# SAIT ITSC206 Winter 2020

**Final**

# Student name: Coleton Sanheim

**Student ID: 000862545**

**Section: N/A**

**Date of submission: 08/16/21 Instructor: Viktor Lyagutsky Mark: /**

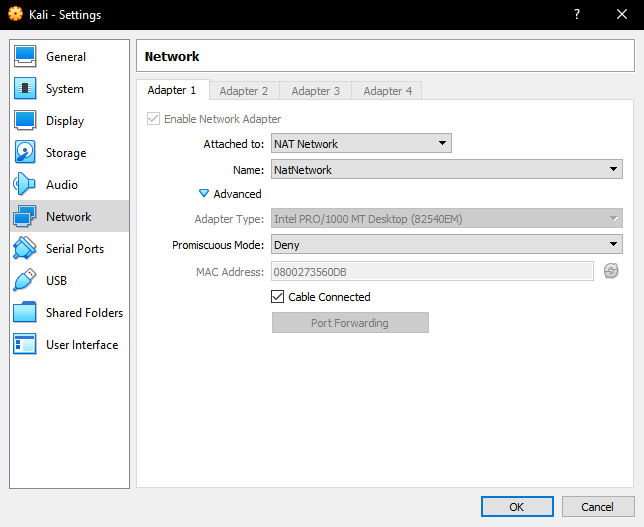
**Objectives:**

* Understand the role of firewalls in corporate environment.
* Understand the role of VPNs in corporate environment.
* Configure security packages according to provided requirements.
* Test and verify the functionality of configured servers.

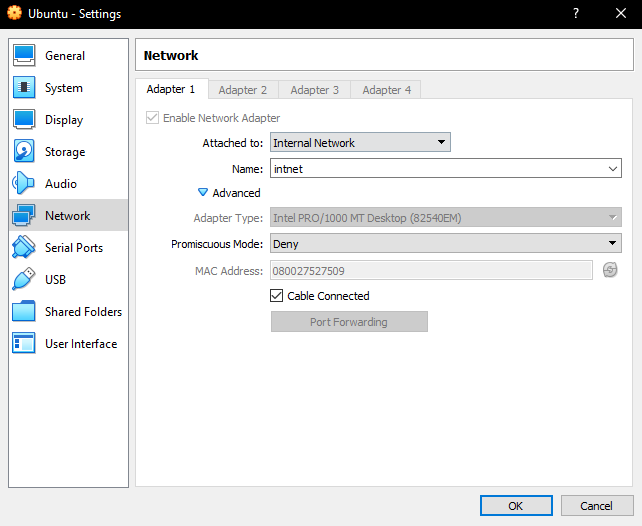
# Tasks:

* Use virtualization software to recreate the topology presented on the provided diagram.

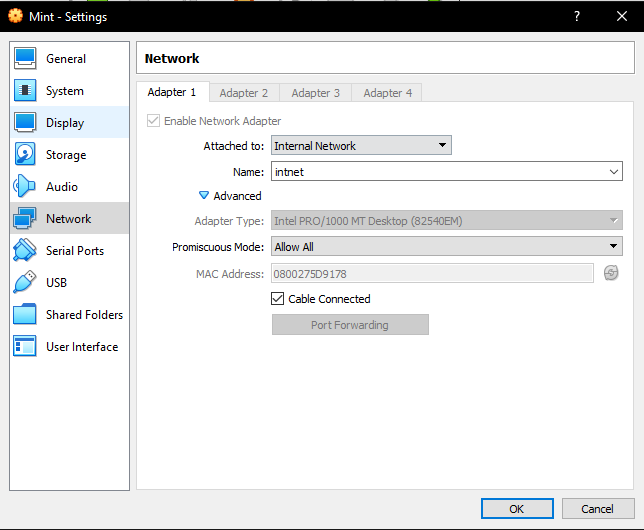
**External Client Network Settings + proof of MAC address**



