CPLUG: red0x's User Guides

User Guide 2:
Tunnelling Past Firewalls

by

Ryan Du Bois

CPLUG Guide Series **CPLUG–2–2005**

Ryan Du Bois **April 2005**

Cal Poly Linux Users' Group
California Polytechnic State University
San Luis Obispo, CA

Tunnel Past Firewalls

Introduction

Have you ever wanted to ssh into your own box from somewhere else? What if your box was behind a router that intercepts ssh traffic, and sends it to another server? This guide will tell you how to dig a tunnel through said firewall, and get to your host.

Applications

- SSH into a firewalled box.
- Browse a firewalled apache server.
- Connect to *XXX* service on a firewalled host.

Tunnels

In order to create the tunnel, you will need access to an ssh server behind the firewall. This server **must** be accessible from the outside world. Once you verify or secure this access, all you need to do is append some syntactical magic to your command line.

```
ssh -L localport:target-host:port user@accessible-host
```

For example, if you have port 2222 available on your local box, and you wanted to access port 22 on machine *vogon*, but could not get to it from the internet, and you happen to have access to machine *blartfast* from the internet, you could tunnel to *vogon* through *blartfast*.

```
ssh -L 2222:vogon:22 myusername@blartfast
```

Now, to connect to SSH, point it at localhost:

```
ssh root@localhost
```

The same goes for similar services. If you want to browse a firewalled apache server, change port 22 to 80 in the above example.

```
ssh -L8080:target-host:80 user@host
```

Then point your browser at: http://localhost:8080