Správa serverů a počítačových sítí

2020/2021
přednáška č.1
(ver. 2021-02-23-01)

Základní informace

- Přednášející :
  - Ing. Luboš Matějka, Ph.D. (Linux/Unix),
    - Email : lmatejka @ kiv.zcu.cz
    - Konzultace : St 10:05-11:00 nebo dle dohody e-mailem
  - Ing. Ladislav Pešička (Windows)
    - Email: pesicka @ kiv.zcu.cz
    - Konzultace: Po 13:00-14:00, St 13:00-14:00
- Cvičící :
  - Ing. Jindřich Skupa (Linux)
    - Email: skupaj @ kiv.zcu.cz
    - Konzultace: St 13:00-13:30, Čt 15:00-15:30

Nutné podmínky pro splnění předmětu

- Účast a práce na cvičeních
- **Úspěšná automatická kontrola virtuálu**
- Zápočet: nastavení a předvedení zadané konfigurace
  - GNU/Linux i MS Windows Server
  - Povolené materiály
  - Max 10b na zápočet 7b
- Zkouška:
  - Část hodnocení ze cvičení – body nad 7b
  - Písemná zkouška

Zkouška

- Písemný test
- Bez materiálů a cizí pomoci
- Hodnocení:

43-35 bodů : 1
34-30 bodů : 2
29-25 bodů : 3
24-0 bodů : 4

- Část hodnocení ze cvičení – body nad 7b

Organizace cvičení

- Cvičení probíhá v UC326 / na Google Meet
- Dva vlastní servery
  - GNU/Linux Debian – trvale spuštěný na ZCU
  - MS Windows Server 2019 – lokálně z VirtualBoxu
- Jednotlivá cvičení budou ***navazovat!!***
- Stejná služba se bude konfigurovat na Linux i na Windows
- Zápočet bude vycházet z procvičených konfigurací

Plán přednášek I.

- Úvod, důvody pro správu a běžná úskalí
- Úvod do HW a OS
- IP, DHCP, Firewally, DNS
- WWW služby
- Databázové systémy
- Poštovní služby
- Souborové servery a bloková zařízení
- Zálohování dat a redundance služeb
- Zabezpečení a Detekce útoků
- Virtualizace a CloudComputing

Závěrem

- Cílem jsou praktické dovednosti
- Servery dostupné po celou dobu semestru
  - V případě potíží email na cvičícího / přednášejícího
- Podněty od studentů vítány...

- Rozumné dotazy kdykoliv ;)

Důvody správy systémů

- Bezpečnost
  - Napadení hackery, viry, roboti
- Stabilita
  - Restart 2-3x denně?? To není řešení ….
- Snadné rozšiřování systémů
  - Instalace 1 balíčku jich sebou chce 200 ….
- Důvěryhodnost
  - Pokud něco opakovaně nejde, klesá důvěra a ochota se dohodnout
- Rychlost řešení požadavků uživatelů
  - Přidání uživatele může být akce na 2 min i 2 dny ...

