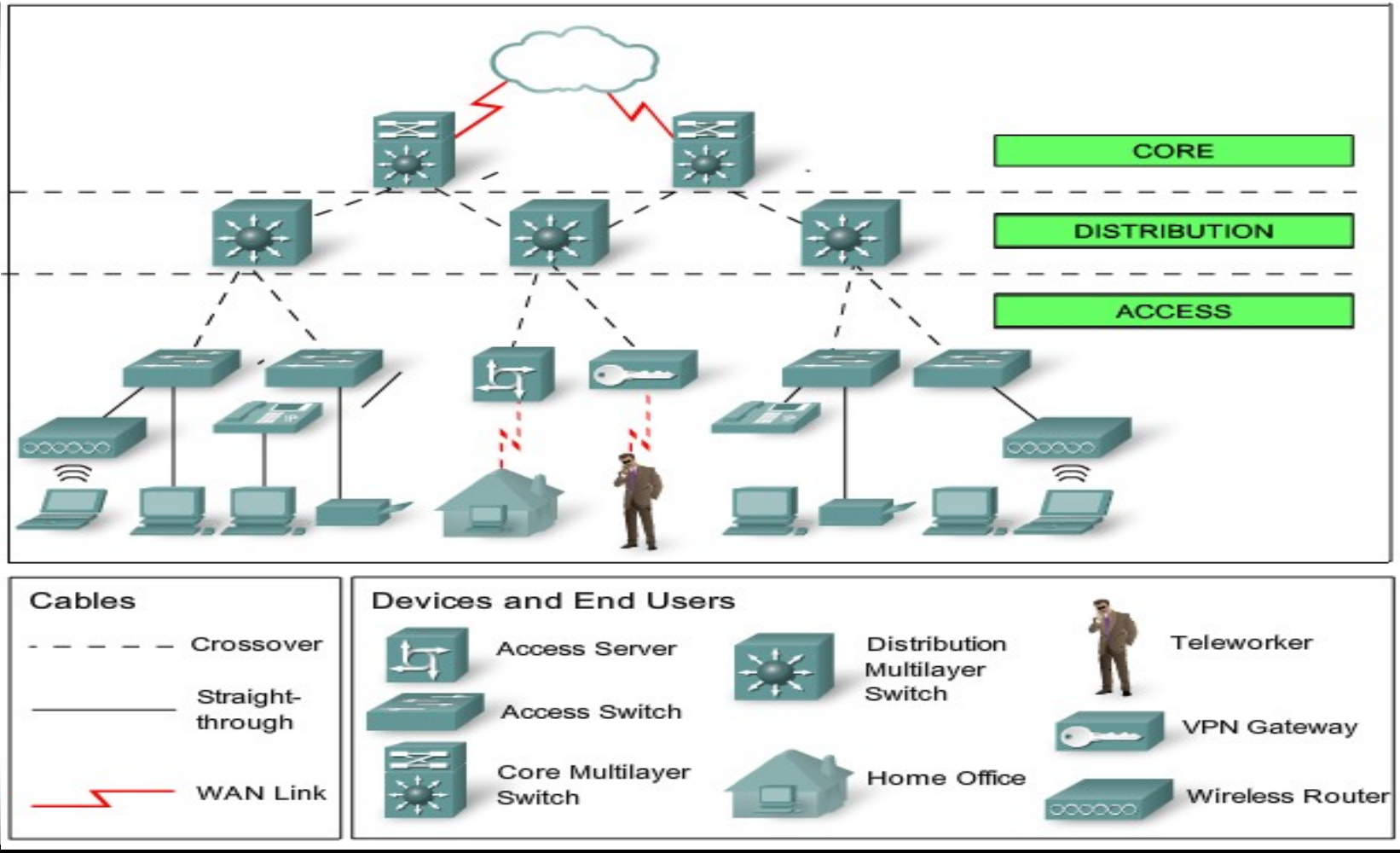
Bezpečnost síťových aplikací

2019/2020

Př 4

Zabezpečení síťového provozu



Zabezpečení síťového provozu

- Omezení připojení
  - Port security, Vlan, 802.1x, WiFi
- Omezení přístupu
  - Firewall, ACL, DNAT, Stunnel, VPN
- Šifrování komunikace, ověření
  - SSL, Routovací protokoly
- Omezení zdrojů
  - Oddělení cest, shaping

