



VLProxy™

User's Guide

Version 2.6
12.09.2009

CLEO

RESTRICTED RIGHTS

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (C)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Manufacturer is:

Cleo Communications

4203 Galleria Drive

Rockford, IL 61111 USA

Phone: 815.654.8110

Fax: 815.654.8294

Email: sales@cleo.com

www.cleo.com

Support: 1.866.444.2536, 1.815.282.7894, or support@cleo.com

Cleo Communications reserves the right to, without notice, modify or revise all or part of this document and/or change product features or specifications and shall not be responsible for any loss, cost or damage, including consequential damage, caused by reliance on these materials.

This document may not be reproduced, stored in a retrieval system, or transmitted, in whole or in part, in any form or by any means (electronic, mechanical, photo-copied or otherwise) without the prior written permission of Cleo Communications.

©2004-2009 CLEO COMMUNICATIONS ALL RIGHTS RESERVED. CLEO IS A REGISTERED TRADEMARK AND LEXICOM AND VERSALEX ARE TRADEMARKS OF CLEO COMMUNICATIONS. ALL OTHER BRAND NAMES USED ARE TRADEMARKS OR REGISTERED TRADEMARKS OF THEIR RESPECTIVE COMPANIES.

TABLE OF CONTENTS

INTRODUCTION.....	5
WELCOME.....	5
KEY FEATURES	5
ABOUT CLEO COMMUNICATIONS.....	6
ABOUT JAVA.....	6
BEFORE YOU BEGIN	7
CLEO TECHNICAL SUPPORT SUBSCRIPTION PROGRAM.....	7
GETTING STARTED	8
INTRODUCTION	8
INSTALL	8
INVOKE CONFIGURATION.....	9
SET UP UNIX DAEMON	9
INVOKE WINDOWS SERVICE / UNIX DAEMON	11
CONFIGURATION.....	13
EXAMPLE	13
VLPROXY CONFIGURATION.....	14
VLTRADER/LEXICOM CONFIGURATION	21
SYSTEM LOG FILE.....	26
SYSTEM LOG FILE FORMAT.....	26
MONITOR SYSTEM LOG FILE	28
USING VLPROXY WITH MULTIPLE VERSALEXES.....	29
INTRODUCTION	29
NON-REDUNDANT VERSALEXES	29
<i>Reverse Proxy Issues</i>	29
<i>VersaLex Settings Used by VLProxy for Reverse Proxying</i>	30
REDUNDANT (SYNCHRONIZED) VERSALEXES.....	31
DEBUG OPTIONS	32
COMMAND-LINE DEBUG OPTIONS	32
SINGLE VLPROXY<>VERSALEX CONFIGURATION GUIDE	33
CONFIGURATION DIAGRAM	33
CONFIGURATION WORKSHEET.....	34
VLPROXY CONFIGURATION SCREEN	36
VLTRADER/LEXICOM CONFIGURATION SCREENS.....	37
HIGH AVAILABILITY CONFIGURATION GUIDE.....	40
FIRST VLPROXY<>VERSALEX	41
ADDITIONAL VERSALEXES	41
<i>Net result:</i>	42

ADDITIONAL VLPROXIES	43
<i>Net result:</i>	44

Section 1

Introduction

In this section...

Welcome

Key Features

About Cleo Communications

About Java

Welcome

Welcome to Cleo VLProxy; automated firewall proxy software from Cleo Communications. Cleo VLProxy is a firewall proxy tool that allows you to place Cleo LexiCom or Cleo VLTrader (hereafter called VersaLex) inside the firewall and keep your documents secure while communicating with your trading partners. VLProxy is an HTTP forward and reverse proxy designed specifically for use with VersaLex. VLProxy normally runs in the DMZ (demilitarized zone) and forwards requests between VersaLex inside the company (behind the firewall) and external hosts on the Internet.

Key Features

With VLProxy you can:

- Use VLProxy as a Forward Proxy for all outbound AS2, ebMS, AS3, HTTP, and FTP (including SSH) communications
- Use VLProxy as a Reverse Proxy for all inbound AS2, ebMS, AS3, FTP, and SSH FTP communications so that internal ports do not need to be exposed to the Internet. This includes web GUI and VLTrader VLPortal requests. VLProxy cannot currently be used as a Reverse Proxy for SMTP or OFTP.
- Use VLProxy to proxy for multiple redundant (synchronized) or non-redundant VersaLexes
- E-mail on connection failure to VersaLex

Note: VLProxy automatically accumulates AS2 and ebMS relationships, FTP and HTTP logins, SSL certificates, and User certificates from all the connected VersaLex products.

About Cleo Communications

Cleo Communications provides reliable, data transfer products and services that enable you to easily establish and manage communications sessions, and easily integrate these solutions with their mission-critical applications.

Since Cleo's founding in 1981, our products have been proven in more than 100,000 installations worldwide. Customers in the manufacturing, retail, healthcare, and financial services industries, among others, rely on our products and services to help them achieve complete automated point-to-point data transfer solutions.

For most applications, we adapt our core capabilities to deliver tailored communications solutions providing exceptional value to you. Our products and services are available for resale by leading vertical-market application solution providers. We also work directly with many end-user organizations to meet their specific data transfer needs.

Our business partners and end-user customers prefer Cleo for our ability to provide the highest quality communications products backed by superior service and support.

For more information on our complete line of communications solutions and how they are being used today, please visit www.cleo.com, call 815.654.8110, or email us at sales@cleo.com.

About Java

VLProxy is a Java application. The source code of a Java application is compiled into "bytecode," which cannot run by itself. The bytecode must be converted into machine code at runtime. A Java interpreter (Java Virtual Machine) translates the bytecode into machine code and runs it. This means that Java applications are not dependent on any specific hardware and will run on any operating system that has the Java Virtual Machine (JVM) installed. A JVM is a component of a Java Runtime Environment (JRE). JRE's are available for most operating systems including Windows, HP-UX, Solaris, Linux, and AIX. The JRE comes bundled with the VLProxy installation program.

Section 2

Before You Begin

In this section...

Cleo Technical Support Subscription Program

Cleo Technical Support Subscription Program

Visit <http://www.cleo.com/support/supsub.asp> for information on Support Subscriptions by Product.

Section 3

Getting Started

In this section...

Introduction

Install

Invoke Configuration

Set Up Unix Daemon

Invoke Windows Service / Unix Daemon

Introduction

Cleo VLProxy is a firewall proxy tool that allows you to place Cleo VersaLex inside the firewall and keep your documents secure while communicating with your trading partners. VLProxy is an HTTP forward and reverse proxy. VLProxy is installed on a separate computer from VersaLex, normally within the DMZ (outside the company firewall - see page 13).

Install

The VLProxy installation program is included on the VLTrader CD only. The latest version can be downloaded from <http://www.cleo.com/vlproxycl>.

Windows: To begin the VLProxy installation, do the following:

1. If installing from CD-ROM, install.exe is located in the Windows folder.
2. Run install.exe.

HP-UX, Solaris, Linux, and AIX: To begin the VLProxy installation, do the following:

1. If installing from CD-ROM, copy the appropriate install.bin from the OS-labeled folder.
2. Open a shell.
3. Change directory (`cd`) to where you placed the installer.
4. Change file permissions to "execute": `chmod +x install.bin`.
5. At the prompt, type: `sh ./install.bin`.

The JRE is automatically installed into a subdirectory (`\jre`) of wherever VLProxy is installed. From this point on, the Windows and Unix installations are identical. **To complete the VLProxy installation, follow the instructions on the screen. It is highly recommended, for security reasons, that the installation program be deleted after the installation has completed successfully.**

NOTE: For Windows users, VLProxy will automatically be installed as a service. The user will have the opportunity to have the VLProxy service start automatically when the computer is restarted. VLProxy generally should always be running unless configuration or maintenance is in progress. Having the VLProxy service start automatically has the following advantages:

- The service can run continuously. A user does not have to be logged into the computer to start VLProxy.
- When the computer is restarted, the operator does not need to manually start the proxy.

Invoke Configuration

Invoke VLProxy configuration by changing the current directory to the VLProxy installation directory and entering

Windows: `VLProxyc -p`

HP-UX, Solaris, Linux, AIX: `./VLProxyc -p`

at the command line prompt. You will first be prompted for the configuration password. If this is a new install, the password is **Admin** (Note: The password is case sensitive). The first time you run the configuration, it is advised that you change the configuration password. Configuration parameters are discussed in detail in the next section.

Please Note: If the VLProxy service is active while making configuration changes, these changes will not take effect until the next time the VLProxy service is started. It is recommended that the service be stopped before modifying the configuration.

Set Up Unix Daemon

This section does not apply to Windows users.

WARNING: The following procedures have been tested with specific distributions of HP-UX, Solaris, Linux, and AIX; consult your system documentation to ensure that these steps are correct before starting. Review the run levels (rc#.d) and sequence numbers (S# and K#) given for appropriate values. Only the system administrator should perform these changes.

HINT: Prior to installing VLProxy as a Unix daemon, the following command from the VLProxy installed directory can be used to first verify that VLProxy is operational:

```
./VLProxyc -s "service"
```

To stop VLProxy as a service (-s):

```
VLProxyc -s "service,stop"
```

If VLProxy is currently running as a *service* (e.g. Windows service, Unix daemon), this will cause a clean shutdown.

HP-UX

1. Log in as root.
2. Change to the VLProxy installed directory.
3. Verify the VLPHOME variable in the VLProxyc script points to the VLProxy installed directory.
4. Copy the VLProxyc script to the startup/shutdown scripts directory:

```
cp VLProxyc /sbin/init.d/.
```
5. Create a symbolic link to start VLProxy:

```
ln -s /sbin/init.d/VLProxyc /sbin/rc3.d/S98VLProxyc
```
6. Log out.
7. Reboot the computer and verify VLProxy is active.

