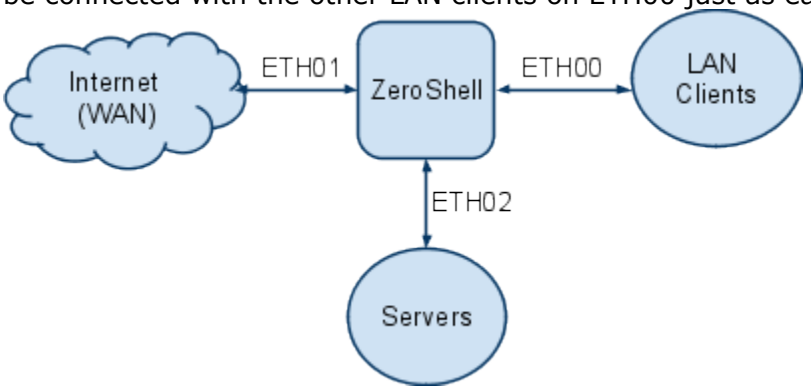
1:1 NAT in ZeroShell

Requirements

The version of ZeroShell used for writing this document is Release 1.0.beta11. This document does not describe installing ZeroShell, it is assumed that the user already has a configured, secured, tested, and working installation of ZeroShell.

Overview

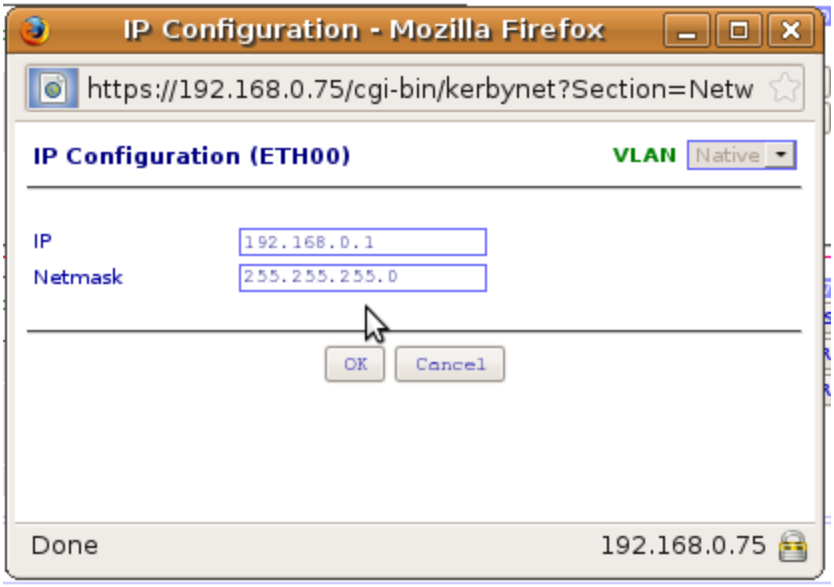
This document will walk through configuring ZeroShell as a router with 1:1 NAT for servers inside the Local Area Network (LAN) and Many:1 NAT/Masquerading for all other clients on the LAN. The LAN servers will be connected to ETH02, the other LAN clients will be connected to ETH00, and the Wide Area Network (WAN) will be connected to ETH01. Note that there is no restriction that the servers have to be on a separate interface; they could be connected with the other LAN clients on ETH00 just as easily.



