Stand-Alone Firewalls - Design Work & Testing

David Tran - A00801942 | Cole Rees - A00741578

COMP 6D

COMP 8006 - Assignment 2

British Columbia Institute of Technology

Aman Abdulla

Thursday, February 20 2014

**Design**

**Firewall**

# User-Defined Variables

// allowed tcp packets on these ports

// allowed udp packets on these ports

// allowed icmp packets based on type numbers

// my network address

// my network interface

// outside address space

// outside network device

# Flush the tables

// iptables flush rule sets

// iptables flush user-defined chains

# Set default policies

// input drop

// output drop

// forward drop

# User-Defined Chains

// create and define tcp\_in chain

// create and define tcp\_out chain

// create and define udp\_in chain

// create and define udp\_out chain

# In / Out TCP on these ports

// rules for in and out tcp on defined ports

// permit all incoming tcp packets with state ESTABLISHED

# In / Out UDP on these ports

// rules for in and out udp on defined ports

# In / Out ICMP based on type numbers

// rules for in and out ICMP on specified type numbers

# Drop stuff destined for Firewall

// rules to drop stuff for firewall

# Drop stuff source IP’s that match our internal network

// rules to drop stuff from sources with the same IP as our internal network

# Drop inbound SYN packets unless permitted

# Drop all TCP packets with flags SYN and FIN

// iptables -A INPUT -i $NET\_INTERFACE -p tcp ! --syn --fin -m state --state NEW -j DROP

# Accept incoming fragments

// rules to accept incoming fragments

# Disallow any traffic on telnet port

// iptables -A INPUT -p tcp --dport 23 -j DROP

// iptables -A OUTPUT -p tcp --sport 23 -j DROP

# Block all external traffic directed to ports 32768 - 32775, 137 - 139 and tcp ports 11 and 515

// rule(s) to drop specified ports

# Set Control connection for FTP and SSH to “Minimum Delay”

# Set Control connection for FTP to be “Maximum Throughput”

// rules to do this here

# Traffic Accounting Rules Here

// rules for traffic accounting through tcp, udp and any other that we choose to implement

