COMP 8006 Assignment 1 Design Doc

Alex Zielinski – A00803488

02/01/2018

Table of Contents

How it Works

There are two scripts within the folder called ***src*** (which can be found in the project folders top directory). The first script is called ***firewall.sh*** which contains the script that configures the firewall. The second script is called ***cleanup.sh*** which flush's all chains, deletes all user defined chains and sets the default policies to ACCEPT.

The firewall implements the following rules:

- Set default policies to DROP
- ACCEPT inbound/outbound SSH traffic (port 22)
- ACCEPT inbound/outbound WWW traffic (HTTP port 80 and HTTPS port 443)
- ACCEPT inbound/outbound DNS traffic (port 53)
- ACCEPT inbound/outbound DHCP traffic (port 67 and 68)
- DROP inbound traffic to port 80 with source port less than 1024
- DROP all port 0 related traffic
- Drop SYN packets unless another rule permits it

On top of this there are three user defined chains (UDC) that implement IP accounting rules:

- **WWW_ACCT chain**
    - This chain is responsible for dealing with all WWW traffic (HTTP and HTTPS). This means that when the INPUT or OUTPUT chain encounter WWW traffic then they forward it to the WWW_ACCT chain where the web traffic is dealt with.
- **SSH_ACCT chain**
    - This chain is responsible for dealing with all SSH traffic. This means that when the INPUT or OUTPUT chain encounter SSH traffic then they forward it to the SSH_ACCT chain where the traffic is dealt with.
- **OTHER_ACCT chain**
    - This chain is responsible for dealing with all other traffic (port 0, DNS, DHCP). This means that when the INPUT or OUTPUT chain encounter traffic that is considered other than that traffic is forwarded to the OTHER_ACCT chain where the traffic is dealt with.

There is also a user defined section located on line 48. This line contains an array variable called USER_PORTS. Users can manually add ports to this array that they would like for the firewall to open. So, is the user wants for example for the firewall to open ports 6000, 7000 and 8000 then they can add those ports to the array variable (the variable would look like this ***USER_PORT=(6000 7000 8000);***).

User Guide

As mentioned earlier there are two scripts located in the ***src*** directory. These two scripts are called ***firewall.sh*** and ***cleanup.sh***. The firewall script configures the firewall based on the rules mentioned in the ***How it Works*** section of this document. In order to run the firewall script, they must navigate to the project's ***src*** folder via terminal and enter the following command:

./firewall.sh

The cleanup script is used to reset the firewall configurations. It flushes all chains, deletes all user defined chains and sets the default chain policies to ACCEPT. In order to run the cleanup script, the user must navigate to the project's ***src*** folder via terminal and enter the following command:

./cleanup.sh

Users can also specify ports that they would like for the firewall to open (that are not part of the script) by adding the port to the USER_PORT array variable located on line 48. So, for example, if the user would like for the firewall to open ports 6000, 7000, 8000 then they simply add the ports to the array as such:

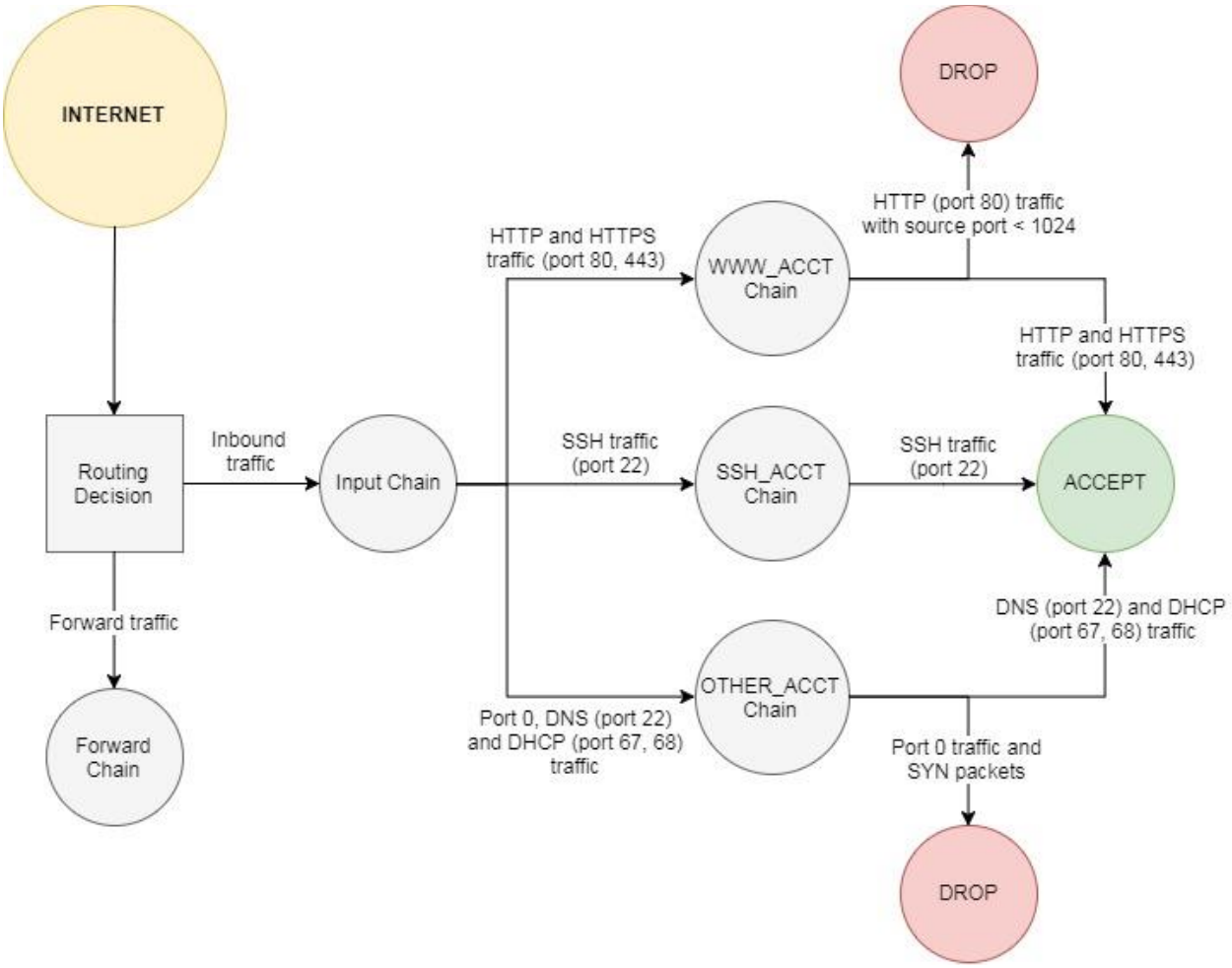
USER_PORT=(6000 7000 8000);

Project folder directory listings

/src
|------ cleanup.sh
|------ firewall.sh
Design Doc
Testing Doc

Finite State Machines

Inbound Firewall Traffic



Outbound Firewall Traffic