

Firewall Lab Basic Setup

Author: Abhishek Karnik

Date: 05/11/05

1. Document Purpose:

This document has been prepared to explain the basic setup of the Firewall lab. at the University of Central Florida. This document can be used as a reference manual by a teaching assistant prior to conducting this lab.

2. Document Scope:

The configuration setup described is specific to the “Cyber-Guard” Firewall. The document covers information relating to issues concerning “Firewall Lab-I” and its topology. In-depth detail of the firewall working is beyond the scope of this document. Readers interested in learning more about the “Cyber-Guard” Firewall are encouraged to read its official manual.

3. Introduction:

This lab has been taught as a part of COT4932 – Computer Network Security. The main focus of the firewall lab is to give students a practical exposure on the working of firewalls. Students are taught how to configure firewall rules to allow or deny packet delivery across the firewalls. “Firewall-labI” introduces the use of basic UNIX and Windows commands to enable users to understand networking and security concepts better.

3.1 Network Topology

Figure 1 shows the setup of the lab.

- There are 4 hardware firewalls (Cyber Guard Firewalls) connected to each other by a router, on their external interfaces.
- The firewalls are named as follows:
Firewall 1: **fw1**
Firewall 2: **fw2**
Firewall 3: **fw3**
Firewall 4: **fw4**
- The Router is a simple Debian Linux Box consisting of 4 interface cards connecting the four firewalls together.
- Each firewall on its internal network is connected to a single PC (Dell Inspiron 500m) running Windows XP Professional.
- The PCs are named as follows:
PC1: **Fire01**
PC2: **Fire02**
PC3: **Fire03**
PC4: **Fire04**
- Each interfaces IP address is shown in the figure.

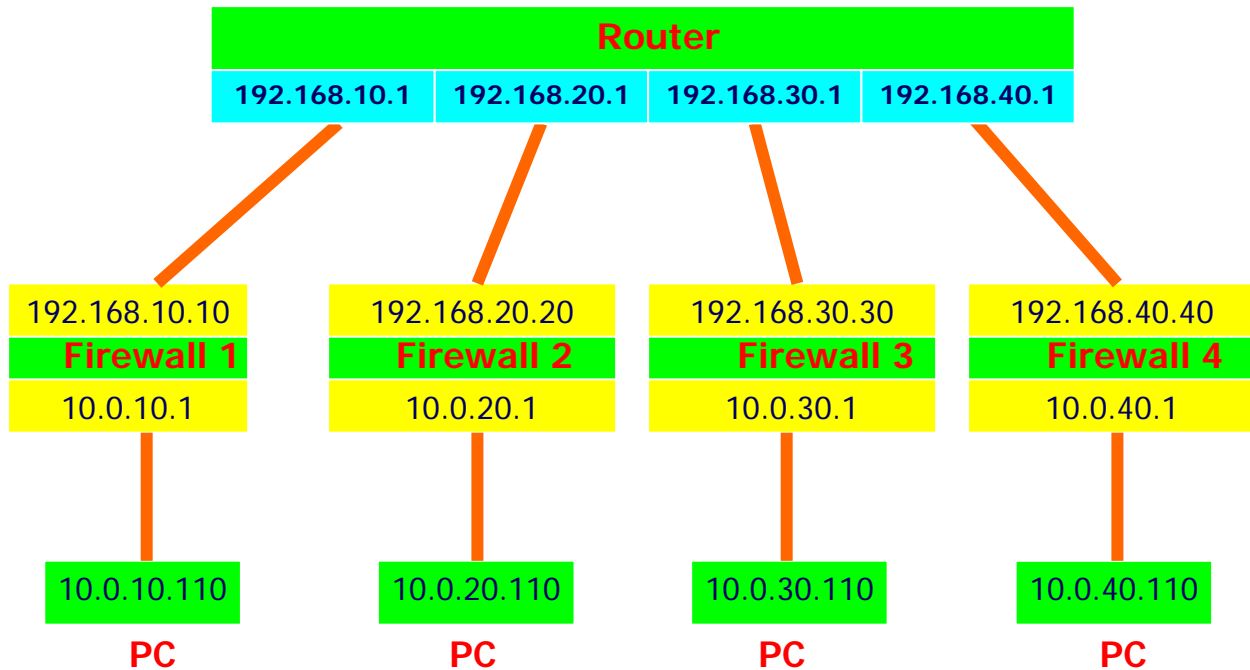


Figure 1: Network Topology

3.2 Resetting the PCs and the Firewalls

3.2.1 PC Setup:

- Log into the PC as follows
 - **Username** : user
 - **Password** : firewall
- The PCs have been pre-configured with static IPs by the administrator.
- The IP Configuration can be viewed by :: Start→Run→Type “cmd”→ipconfig /all

3.2.2 Firewall Setup:

- Log into the Firewall as follows
 - **Username** : cgadmin
 - **Password** : 1234
- On Log on we see a GUI with the following tabs (Figure 2)
 - System
 - Configuration
 - Reports
 - Tools
 - Help

