

Fastream IQ Proxy Server

User Guide

Version 7.2



THIS USER GUIDE IS INTENDED TO BE COMPANION TO FASTREAM IQ PROXY SERVER.
IF YOU DO NOT AGREE WITH FASTREAM IQ PROXY SERVER LICENSE AGREEMENT, YOU
ARE PROHIBITED FROM USING IT.

COPYRIGHT 2005 - 2011 FASTREAM TECHNOLOGIES, ALL RIGHTS RESERVED.

1 INTRODUCTION TO IQ PROXY SERVER.....	1
1.1 ABOUT THIS USER GUIDE	1
1.2 OVERVIEW	1
1.3 FASTREAM IQ PROXY SERVER FEATURES.....	1
2 SYSTEM REQUIREMENTS AND INSTALLATION	2
2.1 IQ PROXY SERVER ENGINE	2
2.2 IQ PROXY SERVER REMOTE GUI.....	2
2.3 INSTALLATION	2
2.4 LOCAL/REMOTE ADMINISTRATION.....	2
3 SETUP GUIDE	5
4 FREQUENTLY ASKED QUESTIONS (FAQ)	7
5 USING IQ PROXY SERVER	12
5.1 MANAGER.....	14
5.1.1 Admin Server Settings.....	14
5.1.2 Admin User Settings.....	16
5.2 CACHE	17
5.2.1 The Cache Tabsheet	17
5.2.2 How Does IQProxy Cache Work?	18
5.3 DYNAMIC DNS.....	19
5.4 CONFIGURING A REVERSE PROXY LISTENER	21
5.4.1 Status.....	21
5.4.2 Web Servers	21
5.4.3 URL Rules.....	24
5.4.4 Options.....	30
5.4.5 Cache Options.....	34
5.4.6 Firewall	36
5.4.6.1 DDoS.....	36
5.4.6.2 SYN	36
5.4.6.3 IP	36
5.4.5.4 Domain	37
5.4.6.5 Country	39
5.4.7 Log	40
5.4.8 SSL/TLS Encryption	42
5.4.9 Compression.....	43
5.4.10 Error Pages.....	45
5.4.11 Anti Hot-Link	47
5.4.12 URL Rewrite	48
5.4.13 Header Rewrite.....	50
5.4.14 Monitor	52
5.4.15 Actions.....	53
5.5 CONFIGURING A CONTENT PROXY LISTENER	54
5.5.1 Status.....	54
5.5.2 Authentication.....	54
5.5.3 Options.....	56

5.5.4 Filter	58
5.5.4.1 Domain	58
5.5.4.2 Country	59
5.5.4.3 Content	61
5.5.4.4 Header	61
5.5.5 Firewall	63
5.5.5.1 DDoS	63
5.5.5.2 SYN	63
5.5.5.3 IP	64
5.5.5.4 Domain	65
5.5.5.5 Country	68
5.5.6 Log	70
5.5.7 Compression	72
5.5.8 Error Pages	73
6 NPAT	74
6.1 What is NAT	74
6.2 What is PAT	74
6.3 IQ Proxy NAT	75
6.4 IQ Proxy PAT	77
7 WAN LOAD-BALANCING (WAN LB)	78
8 REGISTRATION AND SUPPORT	79
8.1 FASTREAM IQ PROXY SERVER VERSIONS	79
8.2 FASTREAM IQ PROXY PROFESSIONAL LICENSE ORDER	79
8.3 HOW TO REGISTER	79
8.4 HOW TO UPGRADE	79
9. UNINSTALLING	80
10 CONTACT INFORMATION	81
11 APPENDIX	82
11.1 A REVIEW OF HTTP	82
11.2 HTTP DETAILS	82
11.3 OVERALL OPERATION	82
11.4 HTTP CLIENT AND DOWNLOAD MANAGER SUGGESTIONS	83
11.5 HTTP TERMINOLOGY	84

1 Introduction to IQ Proxy Server

1.1 About This User Guide

This user guide is designed to be an easy-to-use aid for the Fastream IQ Proxy Server (IQ Proxy) Windows server application. IQ Proxy is the most robust and secure forward/reverse proxy server solution for Windows®. It is the most scalable server engine for both filtering and caching content proxy, securing and accelerating reverse proxy, and can be used on any Windows platform. This user guide is organized to take you through all tasks, from installation to using IQ Proxy to advanced troubleshooting.

1.2 Overview

IQ Proxy is a web proxy cache for the Windows® 2000/XP/2003/Vista/2008/7 platform. IQ Proxy operates as a Windows service that does not support the outdated Win9x platform. We have done our best to ensure a high quality, feature-rich product that is also fast, robust, and secure.

1.3 Fastream IQ Proxy Server Features

IQ Proxy is the ultimate web content proxy solution with the following features:

- Caches static and dynamic content for ultra-hi-speed deferred serving
- 256-bit SSL/TLS accelerator with support for OpenSSL hardware cards and self-signed certificate creation
- Load balancing in URL-aware fashion: point each domain/path to different target LAN server/port
- Anti-Hot-Linking to save bandwidth and to show a customizable error page instead of blocked pages
- Bandwidth limiting per URL rule per IP/port. An administrator can limit the total site bandwidth usage or sub parts of the site
- GZip compression accelerator with configurable compression rates for each object extension
- Able to listen on multiple IP/ports and scalable up to tens of thousands of simultaneous connections
- Cookies created make session persistence possible among client-to-target-server matching
- TCP firewall: Filter with respect to IP, reverse DNS, and even client IP country
- User-friendly HTTP/XML controller interface for remote administrator access
- HTTP/1.1 basic and digest as well as Windows®/NTLM and HTML authentication with users definable per URL rule
- Supports W3C Extended Log Format with selectable fields and NFServer v2 screen and file logging—configurations are definable in URL granularity
- Customizable pages for "target server not found" and "requires authorization" errors
- Client connections pooled with dynamic load determination algorithm
- Supports SNI protocol for serving multiple SSL certificates per IP/port
- Runs as a service on all Windows 32/64-bit platforms with very little resource utilization (1GHz Pentium+ CPU, 256MB RAM, 32MB disk space)

Read more about IQ Proxy Server's latest features at <http://www.iqproxyserver.com/features.php>.

Download the latest version of IQ Proxy Server at <http://www.fastream.com/download>.

View the latest pricing information for IQ Proxy Server at <http://www.fastream.com/orderiqproxy>.

Visit Fastream Technologies home on the web at <http://www.fastream.com>.

2 System Requirements and Installation

The IQ Proxy Server software consists of two components, the IQ Proxy Server Engine and the IQ Proxy Server GUI, which have the following minimal system specifications:

2.1 IQ Proxy Server Engine

The IQ Proxy Server Engine is the main component of the IQ Proxy Server application. Its main purpose is to perform the actual proxy tasks for Intranet/Internet traffic. The Server Engine is a “non-interactive Windows® service,” and as such, does not make use of a user interface. The IQ Proxy Server Engine has the following installation requirements:

- A PC capable of running Windows 2000/XP/2003/Vista/2008/7; (server edition of Windows 2000, Windows 2003, or 2008 recommended for heavy-duty usage)
- 32 MB free hard drive space
- An administrator login to the Windows platform on which it is installed
- A minimum of 64 MB of free RAM; 256MB free RAM recommended for caching
- An active Internet/Intranet (TCP/IP) connection

2.2 IQ Proxy Server Remote GUI

The IQ Proxy Server administration GUI provides a user interface to configure the reverse proxy tasks to be performed by the proxy server engine. It may be installed on the same PC as the engine, or another PC that can access the PC on which the Engine is installed (there must be no firewalls configured to block HTTP traffic to ports 30033-30034) or the client/server executables. The IQ Proxy Server GUI has the following installation requirements:

- A PC running Windows® 95/98/Me/NT4/2000/XP/2003/Vista/2008/7
- 10 MB free hard drive space
- A minimum of 32 MB of free RAM
- An active Internet/Intranet (TCP/IP) connection

2.3 Installation

Installation is easy and straightforward using the installer program. If another version of the IQ Proxy is already installed in your machine, the Windows® installer will update the program to the latest version with your existing configuration preserved. When you run the installer program, you should read the end user agreement. If you accept that agreement, then choose the destination folder for installation of the server engine.

After the service is installed, the installation of the IQ Proxy Administration GUI starts. The installer of the IQ Proxy Administration GUI is also available separately at <http://www.fastream.com/download> as well as bundled with the engine. After installation, the installer program of the GUI itself is also copied to the server engine's **Program Files** folder. If the Windows platform on which the software is installed is 64-bit, then it will be installed to the **Program Files (x86)** folder.

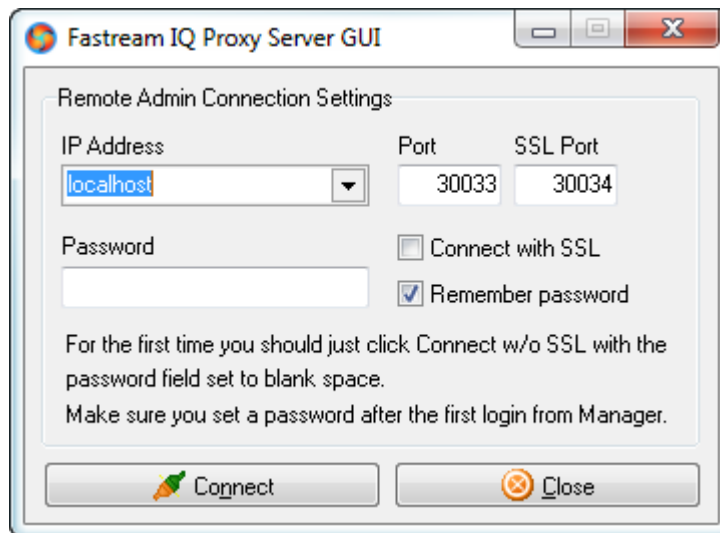
IQ Proxy Server can safely be installed to remote servers over RDP. However in that case, you will need to disconnect your RDP session and reconnect during IQNDIS driver installation. This is due to Windows architectural limitation on NDIS drivers. Once the installation wizard ends, you should reboot Windows for driver installation to guaranteed to be completed.

2.4 Local/Remote Administration

The IQ Proxy Administration GUI allows remote administration connections to your proxy server from any computer on the Internet. The IQ Proxy Administration GUI and the IQ Proxy Server Engine communicate with each other using the standard HTTP(S) protocol and XML formatted messages.

When you open the IQ Proxy Server GUI, a login dialog box displays. You can specify the following at the login dialog box:

- The TCP port numbers (HTTP and HTTPS) of the IQ Proxy Administration service (**Port** and **SSL Port** fields)
- Whether to connect to the SSL port with strong encryption or use cleartext communication (**Connect with SSL** field)
- The IP address and password of the server administrator (**IP Address** and **Password** fields)
- Whether to enable IQ Proxy Server to remember the connection password (**Remember password** field)



Port and SSL Port:

These are the listening ports of the IQ Proxy Engine service for remote administration purposes. The default value is 30033 for HTTP and 30034 for HTTPS.

IP Address and Password:

These fields correspond to the login information of the administrator of the IQ Proxy Engine service. The default IP address is *localhost* and the password is blank. Refer to the "Server Manager" chapter for details on changing the administrator password.

Connect with SSL:

This field specifies whether communication between the IQ Proxy Administration GUI and the IQ Proxy Server Engine uses SSL port or the cleartext HTTP port.

When the IQ Proxy Server Engine is started, the server begins listening for administration commands on the designated administration ports. Only authenticated administration commands are executed. When you are first trying to login, you must use the non-SSL port to connect due to the fact that there is no SSL

certificate assigned for the SSL port and a certificate is required for SSL.

When the IQ Proxy Server GUI is started and the administrator enters administration information, the GUI connects to the server and receives an initial status of the server. This status is displayed in the GUI.

All modifications performed from the GUI are applied at the server machine as if server is running on the local computer.

3 Setup Guide

After you reboot, you are ready to explore the rich feature set for protecting and acceleration your web servers with IQ Reverse Proxy. First thing you should setup is from web server IP/port/paths. To do this open **RProxy->Web Servers** and now you need to make a decision: Do you need to use **routed** or **redirected web server** entries? A routed web server is where all the traffic is proxied through IQ Reverse Proxy is this is what 90% of the time what customers need. A redirected web server is for pure redirection with 301/302/307 HTTP redirection codes. If you choose the latter, you won't have failover as after redirection the connection is out of control of your IQ Reverse Proxy.

Once you create your web server entries, it is time to assign them to URL Rules--assignment rules for the HTTP/HTTPS ports. In its most simple form, these may mean domains. Now IQ Reverse Proxy supports regular expressions. If you upgraded from an older version, you will see that your **URL Rules** are upgraded to regex automatically. Basically in the old syntax we used to only allow the wildcard character * (asterix). Now it is replaced with .* (dot and asterix). Also since . (dot) is the escape character in regex, in regex it is replaced with \. (backslash and dot). If you use the "Add" button in URL Rules, it will accept the old syntax and convert automatically. If you use the "Add regex" button, you would find the chance of setting with no conversion for all the power of regex. After you create your URL Rules, make sure you assign the Web Servers you created to them so that the routing path is ready.

You can use the syntax http://domain/path or ssl://domain/path or *://domain/path (any protocol) for your URL Rules. Make sure you do not enter the port part as that should be defined from the **Options** tabsheet. If your path points to a file instead of a directory/folder on your web site, make sure you check URL points to file.

If you want to preserve the host header from the request so that it would be kept as is in the connection to the web servers assigned, check the **Preserve Request Host Header**. This might be required in the following scenario: You need to point your DNS to IQProxy yet your web servers still expect the same host header to function and serve properly for your sites needs (which is the case with OWA and Sharepoint). If you uncheck this, then the IP address of the target web server definition will be used instead in the host header.

One other thing you should decide per URL Rule is **content (HTML/CSS) & link translation** options. If you have absolute links on your site or relative path in your URL Rule, you should check content translation which is turned on by default. Content translation should not be checked when all the links are relative as it consumes RAM and CPU cycles to parse the content. Link translation is for **location** header in 301/302/307 responses.

For authentication, you can select local DB or NTLM, then you should decide in the method to be used. The most secure one is **digest** for local DB and **Windows NTLM** for NTLM. HTML based authentication sends the password in cleartext so it is strongly advised that you use it in conjunction with SSL.

Country restriction is for restricting a URL Rules application to a client request based on clients geographical location, country. Now, with one click you even can assign an entire continent! This feature is available in Reverse Proxy Enterprise edition only.

For SSL, you must have a certificate, a private key and optionally a CA File for root/intermediate certificates. In the **SSL/TLS Encryption** tabsheet, with the **SNI** feature, you can have as many certificates on single port as you want (this feature is available in Reverse Proxy Enterprise edition only). You can buy your certificates from a Certificate Authority such as Verisign or Comodo or simply create your self-signed certificate. In the latter case, the browsers of your visitors would issue a warning since they would not trust you signing your own certificate. A CSR is a Certificate Signing Request. You must make one before you

order a certificate from a CA. You should always keep the private key it will generate as confidential as that is what the encryption, hence your sites security will depend on.

The **DDoS firewall** in the Firewall tabsheet is by default turned off only for the reason that you might want to test your site first and it might disrupt too many requests from an IP address such as in the case of web stress testing. you can safely turn it on by checking enable and clicking apply. NDIS level protection is available in the Reverse Proxy Enterprise edition only. It blocks the SYN packets before the connection is established so is smarter, faster and causes less traffic in terms of CPU, RAM and bandwidth due to malign visitors.

If you do think your web content that do not issue a cookie can be updated less frequently than a few seconds, then you can safely turn on **Override web server cache expiration policy** from Cache Options. This would make sure the staleness checks are at intervals you define per MIME type.

In **Options** tabsheet, you should decide whether you want to see the 500/501 error pages from your web servers as is or replace them with custom error pages of IQ Reverse Proxy. Uncheck **Accept 500 responses as Server Error** for the latter. If you wish to have your scripts know the client countries the easy way, you can add X-Client-Country request header and check for it in ASPX/PHP/Perl on your web servers...

IQ Content Proxy Setup

IQ Content Proxy is the most intuitive forward/transparent proxy server solution for the Windows platform. The first thing you need to decide before using IQ Content Proxy is if whether to use it in Forward Proxy or Transparent Proxy modes. Former one means you need to enter IQ Content Proxy IP/port into your browsers explicitly but the proxy can reside anywhere on your LAN or on the Internet. The latter one is better as a total cache and filter but you must install it onto your network gateway.

You can use the country firewall to block users from outside your LAN. The NPAT (Network Port Address Translation) feature is for sharing one WAN/Internet IP among multiple users. Filter is for filtering of web content only. You can find more information for these in the user guide.

4 Frequently Asked Questions (FAQ)

Q: How should I start using the reverse proxy?

A: First of all, you should realize that most of the features in IQ Proxy have sound default values. So unless your needs are specific, all you need to do is create the web server entries from "Web Servers" and assign them to "URL Rules". Make sure the port 80 or whatever port you want (you can configure that from "Options" tab sheet as well), is not blocked by any network firewall. To test your server, enter its IP into your browser such as <http://localhost>.

Q: How should I start using the content proxy?

A: You should realize that most of the features in IQ Proxy has sound default values. So unless your needs are specific, all you need to do is configure your browser to use the proxy IP/port. If you do want to limit the access to the proxy, you can simply use the "Firewall" (we would suggest the country filter, permit->LAN Subnet) or "Authentication" features. Make sure the port 8080 or whatever port you want (you can configure that from "Options" tab sheet as well), is not blocked by any firewall.

The content proxy module listens on one IP--in your case it is the LAN IP at the bottom of the GUI and by default on port 8080 which you can configure from CProxy->Options->Listening Port. You will most probably do not need to touch the listening IP though as 0.0.0.0 means all unassigned IPs which should be just fine.

Next step is to configure your browser: We will explain Internet Explorer 8 as that seems to be the most common one as of March 2011. Please open the drop-down menu Tools->Internet Options->Connections->LAN Settings and check "Use a proxy server for your LAN" and enter the LAN IP of the IQP and the port (remember, it was by default 8080).

Q: How does one admin backup entire configuration?

A: All you need to do is to backup *.ini from IQP engine's program files folder. Also, you should print and backup your registration email.

Q: What is the default password for the admin user?

A: The default password for the localhost user in IQ Proxy is blank space.

Q: How do I reset the password for the admin user?

A: Please shut down the service then browse to the program files folder of the IQ Proxy Engine and edit the IQ.ini file ("AdminSettings" section) by deleting the "password" line.

Q: I am using a computer in a LAN. My LAN is behind a router and all computers on the LAN have a single external IP address behind a firewall. Is it possible that I can setup a Web listener using IQ Proxy?

A: Establishing an HTTP Server in the above situation is not challenging. If you configure your router and firewall to pass TCP port 80 or whatever port you are configured for listening in from Options tabsheet, it would forward connections to your computer. You should also do the same for the administration server's IP address and port number if you are willing to administer remotely.

Also, IQ Proxy accesses www.fastream.com and some other site for determining the WAN IP of the machine in the absence of a real IP address.

Q: How do I enable access to network drives as served paths?

A: The default account for IQ Proxy's Engine service is the Local System account. This account is limited by Windows™ as having no access to Microsoft network drives. To enable it, you need to go to Control Panel -> Administrative Tools -> Services and select the "Fastream IQ Reverse/ Content Proxy Engine" service.

Then right click and click on Properties-> Go to Log On Tab. From here you need to select either a network account or an administrative account.

Q: How do I configure SSL/TLS?

A: There are a few items you need to do in order SSL to work: You need to assign a certificate: This could be either a self-signed one (see the "self-sign certificate" button) or you should purchase a certificate from a company (CA) such as Verisign, Thawte, etc. The purchased certificate must be in PEM format. If it comes as a single pem file, you need to edit not with notepad but with another text editor and copy the private key to another pem file. When you buy a certificate from a CA, basically they will give you three files:

1. Root certificate
2. Intermediate certificates
3. Server certificate

Plus you should have the private key file created during CSR creation. With a text editor such as TextPad or CrimsonEditor, you must merge the Intermediate certificate with root certificate by leaving a blank line in between. The intermediate certificates must be at the end and the newly formed file should be assigned to CAFile in the SSL tabsheet.

You should also type the domains that you want to serve encrypted with the SSL layer into the "Accepted Hosts" section such as "localhost;www.fastream-test.com" (without the quotes; notice the semicolon delimiting).

You must forward the TCP port 443 (defined in Options) for serving outside your LAN from your firewall/router (or whichever TCP port you configured for listening from Options tab sheet).

Q: What is an example setup configuration for a typical content/reverse proxy usage in Servers and URL Rules?

A: In a typical case, first you need to decide on the listening IP/port in Options. You will probably want the port to be the standard 80 (for HTTP) and 443 (for HTTPS/SSL). The tricky part is the IP. If you have only one proxy port listening (only one tab sheet for proxy), then it is suggested that you leave this at 0.0.0.0 which means "answer incoming requests from all the IPs assigned on all adapters of the server computer such as 127.0.0.1 (localhost), 192.168.xxx.xxx, 10.xxx.xxx.xxx, other LAN IPs and WAN IPs forwarded from router and/or real IPs. If you assign a real IP here such as 144.122.1.100, then to access the site from the same host computer, you cannot use localhost (127.0.0.1) as the IP. You must use 144.122.1.100 directly.

What is useful in assigning a real IP is that you can listen on other IPs with different proxy tabs—each one in its own thread/listening socket. For example, let's assume that 144.122.1.100-103 is assigned to the same computer via two NICs. Here is how you may want to distribute them:

144.122.1.100:80 listens for proxy A

144.122.1.101:80 listens for proxy B

0.0.0.0:80 (which means the rest of the IPs assigned—102-103 here) listens for proxy C

This gets even more useful when thought with SSL/SSL certificates: There can be only one certificate assigned for each IP/port even though many virtual domains could co-exist in one IP/port. So for each domain to be certified on port 443, you need a listener proxy:

144.122.1.100:443 listens for proxy A which SSL certifies www.domainA.com

144.122.1.101:443 listens for proxy B which SSL certifies www.domainB.com

Now that we explained the IP setting in Options, let's see how the Servers tab works:

In servers, the important parts are IP, port and path. IP can be the real IP of the web server or if the LAN is behind NAT, it should be the LAN IP of the web server such as 192.168.1.200 or 10.1.1.20.

Port is the listening port of the web server. Now what is "path"? Path is for relative URL

rewriting. For example, let's say you do not want the clients to access the root of the web server but the redirected root needs to start from "IQPRoot/" of the web server. To clarify, let's talk in the context of the

file system of the web server. Suppose that it has a structure like: C:\InetPub\wwwroot\
C:\InetPub\wwwroot\IQ ProxyRoot\
Now the first one is the "/" (root) of the web server. If you want this path to be inaccessible for

one URL Rule this server entry is assigned to, then enter /IQ ProxyRoot/ in the Servers" path. Let's now understand how URL Rules work. In order for a URL Rule to work, it needs to have a Rule entry such as,

Default (which cannot be removed—to catch all requests uncaptured by other rules)

*/images (catches all domains" /images folder)

www.domainxyz.com/ (catches the domain domainxyz.com)

Also, for this case and similar ones, you must not check "preserve path" from URL Rules screen for the URL rule and also do check "content translation" from Options.

Q: How should I define web server addresses?

A: In a typical case, first you need to decide on whether you want to keep the host name of the incoming browser request in the connection from IQ Proxy to web servers or replace with the host name of the web server. If you want to have,

www.xyz.com

to be passed to the web server at 144.122.1.10 as it is, then define the web server in "Servers" as

144.122.1.10 (numeric IP). If you want to have it replaced, then use the host name of

144.122.1.10 (i.e. webserver1.xyz.com). In both cases, if you enable "Link Translation", redirections to self of web server will be rewritten. If you want the HTML to be rewritten as well, enable "Content Translation" as well. These are in "Options".

Q: How do I redirect HTTP port to SSL port?

A: You need to create a URL rule like http://* and assign a redirected web server as, https://www.domain.com.

Q: How does one configure Exchange/OWA/SharePoint for IQ Proxy?

A: There are a few things you need to be aware of:

1) You must disable "preserve path" for the url rules for Exchange

2) You must enable "link and content translation" from Options

3) If your OWA mandates an SSL connection to itself from IQ Proxy, then you must create two url rules and two web servers. For example:

URL Rule #1: ssl://*

assigned the web server #1: <https://1.2.3.4:443/>

URL Rule #2: http://*

assigned the web server #2: <http://1.2.3.4:80/>

4) You must disable NTLM authentication from the MS web server product and enable Basic authentication instead. Also, disable authentication on IQP URL Rule(s).

5) You need to point the domain used by OWA to IQP server, and then use the numeric IPs of the OWA (see 3.) to route in URL Rules.

Q: How to achieve maximum performance by playing with IQP configuration?

A: First of all, from v2.6.4R on, all pages can be cached except there is Set-Cookie in response header. To make sure cache is in place, if you have any exceptions in RProxy->Options->Extensions to Exclude from Cache, please clear that. Secondly, you may want to override server "no-cache" response header directive by clicking "override..." from Cache tabsheet. This way, unless a set-cookie is in header, pages will be cached for the duration specified in Cache tabsheet according to their extensions. If there is no file extension such as www.domain.com/path/ then you should use "folder" as extension.

From v2.6.3R on, content translated pages are also cached for 1000% speed! You need to do nothing for this. Of course, let me remind what "link translation" and "content translation" do:

Link translation is for 301/302/307 responses; translates domain and path -when self-directing to web server itself- to point to IQP.

Content translation is for text/html mime type (most .php, .pl, .rb, .asp, .aspx, .htm, .html,...) to be parsed and then URLs to be translated.

Q: How to configure Microsoft Sharepoint to use with IQ reverse proxy server?

A: IQP, as with all reverse proxies cannot translate URLs in Javascripts. Sharepoint has a way to be forced to do correct URL mapping. In order to run Sharepoint with IQProxy, configure as below.

IQ Proxy Server

URL Rules:

Define the Request URL Rules and Assigned Web Server

Highlight the Request URL Rule

Check off "Preserve Request Host Header" and "Preserve Request Path"

Options:

Check "Link Translation" only. "Content Translation" should be unchecked.