# Save, Restart and List the IP tables

// save the tables

// restart the daemon

// list them; they should be as we just described above

**Test Script (on tertiary machine)**

// have some user defined variables here

// check to see if old results file exists

// if exists, delete the old one

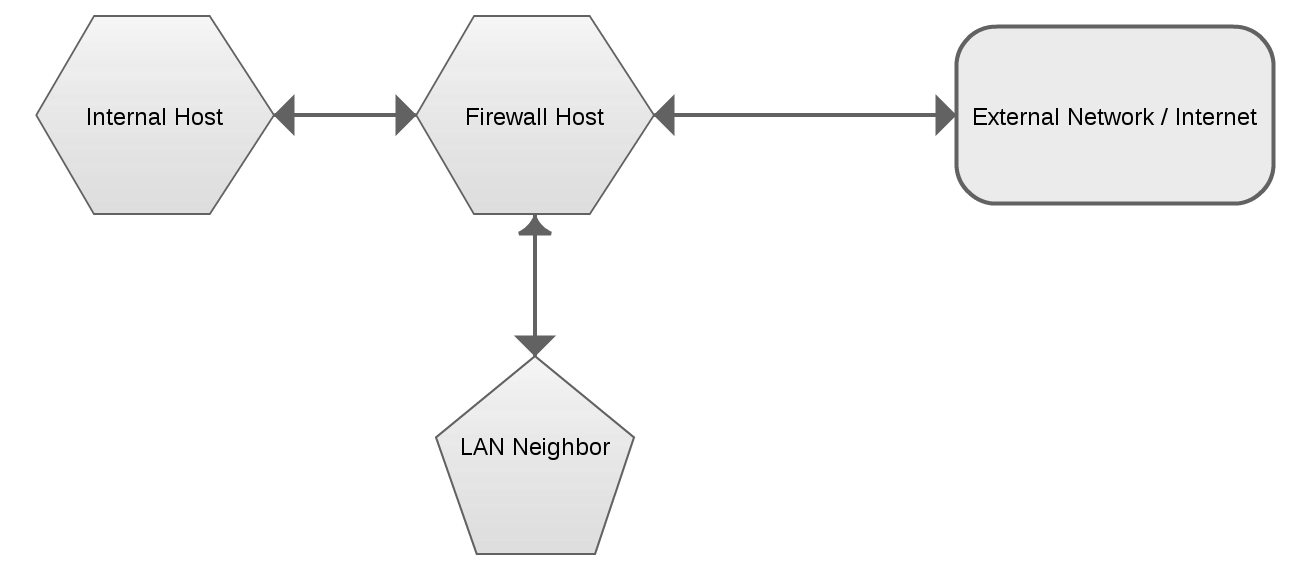
// if doesn’t exist, create a new one

// run hping3 for most of these tests

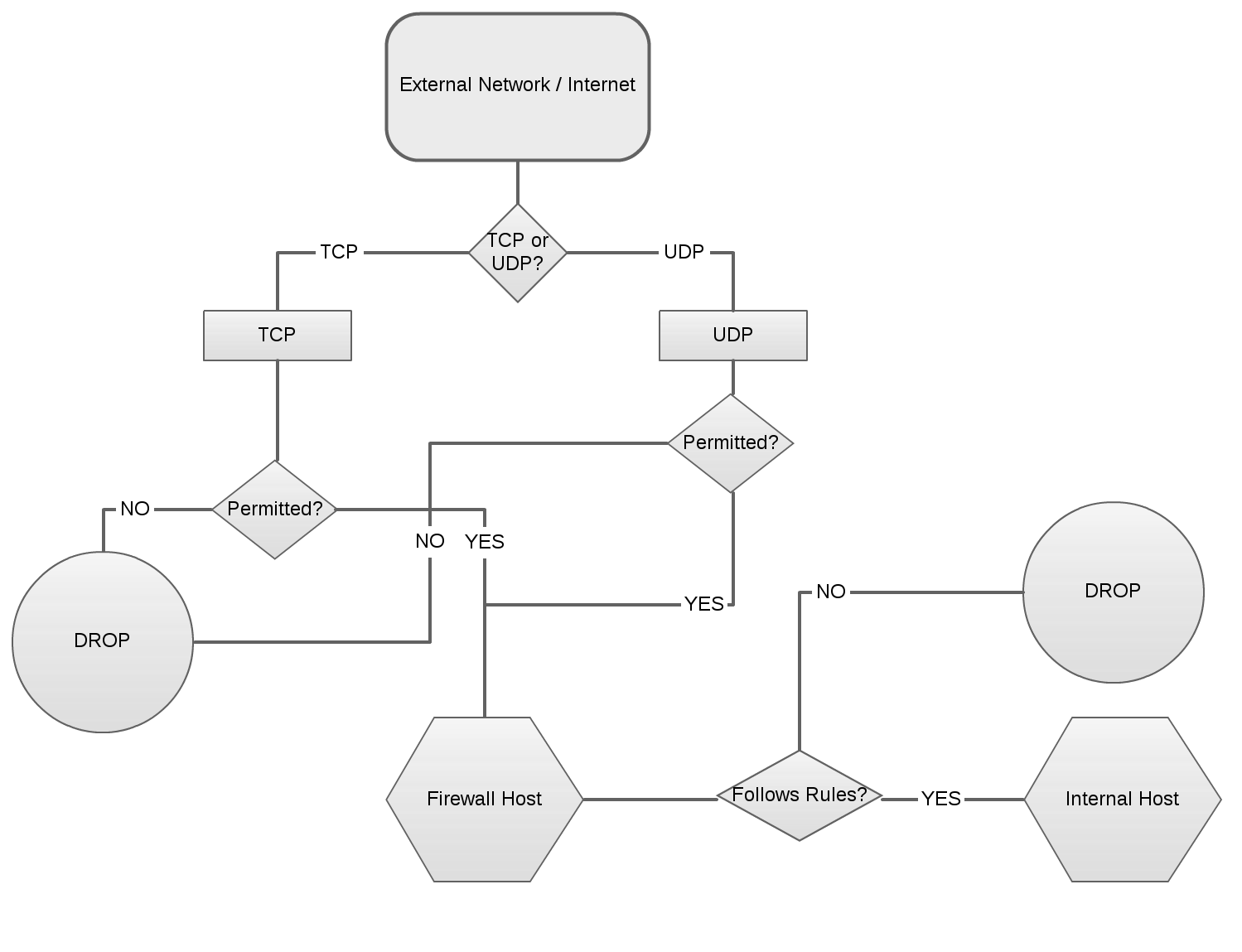
// export to external file

**Diagrams**

**Network Architecture**



**Inbound / Outbound Packet Traversal**



**Testing & Verification**

**Preliminary Setup - Firewall Host**

Go to Settings > Network

For p3p1, click the cogwheel

Select IPv4 and change the Addresses to Link-Local Only

Click Apply and close out of the Settings dialogs.

