Základní principy obrany sítě

Michal Kostěnec
CESNET, z. s. p. o.

Základní stavební kameny

- Správný design sítě
- Víceúrovňové filtrování provozu
- Ochrana koncových stanic
- Ochrana aktivních prvků
- Monitorování služeb
- Monitorování síťové komunikace
- Ochrana klientů (před klienty)

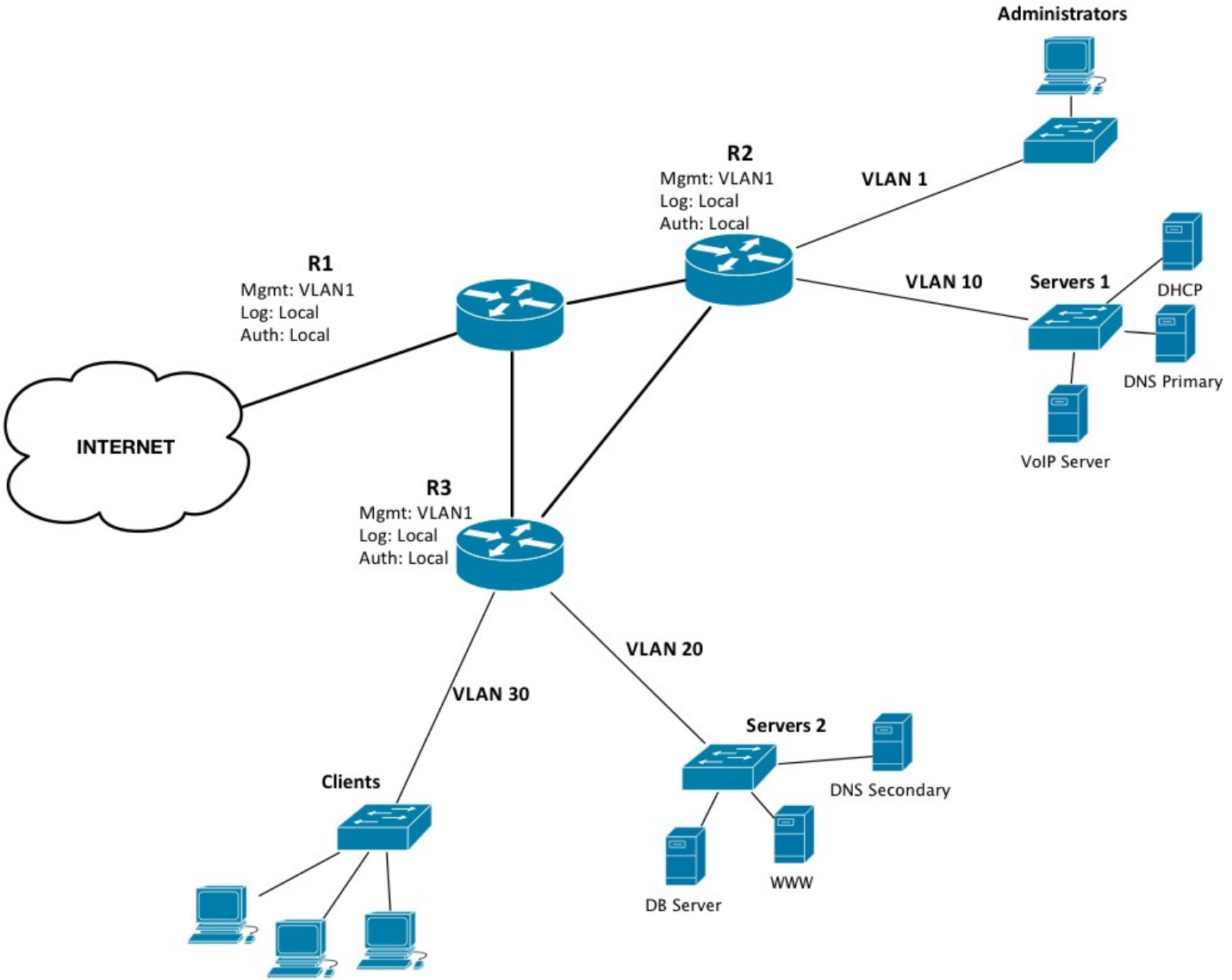
Univerzální, rozšířitelná síť

- Nutné si uvědomit
  - Síť se neprovozuje pro jeden druh služby
  - Přidání dalších služeb neznamená zásadní zásah do současné infrastruktury
  - Přidání dalších služeb neznamená zhoršení kvality současně provozovaných
  - Nebezpečí přichází z venku (z Internetu)
  - Nebezpečí přichází zevnitř (od uživatelů)
    - Vědomě vs nevědomě

Trocha síťařiny – to musíme mít

- Zásadně se neprovozuje jedna velká síť!
- Rozdělení na menší podsítě se společnými vlastnostmi
  - VLANy
  - Směrování
    - Možnost filtrování provozu na hranici podsítě
      - Zdrojová a cílová IP (L3)
      - Cílová služba (port, L4)
  - Ve speciálních případech zcela oddělují směrovací tabulky
    - VRF-lite (Virtual Routing and Forwarding)

Obyčejná síť



Trocha síťařiny – to musíme mít

- Sítě
  - Administrátoři
  - Servery obecného typu
    - DNS, LDAP, AAA, …
  - Servery s citlivými službami
    - VoIP, Databáze, Správa politik, Správa antiviru
  - Mgmt síťových prvků
  - Klienti
    - Drátové vs bezdrátové připojení, VPN
  - Karanténa

Trocha síťařiny – to musíme mít

- Filtrování provozu
  - Hranice sítě
    - FW (dostatečně výkonný pro naší linku)
    - Hraniční (páteřní) prvek
    - Známé porty lokálních služeb
      - Windows 135-139
      - SMB 445
