Network Security
1. Some basic principles

- Least privileges
  - You should only be able to do what you need to do

- Defense in depth
  - It is better to have several layers of security

- Simplicity
  - A complicated system will have more errors and be more difficult to audit
Some basic principles

- User participation
  - If security prevents users from working efficiently, they will find ways around

- Default deny
  - Better to deny everything and make exceptions (white list), than allowing everything and then specify what is forbidden (black list)

- Weakest link
  - A system is not more secure than its weakest part
  - Do not invest much effort on one aspect when other aspects are not covered.
2. Classical network perimeter
Classical perimeter

- Firewall: filter traffic at network level
- Proxy: filter/authenticate/analyze traffic at application level
- DMZ: limit the propagation of attacks
- Intrusion detection (IDS), Anti-virus, spam filter, Unified Threat Management (UTM),
  - Built into firewalls, or stand-alone
  - Analyze traffic, detect attacks
3. Virtual private networks (physical network)
VPN: virtual network

192.168.40.5

11.12.13.14

VPN

192.168.10.x

Internet

5.6.7.8

VPN

192.168.30.x

123.4

VPN

192.168.10.x

192.168.30.x

Ph. Oechslin
VPN: basic elements

- VPN software on routers and/or computers
- Encapsulation of IP packets for their trip through the Internet
- Encryption of data to protect confidentiality
VPN for «anonymous» surfing

- VPN provider knows exactly where you come from and where you got to!
- Can be useful in a public hotspot.
4. BeyondCorp

- Google: "We want to completely get rid of the idea of having some sort of perimeter,"
- "Effectively, firewalls don't help and a lot of other gatekeeper tools that rely on a perimeter simply don't help."
- Strong authentication of devices and users
- Cloud based services behind an access proxy
- Automatic inheritance of least privilege
BeyondCorp

BeyondCorp: A NEW APPROACH TO ENTERPRISE SECURITY

- UNPRIVILEGED NETWORK
- MANAGED DEVICE
- 802.1X
- RADIUS
- ACCESS PROXY
- ACCESS CONTROL ENGINE
- SINGLE SIGN-ON
- USER/GROUP DATABASE
- TRUST INFERENCE
- PIPELINE
- CERTIFICATE ISSUER
- DEVICE INVENTORY DATABASE

BeyondCorp components and access flow