In Terminal, run the following commands:

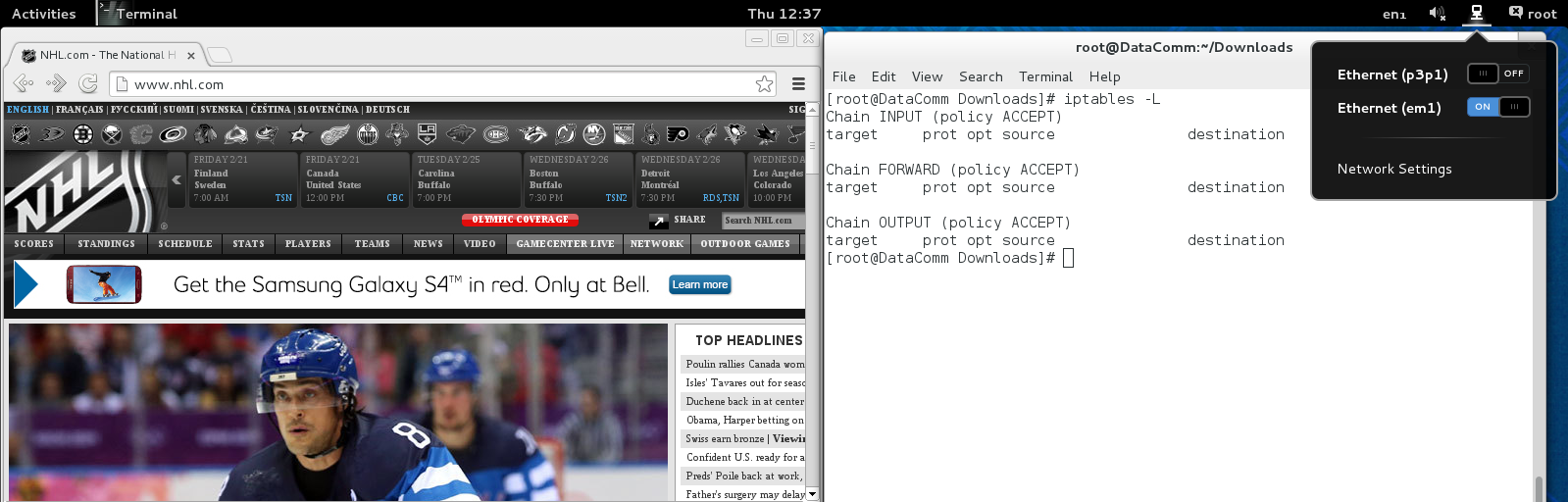
ifconfig -p3p1 192.168.10.1 up

echo "1" >/proc/sys/net/ipv4/ip\_forward

route add -net 192.168.0.0 netmask 255.255.255.0 gw 192.168.0.8

route add -net 192.168.10.0/24 gw 192.168.10.1

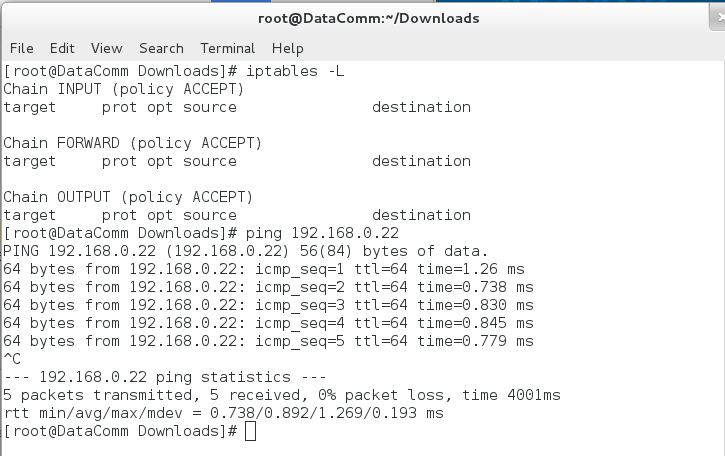
Test Case 1: Test that access to the internet is available through browser



Observations: With no firewall on and with our machine not acting a router to our host, our machine has internet access.

