Lab 5: Firewalls and Network Address Translation (NAT)

The purpose of this lab is to exercise the use of iptables to build a permissive firewall by selectively filtering packets based on protocol type. It also demonstrates how addresses may be translated from private addresses to public and vice versa as they pass in and out of the firewall. The goal of this lab is to allow internet access to the hosts in Rivendell, and to allow hosts in the Shire only telnet access, and no other, to a single server in Rivendell. Elrond will act as the gateway/firewall between Rivendell and the Shire.

Supplies

- VMWare Server 1.08 or higher
- 192 VMs shown below

Preconfiguration

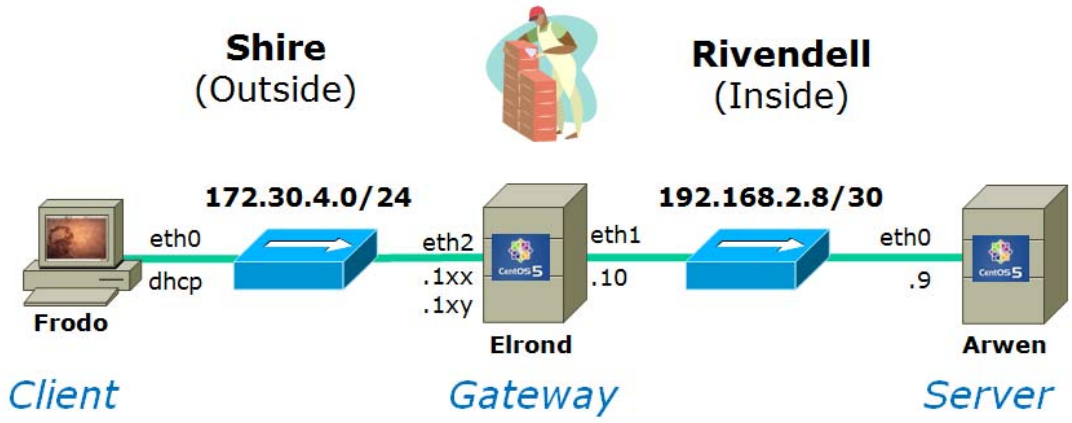
- Original versions of all VMs. Note, this will set the network configurations back to down or DHCP settings.
- You will need access to a DHCP server to assign addresses for the 172.30.4.0/24 network. This is already configured if the lab is done using the CIS VMware Stations in the CIS Lab (room 2504) or the CTC. If you plan to do this lab at home see: http://simms-teach.com/howtos/129-working-at-home.pdf

Forum

Use the forum to ask and answer questions, collaborate, and report any equipment issues. Post tips and any lessons learned when you have finished. Forum is at: http://simms-teach.com/forum/viewforum.php?f=18

Background

Note that the setup shown below indicates that Elrond is the only host in Rivendell that will have access to the Internet. That is because Elrond has a network interface directly onto the 172.30.4.0 network. For the sake of this lab, we will treat the 172. IP addresses as if they were public and the 192. addresses as private. To the world outside of the firewall, your gateway provides the public address of 172.30.4.1N2. The Rivendell telnet server will appear to have a public address of 172.30.4.5



The commands we will be using for this lab are:

- telnet
- lokkit
- modprobe
- iptables
- ping
- route
- ifconfig
- rpm

Procedure

Setup

1. Temporarily connect Arwen to the lab network using DHCP and install the telnet-server package. Refer back to Lab 4 if needed.
2. For static IP addresses for Elrond use the IP table in the appendix.
3. Cable and configure the diagram above using permanent addresses for Elrond and Frodo. You may wish to leverage the NIC configurations you used for Lab4.

Part I

In this step, you will setup the above network with no firewall and verify connectivity in both directions through the gateway/firewall.