Solaris

1. Log in as root.
2. Change to the VLProxy installed directory.
3. Verify the VLPHOME variable in the VLProxyc script points to the VLProxy installed directory.
4. Copy the VLProxyc script to the startup/shutdown scripts directory:

```
cp VLProxyc /etc/init.d/.
```
5. Create a symbolic link to start VLProxy:

```
ln -s /etc/init.d/VLproxyd /etc/rc3.d/S98VLProxyd
```

6. Log out.
7. Reboot the computer and verify VLProxy is active.

Linux

1. Log in as root.
2. Change to the VLProxy installed directory.
3. Verify the VLPHOME variable in the VLProxyd script points to the VLProxy installed directory.
4. Copy the VLProxyd script to the startup/shutdown scripts directory:

```
cp VLProxyd /etc/rc.d/init.d/.
```

5. Create a symbolic link to start VLProxy:

```
ln -s /etc/rc.d/init.d/VLProxyd /etc/rc.d/rc5.d/S98VLProxyd
```

6. Log out.
7. Reboot the computer and verify VLProxy is active

AIX

1. Log in as root.
2. Change to the VLProxy installed directory.
3. Verify the VLPHOME variable in the VLProxyd script points to the VLProxy installed directory.
4. Copy the VLProxyd script to the etc directory:

```
cp VLProxyd /etc/.
```

5. Create or edit the /etc/rc.local file, adding the line:

```
/etc/VLProxyd start
```

6. If the /etc/rc.local file did not previously exist, make rc.local executable and create the inittab entry:

```
chmod +x /etc/rc.local
```

```
mkitab "rclocal:2:wait:/etc/rc.local >/dev/console 2>&1"
```

7. Log out.
8. Reboot the computer and verify VLProxy is active.

Invoke Windows Service / Unix Daemon

After configuration has been completed you need to start VLProxy in the background. If VLProxy was not already started during a reboot, the following describes how you can start VLProxy manually.

Windows: Starting VLProxy can be done either through Services in the Windows Control panel or by entering

```
net start VLProxy
```

at the command prompt. The service can be stopped through Services in the Windows Control panel or by the following command

net stop VLProxy

HP-UX, Solaris, Linux, and AIX: Reboot the system to start VLProxy. It may also be started by entering **VLProxyd start** at the command prompt, but be warned that on most systems, the service will stop when you log out. It may be manually stopped using **VLProxyd stop**.

Section 4

Configuration

In this section...

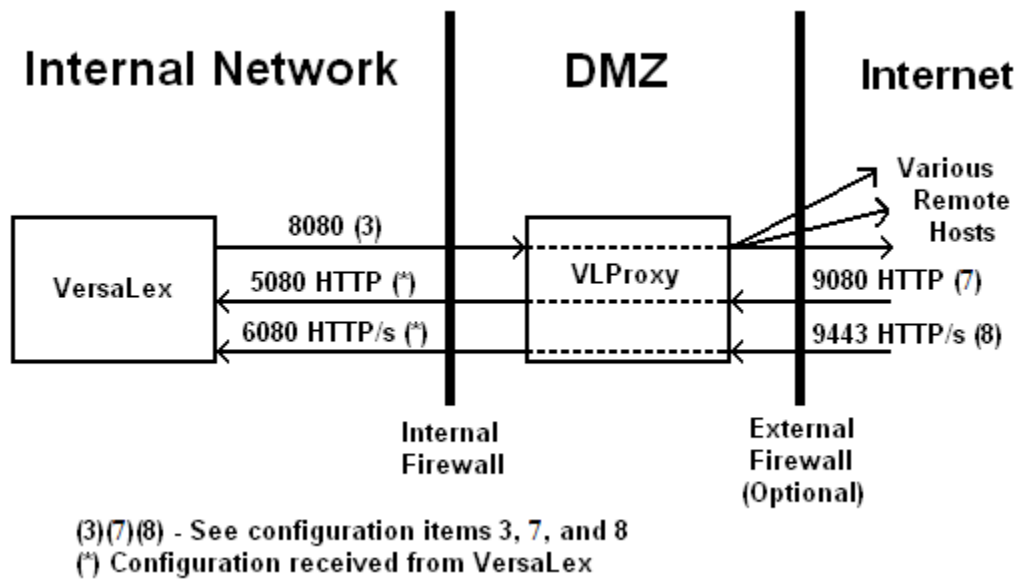
Example

VLProxy Configuration

VLTrader/LexiCom Configuration

Example

The following is a possible firewall setup. In the sample below, port 8080 is allowed from inside the firewall to VLProxy. This port is the only required port for an outbound proxy. With this setup, the VersaLex computer does not need direct access to the Internet for outbound messages. Both VersaLex configuration data and proxy requests go through this port. This port number is configured both in VLProxy and in VersaLex.



If you do not want access to the VersaLex listener ports directly from the internet, then you must enable the reverse proxy. In the example above, both an HTTP and an HTTP/s reverse proxy are enabled. This is not a typical setup but is shown for illustrative purposes. Typically, only HTTP or HTTP/s is used. If that is the case, then two of the inbound ports (either 6080/9443 or 5080/9080) could be removed from the diagram and

configuration. If HTTP and HTTP/s were used outbound and only HTTP was used inbound, then the following would be the set up for the internal and external firewalls.

Internal Firewall

- Port 8080 open outbound from Internal network to DMZ
- Port 5080 open inbound from DMZ to Internal network

External Firewall

- All ports open outbound from DMZ to remote hosts (or configure each remote host separately)
- Port 9080 open inbound from remote hosts to DMZ

VLProxy Configuration

This section describes the different VLProxy configuration values. Before proceeding with the actual configuration of VLProxy, the table in Appendix A should be completed.

Configuration is accomplished through the command line. By entering

VLProxyc -p

at the command line, you will receive an "Enter password:" prompt. The initial password for a new install is **Admin**. It is highly recommended that you change the password. The VLProxy configuration data is stored in an encrypted file called VLProxy.properties in the VLProxy "conf" directory. If this file is deleted, VLProxy can no longer be started and VLProxy will need to be reinstalled. After entering the password (which will not be displayed), a menu displaying the current settings will be displayed (see example below).

```

Configuration Parameters:
 1. Configuration Password           : *****
 2. Serial Numbers                   : VK1234-XY5678
 3. Internal Forward Proxy HTTP Ports : 8080
 4. Internal Address                  : 10.20.30.40
 5. Internal Network IDs              : 10.10,10.20.30
 6. External Address                  : 12.34.56.78
 7. External Reverse Proxy HTTP Ports : 9080
 8. External Reverse Proxy HTTPs Ports : 9443
 9. External Reverse Proxy FTP Ports  :
10. External Reverse Proxy FTPs Explicit Ports:
11. External Reverse Proxy FTPs Implicit Ports:
12. External Reverse Proxy FTP Data Ports :
13. External Reverse Proxy SSH FTP Ports :
14. VersaLex Read Timeout (seconds)    : 150
15. Remote Read Timeout (seconds)     : 150
16. Connection Backlog Size            : 50
17. SMTP Mail Server Address           : MAILSVR
18. SMTP Mail Server Username          :
19. SMTP Mail Server Password         :
20. Email on Fail Addresses            : youremail@comp.com
21. Execute on Failure Command         : failure.bat
22. Max Log File Size (Mb)            : 5
23. Log External Address               : No
24. Unknown Partner Message Action    : Forward
25. Reverse Proxy Load Balancing       : No

```

To modify an item, enter the appropriate number followed by the <Enter> key. Generally, pressing <Enter> without entering a value leaves the item unchanged. To clear entries, enter a space followed by the <Enter> key. The various configuration items are described below.

1. Configuration Password

The Configuration Password is the initial password entered to be allowed to modify the configuration data. The password is CASE SENSITIVE. This password is never displayed. The password must be at least 6 characters long. You will be prompted for this password a second time to verify you typed it correctly since it is not displayed on the screen.

2. Serial Numbers

The serial numbers are the VersaLex serial numbers allowed with this instance of VLProxy. If multiple VersaLexes are being supported, the serial numbers of the VersaLexes should be separated by commas. See Section 6, [Using VLProxy with Multiple VersaLexes](#), if VLProxy will be supporting multiple VersaLexes.

3. Internal Forward Proxy HTTP Ports

These ports are used by VersaLex to send configuration data and Forward Proxy Requests to VLProxy. The ports are also entered into the VersaLex HTTP Proxy configuration.¹

4. Internal Address

The Internal Address is used during the Reverse Proxy process. The Internal Address is the address of VLProxy when accessed from your internal network. The Internal Address will be used in response to the FTP PASV command when the address of the FTP client starts with one of the specified Internal Network IDs (below). If either the Internal Address or Internal Network IDs parameter is not specified, the External Address is used in response to the FTP PASV command.

5. Internal Network IDs

The Internal Network IDs is used during the Reverse Proxy process. This parameter is used to specify the start of addresses (partial addresses) on your internal network which need the Internal Address to be used in the FTP command PASV response or PORT request. For example, if all 10.10.ddd.ddd (where $0 \leq ddd \leq 255$) addresses in your internal network need the Internal Address use "10.10". If multiple ranges are needed, they should be separated by commas. A wildcard ("*") may be specified if you need the Internal Address to be used with any IP address. The wildcard may be necessary if for external outgoing connections your firewall replaces the Internal Address with the External Address for FTP commands.

6. External Address

The External Address is used during the Reverse Proxy process. This address is sent to VersaLex which uses it when requesting Asynchronous MDNS. This address should be the address of VLProxy (the address to which your Trading Partners are sending AS2 messages). An external address is also required for FTP, but it must be in the form of an IP address. If both a fully-qualified domain name for AS2 and an IP address for FTP is needed, it must be configured as IP address, then a comma, then the fully-qualified domain name.

