

## Load Balancing ContentKeeper With RadWare

The RadWare Fireproof may be used with ContentKeeper to provide load balanced and redundant Internet content filtering for your network.

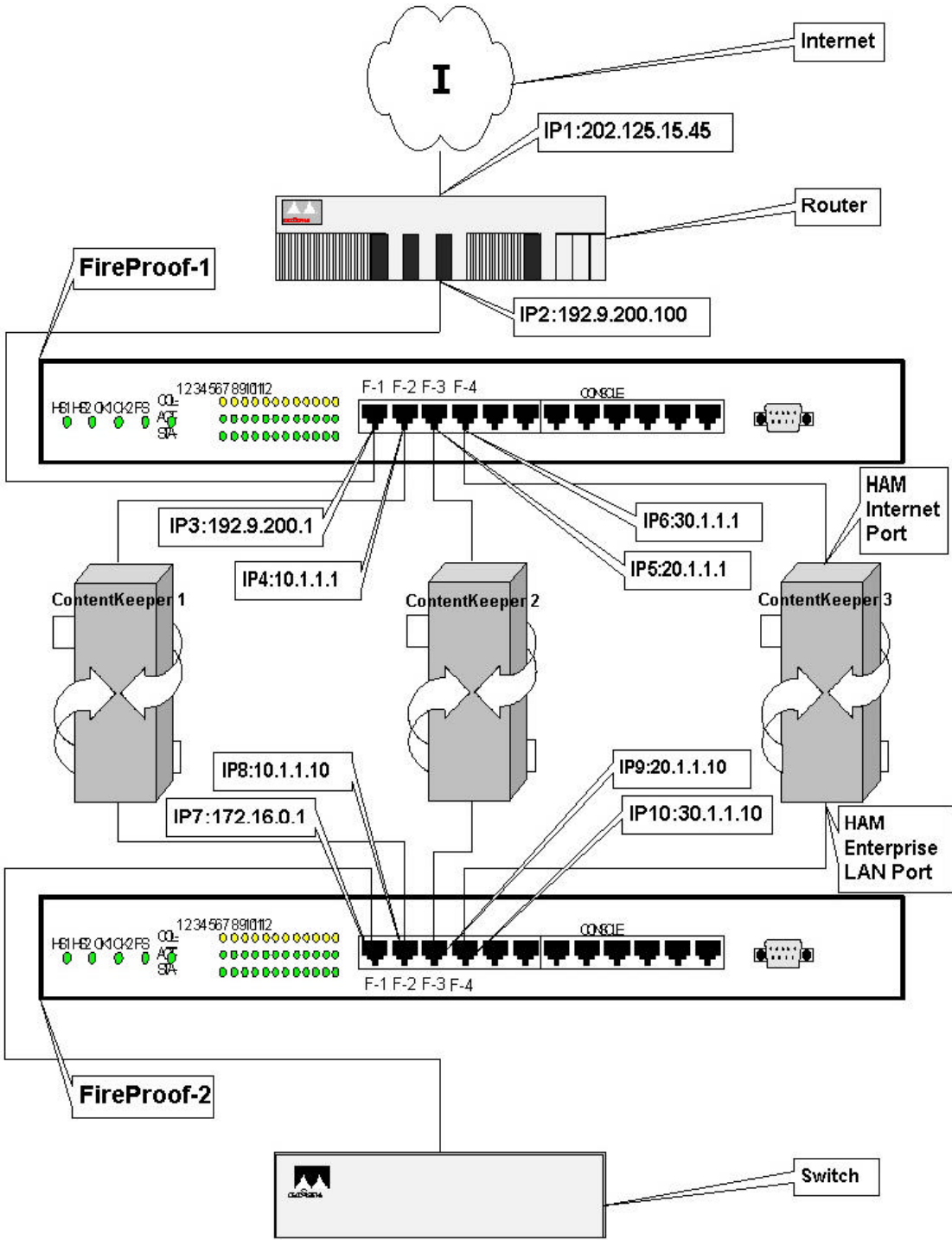
The RadWare FireProof will provide dynamic load balancing of all IP traffic between all of the ContentKeeper appliances in the 'farm'. The FireProof also provides fault tolerance or fail-over between ContentKeeper appliances. This coupled with the High Availability Module provides effective multi-layer dynamic load balancing and redundancy.

