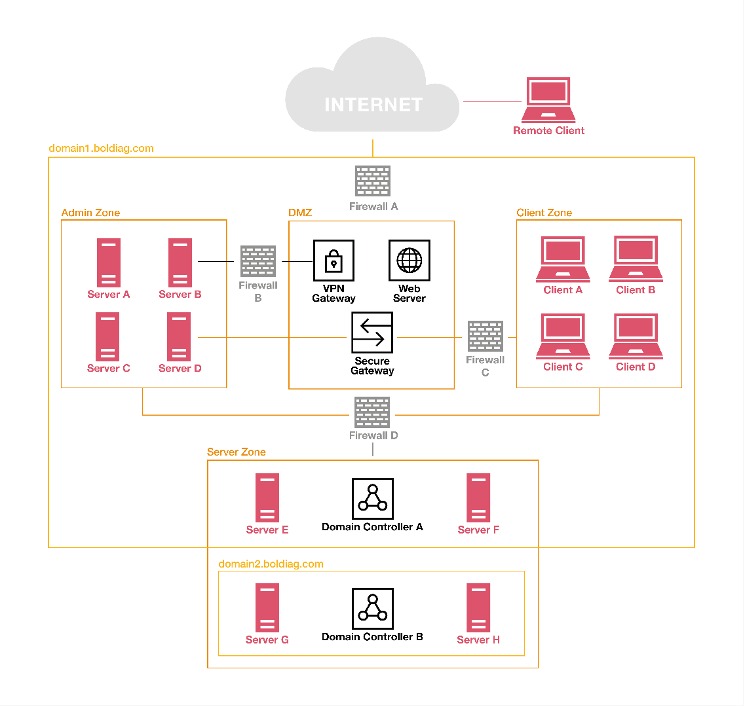
**Network Segmentation**

Segmentation is the process of breaking a large network into smaller ones. Segmentation of a large internet into multiple, smaller network segments provides a number of practical benefits, which affect the choice of how to join segments and at which layer of the protocol stack. The switch or router that runs the segment, and its connection with the next higher segment, are two single points of failure for the segment. If the device fails or the cable is damaged, no device on that segment can communicate with the other devices or the outside world. This can also help isolate other segments from failure of routers or switches, cables, or errors (or attacks) that are flooding a segment with traffic.

Blacklisting is a negative security control model which explicitly defines prohibited and therefore authorises anything that doesn’t fit the definition of being blacklisted.

Whitelisting is a positive security control model which explicitly names or lists approved activities, connections, files, users or applications.



**Domain:**A namespace which logically divides an organisation’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.

**Solution:**

A Person connected to the internet can access the company's website, if the person has the capable software to break through Firewall A then the person is required to break either Firewall B or Firewall C then finally break Firewall D in order to gain the access to domain controllers and the servers of the company.

Providing a blunt view, we can say that a hacker must break through at least 3 Firewalls to gain files and compromise the security of the company.

Meanwhile, giving some time to delay and destroy the attack.