1. Log in to the gateway, Elrond, and join the 172.30.4.0 subnet as your outside (eth2) interface.
2. Turn on IP forwarding, and set the default gateway to 172.30.4.1 (the Internet)
3. Disable the firewall by running the **lokkit** command and select **Disabled.** Turn off SELinux as well.
4. Log in as root on the Rivendell server, Arwen, and enable and start the telnet service by editting the */etc/xinetd.d/telnet* file and restarting xinetd:
   killall -1 xinetd

5. Note: this is an alternative to **service xinetd restart** for re-reading configuration files.
6. Make sure Arwen has a default route to the gateway you are using.
7. Verify that your Rivendell hosts are set up for DNS services.
   You can use 207.62.187.54 as your DNS server
   Question: Why do we need DNS Name Resolution?
   The */etc/resolv.conf* file should look like the following:
   nameserver 207.62.187.54
   (Replace the existing contents of *resolv.conf* if it does not match the above.)
8. Verify that the router (Elrond) can run a telnet session on the Rivendell Telnet server.
9. Verify that you can ping your router/firewall from either side of its interface, i.e. ping it from a host in the Shire (Frodo) and from the Telnet server (Arwen).

Part II

In this procedure we will load the kernel modules required for packet filtering and Network Address Translation. After loading the required modules, we will filter out all packets to, from, and through our firewall, thus isolating the Rivendell network.

1. Log in to your firewall/gateway as root.
2. List the current IPTables settings and note the default values with no firewall: iptables -L
3. Now filter all packets by setting the default policy of the three chains in the filter table to DROP:
   iptables -P INPUT DROP
   iptables -P FORWARD DROP
   iptables -P OUTPUT DROP
4. Verify that no network traffic can enter, leave or pass through the firewall by attempting to ping the firewall/router from within Rivendell and from the Shire:
   From the Telnet server (Arwen): **ping 192.168.2.10**
   From the Shire client (Frodo): **ping 172.30.4.1xx**
   Note that both of these tests worked before we set the filter chains to DROP

Part III

Now we will configure the firewall. Since we want to allow outside hosts to use our Telnet server, will allow only Telnet packets to be forwarded through our firewall from the outside world; however we will allow all packets generated within Rivendell to be forwarded to the outside world.

1. Allow any new connections initiated from inside our firewall to propagate through the firewall to the outside world:
   iptables -A FORWARD -s 192.168.2.8/30 -d 0/0 -m state --state NEW -j ACCEPT
2. Allow packets from the outside destined for our Telnet server to pass through the firewall:
   iptables -A FORWARD -s 0/0 -d 192.168.2.9 -m state --state NEW,ESTABLISHED,RELATED -p tcp --dport 23 -j ACCEPT
3. Now allow all necessary packets supporting established connections to pass through:
   iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

4. For completeness we should also allow our firewall to output packets:
   iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
5. And allow our internal network to send any packets to the firewall/gateway:
   iptables -A INPUT -i eth1 -s 192.168.2.8/30 -d 192.168.2.10 -m state --state NEW -j ACCEPT
   iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
6. Verify that Arwen within Rivendell can now ping the firewall.
7. Verify that Frodo can telnet into Arwen but not ping Elrond.

Part IV

Now we will provide Network Address Translation to allow all hosts within Rivendell to access the Internet, and allow all hosts outside the firewall to access our Telnet server through a "public" address of 172.30.4.5

1. Set up the 172.30.4.5 IP address as an IP-alias to the external interface of our firewall (eth2):
   ifconfig eth2:0 172.30.4.1xy netmask 255.255.255.0 broadcast 172.30.4.255
   Note 1xy is your second static IP address assigned to your station from the IP table in the Appendix.
2. Run the **ifconfig** command to see the new sub-interface.
3. Allow any packets destined to 172.30.4.1xy to be translated to 192.168.2.9
   iptables -t nat -A PREROUTING -i eth2 -d 172.30.4.1xy -j DNAT --to-destination 192.168.2.9
4. Now allow for the translation of packets from our Telnet server to this pseudo-public address:
   iptables -t nat -A POSTROUTING -o eth2 -s 192.168.2.9 -j SNAT --to-source 172.30.4.1xy
5. And finally, allow all other hosts in Rivendell to have their private addresses translated to the public address of our firewall:
   iptables -t nat -A POSTROUTING -o eth2 -s 192.168.2.8/30 -j SNAT --to-source 172.30.4.1xy
6. Verify that any Rivendell host can now surf the Internet, and that any Shire host can access the Telnet server via the public address of 172.30.4.1xy
   Note that you can **not** ping the Telnet server from that same host in the Shire:
   telnet *telnet-server* # use the cis192 account