WSS/SHAREPOINT – Central Administration

Operations / Global Configuration / Alternate AccessMappings

Edit Public URL's

Alternate Access Mapping Collection: (default is SharePoint – 80)

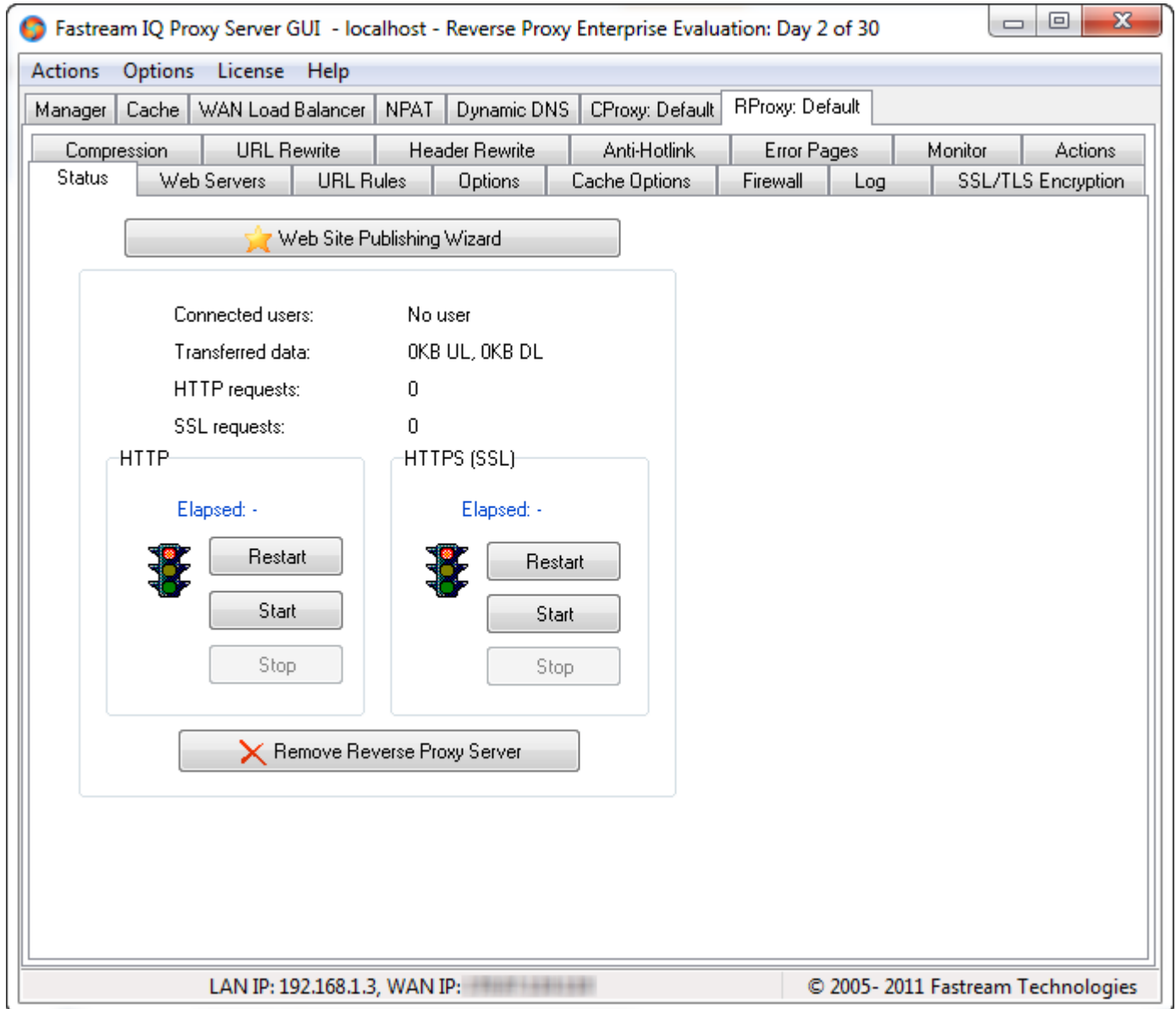
Public URL in the "Internet" field type in the name of your external Website URL (ex http://www.domain.com)

Save

See [http://technet.microsoft.com/en-us/library/cc288609\(office.12\).aspx](http://technet.microsoft.com/en-us/library/cc288609(office.12).aspx) for more Sharepoint information.

5 Using IQ Proxy Server

When you first install and run Fastream IQ Proxy Server, the main window resembles the one shown below. IQ Proxy Server provides a default reverse proxy and default content proxy. You can create as many reverse proxies and content proxies ports as you like.



GUI window:

This is the main window and consists of three main parts:

- A menu bar, consisting of **Actions**, **Options**, **License**, and **Help** options
- A left navigation panel, containing of a hierarchical tree view of the application
- A main detail panel, containing various tab sheets

Menu bar:0

The menu bar provides items for starting main application functions, such as adding reverse and content proxy listeners, and checking for new application updates.

Left panel:

The left panel provides an alternative way of navigating through the various tab sheets. It consists of a tree view of the application. That is, the main nodes match with the upper row of tab sheets in the main panel and the sub-nodes match the second level of tab sheets in the main panel. Clicking a main node reveals that node's sub-nodes.

You can select whether to display the left panel by using the **Show Left Panel** option on the **Options** menu.

Main panel:

The main detail panel consists of various tab sheets. The upper row of tab sheets corresponds to the main configuration settings and the configuration settings per defined server.

Tab sheet:

You display additional details in the main panel by clicking a tab sheet's label. Generally a tab sheet is divided into groups of GUI components or other sub-tab sheets.

GUI group:

A GUI groups refers to a functional cluster of screen components. A group of screen components is surrounded by a gray line. The upper gray lines contain an indication of the group's title.

Button:

Frequently used buttons relate to the tab sheet and group of GUI components in which they appear.

Three types of buttons are used.

- Buttons without an icon are helper buttons, mainly for generating default values in text boxes or adding values to list boxes
- Buttons with an icon are typically used for adding new settings or removing old settings
- Buttons with an icon and the text **Apply** are used for saving new settings and making them persistent

Check box:

A check box is a small square that can be checked or unchecked indicating that the associated setting is on or off. If the check box is unavailable, it displays with a gray background color.

Text box:

A text box is an input field in which you can type free text. If the text box is unavailable, it displays with a gray background color.

Combo box:

A combo box is also an input field; however, its values are predefined and selectable. The predefined values for a combo box can be displayed by clicking the arrow at the right of the combo box. If the combo box is unavailable, it displays with a gray color.

Info box:

An info box resembles a text box, but an info box cannot be used to enter data. For this reason, the background of an info box always displays with a gray color.

List box:

A list box is a two-dimensional table of items. An item within a list box can be selected. If the list box is unavailable, it displays with a gray background color.

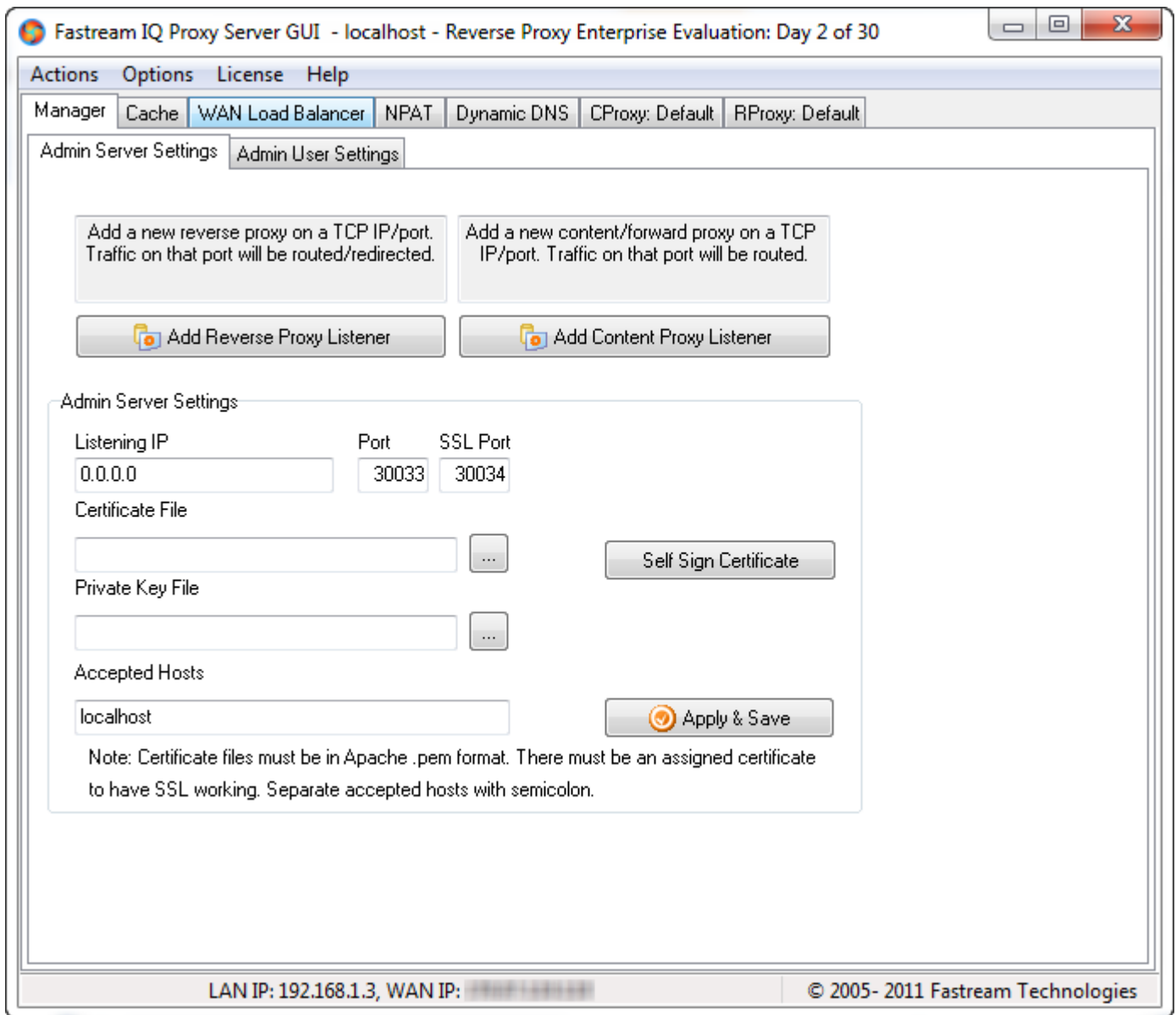
5.1 Manager

The **Manager** tab sheet is made up of two sub-tab sheets: **Admin Server Settings** and **Admin User Settings**.

The **Admin Server Settings** tab sheet enables the administrator user to create new reverse and content proxies. The **Admin User Settings** tab sheet enables the administrator user to change his or her password. The two **Admin Server Settings** and **Admin User Settings** tab sheets are described in the next sections.

5.1.1 Admin Server Settings

In the **Admin Server Settings** tab sheet, the administrator can add new reverse and content proxies. Furthermore, it is here that the IP address and IP port number of the IQ Proxy engine service can be changed.



Adding a reverse proxy listener

To add a new reverse proxy, click the **Add Reverse Proxy Listener** button in the **Admin Server Settings** tab.

Add New Reverse Proxy Server:

By clicking the **Add Reverse Proxy Listener** button, you can add a new reverse proxy. You must specify the new reverse proxy's name, after which a new reverse proxy is created and you will be directed to the new reverse proxy server's tab sheet. You can create as many reverse proxies as you like.

For more information on configuring a reverse proxy, refer to the chapter entitled "Servers".

Adding a content proxy listener port:

To add a new content proxy, click the **Add Content Proxy Listener** button in the **Admin Server Settings** tab.

Add New Content Proxy Server:

By clicking the **Add Content Proxy Listener** button, you can add a new content proxy. You must specify the new content proxy's name, after which a new content proxy is created and you will be directed to the new content proxy server's tab sheet. You can create as many content proxies as you like.

For more information on configuring a content proxy, refer to the chapter entitled "Servers".

Admin Server Settings

The **Admin Server Settings** tab also contains settings for remote administration.

Listening IP:

Specifies the IP address the reverse/content proxy uses to listen for remote administration connections. The value may be any LAN/WAN or real IP address of the server host. The dotted-decimal 0.0.0.0 is used for listening on all adapters' IP addresses. A value of 127.0.0.1 is used for listening only on the local host. The server accepts administration connections addressed only to specified IP address. You can use this property to restrict administration access to your reverse/content proxy, thereby increasing security.

Port:

Specifies the TCP port number on which the reverse/content proxy listens for unencrypted remote administration connections. The default setting is *30033*.

SSL Port:

Specifies the TCP port number on which the reverse/content proxy listens for SSL encrypted remote administration connections. The default setting is *30034*.

Certificate File:

Specifies the certificate file (in pem format) used by the admin SSL server. Notice that the private key must be supplied in another file. See below.

Private Key:

Specifies the private key file used by the admin SSL server.

Accepted Hosts:

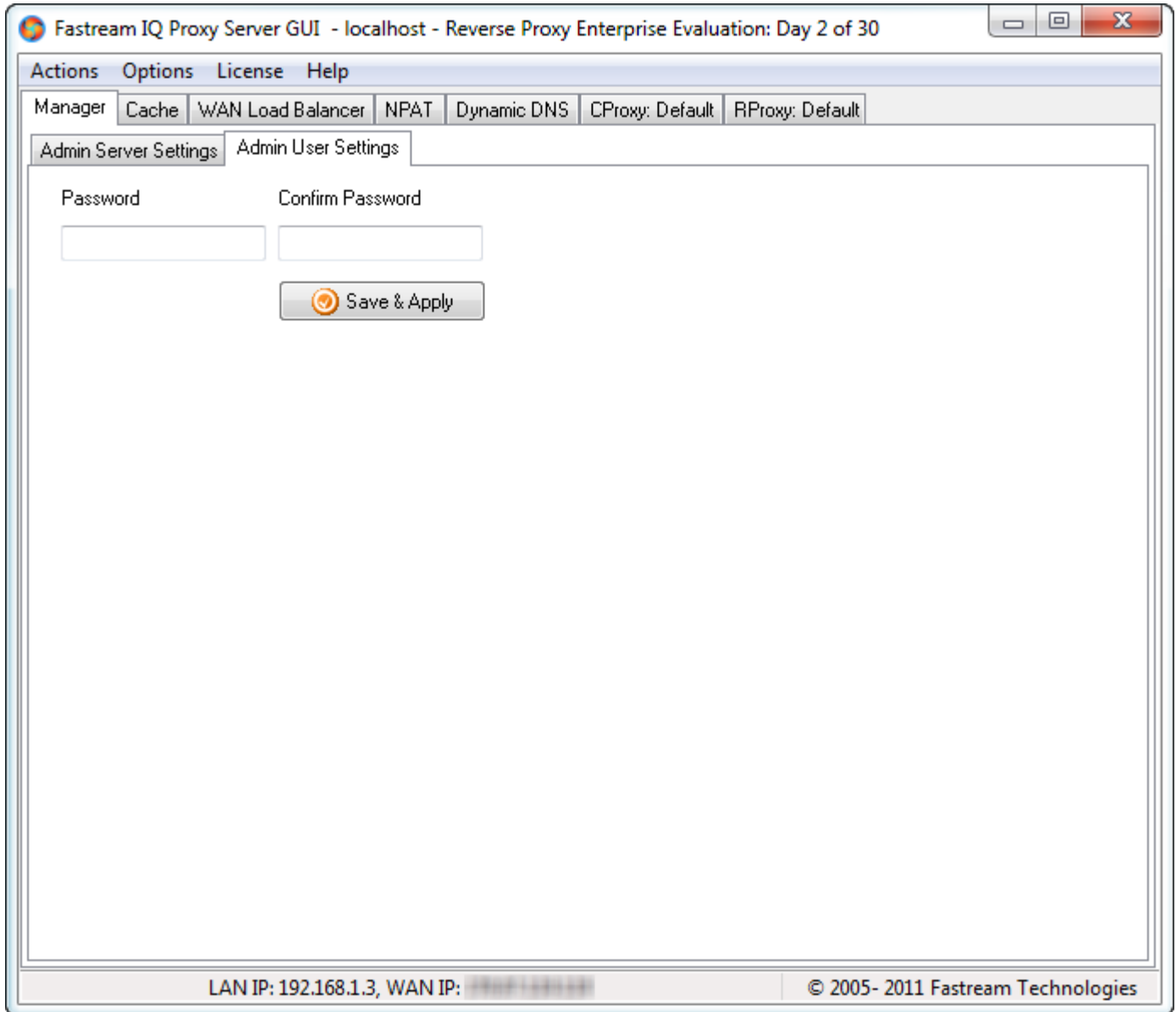
Defines the list of domains to which the SSL server will accept a connection. When you change one of the fields **Listening IP**, **Listening Port**, or **Current Admin password** and apply the changes, IQ Proxy waits for 3 seconds and then tests the changes. If the changes are not successful (i.e. the GUI cannot connect to the administration server after applying the changes), then the previous settings are restored, assuming the administration server could not successfully apply the changes.

For example, if you change the SSL port to the same port as the HTTP admin server (30033), the SSL port would be restored back to its previous value (30034) after 3 seconds due to the fact that the

server ports would clash.

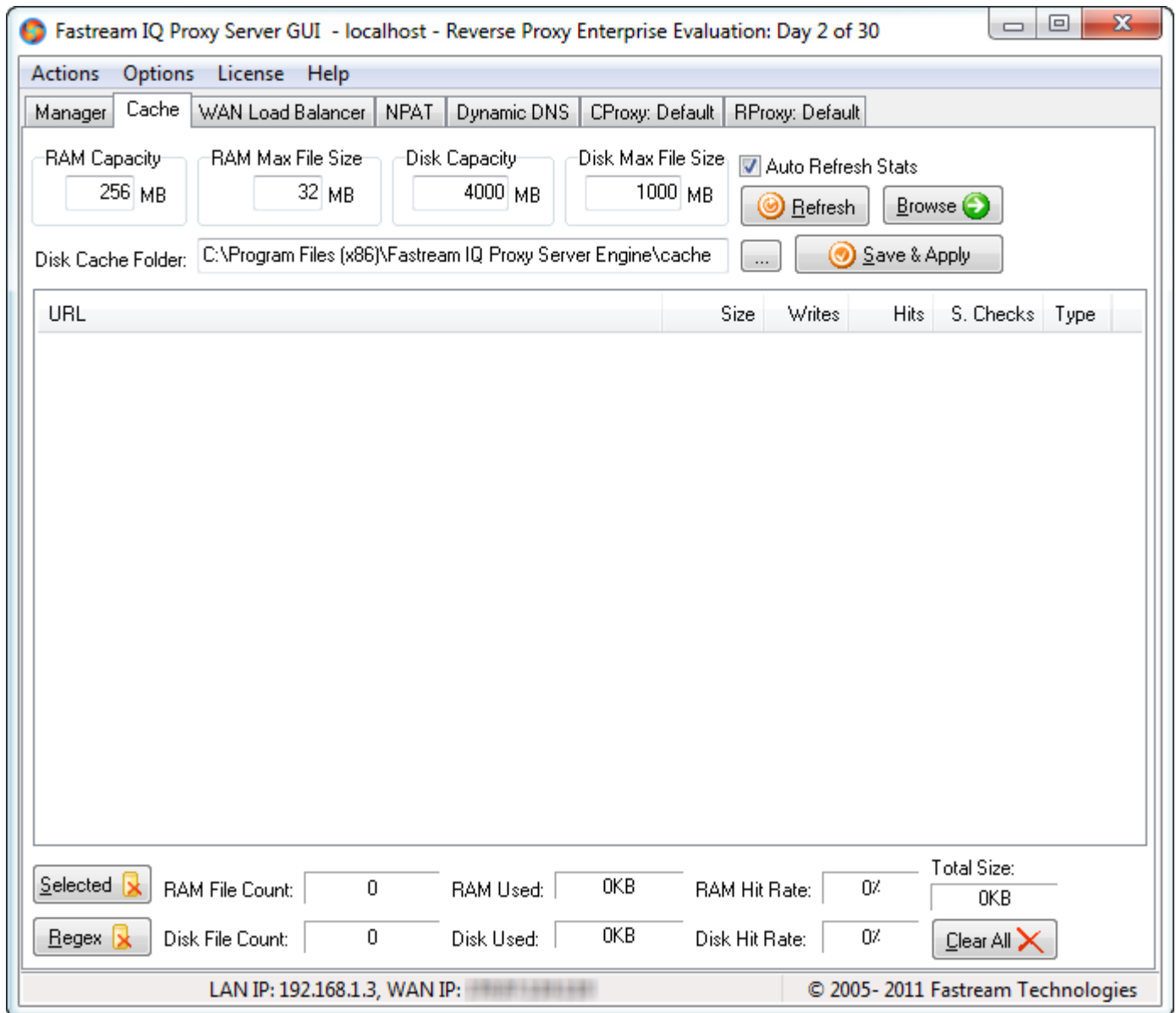
5.1.2 Admin User Settings

You can display the Admin User Settings options by clicking the **Admin User Settings** tab. The purpose of this tab is to allow you to change the password of the current (logged in) admin user. Click **Save & Apply** to place the changes into effect.



5.2 Cache

5.2.1 The Cache Tabsheet



Caching is a way of enhancing server speed by ten times. It stores the files and directory listings after a file is first downloaded in your server's RAM and works for both HTTP and HTTPS. It stores the served documents/files/directory listings in RAM and local/network drive for fast access. Its efficiency is most visible when multiple users are downloading.

You can use the **Cache** tab to adjust the cache size and max single cache object size. You can view the cache hit rate in order to get the serving percentage from the cache, and can check the absolute cache size. If you do not want to benefit from caching you can disable these properties.

Also, you can browse the cache object URL, clear all of the cache, or delete a single cached file. The **Writes** field indicates the number of requests that wrote to the file (as long as the remote file was not

altered) and the **S. Checks** is the positive staleness checks—if the staleness check fails, the object is deleted and a new one is created with new values.

5.2.2 How Does IQProxy Cache Work?

IQP has both RAM and DISK caching with definable separate capacities and maximum file sizes. For heavy usage, it is recommended to run the DISK cache on a 15,000RPM drive for desirable performance.

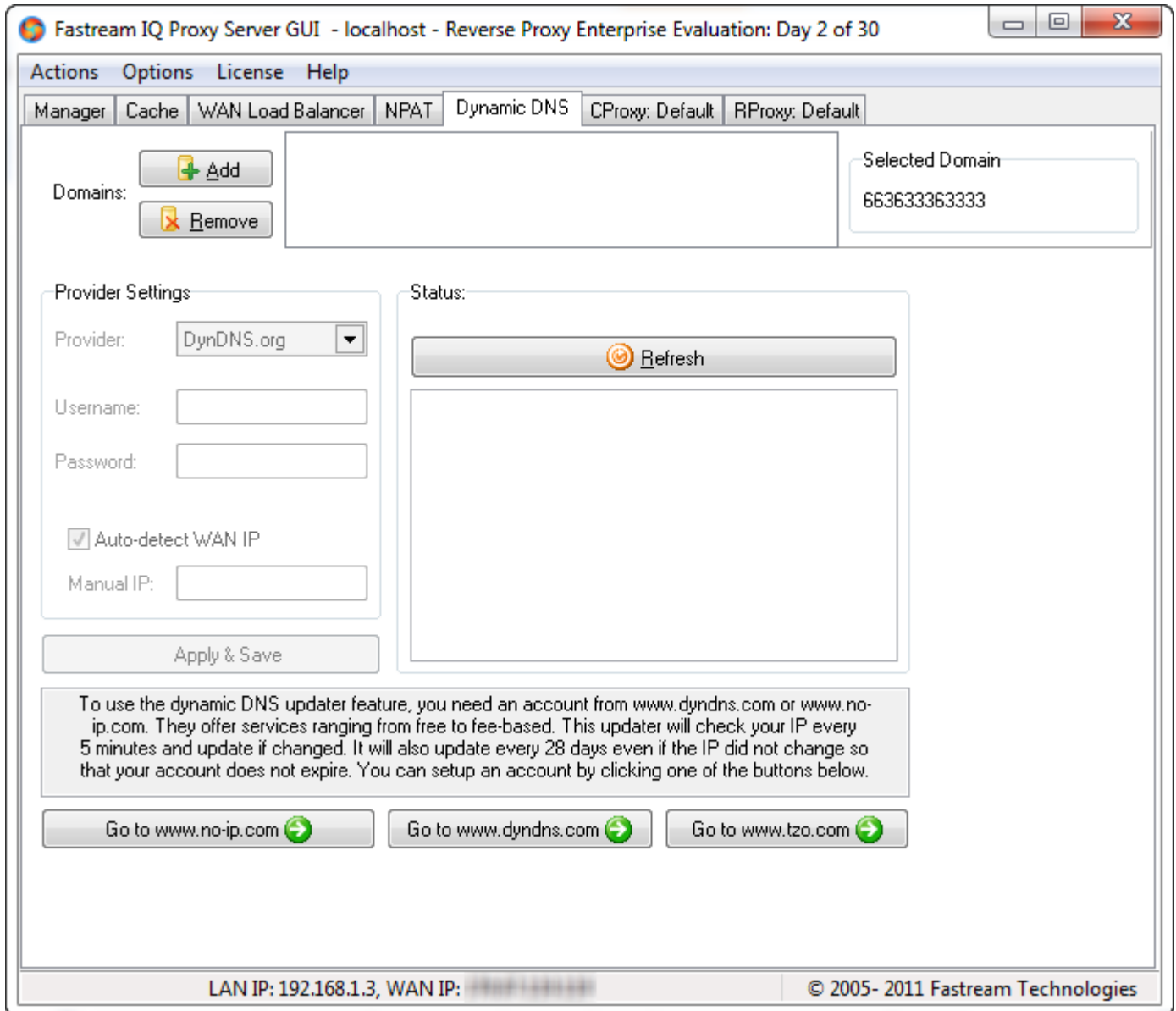
IQP cache has two modes: Obey web server preferences in content staleness checks or override it according to expiry check periods definable per MIME type. In the latter mode, unless a request's MIME type defined, it is checked for staleness every 2 seconds unless there is no "no-cache" indication in the response header. For the latter mode, the no-cache indication in the "Pragma" and "Cache-Control" headers are ignored, however in case of "Set-Cookie" presence, it is still not cached. The period for staleness checking in this mode is done according to rules definable per MIME type.

When a request file is just being accessed on server and when there are other clients requesting the same file, they are queued for 1 second with every 200 milliseconds the cache is checked for new data. Unless some data arrives in 1 second, it opens a new connection to the web server. This way when the first client silently goes away (i.e. power down, network cable unplugged), it does not wait forever.

When writing both to RAM and DISK caches, IQP uses the RAM cache memory space as a 128KB buffer for DISK cache. This way DISK seek time overhead is minimized.

v5.6+, cache can store compressed files without any need for on-the-fly recompression.

5.3 Dynamic DNS



The Dynamic DNS service enables you to alias a dynamic IP address to a static hostname. This allows your computer to be more easily accessed from various locations on the Internet.

The Dynamic DNS service is ideal for a home-based website, file server, or just to keep a pointer back to your home PC so you can access important documents while you are on the road. Using IQ Proxy Server, you can keep your hostname always pointing to your IP address, no matter how often your ISP changes your IP address. No more fumbling to find that piece of paper where you wrote down your IP address or e-mailing all your friends every time it changes.

Note: IQ Proxy Server comes with built-in support for dynamic DNS service of Dynamic Network Services (www.dyndns.org) and Vitalwerks NO-IP (www.no-ip.com). To use dynamic DNS, first register a hostname

at www.dyndns.org or www.no-ip.com. Once you receive the hostname, fill the required fields in the **Dynamic DNS** tab.

Domain:

The **Domain** refers to the name that your users will type in their browser's address bar to reach your proxy server through HTTP(S). It can be something like *yourdomain.dyndns.org*. You must register this domain name at www.dyndns.org or www.no-ip.com.

Provider:

Refers to the type of DNS you are using. Select either **DynDNS.org** or **No-IP.com**.

Username:

Specifies the login name you have registered at www.dyndns.org or www.no-ip.com.

Password:

Specifies the password for the provided **Username**.

When you are complete, click **Apply & Save** to save your entries. From this point forward, your IP address will be automatically updated whenever it is changed. You can follow the messages of the update process in the status box.

Note: Your IP address is checked for changes once every 5 minutes. Therefore you might have to wait 5 minutes before your IP address is updated after an address change.

You can use different hostnames for your site. In such a case, create two accounts at your favorite provider and make configuration changes accordingly on the **Dynamic DNS** tab.

5.4 Configuring a Reverse Proxy Listener

A reverse proxy listener sits in front of your web server(s)—usually in the same LAN—and routes/redirects traffic according to URL Rules you define.

In this tab, you have the ability to monitor the status, configure items like servers, (authenticated) URLs, TCP/IP connection settings, access filters, log files, compression of certain file types as well as SSL encryption settings, error pages, and viewing current user actions and firewalling intruders. These items are described in the next paragraphs.

5.4.1 Status

In the **Status** tab, you can start, stop, and restart the reverse proxy. The tab sheet displays the number of connected users and the transferred data (DL = download, UL = upload) size since the last run of the reverse proxy. Here you can also remove reverse proxy.

5.4.2 Web Servers

In the **Web Servers** tab, you can manage the definitions of the LAN/WAN web servers the reverse proxy will connect to plus your redirection URLs. Please note the difference between the two—in routing, all traffic passes through IQ Proxy Server (real proxying), whereas, in -pure- redirection the client makes a direct new connection to the web server with the defined protocol (HTTP/HTTPS).

You must first specify the server definitions in this tab sheet before you can assign servers to specific URL Rules in the **URLs** tab (see next section).

The currently defined routed servers are shown in the list of the **Web Servers** tab. For each routed web server, the following information is shown:

IP number: This is the server's IP number and can be a non-numeric domain name (for example, www.LANWebServerDomain.com). If you define it as a numeric IP, HTTP request header host will not be modified.

