Demilitarised Zones and Intrusion Detection Systems

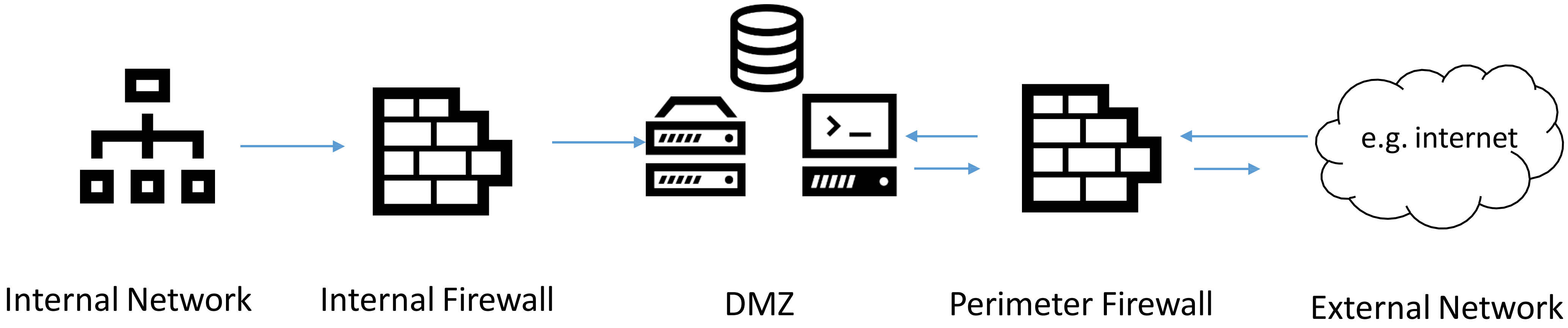
Dr Rosanne English

Demilitarised Zone (DMZ)

- A part of a network which is in place between the protected network and the untrusted external network
- Provides additional security
- Helps manage routes from private network to internet and vice versa

Demilitarised Zone (DMZ) Architecture

- One common approach is a 2 firewall architecture
- perimeter firewall allows access from the external network to the DMZ
- internal firewall allows access from the internal network to the DMZ



Intrusion Detection Systems (IDS)

- Automates the process of monitoring network traffic for potential violations
- Intrusion Prevention System additionally can prevent violations
- Functions
  - record information related to observed events
  - notify security administrators of important events
  - produce reports for management

Limitations

- Only the first step in defence
- Can’t stop
    - Administrator misconfiguration
    - Insider threat
    - Social engineering