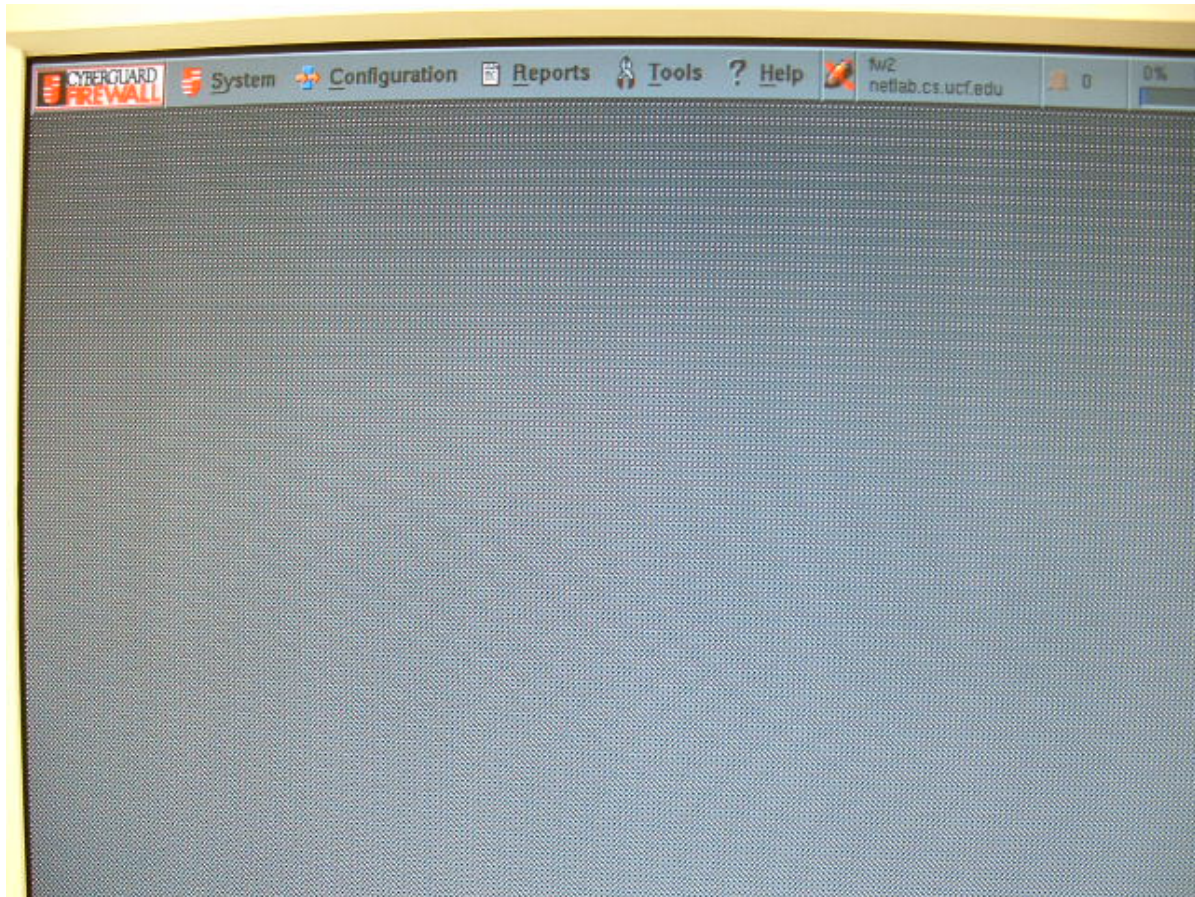


Figure 2: Login Menu Screen

3.2.2.1 Network Interfaces can be viewed by : System → Network Interfaces (Figure 3)

- Setting up Interfaces:
 - Select the Interface tab
 - The System Node Name, Domain Name can be typed in appropriate boxes
 - A list of interfaces has been shown. A user can set up different external and internal interfaces.
 - Set “dec0” as the External Interface with host name : fw’x’-ext (where ‘x’ stands for the firewall number), IP address : 192.168.y.y (where ‘y’ would be 20 for firewall 2), and subnet mask : 255.255.255.0
 - Set “dec1” as the Internal Interface with host name: fw-‘x’-int, IP address: 10.0.y.1
 - “Save” and close the window

