Install PPTP on CentOS 5

Prerequisets

- Install CentOS 5
- Forward GRE protocol and TCP port 1723 through your firewall

Install the Server

Add the Poptop Yum Repository

rpm -Uhv http://poptop.sourceforge.net/yum/stable/rhel5/pptp-release-current.noarch.rpm

Configure iptables

Create iptables_set.sh, chmod +x iptables_set.sh, and run the script.

- Note: The following will work but you may wish to change the source address from 10.10.9.0/24 to the network range of your choosing based on your network.

```
#!/bin/bash
/sbin/iptables -F
/sbin/iptables -P INPUT DROP
/sbin/iptables -P OUTPUT ACCEPT
/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
/sbin/iptables -A FORWARD -i ppp+ -o eth0 -j ACCEPT
/sbin/iptables -A FORWARD -i eth0 -o ppp+ -j ACCEPT
/sbin/iptables -A INPUT -i eth0 -p tcp --dport 1723 -j ACCEPT
/sbin/iptables -A INPUT -i eth0 -p gre -j ACCEPT
/sbin/iptables -A INPUT -p icmp -j ACCEPT
/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
/sbin/service iptables save
/sbin/iptables -L -v
```

In order to make the live chats (**yahoo, msn, google, etc**) work as it should we need to modify the default MTU,

Edit /etc/ppp/ip-up:
vim /etc/ppp/ip-up

Add the following line:

ifconfig $1 mtu 1400

I add it before “exit 0″.

Configure Kernel

Edit **vi /etc/sysctl.conf**
net.ipv4.ip_forward = 1

Make the changes active

- **# sysctl -p**
- **# sysctl -p /etc/sysctl.conf**

Install PPTP Server

Install ppp and pptpd

- yum install ppp pptpd

[RMP for centos 5]
wget http://poptop.sourceforge.net/yum/stable/packages/pptpd-1.3.4-2.rhel5.x86_64.rpm
wget ftp://ftp.pbone.net/mirror/rnd.rajven.net/centos/5.5/os/i386/pptpd-1.3.4-1cnt5.5.i386.rpm

Configure the service to start on boot

- chkconfig --levels 345 pptpd on

Configure Client Network Options

Modify **vi /etc/pptpd.conf**
localip 192.168.102.254
remoteip 192.168.102.1-100

Modify **vi /etc/ppp/options.pptpd**
ms-dns 208.67.222.222 **[DNS]**
ms-dns 8.8.8.8

Configure Client Access

Edit **vi /etc/ppp/chap-secrets**. You will need to customize the client name, secret (password), and you can either allow all IP address or limit as necessary.

```
# Secrets for authentication using CHAP
# client        server  secret                  IP addresses
world           *       123456                  *
```

User name passwd

Start the Server

Start the pptpd service
chkconfig pptpd on

- **service pptpd start**
- **chkconfig pptpd on**
- **service pptpd restart**

Remove PPTPD

yum remove -y pptpd ppp
iptables --flush POSTROUTING --table nat
iptables --flush FORWARD
rm -rf /etc/pptpd.conf
rm -rf /etc/ppp

Configure the Client

RPM Download

For CentOS 5 32 bit:
wget http://sourceforge.net/projects/poptop/files/pptpd/pptpd-1.4.0/pptpd-1.4.0.tar.gz/download
Install by this command:
rpm -ivh pptpd-1.3.4-2.rhel5.i386.rpm

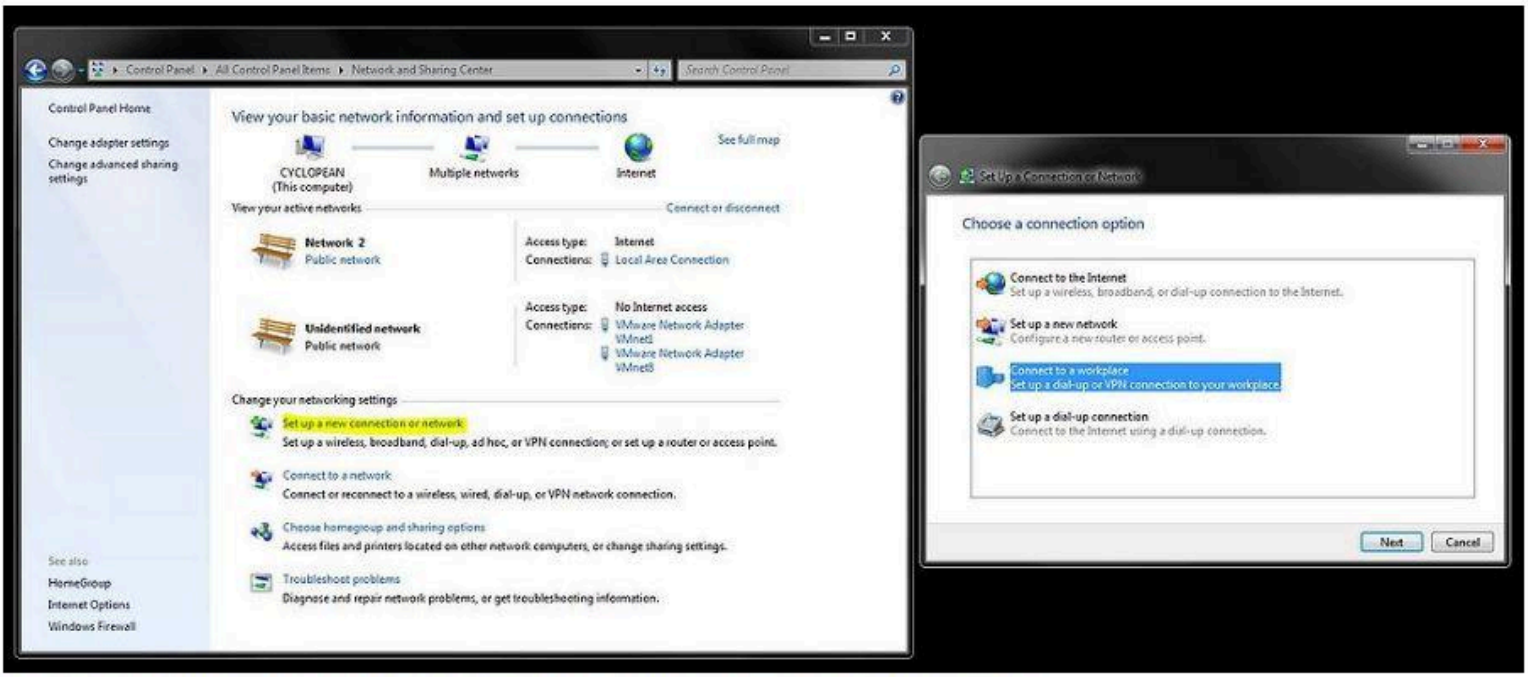
For CentOS 6 32Bit:
wget http://poptop.sourceforge.net/yum/stable/rhel6/x86_64/pptpd-1.4.0-1.el6.x86_64.rpm
Install it by typing the following command:
rpm -ivh pptpd-1.3.4-2.el6.i686.rpm

