ZeroShell Step-By-Step Setup for the Average SOHO User

V1.0

Created by Ben Wiper (bwiper@gmail.com) – http://nerdsonsite.chesterns.ca

Revision Log:

Date	Version	Changes
3/14/2011	1.0	First version

ZeroShell Setup Step-by Step – SOHO

Enterprise Features, Open Source Solution

Basic Install and Setup of Value-Add Services for the SOHO end user

This document outlines the basic setup of ZeroShell 1.00b14 services including PPPOE, INTERFACE SETUP, NAT, DHCP, DNS, DDNS, VPN (Password Authentication), HAVP

Prerequisites:

1. An older, reliable computer, possibly one recently phased-out of your IT environment day to day operations

Recommendation: P4 3.0GHz Lenovo/IBM ThinkCentre, 1GB RAM off-lease ($89-$129) or better

http://igadgetlife.com/desktops/ibm-thinkcentre-8171-refurbished-desktop-pc/

2. A PCI or USB 2.0 gigabit network adapter

Recommendation: Startech 1Gb/s PCI video card ($15-$20)

http://intrl.startech.com/product/ST1000BT32-10100-1000-Mbps-32-bit-PCI-Gigabit-Ethernet-Card

3. ZeroShell

http://www.zeroshell.net/eng/

USB Flash Image, or ISO images available – ZeroShell loads into a RAM disk, so only needed at boot time after configuration completed.

4. Pick your subnet wisely – if you want to use VPN, you should pick an obscure subnet like 10.99.122.0/255.255.255.0 – something that isn't a common subnet on store bought routers

Step 1: Get your NICs installed and setup

1. Install the Gigabit PCI Nic
2. Turn on the computer and go into the BIOS, disable halt on errors, disable all boot devices except CD/DVD Drive (or USB drive if you've burned the ZS image to USB), enable automatic start on power failure (your ZS should be plugged into a UPS!!)
3. Boot from the CD or USB drive to the console
4. Setup your slower NIC (if one is slower) to be your WAN adapter – configure it with the necessary IP address if static or automatic if your internet connection is Dynamic from ISP
5. Setup your gigabit NIC to be your LAN adapter and set it up on the desired subnet (I recommend using something obscure to avoid VPN issues later on – for the purpose of this instruction manual, let's use 10.99.122.0
6. With both NICs (WAN and LAN) setup, connect your computer to the router using a network cable and move to the next section

Step 2: Web Console: Setup a Profile and Activate It

1. Setup your wired NIC in a second computer with a static IP on the same subnet as your LAN interface
2. Open your web browser and browse to the LAN IP address (https://10.99.122.1:81) assigned to your ZeroShell Router and accept the security certificate warning – if problems connecting, remember step #1 in this section – the computer your using should be setup with static IP of 10.99.122.2 or higher!)
3. Login with root/zeroshell
4. Click on Setup, then choose Profiles
5. Find your hard drive or USB flash drive (not the same one as your ZS USB bootable drive!) in the list of drives and select the drive from the list using the radio button
6. Format the Drive to EXT3
7. Create a new profile on the drive and give it a name
8. Activate the profile and reboot when prompted
9. Now it's time to start the configuration!

Step 3: PPPOE (Optional) and NAT

If you're using PPPOE connection, start here, otherwise, jump to step 7.

1. Log back in to ZS
2. Go to Setup section -> Network
3. Click the "New PPPOE" button
4. Give the PPPOE connection a name, link it to your WAN adapter (ETH01 or ETH00)
5. Enter your PPPOE username and password, auto-start connection at boot: YES, NAT: Yes, Make Default Route: YES
6. Click Save
7. Now, in the Router section, go to the NAT tab
8. Add ETH00, ETH01, VPN99 (and ppp0 if using PPPOE) to the NAT enabled interfaces

9. Click Save

Step 4: DHCP, DNS, Virtual Servers

Now, let's setup your DHCP server for your workstations and other devices.