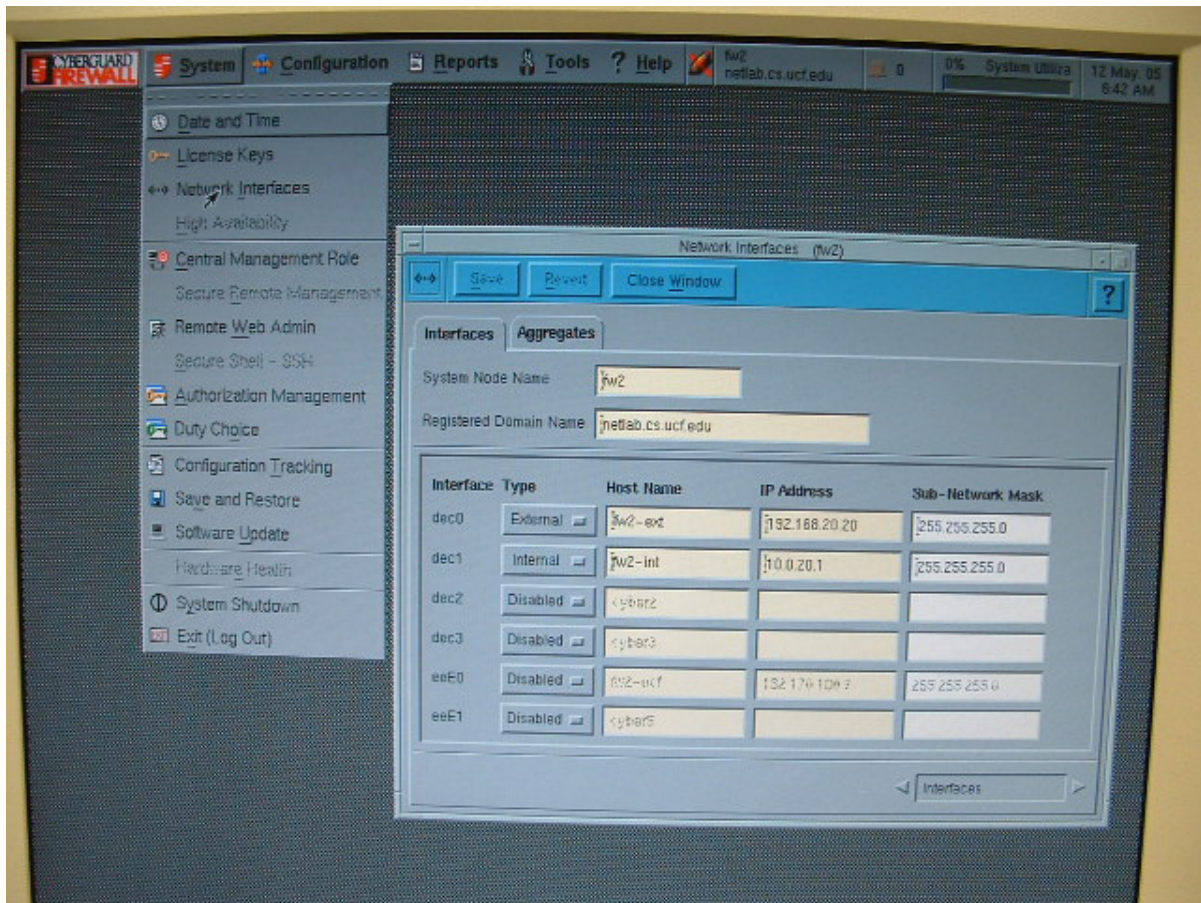


Figure 3: Network Interfaces

3.2.2.2 Packet Filtering rules can be viewed by : Configuration → Packet-Filtering Rules (Figure 4 and 5)

- Deleting Rules:
 - Select all the rules shown in the window (click on the first rule and drag the mouse down)
 - Click “Delete”. This will remove all rules selected in the previous step.
 - Click “Save”. This saves the current packet filtering rules in the window (however this does not reflect in the IP rules tables as yet)
 - Click “Use”. This reflects the changes in the rule table and enforces the rules on packets.
 - Close the Window.
 - If all the rules had been deleted this would ensure that the firewall would be set to its default rule i.e. deny all packets.
- Adding Rules:
 - Firewall rules can be added by selecting “Insert” which enables the lower window with “Basic” Tab.
 - Select appropriate “Port or Service”, Packet Origin and Packet Destination
 - As a rule is being set up, it will appear in the window above.
 - After all the rules have been selected click “Save” and “Use” to enforce the rules on packets
 - Close the Window