      - SMNP 161
      - SMTP 25
    - Naše adresy nepřichází z Internetu
    - Výrazné odhlehčení celé síti

Trocha síťařiny – to musíme mít

- Filtrování provozu
  - Podsítě (předřazené prvky)
    - Router - ACL (Access Control List)
      - Účinné
      - Mohou být nepřehledné
      - Jediná volba, pokud nemáme FW
    - FW
      - Citlivé sítě schované za prvky(prvkem)
      - Centrální správa
      - Omezené výkonem FW
    - Loadbalancery
      - Rozkládání zátěže na jednotlivé servery
      - Možnost filtrování až do L7

Koncová zařízení

- Filtrování provozu
  - Koncová zařízení
    - Windows FW, iptables, ip6tables
      - Používat whitelisting = Výchozí pravidlo „DROP“
    - Povolení pouze potřebných porty
    - Omezení zdrojové adresy na nejnutnější rozsahy
    - Pokud aplikace umožňuje, omezuje se i v ní
      - DNS, SMNP, inetd, ...
    - „ping“ pouze z našich sítí
    - FW, kterému rozumíme (Shorewall?)

Koncová zařízení – systém a aplikace

- Ladění parametrů systému
  - Syncookies
    - Automaticky při zahlcení fronty
    - Ochrana proti synflood
    - Účinné
  - FIN timeout, Keepalive timeout
- Záplatování!
- Apache
  - MPM moduly (Multi-processing modules)
  - Keepalive
  - Connection timeout

Koncová zařízení

- Aktivní prvky
  - Mgmt z vyhrazených podsítí
    - SSH, SNMP
  - Ochrana řídící části (control plane)
    - CPU MIPS apod.
    - Vícejádrové INTEL
    - Rate limiting = CoPP (Control Plane Policing)
  - AAA (Authentication, Authorization, Accounting)
    - Centrální ověřování, autorizace
    - Logování!
  - Silná hesla nejen pro přístup
    - Routing, FHRP, ...