7. External Reverse Proxy HTTP Ports

The External Reverse Proxy HTTP Ports are used during the Reverse Proxy process. VLProxy listens on these ports for incoming HTTP connections. The AS2 or ebMS relationship or HTTP login is verified against those identified by VersaLex, and only if valid is the request sent into VersaLex.¹

8. External Reverse Proxy HTTPs Ports

The External Reverse Proxy HTTPs Ports are used during the Reverse Proxy process. VLProxy listens on these ports for incoming HTTP/s connections. The AS2 or ebMS relationship or HTTP login is verified against those identified by VersaLex, and only if valid is the request sent into VersaLex.¹

9. External Reverse Proxy FTP Ports (for VLTrader users only)

The External Reverse Proxy FTP Ports are used during the Reverse Proxy process. VLProxy listens on these ports for incoming FTP connections. The FTP login is verified against those identified by VersaLex, and only if valid is the request sent into VersaLex.¹

10|11. External Reverse Proxy FTPs Explicit|Implicit Ports (for VLTrader users only)

The External Reverse Proxy FTPs Explicit|Implicit Ports are used during the Reverse Proxy process. VLProxy listens on these ports for incoming explicit|implicit FTP/s connections. The FTP login is verified against those identified by VersaLex, and only if valid is the request sent into VersaLex.¹

12. External Reverse Proxy FTP Data Ports

The External Reverse Proxy FTP Data Ports are used during the Reverse Proxy process. For FTP server reverse proxying (VLTrader users only), VLProxy chooses and listens on one of these ports for each incoming FTP passive mode data connection. For FTP client forward proxying, VLProxy chooses and listens on one of these ports for each incoming FTP active (a.k.a. port) mode data connection. A range of ports must be specified, separated by a dash.

13. External Reverse Proxy SSH FTP Ports (for VLTrader users only)

The External Reverse Proxy SSH FTP Ports are used during the Reverse Proxy process. VLProxy listens on these ports for incoming SSH FTP connections. The SSH FTP login (or public key) is verified with VersaLex to see if it is a valid, and only if valid is the request sent into VersaLex.¹

14. VersaLex Read Timeout (seconds)

This is the timeout value in seconds when reading from VersaLex. If the read takes longer than this value, the socket is closed and the session will be stopped. This value must be at least 30 seconds.

15. Remote Read Timeout (seconds)

This is the timeout value in seconds when reading from the remote hosts. If the read takes longer than this value, the socket is closed and the session will be stopped. This value must be at least 30 seconds.

16. Connection Backlog Size

This is the network socket port backlog size. This number should be set to the number of simultaneous connections expected on a single port. This value is applied to each port on which VLProxy is listening.

17. SMTP Mail Server Address

If you wish to have e-mail notification when VLProxy fails to connect to VersaLex during the Reverse Proxy, then you may optionally set this value to the location of the SMTP mail server. If the SMTP mail server is not set, VLProxy will attempt to derive an SMTP mail server based on the destination email address at the time e-mail notifications are sent. **NOTE:** If the e-mail on failure feature is used and you have specified an e-mail server that resides in the internal network, the internal firewall must also open port 25 for SMTP traffic from the DMZ to the internal network.

18/19. SMTP Mail Server Username/Password

If the SMTP mail server requires authentication, enter the username and password for the specified mail server.

20. Email on Fail Addresses

If you wish to have e-mail notification for certain VLProxy failures, then this value must be set to the list of e-mail addresses that should be notified. If configured, e-mail notifications will be sent if VLProxy fails to connect to VersaLex during the Reverse Proxy or if VLProxy is unable to start a reverse proxy port. The first e-mail address in the list will be considered both the FROM and the TO. Subsequent e-mail addresses will only be considered TO. The first e-mail address should be an internal e-mail address to the company. If multiple e-mail addresses are used, they should be separated by semicolons (;) or commas (,).

21. Execute on Failure Command

If you wish to have an external script or program execute when VLProxy fails to connect to VersaLex during the Reverse Proxy, then this value must be set to the command that should be executed.

22. Max Log File Size

This is the maximum log file size in Mbytes before it is archived. Archive files are created in the logs/archive sub-folder of VLProxy. Each archive will be named using the start and end date/time of the log (a unique filename (VLProxy_YYYYMMDD-HHMMSS_YYYYMMDD-HHMMSS.zip) and contains a zipped archive of the VLProxy.xml file.

23. Log External Address

This flag determines whether or not the External IP and port number are included in log events. For enhanced security you would not want to log these values. Values are Yes and No.

24. Unknown Partner Message Action

This flag determines the action when a message with an unknown AS2 or ebMS relationship is received. The valid settings are **(D)**efer, **(I)**gnore, **(R)**eject, and **(F)**orward. The following describes the actions for each of the settings:

- D**efer: The most stringent setting of the active VersaLexes control the action to perform. In VersaLex the setting can be found under Unknown Message Partner Action on the Local Listener Advanced tab.
- I**gnore: The sending system receives a valid response code ("200 OK") without any explanation of the error, even if the sending system requested a receipt.
- R**eject: Disconnect from the sending system before completing receipt of the entire message entity.
- F**orward: The incoming message is forwarded to an active VersaLex. The 'Unknown Partner Message Action' of the active VersaLex should be set to one of the Save ... options.

25. Reverse Proxy Load Balancing

This flag determines whether or not VLProxy will load balance reverse proxy requests between multiple, synchronized VersaLexes. Refer to Section 6, [Using VLProxy with Multiple VersaLexes](#) for additional information. When this value is Yes, VLProxy uses the following methods to determine which VersaLex will receive the next inbound client request.

- Relationship: Only VersaLexes with the necessary trading partner relationship (refer to Reverse Proxy Issues) are considered.
- Live versus Backup: A live (i.e. active) VersaLex has preference over any backup (i.e. passive) VersaLex. A backup VersaLex is designated with the VersaLex Configure>Synchronization Backup Only setting or through licensing.
- Least connections: A request is sent to the VersaLex with the fewest active connections.
- Round-robin: Requests are sent to each VersaLex in a sequential and circular pattern -- VersaLex 1, VersaLex 2, VersaLex 3, ..., VersaLex N.

For VersaLexes of the same type (i.e. live and synchronized), VLProxy will initially use the least connections method to determine which VersaLex will handle the connection. The VersaLex with the least active inbound and outbound connections through VLProxy will receive the next inbound connection.

- VersaLexes must be synchronized to handle AS2 asynchronous MDNs.
- VersaLexes should both be either LexiCom or both be VLTrader.
- For multiple VLProxies, their load balancing related settings should be identical.

When the number of connections is equal, the round-robin method is used. Values are Yes and No.

¹ If you are expecting more simultaneous connections than the size of the operating system network port backlog, then you may want to configure multiple ports to reduce connection attempts against a single port. If multiple ports are used, they should be separated by commas. This applies to 3. Internal Forward Proxy HTTP Ports, 7. External Reverse Proxy HTTP Ports, 8. External Reverse Proxy HTTPs Ports, 9. External Reverse Proxy FTP Ports, 10|11. External Reverse Proxy FTPs Explicit|Implicit Ports, and 13. External Reverse Proxy SSH FTP Ports.

VLTrader/LexiCom Configuration

This section describes the different VLProxy-related VersaLex configuration options. Before proceeding with the actual configuration of VersaLex, the table in Appendix A should be completed. Select Configure>Proxies... on the VersaLex menu. If the VLProxy server is not configured, then click <New> and select <HTTP Application-Level Proxy>. Enter the address of the computer running VLProxy as seen from the internal network into the 'Proxy Server Address' field. Then enter the Internal Forward Proxy HTTP Port configured in VLProxy into the 'Port #' field. Select 'Using VLProxy' to let VersaLex know the proxy is a VLProxy instead of a generic proxy. If you do not see the 'Using VLProxy' and 'Enable reverse proxying' checkboxes, then either the VersaLex software is not up-to-date or you are not licensed to run VLProxy. If you are not licensed, please contact Cleo Sales for further information.

Reverse/Inbound Proxying:

If Reverse Proxying is necessary for Inbound messages, then select the '**Enable reverse proxying**' checkbox.

1. VLProxy's external address and ports becomes the URL you give your remote trading partners. VLProxy will reverse received messages into VersaLex.
 - a. VersaLex will automatically use the VLProxy URL as the requested location to send asynchronous AS2 MDNs.

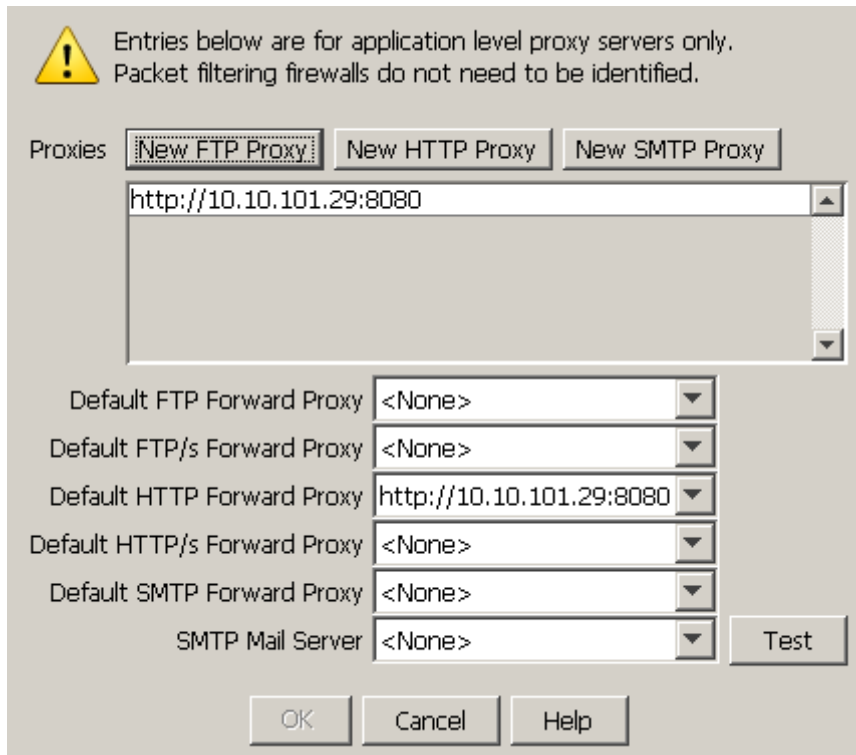
- For additional security, '**Reverse forward connections**' can be selected, which indicates that outbound forward proxy connections from VersaLex should be pooled in VLProxy and used for reverse proxy requests. This option eliminates the need for any inbound ports through the internal firewall to VLTrader/LexiCom.
- Multiple VLProxies can be configured as reverse proxies, either in a load balanced or a primary-backup arrangement. However, third-party or custom hardware/software (e.g. load balancer, manual switch) is needed to facilitate this type of setup.

