SMW Journal 2 Week 12

Done by: Lee Yi Terng (1904189)

Class: DISM/FT/2A/04 | Date: 9th July 2020

Submitted To: Ms Teo Seok Ling

# Topics Covered

* IPsec Implementation
* IPsec Modes and when to use which one
* Enforcing and setting up IPsec communication

# Enforcing and setting up IPsec communication

This is from Practical 6-2. I learnt how to set up an IPsec Policy to enforce IPsec communication between two machines for ICMP traffic. First, I had to use the IPsec Rule Wizard to create a new IPsec rule. In the wizard, I had to specify tunnel endpoints, network type and an IP filter list.

I had to create a new IP filter list too using the IP Filter Wizard. During setup, it was required to give a description for the filter, specify IP Traffic Source, IP Traffic Destination and IP Protocol Type.

After creating and specifying the IP filter list, I had to add a new Filter Action and configure it to “Negotiate Security” and “Do not allow unsecured communication”. I had to create a custom IP Traffic Security settings as well to use SHA1 as AH and SHA1/3DES for ESP.

After creating and choosing my new Filter Action, I used “Pre-shared key” as the authentication method with the string “abc123def.

Finally, I selected my Security Rule Wizard configurations and learnt how to create an IPsec Policy, a Filter List and a Filter Action.

To enforce this IPsec Policy, I assigned it to the OU that hosts my client server “WIN12R2” and tested it with ping tests between WIN12R2, my Win10 VM and my Host machines.

It is really interesting how IPsec can be used to secure network communication. In this case, the machines without a secured communication are unable to communicate, while those which were secured are able to communicate.