Design Document

Jivanjot S. Brar A00774427 January 31, 2014

Firewall Design

The firewall has been design using the Netfilter, iptables. This firewall is a simple personal Linux firewall that implements the following rules:

- Set the default policies to DROP
- Permit inbound/outbound ssh packets
- Permit inbound/outbound www packets
- Allow DNS and DHCP traffic, without which the machine will not function properly.

The firewall is desgined to DROP the following kind of traffic

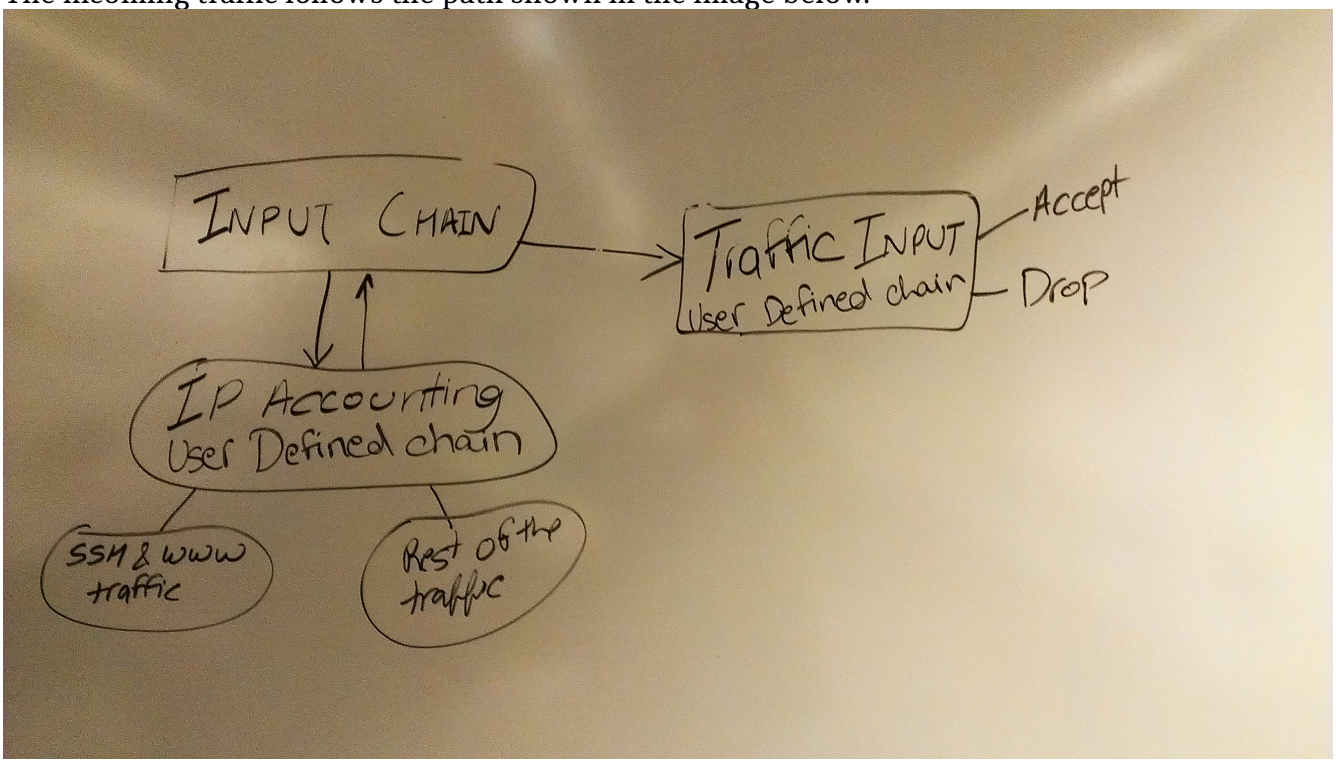
- Drop inbound traffic to port 80 (http) and port 443 (https) from source port less than 1024.
- Drop all incoming traffic from reserved port 0
- Drop all outgoing traffic to port 0
- Drop all inbound SYN packets, unless there is a rule that permits inbound traffic.

The firewall is also designed to keep separate counts for www and ssh traffic versus the rest of the traffic.

Firewall Traffic Path

Incoming Traffic

The incoming traffic follows the path shown in the image below.



Design Document

Jivanjot S. Brar A00774427 January 31, 2014

Any traffic that comes to the default INPUT chain first goes through and IP accounting chains that are user defined. There are two Accounting chains, www-ssh-traffic and noness-traffic. The input chain determines whether the traffic is ssh or www (80, 443), if so, it then sends that traffic to www-ssh-traffic, which is only designed to count and since it doesn't ACCEPT the traffic or DROP it, the traffic comes back to INPUT chains and in which it is then sent into another user defined chain called traffic-in, this chain contains rules, that if matched the traffic is ACCEPT or DROP depending on the rule, and if it doesn't match and the traffic is handled by the default policy, in which cases it is dropped all together.

If the traffic is not www or ssh, it is then sent to noness-traffic chain, whose purpose similar to www-ssh-traffic is only to count and not ACCEPT or DROP. The traffic than follows the same rules as the www and ssh traffic, in which case it is also sent to traffic-in chain and then either ACCEPT or DROPPED by the chain or handled by the default INPUT policy and simply dropped.

Outgoing Traffic

The image below describes the path followed by the traffic when leaving the machine. The path is similar to the path followed by the incoming traffic. The outgoing does the same thing as the incoming traffic. It first goes into the respective user defined accounting chains and then because the traffic hasn't been handled, it then goes into another user defined chain called traffic-out. Traffic-out chain has the same functionality as the traffic-in chain and that is, if the traffic matches any rule defined in this chain, it acts according to the rule the traffic match. If the rules is to ACCEPT the chain accepts the traffic and if the rule says DROP, then it drops the traffic. It the traffic doesn't match any rule in the chain, it is then handled by the default OUTPUT policy, in which case it is simple dropped.