Port: This is the server's port number.

Path: This indicates the relative path of the LAN web server to serve for the IQ Proxy Server requests.

Capacity: This is the overall capacity of the server relative to the other servers.

Ping: This is the server's current ICMP ping time.

Max Connections: This is the maximum amount of simultaneous connections the server will handle.

Current Connections: The current amount of active connections to the specific server.

Use the **Add**, **Remove**, **Edit**, and **Refresh** buttons to manage the server definitions.

Fastream IQ Proxy Server GUI - localhost - Reverse Proxy Enterprise Registered

Actions Options License Help

Manager Cache NPAT Dynamic DNS CProxy: Default RProxy: Default

Compression URL Rewrite Header Rewrite Anti-Hotlink Error Pages Monitor Actions
 Status Web Servers URL Rules Options Cache Options Firewall Log SSL/TLS Encryption

Routed Web Servers (traffic passes through IQProxy)

Auto Refresh
 Backspace removes

IP	Port	SSL	Path	Capacity	Ping (ms)	Max Connections	Current Connections	Failures
127.0.0.1	81	No	/	50	N/A	256	0	0
192.168.1.101	80	No	/	50	Untested	256	0	0
192.168.1.103	80	No	/	50	Untested	256	0	0
owa.fastream.com	80	No	/	50	Untested	256	0	0
sp.fastream.com	80	No	/	50	Untested	256	0	0
www1.fastream.com	80	No	/	50	1232	256	0	0
www1.iqproxyserver...	80	No	/	50	5819	256	0	0
www2.iqproxyserver...	80	No	/	50	2168	256	0	0

Redirected Web Servers (traffic does not pass through IQProxy--pure redirection)

Auto Refresh
 Backspace removes

IP	Port	SSL	Path	Capacity	Ping (ms)	Path Relative	Code	Failures
asia.fastream.com	80	No	/	50	733	No	301	0
emea.fastream.com	80	No	/	50	764	No	302	0

LAN IP: 192.168.40.1, WAN IP: © 2005- 2011 Fastream Technologies

5.4.2.1 Adding routed servers

Clicking **Add Routed Server** displays the Server Information pop-up dialog box. In this dialog box you can specify the following routed server attributes:

IP Address:

This is the server's IP address. You may also use a valid domain name (e.g. *www.LANWebServerDomain.com*).

Port:

This is the server's port number (the default value is port number 80 for HTTP and 443 for HTTPS).

Path:

This is the relative path of the IQ Proxy LAN access to the LAN web server. For example, a request of **/path/index.html** would translate to **/IQ Proxy/path/index.html** (when no **Preserve Target Web Server Path** and **Preserve Request Path** is checked for the assigned URL Rule).

Capacity:

This is the overall capacity of the server relative to the other servers. The capacity must be a value ranging between 0 and 100 inclusive. The default value is a capacity of 50. If this is "0" then the server is suspended. If it is "1" then it is only assigned when all the other assigned servers fail.

Max Connections:

This is the maximum amount of simultaneous connections the server will handle. The default value is a maximum of 256 connections.

Client Connection SSL:

This option ensures that the connection is made with SSL2/3 or TLS1 at the highest level of encryption possible. The optional certificate and private key is for the web server to verify the IQ Proxy Server client as it announces itself in the SSL handshake. The **Verify peer** option enables IQ Proxy Server to verify a web server against the certificate authorities listed in specified **CA File**. **Password** is the client certificate's private key password.

One unique feature of IQ Proxy Server is the SOCKS and chained forward proxy support. This makes it possible to use intermediate proxies between the IQ Proxy Server and web server defined.

Clicking **OK** in the dialog box accepts the server definition. The newly added server definition is shown in the list of servers of the **Web Servers** tab. You can escape from the Server Information dialog by pressing the Escape button or by clicking **Cancel**.

5.4.2.2 Adding redirected servers

Clicking **Add Redirected Server** displays the Redirect Server URL pop-up dialog box. In this dialog box you can specify the following redirected server attributes:

URL:

This is the server's relative or absolute redirect URL. To define an absolute redirect URL, select the **All the paths are redirected to this absolute URL** option. To define a relative redirect URL, select the **Paths are redirected relative to this URL** option.

Redirection Type:

This is the HTTP response code that corresponds to this redirect definition. Options are: **301 Found**, **302 Moved**, and **307 Temporary**.

Capacity:

This is the overall capacity of the server relative to the other servers. The capacity must be a value ranging between 0 and 100 inclusive. The default value is a capacity of 50. If this is "0" then the

server is suspended. If it is "1" then it is only assigned when all the other assigned servers fail.

Clicking **OK** in the dialog box accepts the redirect server definition. The newly added redirect server definition is shown in the list of redirected web servers of the **Web Servers** tab. You can escape from the Redirect Server URL dialog by pressing the Escape button or by clicking **Cancel**.

Removing server definitions

Clicking **Remove** removes the currently selected server in the server list of the tab sheet. Ensure that you first select the proper server definition to be removed and then click **Remove**. The selected server definition is then removed from the server list.

Editing server definitions

Clicking **Edit** will display the Server Information dialog box pop-up for the currently selected server definition. So be sure to first select the proper server definition to be edited and then click **Edit**.

In the Server Information dialog box pop-up, you can change the server's attributes as when when adding a new server (see Adding servers in this section).

Refreshing server definitions

Clicking **Refresh** will update the server definition information such as the Ping and Current connections. The same properties mostly apply to the redirected servers. The new ones:

Permanent redirection: Uses the 301 HTTP response code instead of 302. If you don't want search engines to assume the redirection is permanent, then make this property **no**.

Relative path: In the relative case, the URL of the request is concatenated at the end of the target redirected web server path definition URL when redirection takes place. For example,

GET /images/background.gif is the assumed request, whereas, the target server definition is <http://www.fastream.com/oldsite>

The redirection would occur (with relative path) to:

<http://www.fastream.com/oldsite/images/background.gif> whereas it would be without the relative path as <http://www.fastream.com/oldsite> (same as the target server path).

5.4.3 URL Rules

The **URL Rules** tab allows the administrator to influence the way the reverse proxy listener directs requests for (specific) URLs to the underlying assigned web servers. The URLs for which specific request handling is configured are called "Request URLs."

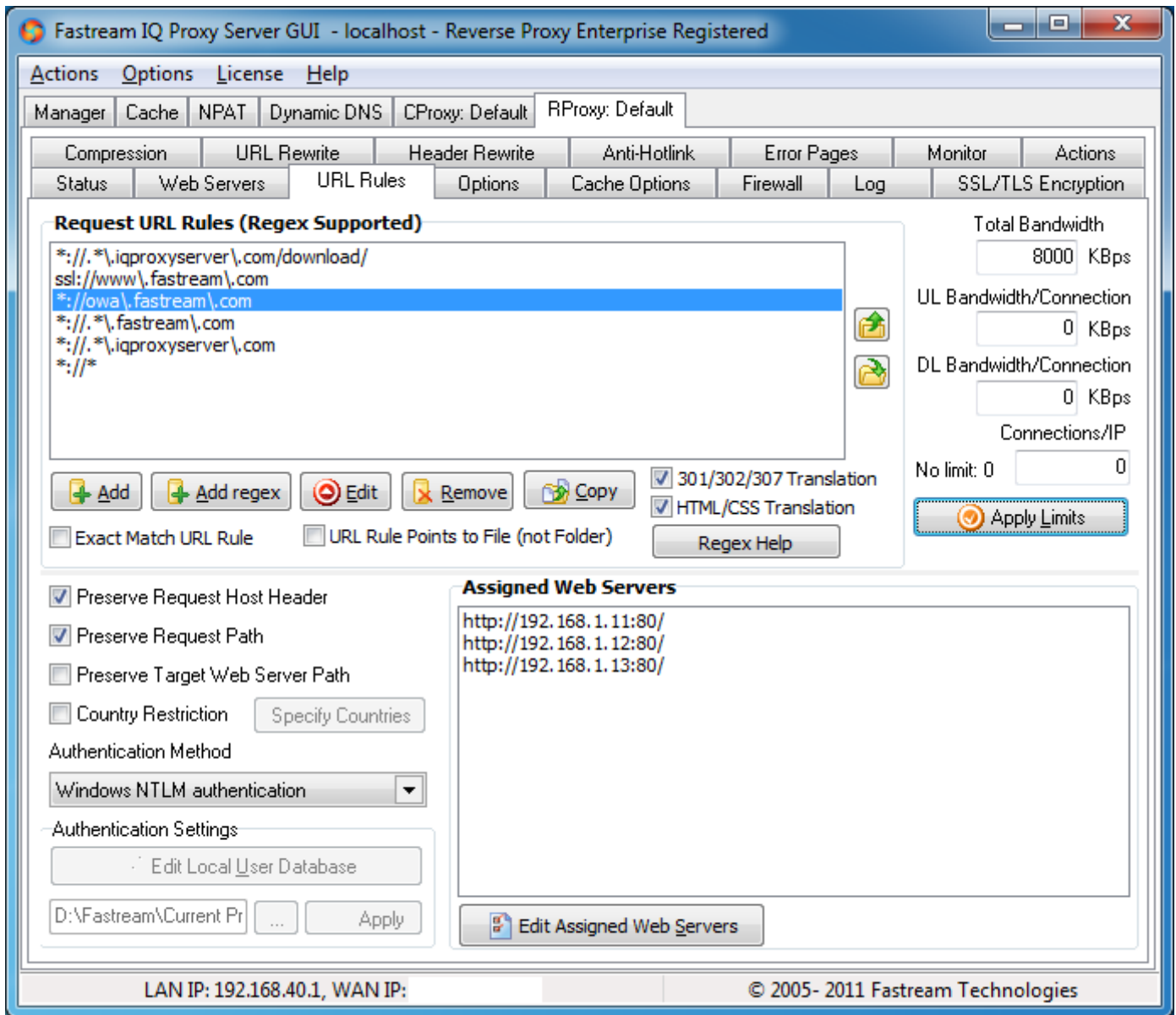
Note that you will have to first specify the server definitions in the **Web Servers** tab before you can assign servers to Request URLs in this tab (see the previous section).

Defining Request URL Rules

You may explicitly direct requests for certain URLs to specific assigned servers. This is managed in the **Request URL Rules** list and the **Assigned Web Servers** list of this tab.

By default the **Request URL Rules** list contains the entry `*://*`, which is the "catch all uncached" rule that is undeletable. Initially the Assigned Web Servers list does not contain any values. So in case of first-time configuration, you must specify an assigned server for the `*://*` Request URL in order to use the reverse proxy at the very basics.

Refer to the "Assigning Servers" section for how to assign servers to a "Request URL."



Adding "URL Rules"

You can add other specific "Request URL Rules" for which you want requests to be handled by specifically assigned servers. A "Request URL Rule" is specified as a URL path but always without the use of port numbers. You may even use a wildcard (indicated by the asterisk * symbol) in place of the leading domain name. It is also possible to assign different URL Rules with http:// and ssl:// as well as *:// prefixes. The first two cases are used for handling HTTP and SSL requests, respectively. The last one is used for handling both HTTP and SSL.

Correct examples of "Request URL Rules" are:

- http://mydomain.dyndns.org/home/user
- *://localhost/home/user
- ssl://192.168.123.101/home/user

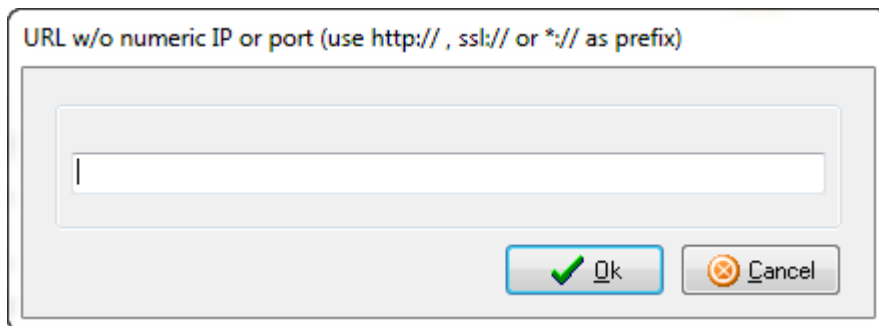
- *.*//*/home/user
- http://www.domain.com/path/file.php

And you must not specify "Request URL Rules" with IP port numbers, such as:

mydomain.dyndns.org:80/home/user

All requests to files in the folder indicated by the "Request URL Rule" and all files in the underlying folders of that rule will be handled by the assigned server(s).

Add a "Request URL" by clicking **Add** below the "Request URL Rules" list. The Enter URL rule w/o port pop-up dialog box displays. Type the "Request URL Rule" that you want to be handled non-default by IQ Proxy Server and then click **OK**. Otherwise, press the Escape button on the keyboard or click **Cancel** to abort the action.



After clicking **OK**, the newly added URL is shown in the list of "Request URL Rules." Also note that the list of assigned servers in the "Assigned Web Servers" list has now become empty. You will have to assign specific servers that will handle the "Request URL Rule." See the next paragraph, "Assigning Servers," for how to assign servers to a "Request URL Rule."

In this way you can add a number of "Request URL Rules" and their assigned servers.

Setting order of "URL Rules"

You can also specify the rule order in which requests to URLs will be handled. That order can be changed with the up and down buttons at the right hand side of the "Request URL Rules" list.

A requested URL is handled by the top-most "Request URL Rule" that has a (partial) match with the requested URL. Ensure that the most specific "Request URL Rules" are higher in the list if you really want to influence the behavior of the reverse proxy.

Note: The "Request URL Rule" named "Default" always has the lowest priority regardless of its placement in the "Request URL Rules" list. In this way, the URL "Default" is a catch-all 25 rule. Also note that the user-definable "Request URL Rule" consisting only of the wildcard symbol "*" can also be used as a catch-all rule, however this rule has the priority indicated by its placement in the "Request URL Rule" list.

Removing "Request URL Rules"

Clicking **Remove** in the "Request URL Rules" list will remove the currently selected "Request URL Rule". First select the URL Rule to be removed and then click **Remove**. This will display a delete confirmation prompt. Clicking **Yes** deletes the URL Rule. Clicking **No** cancels the delete action.

Assigning Web Servers

In the "Assigned Web Servers" list, you can specify the servers that will handle a specific "Request URL

Rule.” First select the concerning URL in the “Request URL Rules” list and then assign servers to that selected URL. Note that the servers’ IP addresses/domain names and IP port numbers first have to be defined in the **Web Servers** tab (refer to the previous section). Select an IP address:IP port combination and click **OK** to assign the server to the currently selected “Request URL Rule.”

Exact Match URL Rule

When you select the **Exact Match URL Rule** option for a URL Rule, it means that the rule is only matched when the request is exactly the same as the URL of the rule. For example if you have two URL Rules as,

1. <http://www.domain.com/path> (exact match)
2. <http://www.domain.com/path/> (exact match not checked)

When you get a request such as, <http://www.domain.com/path>, the first URL rule is matched. However if requests such as, <http://www.domain.com/path/> or <http://www.domain.com/path2/> or <http://www.domain.com/path/file.php> arrive then the second URL Rule is matched. URL Rule matches are case-insensitive. It is disabled by default.

Preserve Request Path

When you select the **Preserve Request Path** option for a URL Rule, it means that the path of the incoming URL is forwarded as is, without any modifications. Usually this option should not be used; therefore, it is disabled by default.

Preserve Target Web Server Path

When you select the **Preserve Target Web Server Path** option for a URL Rule, it means the path of the incoming URL is forwarded and is not taken into consideration. Just the path of the target web server defined in the **Web Servers** tab is forwarded. Usually this option should not be used; therefore it is disabled by default.

URL Rule Points to File

When you select the **URL Rule Point to File (not Folder)** option for a URL Rule, it means the path of the URL Rule is a direct file path. Usually this option should not be enabled so disabled by default.

Preserve Request Host Header

This option forces the reverse proxy to forward the host header as is, without replacing with hostname defined as target web server. This is useful to have one web server definition for multiple domains/URL Rules.

Assigning Bandwidth per URL Rule

You can specify the bandwidth per URL Rule in terms of Kilo Bytes per Second in the “Bandwidth (kBps)” section. If the URL Rule matched for other settings, such as servers and authorization, has no bandwidth setting (“0”), then the next rule in the priority list that covers the URL request is assigned as the “bandwidth rule” per request. And this goes on until the “Default” rule. Use care when assigning bandwidth limits for subfolders as their sum may add up to more than the parent folder limit.

Bandwidths are assigned per URL rule, not per socket. Therefore, this is like the IIS domain bandwidth limit.

Country Restriction

When you select the **Country Restriction** option, the URL Rule selected is matched when the client is either in the specified country list or not included in the list. This is configurable by clicking **Specify Countries**.

Authentication

So far you have defined an ordering of Request URL Rules and assigned servers per "Request URL Rule." As an option, you may want to consider forcing users to authenticate themselves when they try to connect to a specific "Request URL Rule." To activate this, first select an authentication method.

Basic Authentication

In HTTP/1.0/1.1 basic authentication, the username and password are transmitted in the request "Authorization" header as Base64Encoded and no encryption or protection at all. This mode is supplied because not all clients support the other modes.

Digest Authentication

This is a HTTP/1.1 only mode which is secure as the password is not transmitted in cleartext but in hashed form. This means that "wiretappers" cannot read the password or store it for future reuse. However, notice that in all authentication methods, the data payload transmitted is still cleartext. You need to use SSL/TLS for encrypting the entire channel.

Basic or Digest Authentication

IQ Proxy Server supports both schemes and the client chooses which it supports. If the client supports digest, according to RFC2617, it ought to select that authentication scheme as that is more secure.

NTLM Authentication

NTLM is the proprietary authentication method of Microsoft Windows® for both local and domain controller accounts. According to the default Windows security policies, the account must have non-empty password and the IQ Proxy Engine service should be assigned the right privileges/user accounts. You can change the Windows account IQ Proxy NT-service is using from **Start, Control Panel, Administrative Tools, Services**, right-click the IQ Proxy service, **Properties**. This is the most secure authentication scheme IQ Proxy Server supports.

HTML Authentication

This shares the same IQ Proxy Server native user database for users and passwords. Once the user first enters a page in the URL Rule, he is shown the HTML in **(IQ Proxy Program Files Folder)\authHTMLForm.htm**, which can be customized provided that the new new file name (if changed is assigned from the IQ Proxy GUI and a valid POST is done as in **authHTMLForm.htm** with username/password. The password is transmitted in cleartext and stored in client cookies.

HTML-to-NTLM Authentication

This is the same as HTML Authentication, but the user database is now the Windows® NTLM service.

Note: It is recommended that you manage users in the IQ Reverse Proxy and not in the underlying assigned servers. In this way only you will not have to deal with each server's authentication configuration for assigning users. If the configuration is not set in IQ Proxy and they are not the same on all servers, then the pages may not display properly.

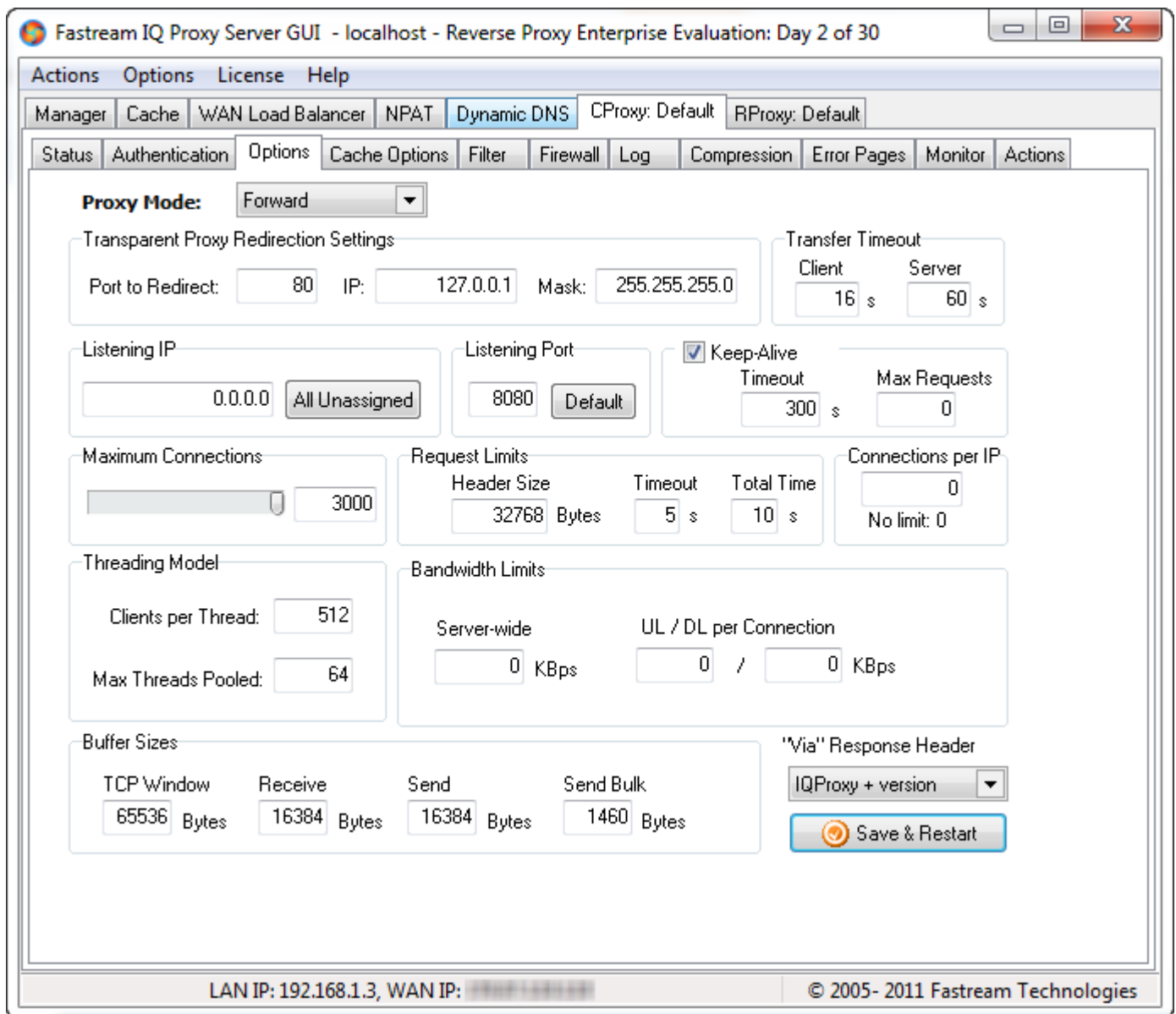
Importing/Exporting Users for Basic/Digest/Basic or Digest/HTML Schemes

If you want to have hundreds or even thousands of authenticated users, there is the option of specifying them with the following dialog box when you click **Import/Export Users**. You can even load/save to a file. The username and passwords are delimited by a space and there is only one username/password per line.



5.4.4 Options

The **Options** tab sheet enables you to configure several HTTP and SSL options.



Mode:

This can be **Forward** or **Transparent**. In order for the transparent mode to be used, the content proxy must be installed on the network gateway and the **redirection IP** cannot be 0.0.0.0 or 127.0.0.1 yet it can be a LAN IP. Mask is the network's subnet mask. Port is the port to listen all outbound traffic for. You cannot use the transparent proxying feature on the same computer the content proxy is installed.

Listening IP:

This is the IP address of the server machine the reverse proxy is running the service. Servers may be run

on machines having several IPs that are obtained by several devices. Set the Listening IP to and then you will be listening on all IPs.

Listening Port:

This is the TCP port on which the reverse proxy service is listening. This is port 80 by default.

Maximum-Connections:

This is the maximum number of simultaneous connections the reverse proxy service will handle.

Keep-Alive:

This timeout value is the idle time period (in seconds) in which each client connection is kept active. By default in HTTP/1.0, for each request a new connection is opened but if keep-alive is supported by the client and enabled on the reverse proxy, the same connection can be used for consecutive requests.

The **Maximum Requests** value is another limiting factor for the keep-alive setting. Unless it is zero, this is the limit for number of requests to be served on the same connection.

Max Fail Times:

This is the number of times a failed server should be retried until it is assumed dead. This is a per-server setting.

Preferred HTTP(S) Ping:

This is the ping limit to consider a fast server. Servers with low ping times are given a priority. This is a per-web server setting, in milliseconds. You can specify ping URLs from Web Servers tabsheet.

Max Threads Pooled:

This is the time a dead server is given to respond. After this period, the dead server will be rechecked. This is a per-server setting, in seconds.

This is the number of clients supported for each thread created. Each thread can run on, at most, one processor core. IQ Proxy Server automatically launches and load-balances among one thread per each core present on the hardware.

This is the number of threads that is pooled in the operating system. Note that Windows® does not support more than 2000 threads at a time per process, so setting this number above 2000 is not recommended.

Transfer Timeout:

This is the timeout period between two consecutive packets during download/uploads.

Persistent cookies for client-server match persistence:

This option allows cookies to be created to support session persistence of client-to-target-server routing. This enables a specific target server defined in the first visit to be responsible for all actions that belong to a specific client browser's session unless that assigned web server is offline/suspended.

This option is important for domains that typically use session information stored in databases to generate web pages dynamically (e.g., shopping carts). You can have two server computers each running IQP reverse proxies configured the same behind a load-balancer in conjunction with this feature since the target web server value in the cookie is just the hash of the target web server IP/port/path. Hence it is not dependent on IQP instance as long as the target web server configurations are the same.

Link & Content Translation:

The **link translation** option allows the 301/302/307 responses' "location" header to be translated with respect to the relative paths and absolute URLs defined.

The **content translation** option enables a high performance on-the-fly HTML link transformer. This is a feature for sites with HTML content, such as the following:

```
<a href="http://localhost:8080">link to my web server</a>
```

In the above case when you close port 8080 and enable only proxy port 80 on your firewall, then you will have the hyperlink not working because it is pointing absolutely to the specific IP address and port number (e.g. localhost:8080).

For these situations, a high-performance run-time HTML parser routine replaces the IP/port pairs into those of the proxy's.

Also, if in the LAN web server definition a path is used (other than "/"), relative static links are also translated accordingly.

Extensions to Exclude From Cache:

This option enables you to specify the file types (delimited by space) that are not to be cached. If you add "folder" than it would not cache www.domain.com or www.domain.com/path/ as well.

Request Header Size Limit:

This option enables you to specify the maximum HTTP header size (in bytes) for the connection is aborted by IQ Proxy Server.

Request Timeout:

This option enables you to specify the timeout value, in seconds, before the connection is aborted between two request header upstream packets.

Request Total Time:

This is the total time period (in seconds) for the request header to be received. Designed to stand against attacks in which the attackers open thousands of connections that send each header line with delay.

