How do I setup a firewall on my Fedora ?

Even though many people purchase firewall/router appliances nowadays these are often severely limited and don't offer the functionality that a more fully featured system provides. For instance, there is no little chance of upgrading the firware should the manufacturer suddenly decide not to support your particular piece of hardware, upgrades when new threats arise are only provided by a single source, and finally a lot of the time there tends to be very limited functionality in a hardware firewall unless you run a enterprise class firewall which is one of the reasons why many people elect to run a Linux or a Fedora system as a firewall/router/gateway system between their local network and the Internet.

Hence, this article will attempt to outline the basic steps towards building a firewall via Fedora.

What is a firewall?

A firewall is basically a means of keeping out the bad and only allowing the good into your computer system or local network. For the most part configuring a firewall is like opening and closing a series of doors of a very large house. Moreover, just like the doors of a house you are able to stop people from coming both into and out of the house. For example, if you wanted to stop people from being able to access the Internet from your system you could block people by implementing a rule that stops outbound connections on port 80. Moreover, if you find out that people are suddenly attempting to mischievously access your system from outside via then you also have the ability to lock your system down by either uninstalling the programs from your particular server themselves or else implementing firewall rules that will stop them prior to even being the service running on your Fedora system.

Moreover, you can even change the way in which your system will respond to certain responses. For example, you can actively reject a connection request, you can "blackhole" it, re-route it, and of course you can allow it through so that other people can access services on your machine (for instance, it is necessary to open port 25 (2525 for some ISP's though because they are overly paranoid and believe that blocking access on this port will slow down the spread of SPAM) in order to allow correct delivery of email to your local system).

By utlizing your rules properly you may also be able to use your Fedora system as a router as well! For instance, you can use it as a gateway between your local network and the rest of the "Internet".

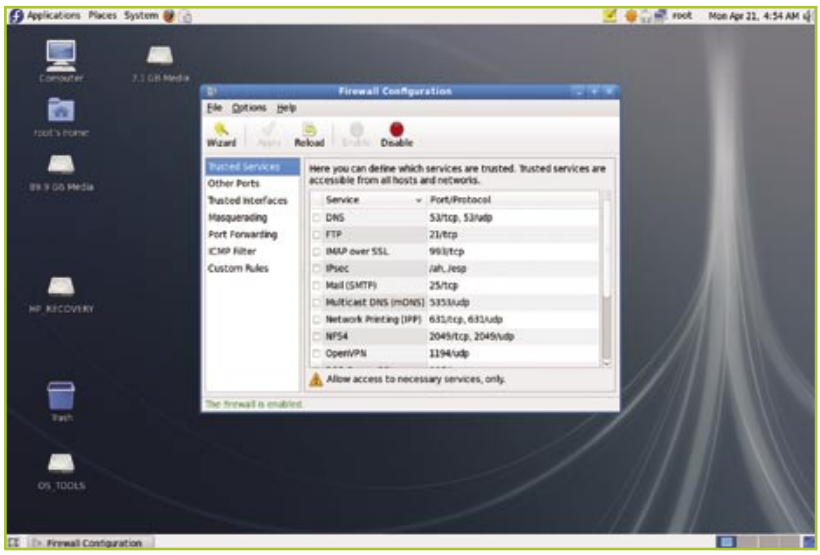

Figure 1. *Firewall configuration - Fedora style*

A quick guide to getting a firewall up and running

The most basic means by which to commence building a firewall via Fedora would be by going to *System –> Administration –> Firewall.* As you'll discover by the prompt this interface is a very basic front end to the much more powerful "iptables" firewall backend. (Note that you'll sometimes come across the "ipchains" term which is essentially the predecessor to "iptables" which is the most commonly used firewall system on Linux systems nowadays (should be noted that the front end systems to manage firewalls across various different Linux distributions varies quite drastically though)). You'll also find that the program can also be run in two modes, one being "beginner" and the other being "expert". To toggle between them just go to *Options –> User Skill Level –> [Beginner | Expert]*. The default is *Expert*.

Moreover, you may also discover that your system is most likely going to already have the firewall enabled already. In most cases, though you'll discover that access to these services is going to be disabled to the outside world (and even within your local network) due to the stringent security policies that are already present within the default installation of Fedora. As such, even if you have a web server running on your machine nobody will be able to access it unless you create a rule which permits access to other people.

Obviously, the easiest way to get around this issue would be to disable your firewall completely by hitting the *Disable* and *Apply* buttons. However, you will then lose the security of your firewall. Hence, we will attempt to show you how to poke a hole in your firewall without reducing the overall integrity of your system. To do so just check the relevant box in the *Trusted Services* section in the *Firewall Configuration* window and hit the *Apply* button.

