
Transparent Proxies in Squid By Ankit Fadia Ankit@bol.net.in

With, the extremely uncontrollable growth in the number of Hackers, not only system administrators of servers have to worry about the security of their system, but even if you are running a standalone PPP Linux box, you simply cannot afford to ignore your system's security.

If your system is the main server which communicates with the external untrusted network called the Internet, or even if you simply use your linux box to connect to your ISP and surf the net through PPP, then you should definitely think about installing a firewall on your system.

The preferable and the best option in this case is to install a commercial firewall. However, this option is not always possible and is more often than not unnecesarry. Buying, installing and configuring a good commercial firewall is not only expensive but most beginners find it pretty formidable. OK, I do not want to go through the hassle of a commercial firewall, what do I do? Well, 'ipchains' hold the key for you.

The Firewalling code in the Linux Kernel chnaged considerably after the release of Kernel 2.2. Since then, a lot of new utilites and features have been added. Amongst these improvements, is a kewl feature called 'ipchains', which is primariarly used for configuring the firewalling rules and other such related details.

****
HACKING TRUTH: The usage of ipchains is very much similiar to that of ipfwadm. For more information(like, help on setting rules.) refer to the wrapper script:
/sbin/ipfwadm_wrapper
****

Anyway, in this manual, we will learn about how to use ipchains to configure a transparent proxy on your linux box. So what exactly is a transparent proxy?

Well, a transparent proxy is basically something which fools the client (who connect to the server running the transparent proxy) into believing that they are directly connected to the web server (and not through a proxy.). OK, I am sorry, that is not exactly the correct way to describe it. ;-) Read on for a better description.

Well, a transparent proxy works in the following manner: It listens to a specific port (like the HTTP port i.e. 80) for any connections. As soon as it gets a request for a connection (in this case a HTTP request for a file.) then it redirects the user i.e. connection to another port on the same machine. Now this new port to which the connection is transferred is actually running a Proxy.

So, in affect what happens is, the client i.e. the user who connects to the server where the transparent proxy installed, assumes that it is directly connected and is communicating with the HTTP daemon. However, the truth of the matter is that all communication is being carried out via the proxy running on the server. All this would be clearer when you see the below picture of what happens:

Client --------> Server(Port 80 or HTTP)

The rules of the ipchains transfers client to the port where the proxy is running. So, now the communication takes place in the following manner:

Client --------> Server(Port of Proxy) --------> Server (Port 80 or HTTP)

So, the connection to Port 80 is indirect, however the client has little idea about it.

Now, that you know the working of transparent proxies, let us get down to configuring them on your machine. However, before we get down to the actual process, you need to check whether this is possible on you system or not. Simply look for the file:

/proct/net/ip_fwchains

If you have this file, then well and good, else you will have to recompile your Kernel. However, I am sure almost 98% of you would definitely have this file.

NOTE: In this case, we will be transferring all connections from Port 80 to Port 8080 where Squid runs by default. You could always transfer connections to any proxy port of your choice, by changing the revelant parts. I have taken up Squid, as it is the most common one.

Firstly, in order to transfer all connections from Port 80 to Port 8080, add the following lines to your startup script, so that they are executed each time you boot up.
Note: The server IP is xxx.xx.xx.xx

```
ipchains -A input -p TCP -d 127.0.0.1/32 www-j ACCEPT
ipchains -A input -p TCP -d xxx.xx.xx.xx/32 www-j ACCEPT
ipchains -A input -p TCP -d 0/0 www-j REDIRECT 8080
```

NOTE: If you are using ipfwadm, then add the following lines to the startup script:

```
ipfwadm -I -a-a -P tcp-s any/0 -D 127.0.0.1
ipfwadm -I -a-a -P tcp-s any/0 -D xxx.xx.xx.xx
ipfwadm -I -a-a -P tcp-s any/0 -D any/0 80 -r 8080
```

Once this is done, then configure Squid by following the below process. Please note that you need atleast Squid 2.x to be able to make use of Transparent Proxies. Anyway, to configure Squid, edit the, /etc/squid/squid.conf file and make the following changes:

```
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

Then,restart Squid by typing:

/etc/rc.d/init.d/squid.init restart

Linux Users: I also suggest you compile and execute the following C program. It is simply great and allows you to configure or control Firewall rules etc. **Click Here To Download**

Voila, your transparent proxy is configured and running!!! Anyway, have fun and watch out for updated versions of this manual.

Ankit Fadia
Ankit@bol.net.in

Wanna ask a question? Got a comment to make? Criticize, Comment and more…..by sending me an Instant Message on MSN Messenger. The ID that I use is: **ankit_fadia@hotmail.com**

Wanna learn Hacking? Wanna attend monthly lectures and discussions on various Networking/Hacking topics? Lectures, Debates and Discussions, get it all by simply joining **The Hacking Truths club** by **clicking Here**

Take the **HTCH examination** to give recognition to your Hacking Skills. **Click Here**