



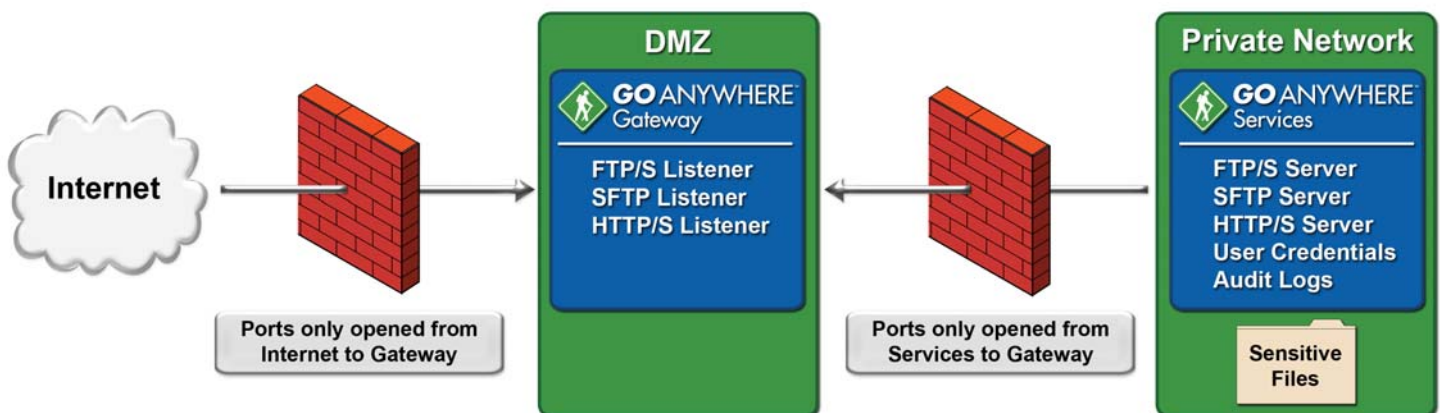
GO ANYWHERE™ Gateway

GoAnywhere Gateway™ keeps sensitive files out of the DMZ while protecting the private network.



Reverse Proxy for the DMZ

GoAnywhere Gateway™ allows your trading partners to connect to your organization without having to open incoming ports into your private network or store sensitive information in the DMZ. It acts as an enhanced reverse proxy that provides an additional layer of network defense. GoAnywhere Gateway integrates with GoAnywhere Services™ to provide a secure and managed environment for hosting and exchanging files.



GoAnywhere Gateway Features:

- No incoming ports are opened into the private (internal) network - reduces the risk of network intrusion
- Internal servers are “masqueraded” behind reverse proxy
- No sensitive files are stored in the DMZ
- User credentials and permissions are maintained/stored in the private network
- Services configurations are maintained/stored in the private network
- Supports FTP/S, SFTP and HTTP/S file transfer protocols
- No special hardware components required; software-only solution

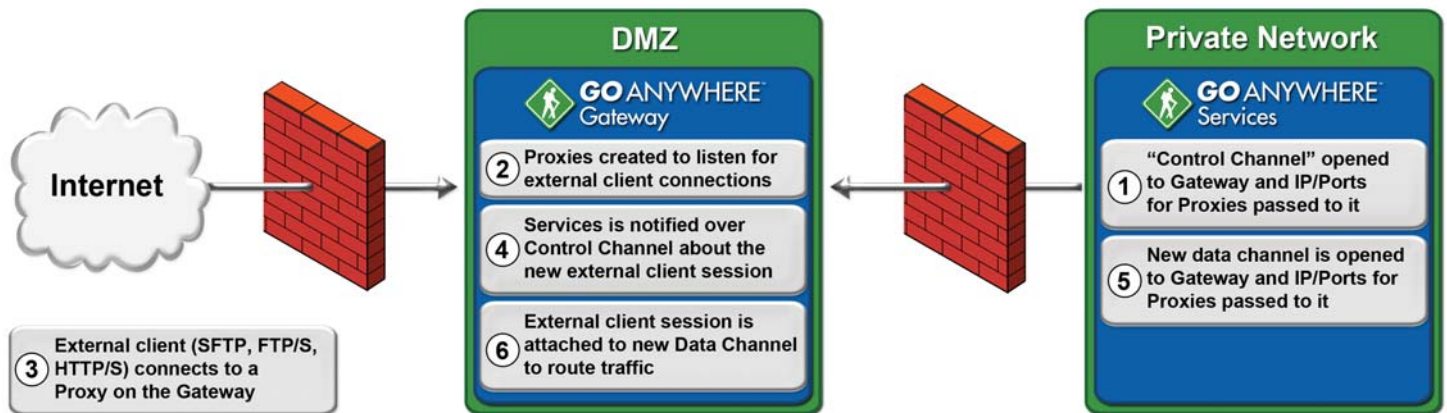


GoAnywhere Gateway is essential for meeting compliance requirements including HIPAA, PCI DSS, SOX and GLBA.

How GoAnywhere Gateway Works

At startup, GoAnywhere Services will establish an outbound connection to GoAnywhere Gateway, which will serve as a “control channel” for passing proprietary commands and messages between the products. GoAnywhere Services will send proxy information to GoAnywhere Gateway including which IP addresses and port numbers to create “listeners” for.

When an external client (trading partner) connects to a listener on GoAnywhere Gateway, it notifies GoAnywhere Services over the control channel. At that point, GoAnywhere Services creates a new outbound connection (“data channel”) to GoAnywhere Gateway. This data channel is attached to the desired service (e.g. FTP/S, SFTP, HTTP/S) and all traffic (client authentication requests, data, commands, etc.) for that session are routed over this new data channel. When the session is terminated, its corresponding data channel is removed.



*Steps 1-2 are only performed at initial startup.

*Steps 3-6 are repeated for each new external client connection.

System Requirements

Windows (32-bit and 64-bit)

Versions: Windows Server 2003
Windows Server 2008 R2
Windows XP
Windows Vista
Windows 7

Disk Space: 100 MB

Memory: 256 MB

Linux (32-bit and 64-bit)

Disk Space: 100 MB

Memory: 256 MB

AIX, HP-UX, Solaris, Mac OS X, UNIX

Disk Space: 50 MB

Memory: 256 MB

JRE: 1.6.0 or higher

About Linoma Software

Founded in 1994, Linoma Software provides innovative technologies for protecting sensitive data and automating data movement. Linoma Software has a diverse install base of over 3,000 customers around the world including corporations, non-profit organizations and government entities.



LINOMA
SOFTWARE

1409 Silver Street
Ashland, Nebraska 68003
(402) 944.4242
(800) 949.4696
email: sales@linomasoftware.com

Visit GoAnywhereMFT.com for more information or to download a free trial!