Logování

- NTP!
- Logování přiměřenou úrovní
  - Lokálně
    - Velké množství informací může vyčerpat místo na disku (obzvláště při síťovém útoku)
    - Detailní log poskytuje kompletní informace
  - Centrální server (syslog-ng)
    - Kopie lokálních logů
    - Klasifikace dle syslog úrovně
    - Klasifikace dle ip/hostname
    - Klasifikace dle data
- Textové logy se dobře komprimují

Vyhodnocování síťového provozu

- Honeypoty
  - Systém emulující služby
  - Dělení podle míry interakce
  - Systém včasného varování
  - Možnost sledování nových postupů útočníků
  - Získávání použitých prostředků
    - IP útočníků
    - Použitý slovník pro bruteforce
    - Shellkódy
    - Skripty
  - Kippo, Dionaea, LaBrea, …
- Systém pro výměnu detekovaných bezpečnostních událostí
  - WARDEN

Monitorování služeb/zařízení

- Lze sledovat
  - Dostupnost serveru (koncového zařízení)
  - Dostupnost služby
  - Stav systémových zdrojů
  - Další volitelné položky
- Nagios (Icinga)
  - Rozšiřitelné přes pluginy
- Dude
  - Dostupnost zařízení (ping)

Sledování síťového provozu

- Exportování Netflow
  - Užitečné informace o síťovém provozu
  - Export hlaviček, nikoliv dat
  - Open-source i komerční softwarové analyzátory
  - Archivace záznamů
    - Agregace dat na IP a porty
    - Doba závisí na objemu dat
    - Měsíce až rok(y)
  - Vlastní skripty pro vyhodnocování anomálií v síti

Vyhodnocování síťového provozu

- Speciální software (a HW)
  - IDS (Intrusion Detection System)
    - Paralelně v síti (zrcadlení provozu)
    - Pokročilé algoritmy pro hledání anomálií
      - Zaškolení obsluhy
      - Trénování algoritmů
        - Přizpůsobení charakteru našeho provozu/sítě
        - Eliminace falešných pozitiv
  - IPS (Intrusion Prevention System)
    - Blokuje nežádoucí provoz
    - HW nákladné, cena úměrná kapacitě linky

Klienti v síti

- Připojujeme pouze „známé“ klienty
  - Tzn. známe jejich identitu nebo zodpovědnou osobu
  - Registrace MAC adresy = vždy stejná IP
    - IP ~ MAC = DHCP, IP ~ hostname = DNS
    - Sauron (http://sauron.jyu.fi/)
  - Přiřazení adresy pouze přes DHCP
    - Vynucení na úrovni aktivních prvků (DHCP snooping)
  - U WiFi složité
    - Řeší 802.1x
- „Neznámí“ klienti
  - Dočasný přístup (heslo s omezenou platností, ...)

Klienti v síti

- 802.1x
  - Nejlepší řešení
  - Řízení fyzického přístupu do sítě
  - Autentizace jménem/heslem
  - Nejčastěji pro bezdrátové připojení
  - Funguje pro IPv4 i IPv6
  - Obtížné nasazení pro drátovou část
    - Horší podpora v OS
  - Infrastruktura ověřovacích serverů
    - RADIUS