Two RadWare FireProof AS1 10 Port (2 x Gigabit, 8 x 10/100) Application Switches may be used to dynamically load balance up to seven ContentKeeper appliances.

Two RadWare FireProof AS2 21 Port (5x Gigabit, 16 x 10/100) Application Switches may be used to dynamically load balance up to fifteen ContentKeeper appliances.

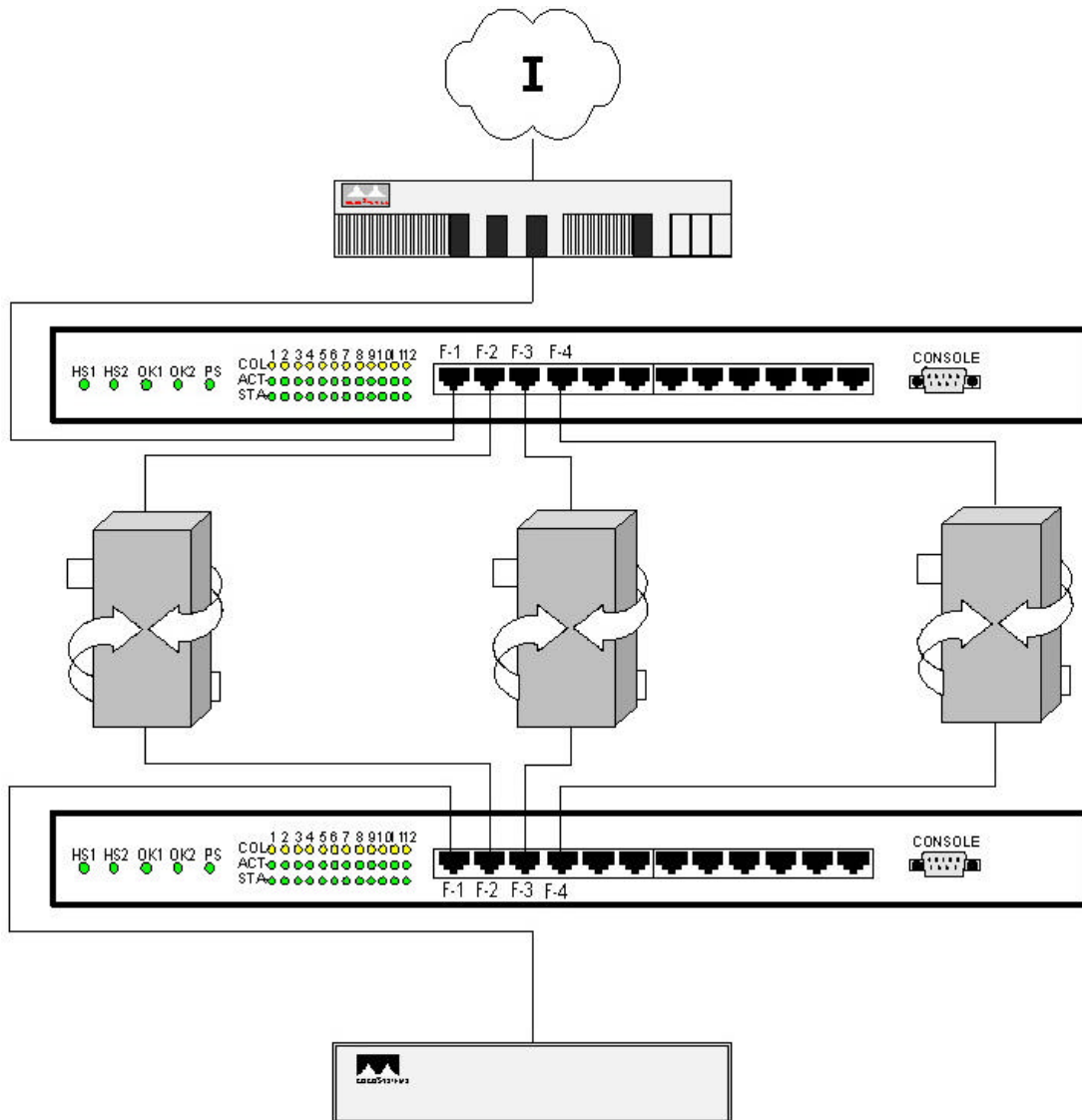
This document outlines the procedures involved in setting up and configuring a load balanced appliance farm. Refer to the network diagram on the next page when setting up.

