JW4158-INFO8580-22S-Portfolio-2

John White

6714158

INFO8580

Anasuya Bhima

July 17, 2022

Table of Contents

Lab 3 - Network to Network VPN - IPsec

Part 1

Description

The purpose of this lab is to teach us how to configure a VPN between 2 pfSense routers using IPsec. We will be authenticating between them using pre-shared keys.

Preparation

To prepare for this lab, we will need 2 pfSense routers which will represent our office (Site A) and home (Site B) networks. We will also need 2 Windows desktops to configure them from. One router will be on the 01 and 02 network and the other will be on the 01 and 03 network. The desktops will be on 02 and 03. The upstream LAN address for the routers will be 10.175.68.1 (as assigned by Conestoga). Configure the routers as shown in the screenshot and we are ready to start the lab.

Observations

On Site A, Go to VPN > IPsec and then click “Add P1”. Configure Phase 1 as shown in the screenshots below. Once Phase 1 is configured, click, “Show Phase 2 Entries” then “Add P2”. Configure Phase 2 as shown in the screenshots below. Site A should now be configured. Do the same for Site B but change the IP addresses where appropriate. Once this is done, go to Status > IPsec and click “Connect VPN”. The connection should then say established as shown in Fig 1.9.

Screenshots

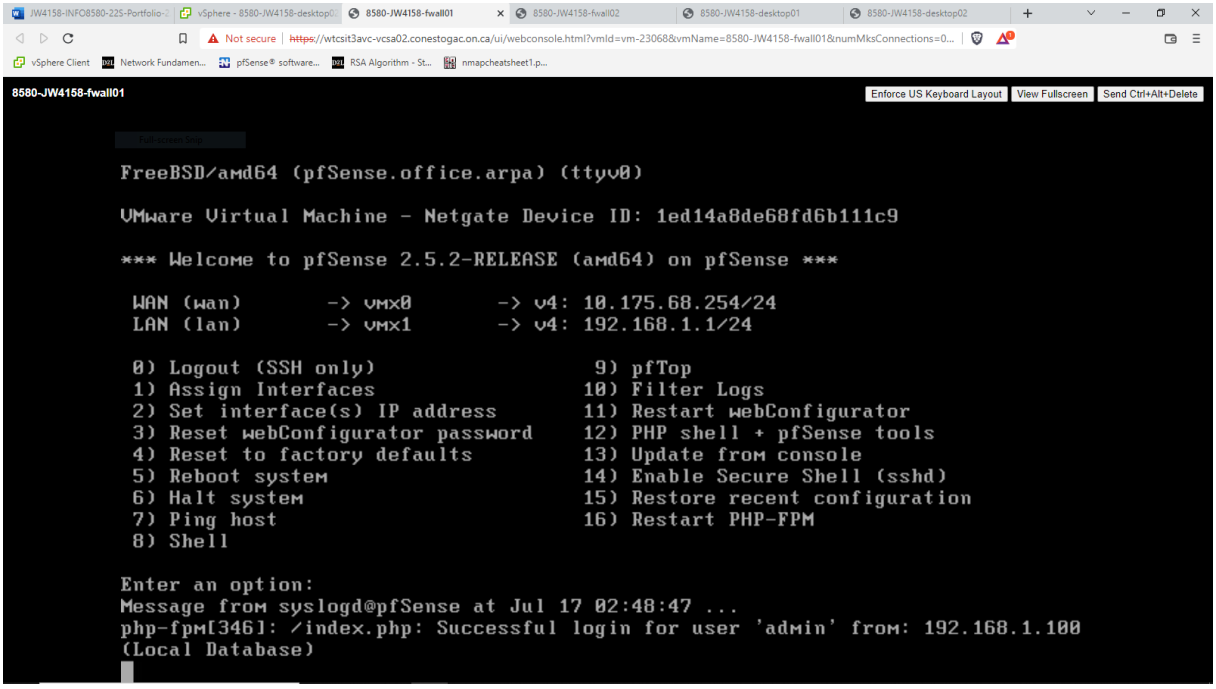

Figure 1.1 - Site A pfSense configuration

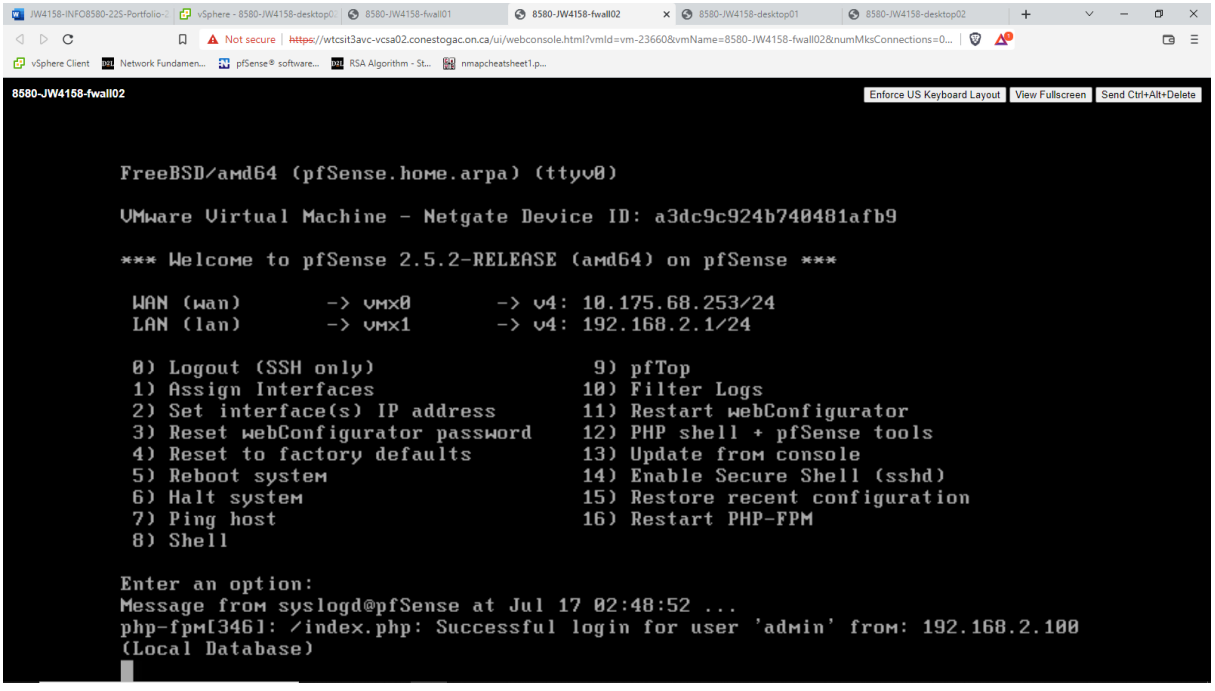

Figure 1.2 - Site B pfSense configuration

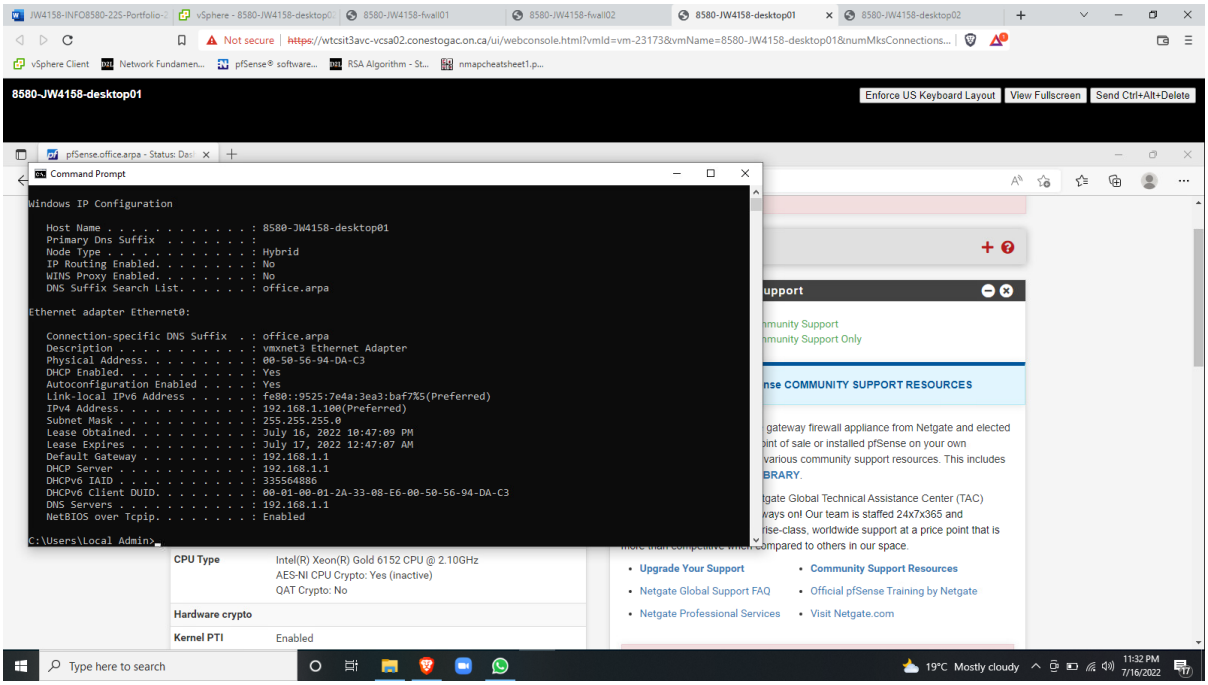

Figure 1.3 - Site A client configuration

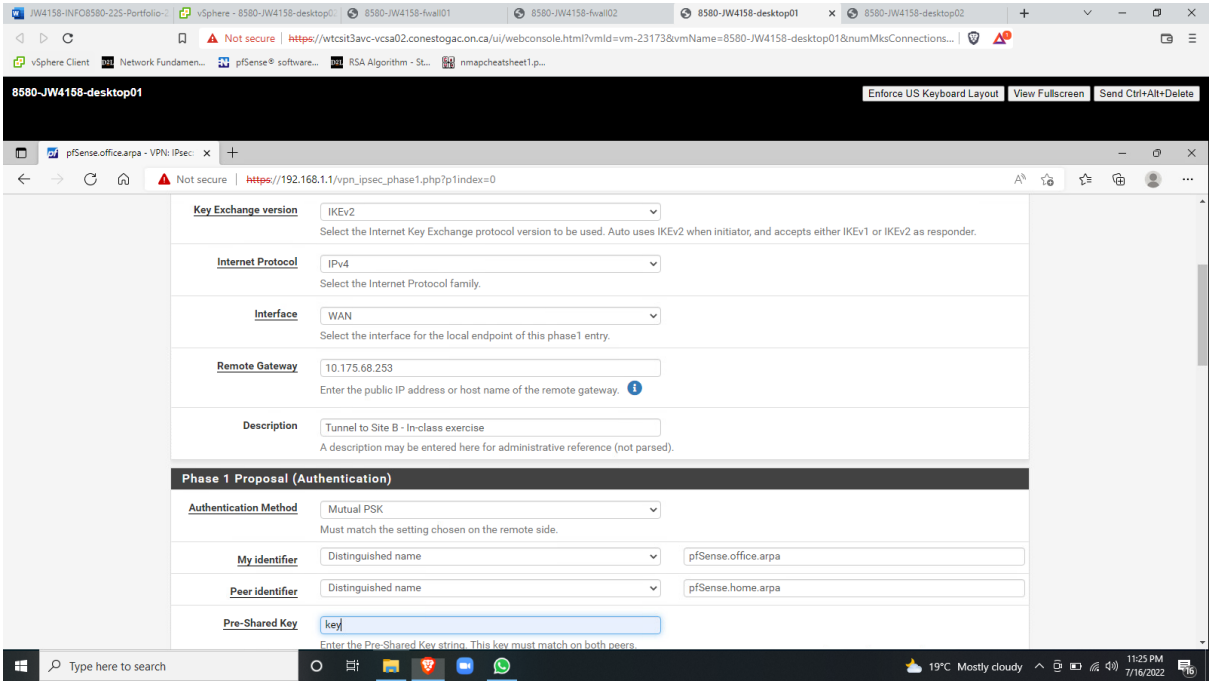

Figure 1.4 - Site A IPsec configuration - Phase 1, Part 1

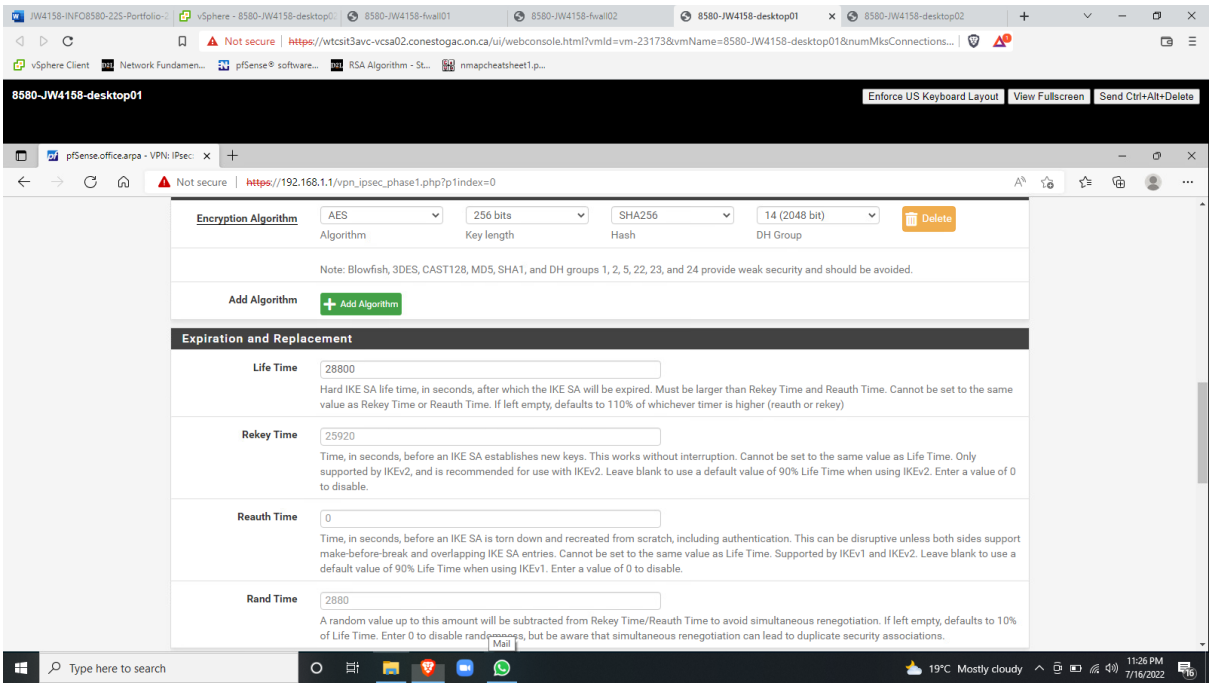

Figure 1.5 - Site A IPsec configuration - Phase 1, Part 2

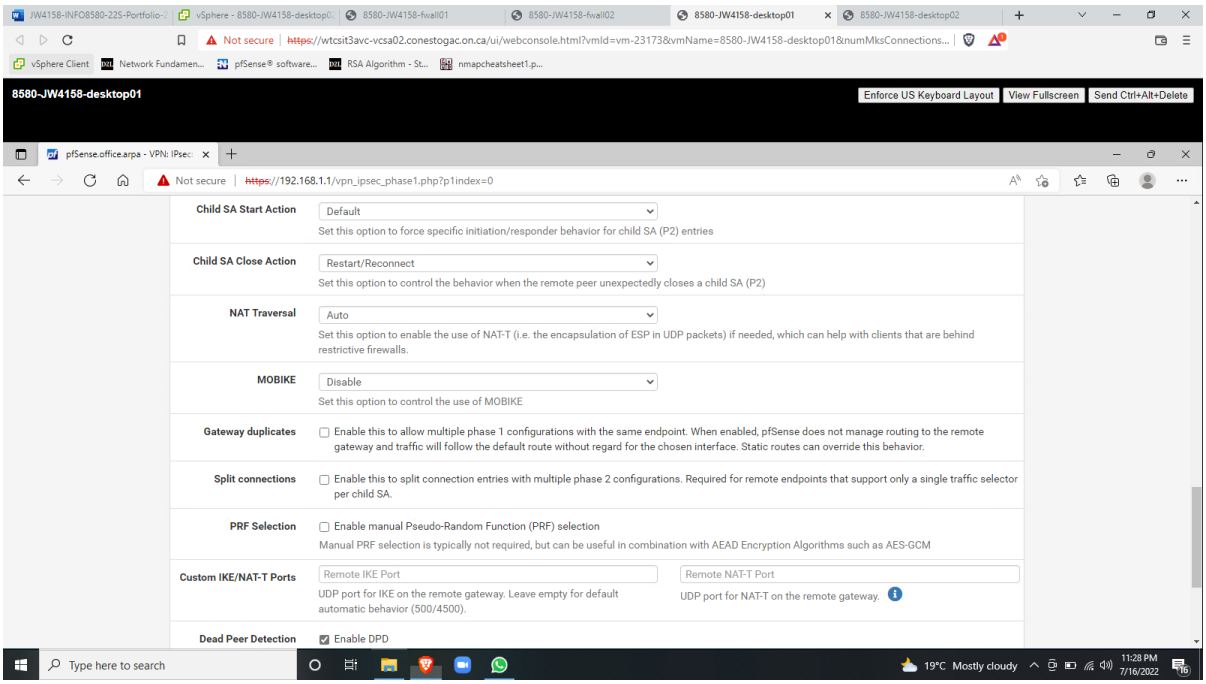

Figure 1.6 - Site A IPsec configuration - Phase 1, Part 3

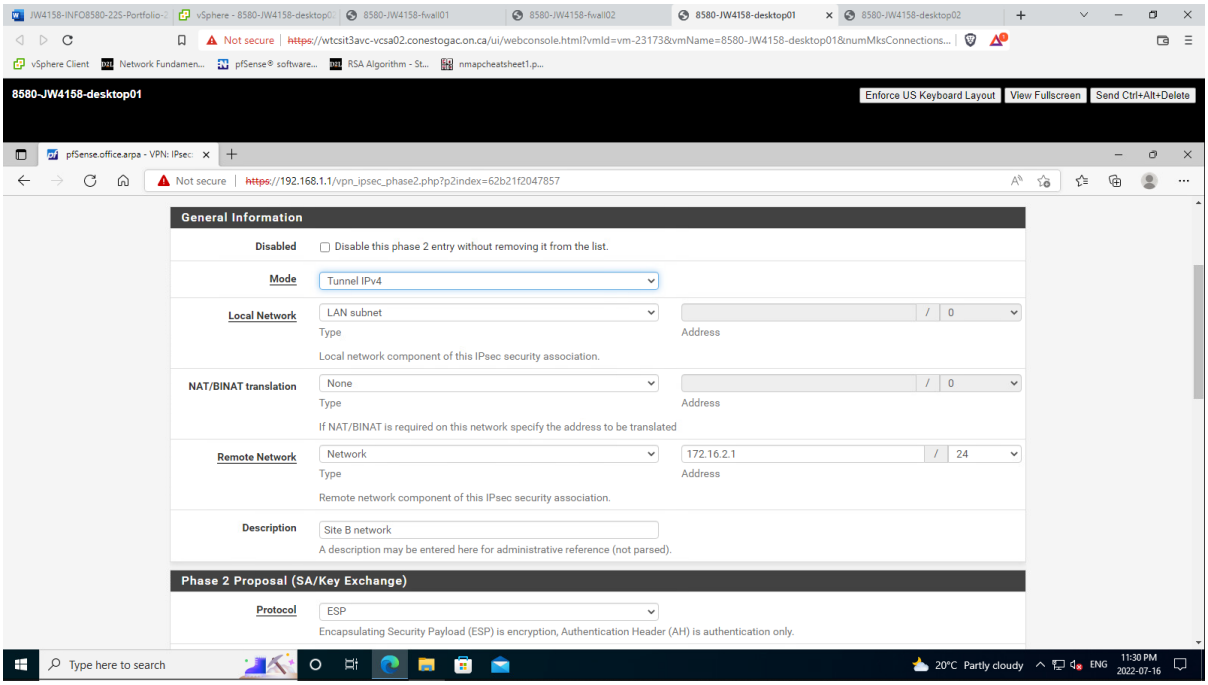

Figure 1.7 - Site A IPsec configuration - Phase 2, Part 1

