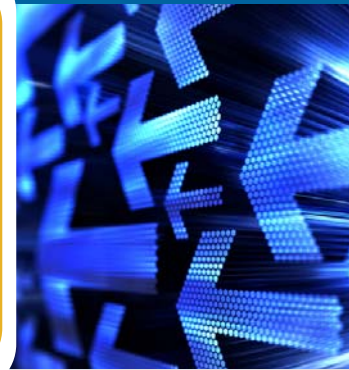


VersaLex Proxy

VersaLex Suite

Forward and Reverse Proxy Server

- Eliminates unencrypted messages in the DMZ
- Eliminates configuration files being written to folder or directory locations in the DMZ
- Simple design, easy set up
- Self-configuration between VLProxy and VersaLex
- Complements VersaLex products' tight security



Security for Strict Network Operations

Network security policies can make implementation of secure communications a challenge. Some protocols, including AS2 and AS3 server, require users to specify an open inbound port on a computer or a firewall with an external IP address. This IP address and port combination must be shared with trading partners who are required to reciprocally share an accessible IP address and port combination. Typically, this open port is claimed by the software running as a service on the host machine. Any external requests made on this port are subject to processing and validation schemes.

Before files are imported and decrypted, packets are parsed for trading partner validation, and the correct digital certificate pairs for any particular partner relationship must be found in the VersaLex system files. If these requirements are not met, the communication session request dies before files are allowed to enter the network through the open inbound port. This validation scheme, plus firewall rules limiting access to the open port, provides ample protection for many networks. However it may be insufficient for organizations with security policies preventing inbound communications sessions from directly entering their secure internal network. For those implementations, VersaLex™ Proxy (VLProxy) provides an enhanced security solution.

Installed outside the firewall or in a DMZ (demilitarized zone), VLProxy 'talks' to the VersaLex software over a single port through the internal firewall. It dynamically self-configures trading partner relationships with VersaLex and does not require configuration files written to folder or directory locations outside the firewall or in the DMZ.

Forward Proxy for outbound AS2, AS3, ebMS, HTTP, and FTP communications

Acting as a forward proxy, VLProxy intercepts outbound communication session requests initiated by VersaLex and passes these session requests on to valid partners. Forward proxy using VLProxy works equally well with client-server implementations of HTTP/(S) and FTP/(S) as it does with peer-to-peer implementations of AS2. The required outbound HTTP/(S) or FTP/(S) connection is performed by VLProxy in the DMZ and all messages or files passed back over this open outbound connection are seamlessly passed through the internal firewall to the VersaLex software on the LAN (local area network). No inbound ports are opened when HTTP/(S) or FTP/(S) is used by VersaLex in a client/server implementation.

Protecting Your Network

- Password protected configuration
- Property values are encrypted on hard drive
- VersaLex/VLProxy relationship validated via exchange of serial numbers
- Email on fail alerts
- Execute on failure process option
- Can be used to manage multiple non-redundant VersaLexes

PLATFORMS

- Windows 98/NT/2000/XP (Windows 2000 or 2003 Server strongly recommended)
- AIX 5.1
- HP-UX 11i
- Red Hat Intel Linux 7.1+
- Solaris SPARC versions 8, 9

SYSTEM REQUIREMENTS

Hardware

- Processor equivalent to a Pentium 4 - 2.4 GHz or better
- 512 Mb RAM minimum
- Graphical User Interface (GUI) (Required for Windows; Recommended for UNIX)
- 10 Mbit network connection (100 Mbit recommended)
- Minimum of 500 Mb of disk space for the VLProxy application and associated files

Other Requirements

- Persistent connection to the Internet with an associated static external IP address (directly on the computer or via NAT)
- If the computer is behind a firewall, appropriate IP addresses and ports must be open based on VLProxy configuration and trading partners to allow the necessary traffic to be transmitted to and from partners.
- The computer running VersaLex must have a static IP address.
- To ensure optimal performance, VLProxy should be run on a dedicated computer (VLProxy should not be run on the same computer as a Web Server).

For Windows XP/2000/2003

VLProxy must be installed as a Windows Service

For Unix Platforms

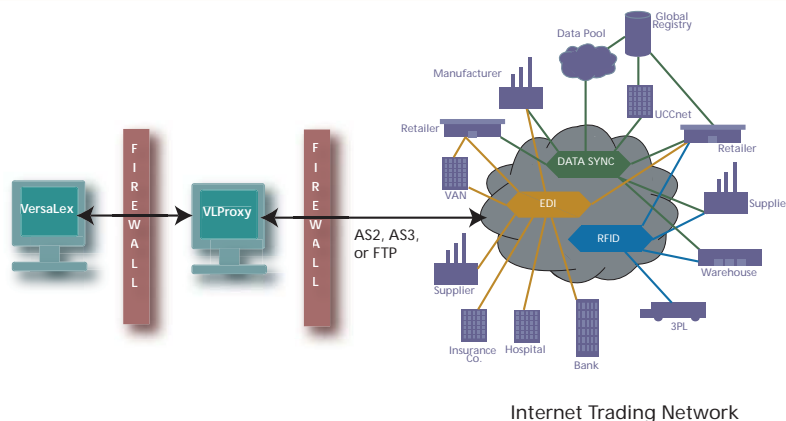
Must be able to run Java 1.3.x (Note: This may require operating system patches)



ECS INTERNATIONAL
P . O . B O X 2 2
1 6 8 7 Z G W O G N U M
T H E N E T H E R L A N D S
P H O N E . + 3 1 2 2 9 5 7 4 3 3 1
S A L E S @ E C S - E U R O P E . C O M
W W W . E C S - E U R O P E . N L

CLEO COMMUNICATIONS
4203 GALLERIA DRIVE
ROCKFORD, ILLINOIS 61111
UNITED STATES OF AMERICA
W W W . C L E O . C O M

CLEO



VLProxy is a forward and reverse proxy server that installs outside the firewall or in a DMZ (demilitarized zone) . VLProxy communicates with VersaLex over a single port through an internal firewall.

Reverse Proxy for inbound AS2, AS3, ebMS, and FTP communications

As a reverse proxy, VLProxy shields the VersaLex open inbound listener port from being exposed directly to the public Internet or external open network. Although VLProxy acts as a gateway or relay agent, no files or messages are left in the DMZ or outside the firewall, and no decryption takes place in the DMZ or outside the firewall. If validation of the incoming session requests is successful, files or messages are passed to VersaLex for decryption and additional back-end processing. Incoming sessions that fail to be validated by VLProxy are killed before getting passed through VLProxy's internal connection to VersaLex.

Self-configuration between VLProxy and VersaLex

When VersaLex and VLProxy are booted up or configuration changes are made on VersaLex, configuration files are transferred and stored in the memory of VLProxy. Configuration files containing trading partner AS2 relationship information or digital certificates are not written to directory locations. This process is initiated by VersaLex using the randomly selected outbound port. VLProxy listens for the request on the specified inbound port. If HTTP/S or FTP/S is used as the transfer method, applicable digital certificates are also stored in the memory of VLProxy. Storing configuration files and certificates in memory allows VLProxy to validate incoming session requests against trading partner relationships established in VersaLex.

VLProxy is included in VLTrader. It is an available add-on to LexiCom. For more details, or to place an order, contact Cleo Communications' authorized reseller, ECS International.