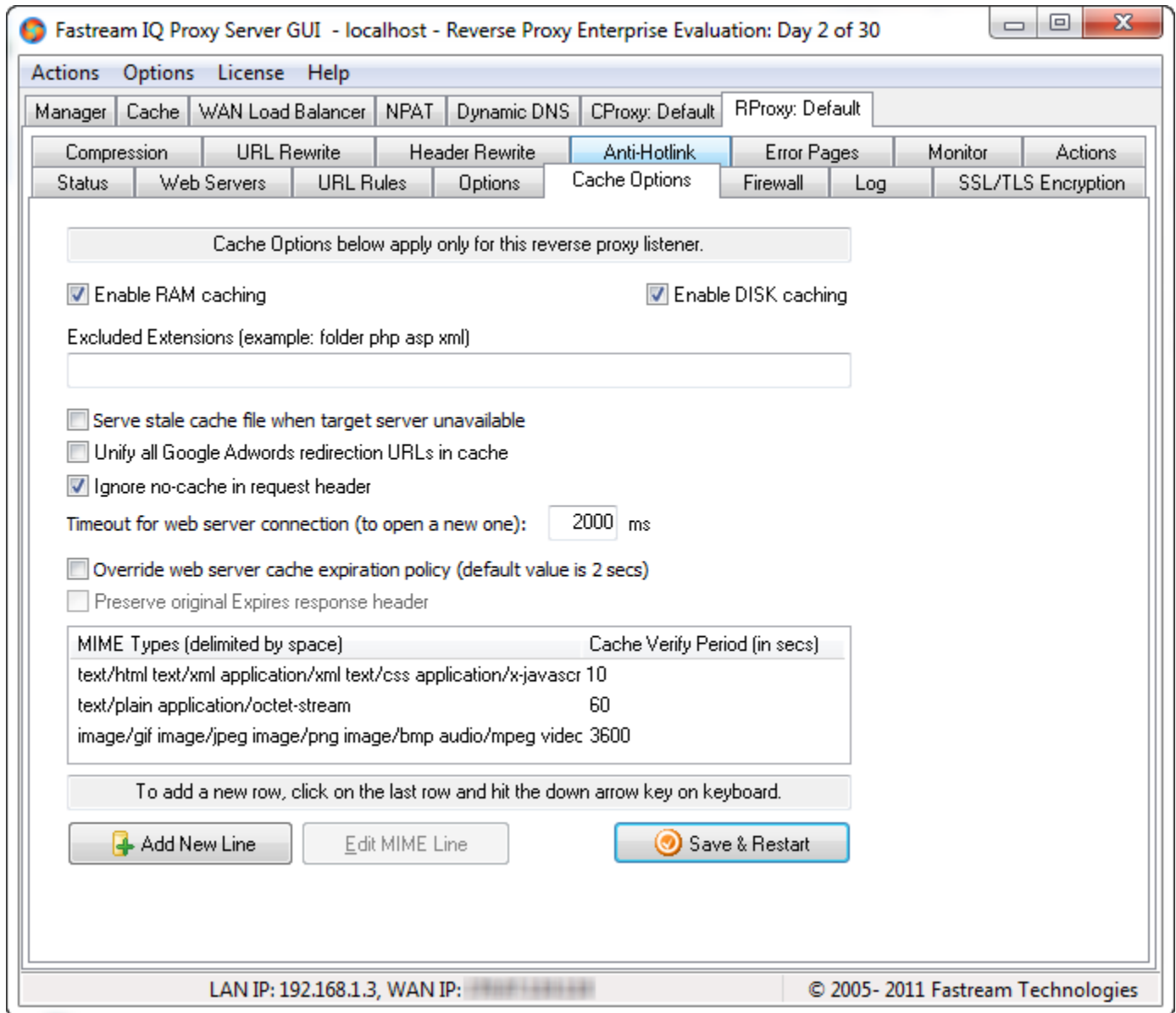
X-Client-Country Header Mode:

IQ Proxy Server can provide the country of the client to the web server by appending that information to the request header by resolving the client's IP with the IP2Location component. There are two formats for this: the short name (e.g., "US") and the full name (e.g., "UNITED STATES"). The web application programmer can read this information by reading the "CLIENT_COUNTRY" HTTP variable.

Unify all Google Adwords redirection URLs in cache:

When a URL is appended with **?param=value** the same page is displayed unless the script the URL points to takes that parameter into account. Google Adwords adds the **?gclid=...** parameter for logging purposes. Previous versions of IQ Proxy Server assigned different cache files to each of these, which resulted in thousands of redundant cache files. This option enables IQ Proxy Server to log the correct full URL, but serve it from a single cache file.

5.4.5 Cache Options



Enable RAM/DISK caching

For RAM and DISK caching preferences such as the capacities and max. file size, see the global Cache tabsheet.

Excluded Extensions

You can have some file extensions excluded from cache. Just delimit them with space and use "folder" (w/o quotes) for paths ending with slash.

Serve Stale Cache File When Target Server Unavailable

If the requested file is available in the cache as stale, unless you check this if all the assigned web servers are tried and tested then a 503 will be returned. If you check it, then the stale cached file will be returned.

Unify Google Adwords Redirection URLs

Unless you check this then all of them will have their own cache files such as,

www.iqproxyserver.com/?gclid=1abcd...

www.iqproxyserver.com/?gclid=12cd...

...

Ignore no-cache in Request Header

Unless this is checked, if the client demands complete refresh, the cached file is re-downloaded from web server.

Override web server preferences

A beneficial feature to consider is this. This feature enables proxy server admin to override web server content expiration policy by letting you specify after how many seconds each response MIME types will expire. This way, you can override server settings to save CPU cycles on the backend when you are sure your scripts/files are updated at what period. The default period is 2 seconds for unspecified MIME types. You can add more rows by simply clicking the down arrow key from keyboard. The **Preserve Original Expires Header** feature makes it possible for you to force the client to validate for new version of files at the original frequency while the proxy server does not access the web server that frequently.

5.4.6 Firewall

The **Firewall** tab enables you to apply filtering rules. Using the filtering rules, specific remote clients can either be permitted or blocked by the reverse proxy. The filtering is specified using IP numbers by default; however, it is also possible to specify filters using domain names or even countries.

5.4.6.1 DDoS

DDoS is an acronym for **D**istributed **D**enial of **S**ervice attack. These attacks are usually difficult to deal with given that there are many malicious clients attacking from many IP addresses.

IQ Proxy Server offers a way to cope with this DDoS attacks using the **DDoS** tab. Note that this feature is not enabled by default because some customers prefer to stress test the proxy, which emulates the same footprint as denial of service attacks.

There are specific settings for each client IP's number-of-accesses to each specific 2xx-3xx URL, any 404 page, and any 4xx page other than 404 with different reset periods (in seconds). There is also a definable period for clearing the client IP database (in minutes). If an attacker writes a tool that randomly creates URLs to exhaust the proxy server, it is easily caught with the 404 limit and disconnected before the header is read. If it passes that stage and, for example, requests the home page continuously, the header is received yet not responded.

5.4.6.2 SYN

The SYN firewall is built to limit the timeout of half-sockets when there are too many of them pending which indicates the attack level. Normally, Windows sends out three SYN-ACKs per half open socket if the first two are un-ACKed. In our firewall, this is reduced to 2 and 1 at higher attack levels. For each attack level, there are ten levels which should be sufficient for all cases. IQProxy SYN firewall also limits the timeout value for each SYN-ACK response.

5.4.6.3 IP

The **IP** tab enables you to restrict access to your Reverse Proxy. You can specify the IP addresses you want to block. In order to set IP rules, you need to enter the IP addresses in the dotted form, such as: *123.123.123.123*.

Selecting type of filtering

First you select the type of filtering by selecting the **Block only IPs below** or the **Permit only IPs below** option in the upper list box.

Adding IP filtering rules

In order to set IP filtering rules, you need to enter the IP address in the **Add Rule** section of the **IP** tab.

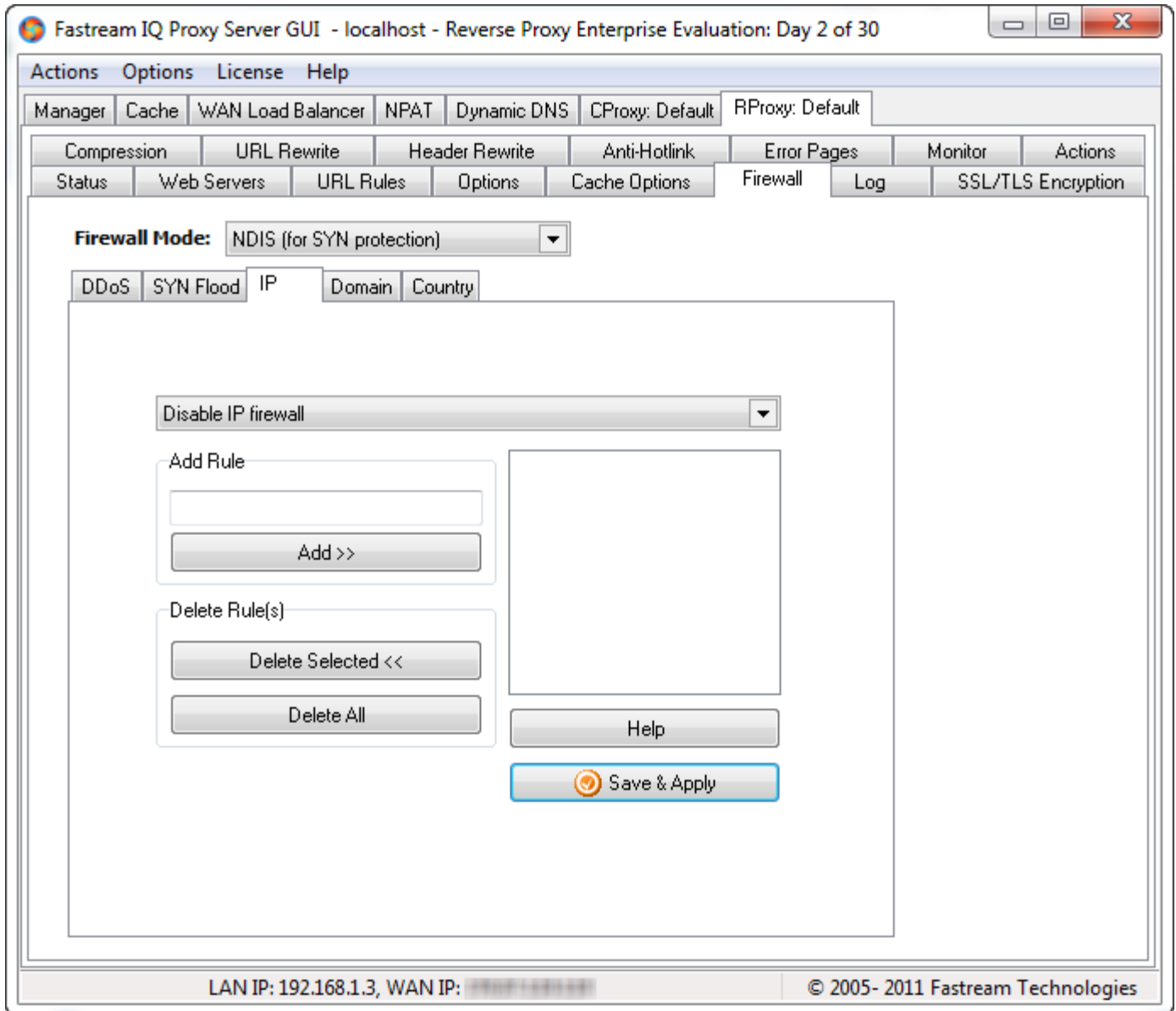
Note that you can specify a range of IP addresses at one time. The filtering type you choose in the upper list box affects the IP address entries, examples of which are provided below:

123.123.123.123 > Blocks/Permits only this IP address

123.123.123.x > Blocks/Permits all IP addresses that start with 123.123.123

123.123.123.xxx > This has the same effect with the one above

123.123.1x3.123 > Blocks/Permits all IP addresses of the form 123.123.1[0...9]3.123



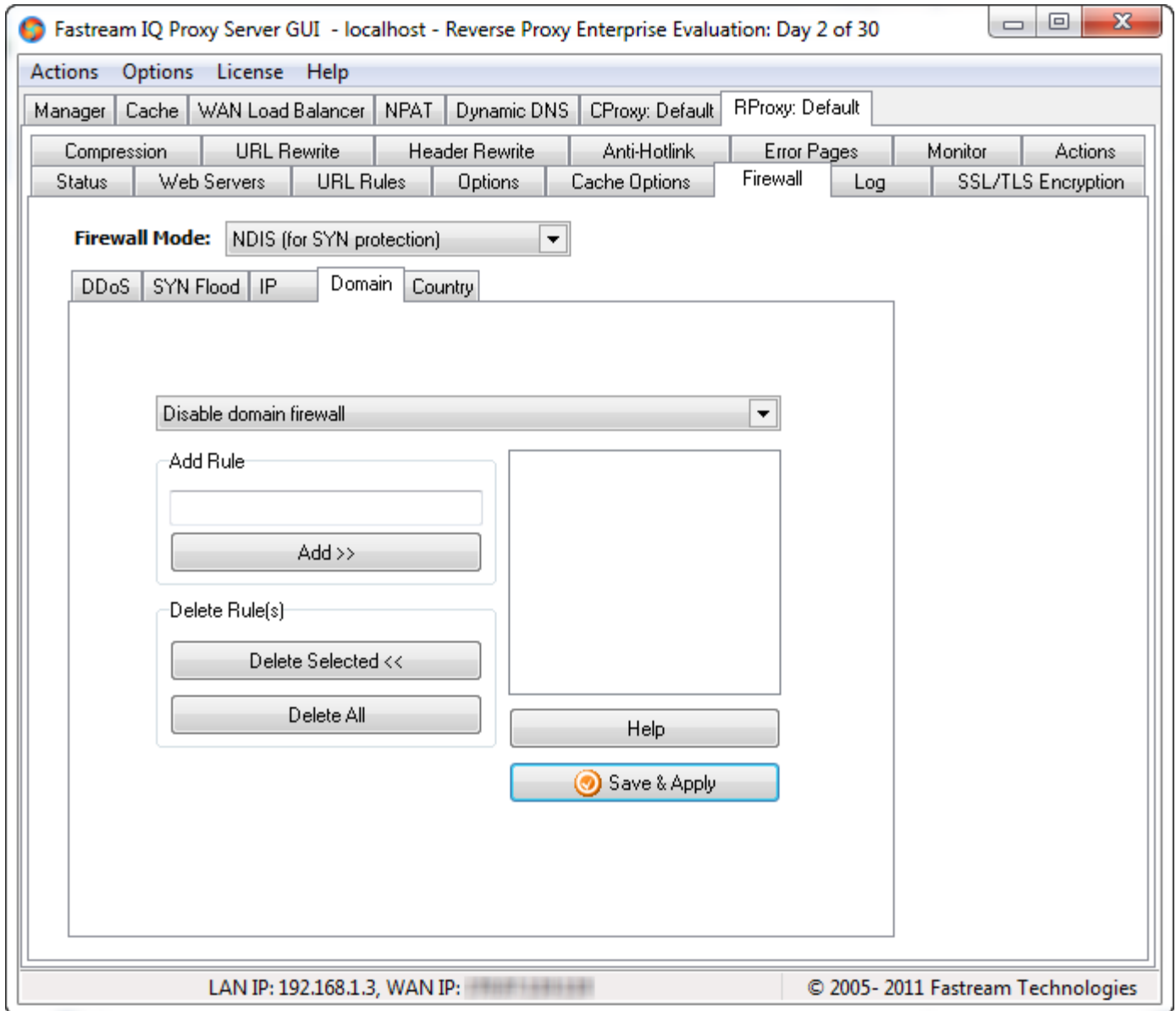
Deleting IP filtering rules

You can delete specific or all defined IP filtering rules by using, respectively, the **Delete Selected** or **Delete All** buttons. Be sure to select the correct IP filtering rule before clicking **Delete Selected**.

Click **Save & Apply** to activate the new or updated settings.

5.4.5.4 Domain

The **Domain** tab is similar to the IP filter but instead works with domain names and not IP addresses. You can block or permit domains and sub-domains. You can block a single computer with its domain name, or all computers within a domain.



Selecting type of filtering

First select the type of filtering by selecting the **Block only domains below** or **Permit only domains below** option in the upper list box. You can stop all domain filtering by selecting **Disable domain firewall**.

Adding domain filtering rules

In order to set domain filtering rules, you need to enter the domain names in the **Add Rule** section. You can use wildcards like in examples below:

- mycomputer.hackerzone.com > Blocks/Permits only this domain name
- *.hackerzone.com > Blocks / Permits all connections from
- domain comp*.hackerzone.com > Blocks / Permits comp1.hackerzone.com, comp2.hackerzone.com, compx.hackerzone.com, etc.

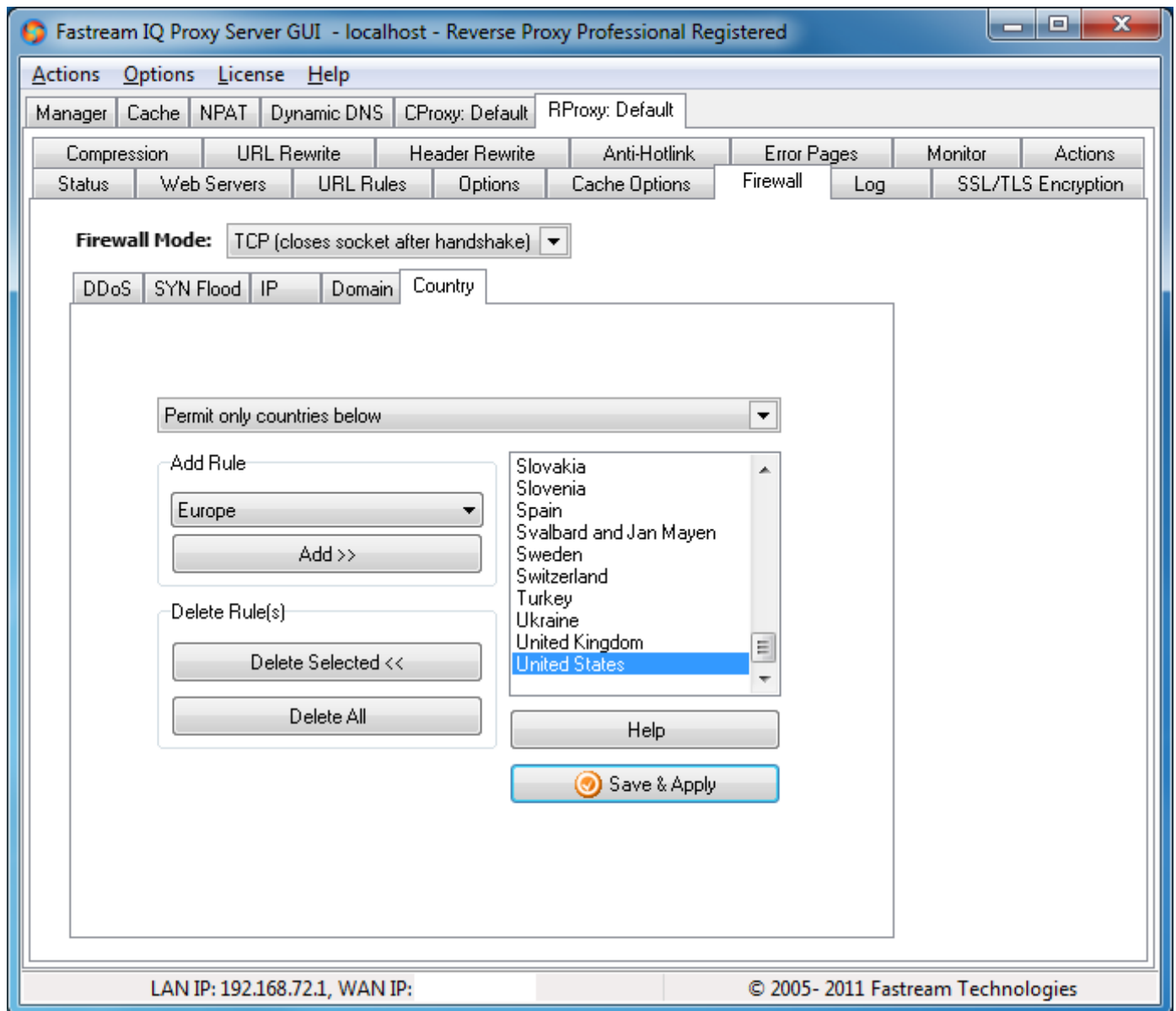
Deleting domain filtering rules

You can delete specific or all defined domain rules by using, respectively, the **Delete Selected** or **Delete All** buttons. Be sure to select the correct domain rule before clicking **Delete Selected**.

Click **Save & Apply** to activate the new or updated settings.

5.4.6.5 Country

IQ Proxy Server is the only reverse proxy tool with built-in country based filtering support. You can allow or deny connections from the countries you select. The IP addresses from the selected countries will be detected by the reverse proxy and will be permitted or blocked according to the rules you define.



Selecting type of filtering

First you choose the type of filtering by selecting the Block only countries below or **Permit only countries below** option in the upper list box. You can stop all country filtering by selecting the **Disable country firewall** option.

Adding country filtering rules

In order to set domain filtering rules, you need to enter the domain names in the **Add Rule** section. You can use wildcards like in examples below.

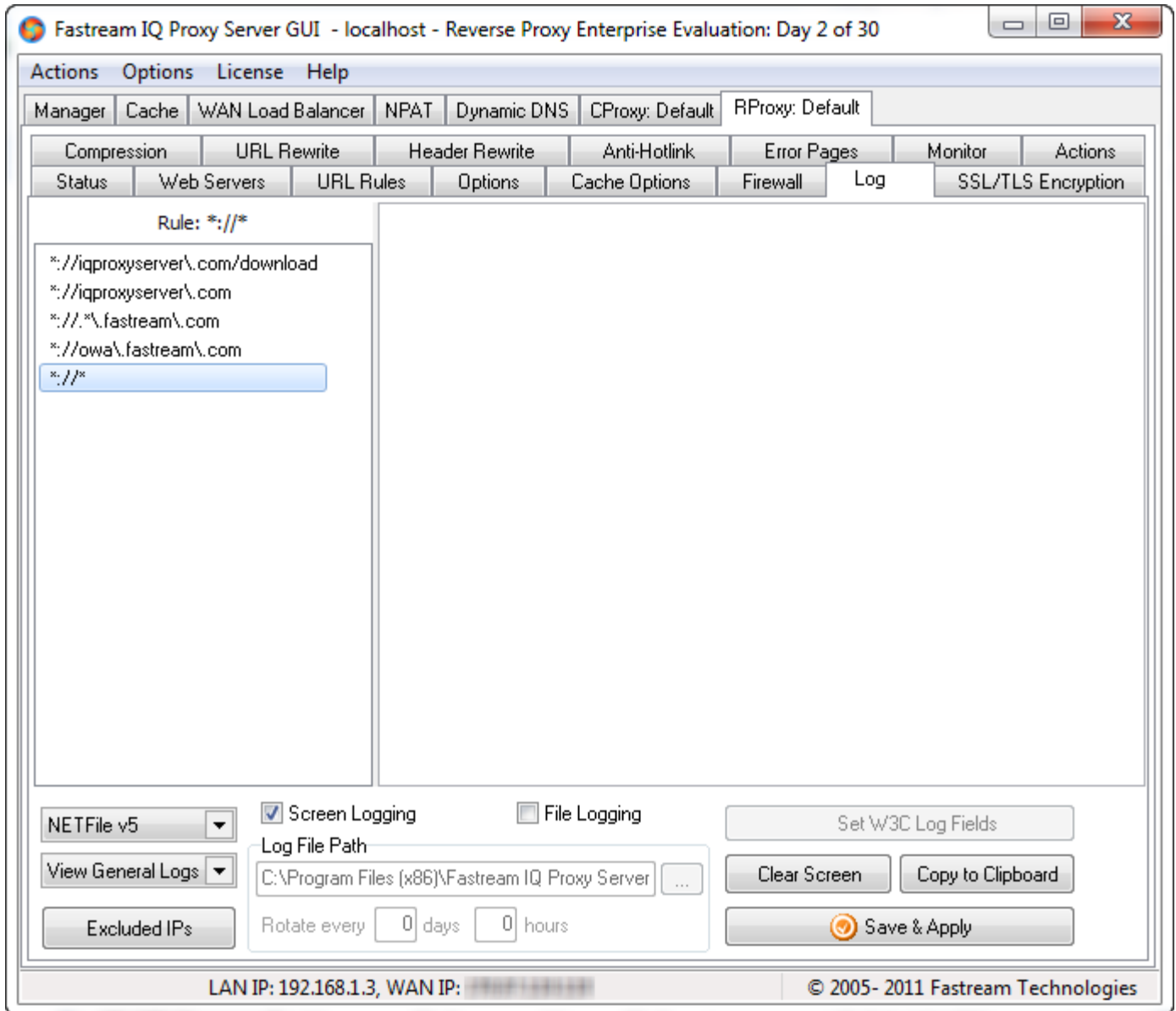
Deleting country filtering rules

You can delete specific or all defined country rules by using, respectively, the **Delete Selected** or **Delete All** buttons. Be sure to select the correct country rule before clicking **Delete Selected**.

Click **Save & Apply** to activate the new or updated settings.

5.4.7 Log

IQ Proxy Server can log the HTTP protocol commands passed between remote HTTP clients and the reverse proxy server engine. The reverse proxy retains the logs for a few seconds and then displays them so that the load will be alleviated making the reverse proxy-serve faster. This proves to be beneficial, especially when the user connection count increases.



The menu at the top of the **Log** tab allows you to arrange the log settings. Here you can choose the log format, enable/disable screen logging, copy logs to the clipboard to save them manually, or write the logs to a file you select.

The log settings can be applied to specifically selected "Request URLs." First select the desired URL, then make the changes in the log settings. Click **Save & Apply** to activate the new or updated settings.

Log formats

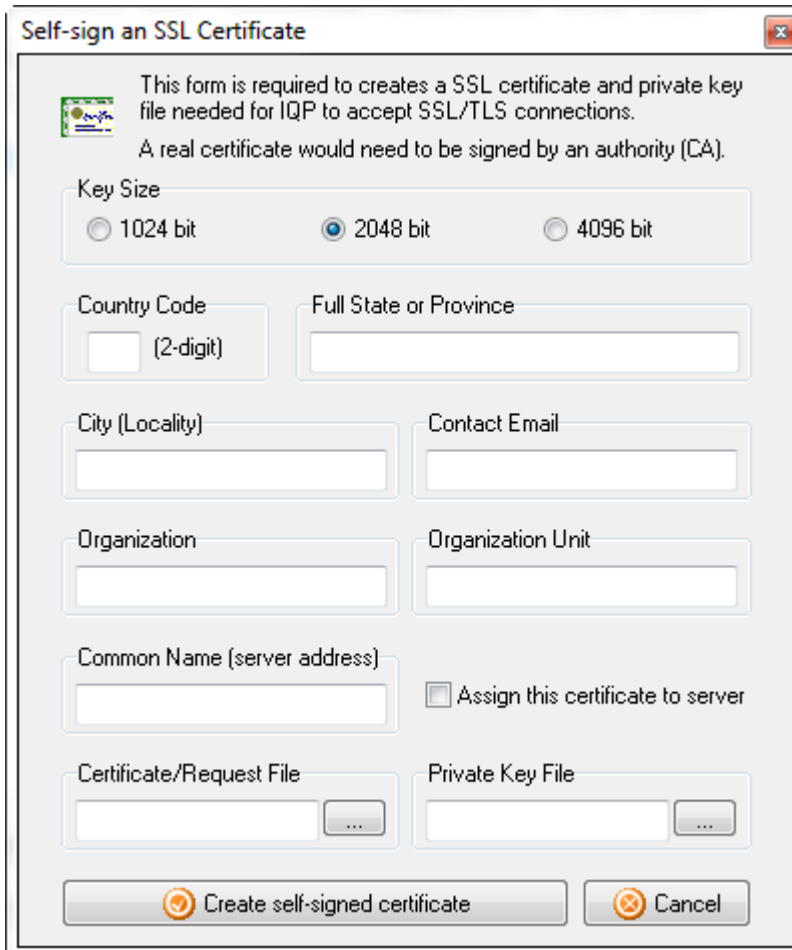
There are two log formats you can choose: (1) the IQ Proxy log format, or (2) the W3C extended log file format. The IQ Proxy log format displays most basic commands passed between clients and the reverse proxy.

The W3C extended log file format is a flexible format for recording HTTP requests, which is particularly suited for log analysis tools. ELF (W3C Extended Log Format) records more information than the common

IQ Proxy log format. It contains a sequence of lines containing 37 ASCII characters delimited by a new line. Lines that start with # are comment directives. The Fields directive indicates the HTTP request fields that are actually written in the log records that follow. You can use free tools such as *Gimli ELF* to analyze your logs if you choose this format.

5.4.8 SSL/TLS Encryption

IQ Proxy Server supports 256-bit strong SSL2.0/3.0/TLS 1.0 encryption. This means that hackers trying to attack your transferred information cannot read the actual data—all they would see is encrypted information. In order to use SSL, you need to have a server certificate, which could be either obtained from a certificate authority such as Verisign or you can create your own self-signed certificate using the **Self-sign certificate** button. Clicking this button displays the Self-sign an SSL Certificate dialog box, which enables you to create and self-sign your certificate. Only clients using this certificate can verify your identity.