### Example Network Diagram



### Load Balancing ContentKeeper with RadWare

This diagram represents a typical load balanced ContentKeeper deployment. This deployment is simple to set up and requires a minimal amount of configuration.



### Diagram Excerpt

This diagram is an excerpt of the network diagram on the previous page. It has been included here for convenience. The setup that this diagram details contains only a few network components including:

- A Router
- A Switch
- Two RadWare FireProof load balncing devices
- A number of ContentKeeper appliances

Any number of ContentKeeper appliances up to fifteen may be load balanced using this configuration. For farms of up to seven ContentKeeper appliances use the FireProof AS1 ten port and for farms of eight to fifteen appliances use the FireProof AS2 twenty-one port.

Contact ContentKeeper Technologies for more information on obtaining RadWare equipment.

## Deploying Load Balanced ContentKeeper Appliances

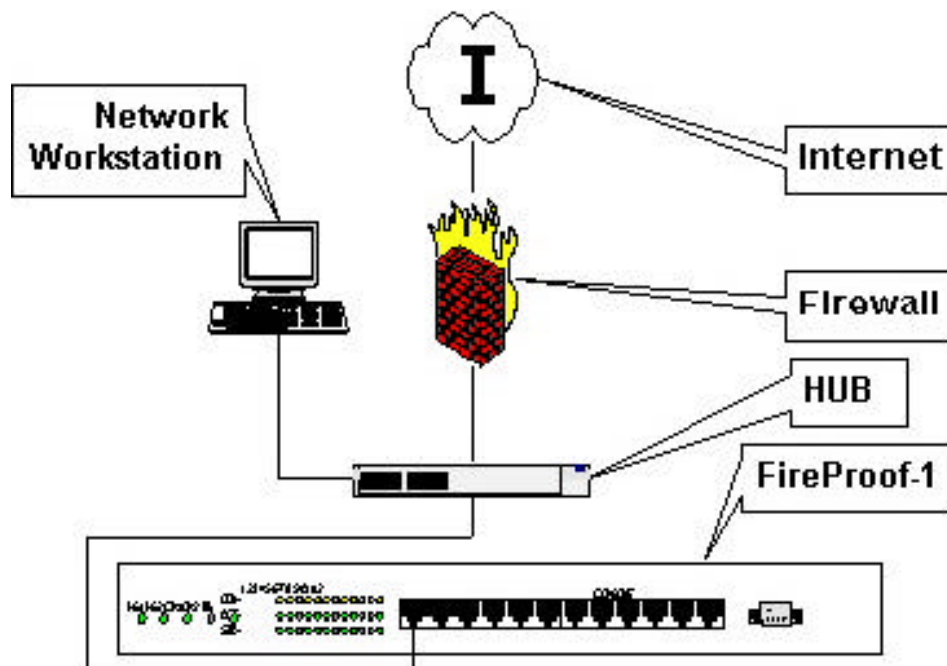
The procedure outlined below was designed from the perspective of someone who is building a new network and may not be suitable for an environment where a network already exists. Deploying a load balanced ContentKeeper installation in such an environment requires minimal reconfiguration and minimal downtime of the existing environment.