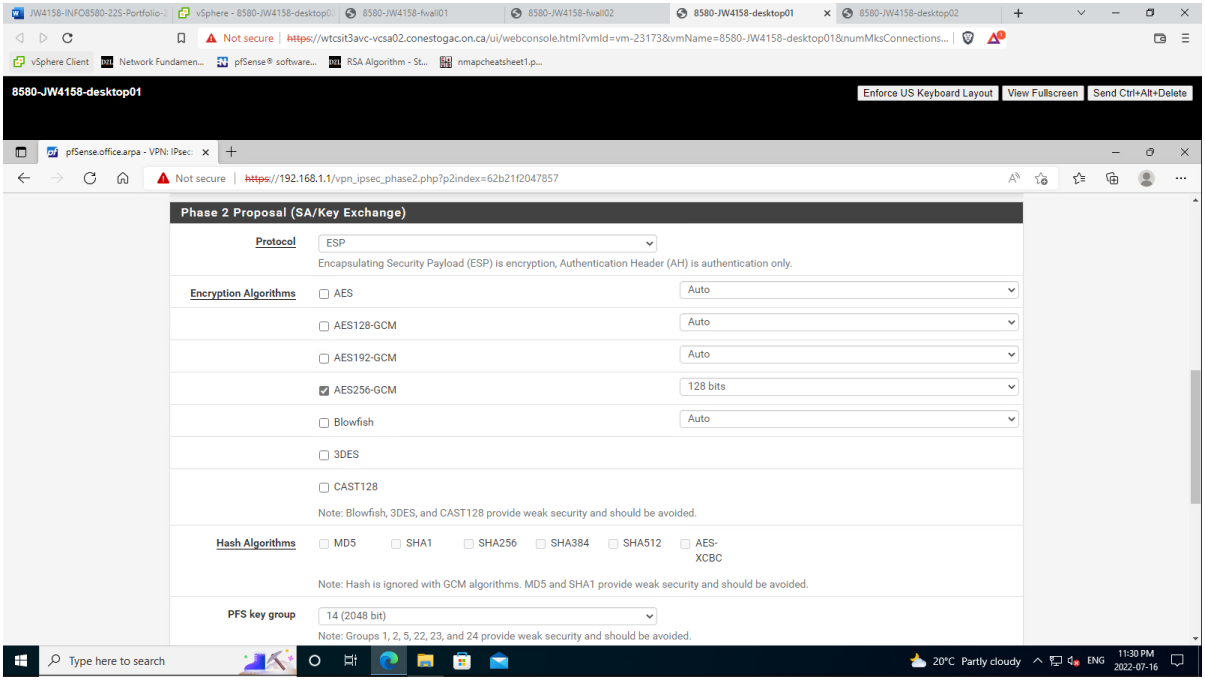

Figure 1.8 - Site A IPsec configuration - Phase 2, Part 2

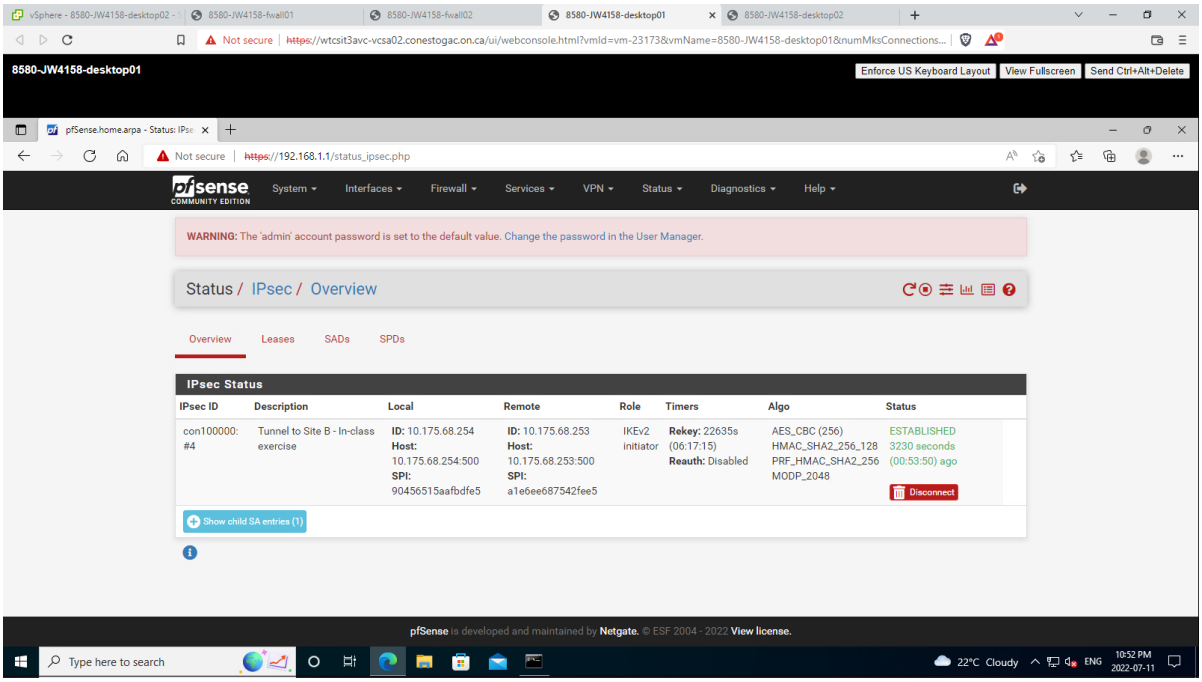

Figure 1.9 - IPsec tunnel is established from Site A

Reflection

The only issue I ran into was when I configured one of the sites to connect to itself rather than the other site. As long as special care is taken to keep the IP addresses straight, this lab is fairly straightforward. If both sites are using the same subnet address, the tunnel cannot be established because the destination IP will be the same at the source IP. To get around this, we can use NAT to translate the addresses so that for the purposes of traffic routing, they will have different IPs. This is an option that is already available in the Phase 1 IPsec settings. An alternative IP address for the router to use can be specified using the “NAT/BINAT Translation” option. I found this solution on Provya.com, listed in the references below. To improve security, we