How does segmentation contribute to network security?

The current Internet is not a complete large segment. It is a combination of millions of small scale segments which combine to become the Internet.
These segments are based on the 7 layers of the OSI Model, so based on the segment layer we can assure network security such as at layer 3 we can only discover the switches and not the devices/routers connected to it.

Approach to Configuring Firewalls:

1. Whitelisting is a positive security control model which explicitly names or lists approved activities, connections, files, users or applications.
2. Blacklisting is a negative security control model which explicitly defines prohibited and therefore authorises anything that doesn't fit the definition of being blacklisted.

Configuration of Boldi AG Firewalls:

- A = Black Listing, this is the main source of contact from the internet to the application, so we need to allow all of them to access the file but the naughty ones.
- B = Black Listing, as DMZ acts as a crown jewel, it is open for the public.
- C = White Listing, only the client zone with verified authentication containing of 4 clients should have access to the
- D = White Listing, this firewall is the most important firewall as it acts a link between the admin system, clients and server and not all of them should have access to this.

In today's world, the security policy Zero Trust is a reliable option for security within networks and applications/data servers. Now there are 6 steps of implementing Zero Trust Policy:

1. Identifying and discovering sensitive data (crown jewels)
   Crown Jewels are those critical points in the network that when exposed can lead multiple other compromised machines. So identifying these jewels are very important to assure security of the organisation.
2. Identifying sensitive data flows
   To maintain a safe and secure environment we need to keep a track on how the data flows.
3. Definition and architecture of micro-perimeters/data enclaves
   This is the next step after identifying the previous 2 steps. Knowing the data flows, we need to configure the user groups as such that only the needed information is shared with them and nothing more.
4. Security policy and control framework

This describes a holistic data security approach, involving data categorization, policy enforcement, and access control at various levels. It emphasises the importance of trust verification and threat assessments to mitigate cyber risks.

5. Continuous security monitoring and intelligent analysis
   Effective security monitoring encompasses IT operations, enterprise security, and compliance monitoring. Compliance monitoring focuses on ensuring security controls and the need-to-know principle for data access are in place. Security monitoring involves identifying and responding to cyber threats, aided by threat intelligence feeds and UEBA in the SIEM.
6. Security orchestration and automation
   Once basic security monitoring and compliance are in place, organisations often turn to automated security analytics to swiftly detect and respond to cyber threats. This automation can isolate users and update access controls, improving security. Security orchestration and automation (SOAR) integrates various tools and data sources for more efficient incident response, enhancing security operations.