Written by : Barak Weichselbaum, all rights reserved 2000-2009

Site: http://www.komodia.com/
Email : barak@komodia.com

KOMODIA'S REDIRECTOR
Installation Manual
By Barak Weichselbaum

Introduction

This manual covers the installation and usage of: “Komodia’s Redirector” product.

Components

The Redirector package includes the following components:

PCProxy Service

Acts both as the proxy that accepts connections from the redirected clients and as the server that handles configuration and control of the product. (exposes API using COM interface and can be programmed by any COM able language such as: VB, Delphi, VC)

LSP DLL

This module performs the actual redirection. It communicates with the PCProxy service to get the redirection rule set.

Komodia’s Advanced LSP Installer

Used to install and uninstall the LSP DLL.

Installation

First, extract the .zip file into a single directory and follow the installation instructions of each component.

All installation commands are run from a console window (cmd.exe). In Vista you must run this with “administrative privileges”. The current directory must be the directory into which you unpacked the .zip file.

Under Vista you can install PCProxy as a **service only**.

PCProxy Service

To install the “PCProxy” as a service run:

```
PCProxy /Service
```

To install the “PCProxy” as an EXE (Will run when the LSP or VB console tries to communicate with it, this option is for XP only):

```
PCProxy /RegServer
```

PCProxy as a service

PCProxy can be started and stopped from either the services control panel or via “net” (OS utility).

To start the service - run from the command prompt:

```
net start pcproxy
```

To stop the service - run from the command prompt:

```
net stop pcproxy
```

PCProxy load sequence

After PCProxy is installed as a standalone or as a service, the first call from the LSP or GUI console will activate it. Of course, it is possible to set PCProxy to load automatically when installed as a service.

LSP DLL

To install the “LSP DLL” run:

```
RegisterLSP –b –d PCProxy.dll
```

Updating

PCProxy

If PCProxy.EXE file has the same COM interface (this will be mentioned whenever an update is sent), then the file can simply be replaced. In case the COM interface was changed (which will be mentioned in the update), then you must replace the file and re-run the installation command like you did at the install phase.

LSP DLL

To update the LSP DLL, replace the old LSP DLL and re-run the installation command like you did at the install phase.

Uninstallation

All uninstallation commands are run from a console window (cmd.exe). In Vista you must run this with "administrative privileges". The current directory must be the directory into which you unpacked the .zip file.

PCProxy Service

To uninstall the "PCProxy" (same procedure for Service and for non Service installation) run:

```
PCProxy /UnregServer
```

LSP DLL

To uninstall the "LSP DLL" run:

```
RegisterLSP –f
```

Usage

The LSP intercepts all traffic based on the rules predefined by the user, and redirects it to the proxy. The rules are all configured by using the application: "PCController.exe"

Required external files

The VB console uses two external system OCX files, comdlg32.ocx and mscomctl.ocx. Some computers don't have them installed, so if the console outputs an error you must obtain them.

Settings load sequence

The Redirector's settings are saved in a file called PCProxy.ini and it is located under %system32% This file is loaded automatically whenever PCProxy starts (this file is updated whenever pressing the "save" button)

Rules type

There are three separate rules. Each can be set into one of two modes:

- Intercept only the items in the list (default) – Only session information that matches the information in the list will be redirected. For example, placing "iexplore.exe" in the applications list will cause all traffic from Internet Explorer to be redirected.
- Intercept all *except* items in the list – The LSP will intercept all sessions but ignore those whose information are on the list. For example, placing "iexplore.exe" in the application list will cause all traffic except that which originates from Internet Explorer to be redirected.

Application rule

Will intercept/exclude (depending on mode) the session based on application name.

Port rule

Will intercept/exclude (depending on mode) the session based on destination port.

IP rule

Will intercept/exclude (depending on mode) the session based on destination IP.

Rules logic

Rules are logical OR, which means that if one of the rules matches the session information, then the session will be redirected.

