FIRERACK

FireRack

On-site Installation Guide

Revision: rfs-050816-2

Table of Contents

Introduction

Default Configuration

In most cases, your FireRack firewall will have been pre-configured for you by your service provider. If at the time of purchase you were asked to provide IP addresses for your Ethernet interfaces and logon details for ADSL/DSL connections (if any), these will already have been set-up for you.

If the FireRack has been correctly pre-configured, you will not need to make any manual changes to it. As long as your FireRack can communicate with it's FireRack Management Server (FMS) from boot-time, all further changes should be made on the FMS.

If your FireRack is already correctly configured, please DO NOT follow the instructions in this document.

Management Console and FMS

The FMS (FireRack Management Server) is a server that manages one or more (possibly hundreds) for FireRack firewalls. Running on the FMS is a secure web site referred to as the FireRack Management Console. Only updates made via the FMS are persistent.

Once communication between the FireRack firewall and the FMS has been established, all further configuration changes should be made using the FMS.

Why override the Default Configuration?

Only if the installed configuration is insufficient to get you on-line, you will have to override the default configuration. Once online, you will be able to permanently update your firewalls configuration using the Management Console on the FMS.

The FMS does not have to reside on the same network as the firewall. If you have not purchased your own FMS, you will be using an FMS provided by your service provider. If this is the case, we merely need to establish an Internet connection in order to communicate with the FMS.

Connecting to the local console

Overview

In order to interrogate and reconfigure the FireRack, you will have to connect to it using one of the following methods:

- SSH (Secure Shell)
- Serial Console
- VGA (On some models)

We strongly recommend that you use either the Serial console, or VGA Console. Even if SSH is available to you and working, it may well cease working during the reconfiguration of the firewall.

For each of these methods you will need to know the “root” password of the FireRack. This will be given to you by your service provider.

SSH

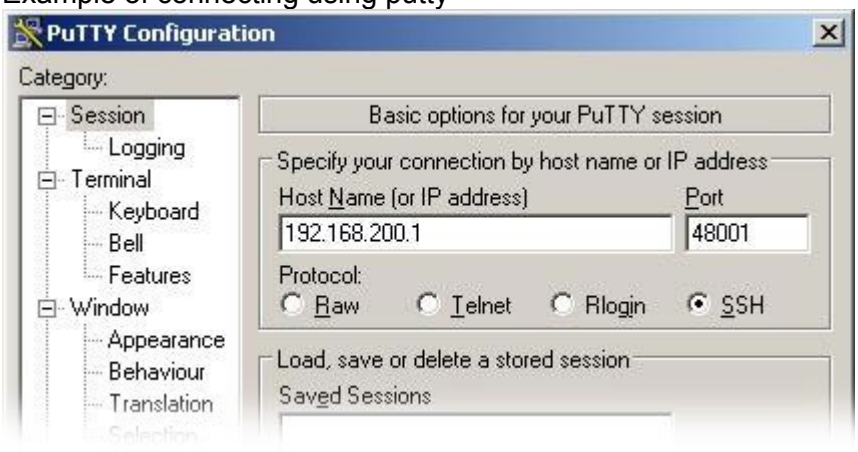
In order to use SSH you must:

a. Know the IP address of the FireRack.
b. Have a workstation with IP connectivity to the FireRack.
c. Have an SSH client (e.g. Putty) installed on the workstation… and
d. Connect from and IP address and network that the FireRack will permit to establish an SSH connection (governed by firewall rules).

You may have to consult with your service provider in order to satisfy these requirements. It may well be that the supplied configuration does not permit SSH access at all. If however these conditions can be satisfied, read on.

FireRack firewalls listen for SSH connections on port 48001 (not port 22).

