# SAIT ITSC206 Winter 2020

**Final**

# Student name: Joshua Miller

**Student ID:**

**Section:**

**Date: Aug 16th, 2021**

**Instructor:**

**Mark: /**

**Questions:**

**1.** **Stateless and Stateful firewalls described (written answer)**

* A stateful firewall has the capability to maintain the state of a network connection, it will also account for the return traffic meaning it does not need to allow each type of traffic specifically. But stores the connection in a “connection table” so that the return traffic is recognized as safe, and procedures can continue.
* Stateless firewalls do not consider the connections made instead they only analyze the individual packets of traffic. They operate on a source and destination base to protect the network meaning it uses “match conditions” to determine how to introduce the traffic into the network and if the match conditions are not met the traffic will be assumed malicious and dropped.

**2. TAP and TUN VPNs described properly (written answer)**

The key difference between TAP and TUN VPN’s is that TAP uses bridging and TUN uses tunneling:

* TAP acts on layer 2 of the OSI model and can transport any protocols the network might want to send but has a large amount of overhead. Can be used in bridged networks.
* TUN acts on layer 3 of the OSI model and only transports layer 3 IP packets which has less overhead and only allows the traffic which is destined for the VPN client. However, TUN can only work in IPv4 and does not receive broadcast traffic.

**Topology:**

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Computer Name** | **IP address** | **Type: Static/Dynamic** | **MAC**  **Address** |
| **VM-Firewall-VMFW01 (pfsense)** | **192.168.1.1/24 :em0**  **10.10.15.119/20 :em1** | **Dynamic :em0**  **Static :em1** | **08:00:27:17:45:66** |
| **VM-VPN-VPN01 (mint)** | **192.168.1.100/24** | **Dynamic** | **08:00:27:c7:5f:d3** |
| **VM-IntClient-VMIC01 (ubuntu)** | **192.168.1.101/24** | **Dynamic** | **08:00:27:22:70:ee** |
| **VM-ExtClient-VMEC01 (kali)** | **10.10.15.123/20** | **Dynamic** | **08:00:27:0e:34:8d** |

**Topology/Connectivity screenshots below:**

**IP addresses // MAC addresses // IP Types:**

VM-Firewall-VMFW01 **:Text

Description automatically generated**

****

VM-IntClient-VMIC01:

**Text

Description automatically generated**

VM-VPN-VPN01:

**Text

Description automatically generated**

VM-ExtClient-VMEC01:

**Text

Description automatically generated**

* **Connectivity for internal network verified:**

TO EACHOTHER:

**Text

Description automatically generatedText

Description automatically generated**

TO PFSENSE FIREWALL:

**Text

Description automatically generatedText

Description automatically generated**

TO GOOGLE:

**Text

Description automatically generatedText

Description automatically generated**

* **Hostnames:**

**Graphical user interface, application

Description automatically generated**

**Configurations and Proof:**

* **Configure VPN service to provide access to internal network for external clients && VPN is configured and working properly:**

First I will show you that external network doesn’t have access to my internal network without the VPN as demonstrated by the ping below:

Text

Description automatically generated

After my VPN is configured:

Graphical user interface, text, application

Description automatically generated

We then can access my VM-VPN-VPN01 externally:





My snip application cut this screen shot in half, not sure why, so I edited it together (hope the formatting doesn’t change on submission.)

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

VM-VPN-VPN01:

Text

Description automatically generatedText

Description automatically generated

VM-IntClient-VMIC01:

Text

Description automatically generatedText

Description automatically generated

However both still allowed Facebook.com, I guess their hackers are better than my firewall.

Text

Description automatically generatedText

Description automatically generated