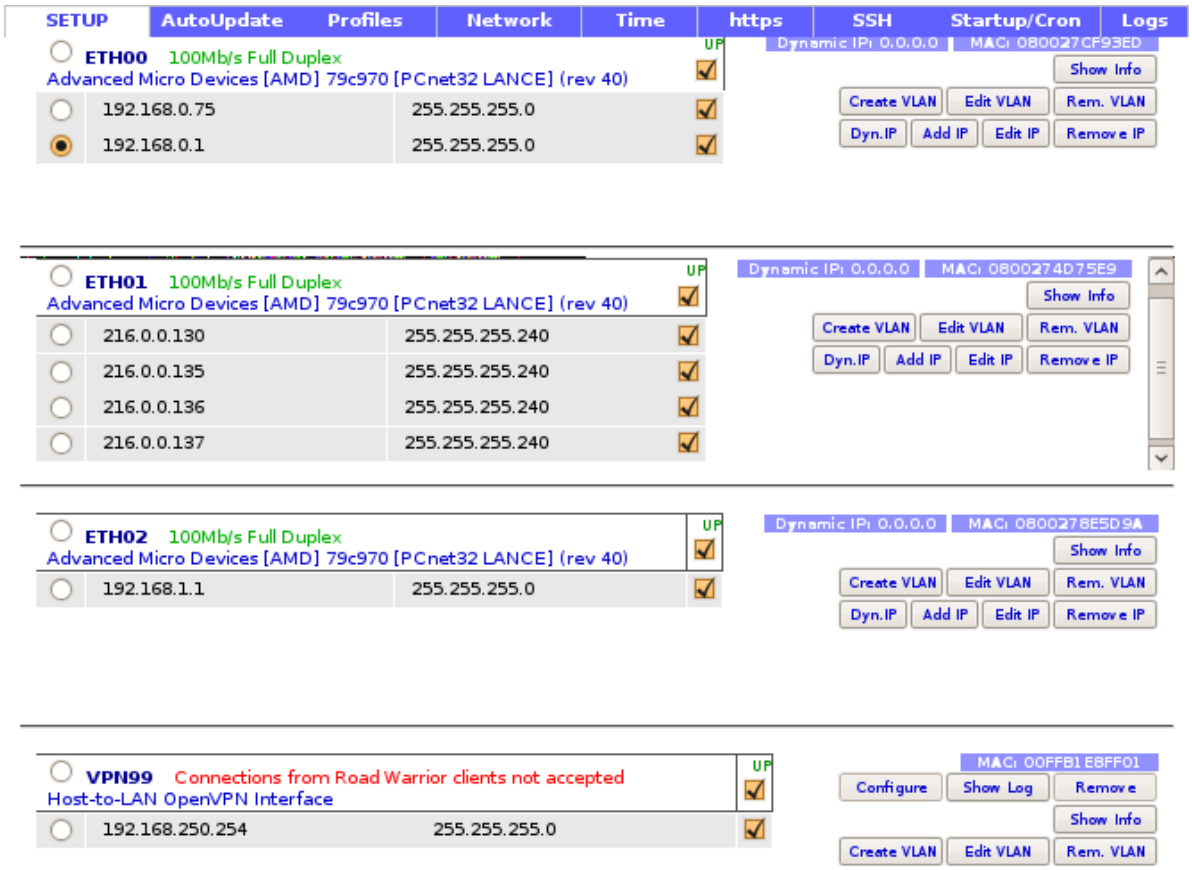
This example assumes that multiple public IP addresses are available on the WAN. One IP address will be used by ZeroShell and the Many:1 NAT for regular clients on the LAN. The rest of the IP addresses will also be used by ZeroShell, but translated for the 1:1 NAT for the servers. The servers are configured with private IP addresses.
In this example, the public IP addresses are assigned from the 216.0.0.129 network with a subnet mask of 255.255.255.240. The default gateway to the Internet is located at IP address 216.0.0.129. The LAN clients will use private addresses from 192.168.0.1 onward. The servers will use private addresses from 192.168.1.1 onward.

Network Setup

Log into the ZeroShell web interface, and click "Setup" under "System" from the menu on the left. Then, click the "Network" tab.
ETH00 will be used for our LAN clients, and ZeroShell will have an IP address of 192.168.0.1. To configure this, click the "Add IP" button and fill in "192.168.0.1" for the IP and "255.255.255.0" for the Netmask.



ETH01 will be used for the WAN connection. ZeroShell's "Primary" IP will be 216.0.0.130 with mask 255.255.255.240. For 1:1 NAT, we'll use the IP addresses from 216.0.0.135 through 216.0.0.137. Add the IP addresses the same way as before.
ETH02 will be used for the servers. In order for route traffic to/from this interface, ZeroShell must be configured with an IP on this subnet. Add the IP address "192.168.1.1" with subnet mask 255.255.255.0 here.
When finished, the Network Setup should looks similar to the following:



The final network setup step is to configure the Default Gateway by clicking the "GATEWAY" button at the top and entering the WAN router's IP address of 216.0.0.129.