could use an encryption algorithm uses more bits or we could use a pregenerated key instead of simply using ‘key’ as our pre-shared key. To decrease security, we could use a simpler encryption algorithm or stop using encryption altogether.

References

1. PfSense, 2022 (IPsec Site-to-Site VPN Example with Pre-Shared Keys, retrieved from https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-s2s-psk.html on July 17, 2022)
2. Provya, 2022 (Site-to-site IPsec VPN with overlapping subnets, retrieved from https://www.provya.com/blog/pfsense-site-to-site-ipsec-vpn-with-overlapping-subnets/ on July 17, 2022)

Lab 4 - Network to Network VPN – IPsec -

Certificates Part 1

Description

To purpose of this lab is to teach us how to authenticate our VPN connections using certificates instead of pre-shared keys which will make our VPN more secure.

Preparation

To prepare for this lab, follow the instructions in the previous lab. Once the VPN connection is established, we are ready to start the lab.

Observations

First we will create our certificate authorities. Go to System > Cert. Manager and click “Add”. Give the certificate authority a common name then hit save. Do this on Site B as well and export both certificate authorities. Import each CA on the other router as shown in Figure 2.2 (I use Dropbox to transfer the files between desktops and notepad to open the certificate data for copying and pasting). Now that we have both CAs on both routers, we just need to create a certificate endpoint on each router. From the Certificate Manager, navigate to ‘Certificates’ and click the button that says ‘Add/Sign’. Create a new certificate as shown in Figures 2.3 and 2.4. Do the same for Site B. Now that we have our certificates created, we just need to change our Phase 1 IPsec configuration to use our certificates instead of pre-shared keys. This is shown in Figure 2.6. Once this is done on both sites and we are still able to establish a connection, we are done.