For CentOS 5 64Bit:
wget wget http://sourceforge.net/projects/poptop/files/pptpd/pptpd-1.4.0/pptpd-1.4.0.tar.gz/download
Install by this command:
rpm -ivh pptpd-1.3.4-2.rhel5.x86_64.rpm

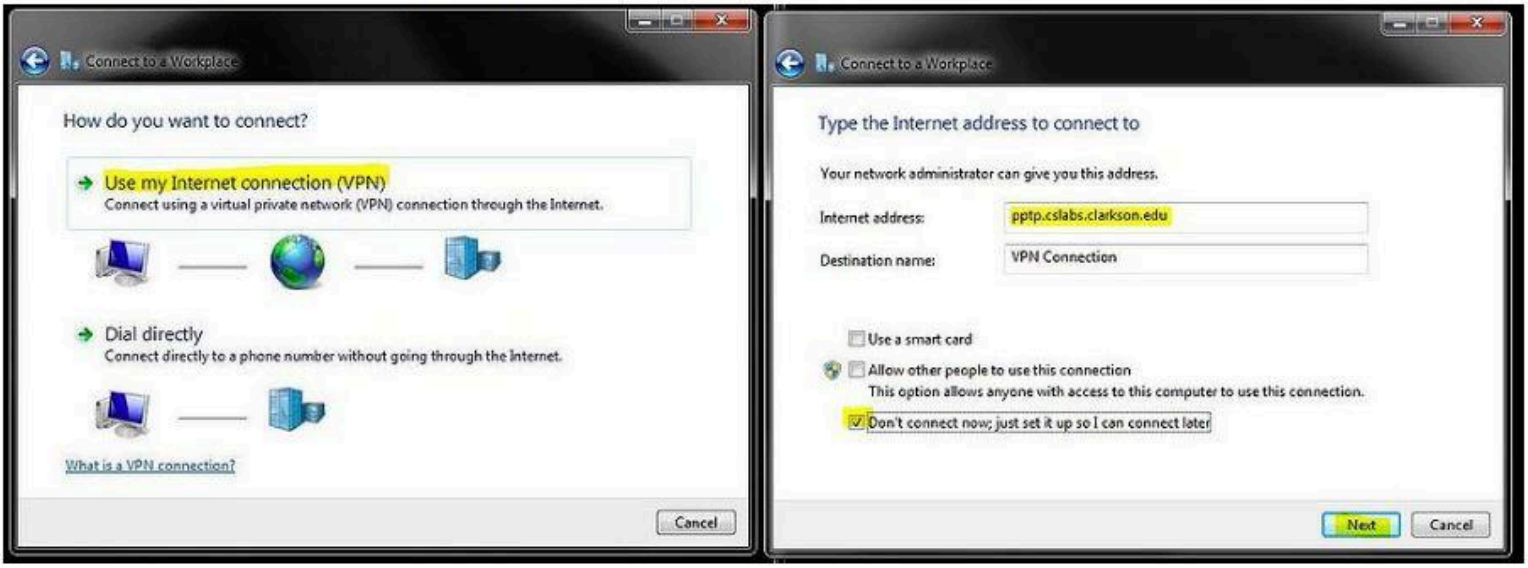
For CentOS 6 64Bit:
wget http://poptop.sourceforge.net/yum/stable/rhel6/x86_64/pptpd-1.4.0-1.el6.x86_64.rpm
Install by this command:
rpm -ivh pptpd-1.3.4-2.el6.x86_64.rpm

Configure the Client

Open up Network and Sharing Center, choose Set up a new connection or network, and select Connect to a workplace.



Choose Use my Internet connection (VPN) and enter in the Internet address of the PPTP server. Select Don't connect now.