The example deployment outlined in this document may be modified to suit environments with more demanding requirements. See the following notes.

### Customising The Example Deployment

Use the following suggestions to help when using and customising the example load balanced ContentKeeper deployment.

- Attach the router to the local network and teach it to access the Internet from there. This is so that the load balanced installation may be successfully tested without disrupting network wide Internet access.
- Place a HUB between FireProof-1 and the router then attach a workstation to the HUB. This creates a simple, direct connection to the configuration interface without traversing the router or FireProof.



- Deploy this installation to the leg of a proxy server or firewall by replacing the router with the proxy server or firewall. All procedures apply to routers, proxy servers and firewalls.

## Overview

The following is an overview of the procedure used to configure the setup in the example network diagram above. Parts of this procedure refer to the example network diagram.

### Part 1 - Install

1. Configure the management interface with an IP address.
2. Install the FireProofs
3. Connect the management ports
4. Connect the ContentKeeper appliances
5. Install ConfigWare

### Part 2 - Configure

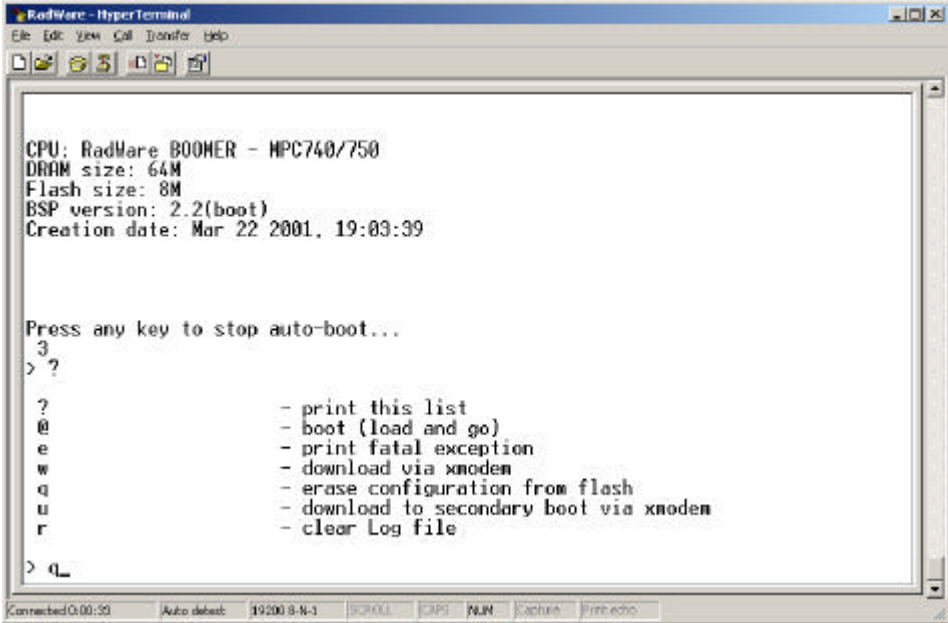
6. Configure VLANs
7. Assign IP addresses to interfaces
8. Set up the firewall tables
9. Configure default and static routes on the FireProofs
10. Configure default and static routes on the remaining network devices (including firewalls, routers and workstations)
11. Configure connectivity checks and test the deployment

### Part 1 - Install

Refer to the RadWare FireProof User Guide, Chapter 2, for more detailed information. The PDF version is available for download from [www.contentkeeper.com](http://www.contentkeeper.com).