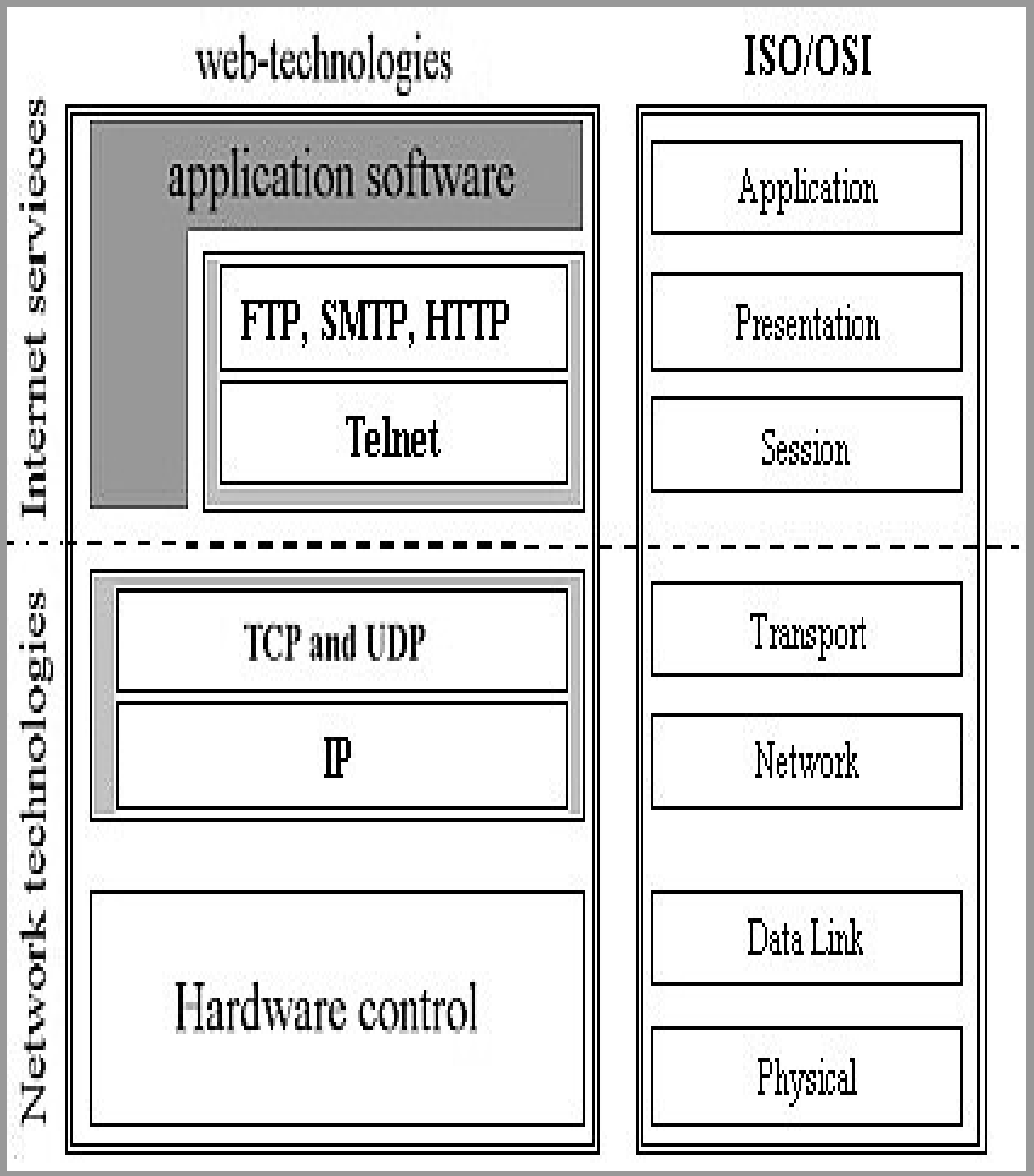
Klasické problémy správců

- Neznalost používaných technologií
- Uživatelé
- Vedení
- Nekvalitní SW či HW
- Nekompletní či chybná dokumentace
- Neochota třetích stran řešit problémy
- Špatné smlouvy – nesplnitelná očekávání
- Marketingová lákadla

Vhodný HW a SW

- Síťové prvky
- Typy serverů
- Úložná zařízení
- Zálohy napájení
- Vzdálená správa
- Umístění serverů – server housing
- Typická využití Unixu a MS Windows

