Summary

The network architecture of the offices in Dunbeg and Ramelteon are identical consisting of an internal network, firewall, DMZ network for guests and one wise area network. For both the offices A separate network LANs has been created for the employees. Connection to the internet from this internal network have been secured and encrypted using SSL. The networks and traffic will be constantly monitored by individual Fortinet firewalls which have been set up in the offices. Unwanted website access can be restricted in the future if the administration wishes to.

The offices in Dunbeg and Ramelteon are securely connected together, the connection uses encryption so that in case of a network breach the data cannot be misused or stolen. Since the connection between the offices are considered to be secure, the connection bypasses the monitoring of the firewall resulting in a faster site to site connection.

For guests and external vendors an additional LAN network has been set up. This network is to secure the internal servers and resources in case the guest users install a malicious application or virus it will not affect the working of any internal systems in the office. Internet connectivity has been granted to the guest users and will be secured by the firewall application. Guest users will not be able to access or corrupt the data within the internal systems of the offices.

A wide area network has been configured so that users will be able to connect to the internet to run Office 365 application and email clients. This connection will also be monitored by firewall client to block malicious webpages and applications.

The firewall client can be upgraded if it needs to accommodate the growing needs of the offices to support more users and a faster connection. The upgradation would be slightly expensive but necessary if more systems are being installed in the offices.