1. Click on the DHCP link in the left menu
2. Setup your DHCP Range 1 – 10.99.122.25 to 10.99.122.150 and click Save
3. Set your default gateway and DNS1 to your ZS LAN address (10.99.122.1)
4. Set DNS2 and DNS3 to use Google's DNS servers – 8.8.8.8 and 4.4.4.4
5. Setup any static IP addresses by clicking the Add button and entering the MAC address of the device and the static IP address on you 10.99.122.x subnet (make sure it is outside of the DHCP range!!)
    a. I recommend that any servers, wireless access points, and hard-wired devices on your network be setup with a static IP for optimal performance
6. Click Save
7. Disconnect your computer from the LAN port of your ZS box and connect the LAN Adapter to your switch
8. If you've configured everything correctly, you can now set your computer to obtain an address automatically (remove static IP on your computers LAN adapter) and connect directly to the switch and get an IP address from ZS now
9. If you're using Dynamic DNS (no static IP address) you should now go to the DNS section and click the Dynamic DNS tab
10. Check the enabled box, and enter your dynamic DNS host and account information and click Save – check the log to confirm it enabled properly (if it didn't the log will indicate that it did not, if it did work correctly, there will be no entries in the log)
11. Now, let's setup virtual servers – you may need this for remote access (RDP) or FTP server, or similar. Go to the Router link under Network in the left column and the Virtual Server tab. Let's assume we're setting up Remote Desktop and start by:
    a. Choose your WAN adapter interface (or PPPOE if using PPPOE)
    b. Set the protocol TCP/UDP, local and remote port of 3389 and IP address of the computer you want to remotely access
    c. Click the + button to add
    d. Repeat steps for each additional server service on your network

If you're setting up wireless access points, I recommend setting them up with static IP addresses, making sure DHCP is off and adding them to the static IP list on the DHCP section in the ZS Web interface.

Step 5: HAVP: (Transparent) HTTP Antivirus Proxy

This step is completely optional and not required. Enabling HAVP provides an extra level of security against viruses and malware.

1. Go to the HTTP Proxy link under the Security section in the left column
2. Check the Enabled Box and click Save
3. Wait 30-60 seconds while the service loads
4. For better performance, disable Image checking, set number of checks to 1 or 2 per day and set your antivirus update country
5. Now we need to add capturing rules by clicking the '+' sign in the HTTP Capturing Rules section. Recommended rules:
    a. Capture all requests on your WAN interface (or PPPOE if using PPPOE)
    b. Capture all requests on your LAN interface (10.99.122.0/255.255.255.0) or at least your DHCP range (for untrusted devices, assuming you've setup all your in office devices with static IP addresses)
6. Click SAVE

Step 6: VPN and Users

These steps outline how to setup a basic Password Authenticated VPN server. For additional security, you would want to setup and configure X.509 authentication, which is not covered in the basic setup.

1. Go to the VPN section under Network in the left column
2. Check the Enabled Box and click Save
3. Download OpenVPN from http://openvpn.net/index.php/open-source/downloads.html
4. After installing go to c:\program files\openvpn\config and edit the sample .ovpn file (or find one online. The line that you'll need to change is:
    a. remote zeroshell.mycompany.com 1194 to remote <your WAN IP or DDNS address> 1194
    b. and change line: "ca zeroshell.pem" to "ca <any name you want>.pem" and remember the name you set
    c. Save the Changes
5. Now, you need to generate your certificate .PEM file which you can do by:
    a. LogOut of ZS and then go back to login screen
    b. In the right side, click in the CA link under X.509 certificates
    c. In the pop-up window change the Export drop down to PEM and click on Export
    d. Copy the download CA.pem file to c:\program files\openvpn\config where your .ovpn file is
    e. Rename it to the same name you specified in step 4b) above
6. That's it! You can now use the VPN using your ZS admin account
7. If you want to add more users to ZS, go to the Users link on the left column and click the Add button. Enter the user details (username and password most important , most others will self populate when you save)

Notes:

i) You cannot test your VPN while on the same subnet as the ZeroShell VPN server
ii) VPN will not work if the subnet you are connected to is the same as the LAN subnet on the ZeroShell (that's why we chose an obscure subnet, 10.99.122.0)
iii) The same two files can be used for all users you've setup on ZS – they just have to provide their unique username and password when prompted by OpenVPN connection
iv) OpenVPN ***must be run as an Administrator*** on Windows Vista and Windows 7 for the connection to work (route.exe requires administrator permissions to run)

Step 7: QoS

While the QoS options are very broad with ZS, most users will only need a few basic classifiers. We'll go through one example of a high priority classifier and low priority classifier.

To setup QoS you must:

1. Login to ZS
2. Go to the QoS link in the left column and then select QoS Class Manager
3. In the pop-up click New and let's call this one "HIGH" for the name and set Priority to High in the drop-down
4. Now click on the Classifiers tab
5. Click on the Add button to add a new classifier, this example will be VoIP traffic that goes over port 63757
    a. Set source IP to your VoIP computer (eg. 10.99.122.10)
    b. Set Protocol Matching to TCP and set your source and destination port to 63757
    c. Set your Target Class to HIGH (created in Step iii)
6. Now go back to the Interface Manager tab and Turn QoS on your WAN, LAN (and PPPOE) interfaces by checking the "On" box and "Activate Changes" button
7. Now under each interface, click Add Class and add your VoIP classifier to each interface
8. Click the Activate Changes button
9. Repeat for any other QoS configuration needs.