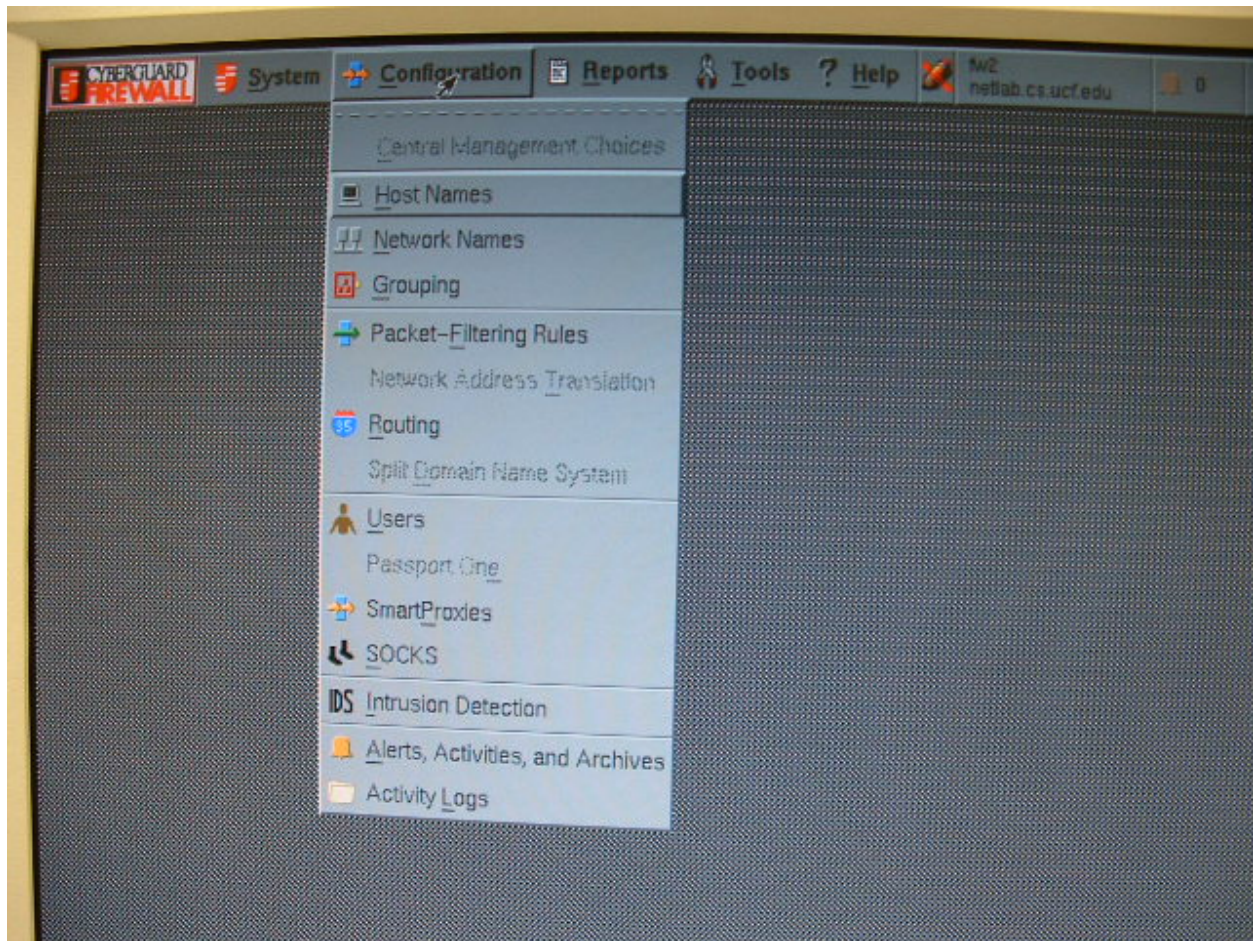


Figure 4: Configuration Menu

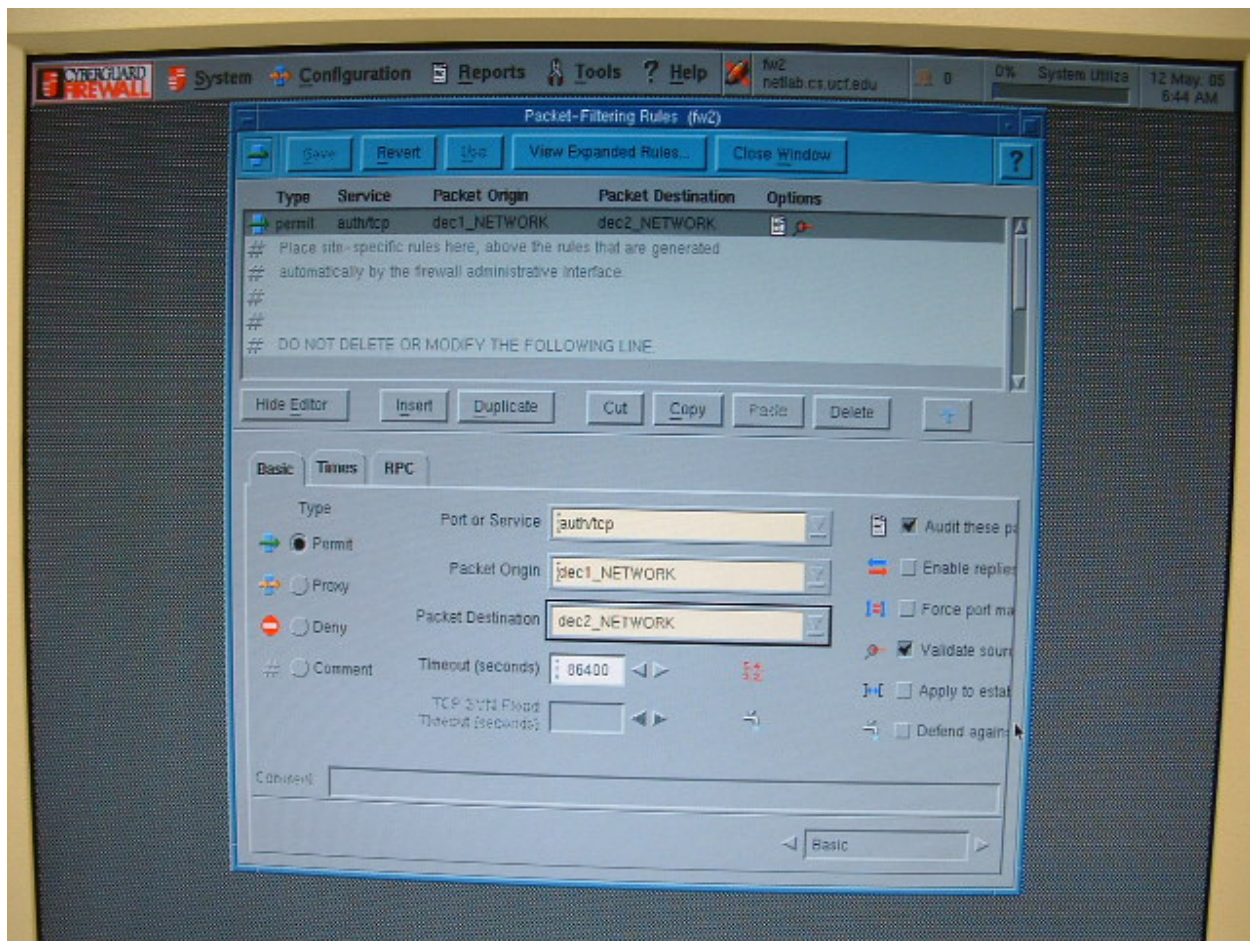


Figure 5: Packet Filtering Rules

3.2.2.3 Setting Up a Default Gateway: Configuration → Routing (Figure 6)

- Set the gateway for the default route as : 192.168.y.1 (where 'y' = 20 for fw2)
- Other Static routes can be set from the “Static Routes” tab
- Dynamic routing can be enabled using the “Dynamic Routes” tab.