Results: PASSED

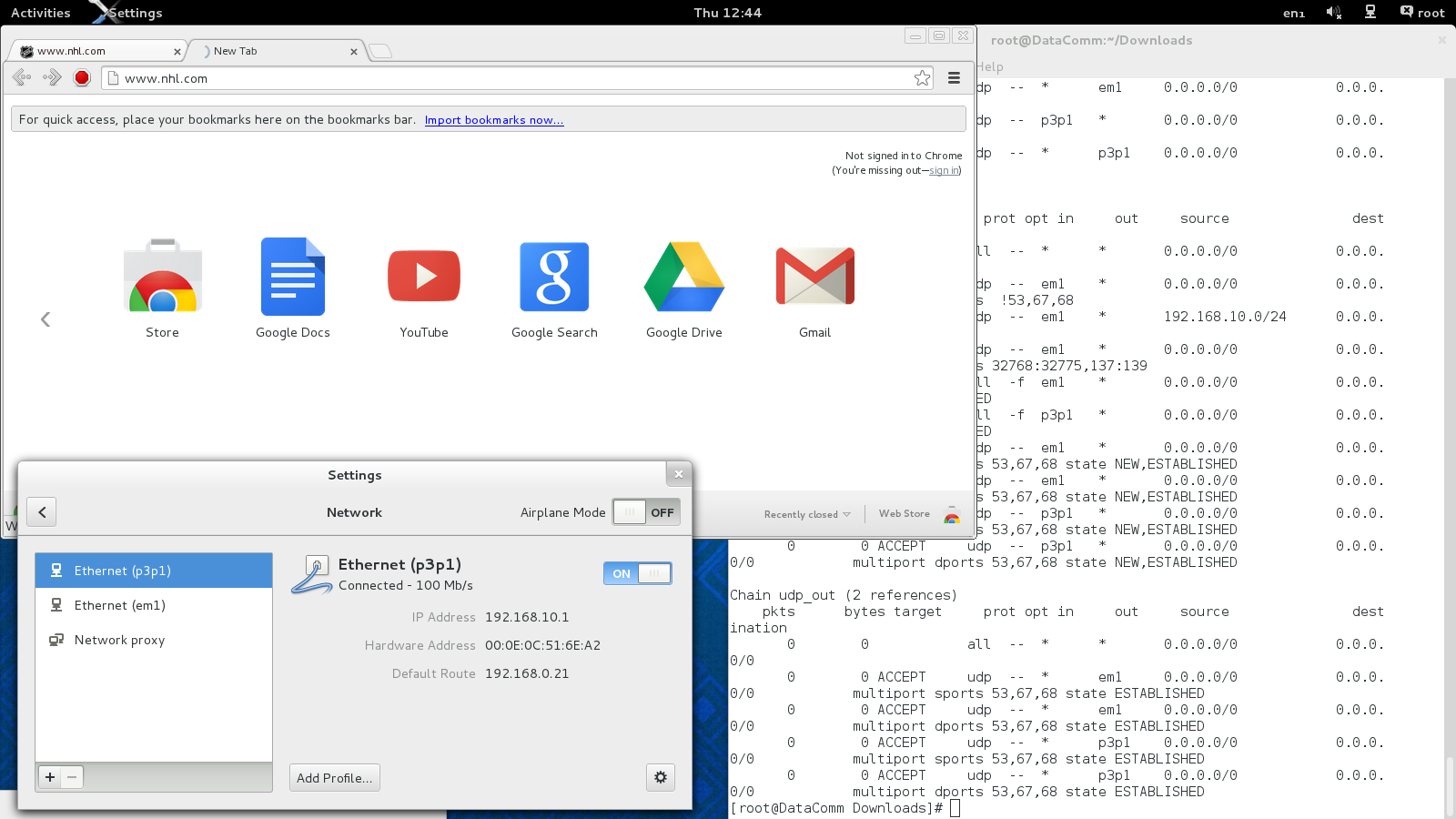
Test Case 2: Ping the internal host



Observations: With no firewall on and with our machine not acting a router to our host, our machine has the ability to PING our host.

Results: PASSED

Test Case 3: Setup the firewall, and test connection again



Observations: Once our machine has been configured to act as a router to our host and the firewall has been applied, we no longer has access to the internet.

