Network Segmentation and Firewall Configuration for Boldi AG

# Part 1: Network Segmentation and Its Role in Security

Network segmentation plays a crucial role in enhancing the security of an organisation by dividing the network into smaller, isolated sections. This approach limits the spread of potential threats and ensures that critical systems and sensitive data are protected from unauthorized access. The key benefits of network segmentation include:  
  
- \*\*Limiting the attack surface\*\*: By segmenting the network, you create boundaries between different parts of the network. This limits the movement of attackers within the organisation, reducing the risk of lateral attacks.  
  
- \*\*Improved access control\*\*: Segmentation allows you to enforce stricter access policies, ensuring that only authorized users and systems can interact with critical network zones.  
  
- \*\*Enhanced monitoring\*\*: With separate network zones, monitoring and detecting unusual activity becomes easier and more focused. You can apply different monitoring techniques to each segment depending on its security needs.  
  
- \*\*Containment of breaches\*\*: If an attacker breaches one segment, they cannot easily access other parts of the network, which helps in containing the breach and limiting its impact on the organisation.  
  
Network segmentation strengthens not just the network but the overall security posture of the organisation. It provides a layered defense mechanism and reduces the potential blast radius of an attack.

# Part 2: Firewall Configuration for Boldi AG

The network segmentation at Boldi AG consists of multiple zones, each serving a different purpose. Firewalls are key to securing these zones and must be configured carefully using whitelisting and blacklisting approaches.

## Firewall A: Between Admin Zone and Other Zones

- \*\*Configuration\*\*: Whitelisting approach.  
 - \*\*Reason\*\*: The Admin Zone contains critical servers such as central logging and SIEM. Only specific, trusted systems (e.g., servers in the Server Zone or specific management consoles) should be allowed to communicate with this zone. By using whitelisting, you allow only approved connections, minimizing the risk of unauthorized access or attacks.

## Firewall B: Between Server Zone and Client Zone

- \*\*Configuration\*\*: Whitelisting approach.  
 - \*\*Reason\*\*: The Server Zone hosts general-purpose servers such as application and database servers. Only client machines with legitimate business needs should be allowed access to specific services. Whitelisting ensures that only authorized client devices can interact with the servers, reducing the attack surface.

## Firewall C: Between Client Zone and External Network

- \*\*Configuration\*\*: Blacklisting approach.  
 - \*\*Reason\*\*: The Client Zone includes user laptops and general-purpose devices that interact with external networks. In this case, it is more effective to block known malicious or unwanted traffic while allowing general internet access for users. A blacklist will block harmful traffic but keep the network open for normal operations.

## Firewall D: Between Server Zone and External Network

- \*\*Configuration\*\*: Whitelisting approach.  
 - \*\*Reason\*\*: Servers in the Server Zone should have minimal interaction with the external network. Only specific, necessary traffic (e.g., updates from trusted vendors or cloud services) should be allowed. Whitelisting ensures that only essential connections are made, safeguarding the servers from external threats.