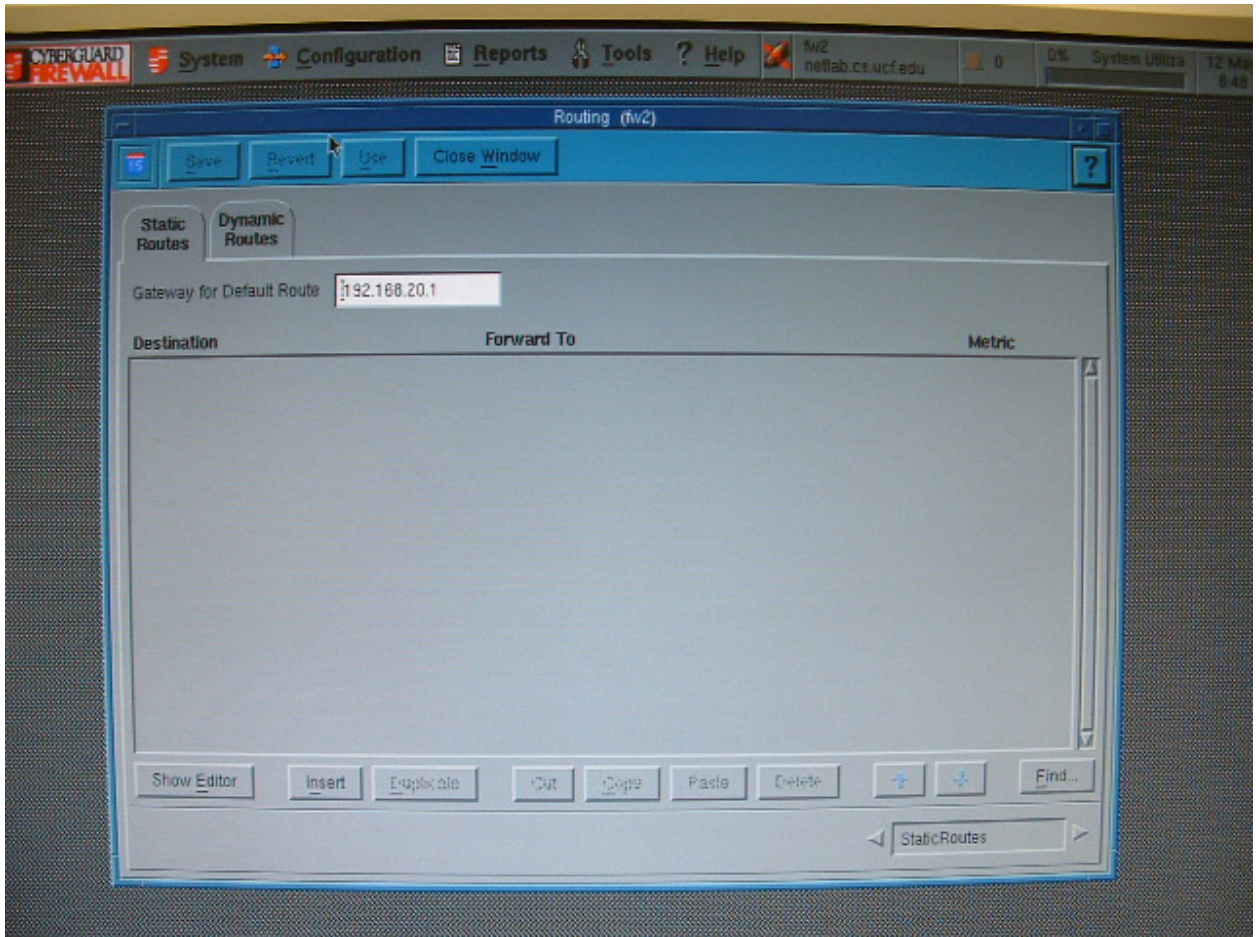


Figure 6: Routing and Default Gateway

3.2.2.4 Network Address Translation: Configuration → Network Address Translation

- Two types of NAT can be set up “Static” or “Dynamic” NAT.
- For Static NAT, an appropriate global address needs to be assigned. This can be done by selecting “Insert”, type as “host”, giving a global address as 192.168.y.110 (where ‘y’ would be 20 on fw2) and assigning this address to an appropriate internal address (example 10.0.20.110)
- For Dynamic NAT, a similar procedure can be followed.
- IMPORTANT: For NAT to reflect, we need to re-login. This can be done as: System → Shutdown → Reinitialize Network.

3.2.2.5 Grouping: Configuration → Grouping (Figure 7)

- Instead of selecting individual rules, for individual hosts and services; if some hosts can have common services or rules, a grouping can be applied.
- Select the Groups tab and select “Insert”.
- Select a “Service” type group or a “Host/Network” type group.
- Give the selected group an appropriate name.

- Select “Save” and “Use”
- Now go to “Members” tab. Here we see three columns. Group, Member and Member Choices. The created group will appear under “Groups”. Select the group and you can add all the members you want associated with this group from “Member Choices” which would be a list of networks if “Host/Network” was selected or Service/Port if “Service” had been selected.
- “Save” and “Use”
- The created groups now appear in the Packet Filtering Rule under “Port Or Service”, “Packet Origin” and “Packet Destination”, as appropriate.

