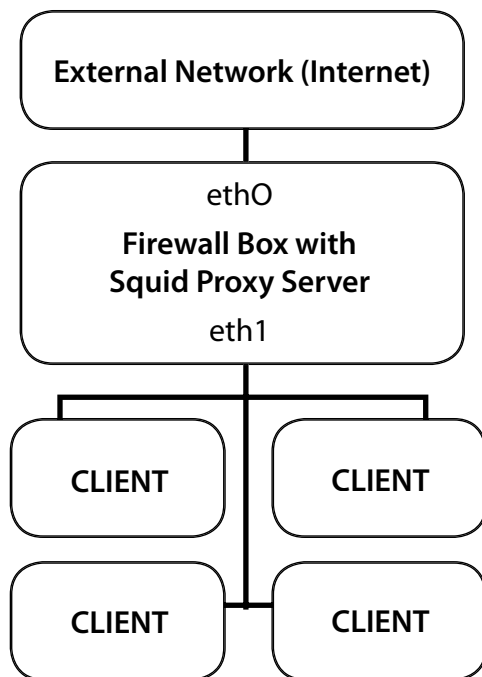


# A simple guide to creating a firewall and squid proxy server

Peter K. Lillian - RHCE  
Red Hat, Inc.

## INTRODUCTION



This paper will cover the configuration and setup of a firewall and squid proxy server. By no means is this meant to be a complete solution; it is a straight forward example of how to get started.

The assumed network infrastructure looks something like Drawing 1. A server acting as both firewall and squid proxy server sits between the internal and external network. Clients are configured to use the IP address for the firewall server as the gateway and proxy server for accessing web pages.

A firewall is extremely important in any environment where systems will be connecting to an insecure network like the Internet. It can also be used to prevent certain types of traffic from leaving a company network. Red Hat Enterprise Linux utilizes the iptables system, which is a kernel-level packet-filtering tool. Iptables uses a list of rules to determine what to do with a given packet from the network. This paper will show how to set up simple forwarding and filtering rules for a firewall appliance.

Squid is a high-performance proxy caching server for web clients. It supports FTP, gopher, and HTTP data objects. Unlike traditional caching software, Squid handles all requests in a single, non-blocking, I/O-driven process. Squid keeps meta data and especially hot objects cached in RAM, caches DNS lookups, supports non-blocking DNS lookups, and implements negative caching of failed requests.

Squid supports SSL, extensive access controls, and full request logging. By using the lightweight Internet Cache Protocol (ICP), Squid caches can be arranged in a hierarchy or mesh for additional bandwidth savings. Squid consists of a main server program (squid), a Domain Name System (DNS) lookup program (dnsserver), optional programs for rewriting requests and performing authentication, and management and client tools. When squid starts up, it spawns a configurable number of dnsserver processes, each able to perform a blocking DNS lookup. This reduces the amount of time the cache waits for DNS lookups.

Internet object caching is a way to store requested Internet objects (i.e., data available via the HTTP, FTP, and gopher protocols) on a system closer to the requesting site than to the source. Web browsers can then use the local Squid cache as a proxy HTTP server, reducing access time as well as bandwidth consumption. (1)

# FIREWALL SETUP AND CONFIGURATION

## PART 1: SETUP

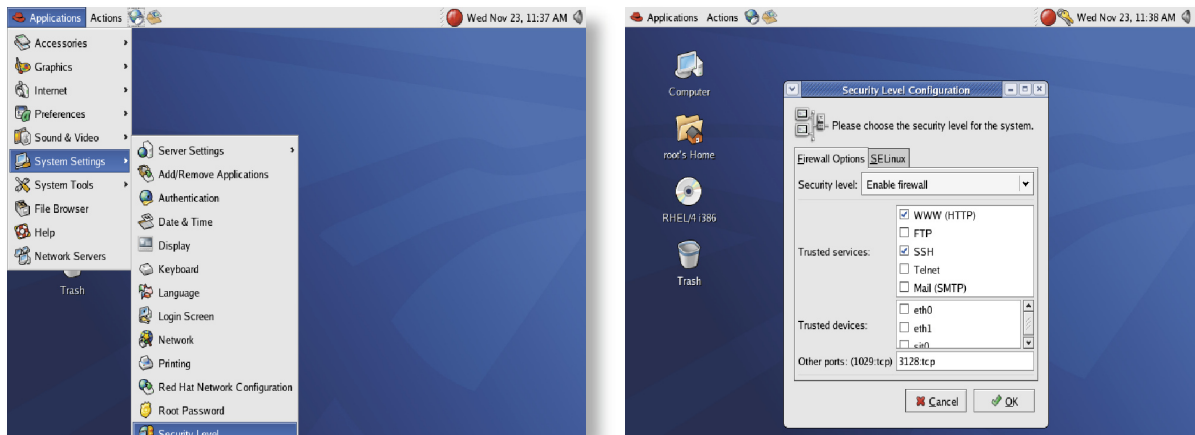
### 1. Log into the system as “root”.

