

Configure Zeroshell as a PPTP Server with MS-CHAPv2 and MPPE support

Basics:

Boot from zeroshell CD then log into your zeroshell box. Using just the default image that the CD starts up with you can start using zeroshell as a PPTP server with just a few changes. First enable RADIUS in the USERS/RADIUS menu.

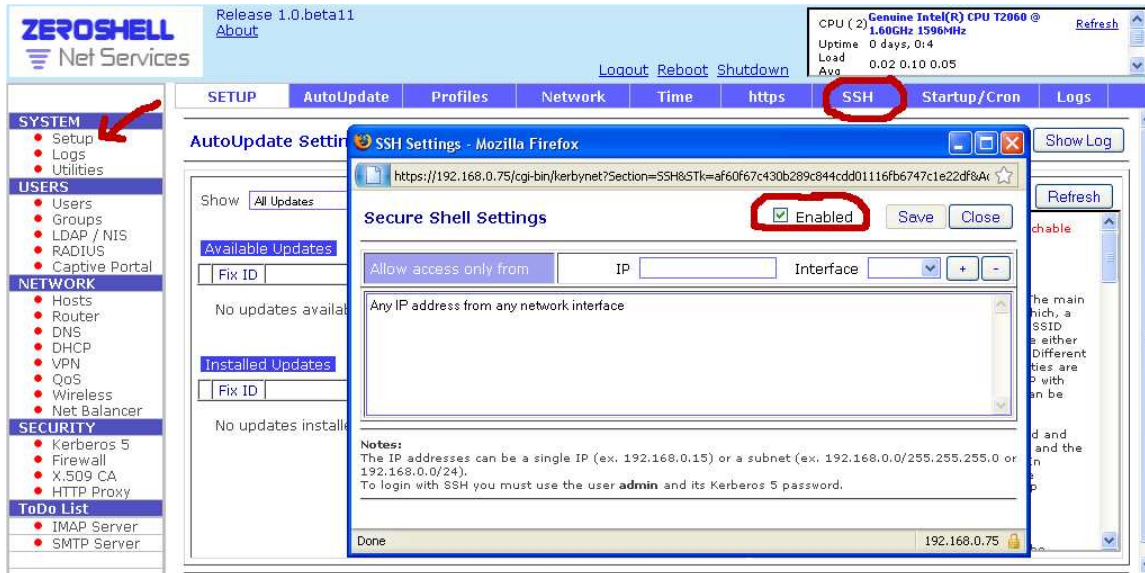
The screenshot shows the Zeroshell Net Services web interface. The top navigation bar includes 'RADIUS', 'Manage', 'Access Points', and 'Proxy'. The left sidebar has a tree view with categories: SYSTEM, USERS, NETWORK, SECURITY, and ToDo List. Under 'USERS', the 'RADIUS' option is selected and highlighted with a red arrow. The main content area is titled 'RADIUS Server for Wireless and Identity Based Networking Services'. It shows the status as 'ACTIVE' and a red circle around the 'Enabled' checkbox. Below this is the '802.1x Configuration' section, which includes an 'X.509 Host Certificate' dropdown set to 'Local CA' and 'OU=Hosts, CN=portal1.premier.hh'. There are 'View', 'Save', and 'Cancel' buttons. A 'Some Notes' section at the bottom explains that the RADIUS server supports EAP-TLS, PEAP, and EAP-TTLS, and provides instructions on certificate management and authentication protocols like MSCHAPv2 and Kerberos 5.

Zeroshell will use the same IP address scope located on the L2TP menu. You can also change it to whatever you want it to be for your application. Preview your settings in NETWORK/VPN/Host-to-LAN (L2TP/IPSec)

The screenshot shows the Zeroshell Net Services web interface with the 'Host-to-LAN (L2TP/IPSec)' menu item selected and circled in red. The left sidebar has a red arrow pointing to the 'VPN' option. The main content area is titled 'L2TP over IPsec with X.509 IKE and MSCHAPv2 client authentication'. It shows the status as 'ACTIVE' and a red circle around the 'Enabled' checkbox. Below this is the 'IPsec IKE Configuration' section, which includes an 'X.509 Host Certificate' dropdown set to 'Local CA' and 'OU=Hosts, CN=portal1.premier.hh'. There are 'View', 'Save', and 'Cancel' buttons. The 'Client IP Address Assignment' section is circled in red and shows 'From 172.16.24.40 to 172.16.24.45'. The 'Routing Method' section has radio buttons for 'Normal', 'ProxyARP', and 'Source NAT', with 'Source NAT' selected. A 'NAT-T' checkbox is also present. A 'Some Notes' section at the bottom explains that this VPN type is a combination of L2TP and IPsec, and provides instructions on certificate management and authentication protocols like MSCHAPv2 and Kerberos 5.