Results: PASSED

**Preliminary Setup - Internal Host**

Go to Settings > Network

For p3p1, click the cogwheel

Select IPv4 and change the Addresses to Manual

Set the following fields with these values:

|  |  |  |
| --- | --- | --- |
| **Address** | **Netmask** | **Gateway** |
| 192.168.10.2 | 255.255.255.0 | 192.168.10.1 |

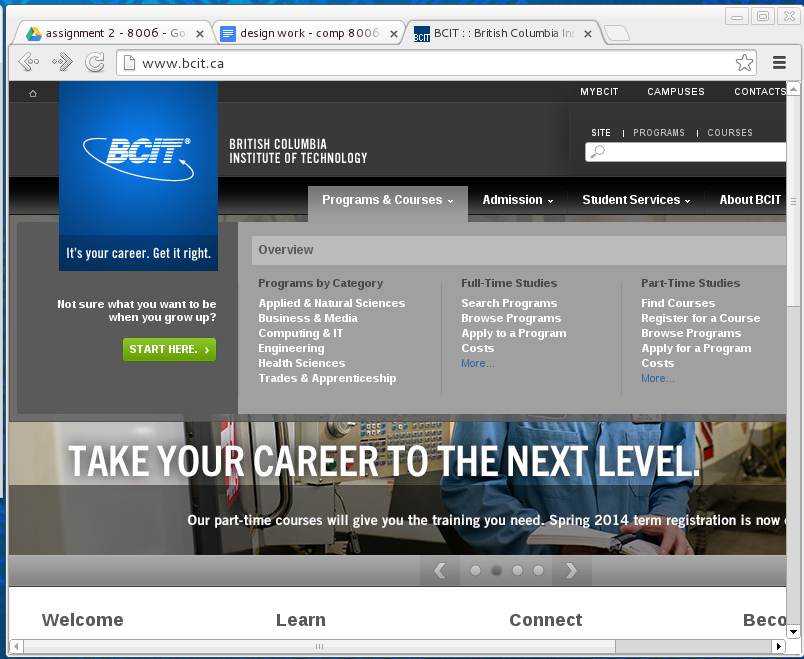
Click Apply and close out of the Settings dialogs.

ifconfig em1 down

ifconfig p3p1 192.168.10.2 up

route add default gw 192.168.10.1

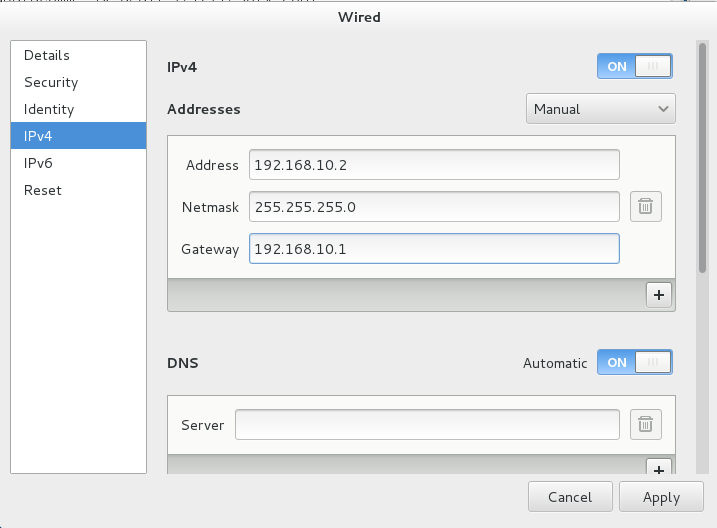
Test Case 4: Test internet access via internet browser without firewall setup



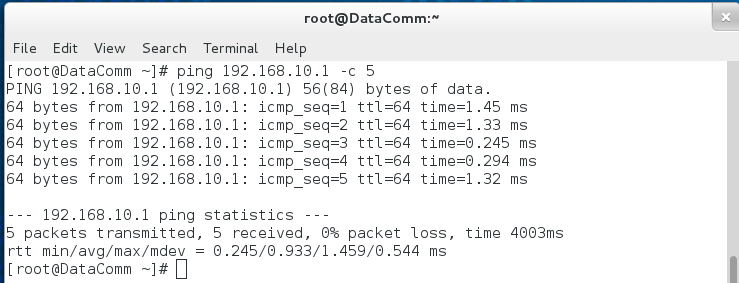
Observations: The lab machine appears to be functional as expected.