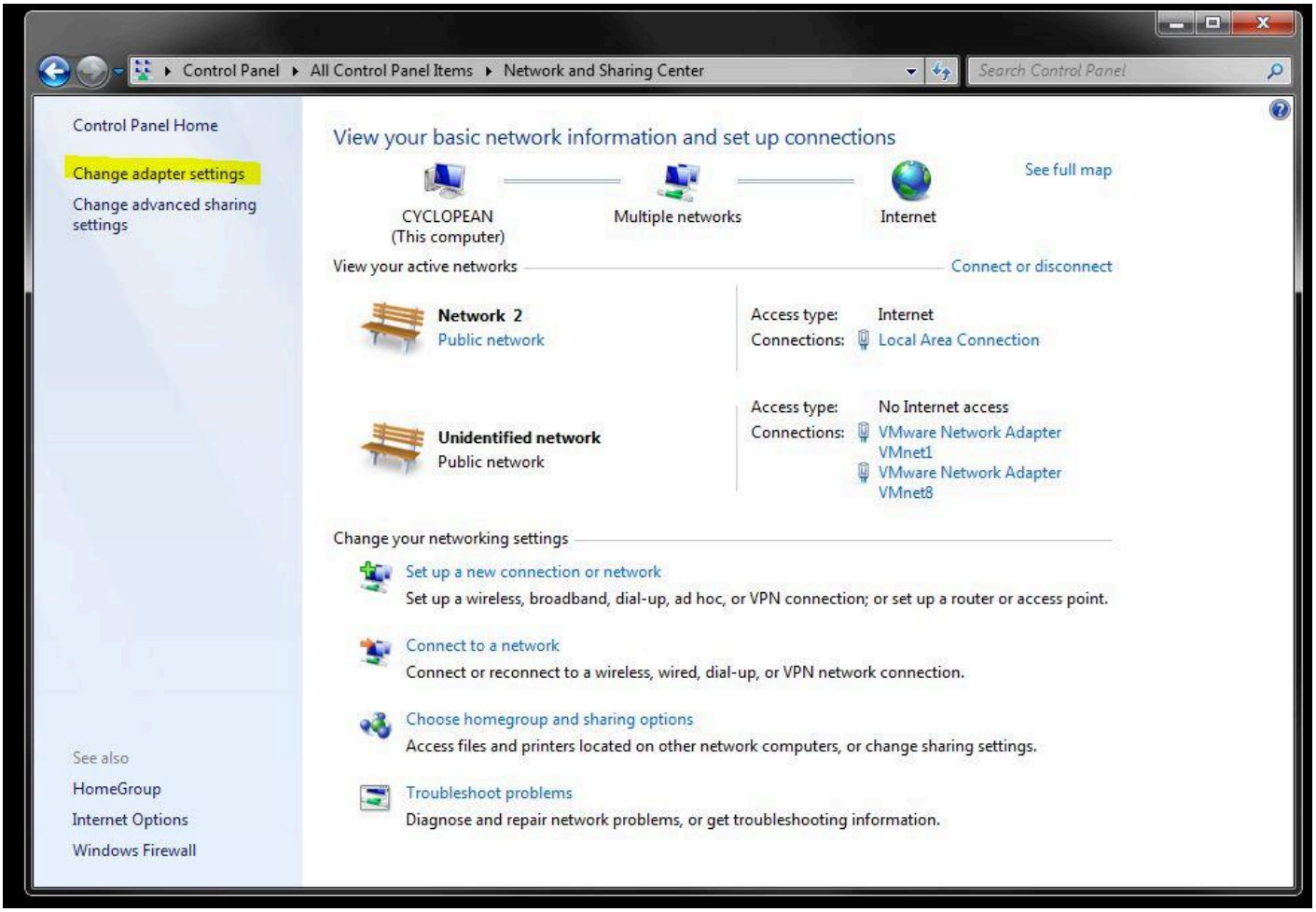


Enter in the user name and password (chap secret), click Create, and click Close.

Choose Use my Internet connection (VPN) and enter in the Internet address of the PPTP server. Select Don't connect now.

