



Edge Security for Multi-Enterprise Data Exchanges using IBM Sterling Secure Proxy

Eswar Toleti (Practice Manager - MFT and B2B Integration)
Miracle Software Systems, Inc.

Edge Security!!

As global business become more and more inter-connected, traditional organization boundaries are being redefined and the exchange of data across these boundaries is increasing rapidly. With such openness being created, a malicious “denial-of-service” (or) “man-in-the-middle” attack could cause terrible damage to your organization and in turn erode the trust of your partner network. We’ve found in our experience that internal networks and legacy systems are more than often vulnerable due to insufficient file transfer security measures.

IBM Sterling Secure Proxy

IBM Sterling Secure Proxy is an application-based proxy that protects your internal network from malicious attacks that may negatively impact your business processes, both internally and externally with your trading partners. With IBM SSP, partner connections are intercepted at the edge and once authenticated are transparently redirected to trusted connections within your enterprise.

Nowadays security experts are turning to Proxy Server based approaches to ensure that internal systems can authenticate requests, terminate sessions and encrypt data and systems. This is exactly what IBM Sterling Secure Proxy provides for your global enterprise.

Why choose IBM SSP?

IBM Sterling Secure Proxy offers a unique solution to your data exchange security problems, which is both simple and powerful. With SSP you can enable the Internet with perimeter security for securely transferring data instead of using dedicated lines.

The IBM Sterling Secure Proxy Solution offers,

- Access Authentication for restricting unauthorized access
- Supports Single-On for integration into your enterprise architecture
- Provides enhanced Edge Security with a Defense-In-Depth strategy
- Rapid Trading Partner On-Boarding with Self-Service Management
- High Scalability in clustered models
- Secure Internet-based data exchange with your trading partners

Application Proxy

- Resides in demilitarized zone for providing Edge Security
- Supports IBM Sterling Connect:Direct, IBM Sterling Connect Express, IBM Sterling B2B Integrator and IBM Sterling File Gateway

- Compatibility with multiple DMZs (or) Layered architecture
- Supports FTP, FTPS, HTTP, SSH/SFTP, PeSIT and Sterling Connect:Direct Protocols
- Ability to use FIPS 140-2 compliant data encryption module

Firewall Navigation Best Practices

- Prevents in-bound holes in the firewall
- Restricts storage of files, data and credentials in the DMZ to prevent rich targets
- Enforces external and internal security policies
- Establishes sessions from more-trusted to less-trusted zones

Perimeter Security

- Prevents direct communications between external and internal sessions by establishing secure sessions breaks in the DMZ using SSL (or) TLS
- Enables configurable error handling for violations through protocol inspection
- Provides protection against DoS attacks with sessions limits and data encryption

Authentication Services

- Customizable portal enables trading partners to self-service password management
- Easy integration with existing security infrastructure including Active Directory and Tivoli Databases
- Supports Single-Sign On which enables integration with existing enterprise architecture
 - Multi-factor authentication provides strict control and authentication before being passed on to trusted zone
 - Ability to authenticate based on User Credentials, IP Address, Digital Certificates, SSH Keys and RSA SecureID

Clustering and Scalability

- Central Configuration Manager for managing and scaling multiple engines running in the DMZ
- High Availability and Load Balancing with clustering provides operational continuity