### Ensure All Prior Configuration Is Removed

Accessing the boot menu by pressing a key in the specified time and selecting 'q' for 'erase configuration from flash'



```
RadWare - HyperTerminal
File Edit View Call Transfer Help

CPU: RadWare BOOHER - MPC740/750
DRAM size: 64M
Flash size: 8M
BSP version: 2.2(boot)
Creation date: Mar 22 2001, 19:03:39

Press any key to stop auto-boot...
3
> ?

?          - print this list
@          - boot (load and go)
e          - print fatal exception
w          - download via xmodem
q          - erase configuration from flash
u          - download to secondary boot via xmodem
r          - clear Log file

> q
```

## Assigning An IP Address To The Management Interface

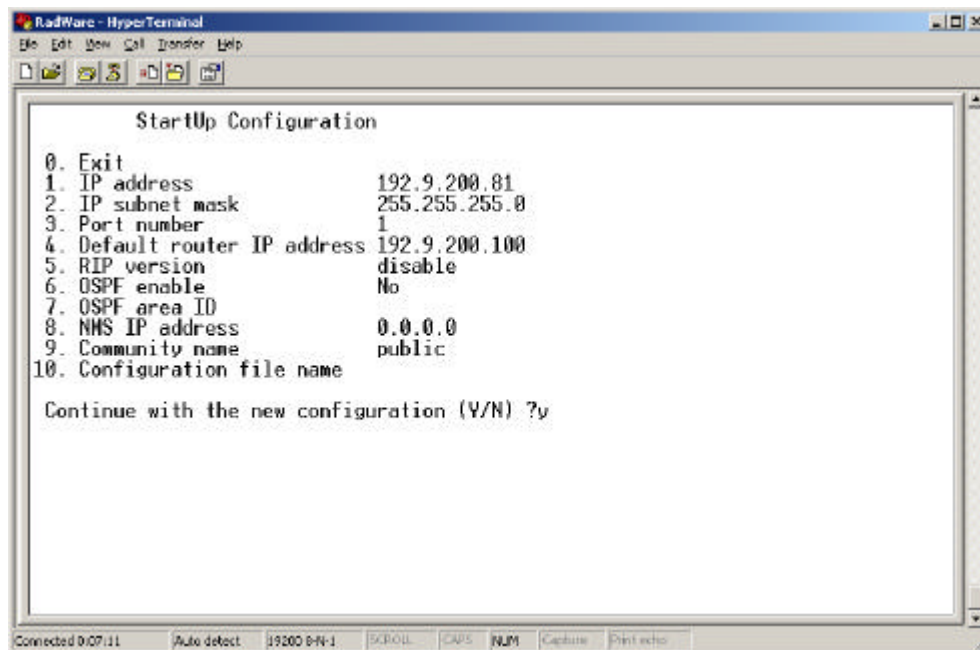
You must assign an IP address to each FireProof before you can configure it. The IP address may be assigned via a terminal session. The connection parameters are:

**Baud:** 19200  
**Data Bits:** 8  
**Parity:** None  
**Stop Bits:** 1  
**Flow Control:** None

You may find it more convenient to assign the IP address before placing the FireProof in a rack or cabinet.

1. Use a terminal emulator, such as hyper terminal, to connect to the serial interface on the front of the FP.
2. Edit a menu item by entering its number and pressing <return>. Configure the FireProof with an IP address (IP3), a subnet mask, a default rout and a management interface (which should be port 1).

Use the default values for the remaining settings by pressing the <RETURN> key while at the 'Enter your choice?' prompt until all default valued have been automatically entered and you are asked to 'Continue with the new configuration (y/n) ?'



3. Confirm the new configuration by pressing <y> <return> and the FireProof will restart.
4. Repeat the procedure for the second FireProof (IP7). **Note: Do not configure a default route at this point.**

## Install The FireProofs, Connect The Configuration Interfaces & Connect The ContentKeeper Appliances

Place the FireProofs in the production environment (i.e. a rack or cabinet) and apply power to them.

Attach Ethernet port 1 on FireProof-1 to the internal interface of your Internet router.  
Attach Ethernet port 1 on FireProof-2 to the internal network.

1. Attach Bridge Port 1 of ContentKeeper 1 to port 2 on FireProof-1.  
Attach Bridge Port 2 of ContentKeeper 1 to port 2 on FireProof-2.
2. Attach Bridge Port 1 of ContentKeeper 2 to port 3 on FireProof-1.  
Attach Bridge Port 2 of ContentKeeper 2 to port 3 on FireProof-2.
3. Repeat the above process for the rest of the ContentKeeper appliances.