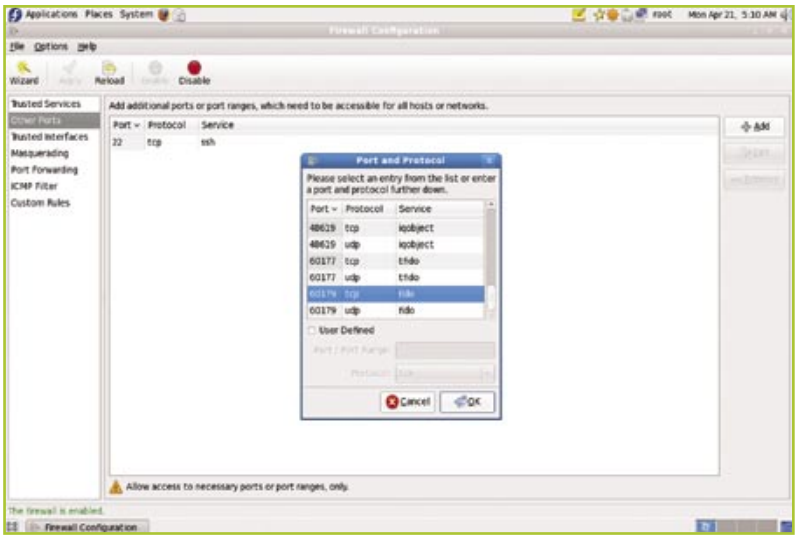

Figure 2. *Every dog needs to be let out for some exercise every once in a while*

On the other hand, if you would like to open a hole in your firewall to a rather obscure service that doesn't appear in the *Trusted Services* section of the console then click on *Other Ports* and click on the *Add* button to create a new rule for your firewall (in a lot of cases, you'll notice that there are multiple protocols for each service. If you are unsure which one to select enable them all and then remove them one by one until you work out which protocol is being used). In this case, we'll be choosing "fido" as our example. Finally, click *Apply* to make sure that the rule is being run.

If this all seems very arduous to you there is of course an easier way. For instance, let's say your system is being run as a gateway between the Internet and your local network which means that, you can trust all traffic coming from one side but not the other side. In order to allow all traffic to come through to your system on one side click on *Trusted Interfaces*. Check the box next to the relevant interface (we'll be using eth0 in this example) and click *Apply*.

If that's not enough functionality for you, your Fedora box can also act as a single point of contact of contact to the rest of the world on behalf of your local network which means that your entire network will be provided with some additional protection. The process for doing this is largely identical to adding a Trusted Interface. First go to Mas-

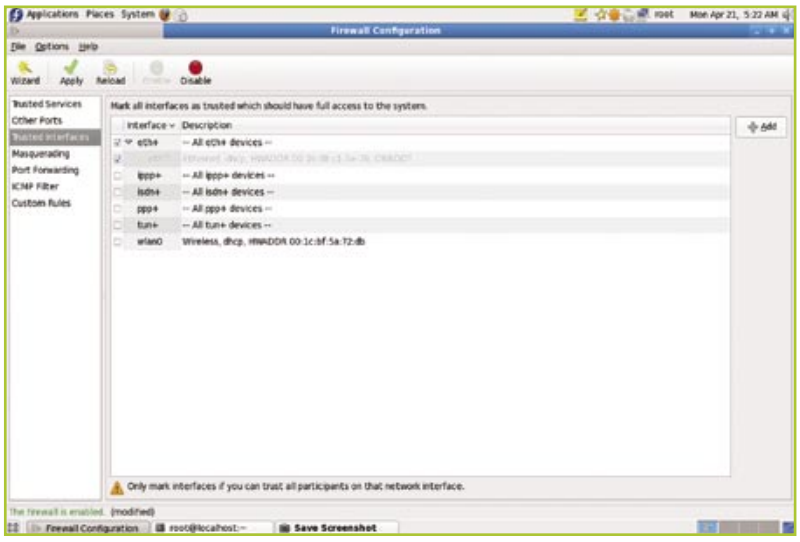

Figure 3. *You can only trust so many interfaces nowadays*

querading, click on the checkbox on the relevant interface. Finally hit the apply button. A good overview of how the theory works is available here, *http://lindesk.com/category/distros/fedora/*. This means that any attempts to connect to the outside world will from within your local network will appear to come from your Fedora box but when the actual data comes back from the "outside" your Fedora box will translate the data to make it appear as though the local computer was being directly served by the outside world. Please note that Masquerading only works if the internal network uses IPv4 addressing. The easiest way to determine this is by looking at the IP address of the network interface cards on your machine. To do this right click on the computer icon in the top right hand corner of the GNOME taskbar. Select *Connection Information*. If the address is entirely in decimal notation then its likely that you're on an Ipv4 network (more information on Ipv4 and Ipv6 is available at *http://en.wikipedia.org/wiki/IPv4* and *http://en.wikipedia.org/wiki/IPv6* respectively).

