Important areas to review in the Network Architecture

- How and where all components are placed?
  - Routers
  - Firewalls
  - Malware/virus protection
  - NAC
  - IPS/IDS
  - App whitelisting
  - etc..
- How network components are segregated and isolated?
- No cleartext communication port should be in action.
- Determine how firewall rules are established to protect assets.
- Make sure ‘default deny’ policy exists in firewall rulebase.
- EDR protection must be in place to protect hosts from anomalies.
- SIEM monitoring must be occurring within the SOC department.
- DLP (Data leakage protection) solutions must be in placed with well-defined controls.
- Host-based IDS/IPS should be capable of detecting zero-days.
- Application whitelisting is controlled by the organisation.
- Firewall logs must be stored on another centralised server.
- ‘Any Any’ rulebase must be not allowed from any source to destination and vice versa.
- Next-generation firewall should be established which can do packet inspection at the application layer, determine users, inspect malware payload, content, traffic etc.
- IDS and IPS systems must be in place which has an ability to protect host and network both.
- Check if the IDS and IPS are placed correctly in the network diagram which protects all assets of the network.
- IDS/IPS signatures must be up-to-date.
- IDS/IPS should detect port scan and payload injection.
- Check how IDS/IPS logs are stored and reviewed.
- Check administration or management access to the firewall, IDS/IPS. Make sure role based access management is setup to access such devices.
- Multiple rules must not be contradicted to one another.
- How security zones are created and designed?