Results: PASSED

Setup the firewall

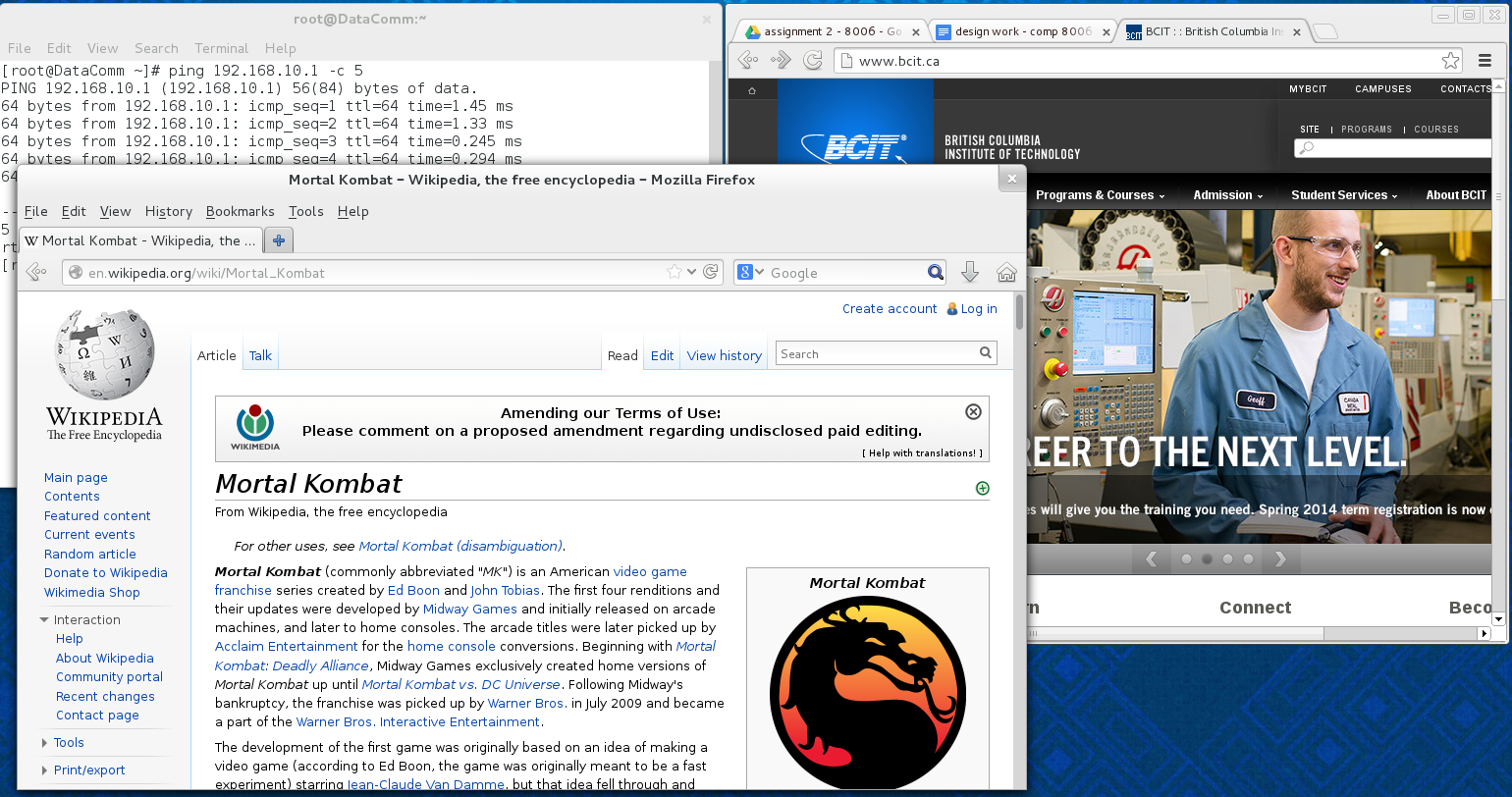


Test Case 5: Ping the internal interface at the firewall host



Observations: After Firewall setup and proper networking configurations, our internal client is able to communicate with the Internal Interface of the firewall.

Results: PASSED

Test Case 6: Test internet access via browser with firewall setup

Observations: After a brief moment of no internet connection, once the firewall was properly implemented and the networking configurations are complete, internet access was restored.

Results: PASSED