Example of connecting using putty -



Example of connecting using openssh-client -

```
workstation:~$ ssh -p 48001 root@192.168.200.1
```

Serial Console

Using a null-modem cable and terminal emulation program such as Hyperterminal or Minicom, you can connect to your FireRack's serial console. The connection settings are as follows:

Bits per second (Bps)	38400
Data bits	8
Parity	None
Flow control	Hardware
Terminal Emulation	VT100 / VT102

On standard FireRack hardware there is only one external serial port. On other hardware platforms, simply connect to the first serial port (COM1).

VGA Console

Although, standard FireRack hardware does not include a VGA console, other platforms may do. FireRack does support logging in using a standard VGA monitor and PS/2 keyboard if they are present. Please note however, the use of a VGA console on FireRack is an unsupported feature (i.e. no technical support).

Logging on

Regardless of the method of connection, logging on to and using the local console is same.

You will be prompted for a login and password. The login to use is "root". The password will have been given to you by your service provider.

Example:

```
Welcome to NetServers FireRack (xxxxxx branch, version rfs-xxxxxx-
1)

firewall.yourdomain.com login: root
Password:
Last login: Thu Aug 10 10:00:58 +0100 2005 on ttyS0.

firewall:~#
```

Overview of hardware

This document deals only with the configuration of Ethernet interfaces, and does not cover the configuration of ISDN or ADSL interfaces.

Your FireRack firewall will have two or more Ethernet interfaces. On typical FireRack hardware these ports will be labelled E0, E1 and so on. This notation is an abbreviation of the port's logical name of eth0, eth1 etc.

The ports may additionally be labelled with real-world names such as "Internal", "External" and "DMZ". It is important however to note that as far as FireRack is concerned these real-world names are meaningless. Any Ethernet port can serve any purpose. How it functions is entirely dependent on how it is configured (IP address etc.) and what the routing table of the firewall looks like.

For the purposes of this document, we will be referring to ports by their "logical name". The first Ethernet port is always called "eth0", the next "eth1" etc. Which Ethernet port you use as your Internal, External etc. is up to you.

Before proceeding any further, you should ensure that your Ethernet ports link LEDs are lit.

Overview of tools and commands

The following are a number of command line tools available in the console that you will need to be familiar with:

- ifconfig
- route
- ping
- traceroute
- mii-tool

ifconfig - configure a network interface

This tool is used to inspect and change the IP address, and subnet mask (netmask) of an interface. To inspect the settings for your eth0 interface do the following:

```
firewall:~# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:10:09:01:6E:73
          inet addr:80.201.205.108  Bcast:255.255.255.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60737279 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65794814 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3605473252 (3438.4 Mb)  TX bytes:3233231229 (3083.4 Mb)
          Interrupt:12 Base address:0x9000
```

The important data above (highlighted) is the IP address (inet addr) and the Subnet Mask (Mask).

route - show / manipulate the IP routing table

The route command allows you to inspect and manipulate the routing table of your FireRack. To inspect the current routing table do the following:

```
firewall:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
80.201.205.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.200.0   0.0.0.0         255.255.255.0   U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         80.1.201.254    0.0.0.0         UG    0      0        0 eth1
0.0.0.0         0.0.0.0         0.0.0.0         U     1      0        0 ipsec0
```

You may or may not have the ipsec0 route shown above. This is present whenever the ipsec service is running and configured. In most circumstances, it can safely be ignored.

ping - send ICMP ECHO_REQUEST to network hosts

Unlike the Windows ping command, the Linux ping command pings continuously by default. To cancel a ping command, just press CTRL-C. To send a fixed number of pings you would use the –c (count) option. For example:

```
firewall:~# ping -c 5 www.google.com
PING www.l.google.com (66.102.7.99) 56(84) bytes of data.
64 bytes from 66.102.7.99: icmp_seq=1 ttl=236 time=166 ms
64 bytes from 66.102.7.99: icmp_seq=2 ttl=236 time=168 ms
64 bytes from 66.102.7.99: icmp_seq=3 ttl=236 time=165 ms
64 bytes from 66.102.7.99: icmp_seq=4 ttl=236 time=165 ms
64 bytes from 66.102.7.99: icmp_seq=5 ttl=236 time=167 ms

--- www.l.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4043ms
rtt min/avg/max/mdev = 165.597/166.768/168.268/1.046 ms
```

