

Contents

- 1 Tunnel SSH over DHS
 - ◆ 1.1 Conditions
 - ◆ 1.2 Download/Setup Files Required for Both Client and Server
 - ◆ 1.3 Config
 - ◇ 1.3.1 Config for Existing DNS Server
 - ◇ 1.3.2 Config for Existing Test Server
 - ◇ 1.3.3 Config for Client Server
 - ◆ 1.4 Original Reference

Tunnel SSH over DHS

If you are on a network, and you dont have access to a Proxy, or you have to pay for a proxy, then it might be possible to get free internet access....albeit at modem (~56kbit) speeds.

Conditions

1. You must be able to join the network, and you must be able to do DNS lookups. I.e.:

```
ping server.com
Pinging server.com [188.1.0.8] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

If it correctly resolved the ip of your server - then you have passed condition 1.

2. You will need a (preferable linux) computer on the Internet, with root access. (Or perhaps a willing friend with one).
3. You will also need access to an existing DNS server, and/or DynDNS account (see reference below for DynDNS).
4. The computer you are using (client) requires linux. A live CD will do nicely.

Download/Setup Files Required for Both Client and Server

http://www.doxpara.com/ozymandns_src_0.1.tgz
http://wiki.kartbuilding.net/ozymandns_src_0.1.tgz

The above download is required for BOTH the client and server Download either one of the above. Gunzip and tar -xvf the above file.

As the above perl files use some perl packages, these need to be installed. Specifically:

```
apt-get install libnet-dns-perl
```

Dnstunnel

```
apt-get install libmime-base32-perl
```

Config

This next setup will vary depending on what you currently use. Ideally you have 2 servers on the internet. The 1st which is currently a DNS server, and 2nd is a normal server which does not have a DNS server.

My Situation: I have 2 physical computers on the internet: 1st = www.server.com (does DNS and mail and web)
2nd = test.server.com (test server).

Config for Existing DNS Server

Basically, you just want to add a DNS rule to point at your second server.

```
vi /etc/bind/zones/server.com.zone
dnstun      IN      NS      dnstun.server.com.
dnstun      IN      A       188.1.0.8

/etc/init.d/bind9 reload
```

Config for Existing Test Server

This is where the special DNS server runs. Root access is required. The ozymandns_src_0.1.tgz and the 2 apt-get packages are also required.

```
./nomde.pl -i 0.0.0.0 dnstun.server.com
# open the firewall allowing in udp 53.
```

Config for Client Server

```
ssh -o ProxyCommand="./droute.pl sshdns.dnstun.server.com" user@localhost
# you will also in the above line, be ssh'ing into your dnstun.server.com
```

If there is a proxy on your dnstun.burkesys.com, then you can go:

```
ssh -o ProxyCommand="./droute.pl sshdns.dnstun.server.com" user@localhost -L 3128:proxy.server.com:3
```

Original Reference

<http://dnstunnel.de/>