Note: The L2TP Server does not have to be enabled to pass the IP address information to the PPTP server. Just change the numbers and hit save while it's enabled or disabled.

Last thing we need to do is enable ssh for the actual configurations that will enable the PPTP server. Use the SYSTEM/Setup/SSH menu to enable this feature.

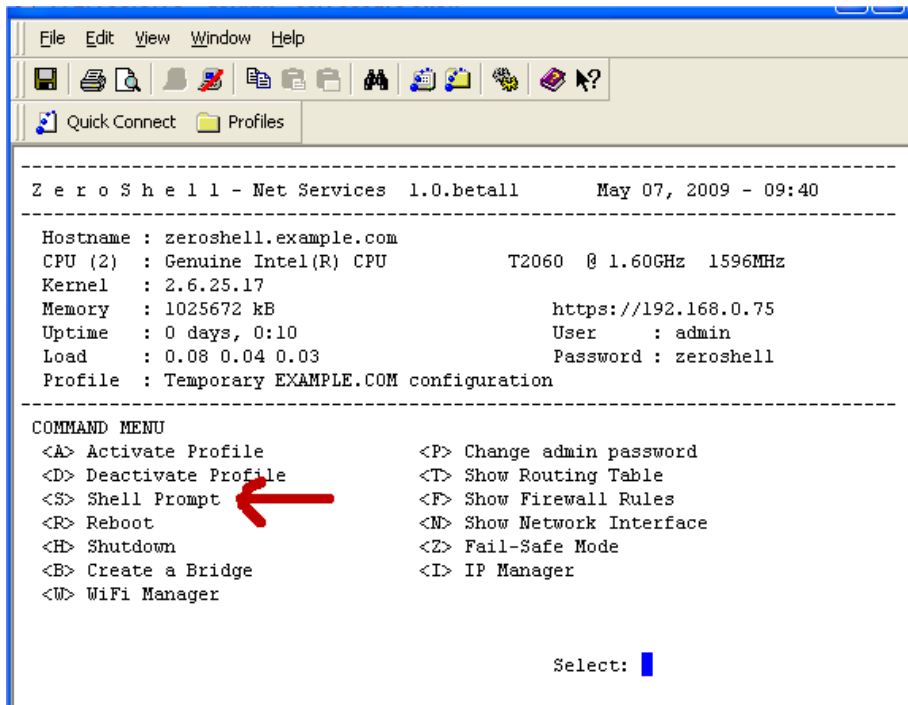


Advanced:

This part of the configurations take place in the CLI so if you don't follow these instructions closely or don't feel confident using the CLI then you probably shouldn't be using zeroshell.

That statement will either inspire you or strike fear in your heart.

Well go and start your ssh session with the zeroshell box and use the shell prompt.



We will be working with 2 files to enable and configure the PPTP server.

/etc/**pptpd.conf**

/etc/ppp/**options.pptpd**

Copy these 2 files to a location that will not get wiped every time you reboot. Use the **/Database** for any static files that you don't want mangled after a reboot or service restart.

Note: cp /etc/pptpd.conf /Database

Note: cp /etc/ppp/options.pptpd /Database

Now edit the first file (pptpd.conf) with the following options.

ppp /usr/local/sbin/pppd

option /etc/ppp/options.pptpd

#noipparam

#bcrelay eth00

Edit the second file (optins.pptpd) with the following options.

#chapms-strip-domain

BSD licensed ppp-2.4.2 upstream with MPPE only, kernel module ppp_mppe.o

{{{

#refuse-pap

#refuse-chap

#refuse-mschap

Require the peer to authenticate itself using MS-CHAPv2 [Microsoft

Challenge Handshake Authentication Protocol, Version 2] authentication.

require-mschap-v2

Require MPPE 128-bit encryption

(note that MPPE requires the use of MSCHAP-V2 during authentication)

require-mppe-128

This is where you can pick and choose which authentication methods you want for your application. Just uncomment the ones you want to refuse and then write your changes and quit out of the shell.

CLI configurations are done. For those of you that made it this far that's great.

Let's go back into the zeroshell web interface and make the PPTP daemon startup at system boot. We'll need to add a script to accomplish that so after you log in go to **SYSTEM/Setup/ Startup/Cron**.