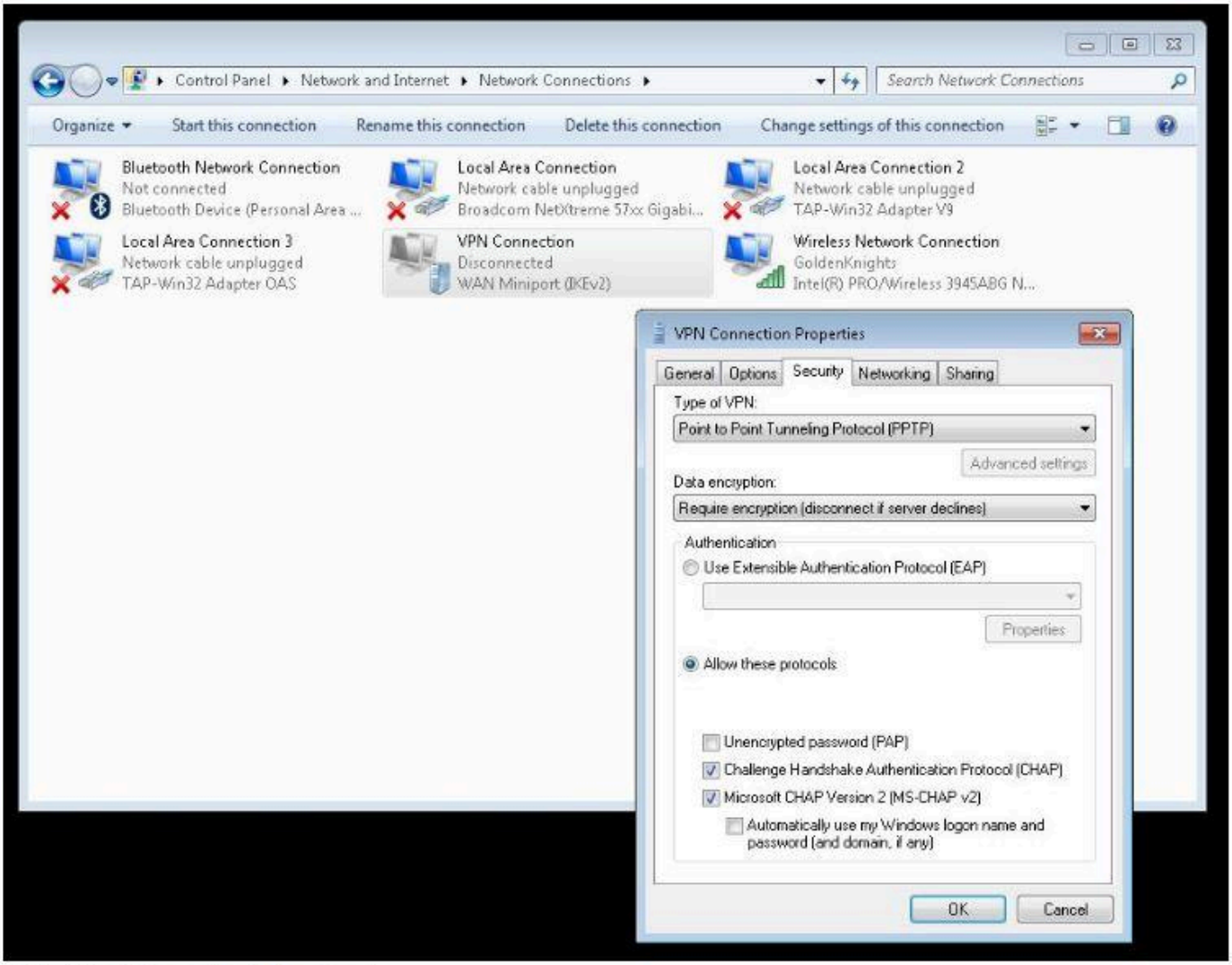
Enter in the user name and password (chap secret), click Create, and click Close.

Return to Network and Sharing Center and click Change adapter settings.



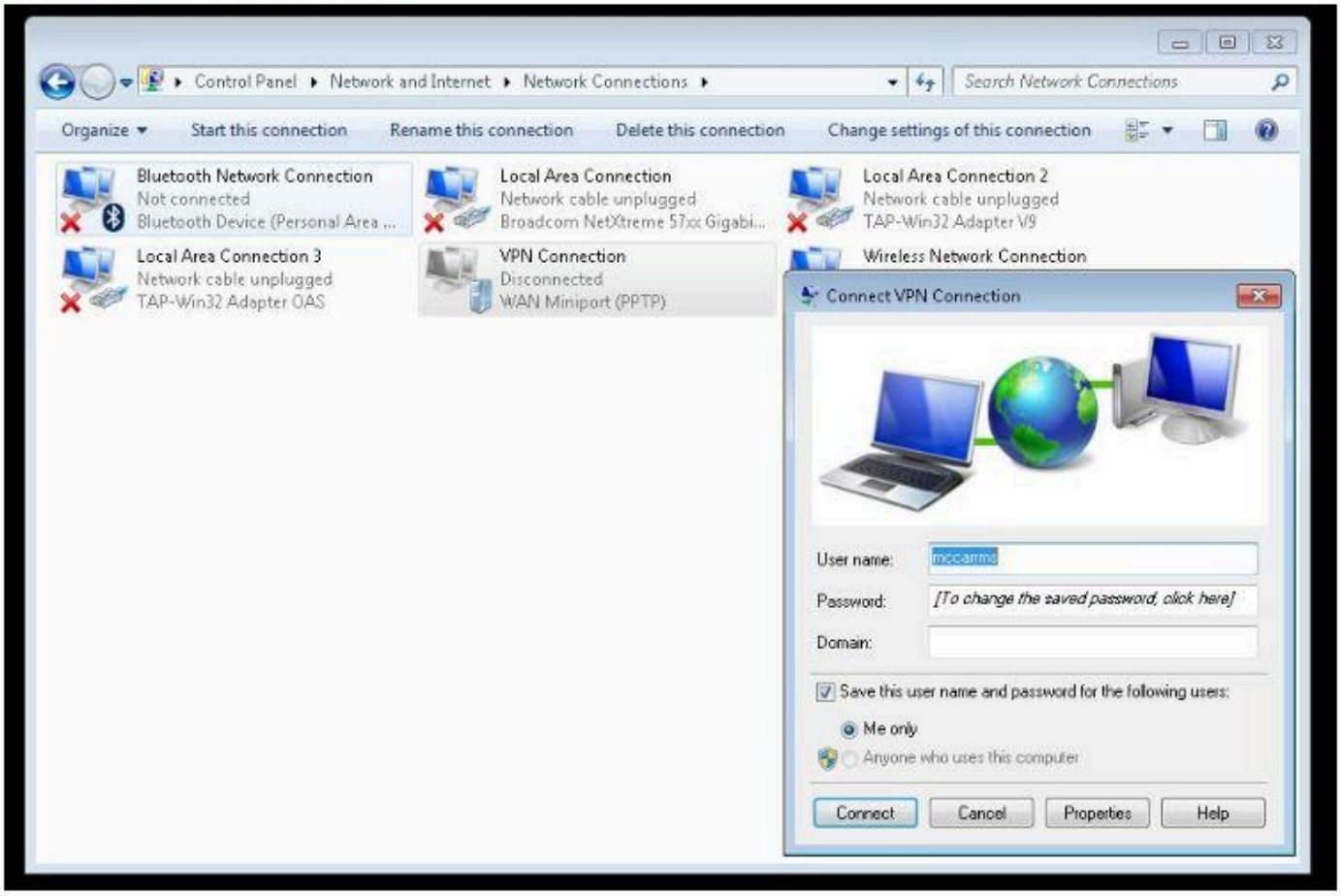
Right click VPN Connection and choose Properties.