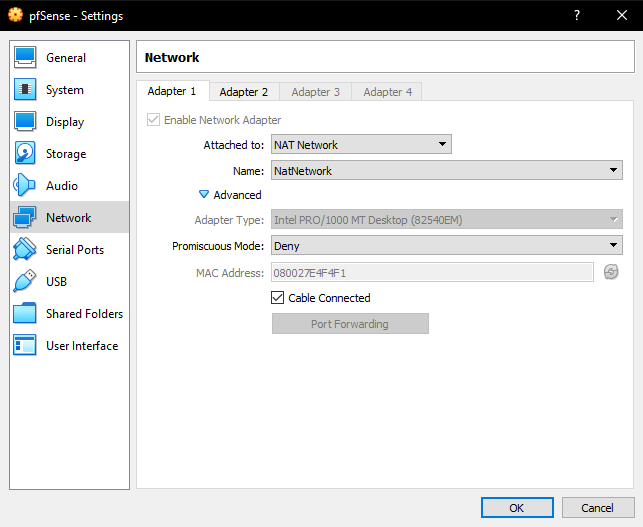
Internal Client Network Settings + proof of MAC address



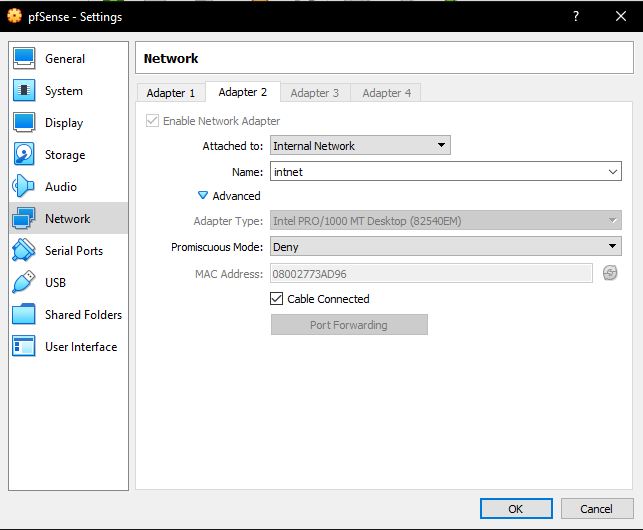
VPN Server Network Settings + proof of MAC address



Firewall Network Settings Adapter 1 + proof of MAC address



Firewall Network Settings Adapter 2 + proof of MAC address



* Assign IP addresses to network adapters and complete the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| **Computer Name** | **IP address** | **Type: Static/Dynamic** | **MAC**  **Address** |
| VM-ExtClient-VMEC01 | 10.0.2.15 | Dynamic | 0800273560DB |
| VM-IntClient-VMIC01 | 192.168.1.102 | Dynamic | 080027527509 |
| VM-VPN-VMPN01 | 192.168.1.100 | Static | 0800275D9178 |
| VM-Firewall-VMFW01 | 10.0.2.7 | Dynamic | 08002773AD96 |
| VM-Firewall-VMFW01 | 192.168.1.1 | Static | 080027E4F4F1 |

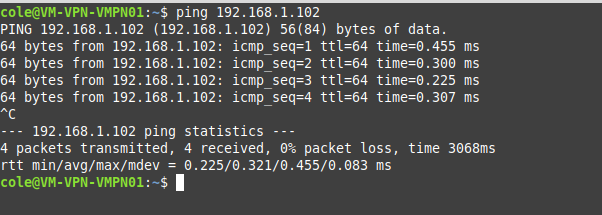
-Describe differences between Stateless and Stateful firewalls

Stateless firewalls filter based on individual packets information

Stateful firewalls filter based on the connecting networks full information

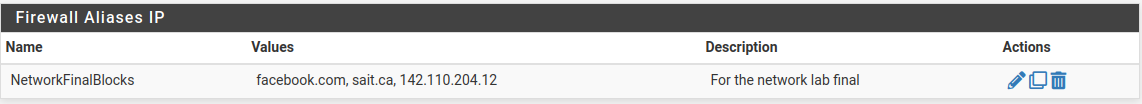
* Configure firewall to provide connectivity to the Internet for the internal network members.