1:1 NAT Setup

Under the Setup menu under "System", click the "Startup/Cron" tab. Then select the "NAT and Virtual Servers" script.
For 1:1 NAT to work properly, we must add two rules by using the Linux "iptables" command. The first set of rules will translate inbound connections from the WAN to the private IP addresses of the servers before sending the packets for routing. The second set of rules will translate the outbound traffic from the private IP addresses of the servers back to their respective public WAN IP addresses. Failure to add the second set of rules will cause ZeroShell to send all outbound traffic from the "primary" public IP address of 216.0.0.130 later when Many:1 NAT is configured.
For this example, we will translate the IP addresses according to the following table:

Public (WAN) IP	Private (LAN) IP
216.0.0.135	192.168.1.35
216.0.0.136	192.168.1.36
216.0.0.137	192.168.1.37

To do this, input the following into the script:

```
# Translate incoming connections to the private server addresses
iptables -t nat -I PREROUTING 1 -d 216.0.0.135 -i ETH01 -j DNAT --to-
destination 192.168.1.35
```

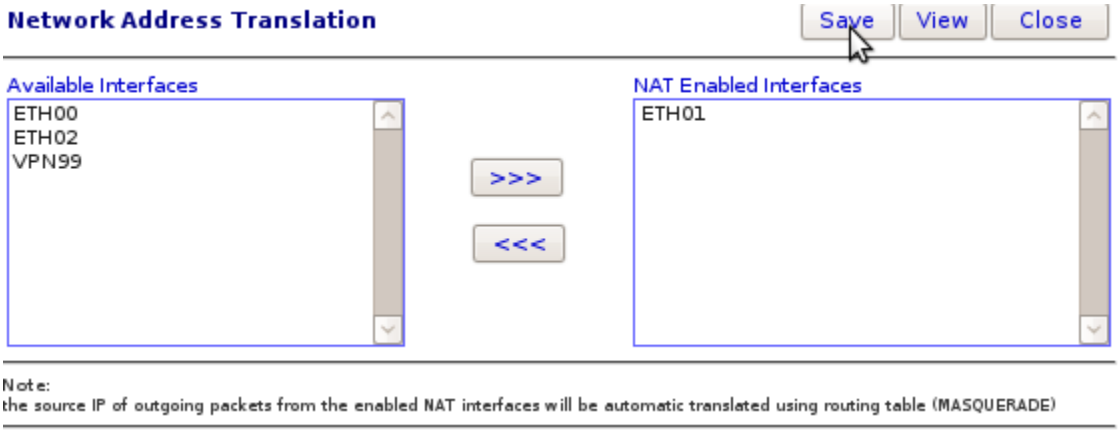
```
iptables -t nat -I PREROUTING 1 -d 216.0.0.136 -i ETH01 -j DNAT --to-
destination 192.168.1.36
iptables -t nat -I PREROUTING 1 -d 216.0.0.137 -i ETH01 -j DNAT --to-
destination 192.168.1.37

# Translate outgoing connections from the private server addresses
iptables -t nat -I POSTROUTING 1 -s 192.168.1.35 -o ETH01 -j SNAT --to-
source 216.0.0.135
iptables -t nat -I POSTROUTING 1 -s 192.168.1.36 -o ETH01 -j SNAT --to-
source 216.0.0.136
iptables -t nat -I POSTROUTING 1 -s 192.168.1.37 -o ETH01 -j SNAT --to-
source 216.0.0.137
```

When finished, click the "Test" button to ensure no errors were made. Then select the box to enable the script and then click "Save" to close the script editor.
Note that the -I (Insert) option was used rather than -A (Add) to insert the rule at the beginning of the table. This is necessary since this script is run after ZeroShell has configured its own rules. Failure to insert these rules at the beginning of the table would result in ZeroShell's own masquerading rules to take precedence over the 1:1 NAT configuration.

Many:1 NAT Setup

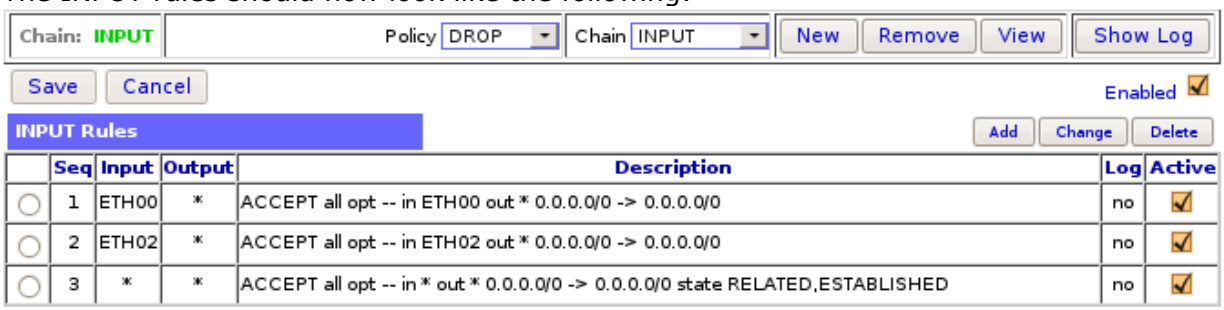
Under the "NETWORK" section on the left menu, click "Router". Click on the "NAT" tab to open up the Network Address Translation window.
This window is used to configure which network interfaces will have all outgoing traffic NAT'ed/masqueraded. In this example, select "ETH01" from the available interfaces and click ">>>" to add it to the NAT Enabled Interfaces. Then click the Save button.