Klienti v síti

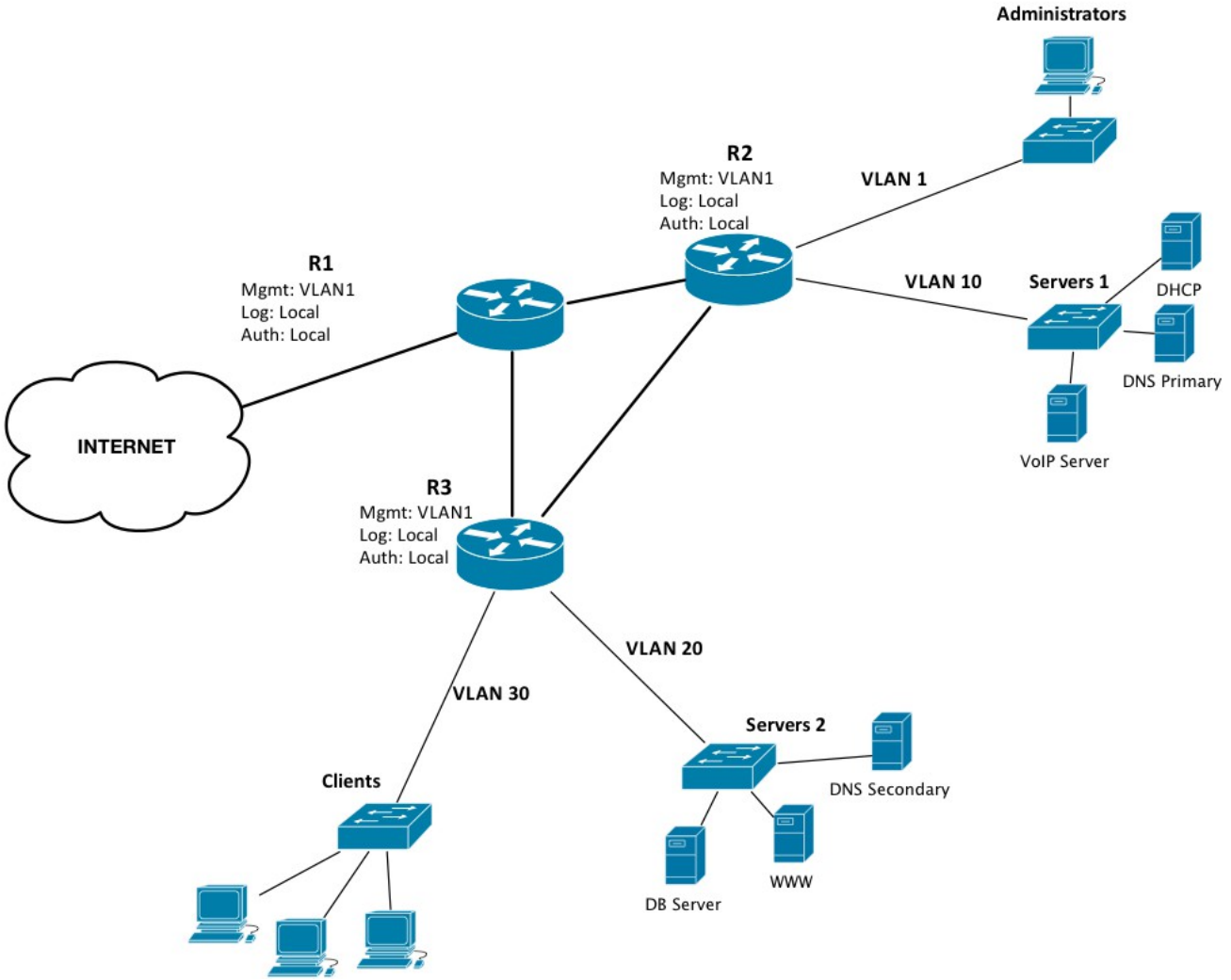
- IPv6
  - Není nastaveno v síti (na směrovačích)
    - = nemusí se řešit?!
    - Stanice nejsou dostupné z Internetu?!
  - Mám nastaveno na směrovačích
    - Několik stanic v síti, pečlivě zabezpečených
    - Ostatních se to netýká?!
  - Stejné návrhové problény jako u IPv4 a mnoho dalších
  - IPv6 Guards na výkonějších platformách
  - Netflow kolektor s IPv6 podporou = FTAS