This is the VPN server pinging the internal client

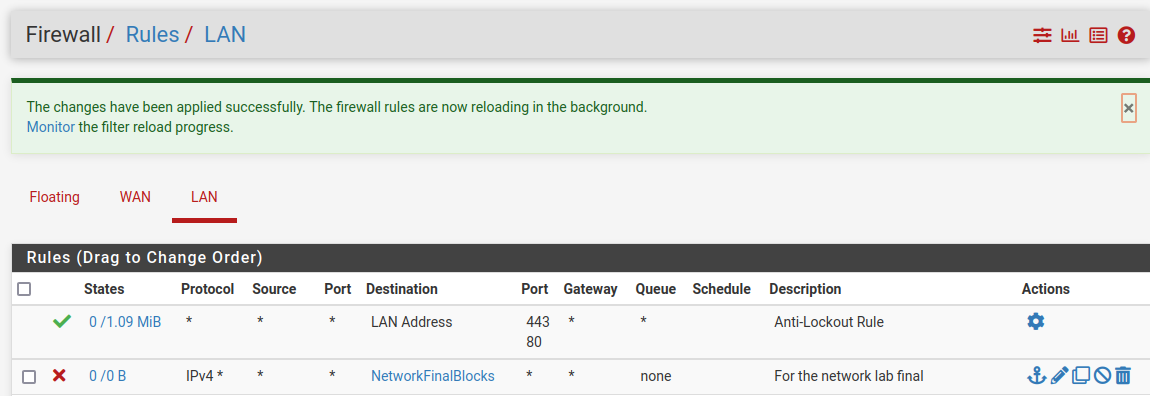


* Restrict access to facebook.com, sait.ca and 142.110.204.12 internet resources for internal network members.

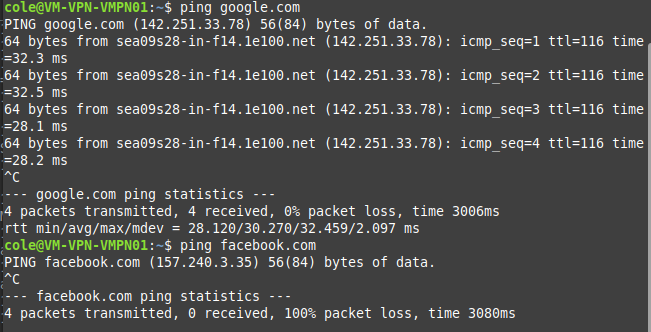
This is the alias list I created based on the parameters given in this question



Using that alias list I created a rule to block traffic to those sources



This is proof from the VPN server that google.com can be reached but facebook.com cannot



-Describe differences between TAP and TUN VPNs.

TAP VPNs function on layer 2 and act like a switch, bridging the connections

TUN VPNs function on layer 3 and instead route packets on the VPN

-Configure port forwarding on the Firewall to provide connectivity to the internal VPN server for the external clients.

This is the OpenVPN rule created in the firewall

Proof of it working is in the question below

-Configure VPN service to provide access to internal network for external clients.

This is the External Client connecting to the Internal Client

A picture containing text, electronics

Description automatically generated

# Marking criteria:

-Topology configured correctly - 5 points Correct hostnames

Correct IP addresses Correct IP types correct MAC addresses

Connectivity for internal network verified

* Stateless and Stateful firewalls described (written answer) - 5 points
* Connectivity to the Internet for internal clients is configured and working properly (attach proof) - 1 point
* Access to facebook.com, sait.ca and 142.110.204.12 internet resources for internal network members is restricted (attach proof) - 3 point
* TAP and TUN VPNs described properly (written answer) - 5 points
* Port forwarding configured (attach proof) - 1 point
* VPN is configured and working properly (attach proof) - 3 points
* Final paper formatting - 5 points

Due date: Friday, August 20 2021, 11:59 pm. Late submissions are not acceptable.