Forward/Outbound Proxying:

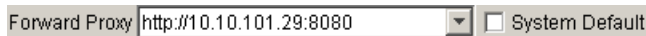
The screenshot shows a dialog box titled "HTTP Application-Level Proxy". It contains the following elements:

- * Proxy Server Address: 10.9.0.2
- * Port #: 8080
- Using VLProxy
- Enable reverse proxying
- Forward proxy backup only
- Reverse forward connections
- Forward proxy load balance
- Proxy Authentication: None (dropdown menu)
- Proxy Realm: (text field)
- * Username: (text field)
- * Password: (text field)
- OK button
- Cancel button

- You can also configure multiple VLProxies as forward proxies, again in either a load balanced arrangement by selecting '**Forward proxy load balance**' or a primary-backup arrangement by selecting '**Forward proxy backup only**'. This does not require any additional third-party or custom hardware/software.
- If you are using VLProxy as a Forward/Outbound proxy, you may do this for all FTP, FTP/s, HTTP, and HTTP/s hosts or selected hosts. For example, if you wish to use VLProxy for all outbound HTTP messages, then select the VLProxy address/port in the 'Default HTTP Forward Proxy' pulldown.

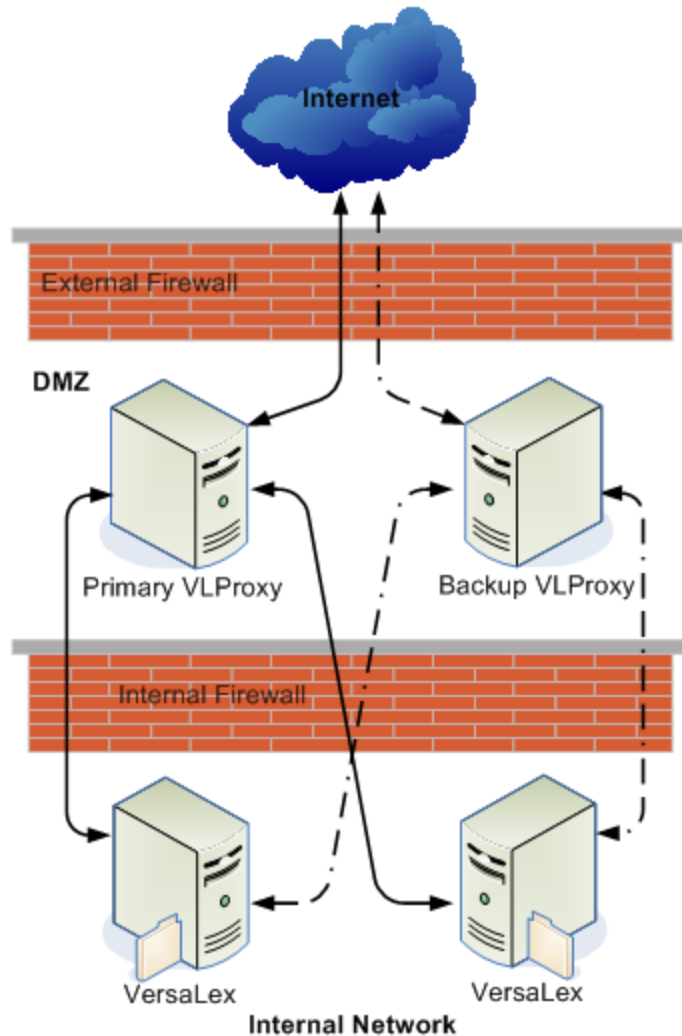


If you are using VLProxy as a Forward/Outbound proxy only for selected hosts, you must select it from the 'Forward Proxy' pulldown for each host (found on the General tab).



Dataflow:

The following figure depicts an example configuration with both a Primary and Backup Forward and Reverse VLProxy. The dashed lines show paths which are used only when the Primary paths (solid lines) are not functioning.

**Failure Scenarios:**

Refer to the figure above for a typical configuration and the following for an explanation of operation during the various failure scenarios.

VLProxy failures:

Forward: A keep-alive is sent to VLProxy every 30 seconds. When the Primary VLProxy fails, it may take up to 30 seconds for VersaLex to start using the Backup VLProxy for forward proxying. There is no limit on the number of VersaLex outbound attempts made during this 30-second time period. When the primary VLProxy is restarted and configured, forward proxying will be switched from the Backup to the Primary.

Reverse: Reverse proxying is enabled on both the Primary and Backup VLProxy as long as their 'Enable reverse proxying' checkboxes are selected. Inbound data can be received on either the Primary or the Backup VLProxy.

VersaLex failures:

Forward: The outbound data must be routed through the backup VersaLex. The backup VersaLex decides which VLProxy to use.

Reverse: It takes 90 seconds from the last keep-alive from the Primary VersaLex for VLProxy to switch to the Backup VersaLex. Then, the inbound connections are routed to the Backup until the Primary is restored and completes initialization. This timeout applies when reverse proxying is enabled for inbound connections only.

Section 5

System Log File

System log file format

Located in '\logs\VLProxy.xml', the system log file is an XML file. While VLProxy is running, the log is continually appended with any messages generated by active Forward and Reverse Proxies. However, even though it is continuously updated, the log is always a valid and well-formed XML file.

The log XML file is formatted as follows:

- One and only one <Log> exists in the file.
- <Log> may contain one or more <Session>s.
- <Session> has the product name and version.
- <Session> contains one <System> and one <Run>.
- <System> has information about the computer.
- <Run> has the <Session> starting date/time stamp, <Thread> number, and <Event> number.
- <Run> may contain one or more <Event>s.
- <Event> contains either <Detail>, <ProxyConnect>, <Request>, <Response>, <Result>, or <ProxyDisconnect> always followed by <Mark>.
- <Detail> provides extra detailed information anywhere in the flow.
- <ProxyConnect> provides information about direction (Inbound or Outbound), URL, and optionally connection IP and port.
- <Request> contains the protocol-specific request made to the host.
- <Response> contains the protocol-specific response from the host.
- <Result> marks the end of a request and has resultant status.
- <ProxyDisconnect> provides information about direction (Inbound or Outbound) and the number of seconds the connection was active.
- <Mark> has the date/time stamp and corresponding <Thread> number (TN=), <Command> number (CN=), and <Event> number (EN=).

Because more than one action can be active at any given time, the <Thread> number and <Command> number references provide a means for grouping related <Event>s together.

The following is a sample log file.

```
<?xml version="1.0" standalone="yes" ?>
<Log descName="Cleo Communications application log file">
  <Session appName="VLProxy" version="1.0" cmdLine="-s service">
    <System name="BBowley1" address="10.10.101.29" locale="USA" timeZone="CST"
      OS="Windows XP" version="5.1" java="1.3.1_09" userName="bbowley"
      workDir="C:\Program Files\VLProxy" />
    <Run date="2004/03/01 15:19:28" TN="1" EN="1">
      <Event>
        <Detail level="1">Operating System backlog is 5 connections.</Detail>
        <Mark date="2004/03/01 15:19:29" TN="1" CN="1" EN="1" />
      </Event>
      <Event>
        <Detail level="1">Starting Forward HTTP proxy on port 8080</Detail>
        <Mark date="2004/03/01 15:19:29" TN="1" CN="1" EN="2" />
      </Event>
      <Event>
        <Detail level="1">Received initialization data from VL0001-XXXXXX</Detail>
        <Mark date="2004/03/01 15:19:40" TN="1" CN="1" EN="3" />
      </Event>
      <Event>
        <Detail level="1">Received AS2 Local Host data from VL0001-XXXXXX</Detail>
        <Mark date="2004/03/01 15:19:40" TN="1" CN="1" EN="4" />
      </Event>
      <Event>
        <Detail level="1">VL0001-XXXXXX set Allow Reverse Proxy to false</Detail>
        <Mark date="2004/03/01 15:19:40" TN="1" CN="1" EN="5" />
      </Event>
      <Event>
        <Detail level="1">Received AS2-To/From data from VL0001-XXXXXX</Detail>
        <Mark date="2004/03/01 15:19:40" TN="1" CN="1" EN="6" />
      </Event>
      <Event>
        <Detail level="1">Received SSL Socket data from VL0001-XXXXXX</Detail>
        <Mark date="2004/03/01 15:19:40" TN="1" CN="1" EN="7" />
      </Event>
      <Event>
        <Detail level="1">VL0001-XXXXXX set Allow Reverse Proxy to false</Detail>
        <Mark date="2004/03/01 15:19:40" TN="1" CN="1" EN="8" />
      </Event>
      <Event>
        <Detail level="1">Received CA Certificate data from VL0001-XXXXXX</Detail>
        <Mark date="2004/03/01 15:19:40" TN="1" CN="1" EN="9" />
      </Event>
      <Event>
        <Detail level="1">VL0001-XXXXXX set Allow Reverse Proxy to true</Detail>
        <Mark date="2004/03/01 15:19:41" TN="1" CN="1" EN="11" />
      </Event>
      <Event>
        <Detail level="1">Starting Reverse HTTP proxy on port 5050</Detail>
        <Mark date="2004/03/01 15:19:41" TN="1" CN="1" EN="12" />
      </Event>
      <Event>
        <Detail level="1">Starting Reverse HTTPs proxy on port 443</Detail>
        <Mark date="2004/03/01 15:19:41" TN="1" CN="1" EN="13" />
      </Event>
      <Event>
    </Event>
  </Run>
</Session>
</Log>
```

```
<ProxyConnect direction="Outbound" sourceIP="10.10.101.29" sourcePort="3146"
  destURL="test.cleo.com" />
<Mark date="2004/03/01 15:20:03" TN="1" CN="6" EN="14" />
</Event>
<Event>
  <Request text="POST" type="HTTP" />
  <Mark date="2004/03/01 15:20:03" TN="1" CN="6" EN="15" />
</Event>
<Event>
  <Response host="200 OK" />
  <Mark date="2004/03/01 15:20:04" TN="1" CN="6" EN="16" />
</Event>
<Event>
  <Result text="Success" direction="Outbound" bytes="2114" seconds="0.02" />
  <Mark date="2004/03/01 15:20:04" TN="1" CN="6" EN="17" />
</Event>
<Event>
  <ProxyDisconnect direction="Outbound" secondsConnected="0.77" />
  <Mark date="2004/03/01 15:20:04" TN="1" CN="6" EN="18" />
</Event>
</Run>
</Session>
</Log>
```