Screenshots

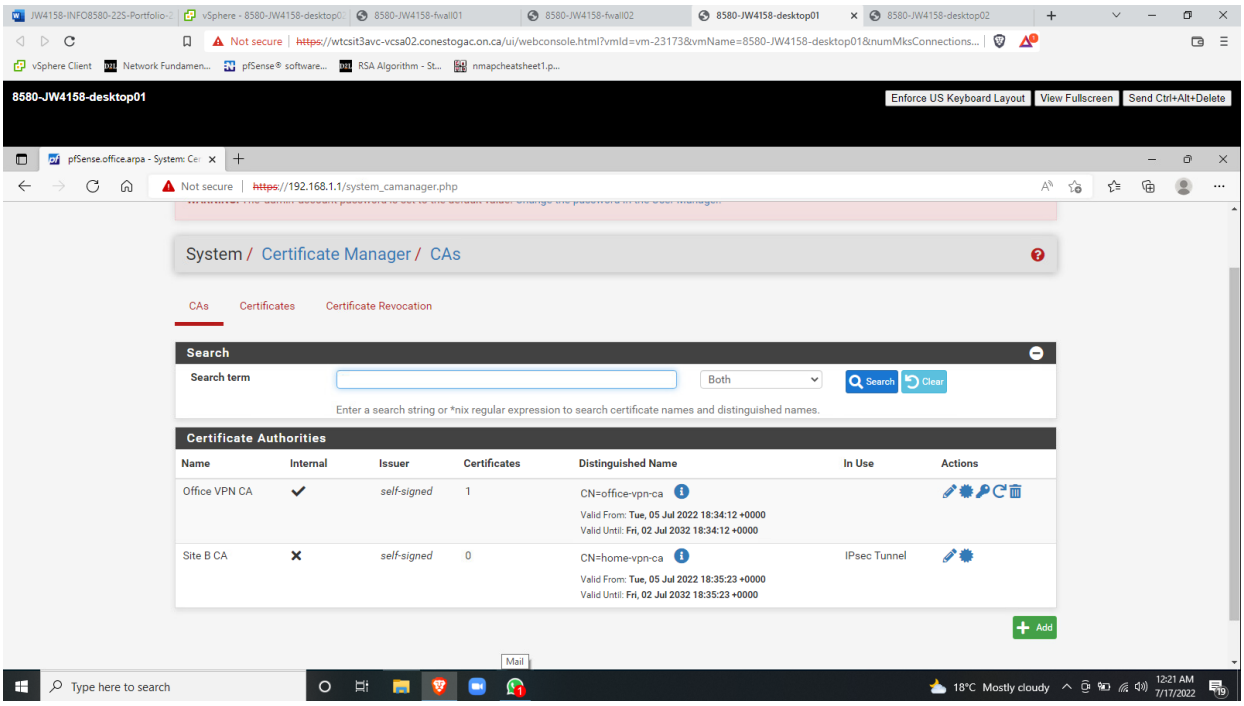

Figure 2.1 - Site A Certificate Authorities

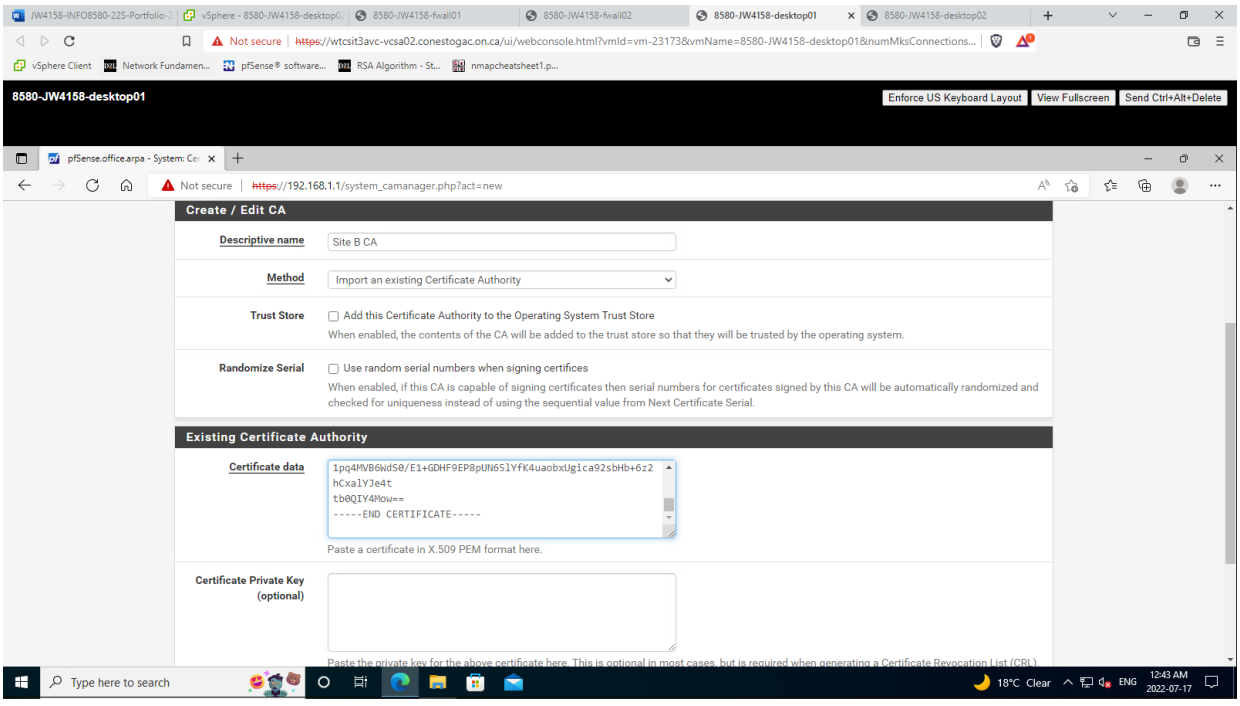

Figure 2.2 - Importing Site B's CA on Site A

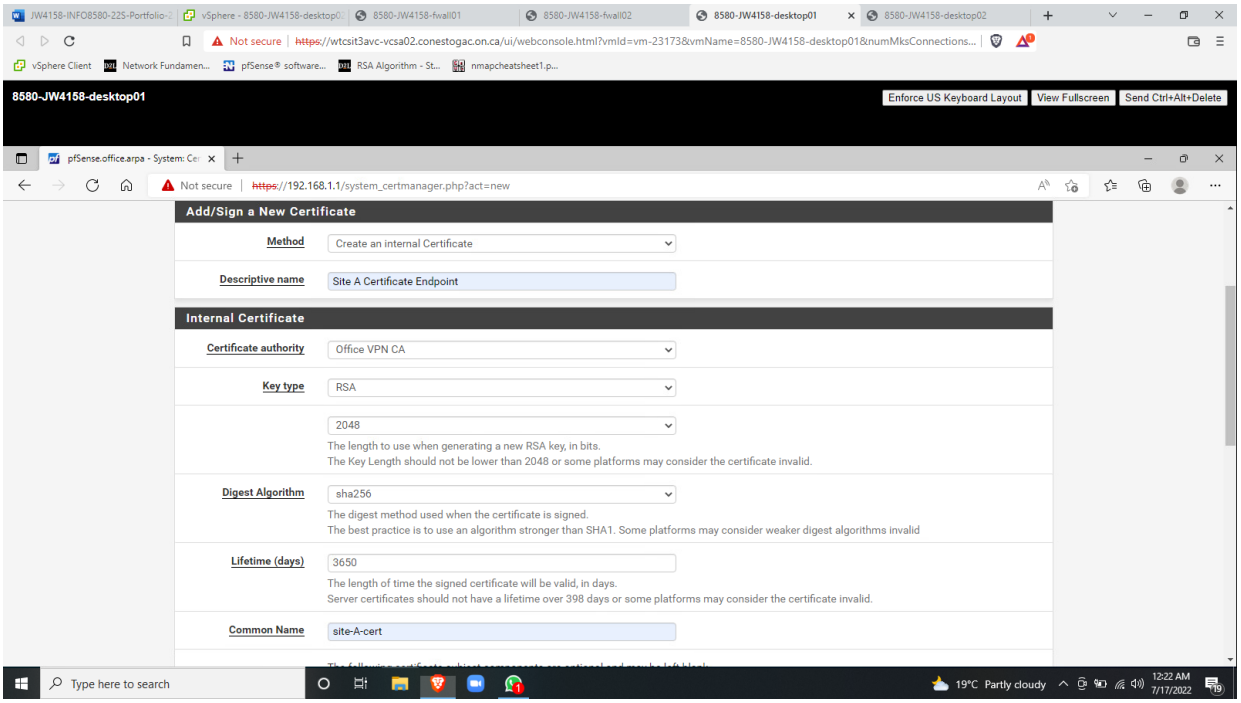

Figure 2.3 - Site A certificate endpoint configuration Part 1

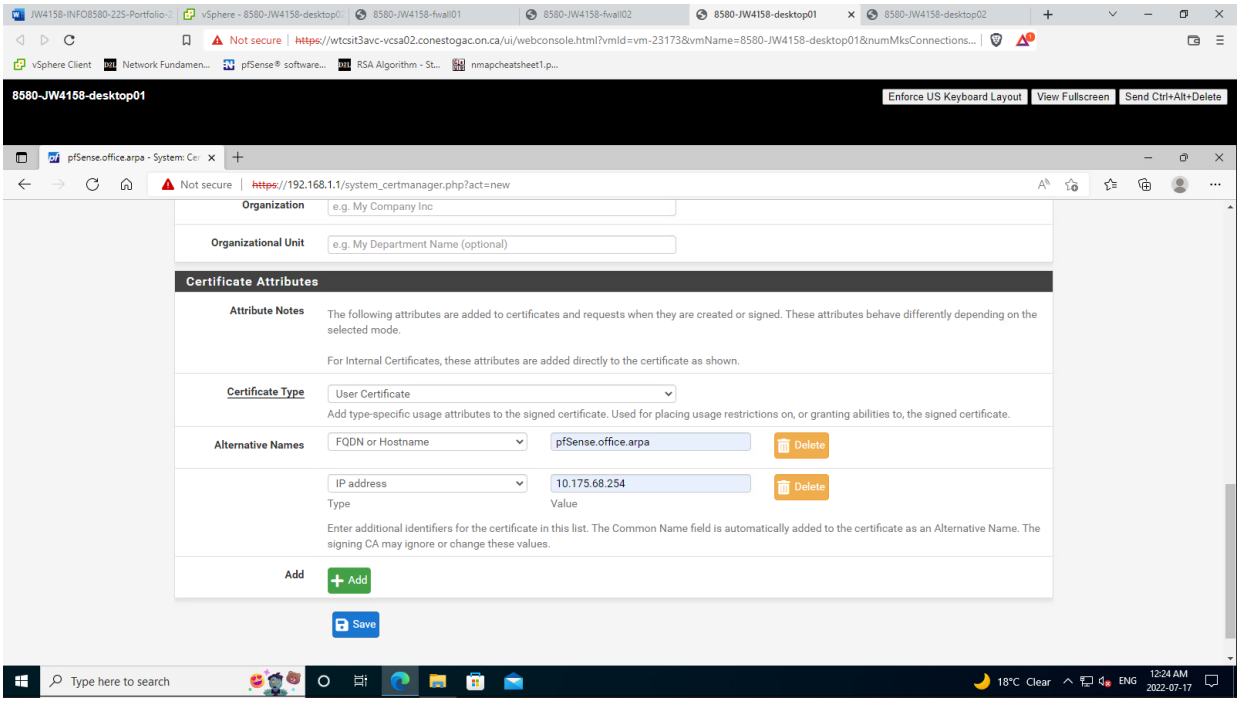

Figure 2.4 - Site A certificate endpoint configuration Part 2

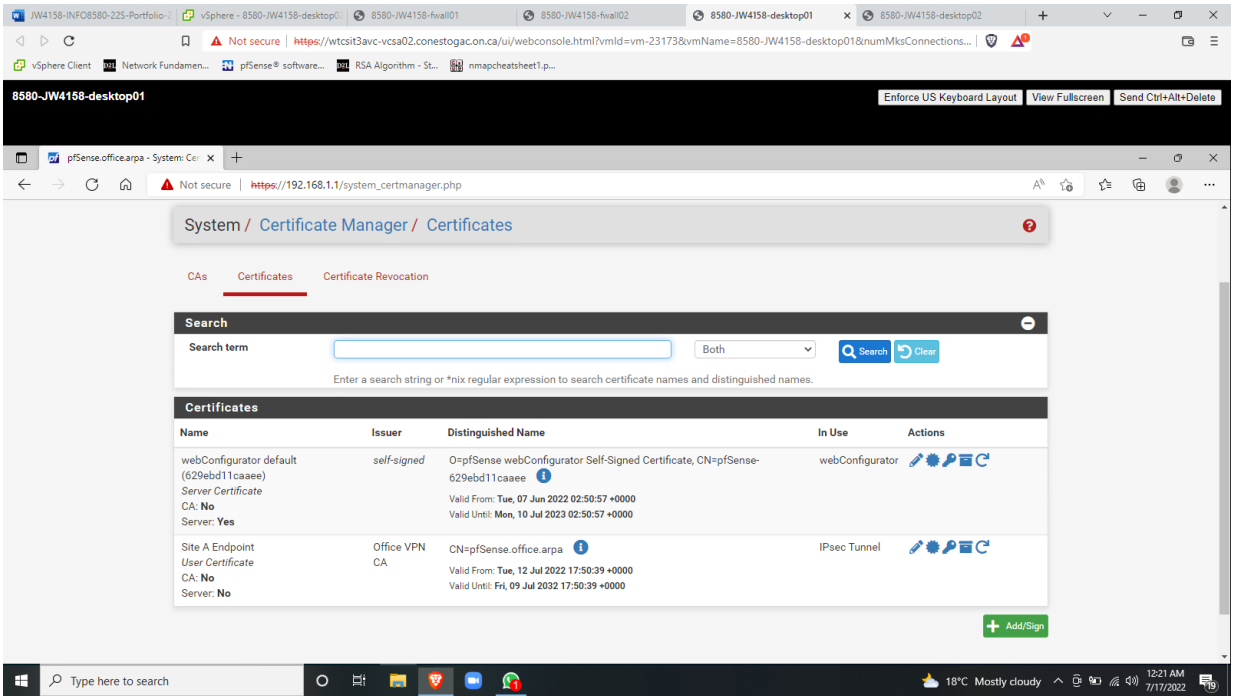