### Install ConfigWare

For each FireProof, install ConfigWare on a workstation that is connected to the same subnet as the FireProof configuration interface. Refer to the RadWare FireProof User Guide, Part 2-11, for more detailed information. The PDF version is available for download from [www.contentkeeper.com](http://www.contentkeeper.com).

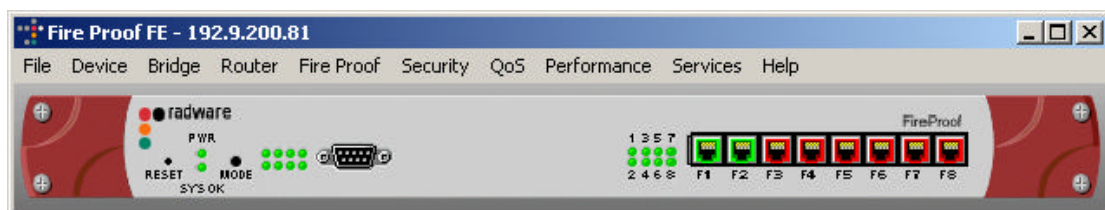


## Part 2 - Configure

Procedures in this section are outlined on a per-FireProof basis. Screen shots are only included for one FireProof as they are the same for both, and as the procedures are almost identical, the differing steps have been highlighted for the second FireProof.

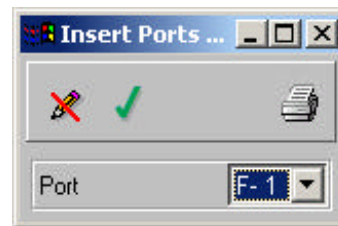
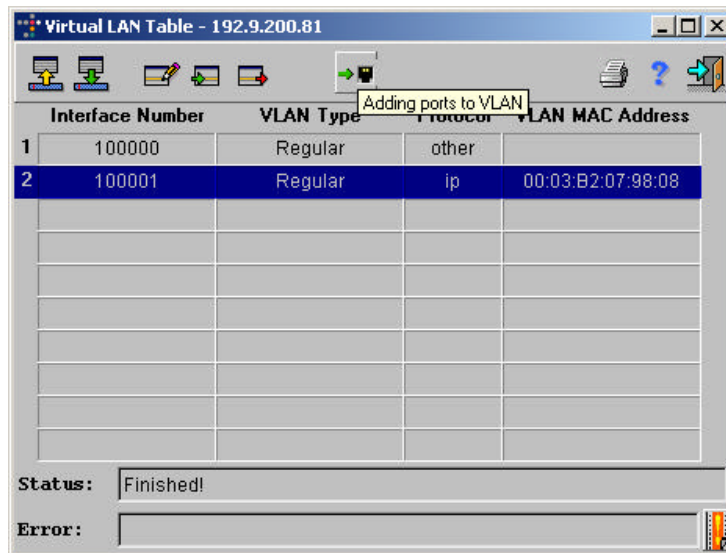
All Screen shots are taken from FireProof-1 in the example.