1. Síť a síťová zařízení



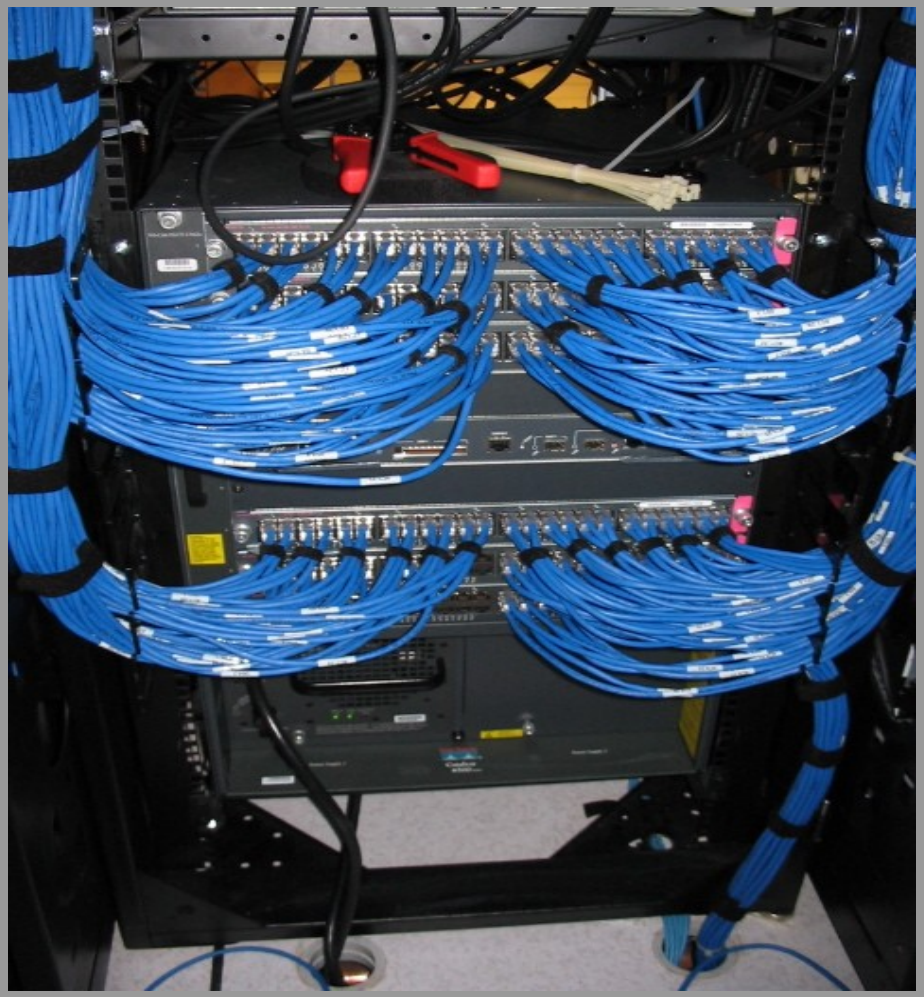
- Nějaká síť je v každé firmě
- Běžné síťové prvky:
  - Router / Firewall
  - Switch / Hub
  - AP / VOIP phone

1.1. Síťové prvky

- Switch, Hub
  - Spojují síťový provoz z více uzlů do jednoho
  - Téměř vždy jednorázová HW zařízení
  - Některá zařízení jsou konfigurovatelná – pozor na *defaultní hesla*
  - Další možnosti jako VLAN, Trunk
  - Nutná důslednost v popisech !!
- Výrobci Cisco, 3Com, Dlink, HP, TP-Link

1.1. Síťové prvky

1.1. Síťové prvky



1.2. Router

- Směřování provozu v sítí
- Filtrují provoz podle pravidel na L2 či L3 vrstvě
- Mohou být HW, ale velmi často se jedná o instalace různých Unixů, typicky Linux či BSD (IPCop)
- Velká škála zařízení od Cisco, Fortigate, Juniper, 3COm či levnější MikroTik

