CptS/EE 455
Spring 2002
Project 4
Assigned: Mon Apr 21, 2002
Due: in class Fri May 3, 2002
10% per day penalty for late submissions;
No submissions accepted after May 7, 5PM

Summary

In this project you will set up a firewall for a simulated network. This should give you a good sense of what firewalling is about, and also will serve as a review of concepts at the application, network and transport layer.

Logistics

- Due to the limited lab equipment available, you may work with up to 4 partners on this project (5 people total).
- For this project, the lab machines involved (see below) are off-limits for remote work: you must be present in the lab to use the machines since it is not possible to have more than one experiment at a time going on with the iptables.
- The other professors whose students are using the lab have agreed that cs455 students have priority on the firewall machines. If you have any difficulty about this let me know.
- In the interests of access for all, observe a 1 hour time limit when others are waiting to use the machines.
- To the extent that you can, develop your rule sets before you show up in the lab. It is *possible* to write all the required rules without ever touching a firewall machine, but you need to actually set them up on a machine to complete the assignment.

What to turn in

In class on the due date, turn in printed listings (in this order please) of your:

1. Cover sheet with your name, your partners' names, project #, submission date, and submission directory name.
2. List of the iptables commands, in order, that you used to set up the firewall rules.
3. Listing of your firewall rules obtained using the `/sbin/iptables –L –v` command
4. COMMENTS file – see below. Even if you work with partners on the project, the COMMENTS file is to be your *personal, individual* work

These files are also to be stored in the /net/cs455/students/YOURNAME/project4/ directory prior to class on the due date. Partners should each store a copy of the files in her or his own directory. Make sure that each file clearly indicates who your partners are.

Either preceding the due date or during finals week you will each need to schedule an individual appointment with one of the TAs to demonstrate your firewall and to describe its operation.

Specifications

In the NIF lab we have set up 3 simple networks behind firewalls. The firewall machines are nif-c17, nif-c24 and nif-c25. Each firewall uses network address translation (NAT), as discussed in class on Friday, April 18, to serve a network of machines attached to a second Ethernet interface. Each of these so-called "protected networks" has network address 10.0.1.0/24. The protected networks each have a single machine on them (in addition to the firewall machine) with address 10.0.1.1. Each firewall machine has address 10.0.1.254 on its protected network while retaining its normal EECS-network address on the EECS network. The correspondence between machines on the protected networks and the firewalls is given in the following table:

Firewall	EECS address	Protected Address	Protected Host	Protected Host Address
nif-c17	199.237.74.148	10.0.1.254	nif-c18	10.0.1.1
nif-c24	199.237.74.160	10.0.1.254	nif-c33	10.0.1.1
nif-c25	199.237.74.161	10.0.1.254	nif-c39	10.0.1.1

The same set of filtering rules will work on any of the firewall machines since the protected network addresses are the same on all of them. (The same cannot be said of the NAT rules which have to be specific to each firewall – but you will **not** be changing the NAT rules which we have set up). The rules you set up will all go in the FORWARD chain of the filter table.

Even though each of the protected networks has only a single machine on it, you must imagine that there are many more machines and set up the rules according to the following specifications:

1. All protected machines must be able to do DNS lookups through the firewall using both TCP and UDP.
2. There is an (imaginary) SMTP server at 10.0.1.250 that serves as an application proxy for mail. This is the only machine allowed to make outgoing SMTP connections and to receive incoming SMTP connections.
3. There is an (imaginary) web server at 10.0.1.245 for external users. External users must be able to initiate http (TCP port 80) and https (TCP port 443) connections to this server.
4. There are (imaginary) internal servers at 10.0.1.100 and 10.0.1.101 for internal users. These machines should have no access from or to the outside except for DNS (rule 1).
5. Outgoing telnet connections are not allowed from any machine.
6. The (real) host at 10.0.1.1 is allowed to send and receive anything except SMTP and telnet.
7. All other machines (not having addresses mentioned above) on the network are workstations for which only incoming ssh connections (TCP

port 22) are allowed; any outgoing TCP connections are allowed unless another policy says not; no incoming or outgoing UDP packets are allowed unless another rule says otherwise.

Note that to actually make incoming connections work would require additional modifications to the nat table. **DO NOT** change the **nat table**: you can really make a mess of things not only for these machines but potentially for others as well. You **must only** change the **filter table**. ***I mean this*: if you change the nat table or the mangle table and it causes problems on the EECS network *you will receive an F as your semester grade for the course*.**

Implementation Notes

Before testing your rules, you will want to make sure that the iptables on the firewall machine are in a known state. You can do this with the command

```
/sbin/iptables-restore /root/nat_iptables
```

You would also have to do this if for some reason you rebooted a firewall machine.

If you have to reboot one of the protected machines make sure that the firewall machine is running and that its iptables are in a known-good state first.

Citizenship: `iptables` and `iptables-restore` normally require root privileges. I have overridden this on the firewall machines. I expect you to exercise due care and not abuse the privilege being granted to you for this project.

Additional resources

The primary references you will need for this project are the iptable man pages and the Packet Filtering HOWTO.

The manual pages for the iptables command:

```
man iptables
```

will tell you everything you need to know, albeit without much explanation.

The Linux 2.4 Packet Filtering HOWTO: http://netfilter.samba.org/documentation/HOWTO//packet-filtering-HOWTO.html. Translations of this document into many languages are available from http://netfilter.samba.org/documentation. This document was created by Rusty Russell, the developer who created iptables. It is only about 20 pages but covers the material well. You only need to be concerned with the use of the iptables command. Ignore everything about how to install iptables and so forth.

IP reference handout from SANS Institute. I have only the hardcopy handout, no web reference. The System Administration, Networking and Security Institute (www.sans.org) is devoted to providing forums where people in these fields can share information about challenges that face them. Among many other valuable pages, they offer in cooperation with the FBI a list of the top 20 internet security vulnerabilities at www.sans.org/top20.htm.

The Iptables Tutorial by Oskar Andreasson is a much longer document (96 pages) that might be of interest. It's at http://www.linuxvoodoo.com/howto/iptables/iptables-tutorial.html. Likewise, here ignore everything except use of the iptables command.

Grading

- 50% of the grade will be for working/correct rules
- The remaining 50% of the grade will be for your COMMENTS file and the justification it contains for the rules that you came up with.
- This project carries half the weight of the previous projects in your final grade. The essay assigned last week carries the same weight as this project.

COMMENTS file

Note: Even if you work with partners, you are required to submit your ***own*** COMMENTS file, that is your *personal, individual* work.
The COMMENTS file for this project will be a mini-paper about firewalls and your firewall implementation. In your paper:

- Describe how NAT allows the protected network to have the same network address behind each of the three firewalls, even though these are separate Ethernets.
- Describe the structure of your rules. Did you use user-defined chains as subroutines? What default policy did you choose and why?
- Argue that your rules are correct: briefly show how they implement each of the specifications.
- The specifications don't say anything about ICMP. What would you recommend as a policy for ICMP packets? Without going into detail, how would implementing such a policy affect your rules?
- What other important policy issues do you think are not addressed by the specifications for this project?
- Finally, please tell me how long you spent on this project.