IBM® Sterling Secure Proxy

Provide robust, auditable edge security for your multi-enterprise data exchanges

Benefits

- Enable trusted Business-to-Business transactions and file exchanges
- Secure your network at the edge, protecting your data, and internal systems
- Comply with security policy and more easily pass security audits

Enable trusted transactions

As global business becomes more and more inter-connected, exchange of information across organizational boundaries is expanding rapidly. IBM® Sterling Secure Proxy secures and shields your trusted network by preventing direct connectivity between external partners and internal servers. Partner connections for B2B transactions and file exchanges are intercepted at the edge and once authorized are transparently redirected to trusted connections within your enterprise.

Secure your network at the edge

Sterling Secure Proxy provides advanced edge security by enabling a defence-in-depth strategy. DMZ-based authentication, session breaks, and SSL termination at the edge prevent external parties from having direct access to trusted systems, regardless of the type or size of payload across a wide range of file transfer communications protocols. Configuration is managed in the trusted zone and no data is stored unencrypted in the DMZ, so your vital business files are secured from external parties.

Governance and compliance

Multiple levels of governance enable compliance with enterprise security policy. Comprehensive logging of security and configuration changes support routine reporting as well as detailed audits. Queued events enable monitoring and alerting for security failures and operational health of the proxy engine and for configuration changes. A fully integrated interface to external ID stores (such as LDAP) eliminates the need for duplicate stores, providing a single source for user and partner credentials. Interfaces to hardware security modules (HSMs) support use of these devices for key storage.

Operational management

Multiple Sterling Secure Proxy engines may be deployed in the DMZ for traffic separation, load balancing, or capacity management. A Configuration Manager console is provided for creation and management of all proxy configuration objects and for managing the proxy engine(s) in the DMZ. Administration is simplified through the ability to load a single configuration set onto multiple proxy engines.

In addition, a full set of REST API's supports full automation of all configuration objects, starting and stopping the engine(s), and importing or exporting configuration sets. Configuration is always performed inside the trusted zone to ensure the protection of configuration and management activities.

Capability	Description
Application proxy	• Resides in the demilitarized zone (DMZ) • Supports IBM® Sterling Connect:Direct, IBM® Sterling B2B Integrator, IBM® Sterling File Gateway, and IBM® Sterling Connect:Express • Compatible with layered- or multiple-DMZ environments • Supports FTP, FTPS, HTTP, HTTPS, AS2, SSH/SFTP, PeSIT and Sterling Connect:Direct protocols • Includes a FIPS 140-2 compliant data encryption module with the option to force "strict FIPS mode" communications
Firewall navigation best practices	• Prevents inbound holes in the firewall • Minimizes rich targets in the DMZ by ensuring that files, user credentials and data are never stored on physical drives in the DMZ • Establishes sessions from more-trusted to less-trusted zones • Enforces internal and external security policies
Perimeter security	• Prevents direct communications between external and internal sessions by establishing secure session breaks in the DMZ using SSL or TLS connections • Inspects protocol and sensitive control information and supports configurable error handling if violations are detected • Session limits and data encryption guard against denial-of-service attacks
Authentication services	• Customizable logon portal provides self-service password management for trading partners • Supports single sign-on and integration with existing security infrastructure, including Active Directory and Tivoli user databases • Multifactor authentication enforces tight controls and validation of trading partner identity in the DMZ before internal sessions are established to the trusted zone • Authentication options include IP address, user ID and password, digital certificates, SSH Keys, RSA SecurID
Clustering	• One central configuration manager pushes out configuration rules to multiple engines running in the DMZ facilitating painless scalability • High-availability and load-balanced clustered environments are supported ensuring business continuity and optimal performance

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
November 2014

Please Recycle

ZZD03039USEN-02