**Student Name:** **Weight: \_\_\_\_2.0\_\_\_\_%**

**Student ID:** **Marks: \_\_\_\_\_\_\_\_\_\_**

Lab 8: VPN

# Learning Outcomes

* Introduce a VPN solution.
* Configure controls for a site-to-site VPN implementation.
* Configure controls for remote host to gateway VPN implementation.

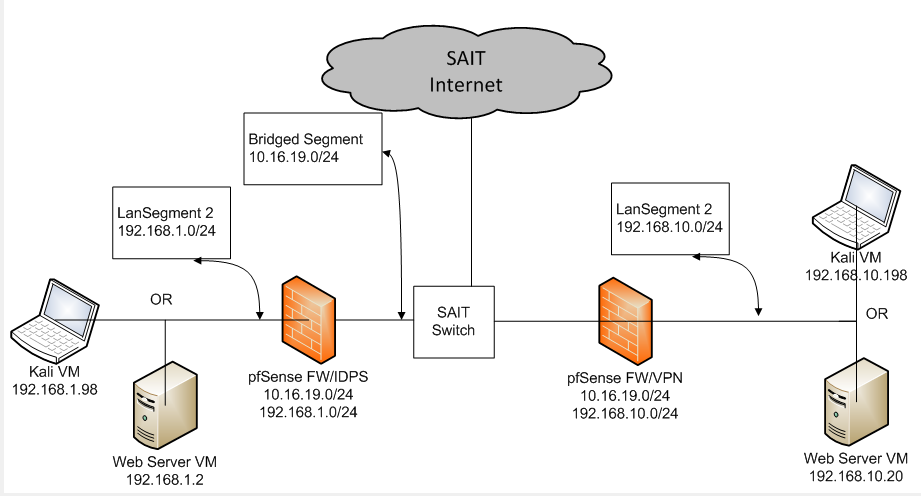
# Purpose

In this lab, you will partner up with one other person and use the pfSense environments to create a site-to-site VPN to connect two networks over an IPSec tunnel.

# Tools

* pfSense x 2
* VM workstation (Kali) or
* VM web server

# Topology



© 2017, Southern Alberta Institute of Technology

# Setup

Before you begin the lab activities, perform the steps below to set up your system.

1. Set up a site A pfSense in Firewall (“pfSense-StudentA”) with the following parameters:

* Set up LAN to: 192.168.1.1/24 with **LANSegment2** interface
* Set up WAN to: 10.16.?.?/24 with **Bridged** interface

1. Set up a site B pfSense in Firewall (“pfSense-StudentB”) with the following parameters:

* Set up LAN to: 192.168.10.1/24 with **LANSegment2** interface
* Set up WAN to: 10.16.?.?/24 with **Bridged** interface

1. Set up an Ubuntu server in the VM using ISO with the following parameters:

* 1 CPU
* 1 GB of RAM
* 80 GB HDD
* Network Adapter: NAT

Reconfigure the network adapter:

* Change network adapter to LAN Segment 2 in the VM console
* Configure the IP address to: 192.168.10.20/24
* Configure the gateway to: 192.168.10.1
* Change setting in /etc/network/interfaces
* Reboot the server for the new IP address to take effect

1. Set up an Linux in the VM using ISO with the following parameters:

* 1 CPU
* 1 GB of RAM
* 80 GB HDD
* Network Adapter: NAT

Reconfigure the network adapter:

* Change network adapter to LAN Segment 2 in the VM console
* Configure the IP address to: 192.168.1.98/24
* Configure the gateway to: 192.168.1.1
* Change setting in /etc/network/interfaces
* Reboot the server for the new IP address to take effect

# Activities

## Configure the Site A server- Site B client OpenVPN

1. On pfSense, using setup document to create OpenVPN
2. Configure a pre-shared key (must match on both ends).
3. Configure and confirm the interface on both sides.
4. Configure and confirm firewall rules are implemented.
5. Review and accept the configuration settings.

## Attempt connectivity over the VPN

* + - 1. Perform ping tests from inside LanSegment2 of each side
         1. Show results of testing:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
      2. Attempt to connect to Apache web server in the other network (nikto, Burp, etc)
         1. Show results of testing:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Configure OpenVPN Remote Access Server/Clien

1. On the server pf Sense, setup OpenVPN Remote Access Server using wizard ie use another port
2. On the server pf Sens, install openvpn-client-export package
3. Click on Client Export, create package

## Verify reachability of the networks between sites

1. From the VM workstation in Site A, ping the VM web server in Site B.
2. Demonstrate in a web browser that the VM workstation can reach the VM web server in Site B.