globalscape™
securely connected

Case Study

OSPI Adds DMZ Gateway® to Protect Internal Network

SUPERINTENDENT OF PUBLIC INSTRUCTION
WASHINGTON

After Dealing with 3,000 to 5,000 Malicious Attacks Per Day, OSPI Decided to Take Action to Protect Their Data.

Introduction

The Office of Superintendent of Public Instruction (OSPI) in Washington State manages educational data assets primarily through data collection and transmission with more than 1500 partners of educational districts, schools, vendors, educational researchers, and many other parties both internal and external.

Their partners transfer more than 10,000 files per month, amounting to ~2GB of data per month. Many of the files processed contain sensitive information of about 1.1 million students and teachers in Washington State. This data is protected by Family Education Rights and Privacy Act (FERPA) and must be protected and secured.

The Challenge

Some of the business processes used by OSPI's file transfer system include:

- Managing all educational information from all students, teachers, and staff throughout the state. This information is received and forwarded to our databases for Federal and State reporting and transactional processing of data to other systems.
- Managing assessment results information from all students through various vendors systems.
- Managing assessment test questions from all students through various vendors systems.
- Collecting financial data in files pertaining to all schools throughout the state. This information is integrated with our financial systems and then reported to our state Office of Financial Management.
- Data and information exchanged among related peers, etc.

These critical business processes were implemented on two Globalscape Secure FTP Servers in 2007, and then were upgraded to EFT version 6 in 2009 and 2012, with one FTP Site and four SFTP Sites. They were not using Globalscape DMZ Gateway®.

While this architecture is functioning, their implementation was not as secure as it could be. EFT was installed outside of the internal firewall. They had 3,000-5,000 malicious attacks on Secure FTP server per day, and at least one attempt per hour after upgrading to EFT.

The Solution

To improve the response to these security concerns, OSPI added Globalscape DMZ Gateway to protect the internal network.

Globalscape DMZ Gateway is a multi-platform solution that works in conjunction with the EFT platform to create a multi-layered security solution for data storage and retrieval, authentication, and firewall traversal.

Using a two-way connection originating inside EFT, the DMZ Gateway acts as a communication proxy to process requests that replace inherently insecure inbound connections from the Demilitarized Zone (DMZ) to our network.

Unlike store-and-forward technologies, GlobalScape DMZ Gateway does not store or process data. It acts as a liaison between external connections and the internal network, ensuring that data remains safe behind the firewall for EFT to store and process. Data remains secure because it’s never stored in the DMZ.

How Does DMZ Gateway Work?

DMZ Gateway resides in the DMZ. EFT resides inside the network, behind a firewall. EFT initiates a persistent session with the DMZ Gateway.

When a client connects to the DMZ Gateway, DMZ Gateway notifies EFT that a client wants to connect over the pre-established session. Subsequently, EFT initiates another outbound session to the DMZ Gateway, and the DMZ Gateway then connects this new session and the client’s session. From that point forward, that client’s communications are streamed through DMZ Gateway to EFT.

Globalscape DMZ Gateway Provides Security and Efficiency at the Same Time.

DMZ Gateway provides the following benefits:

Security benefits:

> Facilitates compliance with mandates such as PCI DSS requirement §1.3.7 that forbid storage of sensitive data in the demilitarized zone (DMZ).

> Eliminates the need for file encryption, store-and-forward systems, or polling for changes to secure data in the DMZ.

> Eliminates the need for a file transfer system in the DMZ or for exposing any part of your network to the DMZ, such as AD services for user authentication or SQL services for auditing.

Efficiency benefits:

> A single outbound connection greatly reduces overhead compared to traditional proxy and firewall configuration.

> Saves time and reduces points of failure over traditional store-and-forward or polling for changes. Data is made available to backend systems in real time.

The DMZ Gateway prevents unauthorized access to sensitive data, avoiding malicious attacks and unauthorized access.