Omezení připojení - pevná

- Switche / Huby
  - Defaulní hesla
- Nemožnost fyzického připojení
- Defaultně deaktivované porty
- Pamatování si adres a jejich limit
  - Log, omezení, zákaz
- Autentizace portů
  - 802.X

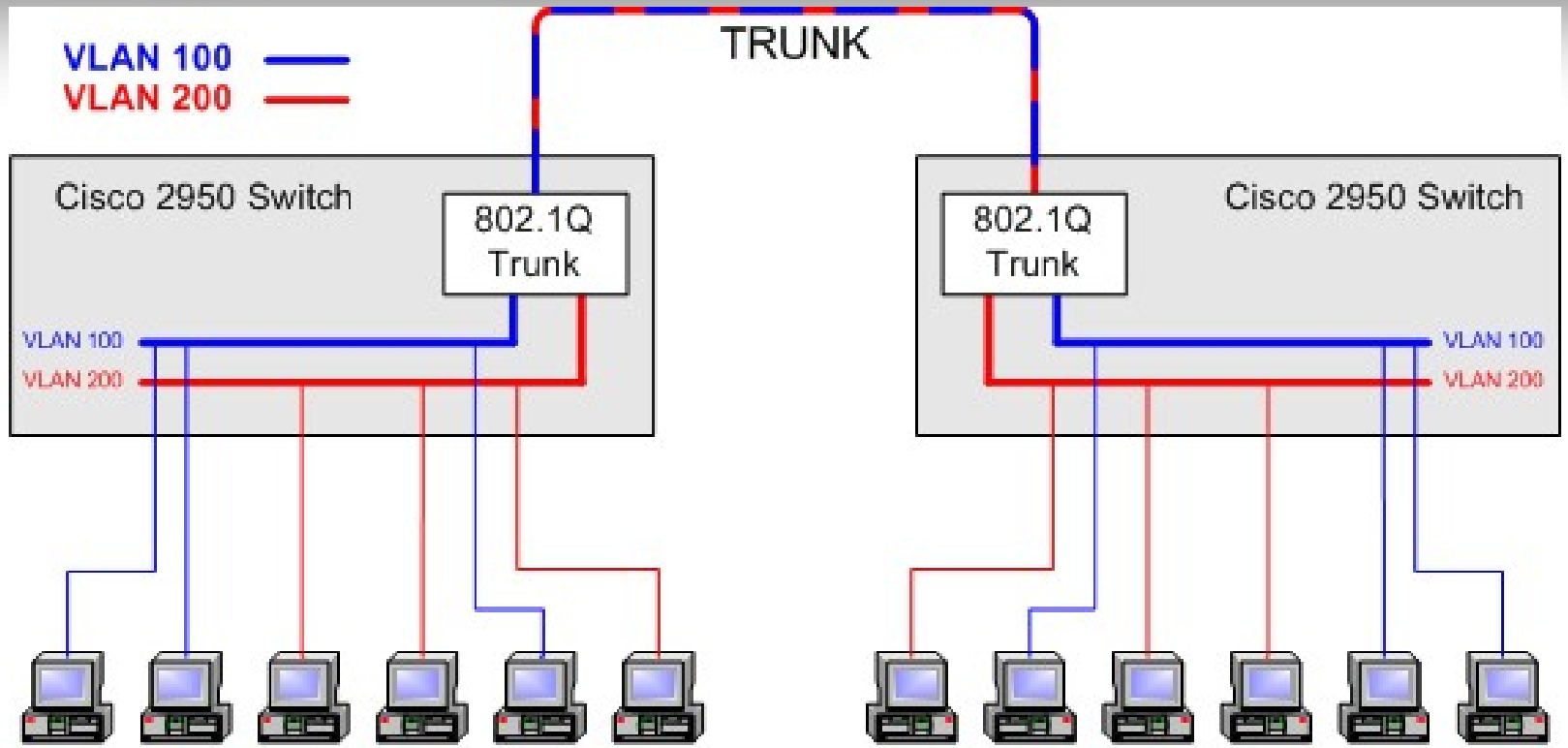
802.1X

- Protokol autorizující přístup na port / WiFi
- Využívá Radius server
- Všechny rámce kromě EAP ignorovat
- Pro neautorizované extra Vlan

Vlan / Trunk

- Rozdělení switche na více samostatných
- Vlan – neplést s WLAN !!
  - Povinné číslo, možnost i jména
  - Přídává ID do hlavičky rámce
- Trunk
  - Agregace více Vlan jednou linkou
  - Taggovaný / Netaggovaný provoz
  - Nativní Vlan

