IPFire DMZ

Setting up a DMZ in IPFire is slightly more complex than most tasks in this excellent distribution.

My situation is this. I have several IP's, some of which are attached to machines with external IP's, some are unused, and some are in the DMZ (Demilitarized Zone).

If you're not familiar with a DMZ, it is basically a hybrid between putting a machine “on the wire” (give it a direct public IP) and using NAT to go to an internal private IP. With a DMZ, you create a completely different subnet in a private IP range, and the router translates external IP's to it. However, machines on the DMZ can not directly talk to other machines on the DMZ, and those machines can not talk to machines in your internal LAN. However, machines on your internal LAN can talk to machines on the DMZ.

To set up an external IP on the DMZ, do the following. NOTE: the external IP must be in the subnet of he external IP of the router. So, if you have 192.0.2.0/24 (ie, range of 192.0.2.1-192.0.2.254) and your router is at 192.0.2.1, the other IP's must be within the range. BTW, 192.0.2.0/24 is a testing IP range that should never be used in any real world application.

So, we assume you have set up your IPFire firewall/Router on 192.0.2.1 with a subnet of 255.255.255.0. Also, let's assume you have the DMZ set up for 10.0.0.0/24, with your IPFire appliance having the IP of 10.0.0.1 and a subnet of 255.255.255.0. We're going to add a new server which will have an external IP of 192.0.2.5, and it's DMZ address will be 10.0.0.5. I like to keep the last octet the same for simplicity.

On the IPFire appliance, go to Network | Aliases and create a new entry. The name is only a label, but you can put your server's name in there. Put the Public IP (192.0.2.5) in the Alias IP, put a check in the Enabled box, and click the the Add button. Your firewall will now respond to that IP.

We need to create two firewall rules, one to route the public IP to the DMZ IP, and one to let the DMZ IP talk back to the public one. I name these dmz and snat respectively.

Firewall | Firewall Rules

1. Click 'New Rule' Button
    1. Source - Standard networks any
    2. NAT - Use network Address Translation
        1. Destination NAT (port forwarding)
            1. Firewall Interface, choose your server from the list
    3. Destination
        1. Destination Address - 10.0.0.5
    4. Protocol - All
    5. Remark - dmz servername
    6. Activate Rule - put check in it
    7. Click Update button
2. Click 'New Rule' Button
    1. Source Address - 10.0.0.5
    2. NAT - Use network Address Translation
        1. Source Nat
            1. choose server from list

    3. Destination
        1. Standard Networks - any
    4. Protocol - All
    5. Remark - snat servername
    6. Activate Rule - put check in it
    7. Click Update button
3. Click Apply Changes button

Your firewall is now set up. Go to your server and assign it an IP address of 10.0.0.5. Once you have done this, you should be able to ping 10.0.0.1 and any external IP address (ie, google at 8.8.8.8).

Now, you should be able to go outside your network and use your server at 192.0.2.5, and also address it from inside your LAN (behind the same firewall).