The screenshot shows the ZeroShell web interface. At the top, there's a header with the ZeroShell logo and system information: Release 1.0.beta11, CPU (2) Genuine Intel(R) CPU T2060 @ 1.60GHz 1596MHz, Uptime 0 days, 0i:4, Load Ave 0.02 0.10 0.05. A navigation menu includes SETUP, AutoUpdate, Profiles, Network, Time, https, Startup/Cron (highlighted with a red circle), and Logs. The main content area is titled 'AutoUpdate Settings' with a status of 'Active' and a check interval of 6 hours. It shows 'Available Updates' and 'Installed Updates' sections, both indicating 'No updates available for release 1.0.beta11'. A 'Message Board' on the right contains news items, including one about ZeroShell 1.0.beta8 and another about a patch for release 1.0.beta7. A sidebar on the left lists various system categories like SYSTEM, USERS, NETWORK, SECURITY, and ToDo List, with a red arrow pointing to the 'Setup' option under the SYSTEM category.

Once you select that a new window will open. Choose the drop down menu for Post Boot.

The screenshot shows a 'SCRIPTING EDITOR' window with a red circle around the 'Post Boot' dropdown menu. The script content is as follows:

```
# Startup Script
rm -f /etc/pptpd.conf
rm -f /etc/ppp/options.pptpd
cp -f /Database/pptpd.conf /etc/
cp -f /Database/options.pptpd /etc/ppp/
/usr/local/sbin/pptpd
```

Below the script editor is a 'Jobs Scheduling' section with dropdown menus for Hour, Minute, Day, Month, Day of the week, and Every. The status is 'Enabled' and the current time is 'Thu May 7 10:21:08 EDT 2009'.

This will overwrite the files on zeroshell after each reboot. Also if you plan to make any changes make them on the /Database copies and not on the ones in the zeroshell file system /etc. Those get overwritten. Now is a good time to test the vpn connection. I will use windows XP for this test.

Create a new connection from the CONTROL PANEL/NETWORK CONNECTIONS.

The screenshot shows two windows from Windows XP. On the left is the 'Network Connections' window in Microsoft Internet Explorer, with 'Create a new connection' highlighted in a red box. On the right is the 'New Connection Wizard' window, which displays the following text:

