Cabrillo College

Lab 5: Firewalls and NAT (Network Address Translation)

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 CIS Lab only telnet access, and no other, to a single server in Rivendell. Elrond will act as the gateway/firewall between Rivendell and the CIS Lab.

Supplies

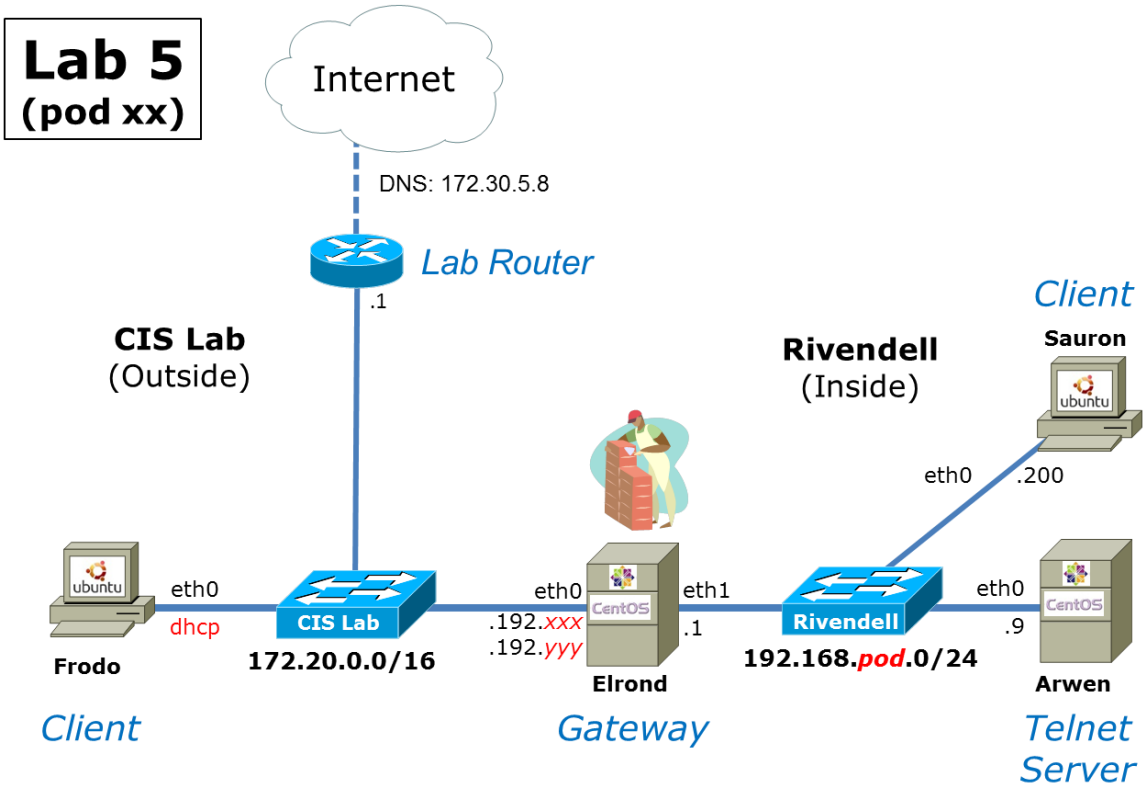
- Virtualization: VMware ESXi/vSphere (VLab)
- Centos VMs: Elrond and Arwen
- Ubuntu VMs: Frodo and Sauron
- Virtual networks: Rivendell and Mordor

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://oslab.cabrillo.edu/forum/

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 CIS Lab network. For the sake of this lab, we will treat the 172 IP addresses as if they were public and the 192 IP addresses as private. To the world outside of the firewall, your gateway provides the public address of 172.20.192.xxx. The Rivendell telnet server will appear to have a public address of 172.20.192.yyy



Select unique static IP addresses *.xxx* and *.yyy* based on your pod number and the CIS Lab VLab Assignments table at: http://simms-teach.com/docs/cis192/Pod-Assignments-192-sp13.pdf

Preparation

- ☐ Revert VMs to their Pristine state
- ☐ Temporarily join Arwen to the CIS Lab network and use yum to install the telnet-server package. Use the Telnet module in Lesson 5 as a reference.
- ☐ Make a network map and show your networks and interface configurations. Add any other crib sheet notes as desired. Ideally you could use your map and notes to quickly reconstruct this lab again in the future.
- ☐ On Opus, make a copy of the *lab05* report template file in */home/cis192/depot* in your home directory. Edit the header of this file with your own information and record all the information requested.

Setup

Build the diagram above using the lab VMs.

- ☐ Cable and permanently configure Rivendell hosts:
  - IP addresses on all interfaces
  - Default gateways (all Rivendell hosts should specify Elrond)
  - DNS server (/etc/resolv.conf) and for short hostnames append cislab.net
  - A second IP address on Elrond using an alias
  - Packet forwarding on Elrond
- ☐ Turn off NetworkManager on Ubuntu systems with **service network-manager stop** so any changes we make do not get undone.