Figure 2.5 - Site A certificates

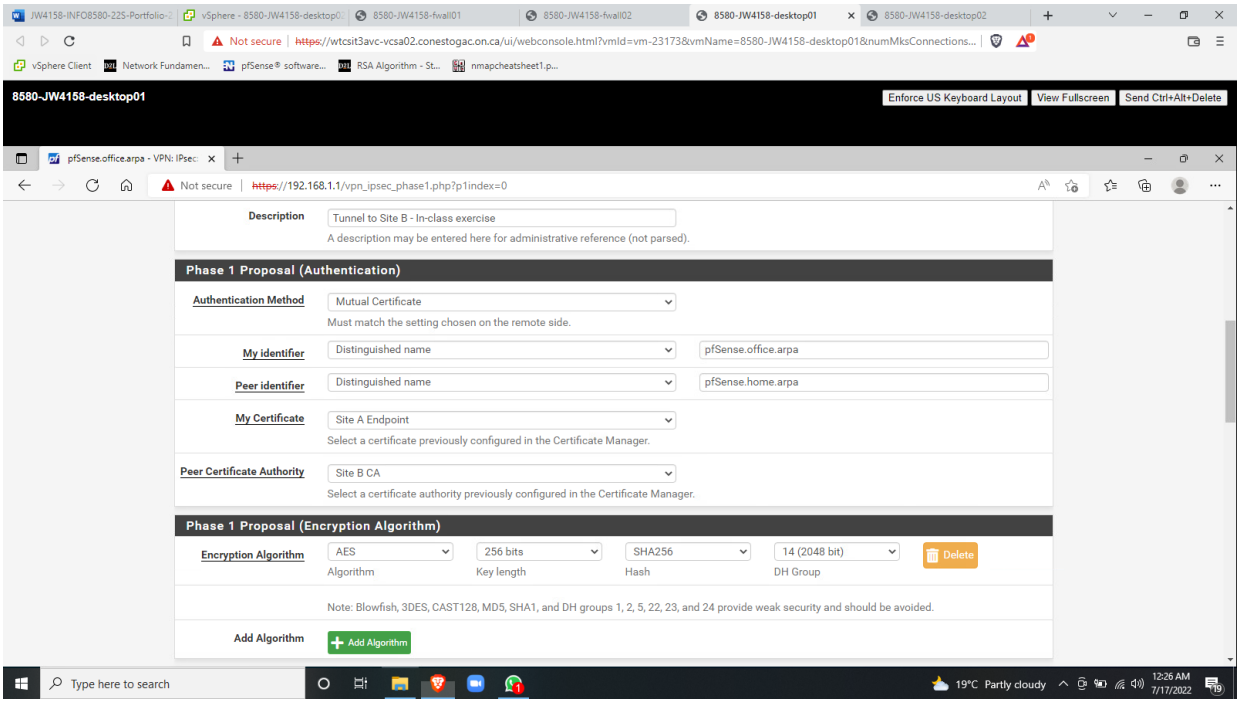

Figure 2.6 - Site A Phase 1 authentication changes

Reflection

On issue that I ran into during this lab was that I accidentally imported my peer Certificate Authorities as Certificates. This made the correct settings unavailable later on. To improve the security of our certificates, we could decrease the lifetime so that they need to be reissued

more often. If we wished to decrease the size of our key at the cost of security, we could switch our key length to one that uses fewer bits.

References

1. PfSense, 2022 (IPsec Site-to-Site VPN Example with Certificate Authentication, retrieved from https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-s2s-tls.html on July 17, 2022)

Edit Link: https://stuconestogacon-my.sharepoint.com/:w:/g/personal/jwhite4158_conestogac_on_ca/EcKiCbLyiUdPn_Hul8N67O4BwbQnO3HULx24sudcslTbvQ?e=kN7R9c