

# CS392/CS682 Lab 2

## Firewalls

### Introduction:

A traditional packet filter is one of the basic protection mechanisms for a network. This type of firewall can be installed and configured in several ways, depending upon the level of protection needed. In this assignment, you will explore how to configure a firewall. As usual, you will be using Linux as your base operating system; you'll use *ipchains* to make it act as a firewall.

### Prerequisites:

Read about *ipchains* from the following links:

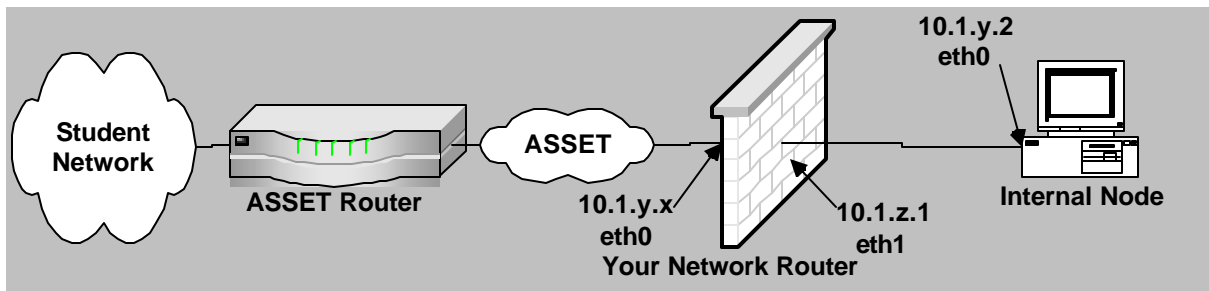
- <http://www.tldp.org/HOWTO/IPCHAINS-HOWTO.html>
- <http://www.flounder.net/ipchains/ipchains-howto.html>

A firewall configuration tool can be found at:

- <http://linux-firewall-tools.com/linux/firewall/index.html>

### Your Task:

This is a group lab and below is the layout of your group network and student network:



### Part A:

Configure the Internal node to meet the following requirements:

- Rules for outgoing traffic:
  - You local machine should be able to communicate with the student network without any restrictions.
- Rules for incoming traffic:
  - All incoming connection requests should be rejected, with the following exception:

- Your machine should respond to Ping from network 10.0.0/24
- Your machine should accept any incoming SSH, HTTP, FTP requests from Network 10.0/16
- Your machine should accept any incoming telnet connections from the machine 10.0.0.1 and 10.0.0.110.
- All multicast traffic should be allowed
- OSPF traffic should be allowed

### **Part B:**

Flush all firewall rules from your internal node and configure your network router to be a firewall with the following requirements:

- Rules for outgoing traffic from internal node:
  - Outgoing SSH, and ICMP traffic should be allowed
  - All multicast traffic should be allowed
  - OSPF traffic should be allowed
  - All other traffic should be blocked
- Rule for incoming traffic to protected server:
  - All incoming SSH, http, SMTP, Ping, and anonymous ftp should be permitted
  - All multicast traffic should be allowed
  - OSPF traffic should be allowed
  - All other incoming traffic should be blocked

### **Part C:**

Answer the following question:

- 1) In your own words describe how ipchains work?
- 2) Why does ipchains need kernel support?
- 3) What is the difference between input, output and forward chains?
- 4) What is the difference between deny, reject, and accept?
- 5) What the problem with ipchains in terms of robustness, speed and functionalities?
- 6) What are the other alternative packages that can be used instead of ipchains in Linux?
- 7) Any idea why multicast and OSPF traffic should is allowed? What are the drawbacks of allowing multicast traffic?

### **What to Submit?**

- 1) ipchains rules fro both part A and B. If you used the firewall tool then only submit the rule you changed.
- 2) Answers for part C