### 2. Enable the firewall on the system. To do this, click on:

- Applications => System Settings => Security Level
- Make sure that the “Firewall Options” tab is selected. Click on the “Security Level” pull down menu and select “Enable Firewall”.

### 3. In the “Trusted Services” area, select “ssh” and “httpd” so that the secure shell and web server on the firewall box are accessible.

### 4. Under “Other Ports” add the port 3128:tcp so that requests to the proxy server can get through the firewall.



### 5. Click “OK”. A warning will appear, verifying that the firewall is to be enabled. Click “OK” again. The firewall is now up and running.

## PART 2: CONFIGURATION

Next, the system needs to be established as a firewall appliance. The system will need to have two separate NICs (Network Interface Cards). For the purposes of this paper, it is assumed that eth0 is connected to the “outside world”, and that eth1 is connected to the internal network.

First, NAT (Network Address Translation) and IP forwarding needs to be configured on the firewall box. This will allow any network requests that come from the internal network to be forwarded to the outside network.

### 1. Open a terminal window, and do the following:

```
cd /etc/  
gedit sysctl.conf
```

### 2. Go to the line with “net.ipv4.ip\_forward = 0” and change the 0 to a 1, so that the line looks like this:

```
net.ipv4.ip_forward = 1
```

This will enable IP Forwarding. Save the file, and close the window.

### 3. The changes just made will be put into effect on the next reboot. To enable the changes immediately from the terminal window, type:

```
sysctl -p
```

This will re-read the configuration file (/etc/sysctl.conf) that was just edited, and put the changes into effect.

### 4. Next, the NAT rules need to be added to the firewall.

From the terminal window, type the following:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

This “rule” says that on the way out, the firewall will masquerade as the requesting server. This means that any requests that originate from inside the firewall will first go through the firewall server, and then out to the Internet. Subsequently, any requests being returned from the Internet that originated from inside the firewall will be routed back to the originating system.

### 5. Now, the iptables need to be set up to forward packets from eth1 to eth0, so that the firewall server will forward them on. For reference, the -I option is for “insert rule”, the -i option is for “input interface”, the -o option is for “output interface”, and the -j specifies what to do if the packet matches the rule (accept it, in this case).

```
iptables -I FORWARD -i eth1 -o eth0 -j ACCEPT
```

### 6. Save your changes:

```
service iptables save
```

The firewall is now configured. On the client systems, the gateway parameter of the network configuration will need to be set to the IP Address of the eth1 interface of the firewall.

# SQUID PROXY SERVER SETUP AND CONFIGURATION

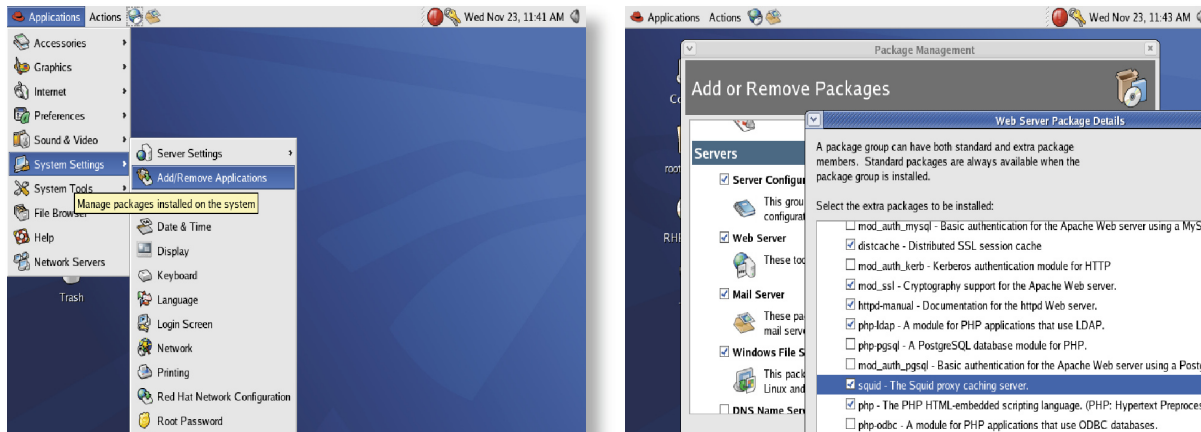
## PART 1: SETUP

### 1. Log in as root.

### 2. Verify the squid package has been installed. Click on:

Applications => System Settings => Add/Remove Packages

Scroll down to the Server area. Verify that the check mark is placed by Web Server. Click on "Details". Scroll down and verify that squid has a check mark. These packages must be installed before proceeding.