For example, placing port 80 in the ports list and "iexplore.exe" in the application list means that redirected sessions will be those that either are opened to port 80, or originate from Internet Explorer, or both.

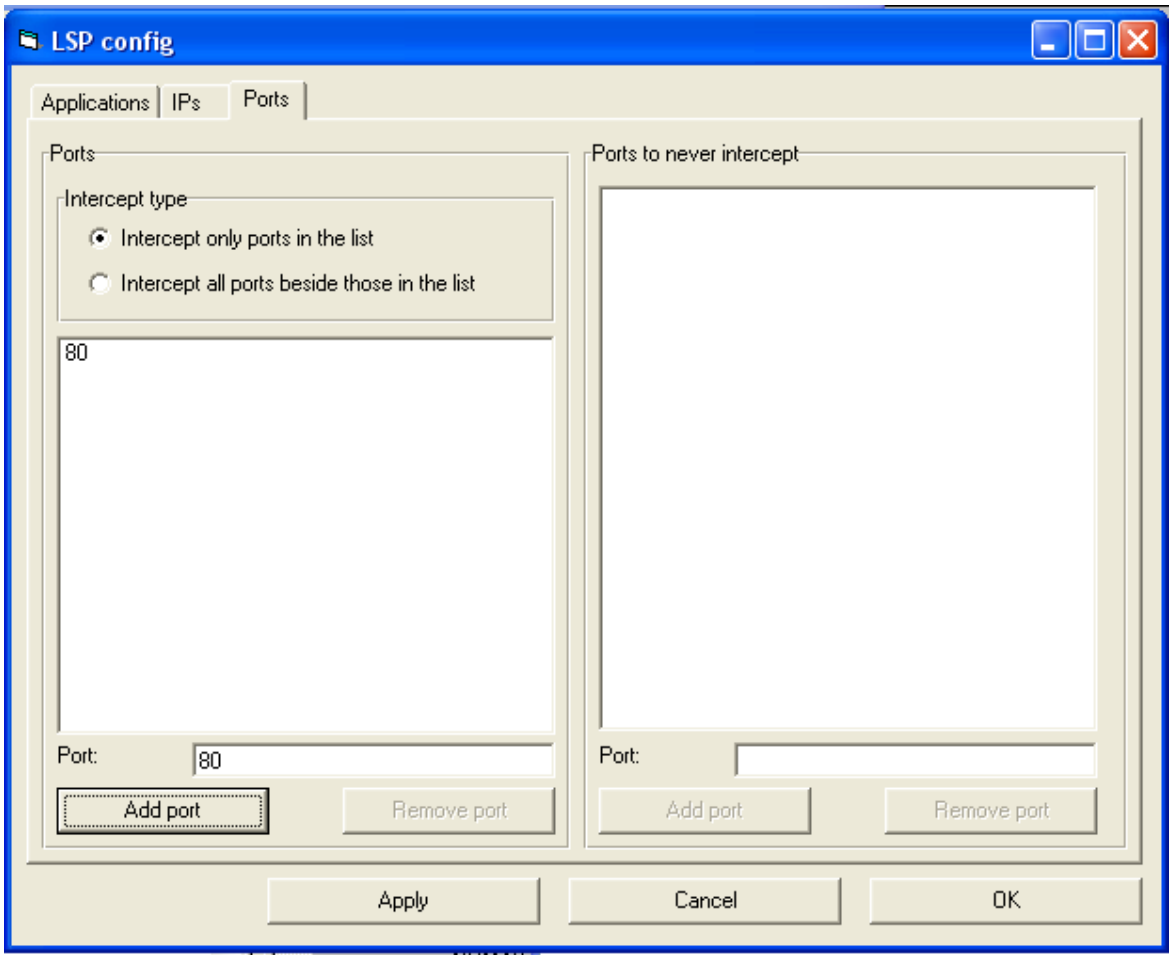
Items to never intercept

Items on this list will never be intercepted regardless of the regular interception list mode (include/exclude). For example, placing "iexplore.exe" in this list means that sessions coming from Internet Explorer will never be intercepted, even if other rules match those sessions' information (a port 80 rule, for example.)

