Design Document

Version 1.0

Eric Tsang, A00841554, 6D

|  |
| --- |
| Table of Contents [Table of Contents 1](#_Toc441274111)  [1 Firewall Flow Diagram 2](#_Toc441274112)  [2 Network Diagram 3](#_Toc441274113) |

# Firewall Flow Diagram



|  |  |
| --- | --- |
| Name | Description |
| Start | The script begins execution with root permissions. |
| Configuration | Configuration variables used to modify firewall behavior are declared and initialized. |
| Reset | All firewall rules are flushed, user chains wiped, and default chain policies are set to ACCEPT. |
| Set policies | All default chain policies are set to DROP. |
| Create user chains | The following user chains are created for IP accounting:   * **ICMP**; accounts for all ICMP traffic * **DHCP**; accounts for all DHCP traffic * **DNS**; accounts for all DNS traffic * **SSH\_SVR**; accounts for all inbound SSH connection traffic * **SSH\_CLNT**; accounts for all outbound SSH connection traffic * **WWW\_SVR**; accounts for all inbound HTTP & HTTPS connection traffic * **WWW\_CLNT**; accounts for all outbound HTTP & HTTPS connection traffic |
| Enable protocols | Append rules to the INPUT and OUTPUT chains to jump traffic to their appropriate chains for IP accounting:   * ICMP, DHCP and DNS traffic are jumped to the **ICMP**, **DHCP** and **DNS** chains respectively. * Inbound SSH connection traffic is jumped to the **SSH\_SVR** chain. * Outbound SSH connection traffic is jumped to the **SSH\_CLNT** chain. * Inbound HTTP & HTTPS connection traffic is jumped to the **WWW\_SVR** chain. * Outbound HTTP & HTTPS connection traffic is jumped to the **WWW\_CLNT** chain. |
| Exit | The shell script terminates as it finishes execution. |

# Network Diagram



|  |  |
| --- | --- |
| Name | Description |
| The Internet | The wide area network |
| Modem | Provides internet for the router |
| Router | Connects multiple nodes together, forming a local area network |
| Firewall | Firewall that is in the same machine as *Computer*. It blocks all traffic, except DNS, DHCP, ICMP, SSH, HTTP, and HTTPS. |
| Computer | Node connected to the *Router*. |