

**Virtual Case Experience**

**Cyber Security**

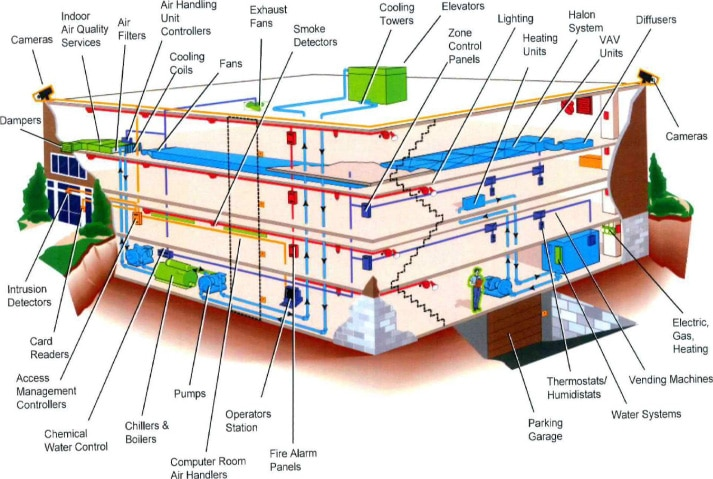
**Task-4**

**Part 1**



Network Segmentation

* Network segmentation is an architectural approach that divides a network into multiple segments or subnets, each acting as its own small network. This allows network administrators to control the flow of traffic between subnets based on granular policies. Organizations use segmentation to improve monitoring, boost performance, localize technical issues and – most importantly – enhance security.
* With network segmentation, network security personnel have a powerful tool with which to prevent unauthorized users, whether curious insiders or malicious attackers, from gaining access to valuable assets, such as customers’ personal information, corporate financial records and highly confidential intellectual property, the so-called “crown jewels” of the enterprise. Today, these assets are frequently found spread across hybrid and multi-cloud environments – public clouds, private clouds and software-defined networks (SDNs) – all of which need to be secured against attacks.



**Part 2**

Network Segmentation

* **Domain:**A namespace which logically divides an organization's network objects that share the same directory.
* **Admin Zone:**Special purpose server zone, e.g. central logging, Security Information and Event Management (SIEM)
* **Server Zone:**General purpose server zone, e.g. application servers, database servers
* **Client Zone:**General purpose client zone, e.g. user laptops

Regarding network segmentation and trust architectures, the base configuration and maintenance of firewalls is of great importance. There are two approaches to configuring firewalls: whitelisting the good or blacklisting the bad.

* **Firewall A (Blacklisting)** –DMZ needs to allow most of the external access while restricting malwares.
* **Firewall B (Whitelisting)** – Only for administrators, it is important to whitelist administrators so that no one without admin privileges can access these servers and only the VPN service would be allowed.
* **Firewall C (Whitelisting)** –Only allows clients and administrators going through secure gateway only.
* **Firewall D (Whitelisting)** – Only authorized person allowed due to criticality of domain controllers.