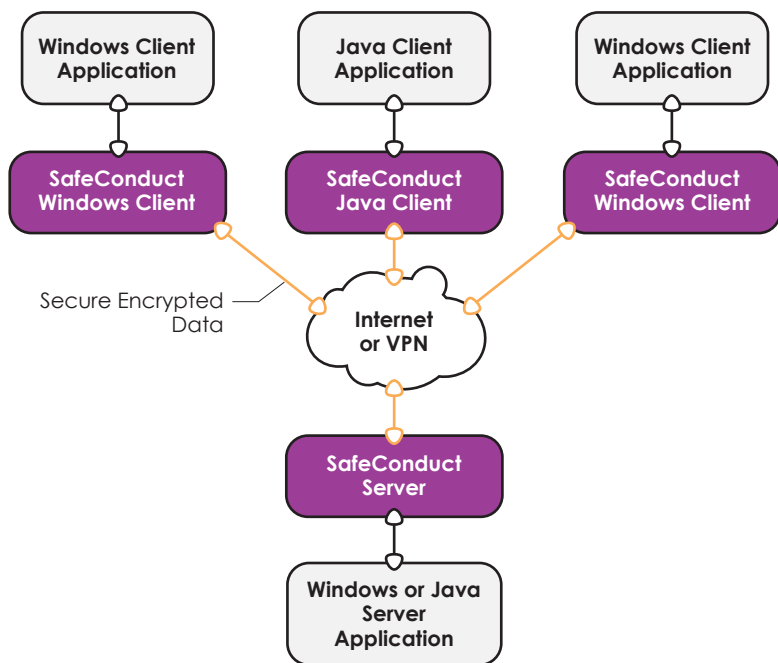
System Requirements:

Server

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

Client

- Any platform with Java Run-time Environment 1.3 and later or
- Windows 2003/XP/2000/NT/ME/98



HiT Software, Inc. • www.hitsw.com

phone: 1-408-345-4001 • fax: 1-408-345-4899 • e-mail: info@hitsw.com

HiTSOFTWARE
Open Up Your Data