

Re: ssh behind firewall

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-04/0106.html>

From: Egor Kobylkin (egork_at_iname.com)

Date: 04/13/04

Date: Tue, 13 Apr 2004 01:12:40 +0200

foofoo2 wrote:

> *and want to ssh to*
> *my home computer while I'm in office. But , it failed, and it seems that*
> *the my office's firewall block the ssh traffic.*

YOU HAVE TO KNOW WHAT YOU ARE DOING AS YOU CAN POSSIBLY VIOLATE YOUR SECURITY GUIDELINES AT WORK BY BYPASSING THE FIREWALL!

I hereby disclaim all responsibility for this hack. If it backfires on you in any way whatsoever, that's the breaks. Not my fault. If you don't understand the risks inherent in doing this, don't do it. If you use this hack and it allows vicious vandals to break into your company's computers and costs you your job and your company millions of dollars, well that's just tough nuggies. Don't come crying to me. (text taken from httptunnel site)

You could try setting sshd to run on port 80 on your home computer (may be your firewall only keeps the port 80 open).

If that does not work for you, you could create an http tunnel and then go with ssh over it. <http://www.nocrew.org/software/httptunnel.html>

after you have installed it on both computers

at work do

– install ssh

– use buldtunnel.sh as normal user.

#####cut here#####

#!/bin/bash

#cleaning up in case previous connection debris is still there

for pid in `ps -ef|grep 'ssh\|awk '{print(\$2)}'; do kill "\$pid"; done

for pid in `ps -ef|grep 'htc\|awk '{print(\$2)}'; do kill "\$pid"; done

/usr/local/bin/htc --forward-port 2200 --strict-content-length -B 5k

--max-connection-age 1000 --proxy your_proxy_at_work:port

your_home_computer:PORT

#####cut here#####

and then log in with

/usr/bin/ssh your_login_on_home_computer@localhost -p 2200

comp.security.ssh: Re: ssh behind firewall

```
at home put under cron as root the following script
#####cut here#####
#!/bin/bash
#cleaning up in case previous connection debris is still there
for pid in `ps -ef|grep 'sshd\'|awk '{print($2)}'; do kill "$pid"; done
for pid in `ps -ef|grep 'hts\'|awk '{print($2)}'; do kill "$pid"; done
sleep 3
sshd
sleep 3
# port number at home should probably set to 80 for you to get through
# firewall at work
hts --forward-port localhost:22 --strict-content-length PORT
#####cut here#####
You have to run the script at home every now and then as the connection can
be broken by your firewall and I have not found any better way to restore
it but restart servers.
```

```
--
Egor Kobylkin
Emails welcome in English, German, Russian and Spanish
GPGKey www.geocities.com/egor\_kobylkin/EgorKOBYLKIN2004.txt
```