Klienti v síti

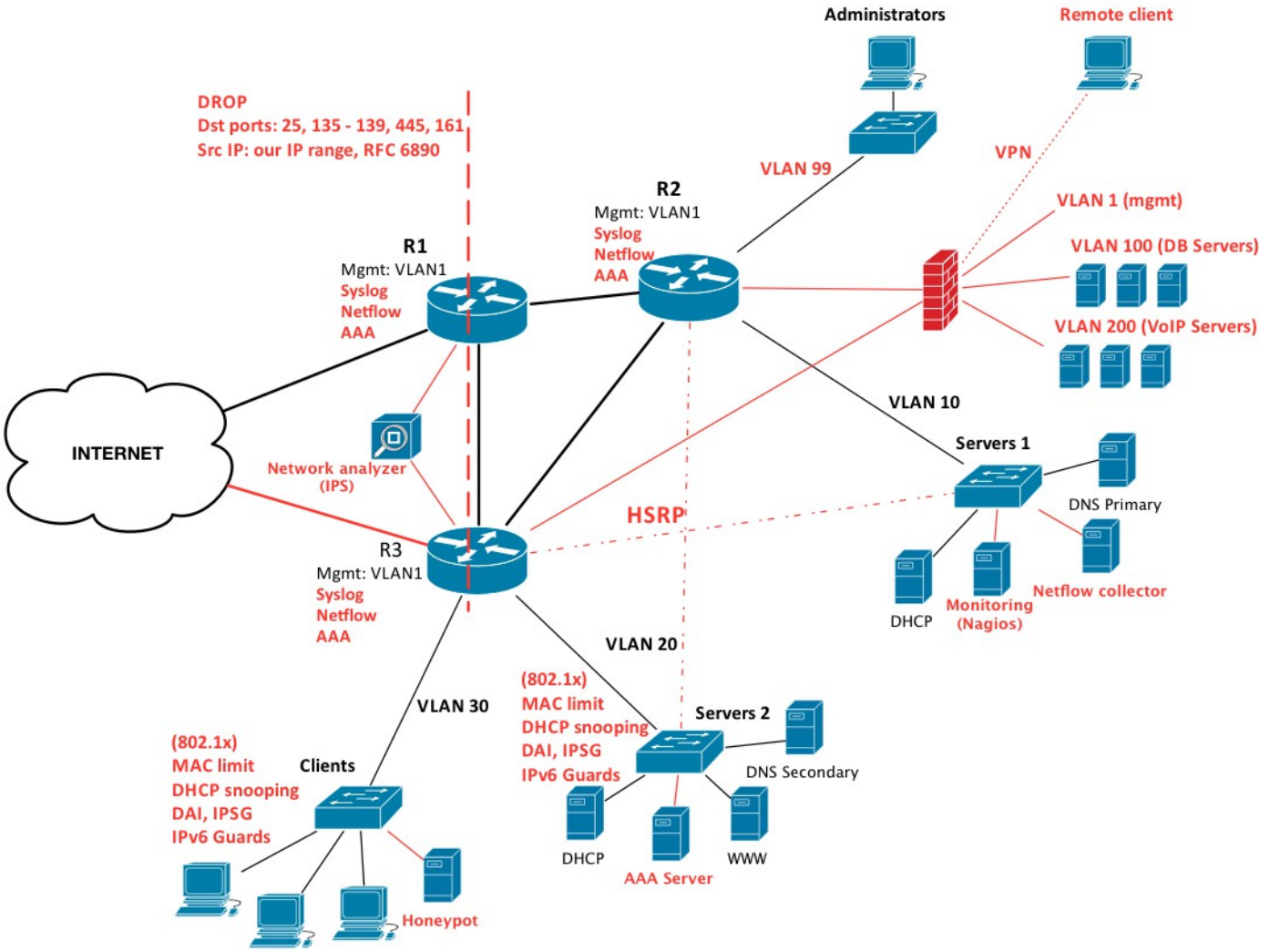
- Bezpečnostní funkce
  - (IPv4) Počítáme s registrací zařízení (DHCP)
    - DHCP Snooping (DHCP spoofing)
    - Dynamic ARP Inspection (DAI) (ARP spoofing)
    - IP Source Guard (IPSG) (IP spoofing)
  - (IPv6)
    - RA Guard, IPv6 Source(Destination) Guard
    - IPv6 snooping,
    - IPv6 ND inspection
    - DHCPv6 Guard

  Omezení počtu MAC adres na portu
    - Zaplavení vnitřních tabulek přepínače

Zpět na začátek, pamatujete si?



Trocha vylepšení...



Vylepšení stávající sítě

- FW v páru (režim High Availability)
- DNS Round Robin
- Loadbalancing
- Anycast
- HSRP, VRRP(GW, servery)
- uRPF
- RTBH routing
  - Varianty Source, Destination

Děkuji za pozornost.