Monitor System log file

While VLProxy is active, you can use a special command in VLProxy to watch the Log file. At the command prompt, enter the following command.

VLProxyc -m

This will display the last few items in the system log and continue to display any new events logged. To stop the log display, press the Enter key.

Section 6

Using VLProxy with Multiple VersaLexes

Introduction

A single VLProxy can support multiple VersaLexes installed on multiple computers inside the firewall. The proxied VersaLexes can be either **non-redundant** (distributed) or **redundant** (synchronized) or a combination of each. This is a very powerful feature to reduce the number of open ports in the outside firewall. All of the VersaLexes can share the same inbound and outbound ports.

Non-Redundant VersaLexes

Each of the distributed VersaLexes can use the same VLProxy in a forward/outbound direction without issue. However, when using VLProxy as a reverse proxy for distributed VersaLexes, there are a few issues of which you must be aware.

Reverse Proxy Issues

1. Inbound (reverse proxy) traffic is routed to the appropriate VersaLex based on the AS2 To/From relationship. The inbound traffic will be routed to the first active VersaLex found with a matching To/From relationship. This means that if duplicate AS2 relationships exist, then it is possible for the incoming message to go to a VersaLex which you did not intend. This is especially true for incoming MDNs where one VersaLex sends the initial message and the MDN comes back to a different VersaLex. Therefore, do not duplicate AS2 relationships between non-redundant VersaLexes. If a host/mailbox is disabled, then the AS2 relationship will not be forwarded to VLProxy and therefore will not be considered a duplicate. **Please note:** This means that a particular "Cleo AS2 System Test" host should not be active/enabled in more than one VersaLex.
2. Similarly for the ebXML message service (ebMS), inbound ebMS traffic is routed to the appropriate VersaLex based on the CPA Id. And similarly, for VLTrader users using the FTP or SSH FTP or HTTP server, inbound traffic is routed to the appropriate VersaLex based on the login.
3. VLProxy's inbound ports will accept incoming connections when at least one of the VersaLexes is active. If an incoming message is determined to be for an inactive

VersaLex, the trading partner will receive a "503 Service Unavailable" and the message will not be transferred.

4. Certain settings are used by VLProxy in setting up the reverse proxy port(s). Having inconsistent settings between the VersaLexes can lead to a communications failure with your trading partners. These settings are described in the following section.

VersaLex Settings Used by VLProxy for Reverse Proxying

It is highly recommended that certain communication items in VersaLex be set up the same between all the different VersaLexes using the same VLProxy. The following item should be set consistently across the VersaLexes if Reverse Proxying is enabled.

- **Unknown Partner Message Action** - VLProxy uses this setting to determine what to do when an unknown AS2 relationship is found during a reverse proxy. If the settings are different between the VersaLexes, then the most conservative setting of the different VersaLexes will be used. The order of the settings from most conservative to least conservative is as following: REJECT, IGNORE, SAVE. If it is determined there are different settings among the VersaLexes, a message will be logged to the VLProxy log file. **NOTE:** VLProxy also has an Unknown Partner Message Action setting that can be used as an overriding factor to the VersaLex setting.

The following items should be set consistently across the VersaLexes if Reverse Proxying via HTTP/s and/or FTP/s is enabled.

- **SSL Server Certificate** - VLProxy uses the SSL Server Certificate from VersaLex for the HTTP/s and FTP/s reverse proxy port(s). Only one server certificate can be active on a port. If each VersaLex has its own SSL certificate, then VLProxy will chose a certificate from one of the active VersaLexes. Your trading partners will then need to trust ALL of the SSL certificates for each of the VersaLexes. If you use the same one on all VersaLexes, then the trading partners will only need the one certificate. If it is determined there are different settings among the VersaLexes, a message will be logged to the VLProxy log file.
- **Authenticate Client** - VLProxy uses the Authenticate Client setting to determine whether the client should be authenticated during the SSL handshake. If any of the VersaLexes have Authenticate Client turned ON, then authentication will occur for all inbound SSL connections. This would require all certificates for all trading partners to be present in the various VersaLexes regardless of the Authenticate Client setting in the respective VersaLex. An inbound connection will pass authentication if the trading partner's certificate is present in any of the active VersaLexes. If it is

determined there are different settings among the VersaLexes, a message will be logged to the VLProxy log file.

Redundant (Synchronized) VersaLexes

Redundant VersaLexes can be easily configured in VLProxy. The order in which the VersaLex serial numbers are listed during configuration indicates precedence. If [Reverse Proxy Load Balancing](#) is not enabled, the first redundant VersaLex listed is the primary installation and the second redundant VersaLex listed is the backup installation. VLProxy will forward incoming traffic to a backup VersaLex if the primary installation is not currently connected. Once a primary installation reconnects to VLProxy, it will again be forwarded incoming traffic.

In fact, multiple redundant backups of a single primary installation are supported. Again simply list the serial numbers of the backups by order of precedence when configuring VLProxy.

Both non-redundant and redundant VersaLexes together are also supported. Just make sure to configure the serial numbers of the redundant VersaLexes by order of precedence. The order of the non-redundant VersaLex serial number "groups" is not important.

If Reverse Proxy Load Balancing is enabled, the ordering of the serial numbers described above does not apply. Instead, the Reverse Proxy Load Balancing methods for determining which VersaLex is forwarded the incoming traffic are used. A backup VersaLex must be designated with the VersaLex Configure>Synchronization Backup Only setting or through licensing.

Section 7

Debug Options

Command-line Debug Options

VLProxy can be started in Debug Mode by running it from the command line. You can debug to the screen, a file, or both. There are two levels of debugging. The first is high-level debugging only and the second is full debug mode. The following shows the syntax for VLProxy debugging.

VLProxyc -s service -d<Level> [<OutputMode>]

<Level> is either **1** for high-level debugging or **2** for full debug.

<OutputMode> is either **file** for outputting to a debug file in the logs directory, **screen** for outputting to the screen only, or **both** to output to both the file and the screen.

The debug data logged is application specific and will not be described. Debug mode is for advanced users or when speaking with Cleo Technical Support.

Note: The debug file is not archived so debug should not be left on for an extended period of time.

To view the version information for VLProxy, enter the following command.

VLProxyc -s version

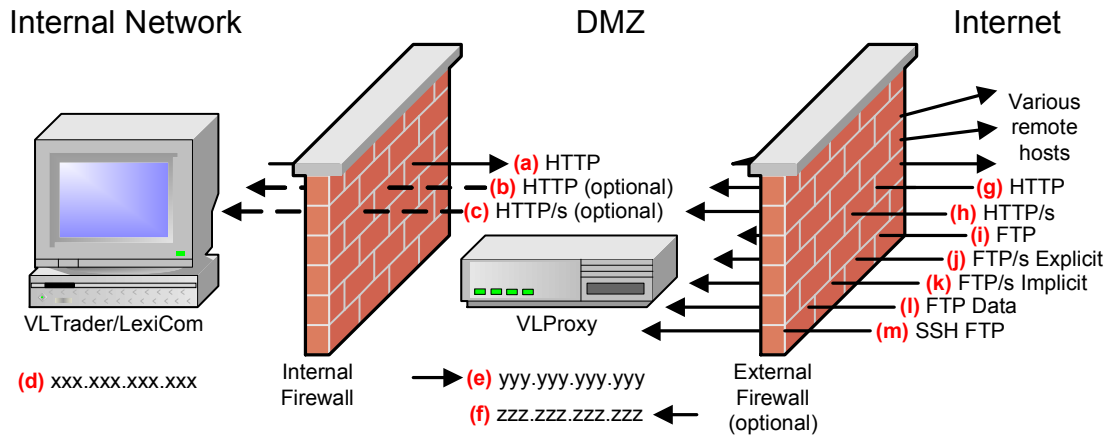
This will display the version of the product along with information for each of the .jar files in the product.

Appendix A

Single VLProxy<>VersaLex Configuration Guide

This Appendix should be used as an aid in setting up your firewall(s), VersaLex, and VLProxy. It describes the ports necessary to be opened through the firewall(s) and where the different VersaLex and VLProxy configuration parameters are located.

