Test Report

Initially sites in Bunbeg and Ramelton were assigned with an individual LAN network and firewall. For guests a separate LAN network was created on each site with SSL tunneling to secure the internal LAN network from external threats. Both the LAN networks were joined by a bigger WAN network through firewalls to gain internet access. For site to site connectivity, an VPN tunnel was created which was encapsulated by IPSec tunnel for secure connectivity and encryption.

Testing:

1. Added client system to both the LAN network and successfully carried out "execute ping" from FortiGate to client system to ensure the working of LAN segments within the local office network and the working of port2 of firewalls.

Name	IP
Client_Dun	192.168.1.3/24
FWDUN(Port2)	192.168.1.1/24
Client_Ram	192.168.2.3/24
FWRAM(Port2)	192.168.2.0/24

2. Successfully carried out pinging client systems from Bunbeg office network to Ramelton office network to test the working of IPSEC VPN Tunnel.

Device	IP
Client_Dun	192.168.1.3/24
Client_Ram	192.168.2.3/24

3. Connected Guest VM to both the DMZ networks and confirmed the connection from web to guest via the ports below.

Device	IP
Client_DMZ1	192.168.3.5/24
Client_DMZ2	192.168.4.5/24

4. Tested the systems malware detecting capabilities with different compression technologies such as TAR.GZ, 7Z, CAB using EICAR test file from Fortinet official website. Client systems passed the test with firewalls able to detect and block malwares. [1]

5. Internet connectivity of the client systems in LAN network and Guest DMZ network was tested. All the internet traffic was monitored for security of the network.

Limitations:

1. The FortiClient profiles have limitation depending on the version of FortiGate that is being used. For a small FortiGate VM (VM1) the maximum client profiles allowed are 512. If the company requires more profiles, they would need to upgrade the Fortinet firewall to add more client profiles. [2]
2. The maximum devices supported by FortiGate (VM1) are 400. [2]
3. If the firewall client software is outdated there would be a higher risk in being infected by new malware due to the failure of detection.
4. Proxy based file scanning have size limitations, files larger than the buffer are passed without being scanned or blocked. It is possible to block the download of large files by setting a threshold file size in MB in Security and Profiles>Proxy Options>Block Oversized file. [3]

References:

[1]. Test Your System's Malware Detection Capabilities [online] (2018) *Fortinet*, available: /offers/test-your-system-malware-detection-capabilities.html [accessed 19 Dec 2018].

[2]. Maximum Values Table [online] (2018) available: https://help.fortinet.com/fgt/54/max-values/5-4-6/max-values.html [accessed 19 Dec 2018].

[3]. Oversized Files and Emails [online] (2018) available: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Antivirus/Oversized%20files%20and%20emails.htm [accessed 19 Dec 2018].