1.2 Router


SEA TEL
Professional IT Solutions

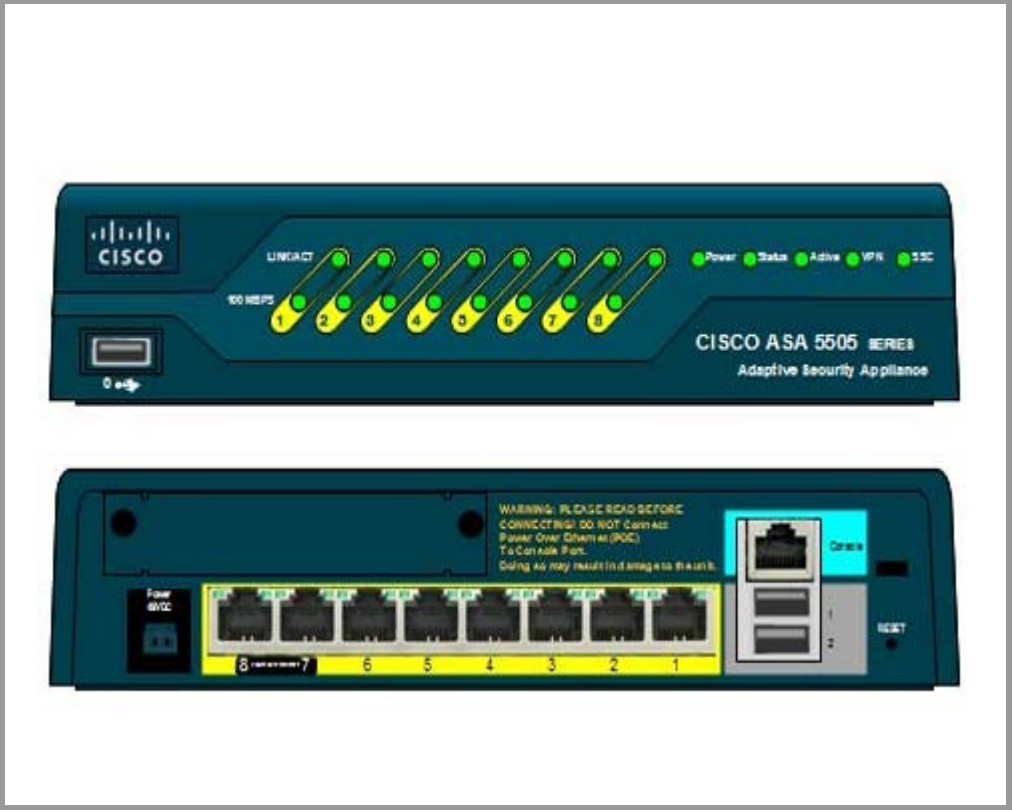

FORTINET
FortiGate 300D


CMD

1.3. Firewall

- Každá síť i server i stanice by měla obsahovat firewall
- Nyní vhodné dělat neomezená mapování do vnitřních sítí, lépe použít VPN
- Na serverech je dobré limitovat i odchozí provoz
  - Zamezí útokům pomocí reverzních kanálů
  - Využívá se stavová tabulka spojení
  - Limitem je velikost tabulky, může zpomalovat provoz
- Cisco PIX, ASA, Fortigate,...