The dialog box titled "Self-sign an SSL Certificate" contains the following fields and options:

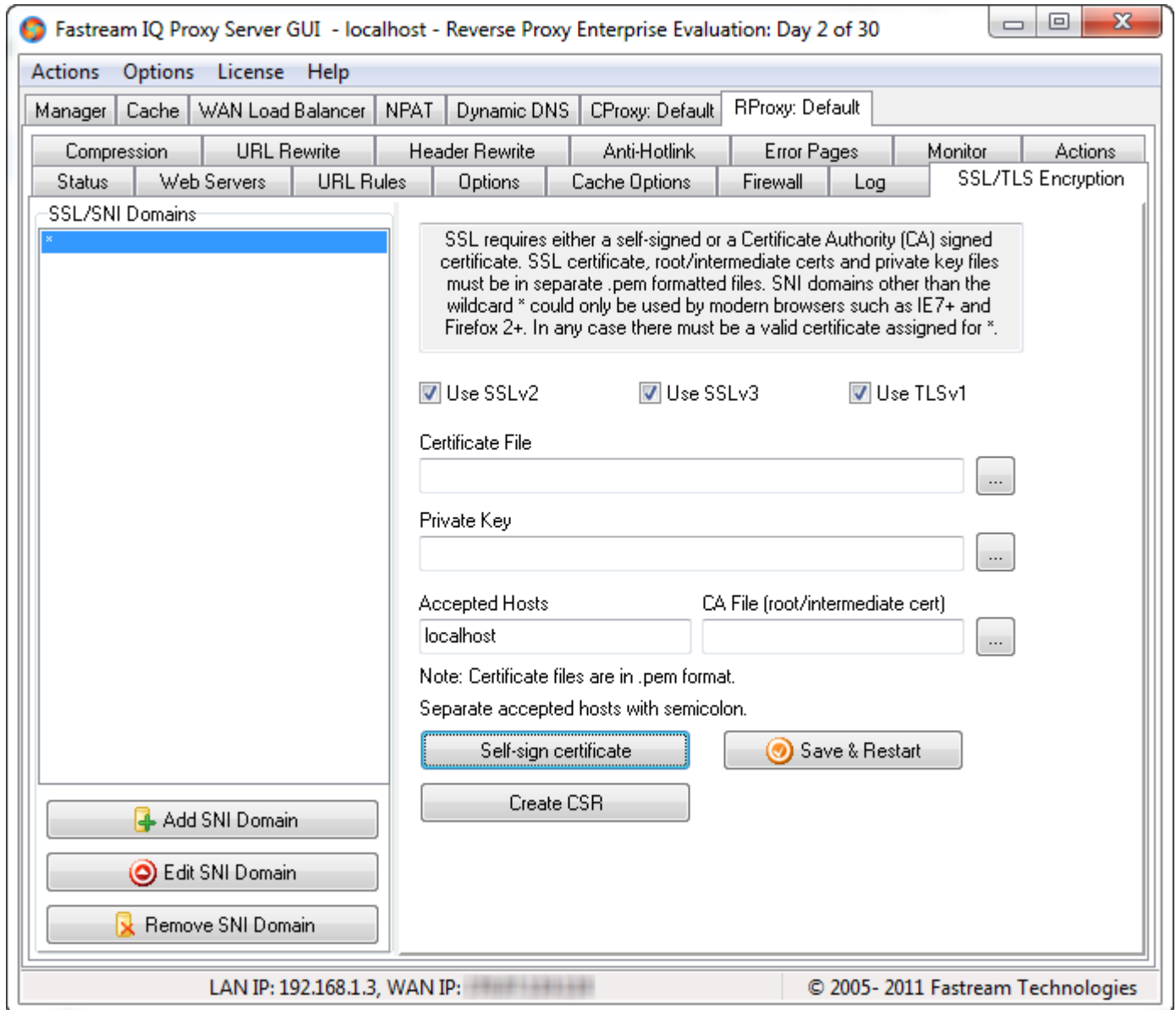
- Key Size:** Radio buttons for 1024 bit, 2048 bit (selected), and 4096 bit.
- Country Code:** A text field with "(2-digit)" below it.
- Full State or Province:** A text field.
- City (Locality):** A text field.
- Contact Email:** A text field.
- Organization:** A text field.
- Organization Unit:** A text field.
- Common Name (server address):** A text field.
- Assign this certificate to server:** A checkbox.
- Certificate/Request File:** A text field with a browse button (...).
- Private Key File:** A text field with a browse button (...).
- Buttons:** "Create self-signed certificate" and "Cancel".

Unless you fill in all the fields correctly, the client browser may report an additional warning to the end users.

To enter a real certificate, such as those purchased from Verisign/Thawte/Comodo, ensure that you convert the certificate to PEM format and make sure the certificate and the private keys are in separate files (sometimes they come in a single text file and you may need to cut-paste using a text editor such as

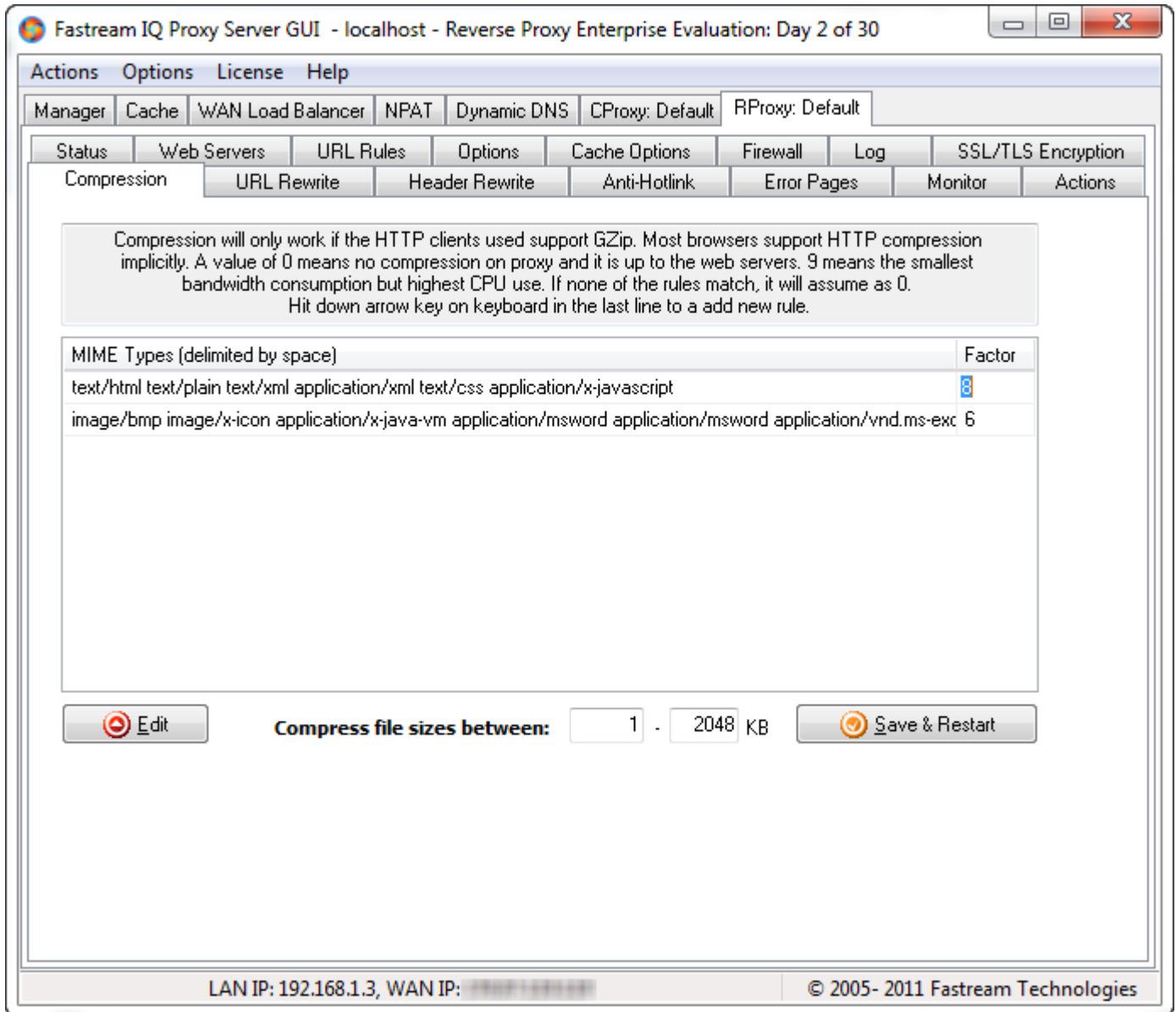
Windows® NotePad).

New in version 3.3R of IQ Proxy Server is the ability to assign multiple certificates for each IP/port using the Server Name Indication (SNI) protocol. You can also now assign "intermediate certificates" using the **CA Path** field.



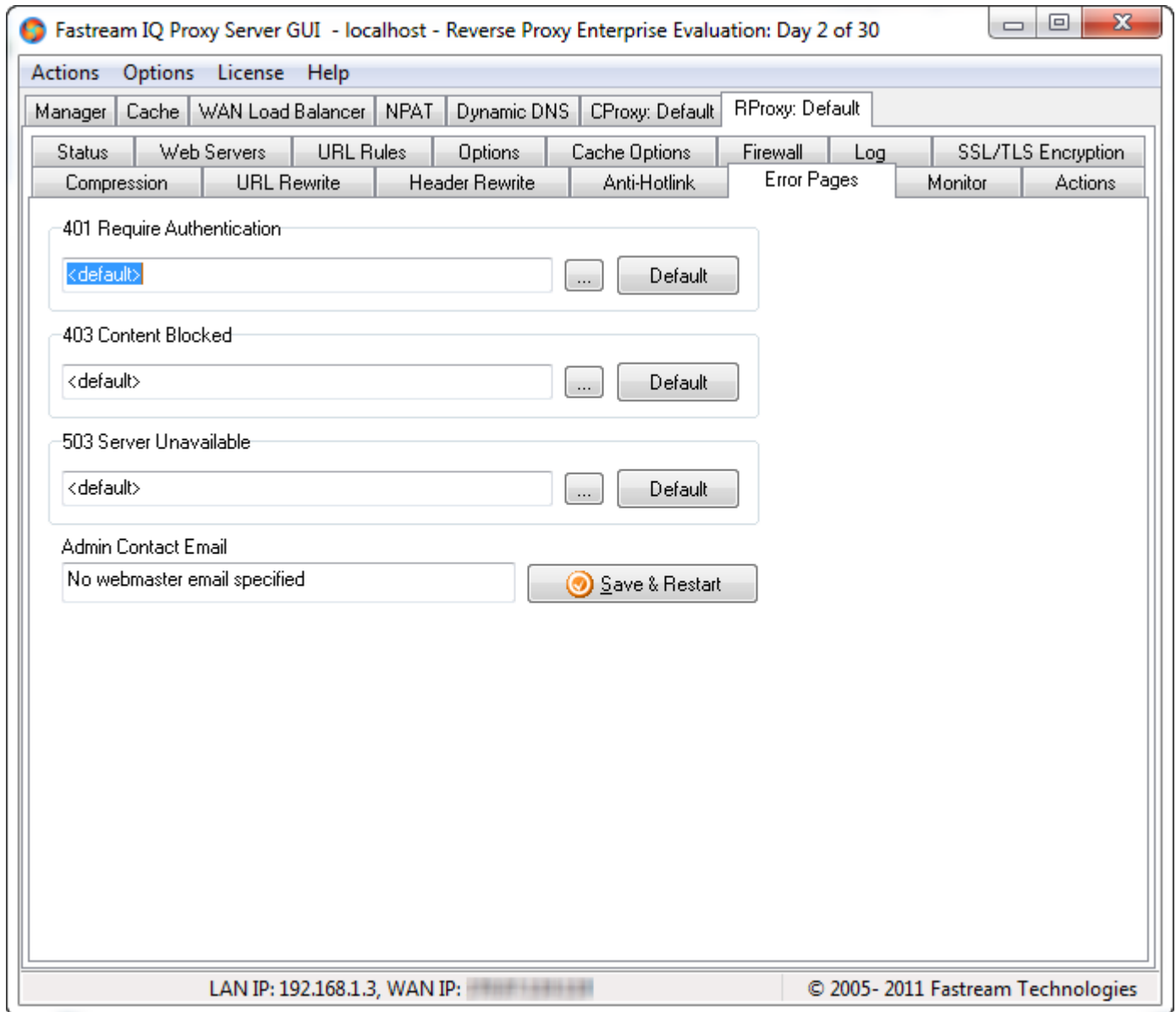
5.4.9 Compression

In the **Compression** tab, files are categorized with respect to their MIME types for GZip compression levels. GZip is the most widely accepted compression format on the Web and is supported by all browsers. The compression is not on-the-fly, which means that the object is buffered, requiring a maximum file-size-to-be-compressed limit set to 2MB by default.



5.4.10 Error Pages

The **Error Pages** tab is used for customizing HTML error pages. In this way you can choose to design custom error pages that match your web design.



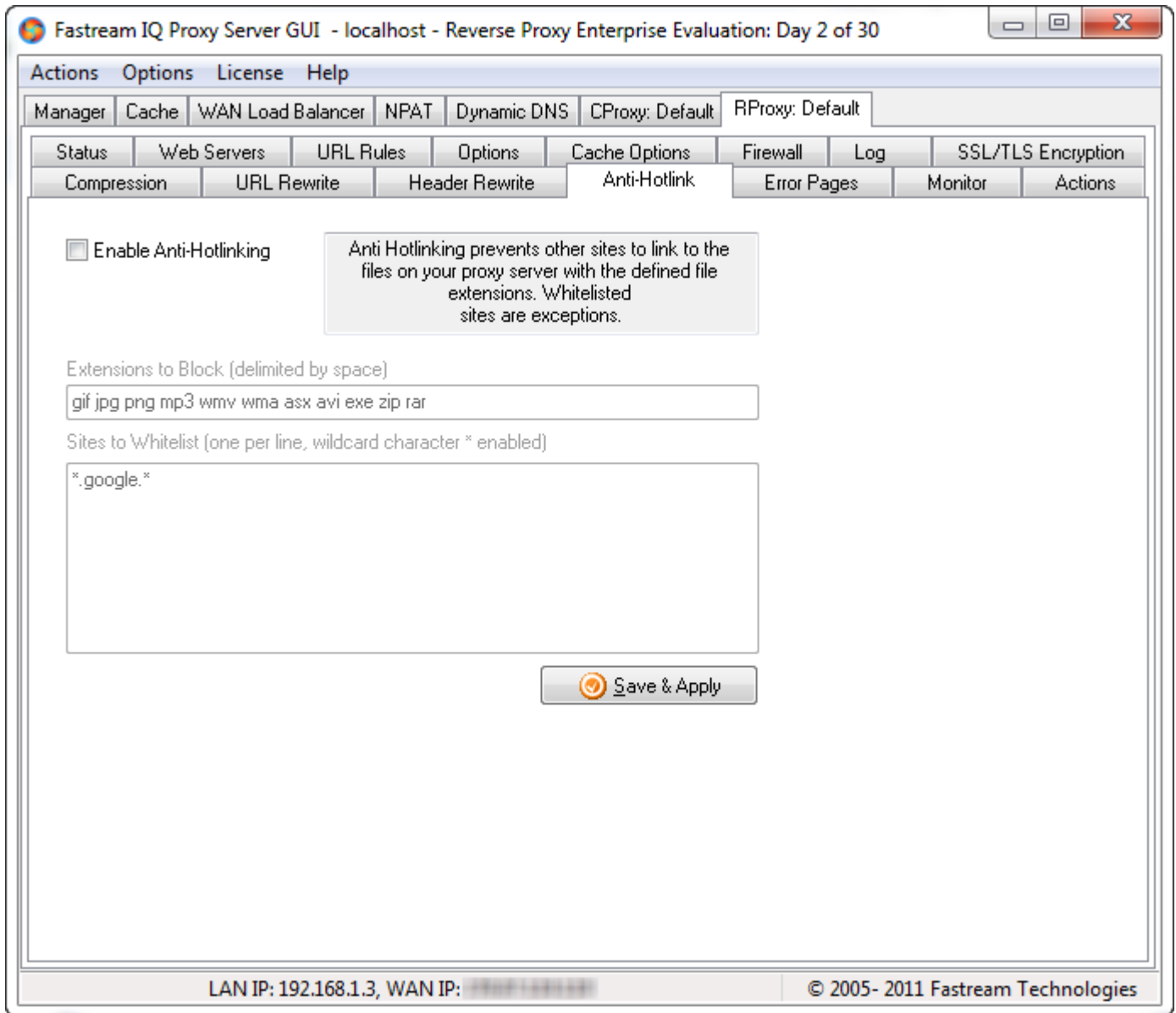
The following HTML error situations can be customized:

- 401 Error – Require Authentication
- 403 Error – Content Blocked
- 404 Error – Target Server Not Found

Use the Browse (...) button to select the desired HTML error page file. After setting one or more alternative error page, click **Save & Restart**.

5.4.11 Anti Hot-Link

The **Anti Hot-Link** tab enables you to block other web sites linking to your defined file extensions such as images, sound, and other multimedia. This way, only clients who access your web site by first visiting an HTML page can see the actual content, saving you bandwidth. When you enable this feature, you also need to check that if the defined default extensions fit your needs and, if not, add/remove them using a space delimiter. Also, you can have a whitelist of domains to enable content access regardless of the extensions rule. To enable a domain, simply enter in the format of *www.xyz.com* (one per line). Do not enter the protocol (*http://*) or port.



5.4.12 URL Rewrite

The **URL Rewrite** tab provides a powerful URL-rewrite with regular expressions feature for translating search engine and human-friendly requests such as:

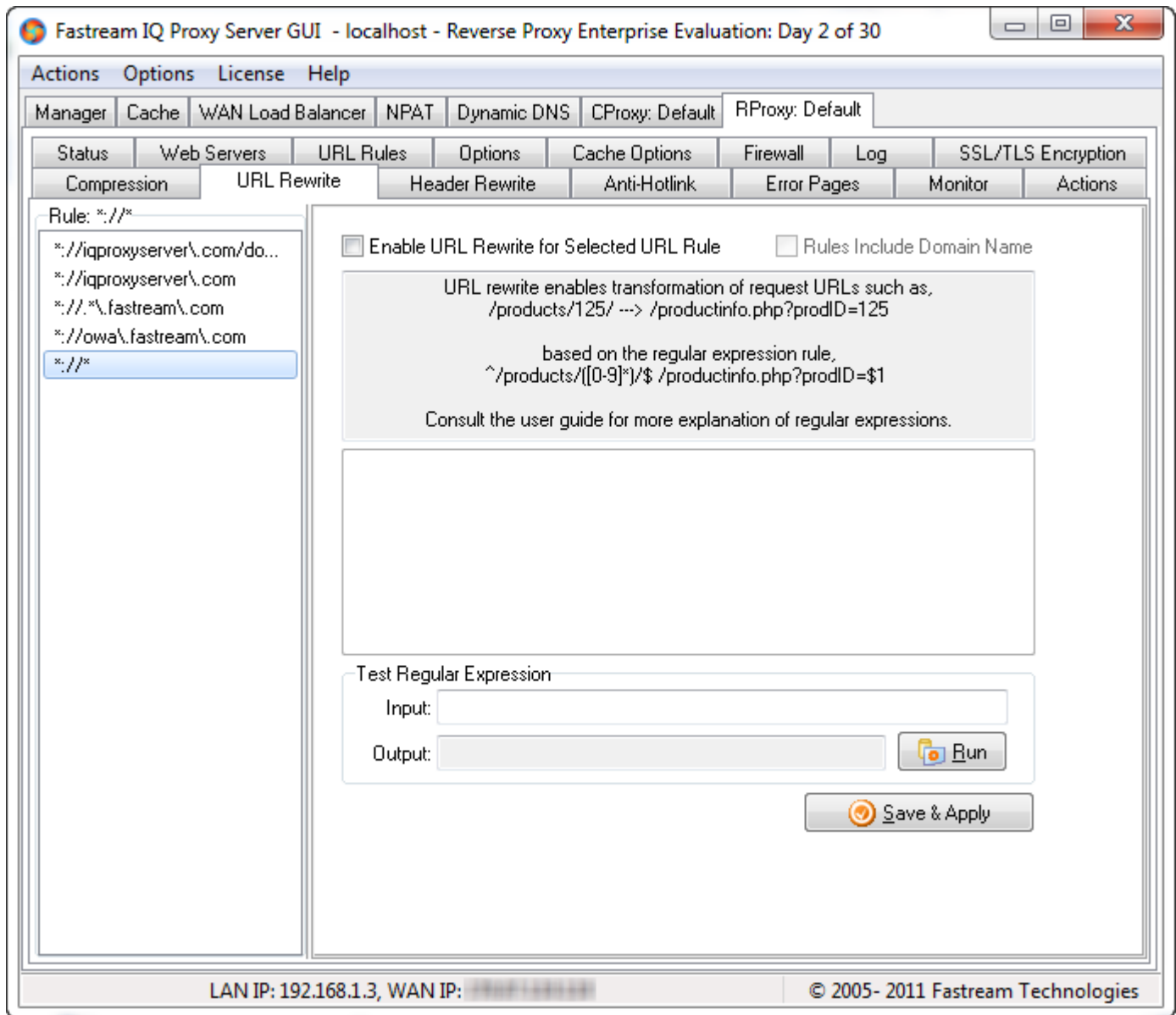
/products/125/

To a URL your web server understands such as:

/productinfo.php?prodID=125

For this particular translation, you would have to write the following regular expression rule:

^/products/([0-9]*)/\$ /productinfo.php?prodID=\$1 [nocase]



For a detailed explanation of regular expressions, please visit the following web pages:

<http://www.regular-expressions.info/>

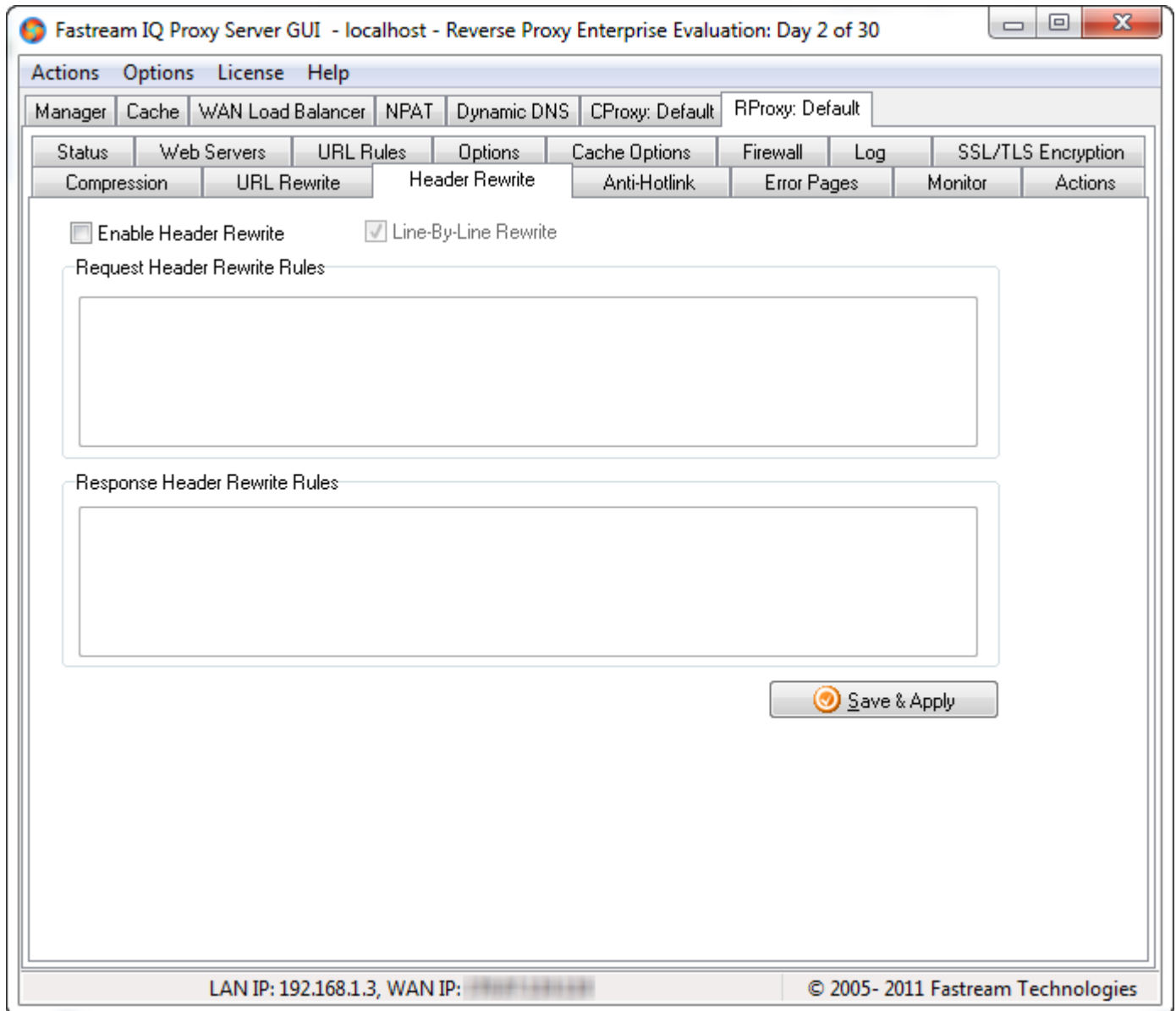
http://en.wikipedia.org/wiki/Regular_expression

<http://www.opengroup.org/onlinepubs/007908799/xbd/re.html>

<http://www.pcre.org/> (the library we use for regular expressions)

5.4.13 Header Rewrite

The **Header Rewrite** tab provides a feature for transforming request and/or response header lines one-by-one against defined regular expression rules. Refer to the URL Rewrite section above for links to regular expressions resources.



This feature transforms request and/or response header lines one-by-one against the regular expression rules defined. An example of a response header rewrite rule is:

"^Server: .*\$" "Server: YOURCOMPANY"

This response header rewrite rule gets the response header line such as,

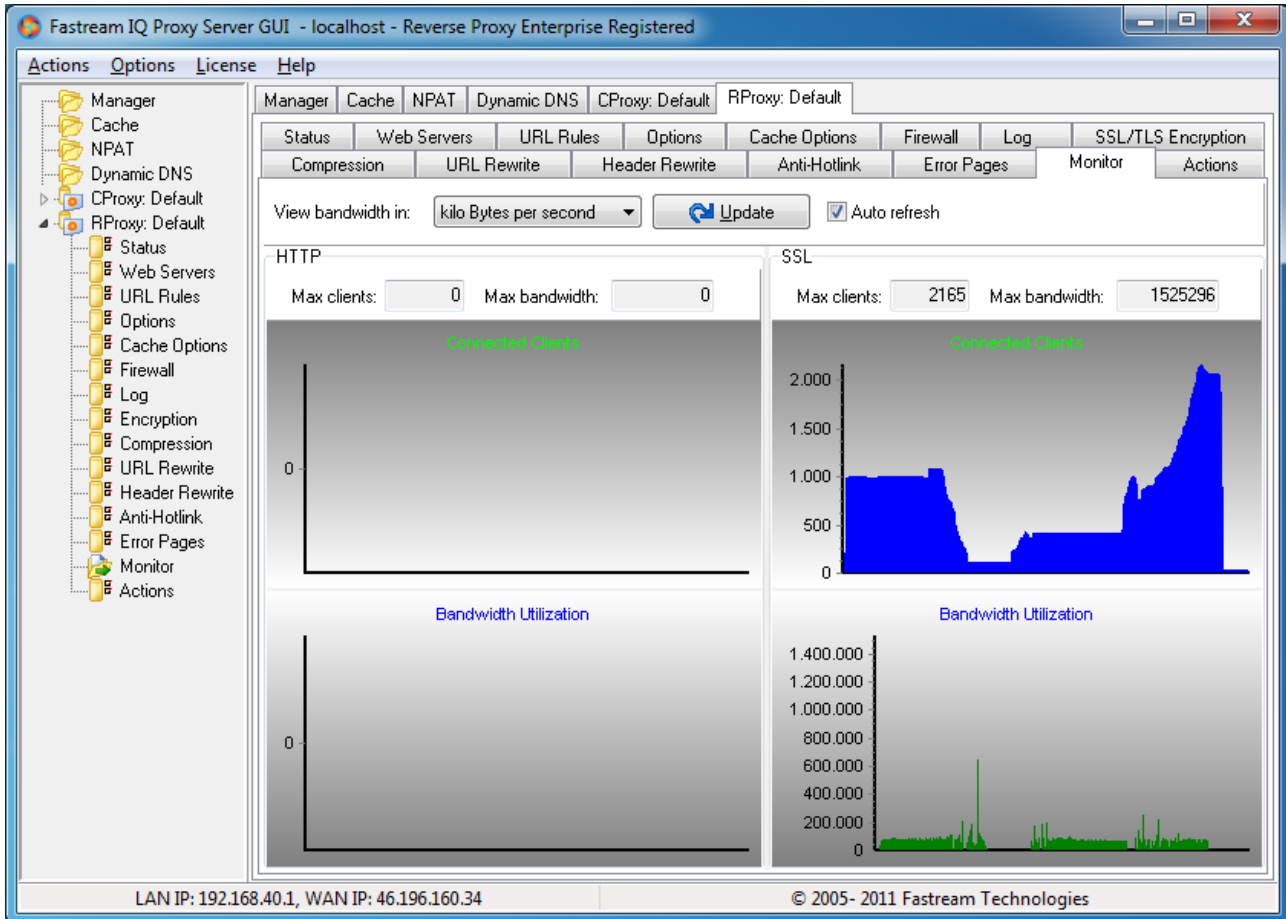
Server: Apache or **Server: Fastream IQ Proxy Server** and translates it to:

Server: YOURCOMPANY

Refer to the "URL Rewrite" section for links to regular expressions resources.