**To install: Either click on the "update" button (This requires having the installation media available, and assumes that the system has not been updated since initial installation.) or use up2date and Red Hat Network to install the packages. To install with up2date, type the following in a terminal window:**  
up2date squid httpd

Once it has been verified that the packages are installed, the squid proxy server will need to be configured.

## PART 2: SERVER CONFIGURATION

### 1. Open a terminal window, and type the following:

```
cd /etc/squid  
gedit squid.conf
```

(note that any text editor can be used in place of gedit)

This is the configuration file for the squid proxy server. It contains documentation about the available configuration options. Take some time to read through some of the options. For this paper, the configuration will be greatly simplified for demonstration purposes.

### 2. Find the line "INSERT YOUR OWN RULE(S) HERE TO ALLOW...". The easiest way to do this is click on "Find" and search for the above phrase. Somewhere below this line, add the following:

```
acl <group> src IPADDRESS  
http_access allow <group>
```

<group> is any arbitrary group name (such as my\_connection), and IPADDRESS is a list or group of IP addresses that you want to have access to your Squid server (such as 192.168.0.0/24). Using these examples, the newly added lines would look like:

```
acl my_connection src 192.168.0.0/24  
http_access allow my_connection
```

### 3. Save the changes, and close your editing program.

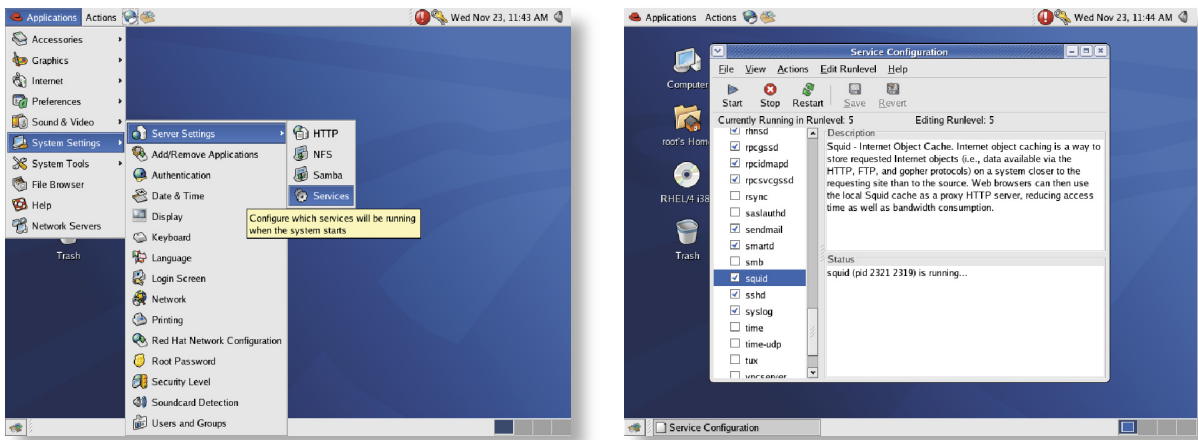
## PART 3: STARTUP

### 1. Now that the squid proxy server has been configured, the service needs to be started.

**Click on:**

Applications =>System Settings =>Server Settings =>Services

Scroll down to entry marked "squid". Place a check mark in the box next to it. This will enable the service to start when the system is rebooted.



### 2. Click on "start" to start the service now. A window should appear to let you know that the service has started successfully.

### 3. Save the changes by clicking on the "save" button at the top, and close the window. The squid proxy server is now configured and running.

## STEP 4: CLIENT CONFIGURATION

The last step is to configure client systems to use this system as their web proxy server.

### 1. On a client system, open up the web browser.

### 2. Find the configuration controls for setting proxy server information.

This varies from browser to browser. For example, in Firefox, click on the following:  
Edit=> Preferences =>General => Connection Settings

### 3. Enter the IP address of the squid server you configured on the HTTP Proxy line. Use port 3128. Click "OK", and then "OK" again.

### 4. Type into the browser's address bar:

`http://www.redhat.com`

This should bring up the Red Hat home page. Repeat Step 4 on any other client systems.

## REFERENCES:

- (1) <http://www.squid-cache.org>
- (2) <http://www.netfilter.org>
- (3) <http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/sysadmin-guide/>