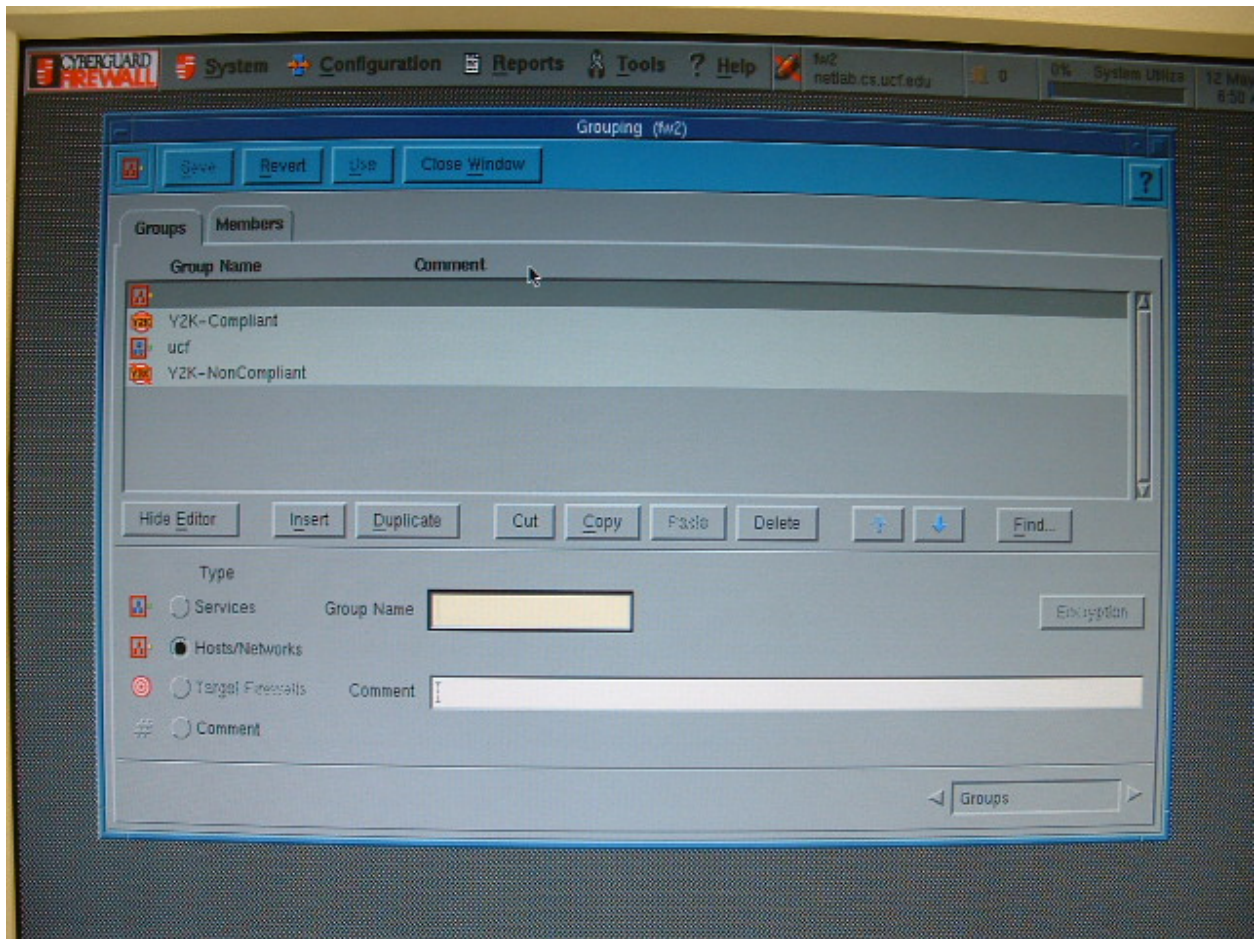


Figure 7: Services or Host/Network Grouping

3.2.2.6 Creating a User: Configuration → Users (Figure 8 and 9)

- Click “Insert”. You will view an extension window with 4 tabs. Select “User Information”. Pick “User Type” as proxy for a Proxy set up.
- Give the Proxy user a “Login ID”.
- Goto “Authentication” tab and select which method of Proxy whether “Internal” or “External” will he/she be using.
- From the password tab below either select a password or auto-generate it.

- FTP Operations can be used to enable/disable certain FTP operation commands.
- “Save” and close the window.

