Gentoo: IPSec, L2TP VPN for iOS

Posted by Jeremy Olexa on September 18, 2012 Go to comments Leave a comment (18)

There are thousands of guides out there on this subject, however I still struggled to set up an IPSEC VPN at first. This is a HOWTO for my own benefit – maybe someone else will use it too. I struggled because most of the guides involved setting up the VPN on a NAT'd host and connecting to the VPN inside the network. I didn't do that on my linode, which has a static public IP.

My objectives were clear:

1. Create a connection point that was semi-secure while connecting to open wifi networks
2. Bypass some "You are not in the US" restrictions while on the road

Step 1: Install applications, net-misc/openswan, net-dialup/xl2tpd
Step 2: Configure openswan:

```
# cat /etc/ipsec.conf
config setup
    nat_traversal=yes
    virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12,%v4:!10.152.2.0/2
    oe=off
    protostack=auto

conn L2TP-PSK-NAT
    rightsubnet=vhost:%priv
    also=L2TP-PSK-noNAT

conn L2TP-PSK-noNAT
    authby=secret
    pfs=no
    auto=add
    keyingtries=3
    rekey=no
    ikelifetime=8h
    keylife=1h
    type=transport
    left=1.1.1.1
    leftprotoport=17/1701
    right=%any
    rightprotoport=17/%any
    dpddelay=15
    dpdtimeout=30
    dpdaction=clear
```

```
# cat /etc/ipsec.secrets
1.1.1.1 %any: PSK "TestSecret"
```

Where 1.1.1.1 is your public eth0 address and 10.152.2.0 is the subnet that xl2tpd will assign IPs from (can be anything, I picked this at the advice of a guide because it is unlikely to be assigned from a router on a public network)

Step 3: Configure xl2tpd:

```
# cat /etc/xl2tpd/xl2tpd.conf
[global]
ipsec saref = no

[lns default]
ip range = 10.152.2.2-10.152.2.254
local ip = 10.152.2.1
require chap = yes
refuse pap = yes
require authentication = yes
ppp debug = yes
pppoptfile = /etc/ppp/options.xl2tpd
length bit = yes
```

The local IP must be inside the subnet but outside the IP range above.

```
# cat /etc/ppp/options.xl2tpd
refuse-mschap-v2
refuse-mschap
ms-dns 8.8.8.8
ms-dns 8.8.4.4
asyncmap 0
auth
lock
hide-password
local
#debug
name l2tpd
proxyarp
lcp-echo-interval 30
lcp-echo-failure 4
```

The ms-dns lines are configurable to any DNS server you have access to.

```
# cat /etc/ppp/chap-secrets
# Format:
# client server secret IP-addresses
#
# Two lines are needed since it is two-sided auth
test l2tpd testpass *
l2tpd test testpass *
```

Step 4: Configure kernel parameters (sysctl)

```
# cat /etc/sysctl.conf
# only values specific for ipsec/l2tp functioning are shown here. merge with
# existing file
# iPad VPN
```

```
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Remember that sysctl.conf is evaluated at boot so run [redacted] to get the settings enabled now as well.

Step 5: Configure firewall (iptables):
This is the **critical step** that I wasn’t grokking from the existing guides in the wild. Even when bringing the firewall down to test, you need the NAT/forwarding rules:

```
# iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
# iptables -A FORWARD -s 10.152.2.0/24 -j ACCEPT
# iptables -A FORWARD -j REJECT
# iptables -t nat -A POSTROUTING -s 10.152.2.0/24 -o eth0 -j MASQUERADE
```

Step 6: Configure the device/client:
Settings -> General -> Network -> VPN -> Add VPN Configuration

L2TP
Description: Description
Server: 1.1.1.1 (or the hostname)
Account: test
RSA SecurID=OFF
Password: testpass
Secret: TestSecret
Send All Traffic=On

Step 7: Verify it works by going to some IP display webpage and it should show 1.1.1.1

Conclusion: The above examples should be enough to get the VPN working. There are some tweaking oppurtunities that I didn’t document or elaborate on. There is plenty of examples out there to look at or research, however. This was all setup without the firewall configuration and the client would connect but there would be no onward internet activity. It acted just like there was a invalid DNS server configured, at that point I looked into setting up a NAT, dnsmasq on the local interface, and other wierd things. In the end, just needed to forward the traffic properly.

With that knowledge of the firewall issue, the ultimate instructions would probably be this page:
https://www.openswan.org/projects/openswan/wiki/L2TPIPsec_configuration_using_openswan_and_xl2tpd

gentoo iOS, linode, VPN