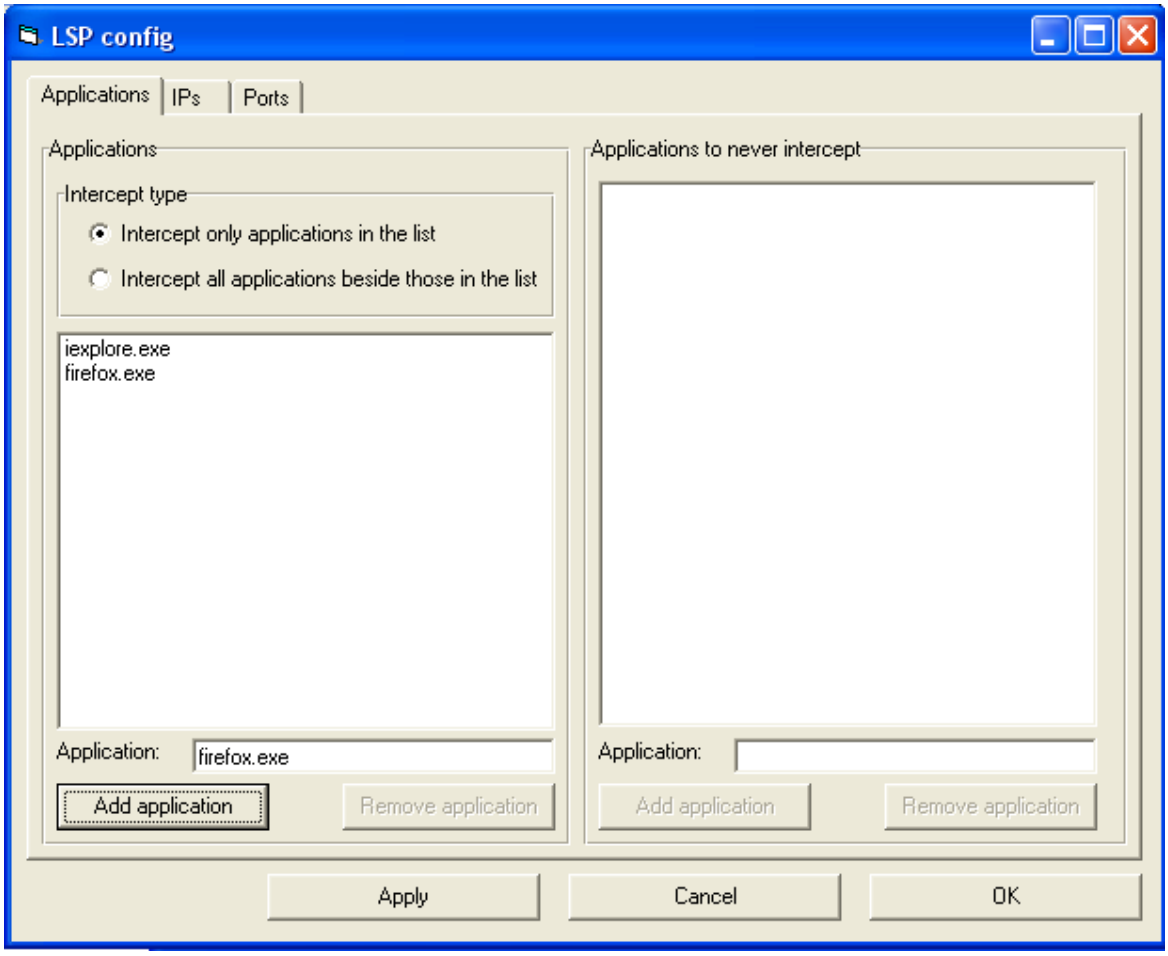
Recommended rules for evaluating the Redirector

To best evaluate the product we suggest adding “iexplore.exe” and “firefox.exe” to the application list, and port 80 to the ports list.

