DATAEXPRESS OPEN PLATFORM

DXSG DataExpress Secure Gateway

Secure Gateway's primary role is to insulate the file transfer server platform from risk. A DataExpress feature, Secure Gateway deploys as a DMZ point-of-presence, isolating both DataExpress and the application server from the internet.

Main Features

Stand-alone Core DXOP (DataExpress for Open Platform) implementations on Windows or Unix/Linux server platforms expose the entire platform to public-facing internet hazards. To provide access and some control, installations will drill holes and limit port assignments via firewalls and routers. This practice does not fully address the potential risk and severely limits protocol selection and interaction with out-side partners.

A Secure Gateway configuration combines a single DataExpress Core Server with one or more Secure Gateway instances. The DXOP Core Server retains all monitoring, administration, operations, and control over the DXOP infra-structure and operation. All files processed by DXOP are stored and maintained by the DXOP Core Server

Configuration

A graphical interface is provided for configuring Secure Gateway to the appropriate DXOP Core Server. Few changes to DXOP are required to implement Secure Gateway.

High Availability

Secure Gateway has a high-availability (HA) option where multiple Secure Gateways may be deployed. Under HA, should a single Secure Gateway instance fail, another Secure Gateway instance will take over all activity. In-flight sessions may fail, but will restart if so configured.

Risk Reduction

Secure Gateway instances function as proxy servers and inline protocol converters, securely streaming data files to and from the Core DXOP server. Restricting all internet-based traffic to communication with Secure Gateway, the DXOP Core Server, database and data storage facilities remain safely protected inside your internal network.

Communication channels between the Secure Gateways and the DXOP Core Server can be configured for software encryption. These links may also use VPN or tunneling protocols between the DXOP Core Server and Secure Gateway. Secure Gateways do not require direct access to the DXOP database; all communication to the database is made by the DXOP Core Server. All configuration, user authentication, monitoring and control are performed via the DXOP Core Server.

DXSG FEATURES

- SECURITY
- RISK REDUCTION
- HIGH AVAILABILITY
- GUI-BASED CONFIGURATION

Security

Secure Gateway provides additional security for DXOP by shielding DXOP from the internet for IP-based communications. Files reside within the secure confines of the enterprise and do not require inbound or outbound files to be staged to edge FTP or application servers where data could be at risk.

Secure Gateway Environment

Secure Gateway may be implemented to either Windows Server or Linux platforms.

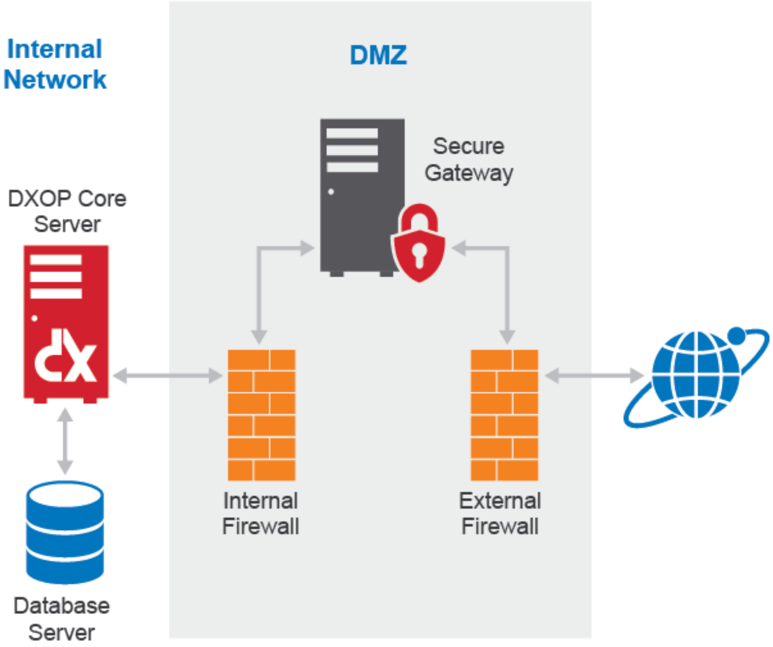
Supported Protocols

Inbound:

FTP
FTPS (implicit / explicit)
SFTP
HTTP
HTTPS
WebDAV
WebDAV(SSL)
AS2/3

Outbound:

FTP
FTPS (implicit / explicit)
SFTP
AS2/3


Internal Network
DMZ
Secure Gateway
DXOP Core Server
Internal Firewall
External Firewall
Database Server