Vlan / Trunk

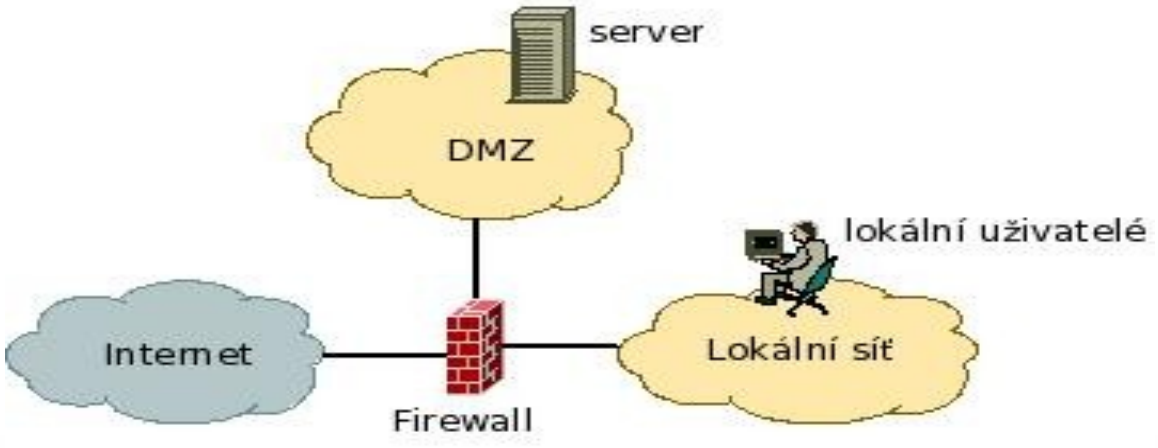


WiFi

- Problém limitace fyz. připojení
- Více typů 802.11 a,b,g,n, ac
  - Různé rychlosti, zpětně kompatibilní
- Ověření
  - Web / WPA / WPA2
  - Heslo / jméno+heslo
- Omezení počtu klientů / řízení

Firewall

- Základ zabezpečení sítí / ACL
- DROP ALL + povolování
- DMZ – volnější pravidla



Firewall II

- DNAT/port forward – díry ve FW
- Autorizované dočasné díry
  - Po autentizaci se otevře propoj
- Možnost přepisovat packety
- Možnost implemetovat pro INPUT I OUT-PUT
  - Omezení pro Proxy

Proxy

- Aplikační firewall
- Pevně svázané s protokolem
- Omezuje, ale i cachuje
  - Jméno + heslo
  - IP adresy
  - White/black listy
  - Upozornění na podezřelou činnost

VPN

- Virtual Private Network
- Zabezpečení prostupů přes FW
- Typ použití
  - Site-to-site / remote access
- Typ zabezpečení
  - SSL / IPSec / MPLS
  - White/black listy
  - Upozornění na podezřelou činnost

VPN - SSL

- Založené na SSL a hierarchii CA
- Kombinace jména a hesla + certifikát
- Typicky pro Remote Acces VPN
- Mnoho implementací
  - OpenVPN, VPND, FortiSSLVPN, SSLVPN

VPN - IPSEC

- Dvě fáze ověření
  - Host, šifrování, pre-shared key, time, NAT-T
  - Sítě, šifrování, time life
- Obecná implementace
  - HW, cisco, juniper
  - SW FreeSwan, StrongsWan
- Různá terminologie
  - ACL, Policy, routing

Šifrování

- Typicky na Access, Distributed, NE CORE
- SSL nebo RSA
  - HTTPS, IMAPS, …. nativní
  - Tunnel – SSH nebo Stunnel
- Šifrovat vše kudy jsou data
- Nárůst dat a snížení rychlosti

Routovací protokoly

- Na core vrstvě nešifrujeme, ale ověření ano
- Core
  - Point-to-point spoje, BGP
  - heslo, bez šifrování
- Access, Distribution
  - Multi-point, RIP, OSPG, EIGRP
  - Hesla, omezení odkud smí přijít

Omezení zdrojů

- Předcházení DOS, DDOS
- Rozdělení provozu
  - Business x Relax
- Shapping
  - Limitace rychlosti, spojení, packetů
- QOS
  - Upřednostňování obsahu