Option 1 image:



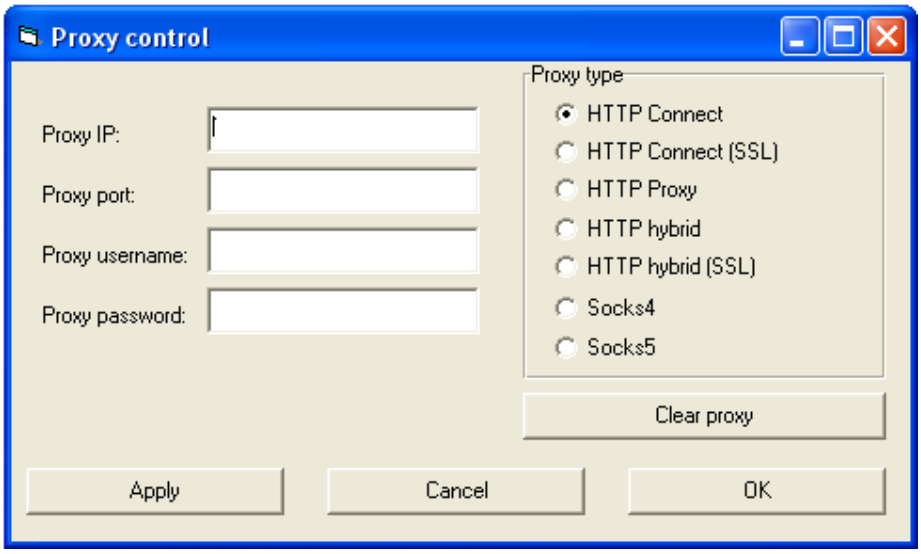
Option 2 image:



Proxy control

Komodia's Redirector supports four kinds of proxy tunneling: Regular HTTP proxy, HTTP Connect proxy, HTTP Connect proxy that connects to the proxy using SSL, and hybrid mode that uses HTTP connect for SSL based connection and HTTP proxy mode for non SSL connections.

To set a proxy, go to "Proxy control" in the main dialog screen:



Proxy IP

The IP address of the proxy (only IP, not domain name)

Proxy port

The port of the proxy

Proxy username and password

Username and password used to access the proxy - applicable only to HTTP Connect proxy.

Proxy type

- HTTP Connect – Uses HTTP Connect directive when trying to relay data, usually used for non HTTP based traffic.
- HTTP Connect (SSL) – Same as HTTP Connect, however the session to the proxy is encrypted using SSL.
- HTTP Proxy – Will send HTTP data only (Redirector checks if the data is HTTP before relaying it) to a HTTP proxy, while adjusting the request for the proxy to use.
- HTTP Hybrid – Redirector checks if the data is HTTP, if it is, it will use HTTP Proxy method, if it isn't it will use HTTP Connect method.
- HTTP Hybrid (SSL) – Same as HTTP Hybrid, however the session to the proxy is encrypted using SSL.
- Socks4 – Socks4 proxy (Socks4 doesn't support authentication)
- Socks5 – Socks5 proxy.