- Add a static route on Frodo so it can reach Rivendell hosts.
- Add IP/name pairs to /etc/hosts to allow hostnames to be used in this lab rather than IP addresses.
- Verify that Elrond can ping the Lab Router, Frodo, Sauron and Arwen and google.com

Part I

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

1. Disable Elrond's firewall:

    - View default firewall with: **iptables -nL**
    - Backup the current firewall:
      cp /etc/sysconfig/iptables /etc/sysconfig/iptables.bak
    - Flush all ruleswith: **iptables -F**
    - Verify changes with: **iptables -nL**
    - Make the firewall changes permanent with: **service iptables save**
    - Verify Frodo can now ping Arwen

2. Open telnet port 23 on Arwen:

    - Show firewall rules with: **iptables -nL --line-numbers**
    - Determine the line number, ***n***, of the final "REJECT all" rule on the INPUT chain.
    - On Arwen, open port 23 for incoming new Telnet connections by inserting a new rule at line ***n***:
      iptables -I INPUT *n* -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
    - Verify ports 22 and 23 are opens with **iptables -nL**
    - Make the firewall permanent with: **service iptables save**

3. Telnet from Elrond into Arwen,
    - Install telnet client with: **yum install telnet**
    - Telnet to Arwen with: **telnet arwen**
      (be patient, it may take some time for DNS to time out before getting a login prompt)
    - Login as cis192
    - Use **exit** to end the session and get back to Elrond.

Part II

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

On Elrond,

- View the firewall again and note the default poilicies:
  iptables -nL
- Now set the default policy on all three chains in the filter table to DROP:
  iptables -P INPUT DROP
  iptables -P FORWARD DROP
  iptables -P OUTPUT DROP

- Verify the new policies with: **iptables -nL**
- Verify that no network traffic can enter, leave or pass through the firewall by:
  - Arwen should no longer be able to ping Elrond
  - Frodo should no longer be able to ping Elrond
  - Elrond should no longer be able to ping the Lab Router

Part III

Now we will configure Elrond's 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. In addition we will allow all packets generated within Rivendell to be forwarded to the outside world.

Elrond's FORWARD chain:

- Allow all necessary packets supporting established connections to pass through:
  iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
- Allow new connections initiated from inside our firewall to propagate through the firewall to the outside world:
  iptables -A FORWARD -s 192.168.*pod*.0/24 -d 0/0 -m state --state NEW -j ACCEPT
- Allow packets from the outside destined for our Telnet server to pass through the firewall:
  iptables -A FORWARD -s 0/0 -d 192.168.*pod*.9 -m state --state NEW -p tcp --dport 23 -j ACCEPT *(all on one line)*

Elrond's OUTPUT chain:

- For completeness we should also allow our firewall to output packets:
  iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

Elrond's INPUT chain:

- Allow return traffic from any connections initiated from Elrond:
  iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
- Accept any new incoming connections from our internal Rivendell network:
  iptables -A INPUT -i eth1 -s 192.168.*pod*.0/24 -d 192.168.*pod*.1 -m state --state NEW -j ACCEPT

Test:

- Verify that Arwen and Sauron can now ping Elrond.
- Verify that Frodo can telnet into Arwen but not ping Arwen
  (be patient, it may take some time for DNS to time out before getting a login prompt)

Part IV

Now we will provide NAT (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" IP address.

Elrond:

- Allow any packets destined to 172.20.192.*yyy* to be translated to 192.168.*pod*.9
  iptables -t nat -A PREROUTING -i eth0 -d 172.20.192.*yyy* -j DNAT --to-destination 192.168.*pod*.9
- 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.*pod*.9 -j SNAT --to-source 172.20.192.*yyy*
- 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.*pod*.0/24 -j SNAT --to-source 172.20.192.*xxx*
- Save your firewall with: **service iptables save**

Test:

- Verify that any Rivendell host can now surf the Internet
- Verify both Frodo and Opus can access (but not ping) the Telnet server via the public address of 172.20.192.*yyy*.

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.

- Add the following line near the top of the RULES section in */etc/rsyslog.conf* file:
  kern.info /var/log/iptables
- Create this log file in the var/log directory:
  > /var/log/iptables
- Restart the system logging daemon:
  service rsyslog restart
- 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: "
- 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 CIS Lab network:
  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 Ctrl-C to break out of the **tail** command.
- Make your new firewall permanent with:
  service iptables save

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

To turn in

Record the following in your lab05 report:

- Fill out all header information at the top of your lab report
- On Frodo, use the script command or Copy & Paste to record a telnet login session from Frodo to Arwen via Elrond's public IP alias.

- On Sauron, record the route to Opus with output from:
  - **mtr -c2 --report opus.cabrillo.edu**
- On Arwen, record your telnet and firewall configuration with output from :
  - **cat /etc/xinetd.d/telnet**
  - **cat /etc/sysconfig/iptables**
- On Elrond, record your interfaces, firewall/NAT rules, and iptables log with output from:
  - **ifconfig**
  - **cat /etc/sysconfig/iptables**
  - **cat /var/log/iptables**

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

- **cp lab05 /home/rsimms/turnin/cis192/lab05.$LOGNAME**
- Email your network map to me at: **risimms@cabrillo.edu**

Grading rubric (30 points)

2 points for complete report header information
4 points for network map

3 points for correct telnet session (to Arwen using Elrond's public IP alias)
3 points for correct trace route from Sauron to Opus

3 points for correctly configuring telnet on Arwen
3 points for correctly configuring firewall on Arwen

3 points for correctly configuring the Elrond firewall rules
3 points for correctly configuring Elrond NAT rules
3 points for INPUT log entries on Elrond caused by Frodo
3 points for FORWARD log entries on Elrond caused by Frodo