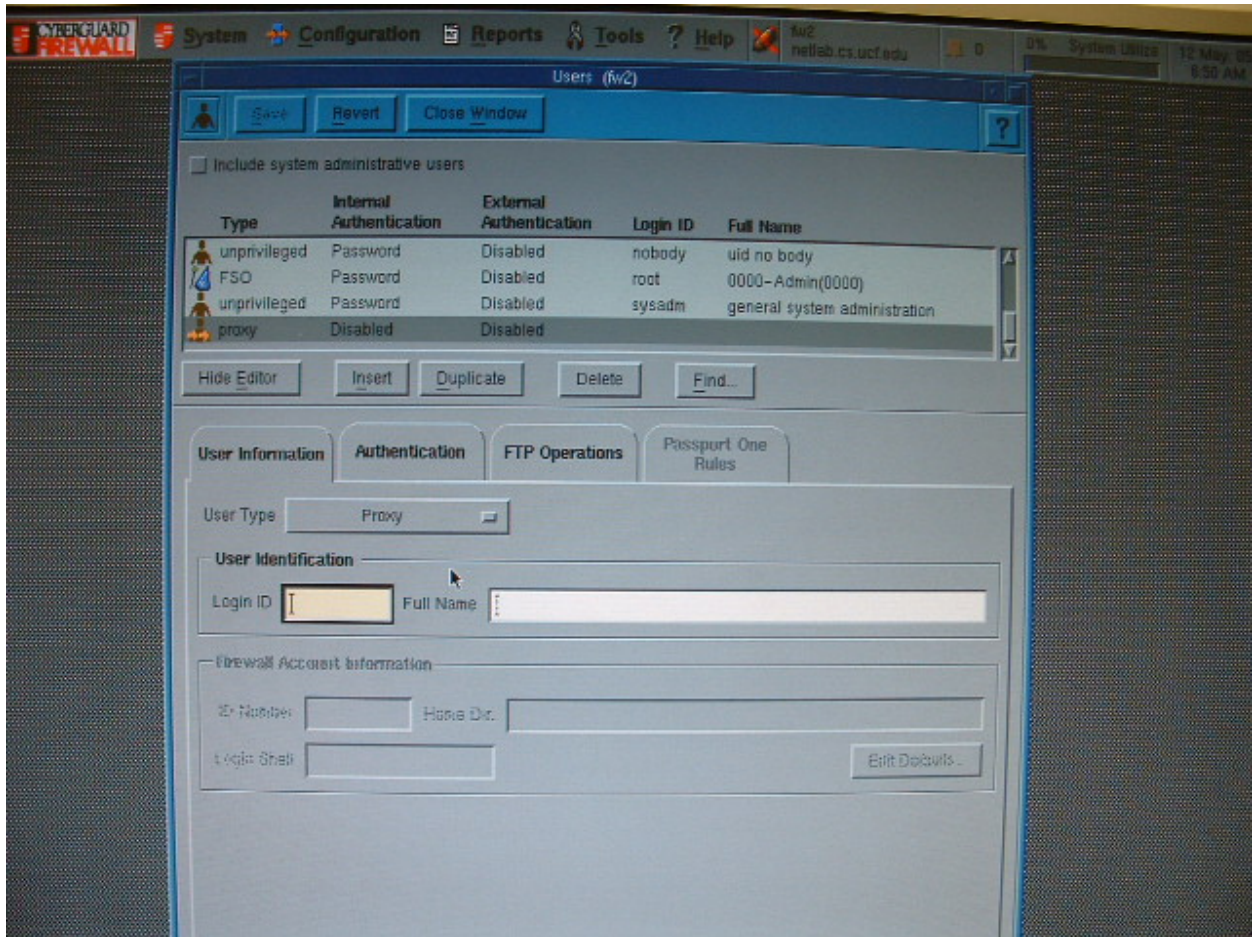


Figure 8: Setting up Proxy Users

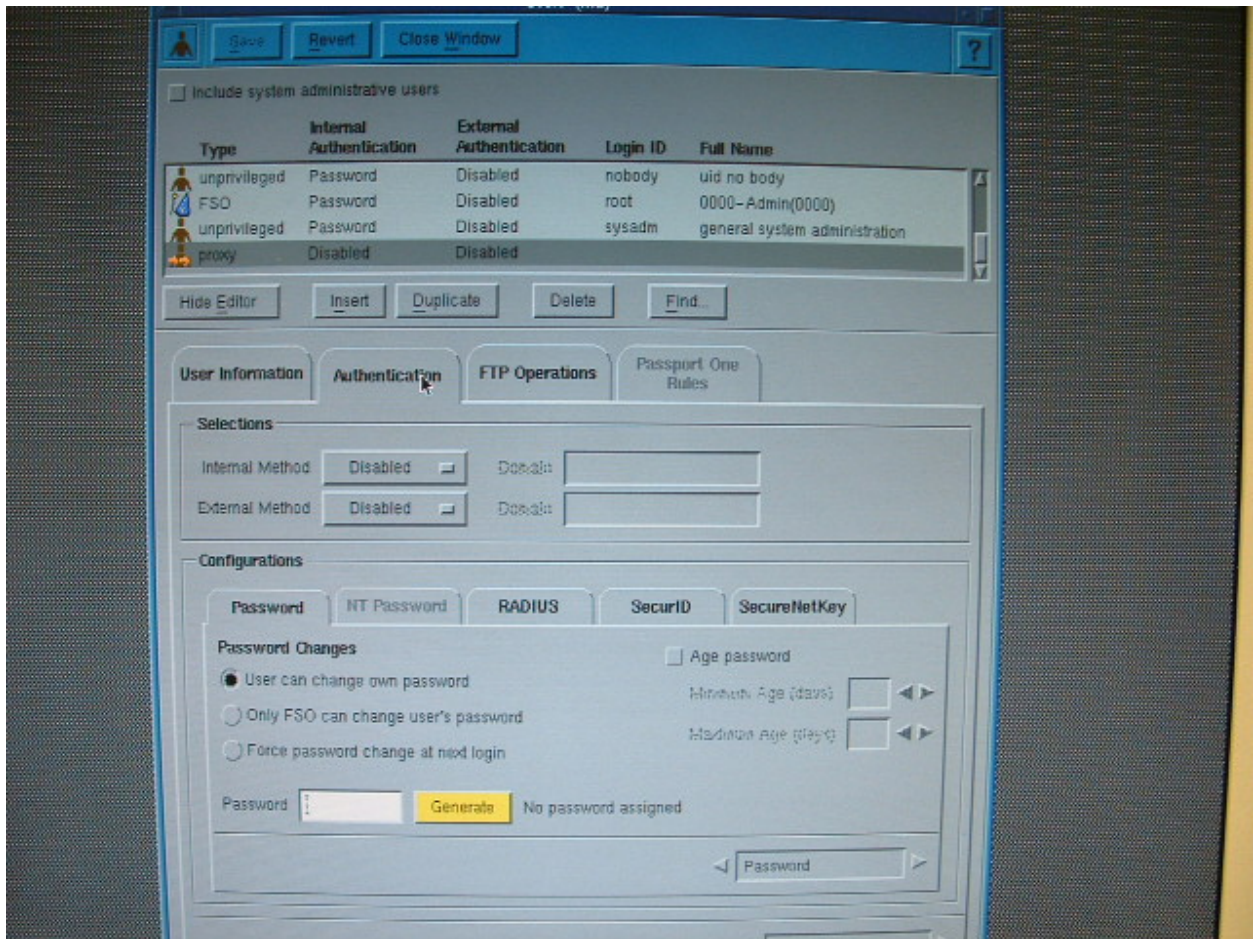


Figure 9: Assigning a User Password

3.2.2.7 Generate Reports: Reports → Audit Logs (Figure 10 and 11)

- Select a time when you want to audit logs. If one types 'now' in the "End Time" you