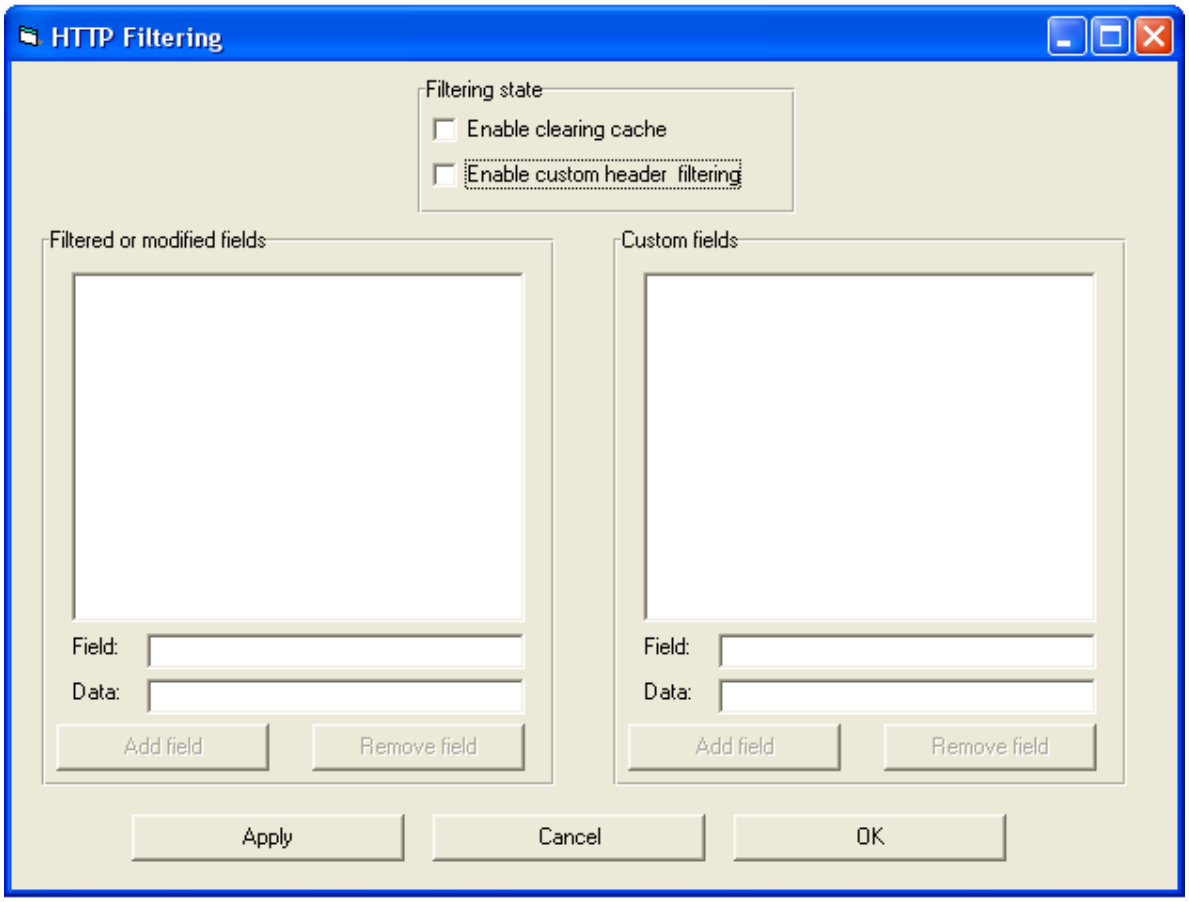
SSL Protection

When using HTTP Connect (SSL) and HTTP Hybrid (SSL), the session between PCProxy and the proxy will be initiated using SSL. NOTE: Make sure the proxy supports this and is configured correctly. The proxy we tested to work with is Squid 2.7 with SSL enabled. All traffic between the client's computer and the proxy is encrypted.

HTTP header manipulation

Komodia's Redirector comes with the ability to perform header manipulation on outgoing HTTP requests, this feature can be programmed by extending PCProxy, its purpose is to save you time.

To set the HTTP filtering go to "HTTP header filter" in the VB console main panel:



Enable clearing cache

This option clears the: "If-modified-since", and "ETag" header flags and appends: "Pragma: No-cache". This will prohibit the web server from sending 304 HTTP reply which means that the browser will use the local cache.

Enable custom header filtering

This option turns on custom HTTP filtering, using the options below. (It is very important not to insert the character ':' inside the "Field" data field.