Configuration Diagram



Note: Generally, HTTP/s is not used for most AS2 trading partners. Therefore, items (c) and (h) are not normally configured in VersaLex or VLProxy when just AS2 is being proxied. However, when using the VLTrader FTP server and reverse proxying FTP/s through VLProxy, then item (c) HTTP/s should be configured in VersaLex. (In fact, if HTTP/s is not configured in the VersaLex Local Listener HTTP tab, then an SSL server certificate must be configured in the FTP tab instead in order to provide a certificate to VLProxy for serving FTP/s connections.)

Configuration Worksheet

This table contains the different configuration values you should determine before proceeding with the actual software configuration. You should work with your firewall administrator to determine which ports are available.

	Title	Firewall Notes	VLProxy Configuration Location	VersaLex Configuration Location	User Values
(a)	Forward Proxy Port(s)	Port(s) must be opened from VLTrader/LexiCom to VLProxy*	<ul style="list-style-type: none"> VLProxy configuration screen (#3) (Figure 1) 	<ul style="list-style-type: none"> HTTP Application-Level Proxy (Figure 4) 	
(b)	Local Listener HTTP Port(s)	Port(s) must be opened from VLProxy to VLTrader/LexiCom* unless using the Reverse forward connections option		<ul style="list-style-type: none"> HTTP tab (Figure 2) 	
(c)	Local Listener HTTP/s Port(s)	Port(s) must be opened from VLProxy to VLTrader/LexiCom* unless using the Reverse forward connections option		<ul style="list-style-type: none"> HTTP tab (Figure 2) 	
(d)	VersaLex Computer IP Address	IP address of VLTrader/LexiCom computer as seen from VLProxy		<ul style="list-style-type: none"> AS2 tab under the Local Listener's AS2 Service (Figure 3) 	
(e)	VLProxy Computer Internal Address	Port(s) for (g)-(m) must be opened from your internal network to VLProxy only if internal trading partners are also accessing VLProxy*	<ul style="list-style-type: none"> VLProxy configuration screen (#4) (Figure 1) 	<ul style="list-style-type: none"> HTTP Application-Level Proxy (Figure 4) 	
(f)	VLProxy Computer External Address	Address of VLProxy computer as seen from the Internet (IP address and/or fully-qualified domain name)	<ul style="list-style-type: none"> VLProxy configuration screen (#6) (Figure 1) 		
(g)	External Reverse Proxy HTTP Port(s)	Port(s) must be opened from the Internet to VLProxy*	<ul style="list-style-type: none"> VLProxy configuration screen (#7) (Figure 1) 		
(h)	External Reverse Proxy HTTP/s Port(s)	Port(s) must be opened from the Internet to VLProxy*	<ul style="list-style-type: none"> VLProxy configuration screen (#8) (Figure 1) 		

(i)	External Reverse Proxy FTP Port(s)	VLTrader users only Port(s) must be opened from the Internet to VLProxy*	• VLProxy configuration screen (#9) (Figure 1)		
(j)	External Reverse Proxy FTP/s Explicit Port(s)	VLTrader users only Port(s) must be opened from the Internet to VLProxy*	• VLProxy configuration screen (#10) (Figure 1)		
(k)	External Reverse Proxy FTP/s Implicit Port(s)	VLTrader users only Port(s) must be opened from the Internet to VLProxy*	• VLProxy configuration screen (#11) (Figure 1)		
(l)	External Reverse Proxy FTP Data Port(s)	Port(s) must be opened from the Internet to VLProxy*	• VLProxy configuration screen (#12) (Figure 1)		
(m)	External Reverse Proxy SSH FTP Port(s)	VLTrader users only Port(s) must be opened from the Internet to VLProxy*	• VLProxy configuration screen (#13) (Figure 1)		

*** In regards to firewall rules, the ports listed above are all destination ports. In all cases, the source ports can be ANY port number.**

VLProxy Configuration Screen

The VLProxy configuration screen is displayed by entering

```
VLProxyc -p
```

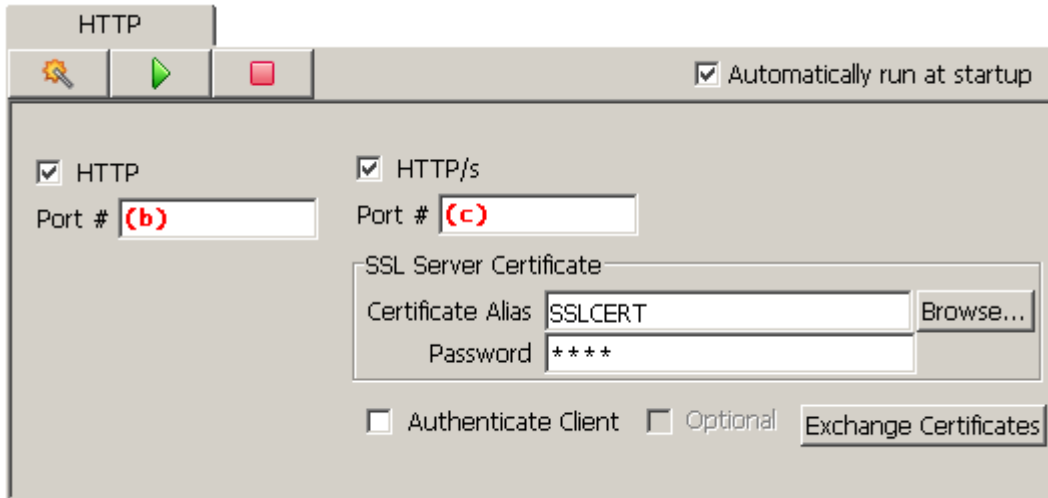
at the command line and entering the correct password.

```
Configuration Parameters:
 1. Configuration Password           : *****
 2. Serial Numbers                   : VK1234-XY5678
 3. Internal Forward Proxy HTTP Ports : (a)
 4. Internal Address                  : (e)
 5. Internal Network IDs              :
 6. External Address                  : (f)
 7. External Reverse Proxy HTTP Ports : (g)
 8. External Reverse Proxy HTTPs Ports : (h)
 9. External Reverse Proxy FTP Ports  : (i)
10. External Reverse Proxy FTPs Explicit Ports: (j)
11. External Reverse Proxy FTPs Implicit Ports: (k)
12. External Reverse Proxy FTP Data Ports : (l)
13. External Reverse Proxy SSH FTP Ports : (m)
14. VersaLex Read Timeout (seconds)    : 200
15. Remote Read Timeout (seconds)     : 150
16. Connection Backlog Size            : 5
17. SMTP Mail Server Address           : MAILSVR
18. SMTP Mail Server Username          :
19. SMTP Mail Server Password         :
20. Email on Fail Addresses            : itsupport@company.com
21. Execute on Failure Command         :
22. Max Log File Size (Mb)             : 5
23. Log External Address                : Yes
24. Unknown Partner Message Action     : Defer
25. Reverse Proxy Load Balancing       : No
```

Figure 1

VLTrader/LexiCom Configuration Screens

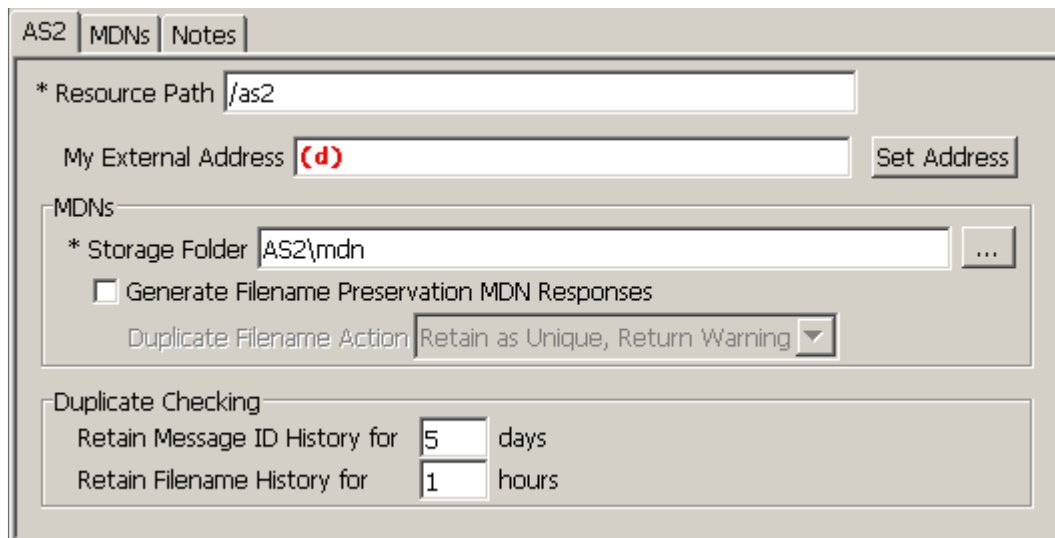
The following screen shows the HTTP tab of the Local Listener.



The screenshot shows the 'HTTP' configuration window. At the top, there are three icons: a lightning bolt, a green play button, and a red stop button. To the right, there is a checkbox labeled 'Automatically run at startup' which is checked. Below this, there are two main sections. The first section has a checked checkbox for 'HTTP' and a text input field for 'Port #' containing '(b)'. The second section has a checked checkbox for 'HTTP/s' and a text input field for 'Port #' containing '(c)'. Below these, there is an 'SSL Server Certificate' section with a text input for 'Certificate Alias' containing 'SSLCERT' and a 'Browse...' button, and a text input for 'Password' containing '****'. At the bottom, there are two unchecked checkboxes: 'Authenticate Client' and 'Optional', followed by an 'Exchange Certificates' button.