Select the Security tab, set the Type of VPN to Point to Point Tunneling Protocol (PPTP), and click OK.



Double click the VPN Connection and choose Connect

Double click the VPN Connection and choose Connect.



Select the Security tab, set the Type of VPN to Point to Point Tunneling Protocol (PPTP), and click OK.
Double click the VPN Connection and choose Connect.

PPTP VPN Installation, configuration and setup. CentOS 5 and 6 for 32 and 64bit and OpenVZ / XEN / KVM

Posted on January 16, 2013 by John Williams

1. Install ppp via yum:
$ yum install ppp -y
2. Download and install pptpd (the daemon for point-to-point tunneling). You can find the correct package at this website http://poptop.sourceforge.net/yum/stable/packages/ :
$ cd /usr/local/src
$ wget http://poptop.sourceforge.net/yum/stable/packages/pptpd-1.3.4-2.el6.x86_64.rpm
$ rpm -Uhv pptpd-1.3.4-2.el6.x86_64.rpm
3. Once installed, open /etc/pptpd.conf using text editor and add following line:
localip 209.85.227.26
remoteip 209.85.227.27-30
4. Open /etc/ppp/options.pptpd and add authenticate method, encryption and DNS resolver value:
require-mschap-v2
require-mppe-128
ms-dns 8.8.8.8
5. Lets create user to access the VPN server. Open /etc/ppp/chap-secrets and add the user as below:
vpnuser pptpd myVPN$99 *
The format is: [username] [space] [server] [space] [password] [space][IP addresses]
6. We need to allow IP packet forwarding for this server. Open /etc/sysctl.conf via text editor and change line below:
net.ipv4.ip_forward = 1
7. Run following command to take effect on the changes:
$ **sysctl -p**
8. Allow IP masquerading in IPtables by executing following line:

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
service iptables save
#service iptables restart

Next, we need to allow TCP port 1723 and the GRE protocol through iptables.

iptables -A INPUT -i eth0 -p tcp --dport 1723 -j ACCEPT
iptables -A INPUT -i eth0 -p gre -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

The following iptables rules are necessary if you want to be able to route all your internet traffic through the VPN server.

iptables -A FORWARD -i ppp+ -o eth0 -j ACCEPT
iptables -A FORWARD -i eth0 -o ppp+ -j ACCEPT

Update: Once you have done with step 8, check the rules at /etc/sysconfig/iptables. Make sure that the POSTROUTING rules is above any REJECT rules.

9. Turn on the pptpd service at startup and reboot the server:

$ **chkconfig pptpd on**

$ **init 6**

Once the server is online after reboot, you should now able to access the PPTP server from the VPN client. You can monitor /var/log/messages for ppp and pptpd related log. Cheers!

Posts related to PPTP VPN Installation, configuration and setup. CentOS 5 and 6 for 32 and 64bit and OpenVZ / XEN / KVM

- Simple CentOS PPTP VPN Automatic Install Script
- Installs a PPTP VPN-only system for CentOS
- PPTPD OpenVPN Install Script
- Install OpenVZ on CentOS 6

How to setup VPN server (PPTP on CentOS, RedHat and Ubuntu)?

This howto describes the steps in how to setup a PPTP VPN on Centos, Fedora, Debian, and Ubuntu with basic RSA authentication.

Before the installation make sure to have your Yum repos updated with the Epel repos.

CentOS and Red Hat Enterprise Linux 5.x

wget http://dl.fedoraproject.org/pub/epel/5/x86_64/epel-release-5-4.noarch.rpm && sudo rpm -Uvh epel-release-5*.rpm

CentOS and Red Hat Enterprise Linux 6.x

wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm && sudo rpm -Uvh epel-release-6*.rpm

CentOS and Red Hat Enterprise Linux 7.x

wget http://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-5.noarch.rpm && sudo rpm -Uvh epel-release-7*.rpm

Step 1. Install PPTPD
CentOS/RedHat 5:

```
yum install pptpd.x86_64 -y
```

CentOS/RedHat 6:
yum install pptpd.x86_64 -y
Fedora 20:

```
yum install pptpd.x86_64 -y
```