Filtered or modified fields

This option tells the Redirector to either change a header flag or to discard it, for example on how to change a field:

1. Write user-agent in the "Field" data field.
2. Write a custom string in the "Data" data field.
3. Press: "Add field"

Now this new addition means the redirector will process every outgoing HTTP request and will modify the field: "user-agent" and will set it with the data entered in the "Data" data field.

To discard a HTTP header flag you need to follow steps 1 and 3 (Don't enter data inside the "Data" data field).

Custom fields

This options tells the Redirector to add a HTTP header flag to an outgoing request in case that flag wasn't present, if it was present in the request, it is not modified or discarded. For example on how to add a custom flag:

1. Write X-Flag in the "Field" data field.
2. Write a custom string in the "Data" data field.
3. Press: "Add field"

Now for every outgoing request if the flag: X-Flag is not there, then the Redirector will append: "X-Flag: custom data" to the request.

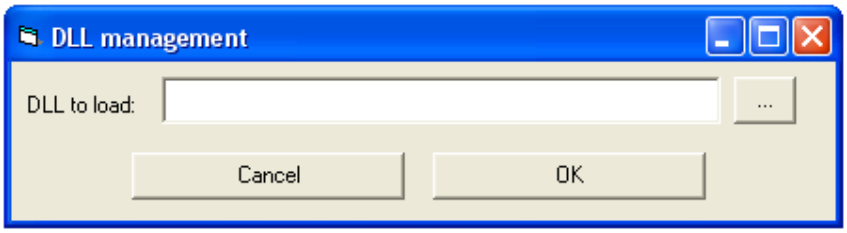
DLL control

PCProxy can load external DLLs written by other programmers to extend its functionality. The DLL must support a specific API and is documented in another article.

It is important to remember that the DLL is loaded only when PCProxy loads, which means that setting or clearing the DLL will not take effect until PCProxy is restarted.

If there is a problem with the DLL, such as incorrect interface or the DLL is not found, then PCProxy will work as usual without the DLL. It will also write in the event log why it failed to load the DLL.

To set the DLL to load or clear an existing DLL, go to “DLL control” in the VB console main panel:



DLL to load

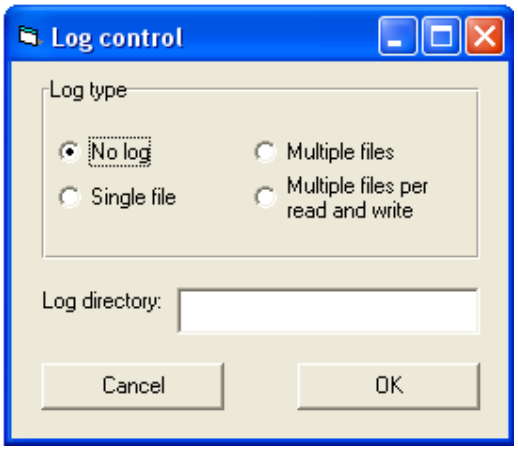
Full path of the DLL to load (browse using the “…” button).

Log control

PCProxy can log all data that it receives before it is modified by internal code (e.g., proxy code) and/or DLL modification code. The log only logs data. Failed connects will not be logged.

The logging setting is non-persistant because it is meant for debugging. Restarting PCProxy will revert the logging state to no-logging.

To set or clear the existing log, go to “Log control” in the main panel:



Log type

- No log – Default. Will not log data.
- Single file – All data will be written into a single file.
- Multiple files – Each connection will be logged to a single file.
- Multiple files per read and write – Each connection will be logged into two files, one for the received data and one for the sent data.

Log directory

The directory where the log/s will be written

Saving, loading and clearing the data

The PCProxy service loads the data as it loads. All subsequent modifications are not saved until the “Save” button is pressed. The “Clear” button will reset the configuration.

Propagation time

LSP only affects application that ran after the installation. For example, if you installed the LSP while an Internet Explorer instance was running, that instance will not be affected, but every new instance will be affected. After restart, all applications, including OS core services, are affected.

Running LSP instances refresh the rule set every 60 seconds. New instances take the latest rules from the service upon loading.