Firewall Setup

Now that the network address translation and router is configured, the firewall should be configured to help secure the network. The Firewall rules in ZeroShell can be very advanced, so only a simple configuration is shown here. Note that this sample configuration has not been production tested to ensure proper security. Also note that making errors on the firewall rules could result in being locked out of the ZeroShell web interface.

First, we want to configure access to the ZeroShell router itself to only be allowed from the LAN.
Under "SECURITY", click "Firewall". Select the "INPUT" chain. Click "Add" and set the Input to "ETH00", changing nothing else, and click Confirm. This rule will permit all traffic from the ETH00 LAN to anywhere on the box.
Next, click "Add" and set the Input to "ETH02" and click Confirm. This rule permits all traffic from the server LAN on ETH02 to anywhere on the box.
For the last rule, click "Add", and check only "ESTABLISHED" and "RELATED" under "Connection State", then click Confirm. This rule will permit response traffic from established connections to the box to wherever they originated.
Click "Save" to make the new input active, then change its policy from "ACCEPT" to "DROP" so the rules actually take affect.
The INPUT rules should now look like the following:



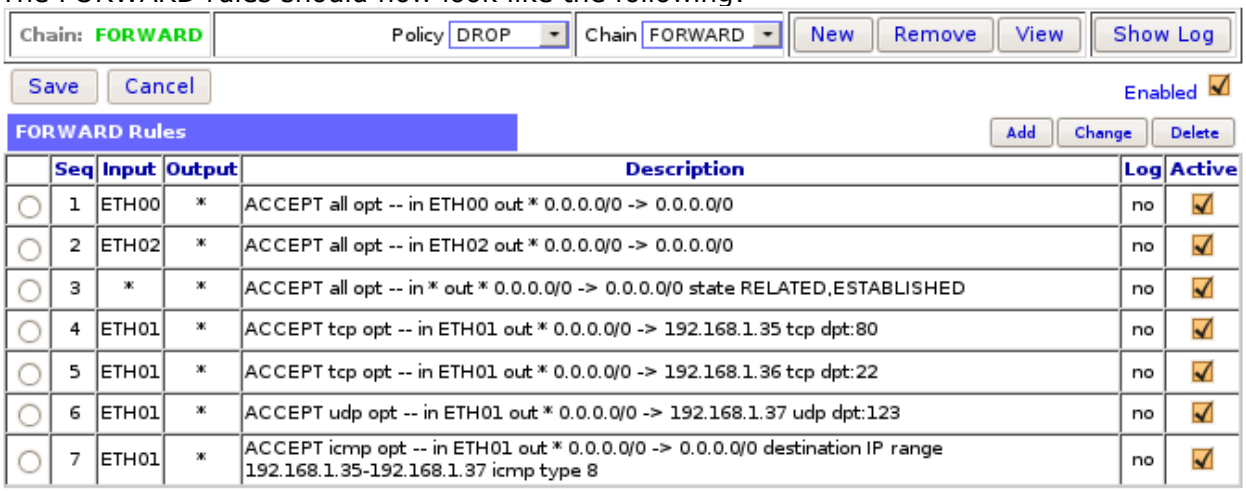
	Seq	Input	Output	Description	Log	Active
○	1	ETH00	*	ACCEPT all opt -- in ETH00 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	2	ETH02	*	ACCEPT all opt -- in ETH02 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	3	*	*	ACCEPT all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 state RELATED,ESTABLISHED	no	☑

Now, we want to configure ZeroShell's "Forwarding" firewall rules. This is where you will protect your servers and LAN clients from the public network. Select the "FORWARD" Chain to show its firewall rules. Here, we will set up simple rules to permit all outgoing traffic originating from the LAN to the Internet (WAN), and open up a few ports on our 1:1 NAT'ed servers to be accessible from the Internet. Traffic between the two LAN ports (ETH00 and ETH01) will be unrestricted.
Click "Add" and set the Input to "ETH00", then click Confirm. This allows unrestricted traffic from the LAN to anywhere the ZeroShell box can route (WAN and Server LAN).
Click "Add" again and set the Input to "ETH02", then click Confirm. This allows unrestricted traffic from the server's LAN to anywhere (WAN and Server LAN).
Click "Add" again and check the boxes for "ESTABLISHED,RELATED" under "Connection State". This will permit two-way communication for established connections initiated by the previous two rules.
Now, we want to open up some ports for our 1:1 NAT'ed servers so they can be accessed from the Internet. The follow table shows which ports need opened up for this example:

