STERLING COMMERCE WHITE PAPER

Removing the Barriers of Traditional FTP to Facilitate Secure File Transfers

Sterling Commerce
An IBM Company

Introduction

Check the headlines. Criminal security breaches are in the news. They are costing business billions of dollars, and liability for damages reaches all the way to the boardroom.

The fact is, identity theft tops the “fastest growing” list for white collar crime in the U.S. And according to the Ponemon Institute’s 2009 Cost of Data Breach Study, companies spent, on average, nearly $6.65 million on recovery after corporate data was stolen or lost.

When it comes to responsibility, the buck stops with business. Without adequate safeguards to protect consumer information, companies inevitably pay a heavy price in terms of damaged public trust, sinking share value, and even prison time for top executives.

Today, more and more criminals are turning their attention to file transfers that carry credit card information of consumers. Many organizations move this information with file transfer protocol (FTP), and these servers are proving to be easy targets for thieves.

Encryption may seem like an easy fix, but there is no easy answer to this complicated problem. This paper outlines techniques and solutions for file transfer security that business can rely on now.

No single point of attack
Breaches can be made at servers on either end, from transmission on the wire, or from man-in-the-middle attacks.

Attacks are increasingly sophisticated
More often than not, attacks are by professional criminals targeting a specific opportunity.

Increased pressure to share data
Partners and suppliers outside the organization are constantly asking for data and it is simple to provide.

No centralized control
Who's in charge? There is little in the way of access control.

Understand the Landscape

Effective file transfer security measures allow trading partners to communicate with each other, while keeping others out.

File transfer security is complicated by a range of factors, including the large number of opportunities for attack, the sophistication of attacks, more sharing of data, and the absence of centralized control.

Unfortunately, the problem is only complicated by the technology that companies use to transfer files. Many companies turn to the FTP that is shipped with most computer operating systems. But FTP is not the best solution. Here's why:

- FTP is not free – Script-based automation requires constant tweaking, it takes time to search logs for error resolution and, again, with no central management you have to touch every server
- FTP has limited management and tracking – That's why it keeps asking you to "just try again"
- FTP is not secure – This means operating access is required for each user, you're dealing with "free text" usernames and passwords, plus, you experience numerous security vulnerabilities on a per platform basis

And those are only a few of the barriers. Others include FTP's lack of large file support, as well as the need for significant scripting, which requires technical IT resources.

The ideal file transfer solution will eliminate the barriers of traditional FTP so that you can continue to transfer important information that is required to run your business, but removes the risk of security breaches. The right solution can enable your business to retain customers and decrease liability. This is what to look for:

- A secure protocol, one that is proven over time
- The ability to leverage your existing security infrastructure, including LDAP servers
- Capability to use the Internet as well as dedicated lines
- Government certified encryption to ensure the safety of consumer data
- One that gives you control and visibility into all your transfers

Demand a Protocol that Has Been Tested

The ideal solution is one that has proven itself in demanding environments. It is also one that has never been breached. That's why it's important to look at those government agencies and organizations in retail, telecommunications, and banking that continue to move large amounts of confidential and sensitive data in a secure and reliable way.

Consider the Entire Package

The right Managed File Transfer solution for your organization should be available with multiple options, and should have these characteristics:

Robust security

Look for security that allows data movement to fit naturally within your existing security policies. If support for secure FTP traffic is required, the data flow can be encrypted. If you need higher security levels, then proxy-based security, coupled with authentication and configurable encryption, should be available.

Strong authentication

Secure Managed File Transfer solutions use authentication to ensure that people establishing a connection are legitimate. This secure connection would use public key cryptography to authenticate the identity of users. Strong authentication provides high levels of security by authenticating trading partners on a number of factors like IP address and certificate checks.

Authentication of this caliber would include LDAP validation and Certificate Revocation List (CRL) checking.

Data integrity

The solution you choose should ensure data integrity. The right solution will provide a SSL/TLS toolkit that generates digital signatures and Message Authentication Codes (MACs) as well.

Confidentiality

The Managed File Transfer solution you go with should provide encryption that protects the SSL/TLS confidentiality of data in transit by preventing unauthorized people from accessing data and passwords. This feature will protect against eavesdropping and other Internet attacks.

Count on Perimeter Security to Enable Use of the Internet

With the increased use of the Internet for file transfer, you should settle for nothing less than robust perimeter security; traditional defenses of firewalls are no longer sufficient. Robust security shields the internal network and incorporates a defense-in-depth strategy, by placing multiple layers between the internal network and the Internet. If an attack does take place, you would have the opportunity to detect it and respond appropriately.

Make Certain You Have an Application Proxy

This is an important feature to look for, because an application proxy will shield your network from external attacks by preventing direct communications between external and internal servers.

