

Key Benefits



- Works within existing firewalls and DMZs
- Protects internal systems from inbound threats
- Controls inbound FTP and HTTP messages
- Hides internal systems during outbound messaging
- Controls outbound FTP and HTTP messages
- Provides user management, authentication and SSL certificate management

Meet the most demanding security requirements

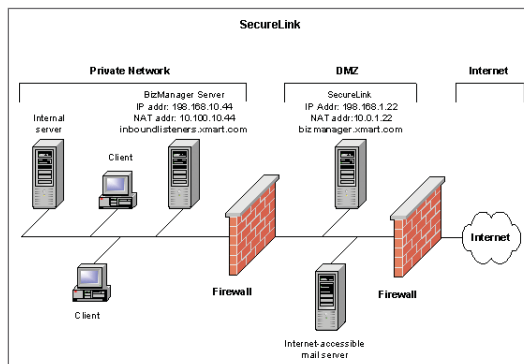
With today's renewed emphasis on protecting sensitive data and infrastructures, more and more private, public and government organizations are implementing advanced security solutions. Inovis SecureLink™ fulfills the strict security requirements of financial, healthcare and government institutions, and the most demanding security requirements of suppliers and retailers in the supply chain.

Protect the integrity of your data

SecureLink is designed to work in conjunction with BizManager™ to securely relay messages received from and sent to your trading partners. A comprehensive set of advanced security components, SecureLink protects internal systems from external threats. With SecureLink, companies can safely and securely participate in business-to-business integration (B2Bi) and the secure exchange of information over the Internet.

Industry standards such as EDI-INT AS2 and ebXML provide ways to send data packages securely over the Internet, while technologies such as Secure Sockets Layer (SSL) provide secure tunnels through which to send those data packages. SecureLink works with these standards and technologies, providing a secure gateway so that all inbound and outbound HTTP and FTP data can pass through a single, secure and manageable solution.

SecureLink resides within the DMZ and works with BizManager to provide a single, secure gateway for all inbound and outbound data.



SecureLink incorporates configurable security rules and services that regulate the inbound and outbound flow of electronic messages exchanged over the Internet via secure transport standards that include AS2, ebXML, NAESB, EBMX, Web Services, secure HTTP and secure FTP.

SecureLink Configurator

The configurator is an easy-to-use and intuitive graphical user interface (GUI) for configuring, managing and administering setup and configuration information within SecureLink.

Certificate Administration

The Certificate Administration function allows you to manage internal private keys and unlimited trusted keys for SecureLink.

User management and authentication

All user information is encrypted for security, giving you complete control over who can view sensitive data:

- SecureLink users are setup for HTTP/Tomcat configuration management with user authentication.
- SecureLink FTP server users are setup primarily for external user access with a logon and user authentication. Users can be restricted to a specific directory/folder.

Integrated secure FTP server

An integrated FTP server provides important infrastructure support within the DMZ, and complements other SecureLink components to provide a one-stop DMZ infrastructure solution. The SecureLink FTP server also provides complete support for Inovis BizManager solutions, including AS2 asynchronous Message Disposition Notifications (MDNs) and FTP-based agents.

SecureLink™

SUPPORTED PLATFORMS

- IBM AIX
- HP-UX
- Sun Solaris
- Red Hat Linux
- Microsoft Windows

FTP Proxy

The FTP proxy enables BizManager BizLink™ users to securely relay files via FTP connections between clients and servers. This proxy is bidirectional, which means that it is able to relay inbound and outbound FTP traffic. The SecureLink FTP proxy is a valuable tool for relaying outbound FTP traffic, especially in a restrictive firewall environment and/or when the target FTP server does not support passive mode of data transfer.

HTTP proxy

An HTTP reverse proxy service allows the relay of messages from outside the firewall to a computer running a messaging server (i.e. BizLink) in the protected zone. An HTTP forward proxy is an intermediate server located between the internal source and the external target server that relays outbound connections/messages, and hides a client from an external target server.

SecureLink Outpost Redirector

SecureLink Outpost Redirector extends the solution by supporting two key security tenets:

- No external party can push data/files directly to internal systems via open ports
- No data/files are stored on a server in the DMZ, not even temporarily

Outpost Redirector is used where security policies do not allow inbound connections from the DMZ into the enterprise, providing seamless tunneling of incoming HTTP-based messages.

Fallback and load balancing

Fallback capabilities provide fault tolerance, or the ability to route messages to backup/secondary BizLink Inbound Listener servers when the primary server is inaccessible. Load balancing provides for the even distribution of messages across a distributed BizLink installation so that

no single Inbound Listener is overwhelmed, creating a highly available environment. These protective features help direct inbound messages to ensure your back-end systems don't get backlogged and inbound documents don't fall through the cracks.

PRODUCT HIGHLIGHTS

- SecureLink Configurator
- Support for multiple HTTP-based message transports: AS2 EDI-INT, ebXML, EBMX, NAESB, Web Services, Web Apps
- Certificate administration and generation
- User management/authentication
- Integrated secure FTP server
- FTP reverse/forward proxy
- Named FTP server users
- Configurable FTP pull or push option
- Active or passive FTP
- FTP host masquerading
- FTP remote host verification
- FTP transparent gateway
- FTP support of TLS and SSL
- FTP clear or private data connections
- HTTP & JSP Servlet Engine (Tomcat)
- HTTP reverse/forward proxy
- AS2 asynchronous pull
- AS2 message validation
- SecureLink Outpost Redirector
- Fallback (fault tolerance)
- Load balancing (high availability)

For more information, visit www.inovis.com.