5.4.14 Monitor

The **Monitor** tab provides a graphical representation of existing HTTP and SSL traffic on your reverse proxy server. Options for the graphical monitor include: viewing the bandwidth in kilobytes/second or kilobits/second, manually refreshing the graph using the **Update** button, and setting an automatic update every three seconds.



5.4.15 Actions

The **Actions** tab provides a real-time listing of HTTP/SSL actions for your reverse proxy server. Options for this tab include: manually or automatically refreshing the actions listing and forcing the resolution of IP addresses when using country restrictions. For information on defining country restrictions, refer to the "URL Rules" section.

5.5 Configuring a Content Proxy Listener

For each content proxy you can, besides controlling the running status, authentication, TCP/IP connection settings, access filters, log files, compression of certain file types as well as SSL encryption settings, and error pages. These items are described in the next paragraphs.

5.5.1 Status

The **Status** tab enables you to start, stop, and restart the content proxy. The tab sheet displays the number of connected users and the transferred data (DL = download, UL = upload) size since the last run of the content proxy. You can also remove a content proxy here.

5.5.2 Authentication

The **Authentication** tab enables you to manage the authentication of the users using any of the following authentication types:

Basic Authentication

In HTTP/1.0/1.1 basic authentication, the username and password are transmitted in the request Authorization header as Base64Encoded and no encryption or protection at all. This mode is supplied because not all clients support the other modes.

Digest Authentication

This is a HTTP/1.1-only mode which is secure due to the fact that the password is not transmitted in cleartext but in hashed form. This means that wiretappers cannot read the password or store it for future reuse. However, notice that in all authentication methods, the data payload transmitted is still cleartext. You need to use SSL/TLS for encrypting the entire channel. This is the most secure authentication scheme that IQ Proxy Server supports.

Basic or Digest Authentication

Both Basic and Digest Authentication schemes are supported and the client chooses which to use. If the client supports digest, according to RFC2617, it should select that authentication scheme as that is more secure.

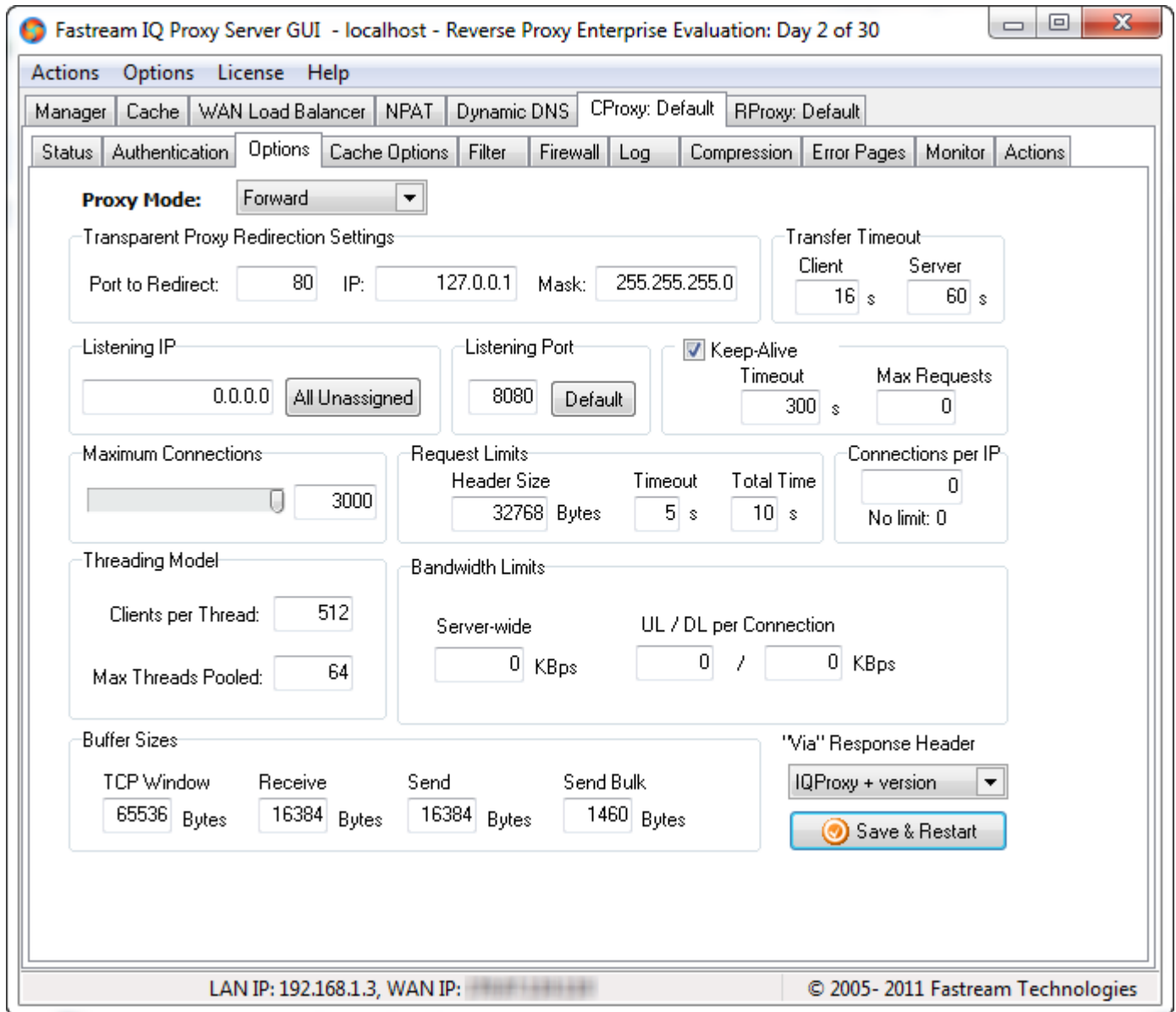
NTLM Authentication

NTLM is the proprietary authentication method of Microsoft Windows® for local and domain controller accounts. According to the default Windows security policies, the account must have non-empty password and the IQ Proxy Engine service should be assigned the right privileges/user accounts. You can change the Windows account IQ Proxy NT-service is using by selecting **Start, Control Panel, Administrative Tools, Services**, right-click the IQ Proxy service, **Properties**.



5.5.3 Options

The **Options** tab enables you to configure the content proxy service.



Listening IP:

This is the IP address of the server machine on which the content proxy service is running. Servers may be run on machines having several IPs that are obtained by several devices. Set the Listening IP to *0.0.0.0* to listen on all IPs.

Listening Port:

This is the TCP port on which the content proxy service is listening. This port is *8080* by default.

Maximum connections:

This is the maximum number of connections allowed. This value is *1000* by default.

Keep-Alive:

This **timeout** value is the idle time period (in seconds) in which the each client connection is kept active. By default in HTTP/1.0, a new connection is opened for each request, however, if keep-alive is supported by the client and enabled on the reverse proxy; the same connection can be used for consecutive requests.

The **Maximum Requests** value is another limiting factor for the keep-alive setting. Unless it is zero, this is the limit for the number of requests to be served on the same connection.

Clients per Thread:

This is the maximum number of client connections per process thread.

Max Threads Pooled:

This is the time an unresponsive server is given to resurrect itself. After this period, the unresponsive server will be rechecked. This is a per-server setting, in seconds.

This is the number of clients allowed to be supported for each thread created. Each thread can run on a maximum of one processor core and IQ Proxy Server automatically launches and load-balances among one thread per each core present on hardware.

This is the number of threads that is pooled in the operating system. Note that Windows® does not support more than 2000 threads at a time per process so setting this number above 2000 is not recommended.

Extensions Excluded from Cache:

Here you can specify the document extensions of files that are not going to be kept in the cache.

Request Timeout:

Here you can specify the timeout value, in seconds, before the connection is aborted between two request header upstream packets.

Request Header Size Limit:

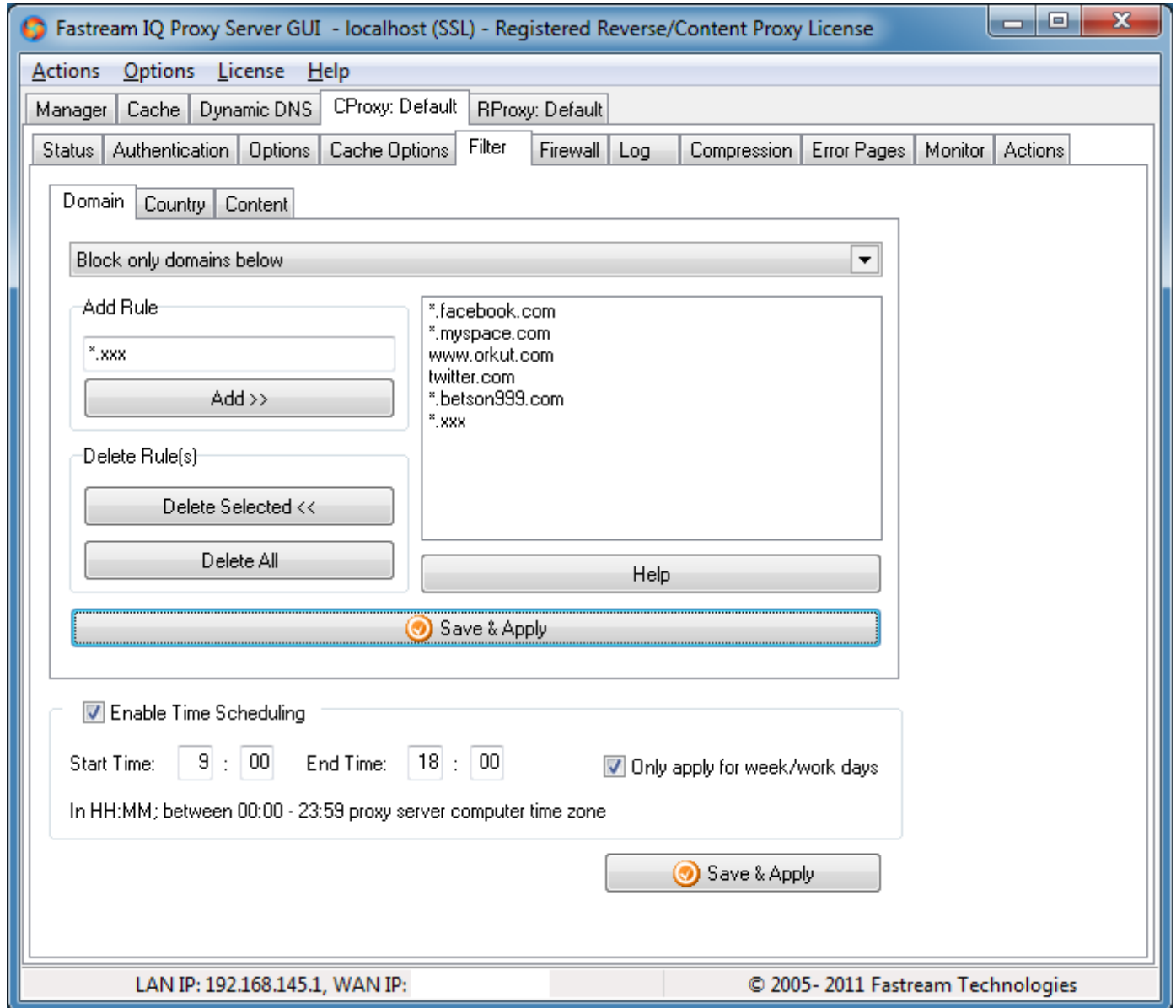
Here you can specify the maximum HTTP header size, in bytes, for the connection.

5.5.4 Filter

The **Filter** tab enables you to filter based on domain, country, and content.

5.5.4.1 Domain

The **Domain** tab is similar to the IP filter but works with domain names instead of IP addresses. You can block or permit domains and sub-domains. You can block a single computer with its domain name or all computers within a domain.



Selecting type of filtering

First you choose the type of filtering by selecting either the **Block only domains below** or **Permit only domains below** option in the upper list box. You can stop domain filtering entirely by selecting **Disable domain filter**.

Adding domain filtering rules

In order to set domain filtering rules, you need to enter the domain names in the Add Rule list box. You can use wildcards when defining filtering rules, such as those shown below:

- mycomputer.hackerzone.com > Blocks/Permits only this domain name
- *.hackerzone.com => Blocks / Permits all connections from domain
- comp*.hackerzone.com => Blocks / Permits comp1.hackerzone.com, comp2.hackerzone.com, compx.hackerzone.com, etc.

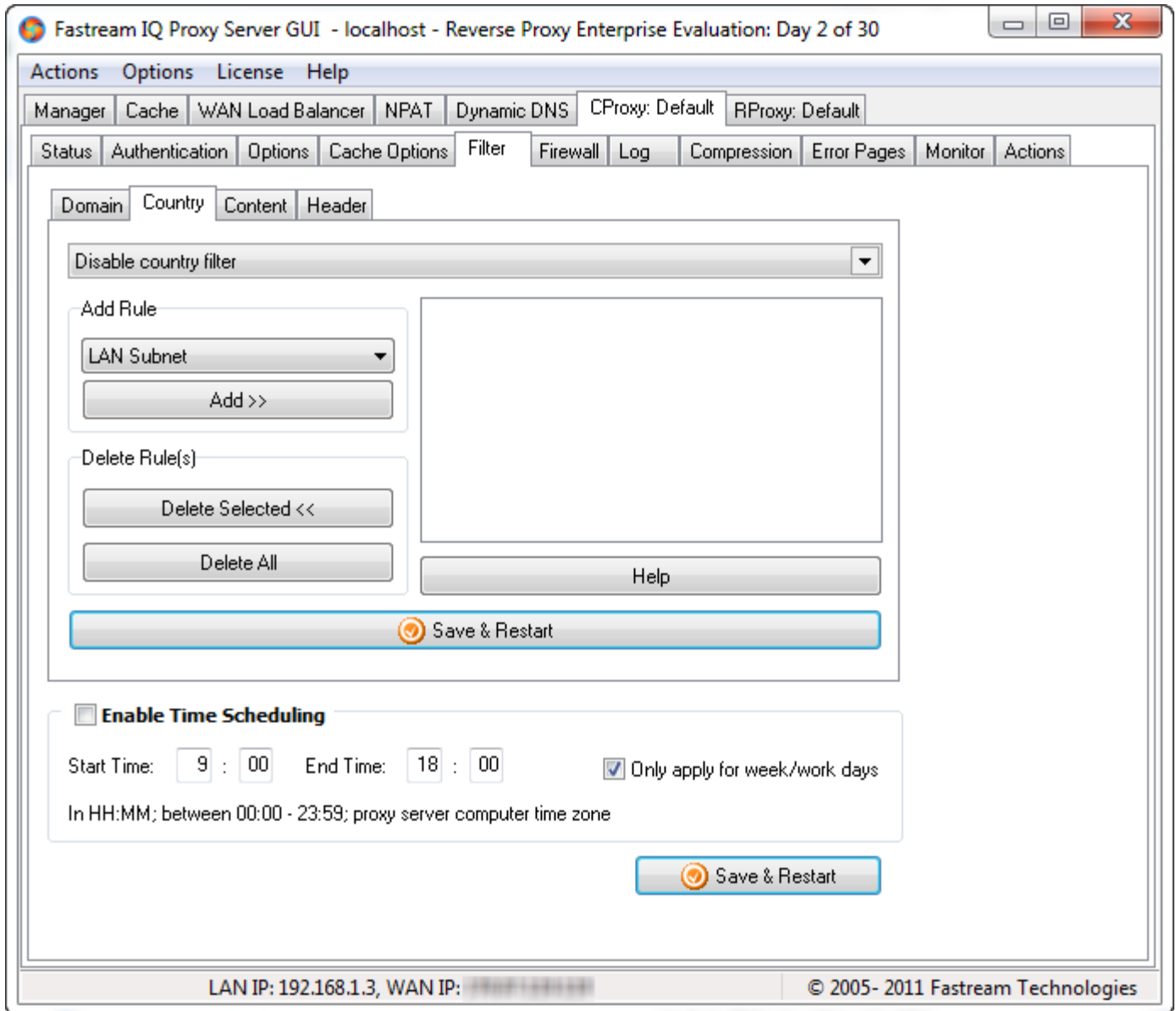
Deleting domain filtering rules

You can delete specific or all defined domain rules by using the **Delete Selected** or **Delete All** button, respectively. Be sure to select the correct domain rule before clicking **Delete Selected**.

Click **Save & Apply** to activate new or updated settings.

5.5.4.2 Country

The IQ Content Proxy is the only content proxy tool with built-in country based filtering support. You can allow or deny connections from the countries you select. The IP addresses from the selected countries will be detected by the content proxy and will be permitted or blocked according to the rules you define.



Selecting type of filtering

Choose the type of filtering by selecting either the **Block only countries below** or **Permit only countries below** option in the upper list box. You can stop country filtering entirely by selecting the **Disable country filter** option.

Adding country filtering rules

In order to set domain filtering rules, you need to enter the domain names in the Add Rule list box. Note that you can use wildcards in your filtering rules.

Deleting country filtering rules

You can delete specific or all defined country rules by using the **Delete Selected** or **Delete All** button, respectively. Be sure the select the correct country rule before clicking **Delete Selected**.

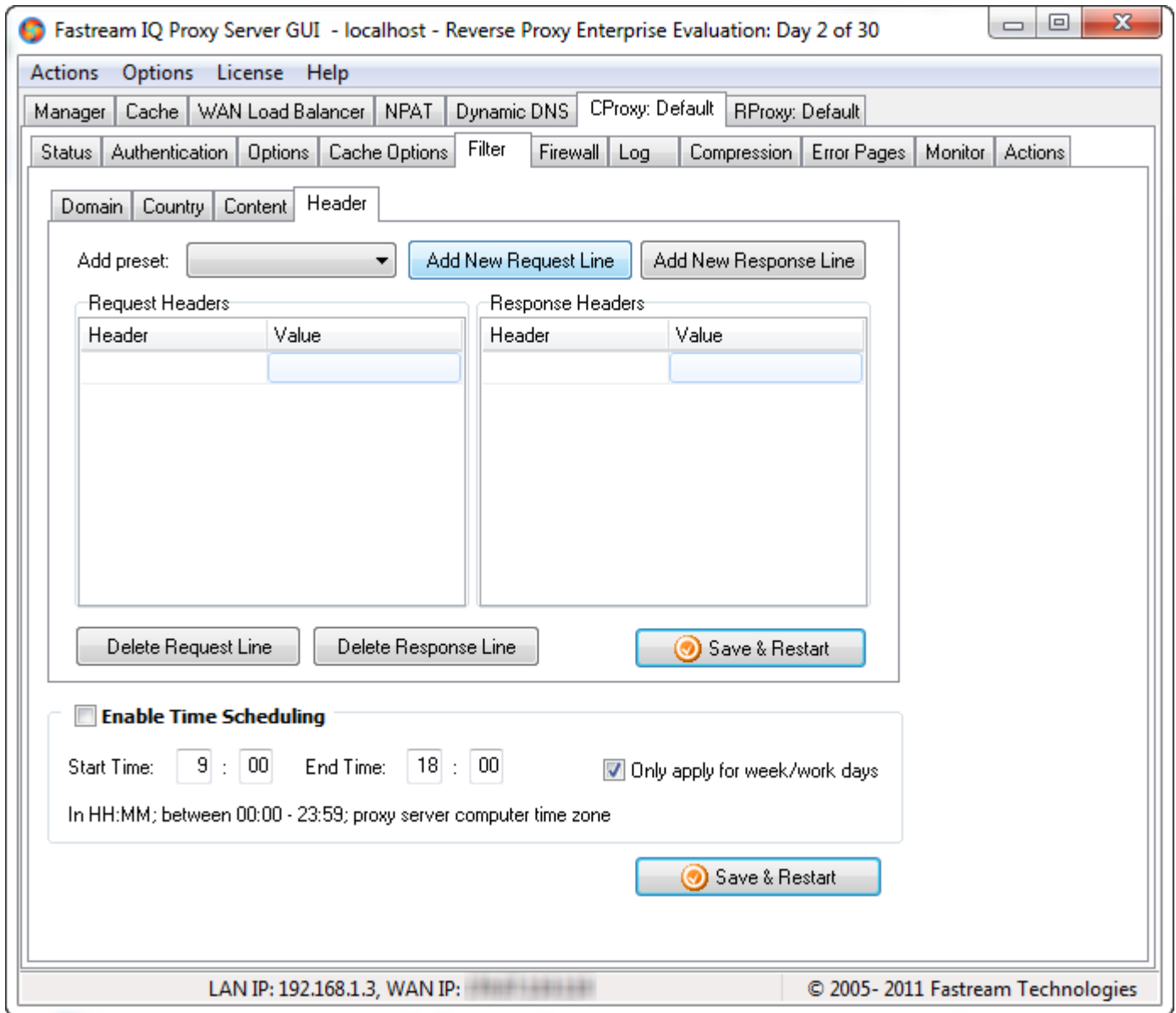
Click **Save & Apply** to activate new or updated settings.

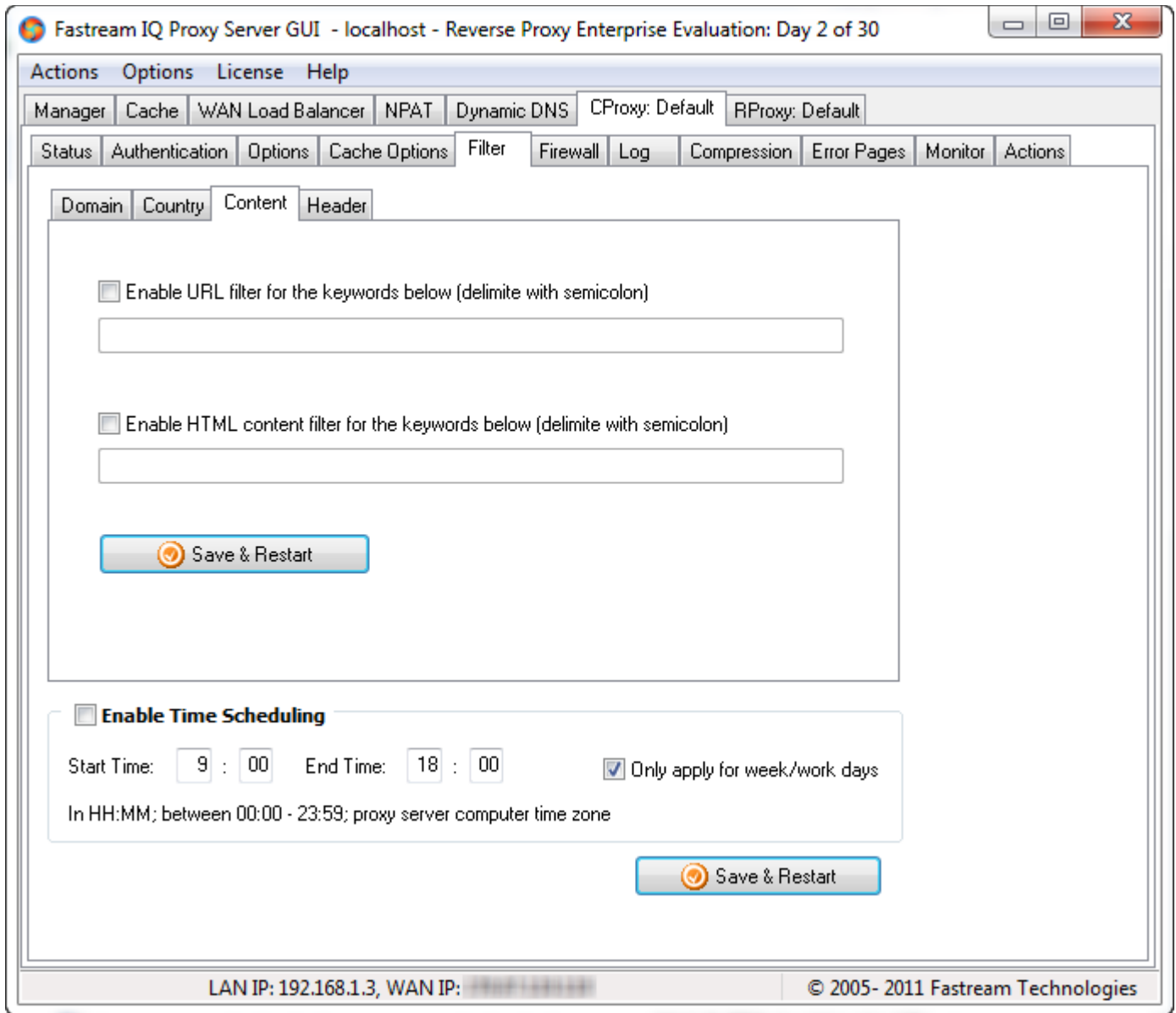
5.5.4.3 Content

The **Content** tab is similar to the domain filter but works with content instead of domain names. You can block or permit content in URL or HTML. You can block a site based on the content in its URL or in the HTML pages themselves.

5.5.4.4 Header

The **Header** tab is similar to the domain filter but works with HTTP request/response headers instead of domain names. You can block or permit content in request or response headers. This filtering method is useful for blocking Instant Messaging and peer-to-peer programs. You should use this in **transparent proxy** mode from Options so that it would block traffic of programs that are not configured for forward proxy.





Selecting type of filtering

First select the type of filtering by selecting the **Enable URL filter for the keywords below** and/or **Enable HTML content filter for the keywords below** option.

Click **Save & Apply** to activate new or updated settings.

5.5.5 Firewall

The **Firewall** tab enables you to apply filtering rules. Using the filtering rules, specific remote clients can either be permitted or blocked by the content proxy. By default the filtering is specified using IP numbers, however, it is also possible to filter using domain names or even countries.

5.5.5.1 DDoS

DDoS is an acronym for a **D**istributed **D**enial **o**f **S**ervice attack. In these attacks, given that there are many malicious clients attacking from many IP addresses, it is usually difficult to deal with them.

IQ Proxy Server offers a feature to cope with this type of malicious act. This feature is not enabled by default because some customers prefer to stress test the proxy and stress testing corresponds to the same footprint as denial of service attacks.