traceroute - print the route packets take to network host

In order to detect the precise point of failure in your connectivity to a remote host, you would use traceroute. Normally traceroute performs a DNS lookup on the IP address of each router en-route. To turn this behaviour off, simply use the –n (numeric) option. Like so:

```
firewall:~# traceroute -n 217.32.244.70
traceroute to 217.32.244.70 (217.32.244.70), 30 hops max, 40 byte packets
 1  213.105.172.149  18.618 ms  41.889 ms  13.700 ms
 2  62.253.188.106  15.052 ms  15.123 ms  15.972 ms
 3  194.74.65.21  14.961 ms  14.999 ms  15.144 ms
 4  194.74.65.197  14.470 ms  16.521 ms  20.342 ms
 5  62.6.196.217  16.744 ms  14.841 ms  15.979 ms
 6  62.6.197.134  16.628 ms  20.124 ms  15.182 ms
 7  217.32.244.70  17.396 ms *  15.914 ms
```

mii-tool – view and manipulate interface status

This enables you to inspect the link status and speed of your Ethernet interfaces. To show both the speed and link status of all your Ethernet interfaces type:

```
firewall:~# mii-tool
eth0: negotiated 100baseTx-FD flow-control, link ok
eth1: no autonegotiation, 10baseT-HD, link ok
```

For additional help on using the tool type:

```
firewall:~# mii-tool --help
usage: mii-tool [-VvRrwl] [-A media,... | -F media] [interface ...]
       -V, --version               display version information
       -v, --verbose               more verbose output
       -R, --reset                 reset MII to poweron state
       -r, --restart               restart autonegotiation
       -w, --watch                 monitor for link status changes
       -l, --log                   with -w, write events to syslog
       -A, --advertise=media,...   advertise only specified media
       -F, --force=media           force specified media technology
media: 100baseT4, 100baseTx-FD, 100baseTx-HD, 10baseT-FD, 10baseT-HD,
       (to advertise both HD and FD) 100baseTx, 10baseT
```

Other tools

There are many more command-line tools on FireRack. Too many to go into in this document. Experienced users might be interested is using some of the following:

- nmap – a port scanner
- arping – send arp requests to detect firewalled or misconfigured machines
- tcpdump – Packet Sniffer
- ngrep – Packet Sniffer with “grep” functionality
- iptraf – IP Network Statistics Utility
- garp – Gratuitous ARP sending utility (Sorts out Cisco router ARP cache issues)
- telnet – a telnet client
- ssh – openssh client
- dig – DNS interrogation tool

Overriding the default configuration

Objectives

Our primary objective is to establish connectivity between the FireRack and its FMS. If this FMS is off-site, we will be concentrating on getting a working Internet Connection. If the FMS is on the local network (LAN), we will be focusing on out internal network.

After successfully connecting the FireRack to the Internet, the configuration must be updates on the FMS Management Console, and a new configuration must be "pushed". This will then lock-in the changes to the network configuration.

As a secondary objective, you may want to provide Internet access for your internal network. If, for instance, the FMS was remote (on the Internet) and your only means of accessing it was via the FireRack, having Internet access would become essential.

If your FireRack is already correctly configured, please DO NOT follow the instructions below.

Example

In the following examples, we will be using the following target configuration:

Real-world function	Label	Interface	IP Addr	Netmask	Gateway
Internal Interface	E0	eth0	192.168.200.1	255.255.255.0	
External Interface	E1	eth1	80.201.202.1	255.255.255.0	80.201.202.254

Please note that the above settings are not in any way a recommended configuration, and may differ radically from your own. They are used for illustration purposes only.