At minimum, your application proxy should:

- Support FTP, FTPS, HTTP, HTTPS and IBM® Sterling Connect:Direct® protocols using DMZ-based application proxy
- Enforce firewall navigation best practices with no inbound holes in the firewall and no files stored in DMZ
- Prevent—through session breaks—direct communications between internal and external sessions
- Authenticate incoming connections using the SSL or TLS protocol, and exchange and validate the trading partner prior to establishing a session
- Guard against common attacks and ensure business continuity

Gain Greater Security with Multifactor Authentication

Multifactor authentication and additional certificate checks will provide even more security. Make certain the solution you are considering will validate digital certificates that are exchanged during file transfer sessions.

The capabilities to look for should include:

- CRL Checking that validates certificates against one or more Certificate Revocation Lists (CRLs) located on an LDAP server
- Standard Certificate Validation that allows you to perform standard certificate validation functions, including enforcement of valid dates and validation of issuer signature
- Application Policy Enforcement that allows your to validate certificate extensions using custom formulas
- LDAP queries against the contents of a Certificate
- Additional validation for CRL checking, LDAP validations and custom lookups

What's more, the ideal solution will offer flexible deployment options, including single-tier and multi-tier deployment that enable the proxy to enforce a range of perimeter security policies that fit your business requirements.

Know that Certified Encryption Ensures the Safety of Data

You will want to know that your solution includes the proper government security certifications.

The U.S. Federal government requires that all encryption software and hardware products they deploy be FIPS 140-2 certified. This certification is gaining worldwide recognition as a benchmark for third-party validation of encryption products. Customers who exchange files with the Federal government, financial services in particular, are required to utilize FIPS certified encryption products.

You will also want to consider Common Criteria. Accepted by 24 governments worldwide, the Common Criteria evaluation assesses the security features of a product against a published security target. If a product meets Common Criteria standards, you'll know it has been successfully evaluated and that it actually delivers against a set of security specifications.

If you choose the right file transfer solution, you can be confident that you have decreased your liability and helped increase customer retention.

Why IBM?

IBM® Sterling Managed File Transfer enables enterprises to manage and control the critical information flows that run their dynamic business networks. Through seamless, reliable and secure data delivery you can improve business performance, reduce IT complexity, support growth and reduce your risk. The IBM solution incorporates robust perimeter security and includes products that ensure data confidentiality, enforce strong authentication, and provide robust perimeter security.

IBM® Sterling Connect:Direct® is the point-to-point file transfer software optimized for high-volume, secure, assured delivery of files within and among enterprises. Security is a critical element of these transactions and involves all of the levels in the pyramid of trust: authentication, access control, data integrity, confidentiality and non-repudiation. IBM® Sterling Connect:Direct® Secure Plus, a component of Sterling Connect:Direct, provides comprehensive cryptographic security for data exchange to ensure your mission-critical data is transferred safely and reliably.

IBM® Sterling File Gateway is an SOA based solution which allows you to incorporate your file transfer communities into all your business processes and incorporates Web-based interfaces for customer self-services and rapid onboarding. It consolidates disparate centers of file transfer activity, and facilitates the secure exchange of file-based data over the internet.

IBM® Websphere MQ File Transfer Edition is a reliable, enterprise wide file transfer software using messaging that leverages MQ. It leverages existing messaging infrastructure for universal service delivery including messages, files and events, and facilitates a secure and reliable Managed File Transfer environment across IBM Sterling Connect:Direct and WebSphere MQ File Transfer Edition endpoints

IBM® Sterling Secure Proxy is a demilitarized zone (DMZ)-based application proxy that protects your file transfers from the public Internet, by enforcing tight controls that include trading-partner authorization, multi-factor authentication and session break all before the transfer ever enters your trusted zone. Sterling External Authentication Server performs advanced certificate validation. Its configurable certificate validation functions include: CRL checking, Standard certificate validation, Application policy enforcement, and LDAP queries.

IBM® Sterling Control Center is a management solution for all your file transfer activity and associated Service Level Agreements. It gives you a consolidated view of your entire file transfer environment—plus the power to respond quickly and efficiently to exceptions, and changes in your environment.

IBM® Sterling File Transfer Service is a cloud service for file based business interactions with trading partners. An alternative to on-premise software, Sterling File Transfer Service allows you to manage a single, secure, reliable connection with the cloud to reach your partners without the capital expense associated with on premise software or the operational impact on your IT staff.

For additional information on the IBM Managed File Transfer solution, please contact us.

About Sterling Commerce

Sterling Commerce, an IBM® Company, helps organizations worldwide increase business agility in their dynamic business network through innovative solutions for selling and fulfillment and for seamless and secure integration with customers, partners and suppliers. More information can be found at **www.sterlingcommerce.com.**

Sterling Commerce
An IBM Company

For all Sterling Commerce offices worldwide,
visit **www.sterlingcommerce.com**