Part V

Part of maintaining a secure firewall is monitoring attempts to contact or pass through the firewall. This may be done using the LOG action on the firewall.

1. Add the following line near the top of the */etc/syslog.conf* file:
   kern.info /var/log/iptables
2. Create this log file in the var/log directory:
   > /var/log/iptables

3. Restart the syslog daemon:
   service syslog restart
4. Add the following two lines to the filter table:
   iptables -A INPUT -j LOG --log-level info --log-prefix "iptables INPUT: "
   iptables -A FORWARD -j LOG --log-level info --log-prefix "iptables FORWARD: "
5. To view the entries added to the log file, run the following command on your Gateway while you ping or otherwise try to attack Rivendell from the Shire:
   tail -f /var/log/iptables
   See if you can collect both log types, input and forward.
   When you are finished viewing the log activity, use ^C to break out of the **tail** command.

Congratulations! You have created a secure network in Rivendell with all machines having access to the Internet!

To turn in

Your *lab05* **text** file should contain the following sections.

- Standard boilerplate information:
  - CIS 192 Lab *XX*
  - *Name*
  - *Date*
  - TBA hours*: X.X*
  - Station number: CIS-Lab-*XX*
- /etc/xinetd.d/telnet file contents
- **iptables –L** output
- i**ptables -t nat –L** output
- enough lines of the **/var/log/iptables** file to show both log messages.
- Command summary

Check your work for completeness then submit as many times as you wish up until the due date deadline. Remember, **late work is not accepted**, so start early, plan ahead for things to go wrong and use the forum to ask questions.

[p]scp lab05 cis192@opus.cabrillo.edu:lab05.lastname

Grading rubric (30 points)

3 points for complete submittal, professional appearance and quality
6 points for correctly configuring the telnet server
6 points for correctly configuring the filter table
6 points for correctly configuring the nat table for the Rivendell hosts
6 points for gathering logfile entries in */var/log/iptables* showing both *input* and *forward* log messages.
3 points for concise and useful command summary

Appendix

Static IP Address Table

Station	IP	Static 1	Static 2
CIS-Lab-01	172.30.4.101	172.30.4.121	172.30.4.122
CIS-Lab-02	172.30.4.102	172.30.4.123	172.30.4.124
CIS-Lab-03	172.30.4.103	172.30.4.125	172.30.4.126
CIS-Lab-04	172.30.4.104	172.30.4.127	172.30.4.128
CIS-Lab-05	172.30.4.105	172.30.4.129	172.30.4.130
CIS-Lab-06	172.30.4.106	172.30.4.131	172.30.4.132
CIS-Lab-07	172.30.4.107	172.30.4.133	172.30.4.134
CIS-Lab-08	172.30.4.108	172.30.4.135	172.30.4.136
CIS-Lab-09	172.30.4.109	172.30.4.137	172.30.4.138
CIS-Lab-10	172.30.4.110	172.30.4.139	172.30.4.140
CIS-Lab-11	172.30.4.111	172.30.4.141	172.30.4.142
CIS-Lab-12	172.30.4.112	172.30.4.143	172.30.4.144
Pod 1		172.30.4.113	172.30.4.145
Pod 2		172.30.4.114	172.30.4.146
Pod 3		172.30.4.115	172.30.4.147
Pod 4		172.30.4.116	172.30.4.148