Personal Firewall

Ben Soer

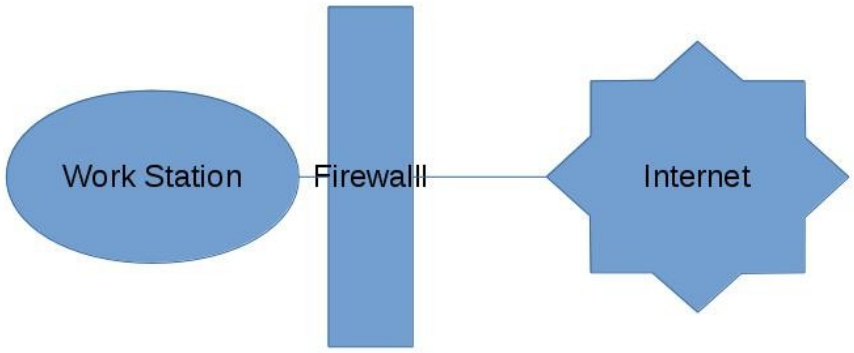
COMP 8006

BTECH Set 6D

Table of Contents

Network Diagram

Below is a high level diagram of what this assignment is accomplishing. The firewall is very simplistic from this view in that it is simply trying to protect a single computer from the outside world. The firewall is installed localy on the workstation it is trying to protect.

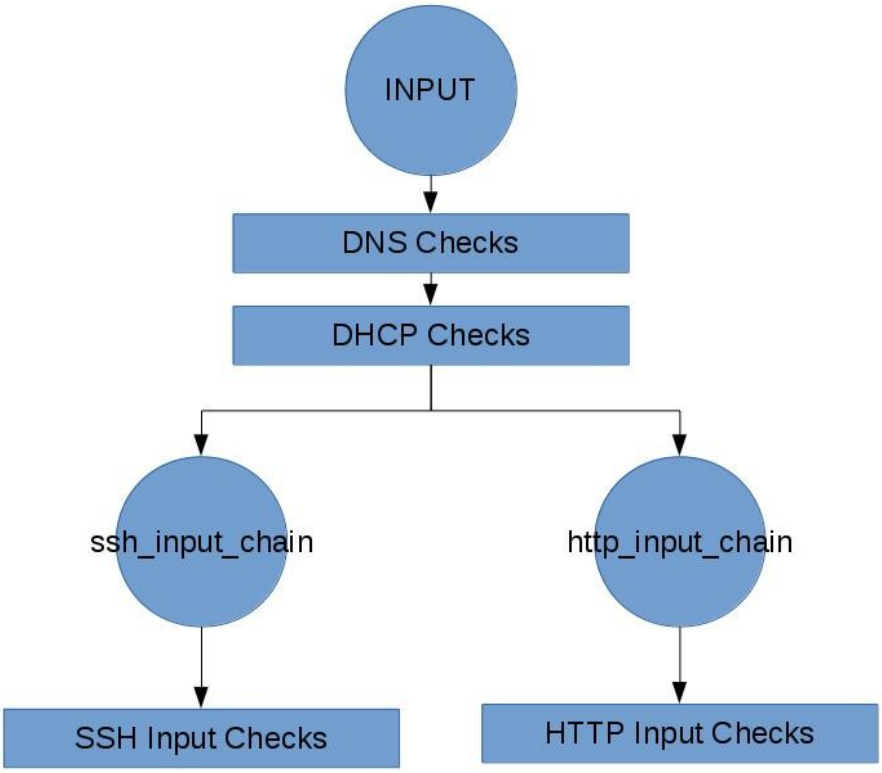


Flow Diagrams

The following diagrams show how packets flow through the firewall from the INPUT and OUTPUT chains. There is a total of 4 user chains that are added aswell to handle the input and output of ssh and http packets. This reduces the number of checks the firewall has to do in order to find a successful chain case and let the packet through.

Input Chain

From the INPUT chain, all data is checked if it is DNS or DHCP data. As this data is likely to be the most common and most time sensitive in terms of responsiveness on the user end, these are evaluated first. After checks are made as to whether the data is SSH or HTTP related. This is done by simply checking source and destination ports. If the source or destination port is 22, the ssh_input_chain user chain is used to evaluate the packet. If the source or destination port is 80 or 443, the http_input chain user chain is used to evaluate the packet. Within each of the ssh_input_chain and http_input_chain there are both evaluation steps and accounting steps that keep track of all accepted packets. With the default policy set to DROP, if the packet completes the chain with no matches, it is automaticly dropped.



Output Chain

From the OUTPUT chain, all data is checked if it is DNS or DHCP data. As this data is likely to be the most common and most time sensitive in terms of responsiveness on the user end, these are evaluated first. After checks are made as to whether the data is SSH or HTTP related. This is done by simply checking source and destination ports. If the source or destination port is 22, the ssh_output_chain user chain is used to evaluate the packet. If the source or destination port is 80 or 443, the http_output_chain user chain is used to evaluate the packet. Within each of the ssh_output_chain and http_output_chain there are both evaluation steps and accounting steps that keep track of all accepted packets. With the default policy set to DROP, if the packet completes the chain with no matches, it is automaticly dropped.