1.3. Firewall


CISCO
CISCO ASA 5505 SERIES
Adaptive Security Appliance

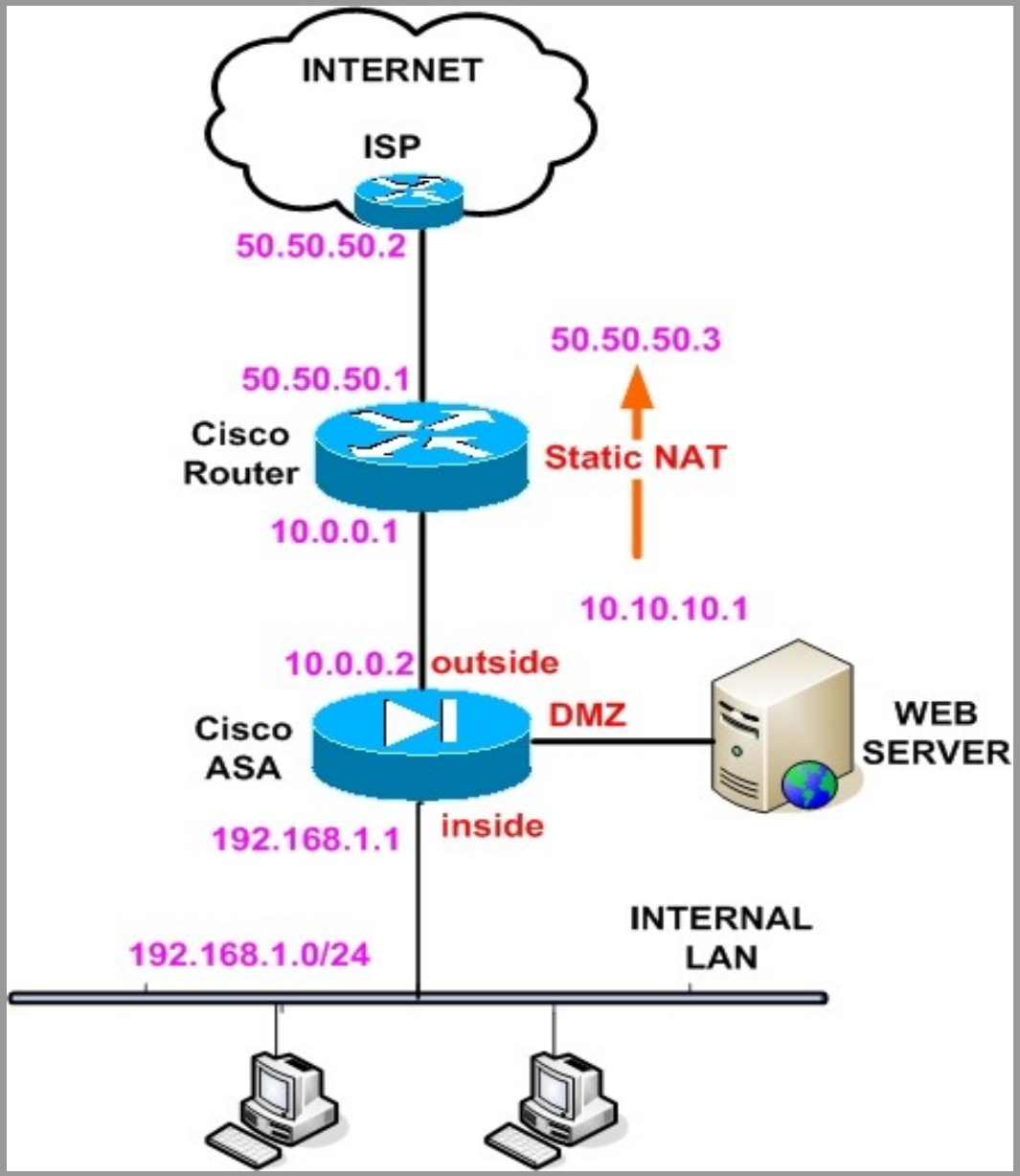

ZyXEL
ZyWALL USG 50
WAN 10/100/1000
LAN/DMZ 10/100/1000


CMD

1.4. Neveřejné sítě

- Síť není běžné adresovatelná z internetu
- Adresy jsou typicky v jednom z rozsahů:
  - 10.0.0.0 / 8 16777214
  - 172.16.0.0 / 12 1048574
  - 192.168.0.0 / 16 65534
- Neveřejné adresy se převádí routeru na jednu či více veřejných adres - NAT
- POZOR – někdy je jako neveřejný užito cizích adresních rozsahů, např 1.1.1.0/24

1.4. Neveřejné sítě



1.5. Sdílené/přepravní sítě

- Nově vyčleněný v rámci RFC6598 / 2012
- 100.64.0.0/10
- Určený pro Carrier-Grade NAT (CGN)
  - Řeší NAT v sítích proviadrů, kde na obou stranách mohou být stejné neveřejné sítě
  - Eliminuje konflikt při NAT444
- Bývá používám v u ISP i v datových centrech

1.6. Vhodné zařízení pro vaši síť

- Volba podle počtu uživatelů a provozu
- Velmi často rozhoduje cena :(
- SW zařízení mají nižší pořizovací, ale vyšší provozní náklady, více možností konfigurace, ale i útoků
- HW zařízení bývají lépe odzkoušena a odladěna na vzájemnou spolupráci, lepé odbavují větší provoz