

## Network security

### Network security controls

- Include: Access control, Identification, Authentication, Authorization, Accounting, Cryptography, Security Policy

### Access control

- Restrictions that determine who has access to what on a system/network.
- **Physical access control**
  - Restricts access to physical locations and buildings.
- **Logical access control**
  - Restricts the access to networks and information.
- Terminology
  - **Subject** = Who's reaching, user or process which accesses the objects
  - **Object** = What's being reached, resources upon which the restrictions are placed
  - **Operation** = Verb, What's being done, the action performed by the subject on the object
  - **Reference Monitor** = implements the rules which define what actions on the object can a subject perform
- Involves
  - **Identification**: unique identity in any given system
    - There are your credentials
    - e.g. social security number, username and password.
  - **Authentication**
    - You're granted access via credentials
    - You use the credentials
  - **Authorization**:
    - What you can access, where you can go, can you park somewhere

- **Accounting**

- Act of logging and creating account of all actions, what has been done.

## **Network security zoning**


- Grouping networks for efficient management of networks.
- Any network has physical firewalls (routers) which has software to act as firewall and control the traffic
  - However it's hard to manage each network instead best to group them in zones and apply rules in that zone.

## **Security zone**

- Group of similar people or systems by characteristics e.g. functionalities to apply same rules.
- Properties include:
  - Active security policies in regard to the network traffic
    - E.g. to implement the policy "secretaries cannot reach twitter", can block those sites through firewall rule in their zone
  - Detection and blocking of malicious traffic
    - Software needs to actively scan and label what's malicious or not and stop malicious traffic
  - List of known IP addresses and address sets
    - IP address of device and interface are different
  - List of the zone interfaces
- A device or an interface can have multiple IP addresses
  - E.g. wired connection has one interface, another interface to connect to DB
  - **Maintenance interface**
    - Last resort to fix stuff
    - Usually no security boundaries/guards on those interfaces
    - Must have physical security

- E.g. someone goes in to server room in cold jacket codes, plugs in a laptop and uses maintenance interface to fix something.

## Zone examples

- **Internet zone**
  - Uncontrolled zone out of boundaries of an organization.
-  **DMZ Zone**
  - Controlled zone.
  - Also known as demilitarized zone
  - Provides a barrier between the external and internal networks.
  - Included in every router.
  - Uses firewalls control what can go in and out.
- **Production zone**
  - Restricted zone.
  - Firewalls are used to filter inbound and outbound traffic
  - Access from uncontrolled networks is strictly controlled.
- **Intranet zone**
  - Controlled zone with less restrictions
- **Management zone**
  - Secured zone which enforces strict policies and limits access to a few authorized users.