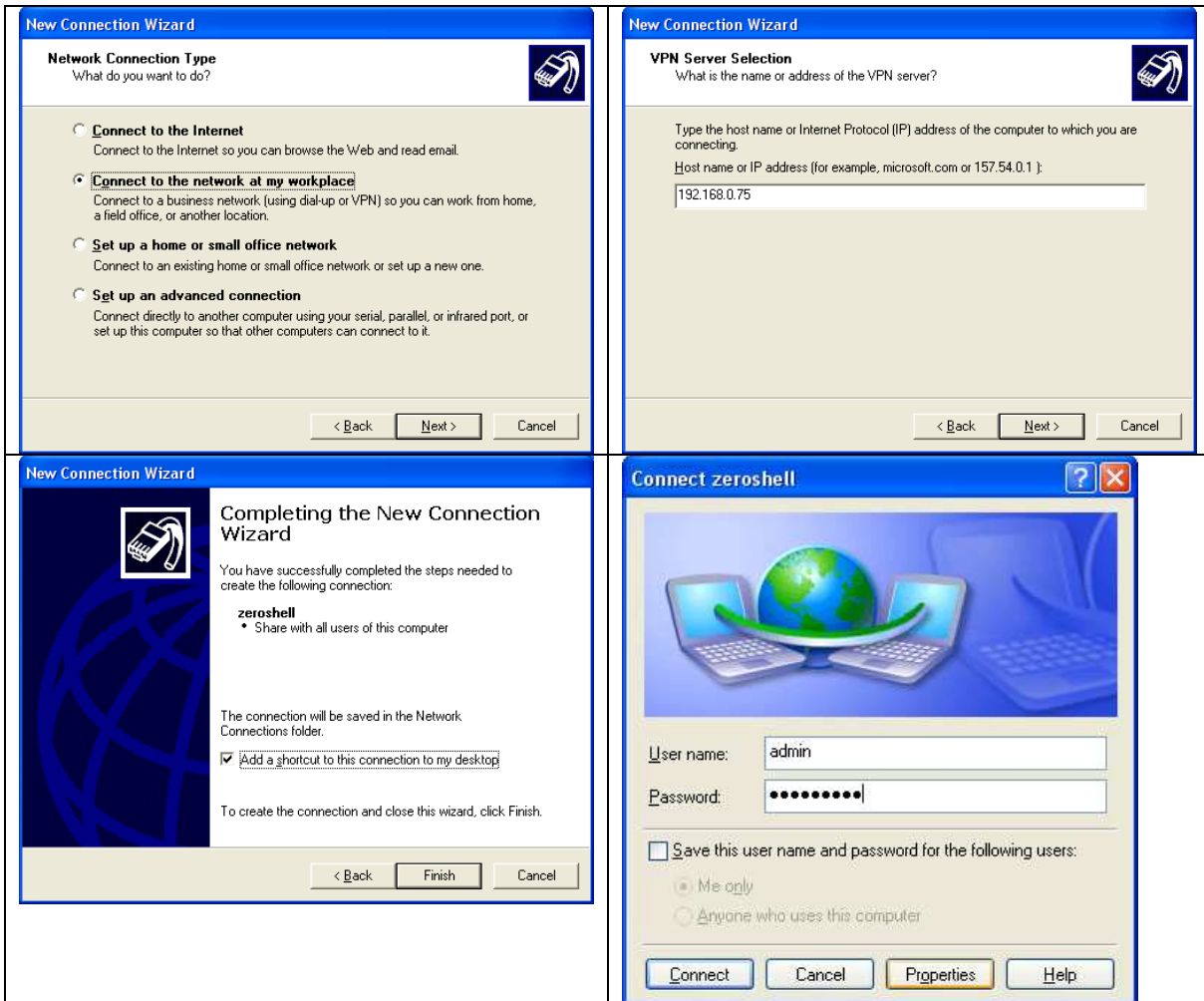
Welcome to the New Connection Wizard

This wizard helps you:

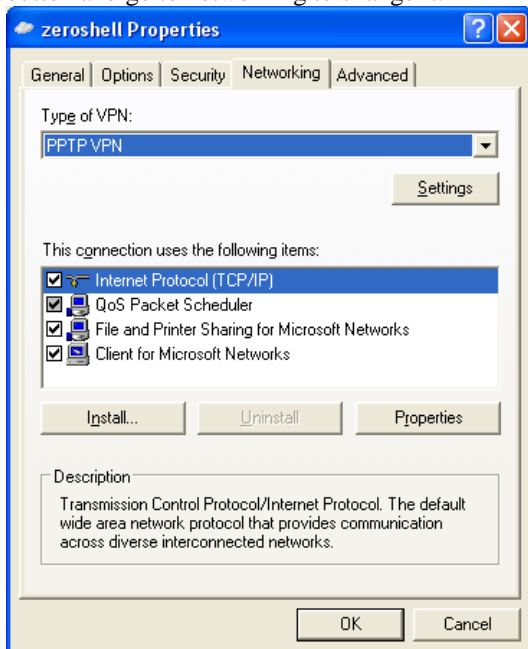
- Connect to the Internet.
- Connect to a private network, such as your workplace network.
- Set up a home or small office network.

To connect to a wireless network, view [wireless networks in range](#).

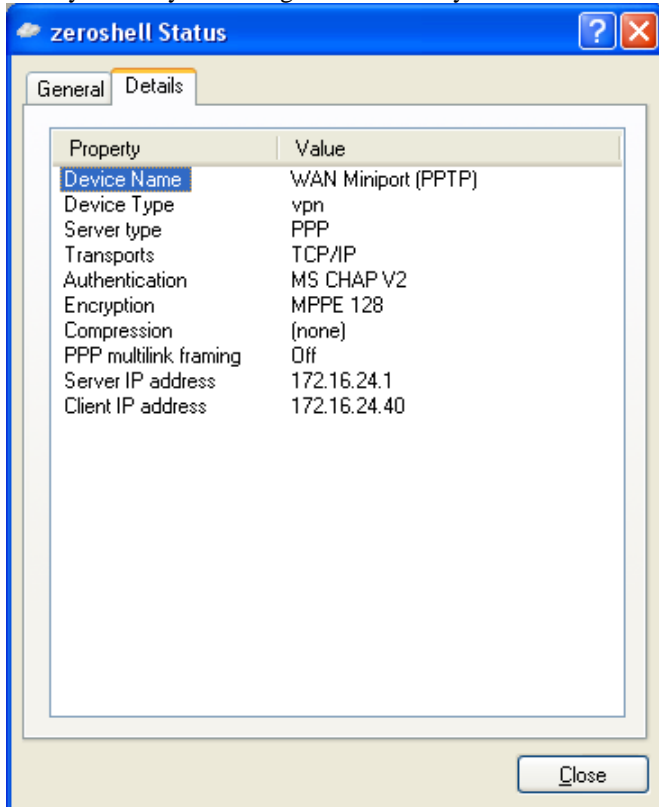
To continue, click Next.



The default connectoid will work automatically but if you need to specify PPTP session use the properties button and go to networking to change it.



After you save your settings connect with your default zeroshell admin account.



The End

Created by vpn_rollercoaster