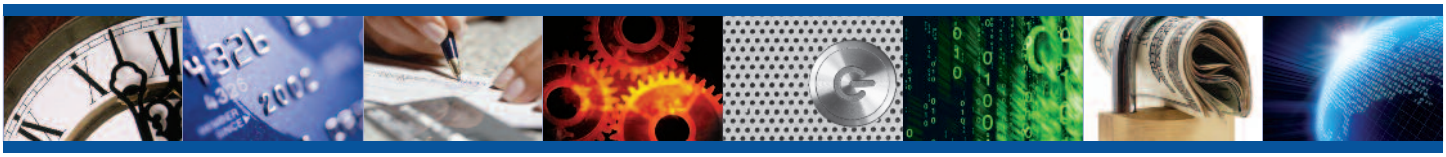
A LINOMA SOFTWARE WHITE PAPER

PCI DSS Compliance with Managed File Transfer



A LINOMA SOFTWARE WHITE PAPER

PCI DSS Compliance with Managed File Transfer

By Thomas M. Stockwell

EXECUTIVE SUMMARY

PCI DSS compliance requirements will continually evolve under the auspices of the PCI Security Standards Council throughout a newly defined 36-month lifecycle. This may mean that the security "tweaks" that IT implements today for PCI DSS 2.0 may be inadequate to handle the data security requirements of the next version of the standard.

However, by rethinking the use of underlying components that IT uses in its data transfer arsenal, forward-thinking IT shops are arming themselves to meet the changing requirements of PCI DSS and other compliance requirements. With better as well as more configurable, automated and secure data transfer tools, these professionals are building new technology strategies to meet and/or exceed the compliance requirements for today and tomorrow.

LINOMA SOFTWARE

Publication date: April 2, 2012

Introduction

PCI DSS Version 2.0 is here, and companies are challenged with the task of modifying their security systems to meet the requirements. But some IT groups are taking a new and creative path towards PCI DSS compliance. Instead of struggling to meet compliance requirements with legacy data transfer tools, they are implementing managed file transfer solutions that include DMZ gateways.

This unique and cost-effective strategy provides better, more configurable tools to help IT staffs achieve PCI DSS compliance more easily, while laying a good foundation for future security enhancements.

Validation of compliance with PCI DSS must be **performed annually,** beginning January 1, 2012.

What Is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is the information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM and POS cards. It's defined by the Payment Card Industry Security Standards Council as a method to increase privacy controls over cardholder data and reduce credit card fraud due to accidental or deliberate exposure.

PCI DSS 2.0 was released in 2010 and required for adoption by all entities that process, store, or transmit credit/debit card data by January of 2011.

Validation of compliance with PCI DSS must be performed annually, beginning January 1, 2012 by an external Qualified Security Assessor (QSA) at organizations that handle large volumes of transactions, or by a Self-Assessment Questionnaire (SAQ) at companies managing smaller volumes.

The Danger of Non-Compliance

If your organization experiences a security breach -- without proof of compliance to PCI DSS 2.0 at the time of the breach – the lack of compliance will result in fines and penalties from the payment card brand (Visa, MasterCard, etc.). The fines are not trivial: $5,000 to $100,000 per month until your organization attains compliance, and could result in termination of your merchant account by the bank.

Therefore it's imperative that IT professionals become well-versed in all of the PCI DSS regulations to learn how to most efficiently implement its technical compliance requirements in their organizations.

The Impact of PCI DSS on IT

PCI DSS 2.0 is a broad-reaching security standard with many requirements and recommendations. At first glance, the IT elements for achieving PCI DSS 2.0 compliance may not appear too onerous. Some are common sense requirements, such as enforcing password policies, locking down networks and restricting access to systems that store PCI data. All require testing and validation on a scheduled basis. But, like many compliance regulations, the devil is in the details.

