**Computer Systems Technology**

British Columbia Institute of Technology

COMP 8006 - Assignment2- Design

Albert Huang &

Aiyan Ma

Jan 28, 2018

# Table of Contents

[Table of Contents 1](#_Toc17482)

[Design 2](#_Toc30358)

[1.1 Inbound Traffic 2](#_Toc32582)

[1.1.1 Flowchart 2](#_Toc14121)

[1.1.2 Description 6](#_Toc18329)

[1.2 Outbound Traffic 7](#_Toc9266)

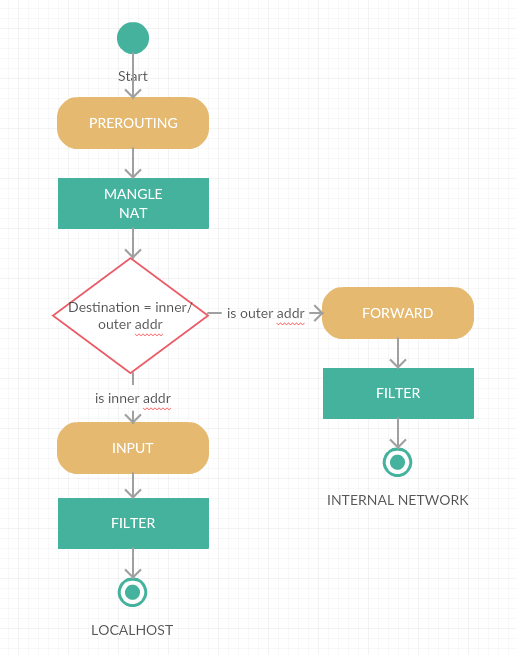
[1.2.1 Flowchart 7](#_Toc540)

[1.2.2 Description 8](#_Toc29931)