Ubuntu/Debian:
apt-get install pptpd
Step 2. Edit IP setttings in /etc/pptpd.conf
echo > /etc/pptpd.conf

paste the following content into the pptpd.conf file

#start of custom file
#logwtmp
option **/etc/ppp/options**.pptpd

localip 192.168.0.1 # local vpn IP
remoteip 192.168.0.100-200 # ip range for connections
listen 23.216.x.x # eth0 my example public IP and network interface

#end of custom file
Step 3. Add user account in/etc/ppp/chap-secrets (assign username and password)
vi /etc/ppp/chap-secrets
usernameForuser1 * setpassword1here *
usernameForuser2 * setpassword2here *

Step 4. Optional settings in /etc/ppp/options.pptpd
echo > /etc/ppp/options.pptpd

Paste the following to your options.pptp

#custom settings for a simple fast pptp server

ms-dns 8.8.8.8
ms-dns 4.2.2.2
lock
name pptpd
require-mschap-v2

Require MPPE 128-bit encryption
(note that MPPE requires the use of MSCHAP-V2 during authentication)
 require-mppe-128

Step 5. Enable network forwarding in /etc/sysctl.conf

vi /etc/sysctl.conf
net.ipv4.ip_forward = 1
use the following command to apply the change:
sysctl -p
Step 6. Configure firewall
iptables -A INPUT -i eth0 -p tcp --dport 1723 -j ACCEPT
iptables -A INPUT -i eth0 -p gre -j ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A FORWARD -i ppp+ -o eth0 -j ACCEPT
iptables -A FORWARD -i eth0 -o ppp+ -j ACCEPT

service iptables save
service iptables restart

Step6-Ubuntu/Debian: Firewall

apt-get install iptables-persistent
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE && /etc/init.d/iptables-persistent save
iptables -A INPUT -i eth0 -p tcp --dport 1723 -j ACCEPT && iptables -A INPUT -i eth0 -p gre -j ACCEPT && iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

If you are using CSF firewall, you may refer to this post on firewall settings.
Step 7. Start PPTP VPN server
Fedora/Debian:
service pptpd restart

Centos/Fedora:
/etc/init.d/pptpd restart-kill && /etc/init.d/pptpd start

Note: To avoid starting pptp on every reboot you can automated by running **chkconfig pptp on**

Now you can test the VPN server from any client: Windows PCs, Linux PCs, Android phones/tablets, or iPhone and iPad.
The log of the VPN server, by default, is combined with system log located at /var/log/messages.

install your own VPN server in 5 mins (PPTP on CentOS, RedHat and Ubuntu)

There are mainly 3 types of VPN servers: Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and OpenVPN. In this tutorial, we use PPTP because it is supported natively on almost all devices, Windows, Linux, Android, IOS and Mac OS.

Step 1. Install PPTPD

If your OS is **CentOS/RedHat 5**:
yum install ppp
cd /usr/local/src
wget http://poptop.sourceforge.net/yum/stable/packages/pptpd-1.4.0-1.rhel5.x86_64.rpm
rpm -Uhv pptpd-1.4.0-1.rhel5.x86_64.rpm
If your OS is **CentOS/RedHat 6**:
yum install ppp
cd /usr/local/src
wget http://poptop.sourceforge.net/yum/stable/packages/pptpd-1.4.0-1.el6.x86_64.rpm
rpm -Uhv pptpd-1.4.0-1.el6.x86_64.rpm
If you are using **Ubuntu**:
apt-get install pptpd

Step 2. Edit IP setttings in /etc/pptpd.conf

vi /etc/pptpd.conf
or
nano -w /etc/pptpd.conf
localip 192.168.0.1
remoteip 192.168.0.101-200

Step 3. Add user account in/etc/ppp/chap-secrets (assign username and password)

vi /etc/ppp/chap-secrets
or
nano -w /etc/ppp/chap-secrets
usernameForuser1 * setpassword1here *
usernameForuser2 * setpassword2here *

Step 4. Optional settings in /etc/ppp/options.pptpd

vi /etc/ppp/options.pptpd
or
nano -w /etc/ppp/options.pptpd
ms-dns 8.8.8.8
ms-dns 4.4.4.4

Step 5. Enable network forwarding in /etc/sysctl.conf

vi /etc/sysctl.conf
or
nano -w /etc/sysctl.conf
net.ipv4.ip_forward = 1
Use the following command to apply the change:
sysctl -p

Step 6. Configure firewall

iptables -A INPUT -i eth0 -p tcp --dport 1723 -j ACCEPT
iptables -A INPUT -i eth0 -p gre -j ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A FORWARD -i ppp+ -o eth0 -j ACCEPT
iptables -A FORWARD -i eth0 -o ppp+ -j ACCEPT
service iptables save
service iptables restart
If you are using CSF firewall, you may refer to this post on firewall settings.

Step 7. Start PPTP VPN server

If your OS is CentOS or Redhat, using the following command:
service pptpd restart
To start PPTP Daemon automatically when rebooting next time, use command:
chkconfig pptpd on
If your OS is **Ubuntu**, you just reboot your machine.
Now you can test the VPN server from any client: Windows PCs, Linux PCs, Android phones/tablets, or iPhone and iPad.
The log of the VPN server, by default, is combined with system log located at /var/log/messages.
PS: for text editor you can also use **nano**, instead of vi, if you are not comfortable with vi. If you are using nano, make sure you start nano with “-w”.
Any questions? you post them in the comment section.
Updated 1: update the version of pptp daemon.