Public IP	**Private IP**	**Protocol**	**Port**
216.0.0.135	192.168.1.35	TCP	80
216.0.0.136	192.168.1.36	TCP	22
216.0.0.137	192.168.1.37	UDP	123
(all)	(all)	ICMP	(ping)

Click "Add", set Input to "ETH01", Destination IP to "192.168.1.35", Protocol Matching to "TCP", and Dest. Port to "80". Click Confirm.
Click "Add", set Input to "ETH01", Destination IP to "192.168.1.36", Protocol Matching to "TCP", and Dest. Port to "22". Click Confirm.
Click "Add", set Input to "ETH01", Destination IP to "192.168.1.37", Protocol Matching to "UDP", and Dest. Port to "123". Click Confirm.
Click "Add", set Input to "ETH01", Destination IP to "192.168.1.35-192.168.1.37", Protocol Matching to "ICMP", and ICMP Type to "echo-request (ping)". Click Confirm.

Now, click "Save" to make the new rules active, and change the Policy to "DROP" so the rules actually take affect.
The FORWARD rules should now look like the following:



	Seq	Input	Output	Description	Log	Active
○	1	ETH00	*	ACCEPT all opt -- in ETH00 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	2	ETH02	*	ACCEPT all opt -- in ETH02 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	3	*	*	ACCEPT all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 state RELATED,ESTABLISHED	no	☑
○	4	ETH01	*	ACCEPT tcp opt -- in ETH01 out * 0.0.0.0/0 -> 192.168.1.35 tcp dpt:80	no	☑
○	5	ETH01	*	ACCEPT tcp opt -- in ETH01 out * 0.0.0.0/0 -> 192.168.1.36 tcp dpt:22	no	☑
○	6	ETH01	*	ACCEPT udp opt -- in ETH01 out * 0.0.0.0/0 -> 192.168.1.37 udp dpt:123	no	☑
○	7	ETH01	*	ACCEPT icmp opt -- in ETH01 out * 0.0.0.0/0 -> 0.0.0.0/0 destination IP range 192.168.1.35-192.168.1.37 icmp type 8	no	☑

Finishing Up

Configure the servers connected to ETH02 with appropriate IP addresses and set their Default Gateway to ZeroShell's IP Address of "192.168.1.1". Do the same with the LAN clients on ETH00, except their Default Gateway is "192.168.0.1". Or, configure ZeroShell's DHCP servers to do the same (instructions for this is beyond the scope of this document). Now, click on the Reboot link to restart ZeroShell to ensure everything still works after restarting. Test both incoming connections and outgoing connections to your servers to ensure the 1:1 NAT is working properly. Confirm that the Port Forwarding and Source NAT table looks correct following by clicking "Router", "NAT", then "View":

Port Forwarding and Source NAT (NAT)

```
Chain PREROUTING (policy ACCEPT 30 packets, 1560 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       all  --  ETH01  *       0.0.0.0/0            216.0.0.137         to:192.168.1.37
    0     0 DNAT       all  --  ETH01  *       0.0.0.0/0            216.0.0.136         to:192.168.1.36
    0     0 DNAT       all  --  ETH01  *       0.0.0.0/0            216.0.0.135         to:192.168.1.35

Chain POSTROUTING (policy ACCEPT 4 packets, 511 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 SNAT       all  --  *      ETH01   192.168.1.37         0.0.0.0/0           to:216.0.0.137
    0     0 SNAT       all  --  *      ETH01   192.168.1.36         0.0.0.0/0           to:216.0.0.136
    0     0 SNAT       all  --  *      ETH01   192.168.1.35         0.0.0.0/0           to:216.0.0.135
   91  5451 SNATVS     all  --  *      *       0.0.0.0/0            0.0.0.0/0
   87  4940 MASQUERADE  all  --  *      ETH01   0.0.0.0/0            0.0.0.0/0

Chain SNATVS (1 references)
 pkts bytes target     prot opt in     out     source               destination
```