Connecting the (Seemingly) Unconnectable

Have you ever wanted to connect to a remote machine but your VNC or Remote Desktop connections are being refused by the firewall? How much easier it would be just to open the world and go where you want to go when you need to go there. Don't get me wrong, I'm all for security of information in this day and age and want to protect my network as much as the next guy. I realize an open system is NOT a practical solution.

But then I've already solved this problem so it's no longer an issue for me…

Ok, ok… I'll tell you how.

I have a batch file

```
@echo 0ff
ssh -L 5920:myMachine:5900 -L 5930:myMachine:5910 \
    -L 3390:myMachine:3389 myISP.com
```

What this does it establish an SSH session to my firewall (which, by the way, is a Linksys router with the SSH port forwarded to a Microsoft Windows XP machine running MKS Toolkit and it's Secure Shell service—your firewall may be a different configuration but the principles are the same). Since I am running MKS Toolkit on my local machine I can easily invoke **ssh** (and a ton of other useful commands and utilities) from a KornShell on my desktop.

Along with the command line Secure Shell session, this script also tunnels ports 5900 (VNC), 5910 (VMRC) and 3389 (RDP) from local ports (5920, 5930, 3390 respectively) to a machine called `myMachine` in my network. The result is that once this link is up I can then connect using any of these remote technologies to the various machines behind the firewall:

```
vnc - localhost:20
```

gets me to `myMachine:0`,

```
RDP - mstsc -v:localhost:3390 -console
```

connects RDP (Terminal Services) to the console session on `myMachine`, and VMRC has an option to specify relative port to VNC 5900 base port.

The net effect of this simple script is that without an existing VPN connection I can get behind the firewall very safely and very easily where before this I was out of luck if I wanted to stay secure.

Enjoy… Or… Do what I did and take it…

ONE STEP BEYOND !

If you are using MKS Toolkit, you can automate all of this forwarding for any given host.

From within the Windows Control Panel, open the MKS Toolkit Configuration applet. From the **Secure Shell Client** tab, create a new Host Pattern by typing a name, I used `myISP`, in the listed field and clicking the **Add** button. Select that new item and click the **Configure** button to bring up the **Secure Shell Host Configuration** dialog box.

From the **TCP/IP** tab, put your actual hostname in the **Hostname** field. In our case, it is `myISP.com`. Then, from the **Forwarding** tab, click the **Add** button to

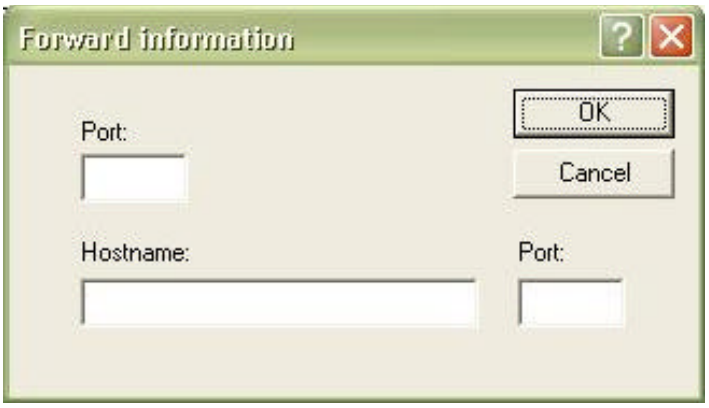

Figure 1: Add Port Forwarding Addresses

create an entry for each port you want to forward.

Referring to *Figure 1*, you will need to use the first **Port** field for the local port and the **Hostname** and **Port** pairing fields for setting the remote host and port number.

Figure 2 shows the configuration dialog box with the settings similar to those discussed earlier in this article.

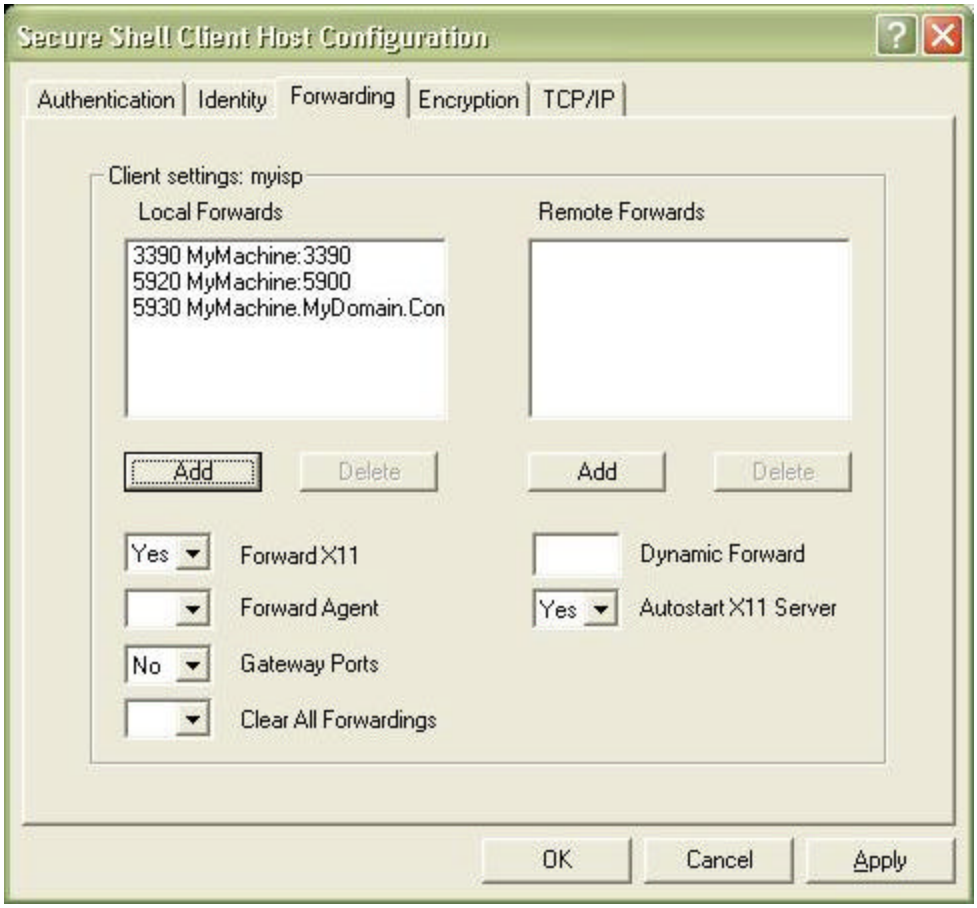

Figure 2: Host Configuration

Click **OK** and you're done... you now just have to modify the command line above to:

```
ssh [-g] myISP
```

Where the `-g` option would allow local ports to bind to all IP addresses on your NIC card rather than just `localhost` If you select **Yes** for Gateway Ports in the Host Configuration dialog shown in *Figure 2* you can omit –g from your command line as it performs the same task.

Of course there are many other options, like identities and passwordless authentication, that can be configured. To learn more about those, refer to the *MKS Toolkit Connectivity Solutions Guide*. If you are running Microsoft Windows XP SP2, you will also have to set exceptions for the ports in the Windows Firewall.

Feel free to comment on this or any other MKS article in the `mks.public.toolkit` public newsgroup. Suggest your own enhancements and contribute your scripts to the MKS Toolkit resource kit.

For more information about the MKS Toolkit products please visit http://www.mkssoftware.com and to view the full reference pages for the commands mentioned in this document visit http://www.mkssoftware.com/docs/cmd_index.asp.