Lab 4 – Network to Network (Site to Site) IPSEC Certificate VPN

Overview

In this lab we will practice configuring a basic pfSense firewall to connect to a second pfSense firewall to createa network to network VPN. This differs from Lab 3 in that this will use certificates rather than a pre-shared key. **This must be done using the vSphere environment. This is individual work. You may consult with peers while doing practice work on the concepts, but when working through the lab book it is must be done yourself. Please reach out to your professor if you get stuck or need help!**

This lab must be completed online, with all work being done and written as it is done into Word 365 Online.Use the Lab Book Template and upload to your Word 365 Online and begin working there. You must also sharean edit link from Word 365 Online in the comments of the assignment document submission (export a PDF and upload it to eConestoga). Not following these instructions and showing ongoing work through the change revisions tracked in the online Word mean a score of zero on the lab.

Preparation

- Familiarize yourself with class work done introducing the use of vSphere and pfSense

Deliverables

- Install two pfSense firewalls on vSphere with the following specifications:
    - Name your pfSense firewalls 8580-<id>-fwall01, where <id>- is your initials plus last four numbers in student ID, for example – my1234-8580-fwall01
    - Use your _01 networks for the WAN adapters on each, giving each an appropriate and available IP address on your assigned 10.0.0.0/8 network that routes and connects to the internet as perthe documentation on eConestoga.
    - Use your _02 network for the LAN network for fw01, and _03 network for LAN network for fw02
    - Assign the LAN a /24 network from 192.168.0.0/16 private address space; use a different networkfor each firewall.
    - Configure your pfSense device to provide DHCP to devices on your LAN; ensure they get a correctIP address, default gateway, and use your pfSense device for DNS.
    - Configure pfSense to run a DNS server for devices on the LAN - DNS Forwarder to 8.8.8.8
    - Test this is working with Windows 10 desktops you create and name appropriate, with your <id> as a prefix. **NOTE: You may re-use your configurations from Lab 3! Document the changes you do to that setup to convert to Lab 4.**
    - Connect your two networks together using a net to net (site to site) IPSec VPN using certificates following this guide:
        - https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-s2s-tls.html
          Test it is working for communication between network using a method of your choice.

Screenshots

- Appropriate screenshots that demonstrate the above was done and all is working

Reflection

- Record any of your own observations, solutions, or comments about the work you did. What problems did you have, what was not clear, what did you take away that you value? Explain yourconfiguration choices. This is mandatory. You may refer back to your observations section of your lab book in answering this question
- Discuss one of the setting areas related to certificate based IPSEC VPNs that could improve security, and one that could reduce security.