For some IT shops, the technical elements of PCI compliance may already be in place as a part of a larger IT data security scheme. But for others, the stricter security focus of PCI DSS 2.0 will necessitate a thorough technical review of the existing IT infrastructure and validation processes including:

- Infrastructure reconfiguration
- New equipment investment
- New and/or extended auditing processes

A New Technical Strategy for Compliance

As companies have prepared to address their PCI DSS compliance processes, many have decided that the focus of their IT staff compliance efforts needs to change. They have learned that it's no longer cost-effective to "tweak" an existing aging security infrastructure – especially where critical and confidential data is being transferred to other entities.

Instead, these IT organizations are building a technical strategy within the IT infrastructure that can evolve easily to accommodate new compliance demands as they are defined.

How are IT shops developing such a technical strategy? One key component being used by leading edge IT shops is the implementation of a managed file transfer solution.

Managed file transfer solutions are a more effective way to achieve PCI DSS 2.0 compliance.

What Is Managed File Transfer?

Managed File Transfer (MFT) is a comprehensive, centrally controlled software solution that facilitates and secures the movement of data between systems across internal networks, external WANs and the public Internet.

MFT solutions move file transfers activities into a controlled environment with oversight, authentication, encryption, role-based administration, auditing and reporting.

An effective MFT solution does all of the following:

- automates file transfer processes between trading partners and internal systems including detection and handling of failed transfers;
- supports multiple file transfer standards including FTP/S, SFTP, SCP, AS2 and HTTP/S;
- protects transmissions over public and private networks using secure protocols (e.g. SSL, TLS, SSH);
- provides strong authentication schemes using a combination of user ids, passwords, keys and/or certificates;
- protects files while at rest using strong encryption methods such as AES and Open PGP;
- integrates with existing applications using documented APIs; and
- generates detailed reports on user and file transfer activity.

MFT solutions resolve many of the known security limitations normally associated with FTP while permitting IT to automate and validate the file transfer processes.

Most importantly for PCI DSS compliance, MFT solutions protect sensitive data so that exposure to threats due to attacks or user errors can be minimized or eliminated. By utilizing the flexible and configurable components of MFT, an organization will decrease its exposures, increase the success rates of file transfers, and remove many of the obstacles that are common with business-to-business transfers.

But implementing a typical MFT solution doesn't satisfy PCI DSS data security requirements by itself. To help achieve compliance, a DMZ gateway is also needed.

MFT solutions have resolved security issues associated with FTP while automating and validating data transfer.

What Is a DMZ gateway?

A DMZ gateway is designed to add an extra layer of security to the company's network. It is configured to reside in the public-facing segment of a company's network called the demilitarized zone (DMZ).

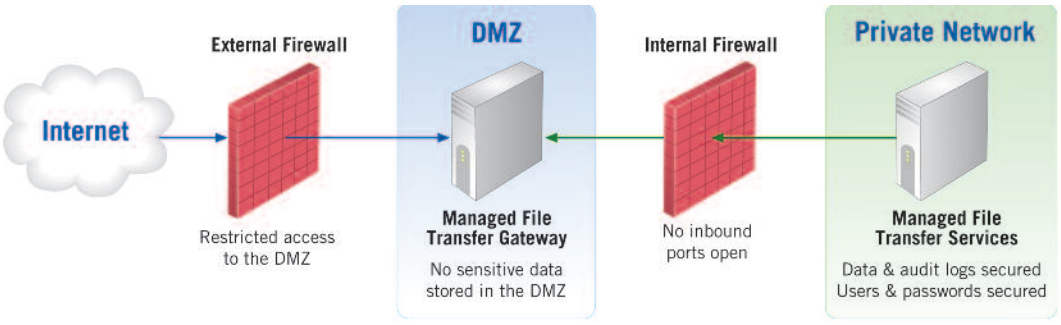
By acting as a reverse proxy, a DMZ gateway prohibits direct public access from the Internet to any systems in the company's private network. At the same time, it can serve as a forward proxy by passing transfer requests from the private network out to the Internet, coordinating these transfers with the MFT software in the company's internal network.

Implementing a DMZ gateway is critical in helping to solve the onerous elements of PCI Requirement 1.3, the prohibition of direct public access to the cardholder data environment.

