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

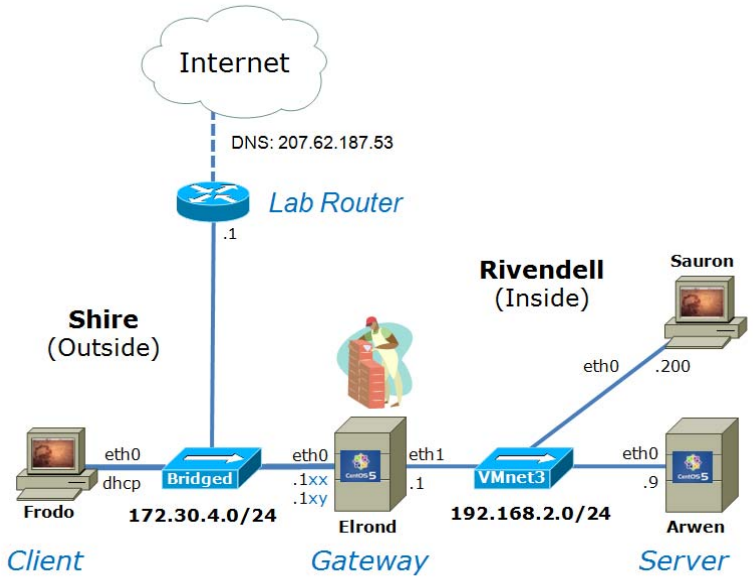
- Original versions of all VMs. Note, this will set the network configurations back to down or DHCP settings.
- You will need access to a DHCP server to assign addresses for the 172.30.4.0/24 network. This is already configured if the lab is done using the CIS VMware Stations in the CIS Lab (room 2504) or the CTC. If you plan to do this lab at home see: http://simms-teach.com/howtos/202-working-at-home-nat.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://opus.cabrillo.edu/forum/viewforum.php?f=5

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 172.30.4.1xx. The Rivendell telnet server will appear to have a public address of 172.30.4.1xy



Select static IP addresses .1xx and .1xy for Elrond from the static IP address table in the Appendix.

Setup

Build the diagram above using the lab VMs.

1. Revert the VMs to their original state.
2. Install the telnet-server package on Arwen:
   - **rpm –qa | grep telnet** to see if it is already installed
   - If not installed:
     - Cable Arwen's first interface to the lab network and use **dhclient eth0** to join the network.
     - Use **yum install telnet-server** to install the service.
     - Configure **/etc/xinetd.d/telnet** and modify **disable = yes** line to **disable = no**
     - Start the Telnet service with **service xinetd restart** or **killall -1 xinetd**
3. Review the commands/files used in previous labs/lessons to configure permanent interface settings, IP aliases, DNS settings, and IP forwarding.
4. Cable and permanently configure the interfaces using the diagram above. Note .1xy on Elrond is an alias.
5. Configure permanently IP forwarding on Elrond.
6. The default routes on Rivendell hosts should be the gateway (Elrond).
7. Don't configure any static routes. For now that means Arwen will not be able to ping Frodo and that's OK.
8. Configure 207.62.187.53 as the DNS server for the Rivendell VMs.
9. Restart network services with **service network restart** (CentOS VMs) and **/etc/init.d/networking restart** (Ubuntu VM).
10. Test that both Shire and Rivendell hosts can ping their side of the Gateway (Elrond).
11. Test internet connectivity for both Frodo and Elrond.

Part I

In this step, you will open port 23 on Arwen and disable the firewall on Elrond.

1. Make a backup of the current firewall
   iptables-save > /etc/sysconfig/iptables.bak
2. On Elrond, disable the firewall by running the **lokkit** command and select **Disabled.**
3. On Elrond, show the firewall with **iptables –L -n**
4. On Arwen, show the firewall with **iptables -L -n --line-numbers**
5. On Arwen, open port 23 for incoming new Telnet connections by inserting a new rule at line 10: **iptables -I RH-Firewall-1-INPUT 10 -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT** (all on one line)
6. Show the firewall again to check your change was made. Both port 22 (SSH) and 23 (Telnet) should accept new connections.
7. Just to practice deleting some rules, lets plug the CUPS universal printing ports (TCP & UDP 631) on Arwen by using **iptables -D RH-Firewall-1-INPUT 6** twice. Note this deletes original lines 6 and 7 because the file is renumbered after the first rule is deleted.
8. On Elrond, run a telnet session on the Rivendell Telnet server (Arwen).
9. Verify that you can ping your gateway/firewall (Elrond) from either side, i.e. ping it from a Shire host and from a Rivendell host.

Part II

In this section we will filter out all packets to, from, and through our firewall, thus isolating the Rivendell network.

1. Log in to your firewall/gateway (Elrond) as root.
2. List the current IP Tables settings and note the default policies 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 192.168.2.1**
   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. FORWARD chain: Allow any new connections initiated from inside our firewall to propagate through the firewall to the outside world:
   iptables -A FORWARD -s 192.168.2.0/24 -d 0/0 -m state --state NEW -j ACCEPT

2. FORWARD chain: 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. FORWARD chain: Now allow all necessary packets supporting established connections to pass through:
   iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
4. OUTPUT chain: For completeness we should also allow our firewall to output packets:
   iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
5. INPUT chain: Allow our internal network to send any packets to the firewall/gateway:
   iptables -A INPUT -i eth1 -s 192.168.2.0/24 -d 192.168.2.1 -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 172.30.4.1xy

1. Allow any packets destined to 172.30.4.1xy to be translated to 192.168.2.9
   iptables -t nat -A PREROUTING -i eth0 -d 172.30.4.1xy -j DNAT --to-destination 192.168.2.9
2. Now allow for the translation of packets from our Telnet server to this pseudo-public address:
   iptables -t nat -A POSTROUTING -o eth0 -s 192.168.2.9 -j SNAT --to-source 172.30.4.1xy
3. 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 eth0 -s 192.168.2.0/24 -j SNAT --to-source 172.30.4.1xx
4. 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't ping the Telnet server from that same host in the Shire.

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.
6. Make your new firewall permanent with
   iptables-save > /etc/sysconfig/iptables then **service iptables restart**

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*
- On Arwen: **cat /etc/xinetd.d/telnet** output
- On Arwen: **iptables –L -n** output
- On Elrond: **ifconfig | grep –C1 eth** output
- On Elrond: **iptables –L -n** output
- On Elrond: **iptables -t nat –L –n** output
- On Elrond: **cat /etc/sysconfig/iptables**
- On Elrond: 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
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 (http://simms-teach.com/docs/static-ip-addrs.pdf)

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