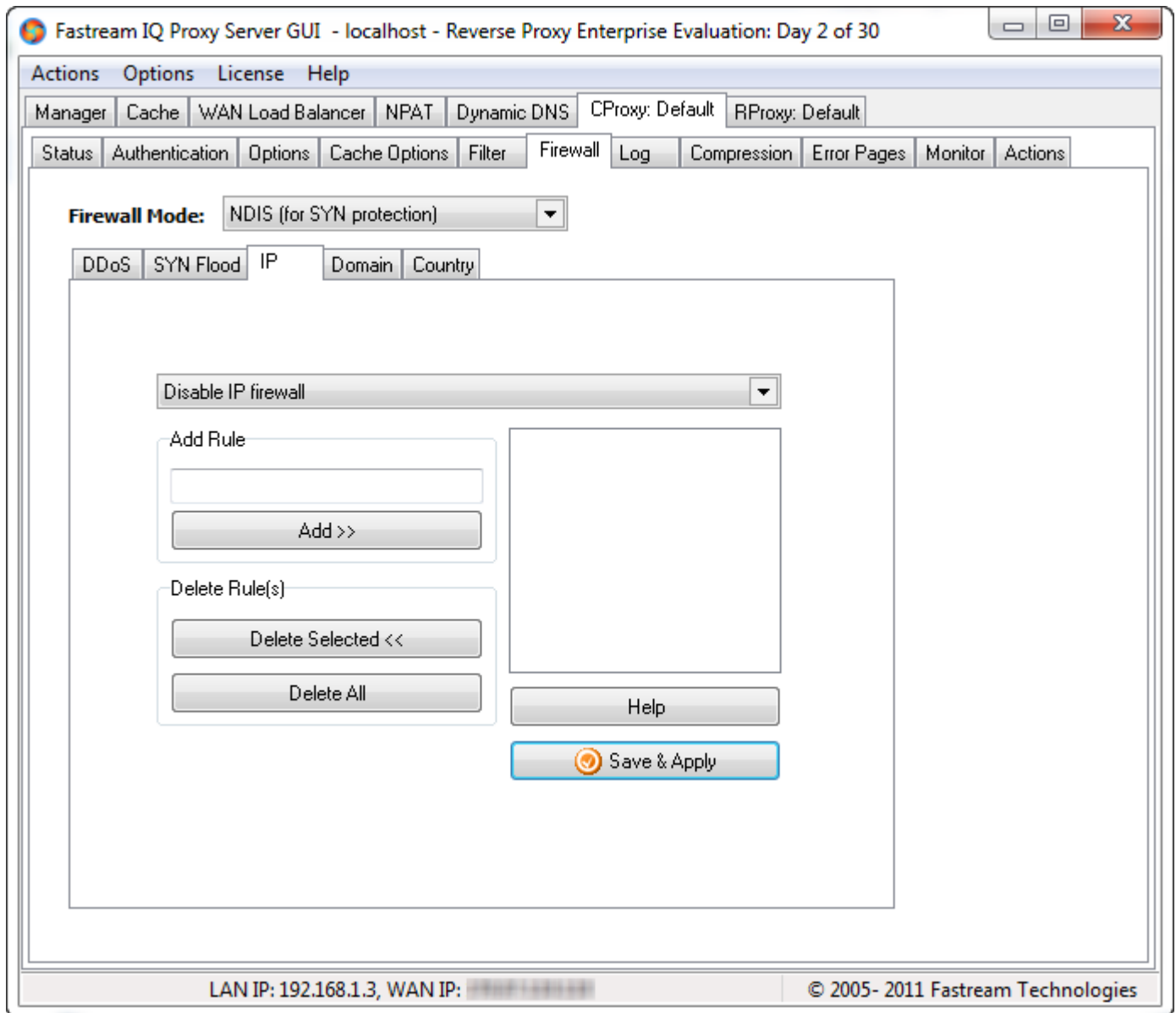
There are distinct settings for each client IP's number of accesses to each specific 2xx-3xx URL, any 404 page and any 4xx page other than 404 with different reset periods (in seconds). There is also a definable period for clearing the client IP database (in minutes). Therefore, if an attacker writes a tool that uses randomly created URLs to exhaust the proxy server, it is easily caught with the 404 limit and disconnected before the header is read. If it passes that stage and, for example, requests the home page continuously, the header is received but there is no response.

5.5.5.2 SYN

The SYN firewall is built to limit the timeout of half-sockets when there are too many of them pending which indicates the attack level. Normally, Windows sends out three SYN-ACKs per half open socket if the first two are un-ACKed. In our firewall, this is reduced to 2 and 1 at higher attack levels. For each attack level, there are ten levels which should be sufficient for all cases. IQProxy SYN firewall also limits the timeout value for each SYN-ACK response.

5.5.5.3 IP

You can use the **IP** tab to restrict access to your Content Proxy by specifying IP addresses to block. In order to set IP rules, you need to enter the IP addresses in the dotted form, such as: *123.123.123.123*.



Selecting type of filtering

Choose the type of filtering by selecting either the **Block only IPs below** or **Permit only IPs below** option in the upper list box.

Adding IP filtering rules

In order to set IP filtering rules, you need to enter the IP address in the Add Rule list box.

Note that you can specify a range of IP addresses at once. The filtering type you choose affects the following entries given:

123.123.123.123 > Blocks/Permits only this IP address

123.123.123.x > Blocks/Permits all IP addresses that start with

123.123.123.xxx > This has the same effect as the one above

123.123.1x3.123 => Blocks/Permits all IP addresses of the form 123.123.1[0...9]3.123

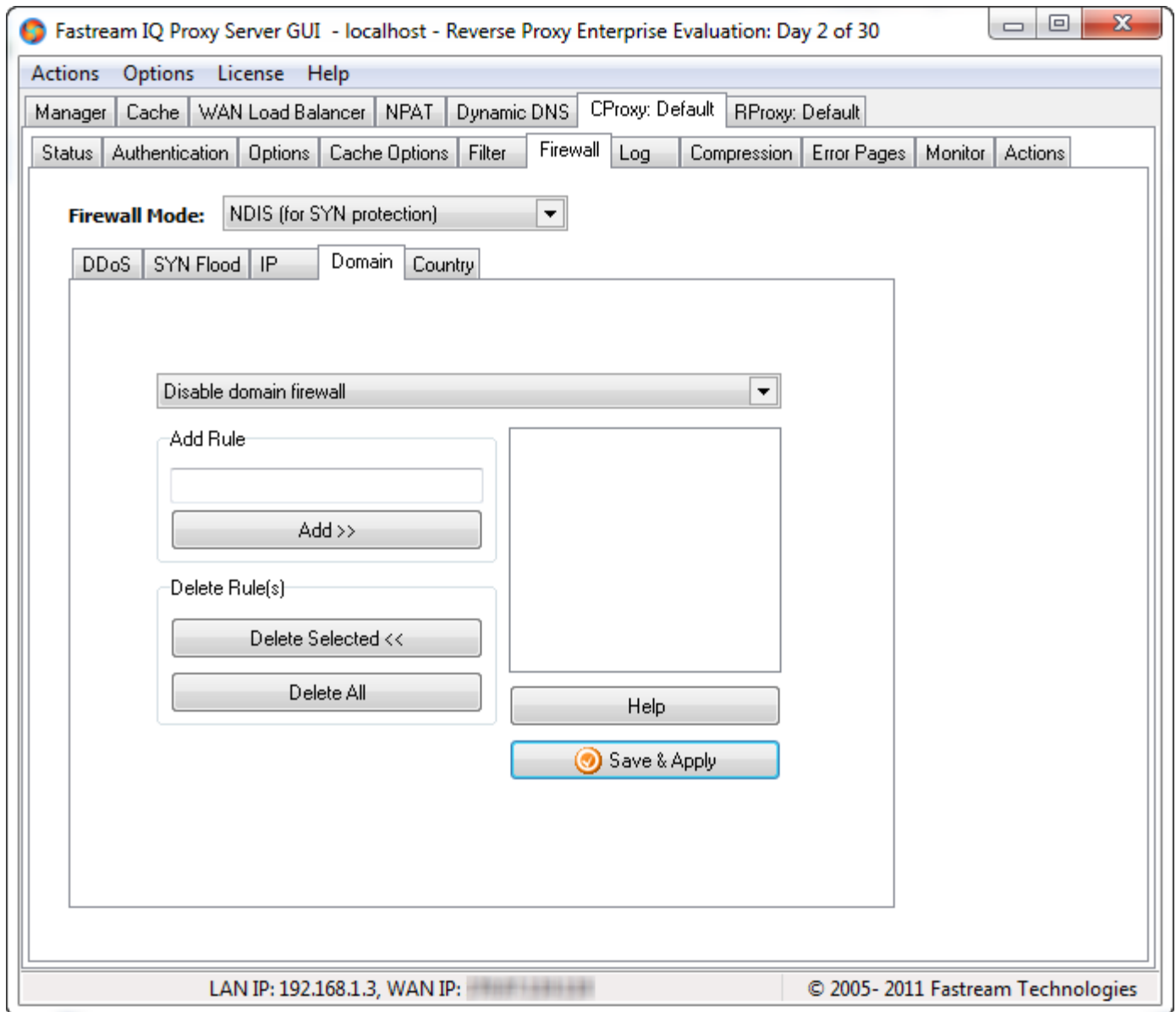
Deleting IP filtering rules

You can delete specific or all defined IP filtering rules by clicking the **Delete Selected** or **Delete All** button, respectively. Be sure to select the correct IP filtering rule before clicking **Delete Selected**.

Click **Save & Apply** to activate new or updated settings.

5.5.5.4 Domain

The **Domain** tab is similar to the IP filter, but works with domain names instead of IP addresses. You can block or permit domains and sub-domains. You can block a single computer with its domain name or all computers within a domain.



Selecting type of filtering

Choose the type of filtering by selecting either the **Block only domains below** or **Permit only domains below** option in the upper list box. You can stop domain filtering entirely by selecting the **Disable domain filter** option.

Adding domain filtering rules

In order to set domain filtering rules, you need to enter the domain names in the Add Rule list box. You can use wildcards, such as those used in the examples below:

- mycomputer.hackerzone.com > Blocks/Permits only this domain name
- *.hackerzone.com => Blocks / Permits all connections from domain
- comp*.hackerzone.com => Blocks / Permits comp1.hackerzone.com, comp2.hackerzone.com, compx.hackerzone.com, etc.

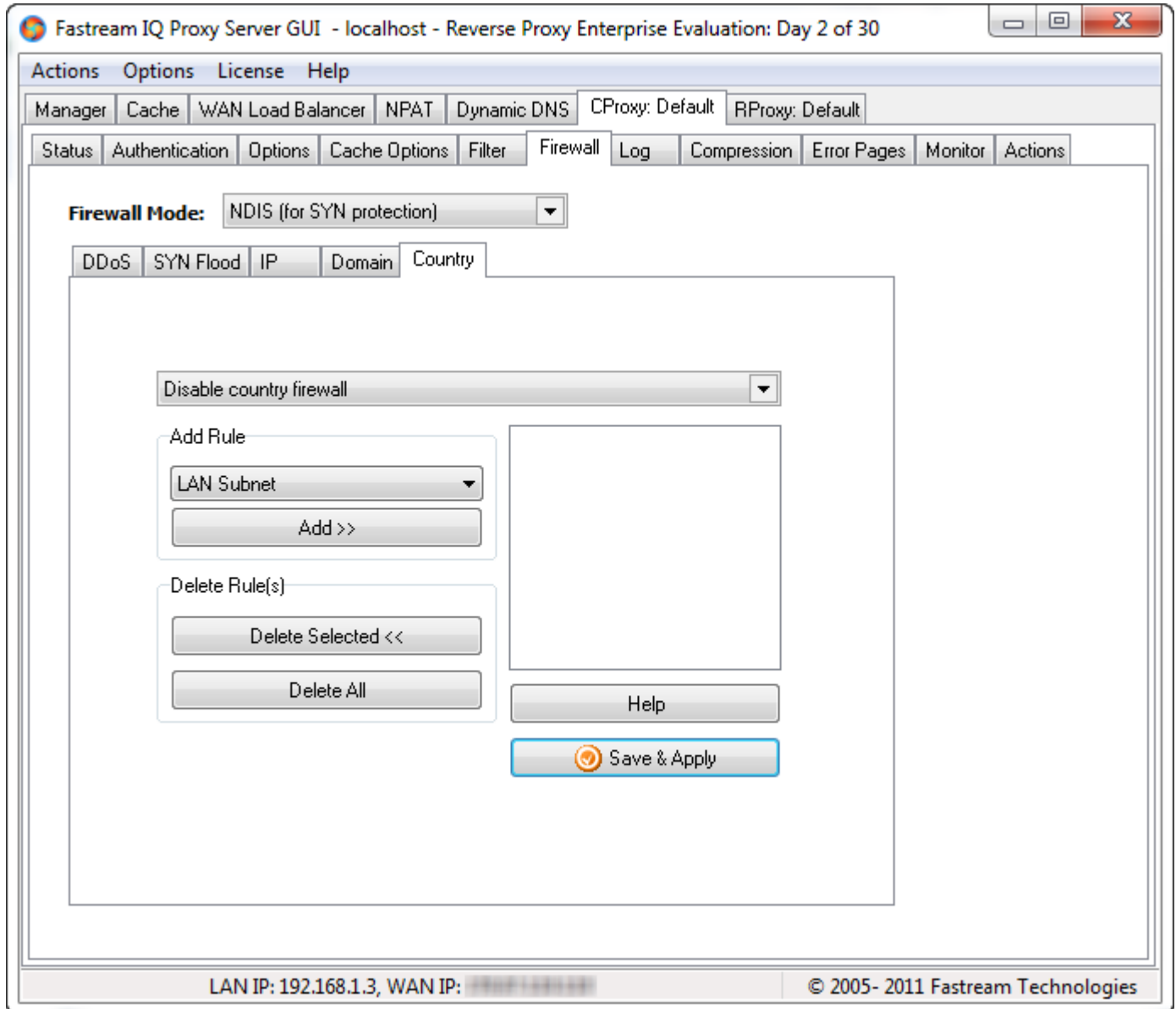
Deleting domain filtering rules

You can delete specific or all defined domain rules by clicking the **Delete Selected** or **Delete All** button, respectively. Be sure to select the correct domain rule before clicking **Delete Selected**.

Click **Save & Apply** to activate new or updated settings.

5.5.5.5 Country

IQ Content Proxy is the only content proxy tool with built-in country based filtering support. You can allow or deny connections from the countries you select. The IP addresses from the selected countries will be detected by the content proxy and will be permitted or blocked according to the rules you define.



Selecting type of filtering

Choose the type of filtering by selecting either the **Block only countries below** or **Permit only countries below** option in the upper list box. You can stop country filtering entirely by selecting the **Disable country filter** option.

Adding country filtering rules

In order to set domain filtering rules, you need to enter the domain names in the Add Rule list box. Note

that you can use wildcards in your filter definitions.

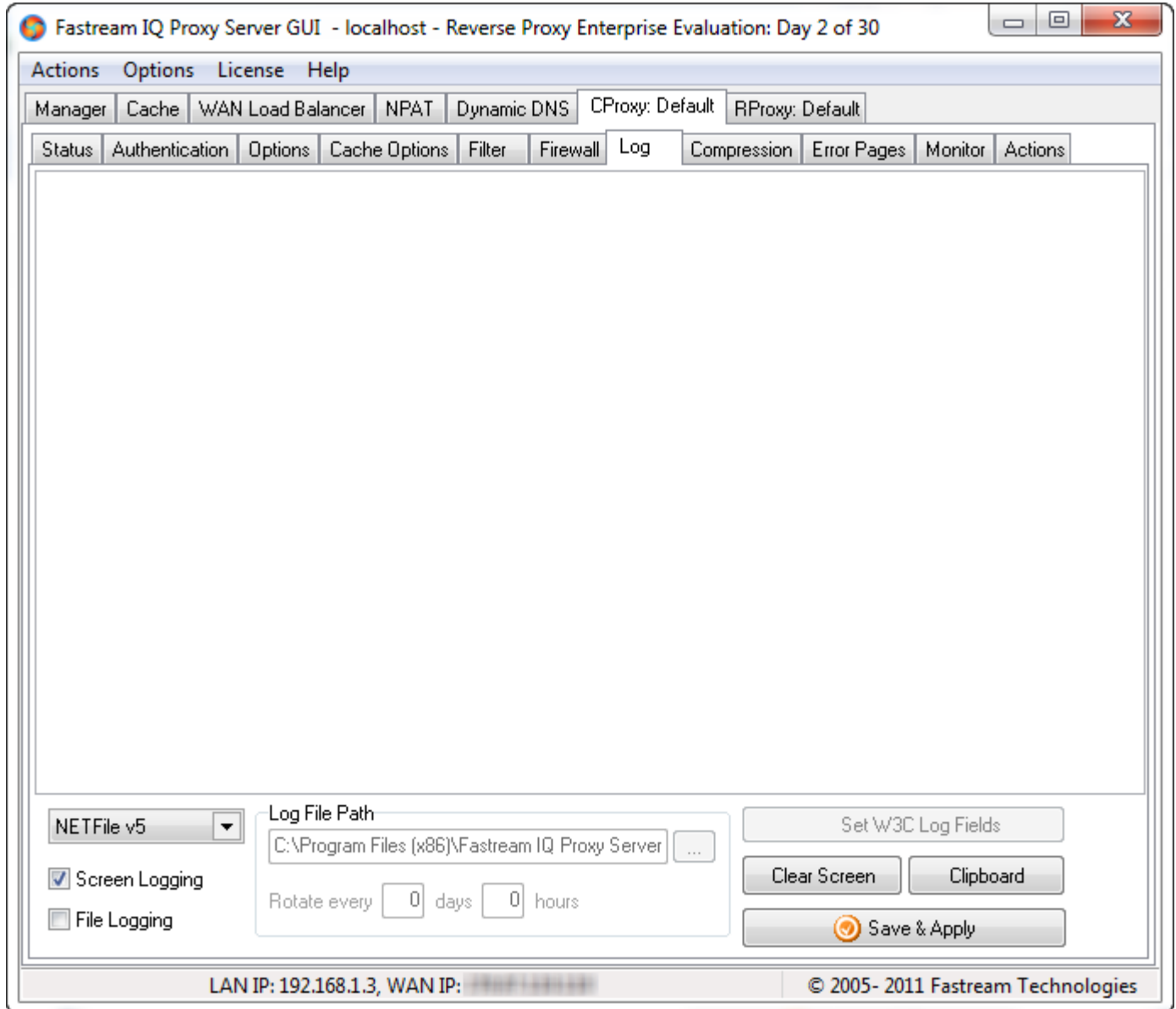
Deleting country filtering rules

You can delete specific or all defined country rules by clicking either the **Delete Selected** or **Delete All** button, respectively. Be sure to select the correct country rule before clicking **Delete Selected**.

Click **Save & Apply** to activate new or updated settings.

5.5.6 Log

IQ Proxy Server can log the HTTP protocol commands passed between remote HTTP clients and the content proxy server engine. The content proxy keeps the logs in memory for a few seconds and then displays them so as to minimize the load and improve the performance of the content proxy server. This becomes more important as the user connection count increases.



The menu at the top of the **Log** tab enables you to arrange the log settings. Here you can choose the log format, enable/disable screen logs, copy logs to the clipboard to save them manually, or write the logs to a file you select.

The log settings can be applied to specific selected Request URLs. First select the desired URL, then make the changes in the log settings.

Click **Save & Apply** to activate new or updated settings.

Log formats

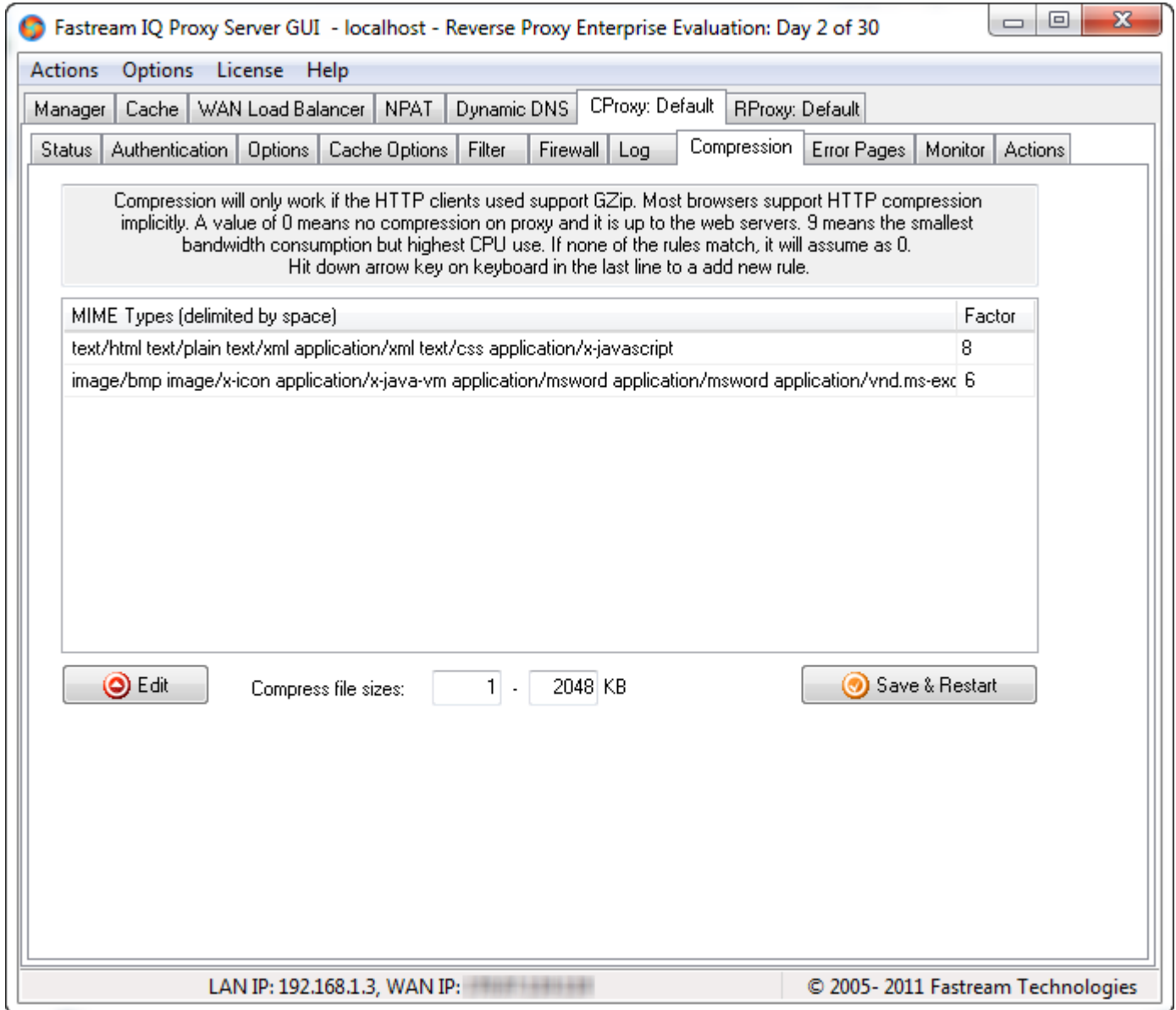
There are two log formats you can choose: (1) NET file log format, or (2) the W3C extended log file format.

NET file log format is used for recording basic requests.

The W3C extended log file format is a flexible format for recording HTTP requests, which is particularly suited for log analysis tools. ELF (W3C Extended Log Format) records more information than the common NET file log format. It contains a sequence of lines containing ASCII characters delimited by a new line. Lines that start with # are comment directives. The Fields directive indicates the HTTP request fields that are actually written in the log records that follow. You can use free tools such as *Gimli ELF* to analyze your logs if you choose this format.

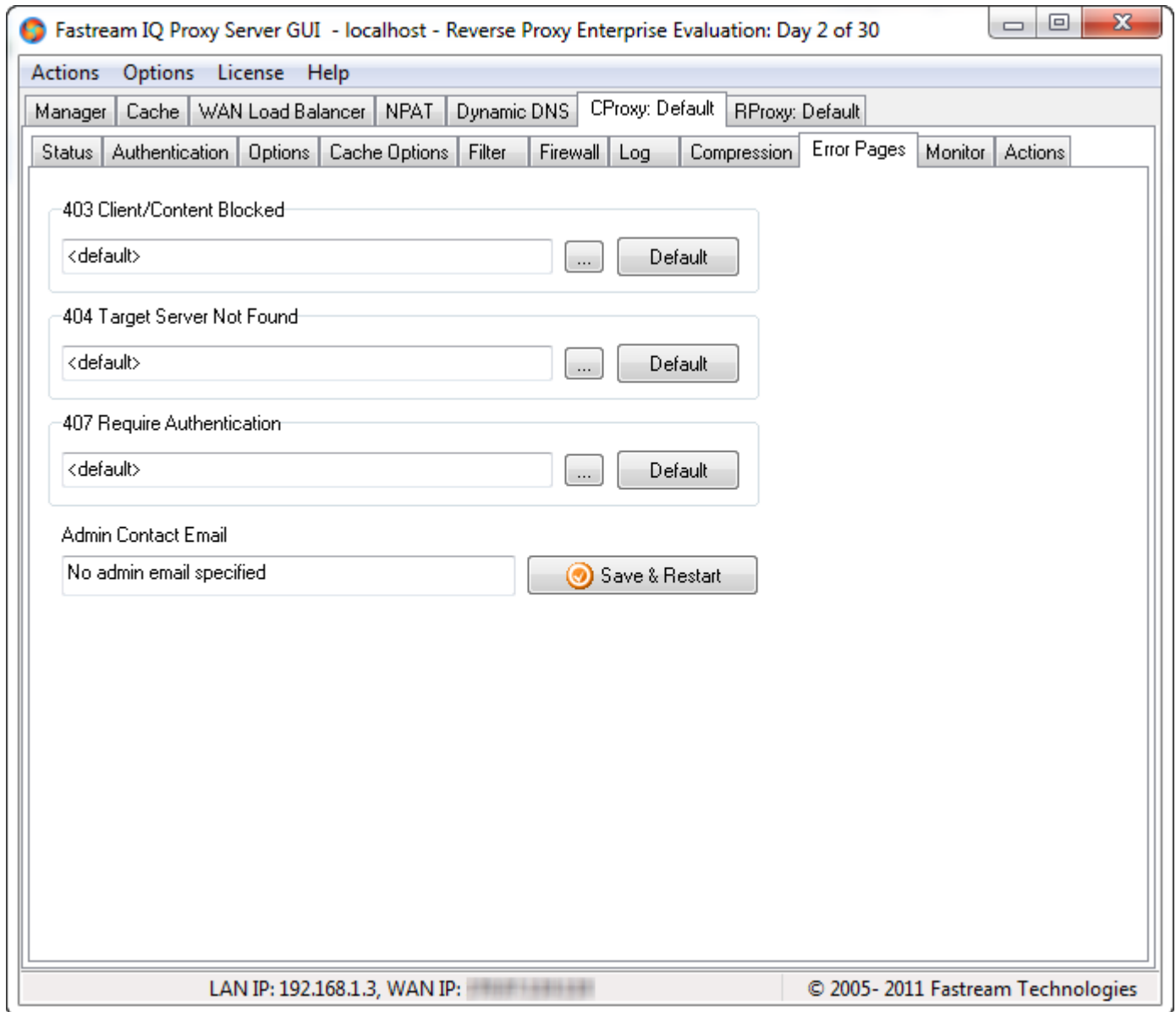
5.5.7 Compression

In the **Compression** tab, files are categorized with respect to their MIME types for GZip compression levels. GZip is the most widely accepted compression format on the Web and is supported by all browsers. The compression is not on-the-fly, which means that the entire object is buffered; therefore, a maximum file-size-to-be-compressed limit is set at 2MB by default.



5.5.8 Error Pages

The **Error Pages** tab enables you to provide custom HTML error pages. This allows you to design error pages that match your web design.



Using the Browse (...) button, you can browse to the desired HTML error page. After setting the alternative error pages, click **Save & Restart**.