PPTPD OpenVPN Install Script

yum remove -y pptpd ppp
iptables --flush POSTROUTING --table nat
iptables --flush FORWARD
rm -rf /etc/pptpd.conf
rm -rf /etc/ppp
wget http://up2vps.com/pptpd/dkms-2.0.17.5-1.noarch.rpm
wget http://up2vps.com/pptpd/kernel_ppp_mppe-1.0.2-3dkms.noarch.rpm
wget http://up2vps.com/pptpd/pptpd-1.3.4-1.rhel5.1.i386.rpm
wget http://up2vps.com/pptpd/ppp-2.4.4-9.0.rhel5.i386.rpm
yum -y install make libpcap iptables gcc-c++ logrotate tar cpio perl pam tcp_wrappers
rpm -ivh dkms-2.0.17.5-1.noarch.rpm
rpm -ivh kernel_ppp_mppe-1.0.2-3dkms.noarch.rpm
rpm -qa kernel_ppp_mppe

```
rpm -Uvh ppp-2.4.4-9.0.rhel5.i386.rpm
rpm -ivh pptpd-1.3.4-1.rhel5.1.i386.rpm
mknod /dev/ppp c 108 0
echo 1 > /proc/sys/net/ipv4/ip_forward
echo "mknod /dev/ppp c 108 0" >> /etc/rc.local
echo "echo 1 > /proc/sys/net/ipv4/ip_forward" >> /etc/rc.local
echo "localip 172.16.36.1" >> /etc/pptpd.conf
echo "remoteip 172.16.36.2-254" >> /etc/pptpd.conf
echo "ms-dns 8.8.8.8" >> /etc/ppp/options.pptpd
echo "ms-dns 8.8.4.4" >> /etc/ppp/options.pptpd
pass=`openssl rand 6 -base64`
if [ "$1" != "" ]
then pass=$1
fi
echo "vpn pptpd ${pass} *" >> /etc/ppp/chap-secrets
iptables -t nat -A POSTROUTING -s 172.16.36.0/24 -j SNAT --to-source `ifconfig | grep 'inet addr: '| grep -v ' 127.0.0.1 ' |
cut -d: -f2 | awk ' NR==1 { print $1}'`
iptables -A FORWARD -p tcp --syn -s 172.16.36.0/24 -j TCPMSS --set-mss 1356
service iptables save
chkconfig iptables on
chkconfig pptpd on
service iptables start
service pptpd start
echo "VPN service is installed, your VPN username is vpn, VPN password is ${pass}"
```

Posts related to PPTPD OpenVPN Install Script

- Simple CentOS PPTP VPN Automatic Install Script
- Installs a PPTP VPN-only system for CentOS
- PPTP VPN Installation, configuration and setup. CentOS 5 and 6 for 32 and 64bit and OpenVZ / XEN / KVM
- Interactive OpenVPN install script on a OpenVZ VPS

WEB:
http://docs.cslabs.clarkson.edu/wiki/Install_PPTP_on_CentOS_5
http://blog.solidshellsecurity.com/2013/01/16/pptp-vpn-installation-configuration-setup-centos-5-6-32-64bit-openvz-xen-kvm/#

https://www.photonvps.com/billing/knowledgebase.php?action=displayarticle&id=58
http://freehostinganswers.com/blog/how-to-install-your-own-vpn-server-in-5-mins-pptp-on-centos-redhat-and-ubuntu/
http://blog.solidshellsecurity.com/2012/04/24/pptpd-openvpn-install-script/

PPTP VPN Installer

How to Install PPTP VPN Server on CentOS 6.x

```
yum install -y git
cd /opt && git clone git://github.com/drewsymo/VPN.git
cd VPN && bash vpn-setup-vanilla.sh
```

If you're on Linode, you can simply rebuild your instance with the PPTP VPN Installer StackScript.

Installs an easy-to-use PPTP VPN solution on your box. See: http://drewsymo.com/networking/vpn/install-ptpp/
Compatible with: No distros currently supported

Scripts

```
---------------------------------------------------------------------------
#!/bin/bash -x

#
# drewsymo/VPN
#
# Installs a PPTP VPN-only system for CentOS
#
# @package VPN 2.0
# @since VPN 1.0
# @author Drew Morris
# @url http://drewsymo.com/networking/vpn/install-ptpp/
```

```
#

# Create UDF Options

## VPN Username
#<udf name="vpn_user" label="Enter your VPN Username"
#    default="myuser"
#    example="vpn-user">

## VPN Password
#<udf name="vpn_pass" label="Enter the Password of VPN User"
#    default="sudoninja"
#    example="wackytubeman23x">

## VPN Local IP
#<udf name="vpn_local" label="Enter the Local IP Address of your Server"
#    default="192.168.0.1"
#   example="10.0.0.1">

## VPN Remote IP
#<udf name="vpn_remote" label="Enter the Local IP Address of your Home Device (or range)"
#    default="192.168.0.1"
#    example="192.168.0.151-200">

(

VPN_IP=`curl ipv4.icanhazip.com>/dev/null 2>&1`

yum -y groupinstall "Development Tools"
rpm -Uvh http://poptop.sourceforge.net/yum/stable/rhel6/pptp-release-current.noarch.rpm
yum -y install policycoreutils policycoreutils
yum -y install ppp pptpd
yum -y update

echo "1" > /proc/sys/net/ipv4/ip_forward
sed -i 's/net.ipv4.ip_forward = 0/net.ipv4.ip_forward = 1/g' /etc/sysctl.conf

sysctl -p /etc/sysctl.conf

echo "localip $VPN_LOCAL" >> /etc/pptpd.conf # Local IP address of your VPN server
echo "remoteip $VPN_REMOTE" >> /etc/pptpd.conf # Scope for your home network

echo "ms-dns 8.8.8.8" >> /etc/ppp/options.pptpd # Google DNS Primary
```

```
echo "ms-dns 209.244.0.3" >> /etc/ppp/options.pptpd # Level3 Primary
echo "ms-dns 208.67.222.222" >> /etc/ppp/options.pptpd # OpenDNS Primary

echo "$VPN_USER pptpd $VPN_PASS *" >> /etc/ppp/chap-secrets

service iptables start
echo "iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE" >> /etc/rc.local
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
service iptables save
service iptables restart

service pptpd restart

echo -e '\E[37;44m'"\033[1m Installation Log: /var/log/vpn-installer.log \033[0m"
echo -e '\E[37;44m'"\033[1m You can now connect to your VPN via your external IP ($VPN_IP)\033[0m"

echo -e '\E[37;44m'"\033[1m Username: $VPN_USER\033[0m"
echo -e '\E[37;44m'"\033[1m Password: $VPN_PASS\033[0m"

) 2>&1 | tee /var/log/vpn-installer.log
```