Finally, there's one other option that may prove to be useful to some users. That is, the notion of port forwarding. Let's say you have a router in front of your Linux box that is attached to the Internet. Your Linux box is then masqueraded to be the only system that is connected to the Internet. What happens if someone attempts to connect to a web server that is on your Fedora gateway which is not present? Obviously, they'll be unsuccessful...

This is where the notion of port forwarding comes in. If another system on your network has a web server running on it you can forward web requests from outside to your Fedora box which then forwards this request to the local system on your network. It will then do some translation so that the webpage then appears as though it came directly from the Fedora box.

To do this click on *Port Forwarding*. Then click the *Add* button and add in the relevant details. In the example provided below we will be forwarding all requests from the eth0 network interface to 192.168.1.107. Finally, click *Apply*.

Other ways to configure your firewall

Another way is to use a pseudo-system in order to attempt to build a firewall system, *http://www.fwbuilder.org*. You basically attempt to build the firewall by using diagrams which represent various abstract representations of networking devices in your system. Then the program will itself create the actual "iptables" rules which you will have to manually run on your own system.

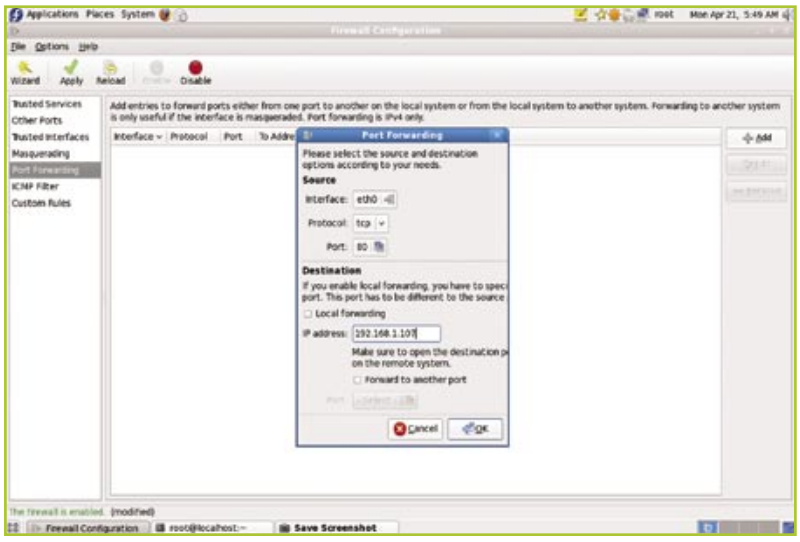

Figure 4. *Forwarding to a more appropriate machine*

Finally, you can actually configure the firewall yourself by using manual "iptables" rules. Good guides are available at the following locations.

- *http://iptables-tutorial.frozentux.net/iptables-tutorial.html*
- *http://linux.ardynet.com/ipmasq/ipmasq.php3#iptables*
- *http://en.wikipedia.org/wiki/Iptables*

In most cases, this is the options that most people will want to avoid as it is prone to error because reading the rules can be difficult at times due to the large amount of vocabulary involved in the language.

Troubleshooting

If you receive an error from SELinux stating that this rule has been disallowed then *start system-config-selinux* by hitting [*Alt*] + [*F2*] typing in this command and then hitting *OK*. Select *Status*, and finally reduce the *Enforcing Mode* from *Enforcing* to *Permissive* or *Disabled* (you'll have to reboot if you choose the *Disabled* option).

If you are unable to connect to a service please ensure that the service is installed and running first prior to testing and that there isn't an intermediate device in between that is interfering with the your firewall rules.

Conclusion

Even though configuring a firewall can be be difficult there is no doubt that a Fedora system possesses many capabilities that a conventional firewall/router appliance does not. First of all, you already have and don't have to purchase another device in order to use. Second you're actually able to upgrade the system. Finally, you're not limited in what you can actually do with it since it possesses many of the same capabilities that many higher end "enterprise" firewalls already have at a fraction of the price.