Figure 2

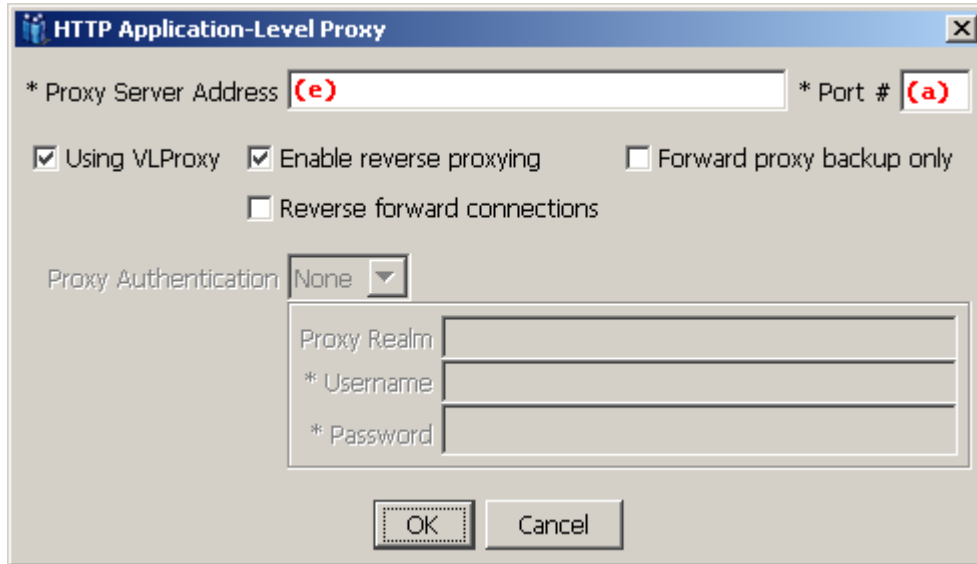
The following screen displays the AS2 tab under the Local Listener's AS2 Service.



The screenshot shows the 'AS2' configuration window. At the top, there are three tabs: 'AS2', 'MDNs', and 'Notes'. The 'AS2' tab is selected. Below the tabs, there is a text input field for '* Resource Path' containing '/as2'. Below that, there is a text input field for 'My External Address' containing '(d)' and a 'Set Address' button. Below this, there is an 'MDNs' section with a text input field for '* Storage Folder' containing 'AS2\mdn' and a '...' button. Below that, there is a checkbox for 'Generate Filename Preservation MDN Responses' which is unchecked, and a dropdown menu for 'Duplicate Filename Action' containing 'Retain as Unique, Return Warning'. Below this, there is a 'Duplicate Checking' section with two text input fields: 'Retain Message ID History for' containing '5' and 'days', and 'Retain Filename History for' containing '1' and 'hours'.

Figure 3

The following screen shows the HTTP Application-Level Proxy screen. It can be found under Configure>Proxies and is used when either editing an existing HTTP proxy or adding a new HTTP proxy. Select [Reverse forward connections](#) to eliminate the need for any inbound ports through the internal firewall to VLTrader/LexiCom.



The screenshot shows a dialog box titled "HTTP Application-Level Proxy". It contains the following fields and options:

- * Proxy Server Address: (e)
- * Port #: (a)
- Using VLProxy
- Enable reverse proxying
- Forward proxy backup only
- Reverse forward connections
- Proxy Authentication: None (dropdown menu)
- Proxy Realm: [text field]
- * Username: [text field]
- * Password: [text field]
- OK button
- Cancel button

Figure 4

The following screen shows the Configure>Proxies screen after VLProxy has been configured and selected as the default forward proxy.

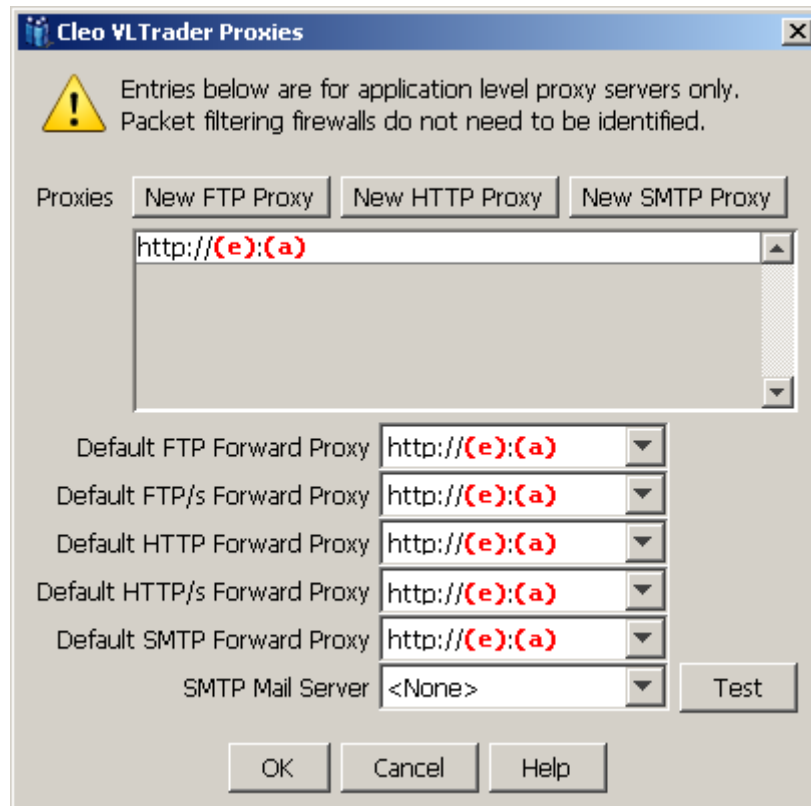
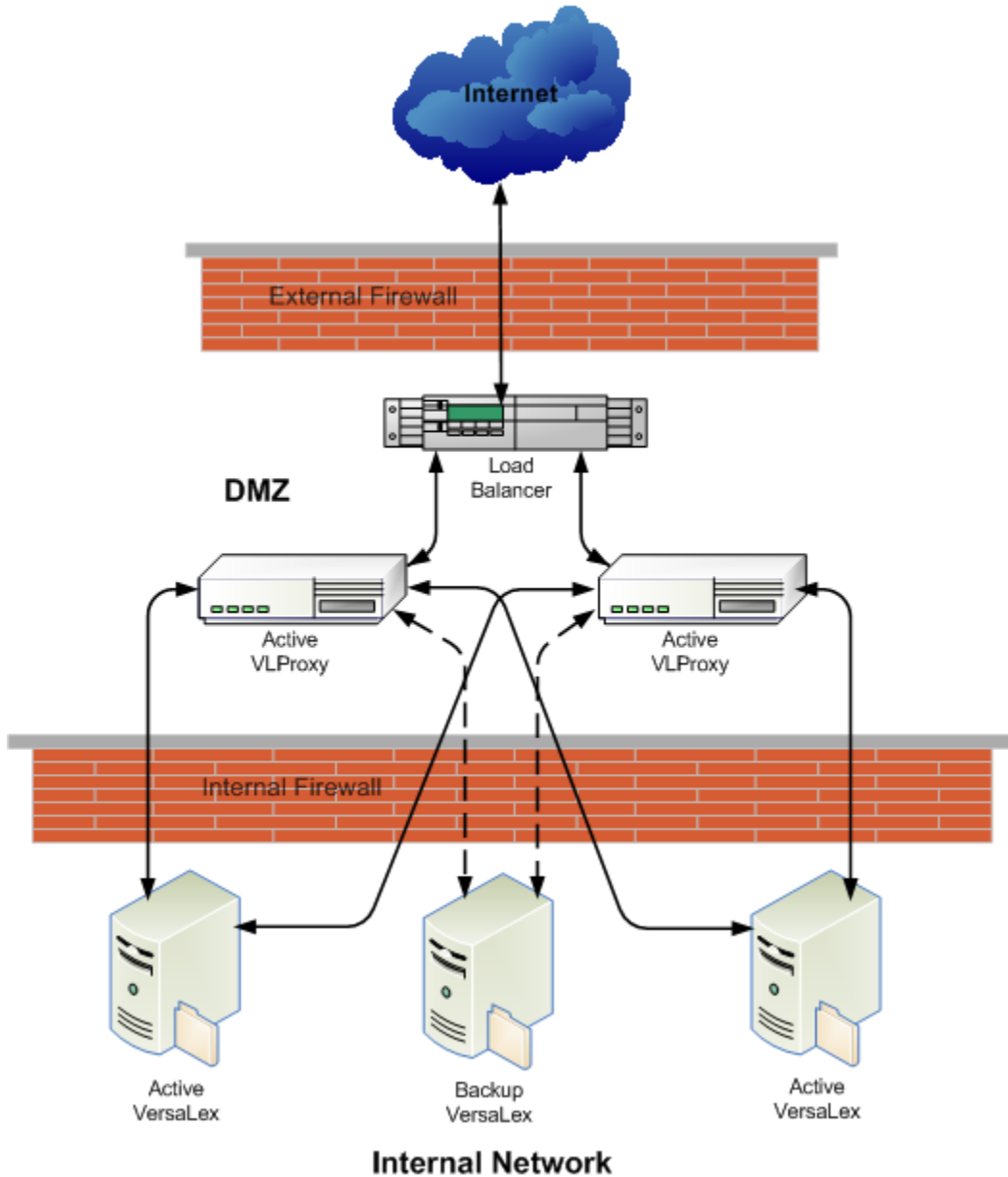


Figure 5

Appendix B

High Availability Configuration Guide

This Appendix should be used as an aid in setting up a high availability environment with multiple, synchronized VersaLexes and, optionally, multiple VLProxies. For example:



Please read the guide carefully and follow the steps in the order outlined.

First VLProxy<>VersaLex

Setup addresses and ports in the first VLProxy and VersaLex as outlined in Appendix A [Single VLProxy<>VersaLex Configuration Guide](#).

Additional VersaLexes

Install and license the additional VersaLex(es), but do not enter any configuration other than setting the Local Listener HTTP port if the default is not to be used. This is because the first VersaLex contains the starting point of the configuration, and any modifications entered now into an additional VersaLex will be overlaid when synchronization is initialized.