6 NPAT

6.1 What is NAT

NAT (Network Address Translation or Network Address Translator) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its inside network addresses to one or more global outside IP addresses and maps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication

NAT is included as part of a router and is often part of a corporate firewall. Network administrators create a NAT table that does the global-to-local and local-to-global IP address mapping. NAT can also be used in conjunction with policy routing. NAT can be statically defined or it can be set up to dynamically translate from and to a pool of IP addresses.

NAT is described in general terms in RFC 1631, which discusses NAT's relationship to Classless Interdomain Routing (CIDR) as a way to reduce the IP address depletion problem. NAT reduces the need for a large amount of publicly known IP addresses by creating a separation between publicly known and privately known IP addresses. CIDR aggregates publicly known IP addresses into blocks so that fewer IP addresses are wasted. In the end, both extend the use of IPv4 IP addresses for a few more years before IPv6 is generally supported.

Source: <http://searchenterprisewan.techtarget.com/definition/Network-Address-Translation>

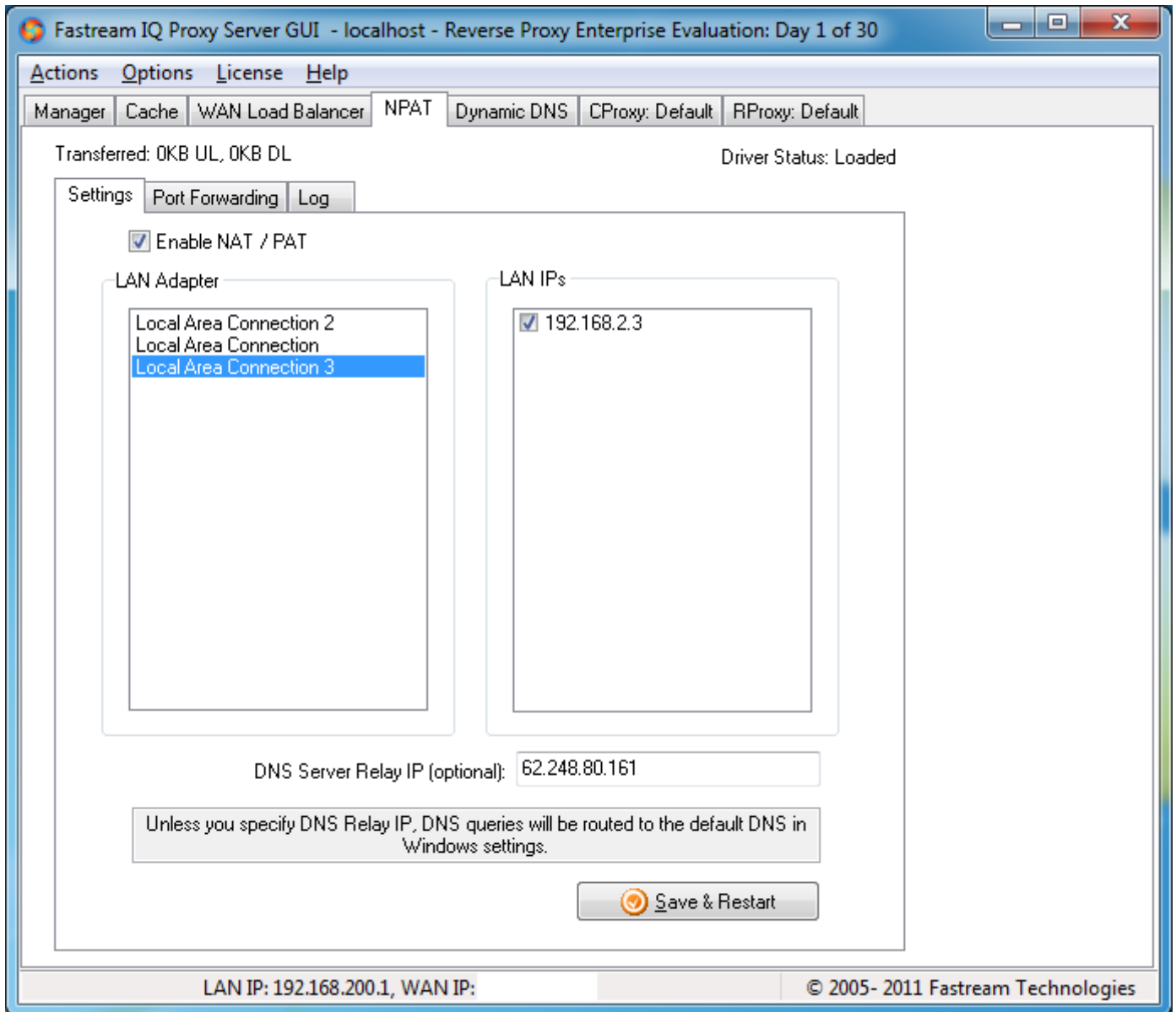
6.2 What is PAT

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

Most home networks use PAT. In such a scenario, the Internet Service Provider (ISP) assigns a single IP address to the home network's router. When Computer X logs on the Internet, the router assigns the client a port number, which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific packets to because each computer has a unique internal address. Port Address Translation is also called porting, port overloading, port-level multiplexed NAT and single address NAT.

Source: <http://searchnetworking.techtarget.com/definition/Port-Address-Translation-PAT>

6.3 IQ Proxy NAT



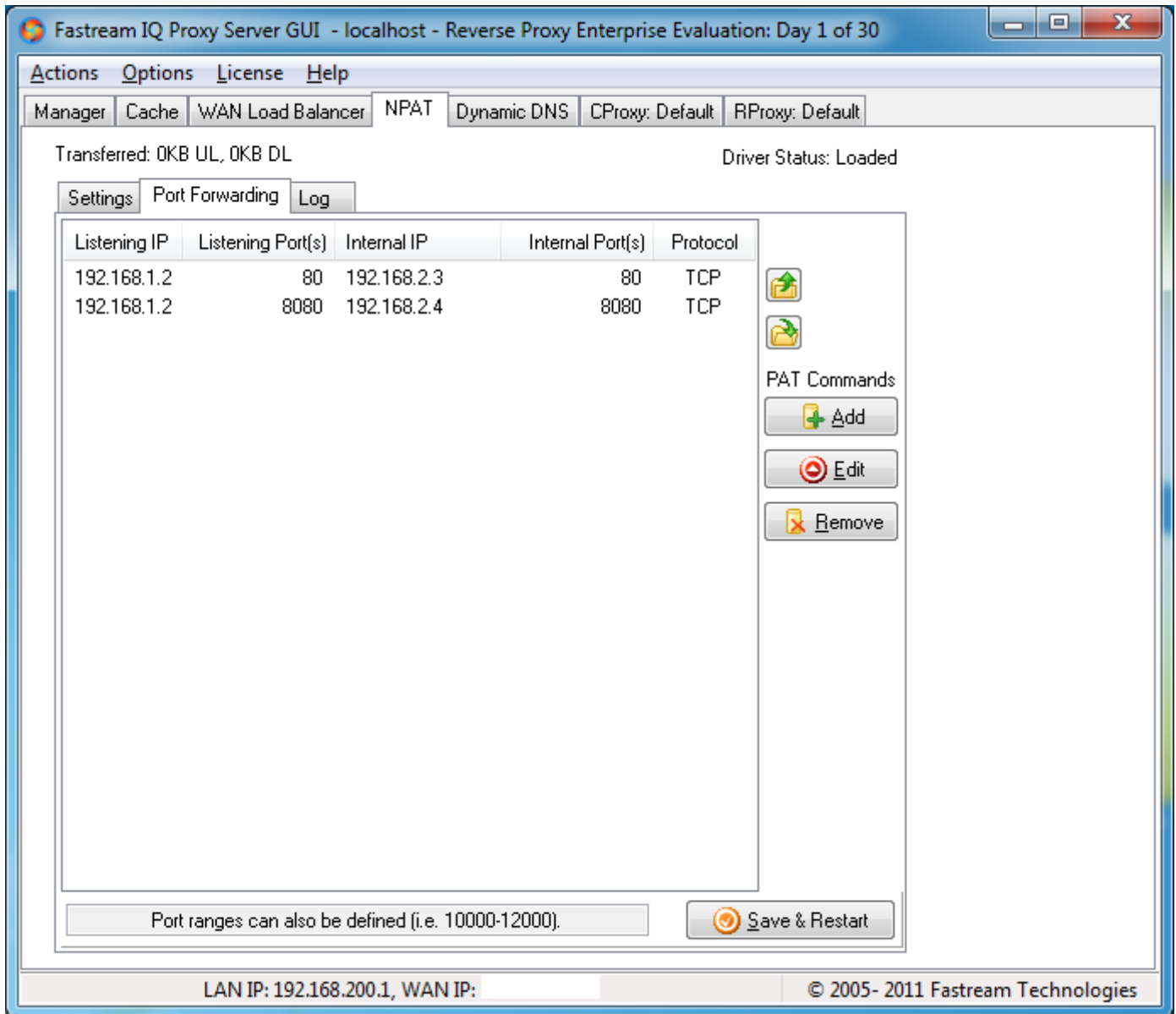
IQProxy supports IP/TCP/UDP/FTP/DNS/PPTP/ICMP in its kernel-mode driver for NATing at speeds higher than 1Gbps being achievable.

IQProxy NAT has five settings. You can have only one subnet NATed but you can have many listening IPs on the selected LAN adapter by using check boxes in the GUI. The IPs selected as LAN IPs are the ones you can set on your client computers as gateway IPs.

The WAN IP is the one that the NAT will translate to. V7.0+, you should define WAN IP from WAN LB tabsheet. However in order for Windows to route packets to IQNDIS driver, the LAN and WAN IP subnets must be different. For example you cannot have 192.168.1.2 as LAN IP and 192.168.1.3 as WAN IP. And of course you cannot have the same IP to do the both.

You can also specify the outbound DNS server IP for servers not-defined in Windows networking.

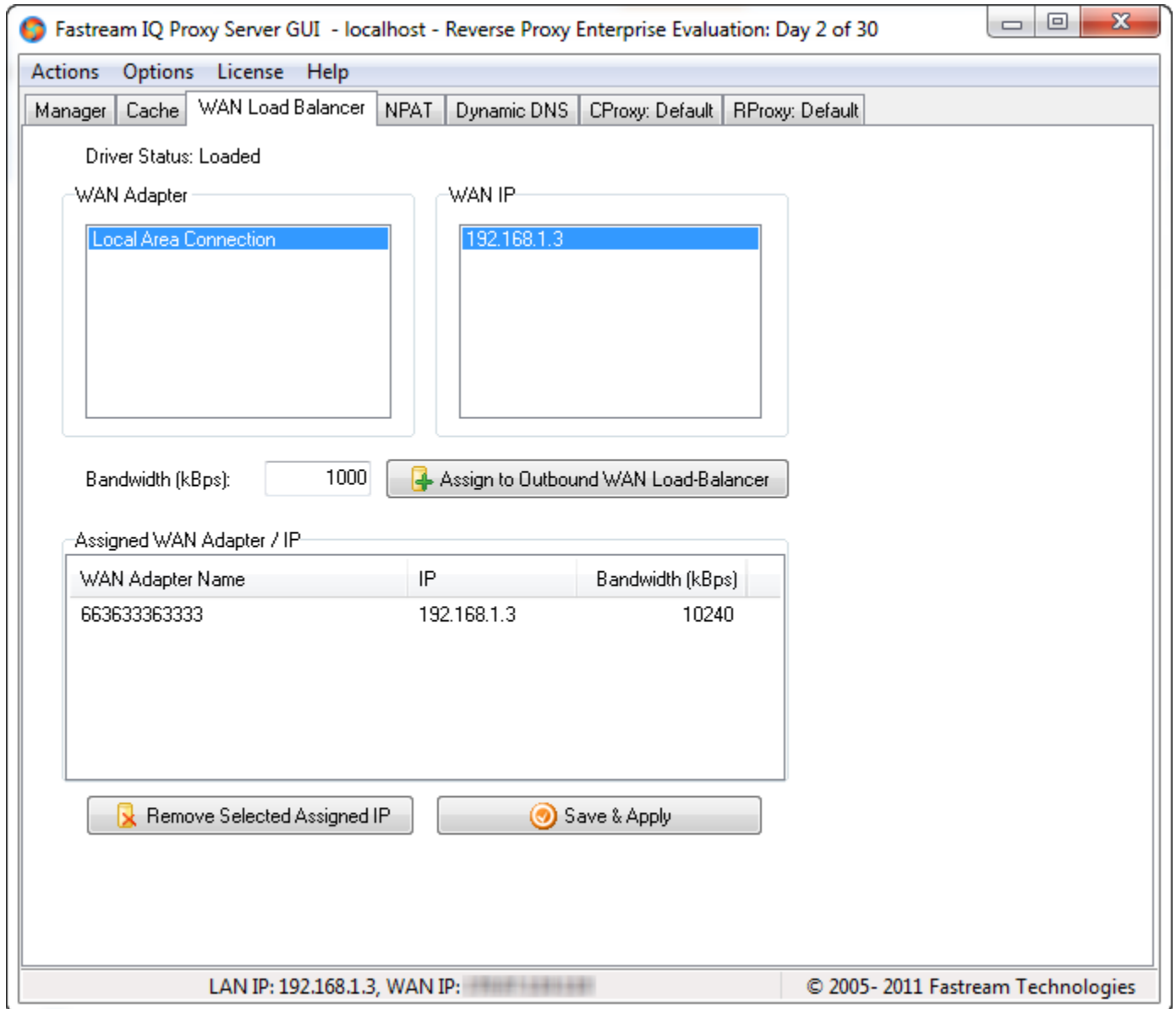
6.4 IQ Proxy PAT



IQProxy supports PAT for TCP and UDP server sockets. You can have internal (LAN) server sockets to be assigned to inbound WAN ports with it. All the mapping will be made in kernel mode.

You can add/edit/remove port mappings from the intuitive GUI tabsheet.

7 WAN Load-Balancing (WAN LB)



Fastream IQ Proxy Server, in all Content Proxy and Reverse Proxy editions supports WAN LB with failover for outbound connections. You can assign as many WAN Ethernet connections as you want to load-balance for your NAT/proxy outgoing connections. Since this is done at kernel-level in IQNDIS driver, it would work for all connections of the machine IQProxy is installed—even when IQProxy service is shut down

IQProxy WAN LB is weighed round robin with respect to bandwidth (in kilo Bytes per second) and current utilization per WAN adapter.

IQProxy WAN LB failover the same way as reverse proxy failover: If a connection is detected unavailable with SYN's sent being un-ACKed, it is suspended for a few minutes. To assign an adapter/IP as backup, set bandwidth to "1". Simple yet effective!

8 Registration and Support

8.1 Fastream IQ Proxy Server Versions

The IQ Proxy Server has a trial version with a 30-days trial period. Before or after this period expires, if you decide to use the software, you must register.

The Fastream IQ Proxy Server software consists of two modules: (1) the Server Engine and (2) the Remote Administration GUI. The remote administration GUI is also included in the engine package but you can also download the GUI separately for remotely controlling from another computer here.

There are three editions of IQ Proxy: the Content-Proxy-only version and the Reverse Proxy Professional edition and the full Reverse Proxy Enterprise edition. All three editions are licensed differently priced for Personal/Academic users and Business Users—no matter how many users will be connecting. All editions pricings are per CPU-slot no matter how many cores they include.

There is also "site licenses" for Reverse Proxy edition, priced differently for Personal/Academic and Business usage.

8.2 Fastream IQ Proxy Professional License Order

If you want to use IQ Proxy after 30 days, you have to register safely on Fastream Secure Order Site. Ordering and becoming a business registered user of IQ Proxy Server over the Internet is 100% secure with industry standard 256-bit SSL protection and with full 30-day money-back guarantee.

8.3 How to Register

Registration makes you a legal owner of the IQ Proxy Server.

Click "Order and Enter License" in the License menu to register your software. A new window will come up:

Any information you provide during the delivery process will remain confidential. After the payment, you will receive an e-mail message containing the applicable billing and serial number information. Be sure to retain/print this message, as you will need information from it to reinstall your software.

To emphasize, online registration is 100% secure and guaranteed. If you face any problems, please contact sales@fastream.com. Please go to <http://www.fastream.com/order.php> for the latest pricing and placing your order.

8.4 How to Upgrade

For customers who ordered in the past 1 year, upgrades are totally free of charge. For customers who last ordered more than 1 year ago, we offer 70% discount for upgrades. In both of the cases, please contact sales@fastream.com for the discount coupon code. You can always find out our contact information at our web site: <http://www.fastream.com/contact.php>.

9. Uninstalling

To uninstall the Fastream IQ Proxy Server Engine from Windows™ 2000/XP/2003/Vista/2008/7:

1. Click the Start button, select Settings, select Control Panel, and then select "Add/Remove Programs" or "Programs and Features" (depends on your Windows version).
2. Choose "Fastream IQ Proxy Server" from the list; click the Add/Remove button.
3. Follow the on-screen instructions.

10 Contact Information

To be eligible for support, you should always use the latest version from <http://www.fastream.com/download.php>. Always feel free to contact us from the addresses below:

sales@fastream.com (Product Sales)
support@fastream.com (Product Support).
pr@fastream.com (Public Relations)
rd@fastream.com (Research & Development)

Or call Fastream International Sales & Support Hotline:
+90-312-223-2830 (GMT+200, 9am-6pm workdays + Saturday)

IQ Proxy Server has an open Yahoo Group, dedicated for users and anybody interested. To subscribe to the mailing lists, simply go to <http://groups.yahoo.com/group/IQProxyServer>

We have done our best to make IQ Proxy Server as bug-free as possible but we are open to constructive suggestions. If you see and report a valid bug please report to igproxyfeedback@fastream.com and we will be more than glad to fix it for everyone!

Thank you for choosing Fastream Products!

IQ Proxy Server Development Squad

Fastream Technologies
Software IQ: Innovation & Quality
<http://www.fastream.com> | <http://www.iqproxyserver.com>

11 Appendix

11.1 A Review of HTTP

HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).

HTTP concepts include (as the Hypertext part of the name implies) the idea that files can contain references to other files whose selection will elicit additional transfer requests. Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. Your Web browser is an HTTP client, sending requests to server machines. When the browser user enters file requests by either "opening" a Web file (typing in a Uniform Resource Locator or URL) or clicking on a hypertext link, the browser builds an HTTP request and sends it to the Internet Protocol address (IP address) indicated by the URL. The HTTP daemon in the destination server machine receives the request and sends back the requested file or files associated with the request. (A Web page often consists of more than one file.)

Reference: <http://www.whatis.com>

11.2 HTTP Details

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. HTTP has been in use by the World-Wide Web global information initiative since 1990. The first version of HTTP, referred to as HTTP/0.9, was a simple protocol for raw data transfer across the Internet. HTTP/1.0, as defined by RFC 1945, improved the protocol by allowing messages to be in the format of MIME-like messages, containing meta-information about the data transferred and modifiers on the request/response semantics. However, HTTP/1.0 does not sufficiently take into consideration the effects of hierarchical proxies, caching, the need for persistent connections, or virtual hosts. In addition, the proliferation of incompletely-implemented applications calling themselves "HTTP/1.0" has necessitated a protocol version change in order for two communicating applications to determine each other's true capabilities.

"HTTP/1.1" includes more stringent requirements than HTTP/1.0 in order to ensure reliable implementation of its features.

Reference: <http://www.w3.org/Protocols/rfc2616/rfc2616-sec1.html#sec1> 48

11.3 Overall Operation

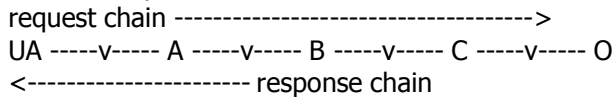
The HTTP protocol is a request/response protocol. A client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a connection with a server.

The server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity-body content.

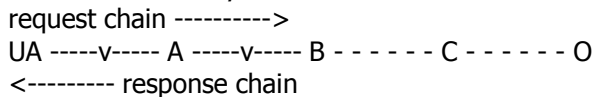
Most HTTP communication is initiated by a user agent and consists of a request to be applied to a resource on some origin server. In the simplest case, this may be accomplished via a single connection (v) between the user agent (UA) and the origin server (O).

```
request chain ----->
UA -----v----- O
<----- response chain
```

A more complicated situation occurs when one or more intermediaries are present in the request/response chain. There are three common forms of intermediary: proxy, gateway, and tunnel. A proxy is a forwarding agent, receiving requests for a URI in its absolute form, rewriting all or part of the message, and forwarding the reformatted request toward the server identified by the URI. A gateway is a receiving agent, acting as a layer above some other server(s) and, if necessary, translating the requests to the underlying server's protocol. A tunnel acts as a relay point between two connections without changing the messages; tunnels are used when the communication needs to pass through an intermediary (such as a firewall) even when the intermediary cannot understand the contents of the messages.



The figure above shows three intermediaries (A, B, and C) between the user agent and origin server. A request or response message that travels the whole chain will pass through four separate connections. This distinction is important because some HTTP communication options may apply only to the connection with the nearest, non-tunnel neighbor, only to the end-points of the chain, or to all connections along the chain. Although the diagram is linear, each participant may be engaged in multiple, simultaneous communications. For example, B may be receiving requests from many clients other than A, and/or forwarding requests to servers other than C, at the same time that it is handling A's request. Any party to the communication which is not acting as a tunnel may employ an internal cache for handling requests. The effect of a cache is that the request/response chain is shortened if one of the participants along the chain has a cached response applicable to that request. The following illustrates the resulting chain if B has a cached copy of an earlier response from O (via C) for a request which has not been cached by UA or A.



Not all responses are usefully cacheable, and some requests may contain modifiers which place special requirements on cache behavior. 49

In fact, there are a wide variety of architectures and configurations of caches and proxies currently being experimented with or deployed across the World Wide Web. These systems include national hierarchies of proxy caches to save transoceanic bandwidth, systems broadcast or multicast cache entries, organizations that distribute subsets of cached data via CD-ROM, and so on. HTTP systems are used in corporate intranets over high-bandwidth links, and for access via PDAs with low-power radio links and intermittent connectivity. The goal of HTTP/1.1 is to support the wide diversity of configurations already deployed while introducing protocol constructs that meet the needs of those who build web applications that require high reliability and, failing that, at least reliable indications of failure.

HTTP communication usually takes place over TCP/IP connections. The default port is TCP 80, but other ports can be used. This does not preclude HTTP from being implemented on top of any other protocol on the Internet, or on other networks. HTTP only presumes a reliable transport; any protocol that provides such guarantees can be used; the mapping of the HTTP/1.1 request and response structures onto the transport data units of the protocol in question is outside the scope of this specification.

In HTTP/1.0, most implementations used a new connection for each request/response exchange. In HTTP/1.1, a connection may be used for one or more request/response exchanges, although connections may be closed for a variety of reasons.

11.4 HTTP Client and Download Manager Suggestions

IQ Reverse Proxy HTTP Server is accessible with all web browsers. In the Windows™ environment you can simply use Microsoft Internet Explorer to access IQ Reverse Proxy HTTP Server.

You may also use a download manager to download large files from a server. A download manager is an application that is designed to make HTTP connections to download files. Download managers ease the download by opening multiple connections for a single file and resuming broken

downloads where possible.

Below there are alternate browser and download manager suggestions. PRODUCT	VENDOR	PRICE/LICENSE TYPE	WEB SITE
Download Managers			
FlashGet	AmazeSoft	Registration fee is \$29.95	http://www.amazesoft.com/
ReGet	ReGet Software	Check web page for pricing details.	http://www.regetsoft.com/
Download Accelerator Plus	SpeedBit	Premium Version is \$29.95.	http://www.speedbit.com/
Browsers			
Opera	Opera Software	Free of Charge	http://www.opera.com/
Mozilla Firefox	Mozilla Foundation	Free of Charge	http://www.getfirefox.com/

Reference: <http://www.w3.org/Protocols/rfc2616/rfc2616-sec1.html#sec1>

11.5 HTTP Terminology

This specification uses a number of terms to refer to the roles played by participants in, and objects of, the HTTP communication.

Age: The age of a response is the time since it was sent by, or successfully validated with, the origin server.

Cache: A program's local store of response messages and the subsystem that controls its message storage, retrieval, and deletion. A cache stores cacheable responses in order to reduce the response time and network bandwidth consumption on future, equivalent requests. Any client or server may include a cache, though a cache cannot be used by a server that is acting as a tunnel.

Cacheable: A response is cacheable if a cache is allowed to store a copy of the response message for use in answering subsequent requests. Even if a resource is cacheable, there may be additional constraints on whether a cache can use the cached copy for a particular request.

Client: A program that establishes connections for the purpose of sending requests.

Content Negotiation: The mechanism for selecting the appropriate representation when servicing a request. The representation of entities in any response can be negotiated (including error responses).

Entity: The information transferred as the payload of a request or response. An entity consists of meta-information in the form of entity-header fields and content in the form of an entity-body. Explicit

expiration time: The time at which the origin server intends that an entity should no longer be returned by a cache without further validation.

First-hand: A response is first-hand if it comes directly and without unnecessary delay from the origin server, perhaps via one or more proxies. A response is also first-hand if its validity has just been checked directly with the origin server.

Fresh: A response is fresh if its age has not yet exceeded its freshness lifetime.

Freshness Lifetime: The length of time between the generation of a response and its expiration time.

Gateway: A server which acts as an intermediary for some other server. Unlike a proxy, a gateway receives requests as if it were the origin server for the requested resource; the requesting client may not be aware that it is communicating with a gateway.

Heuristic expiration time: An expiration time assigned by a cache when no explicit expiration time is available.

Inbound/Outbound: Inbound and outbound refer to the request and response paths for messages: "inbound" means "traveling toward the origin server", and "outbound" means "traveling toward the user agent". 51

Message: The basic unit of HTTP communication, consisting of a structured sequence of octets and transmitted via the connection.

Origin Server: The server on which a given resource resides or is to be created.

Proxy: An intermediary program which acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, with possible translation, to other servers. A proxy MUST implement both the client and server requirements of this specification. A "transparent proxy" is a proxy that does not modify the request or response beyond what is required for proxy authentication and identification. A "non-transparent proxy" is a proxy that modifies the request or response in order to provide some added service to the user agent, such as group annotation services, media type transformation, protocol reduction, or anonymity filtering. Except where either transparent or non-transparent behavior is explicitly stated, the HTTP proxy requirements apply to both types of proxies.

Representation: An entity included with a response that is subject to content negotiation. There may be multiple representations associated with a particular response status.

Request: An HTTP request message.

Response: An HTTP response message.

Resource: A network data object or service that can be identified by a URI. Resources may be available in multiple representations (e.g. multiple languages, data formats, size, and resolutions) or vary in other ways.

Semantically Transparent: A cache behaves in a "semantically transparent" manner, with respect to a particular response, when its use affects neither the requesting client nor the origin server, except to improve performance. When a cache is semantically transparent, the client receives exactly the same response (except for hop-by-hop headers) that it would have received had its

request been handled directly by the origin server.

Server: An application program that accepts connections in order to service requests by sending back responses. Any given program may be capable of being both a client and a server; our use of these terms refers only to the role being performed by the program for a particular connection, rather than to the program's capabilities in general. Likewise, any server may act as an origin server, proxy, gateway, or tunnel, switching behavior based on the nature of each request.

Stale: A response is stale if its age has passed its freshness lifetime.

Tunnel: An intermediary program which is acting as a blind relay between two connections. Once active, a tunnel is not considered a party to the HTTP communication, though the tunnel may have been initiated by an HTTP request. The tunnel ceases to exist when both ends of the relayed connections are closed.

Upstream/Downstream: Upstream and downstream describe the flow of a message: all messages flow from upstream to downstream. 52

User Agent: The client which initiates a request. These are often browsers, editors, spiders (web-traversing robots), or other end user tools.

Variant: A resource may have one, or more than one, representation(s) associated with it at any given instant. Each of these representations is termed a `variant'. Use of the term `variant' does not necessarily imply that the resource is subject to content negotiation.

Validator: A protocol element (e.g., an entity tag or a Last-Modified time) that is used to find out whether a cache entry is an equivalent copy of an entity.

Source:

<http://www.whatis.com>