Note: OpenVZ users, currently one of the iptables rules used in this script is not virtualised in OpenVZ (masquerade). This means you will need to run this line of code once you have finished installing the CentOS PPTP VPN script for it to work:
iptables -t nat -A POSTROUTING -j SNAT --to-source x.x.x.x
Where x.x.x.x is your venet0 IP address
In addition to this, you will also need OpenVZ kernel 2.6.32

How do I connect to my VPN?

You can now connect to your VPN using your servers IP as the hostname (this depends on your VPN client)
The default username and password for your VPN server is:
Username: myuser
Password: mypass

How to setup VPN server (PPTP on CentOS, RedHat and Ubuntu)?

This howto describes the steps in how to setup a PPTP VPN on Centos, Fedora, Debian, and Ubuntu with basic RSA authentication.

Before the installation make sure to have your Yum repos updated with the Epel repos.

CentOS and Red Hat Enterprise Linux 5.x

wget http://dl.fedoraproject.org/pub/epel/5/x86_64/epel-release-5-4.noarch.rpm && sudo rpm -Uvh epel-release-5*.rpm

CentOS and Red Hat Enterprise Linux 6.x

```
wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm && sudo rpm -Uvh epel-release-6*.rpm
```

CentOS and Red Hat Enterprise Linux 7.x

wget http://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-5.noarch.rpm && sudo rpm -Uvh epel-release-7*.rpm

Step 1. Install PPTPD

CentOS/RedHat 5:

yum install pptpd.x86_64 -y

CentOS/RedHat 6:

```
yum install pptpd.x86_64 -y
```

Fedora 20:

yum install pptpd.x86_64 -y

Ubuntu/Debian:

```
apt-get install pptpd
```

Step 2. Edit IP setttings in /etc/pptpd.conf

```
echo > /etc/pptpd.conf
```

```
paste the following content into the pptpd.conf file
```

```
#start of custom file
#logwtmp
option /etc/ppp/options.pptpd
localip 192.168.0.1   # local vpn IP
remoteip 192.168.0.100-200  # ip range for connections
listen 23.216.x.x # eth0 my example public IP and network interface
#end of custom file
```

Step 3. Add user account in/etc/ppp/chap-secrets (assign username and password)

```
vi /etc/ppp/chap-secrets
```

usernameForuser1 * setpassword1here *

usernameForuser2 * setpassword2here *

Step 4. Optional settings in /etc/ppp/options.pptpd

```
echo > /etc/ppp/options.pptpd
```

```
Paste the following to your options.pptp
```

```
#custom settings for a simple fast pptp server
ms-dns 8.8.8.8
ms-dns 4.2.2.2
lock
name pptpd
require-mschap-v2
# Require MPPE 128-bit encryption
# (note that MPPE requires the use of MSCHAP-V2 during authentication)
 require-mppe-128
```

Step 5. Enable network forwarding in /etc/sysctl.conf

```
vi /etc/sysctl.conf
```

net.ipv4.ip_forward = 1

use the following command to apply the change:

```
sysctl -p
```

Step 6. Configure firewall

```
iptables -A INPUT -i eth0 -p tcp --dport 1723 -j ACCEPT
```

```
iptables -A INPUT -i eth0 -p gre -j ACCEPT
```

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

```
iptables -A FORWARD -i ppp+ -o eth0 -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -o ppp+ -j ACCEPT
```

```
service iptables save
```

```
service iptables restart
```

Step6-Ubuntu/Debian: Firewall

apt-get install iptables-persistent

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE &&
/etc/init.d/iptables-persistent save

iptables -A INPUT -i eth0 -p tcp --dport 1723 -j ACCEPT && iptables -A INPUT -i eth0 -p gre -j ACCEPT && iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

If you are using CSF firewall, you may refer to this post on firewall settings.

Step 7. Start PPTP VPN server

Fedora/Debian:

```
service pptpd restart
```

```
Centos/Fedora:
```

```
/etc/init.d/pptpd restart-kill && /etc/init.d/pptpd start
```

```
Note: To avoid starting pptp on every reboot you can automated by running chkconfig pptp on
```