Requirements

In order to get on-line you will only need to know the following:

- IP Address, Subnet Mask and Gateway address for the External Interface

To additionally enable the Internal network, you will need to know:

- IP Address and Subnet Mask for the Internal Interface.

Configuring Your External Interface

Before proceeding any further, you may wish to inspect your existing interface and routing configuration. Please see the examples in the “Overview of commands” section to learn about this.

Assuming your External Interface is eth1 (labelled E1), your external IP addresses is 80.201.202.1, and your subnet mask is 255.255.255.0, you would type the following commands:

```
firewall:~# ifconfig eth1 80.201.202.1 netmask 255.255.255.0
firewall:~# route del default
firewall:~# route del default
firewall:~# route add default gw 80.201.202.254
```

Explanation:

- The ifconfig command sets the IP Address and Subnet mask of eth1
- “route del default” is run twice to remove the existing default gateway route(s). If ipsec was running there would have been two default gateway routes.
- The final route add command sets the default gateway

Now try to ping your default gateway. If this works, try to ping a remote IP address that you know responds to pings. It might be wise at this point to ping by IP address rather than hostname, to avoid DNS complications.

If you have any difficulties check your routing table and ensure that there is only one default gateway, and that it matches the IP address you provided.

Configuring your Internal Interface

Once again, you may wish to inspect your existing interface and routing configuration before continuing.

Assuming your Internal Interface is eth0 (labelled E0), your internal IP addresses is 192.168.200.1, and your subnet mask is 255.255.255.0, you would type the following command:

```
firewall:~# ifconfig eth0 192.168.200.1 netmask 255.255.255.0
```

That’s all you have to do. You might want to inspect your routing table at the point to satisfy yourself that everything is in order.

Setting firewall rules

Firstly we must “flush” existing anti-spoofing and NAT rules that might get in our way:

```
firewall:~# iptables -t raw -F
firewall:~# iptables -t nat -F
```

Next we must ensure that all connections from the Internal network going to the Internet will be permitted. We will also ensure that those packets are NATed (or masqueraded) as they are forwarded to the Internet.

Assuming that eth0 is Internal and eth1 is external, you would type the following commands:

```
firewall:~# iptables -t nat -I POSTROUTING -o eth1 -j MASQUERADE
firewall:~# iptables -I FORWARD -i eth0 -o eth1 -j ACCEPT
firewall:~# iptables -I INPUT -i eth0 -j ACCEPT
```

Internal workstation settings

Any correctly configured machine connected in the internal network should now be able to connect to the Internet.

Your workstation should be configured as follows.

IP Address	Same network range as firewall (e.g. 192.168.200.2)
Subnet mask	Same as firewall (e.g. 255.255.255.0)
Default Gateway	The firewall’s IP address (e.g. 192.168.200.1)
DNS Server(s)	ISP’s DNS servers (preferred), or firewall (e.g. 192.168.200.1)

You should now be on the Internet.

DNS Considerations

The FMS will try to connect to your FireRack by hostname. If you have had to change the public IP address of your FireRack such that it no longer matches its DNS record, this will have to be rectified immediately.

If your FireRack is configured to use Dynamic DNS, you can update your DNS like so:

```
firewall:~# dipupdate
====  gdipc.pl running:  Thu Aug 18 15:47:18 2005  ====
Configuration file name: /etc/gnudip/firewall.yourdomain.com.conf
Attempting update at 193.115.249.4 ...
Update to address 80.201.202.1 successful for you.flexdns.net
```

Making changes permanent

At this point it is essential that you log on to the FMS Management Console and make your changes permanent. The settings of each interface you've altered should be checked in every detail.

You may also have to make changes to the firewall rules on the FMS to ensure that when you next push a configuration through, you will not be cutting yourself off from the Internet once again.

Once you have successfully pushed to your FireRack for the first time, and have not cut yourself off from the Internet, you should never need to consult this document again.