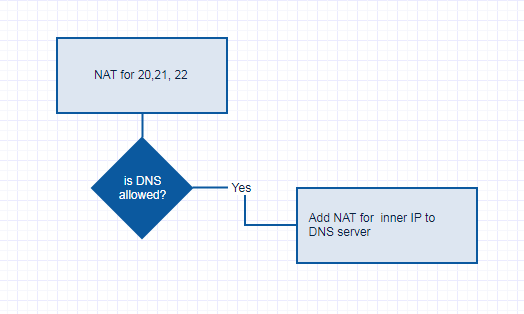
# Design

## 1.1 Inbound Traffic

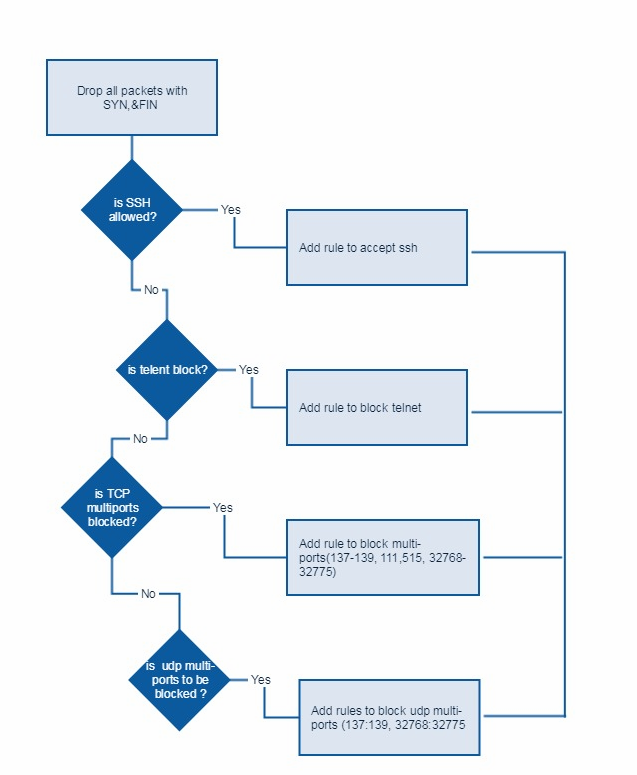
### 1.1.1 Flowchart



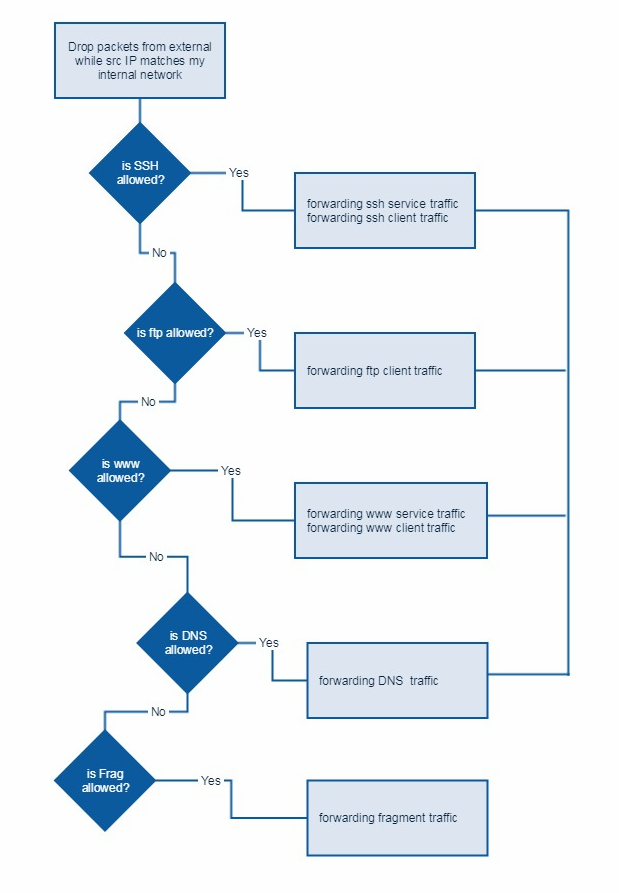
Pre-routing is doing the NAT as below:



Input chain flows as below:



Forwarding Chain Flow as below:



### 1.1.2 Description

1. Setting default policy to DROP
2. Firewall accept Inbound TCP/UDP packets on allowed ports.
3. Firewall accept Inbound ICMP packets based on type numbers.
4. Firewall drop all packets with a source address from the outside matching your internal network
5. Firewall forward DNS inbound/outbound traffic

Firewall accept traffic from port 53 to local machine.

1. Firewall forward SSH inbound/outbound traffic

Firewall accept traffic from/to port 22 to local machine.

1. Firewall forward HTTP/HTTPS inbound/outbound traffic

Firewall accept traffic from/to port 80 and 443 to local machine.

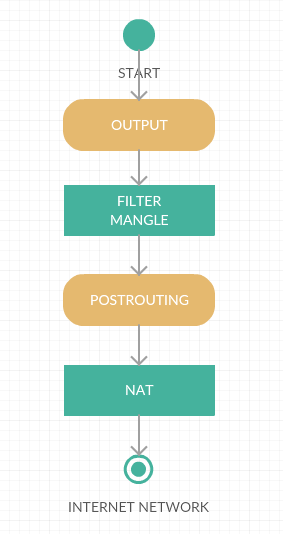
1. Firewall accept fragments.
2. Firewall reject inbound SYN packets to high ports

Firewall drop SYN packets traffic to port 1024~65535

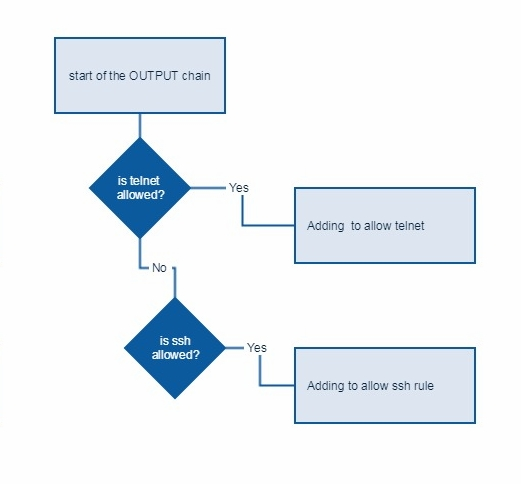
1. Firewall reject TELNET traffic
2. Firewall drop all packets with the SYN and FIN
3. Firewall block all external traffic direct to ports 32768-32775, 137-139, TCP ports 111 and 515

## 1.2 Outbound Traffic

### 1.2.1 Flowchart



Output chain flow chart as:



Post Routing is quite simple to enable SNAT at INET.

### 1.2.2 Description

1. Setting default policy to DROP
2. Firewall do not allow Telnet

Firewall drop all outbound traffic from port 23.

1. Firewall accept SSH outbound traffic

Firewall accept traffic go to internal network machine port 22 from local machine.

1. Firewall accept FTP outbound traffic

Firewall accept traffic go to internet server with port 21.