# Confidentity

Passwords

Acces atacks zijn er om zo lte laten zien waarom password nodig zijn. En paswoord mogen nooit gegeven worden aan mensen.

* Max password age
* Bepaalde checklist

Ipsec

* VPN
  + Remote-access
  + Site-to-site

Access controle models

* Mandatory Access Control
  + Strikt Defensie
* Distretionary Access Controle
  + Gebruiker zegt wlke gebruikerz zijn haar documenten kan bekijken
* Role-Based Access Controle
  + Toegan gebaseerd op functie
* Attribute-based Access Control
  + Zoals Role-based maar gebruikt verschillende attributen voor gebruiker, middelen, object. If-then

Authentication – Authorization – Accouting

* Account voor meerder gebruikers.

# Integrity

* Consistente , nauwkeurige en betrouwbare data

Version Controle :: Configuraties

* Up-to-date
* Juiste versie
* Terug draaien

Cryptographic hash

* Berichte + hasing(wiskundige formule) = hash

Host-Based Intrusion Detection

* Monitors en stuurd alerts naarAdmin
  + Host-based --> beschermt host tegen Malware en stuurd raport
  + Integrety check --> zorgt ervoor dat alle date in netwerk intergeriteit behoud

Back-ups

* Meerdere back up

# Availability

* QOS Improves 🡪 beschikbaarheid goed

Harware & Software

* Up-to-date software en hardware
  + Performance verminderd
* Onderhoud software en hardware

🡪 kabels, machines

* Redudantie : netwerk is altijd op
  + Spanning Tree Protocole
    - Verkomt loops, netwerkt blijft werken
  + Etherchannel
    - Load balance
    - Sneller verkeer

# Auto-Qos Configureren

### Auto-QoS VoIP

* Media Access Control -- > Priority to phones
* Qos 🡪 bandwidth en prioriteiten