### Launch ConfigWare And Connect To The FireProofs



### Configuring VLANs

1. Open VLAN in the Device menu on FireProof-1 and add interface F-1 to the default VLAN 100001.



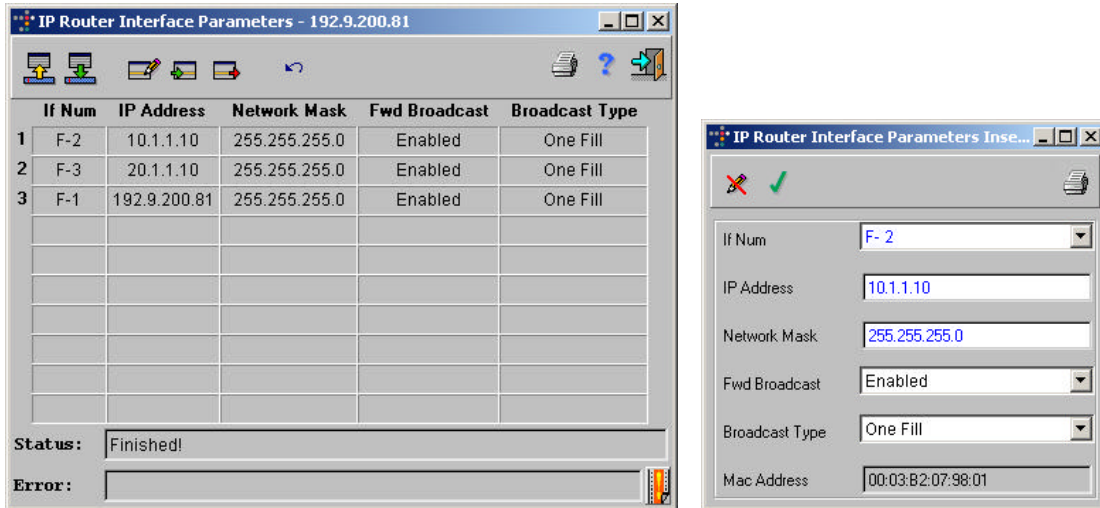
2. Perform the same procedure on FireProof-2.

### Assigning IP Addresses To Interfaces

1. Open Interface Parameters under IP Router in the Router menu on FireProof-1 and insert an IP address for each ContentKeeper appliance. Ensure that it is assigned to the correct interface.

**Important:** Each IP Address assigned for a ContentKeeper appliance must be on a different IP subnet. Refer to the example network diagram, IP4, IP5 and IP6.

2. Use the default values for Fwd Broadcast and Broadcast Type.

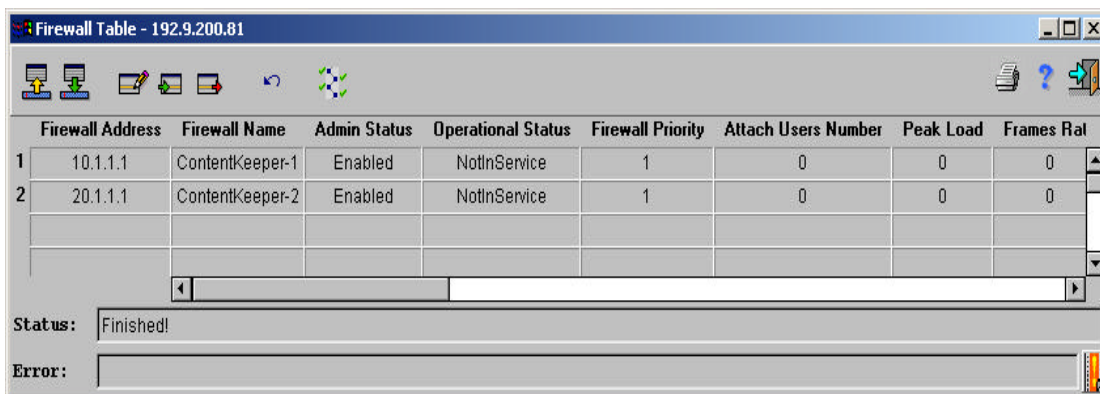


- Repeat the procedure for FireProof-2. **Ensure that the IP addresses assigned are on the correct subnet and do not clash with already assigned addresses. Refer to the example network diagram, IP8, IP9, and IP10.**

### Setting Up Firewall Tables

**WARNING!** You must have a device connected to a port with a link light for each entry in the firewall table that you want to make. The best practise is to connect the ContentKeeper appliances before configuring the FireProofs.