Once installation and licensing of the additional VersaLex(es) is complete, go to VLProxy and add the additional VersaLex [Serial Number\(s\)](#) in the [VLProxy Configuration Screen](#).

Now go back to the first VersaLex and Configure>Synchronization>[Add VersaLex] to add each VersaLex pairing:

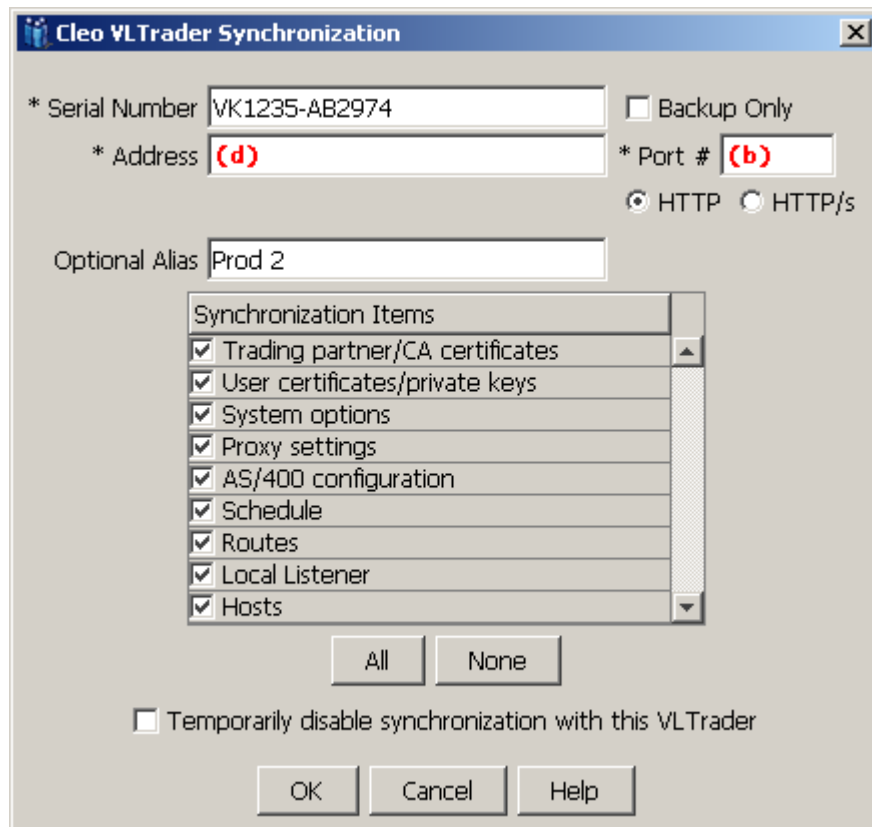


Figure 6

Enter the **Serial Number** of the additional VersaLex. The **Address** and **Port** are the address and port of the additional VersaLex as seen by the first VersaLex (from Appendix A [Single VLProxy<>VersaLex Configuration Guide](#), the **(d)** and **(b)** values for this VersaLex). To

distinguish the multiple VersaLexes, an **Optional Alias** can be entered which will be included in the VersaLex UI title bar.

Normally all items are synchronized, but at a minimum the following should be selected:

- Trading partner/CA certificates**
- User certificates/private keys**
- Proxy settings** (if using VLProxy or a 3rd party forward proxy)
- Schedule**
- Routes** (if applicable)
- Hosts**

Note: Synchronized VersaLexes should use shared file server inbox/outbox directories (or a shared database if using VLTrader database payload). If using the VLTrader payload router, synchronized VersaLexes should also use a shared file server autoroute directory.

For an active-active VersaLex inbound/outbound configuration (i.e. load balanced),

- Make sure **Backup Only** is turned off in the Configure>Synchronization pairing, and
- If using VLProxy to reverse proxy inbound requests, go to VLProxy and turn on [Reverse Proxy Load Balancing](#) in the [VLProxy Configuration Screen](#).

Otherwise, for an active-passive VersaLex inbound/outbound configuration (i.e. primary/backup),

- Turn on **Backup Only** in the Configure>Synchronization pairing, and
- If using VLProxy to reverse proxy inbound requests, go to VLProxy and ensure the primary VersaLex [Serial Number\(s\)](#) are listed first in the VLProxy configuration before the backup VersaLex [Serial Number\(s\)](#) in the [VLProxy Configuration Screen](#).

Once the Configure>Synchronization>[Add VersaLex] dialog is OKed, select [Yes] to the subsequent prompts to allow the initial synchronization to occur. Once the VersaLex synchronization status indicates "Waiting for sync requests", initialization has been completed. At this point, modifications entered at either VersaLex are synchronized instantly with the other VersaLex(es).

In VersaLex, go to Configure>Options>Other>Synchronized Backup Failover to set the amount of minutes between when an active VersaLex is first detected as down before a backup VersaLex is activated (default 5 minutes).

If not using VLProxy to reverse proxy inbound requests, then a 3rd party software/hardware device (e.g. network load balancer or router, etc., not provided by Cleo) must be placed in front of the synchronized VersaLexes. Depending on the device, it may offer options for either an active-active or active-passive configuration inbound to the VersaLexes.

Net result:

- The VersaLex schedule will be load balanced between the active, primary VersaLexes. The active VersaLex with the lowest serial number is the "master" scheduler. If an active VersaLex should go down, a backup VersaLex is activated and will begin to run scheduled actions.
 - o If using VLTrader outgoing database payload, load balanced and backup VersaLexes are managed similar to the VersaLex schedule using a "master" database payload controller.
 - o If using the VLTrader payload router, again a "master" router is employed, but even if the VersaLexes are configured in an active-active configuration, only the "master" router sends outgoing requests.

- If using VLProxy as a forward proxy, each active VersaLex will forward outbound requests through VLProxy.
- If using VLProxy as a reverse proxy, VLProxy will load balance inbound requests between the active, primary VersaLexes. If an active VersaLex should go down, VLProxy will activate a backup VersaLex and begin to send it inbound requests.
- For layouts involving more than two VersaLexes, a mixture of active-active and active-passive can be deployed (e.g. three VersaLexes in an active-active-passive configuration).

Additional VLProxies

Install the additional VLProxy(es) and enter the same configuration in the [VLProxy Configuration Screen](#) as the first VLProxy except for the Internal Address **(e)** and maybe the Internal Forward Proxy HTTP Port **(a)**.

Then, on any VersaLex, go to Configure>Proxies>[New HTTP Proxy] to make VersaLex aware of each additional VLProxy:

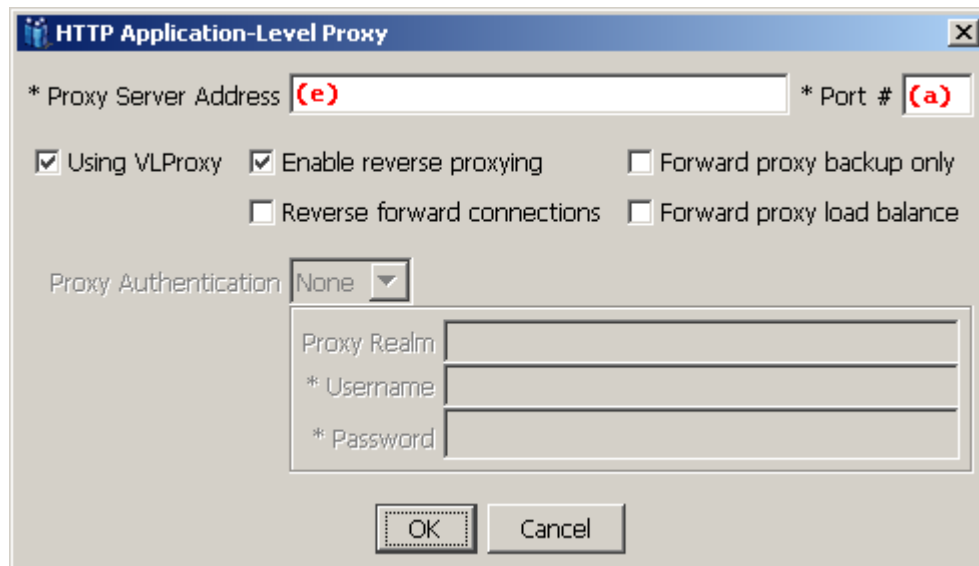


Figure 7

Enter the proxy address and port (from Appendix A [Single VLProxy<->VersaLex Configuration Guide](#), the Internal Address **(e)** and Internal Forward Proxy HTTP Port **(a)** values for this VLProxy).

Match the settings from the first VLProxy for **Enable reverse proxying** and [Reverse forward connections](#).

For an active-active VLProxy outbound configuration (i.e. load balanced),

- Turn on **Forward proxy load balance** (which turns it on for all VLProxies).

Otherwise, for an active-passive VLProxy outbound configuration (i.e. primary/backup),

- The first VLProxy is the primary proxy. Set this additional VLProxy to **Forward proxy backup only**.

Note: With either **Forward proxy load balance** or **Forward proxy backup only** selected, the default forward proxy settings for the first VLProxy (see [Figure 5](#)) carry over to this additional VLProxy.

If using VLProxy to reverse proxy inbound requests, then a 3rd party software/hardware device (e.g. network load balancer or router, etc., not provided by Cleo) must be placed in front of the multiple VLProxies. Depending on the device, it may offer options for either an active-active or active-passive configuration inbound to the VLProxies.

Net result:

- If using VLProxy as a forward proxy, each active VersaLex will split outbound requests between the load balanced VLProxies. If an active VLProxy should go down, VersaLex will begin to send a backup VLProxy outbound requests.
- If using VLProxy as a reverse proxy, a 3rd party device (i.e.) is needed in front of the VLProxies.
- For layouts involving more than two VLProxies, a mixture of active-active and active-passive can be deployed (e.g. three VLProxies in an active-active-passive configuration).