will see a rolling screen similar to the *tcpdump* utility.
- The Report can be stopped and saved to study at some later time.
- Activity Reports from Reports → Activity Reports can be used to filter out captured data.

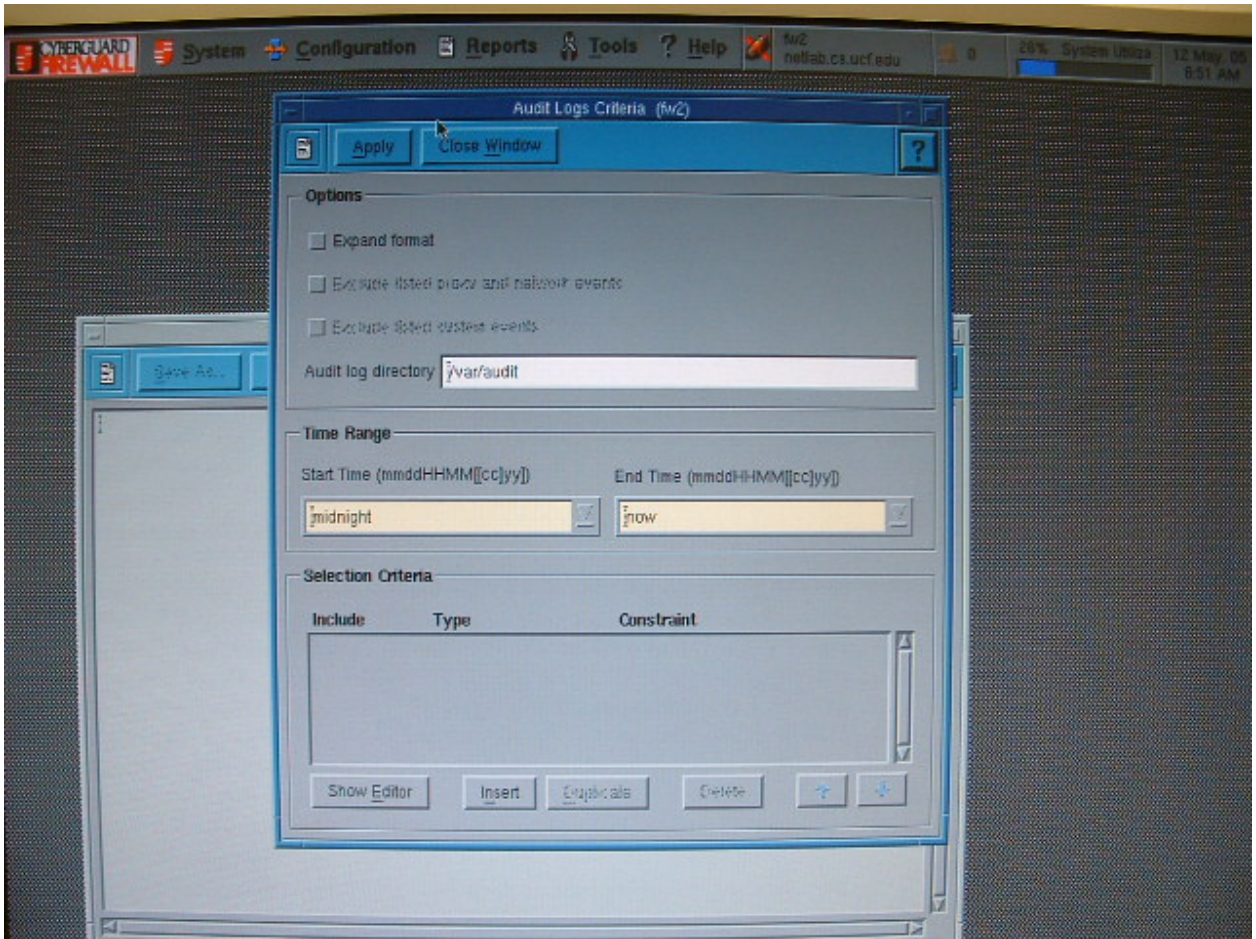


Figure 10: Setting Audit Report logging times