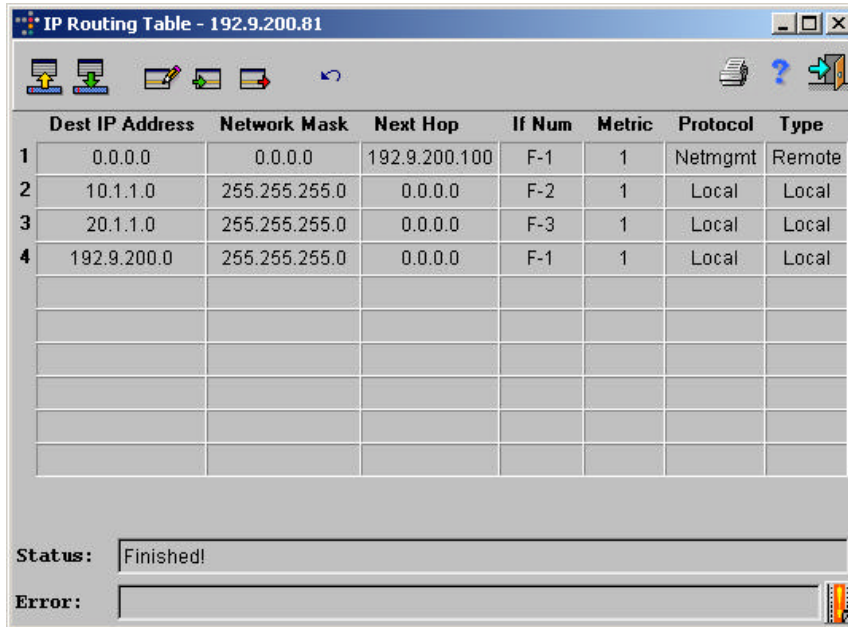
- Open the Firewall Table from the FireProof menu on FireProof-1 and add one firewall for each ContentKeeper appliance. Use the IP address of the ports on FireProof-2. Refer to the example network diagram, IP8, IP9 and IP10.



- Repeat the procedure for FireProof-2, **but reverse the IP addresses used. Refer to the example network diagram, IP4, IP5 and IP6.**

## Configuring Default And Static Routes On The FireProofs

1. Open Routing Table from the Router menu on FireProof-1 and ensure that there are routes for each defined IP address as well as a default route. The default route for FireProof-1 should be the IP address of the internal interface of the router.



	Dest IP Address	Network Mask	Next Hop	If Num	Metric	Protocol	Type
1	0.0.0.0	0.0.0.0	192.9.200.100	F-1	1	Netmgmt	Remote
2	10.1.1.0	255.255.255.0	0.0.0.0	F-2	1	Local	Local
3	20.1.1.0	255.255.255.0	0.0.0.0	F-3	1	Local	Local
4	192.9.200.0	255.255.255.0	0.0.0.0	F-1	1	Local	Local

Status: Finished!

Error:

2. Add a static route to map the internal network (172.16.0.0 based on the example) to any one of the addresses in the firewall table. When a packet traverses this route, the FireProof sees that it is destined for an address in the firewall table and automatically load balances the incoming traffic between all addresses in the firewall table.
3. Perform only step 1 for FireProof-2. **The default route for FireProof-2 is one of the addresses in its firewall table.**

## Configuring Default And Static Routes On Network Devices

The following routes must be configured in order for traffic to traverse the deployment in both directions.

- The Router must have a default route that will allow traffic to get to the Internet. This also applies to Firewalls and Proxy servers.
- The Router must have a static route that maps the internal network (172.16.0.0 based on the example) to the configuration interface address of FireProof-1. This also applies to Firewalls and Proxy servers.
- Network devices that are behind FireProof-2 (i.e. on the internal network) must have their gateway address set to the configuration interface address of FireProof-2.

## **Important Points To Consider**

- Ensure that the ContentKeeper appliances are passing traffic.
- Ensure that two bridge ports are never plugged into the same network.
- Erase any existing configuration from the FireProofs before starting.
- Refer to the RadWare FireProof User Guide for detailed information such as FireProof hardware specifications and protocol information.