Lab 9.2 Introduction to PF
IN715 Networks Three

September 18, 2014

Introduction

Packet Filter (PF) is the powerful and fairly easy to configure firewall system included in OpenBSD since version 3.0. In this lab we will begin exploring the capabilities of PF.

Carry out this lab on the `router2` system on your virtual network. Since you control both sides of that system it is easy to test the effects of your firewall rules.

1 Check your firewall status

Use the command `pfctl -sr` to see your active rules (There should be three of them). Use the online documentation to see what they do.

In practical terms, these rules will let most traffic through. We would like to establish a more restrictive rule set. To begin, edit the file `/etc/pf.conf` and comment out the line that simply says "`pass`". We will add our rules immediately under this point

2 Establish a new rule set

Let's allow the following:

- Allow all ssh traffic.
- Allow DNS requests from 192.168.2.0/24.
- Allow DHCP Relay, meaning DHCP requests must be allowed in, and DHCP Relay traffic must be allowed out.

Since PF is *stateful*, once we allow a particular sort of traffic out we allow responses to that traffic in.

You will need to consult the docs to write your rules. To write each rule, answer the following:

- What action will be taken?
- On what network interface will the traffic be sent or received?
- What is the source (address and port) of the traffic?
- What is the destination (address and port) of the traffic?
- What is the transport protocol of the traffic?

Once you know these things (or have determined that they are not relevant), you can write your rules into the file `/etc/pf.conf`.

3 Load and test your rules

Load the new rules with the command `pfctl -f /etc/pf.conf`. Test your rules to see if they allow the desired traffic while blocking undesired traffic.