By implementing a DMZ gateway solution, the IT staff can quickly configure and automate data transfers, eliminating the complexity of staging files in the DMZ.

Strategic Tools for Compliance

Managed File Transfer, in tandem with a DMZ gateway, enhances the overall IT security scheme by bringing the day-to-day tasks of data exchange into a configurable, scalable system that can meet or exceed the IT security requirements of compliance regulations.



A DMZ gateway functions as both a reverse and forward proxy, keeping sensitive data out of the public-facing DMZ, masking private network addresses, and leaving inbound ports closed to the internal network.

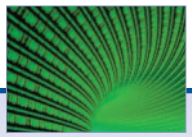
MFT dovetails with the current IT requirements for PCI DSS, while positioning the organization to meet new requirements down the road. This is why it is such an effective technical strategy for compliance.

Therefore, a managed file transfer solution, combined with a DMZ gateway, accomplishes the following goals:

- Centralizes the control and management of file transfers
- Provides role-based administration and permissions
- Institutes secure connections for the transmission of sensitive data
- Provides strong encryption key management with separation of duties
- Keeps PCI-related data out of the DMZ
- Closes inbound ports into the private network to prevent unwanted intrusion
- Provides detailed audit logs for reporting

Organizations who want to ensure PCI DSS compliance find that MFT allows IT administrators to control and secure the day-to-day data exchange activities, boosted by DMZ gateways that extend that security to the network itself.

Using this MFT strategy, IT groups can reduce the amount of time required to implement PCI DSS 2.0, increase the security of the network, and control the access to sensitive information while providing a future-proof technical strategy that is robust, scalable, predictable, and secure.



Managed File Transfer, in tandem with a DMZ gateway, enhances the overall IT security.

Appendix: PCI DSS 2.0 Requirements

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

- 1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
- 1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.
- 1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.
- 1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.
- 1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the internet.
- 1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)
- 1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.
- 1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to:
  - Network Address Translation (NAT),
  - Placing servers containing cardholder data behind proxy servers/firewalls or content caches,
  - Removal or filtering of route advertisements for private networks that employ registered addressing,
  - Internal use of RFC1918 address space instead of registered addresses.

PCI DSS 2.0 requires that **inbound internet traffic be limited** to IP addresses within the DMZ.

About GoAnywhere™ MFT Solutions

Linoma Software provides innovative technologies for protecting sensitive data and automating data movement. Linoma Software has engineered GoAnywhere, an advanced managed file transfer and secure FTP solution that will streamline and automate file transfers with trading partners, customers, employees and internal servers. Enterprise level controls and detailed audit logs are provided for meeting strict security policies and compliance requirements including PCI DSS, HIPAA, HITECH, SOX, GLBA and state privacy laws.

The GoAnywhere solution is comprised of three integrated products:

- GoAnywhere Director™ – Managed File Transfer (scheduler, workflow automation, file encryption, etc.)
- GoAnywhere Services™ – Secure FTP Server with optional Secure Mail feature to manage ad-hoc file transfers
- GoAnywhere Gateway™ – DMZ Gateway with Reverse and Forward Proxy

To learn more about GoAnywhere or to request a demo or download a free trial, visit www.GoAnywhereMFT.com

GoAnywhere

Managed File Transfer Solutions

- Browser-based administration
- Support for popular encryption and file transfer standards
- Robust workflows
- DMZ gateway
- Detailed audit logs

About Linoma Software

Founded in 1994, Linoma Software provides innovative technologies for managed file transfer and data encryption solutions, with a diverse install base of more than 3,000 customers around the world including Fortune 500 companies, non-profit organizations and government entities.

Electronic Contact Information

Sales: sales@LinomaSoftware.com

Support: support@LinomaSoftware.com

Website: www.LinomaSoftware.com

Phone Numbers

Toll-free: 800.949.4696

Outside USA: 402.944.4242

Fax: 402.944.4243

Address

Linoma Software
1409 Silver Street
Ashland, NE 68003 USA