Crumlin Computers Limited (CCL) is a Small Business Enterprise providing computing services to local SMEs. They do not have a proper network infrastructure for the time being & security is been neglected at all in the existing infrastructure. However, due to the recent business growth, CCL has decided to revamp their Networking Infrastructure in a Secure Manner. After several internal discussions, CCL has finalized their Networking Requirement as follows,

- CCL has recently purchased CLASS C subnet from an ISP as below. 210.211.212.0/24. All subnetworks in new CCL Network Infrastructure shall be devised using above IP Block.
- In the main branch there shall be three Networks Namely Internal User.
- Conference Room & Internet
- Both Internal User network & Conference Room network shall have two PCs in each.
- Marketing & Development units shall be separated from main branch.
- Main branch shall have an External Firewall in placed.
- Development branch Router shall be directly connected to Firewall.
- Development branch shall have three networks comprising a Web Server, Development Unit & Dev_Admin Unit.
- Both Development & Dev_Admin Units shall have two PCs in each.
- Marketing Branch shall be connected to Development branch router.
- Marketing branch shall have three networks comprising an Artwork Server, Creative Teams & NW_Admin.
- Creative Team Network shall have three VLANS (VLAN10, VLAN20 & VLAN30) comprising two PCs in each. VLAN10 & VLAN30 shall be able to communicate with each other but VLAN20 shall not be able to communicate with wither VLAN10 or VLAN30.
- Traffic between Development Unit & NW_Admin shall be encrypted via IPsec Tunnel.
- Artwork Server shall be accessed by Dev_Admin Network only using FTP protocol via port 21.
- Main Branch External Firewall shall be configured as follows,
    1. No traffic initiated from the Internet should be allowed into the internal user or conference room networks.
    2. Returning Internet traffic (return packets coming from the Internet into the main site, in response to requests originating from any of the main site networks) should be allowed.
    3. Computers in the main internal user network are considered trusted and are allowed to initiate any type traffic (TCP, UDP or ICMP based traffic).
    4. Computers in the main conference room network are considered untrusted and are allowed to initiate only web traffic (HTTP or HTTPS) to the Internet.
    5. No traffic is allowed between the internal network and the conference room network. There is no guarantee regarding the condition of guest computers in the conference room network. Such machines could be infected with malware and might attempt to send out spam or other malicious traffic.

- All networking devices shall be Configured with Basic Device Settings,
    1. Routers names.
    2. IP addresses on routers.
    3. Routing configuration (using RIP).
    4. Configure PC hosts/Servers IP setting.

- Further, it shall be Configured Secure Router Administrative Access on all routers in Main Branch ONLY as follows,
    1. Configure encrypted passwords and a login banners.
    2. Configure the EXEC timeout value on console and VTY lines.
    3. Configure a local database administrative user.
    4. Configure Secure Shell (SSH) access and disable Telnet.