Základní principy obrany sítě II.

Michal Kostěnec
CESNET, z. s. p. o.

Bezpečnost prakticky

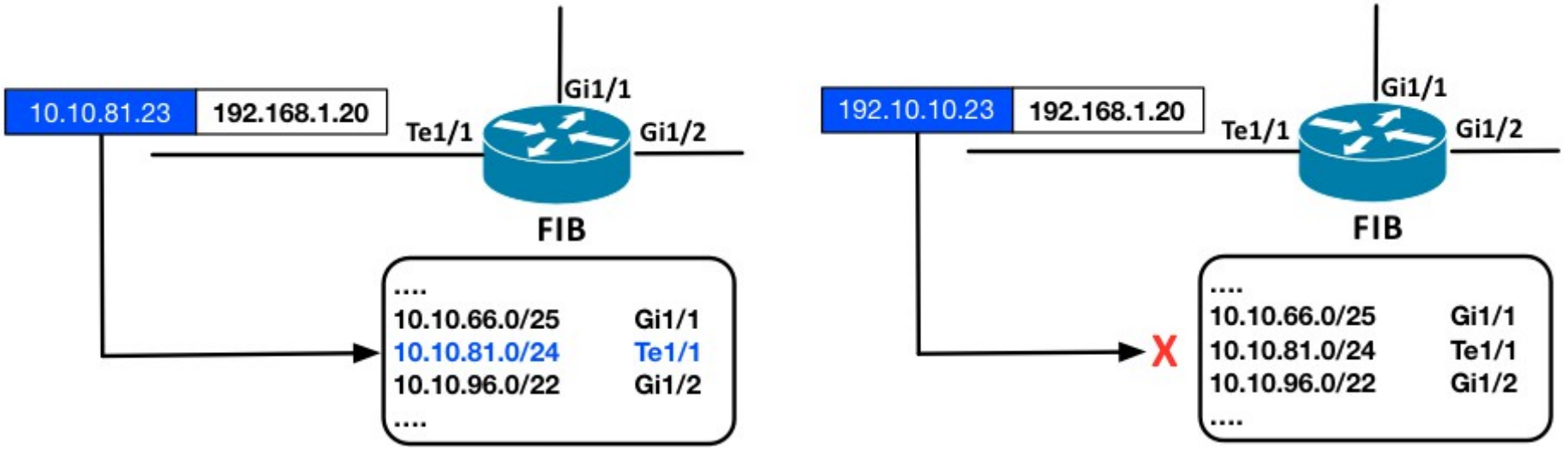
- uRPF
  - Kontrola správnosti zdrojových adres
- RTBH směrování
  - Efektivní blokování zdrojových/cílových IP adres/rozsahů
- Anycast DNS
  - Zvýšení dostupnosti DNS služeb
- Honeypot snadno a rychle
  - SSH honeypot Kippo
- Aktualizujte!
  - Windows, Java

uRPF

- Unicast Reverse Path Forwarding
  - Prevence proti DoS útoku
  - Testování správnosti zdrojové IP adresy
  - Zamezení podvržení zdrojové IP
    - IPv4
    - IPv6 – Cisco Sup720 v SW, Sup2T v HW
  - Odfiltrováno před dalším směrováním
  - Rychlé, testuje se v HW

uRPF - Princip

- Prohledává se Forward Information Base (FIB)
  - Obsahuje = Cílovou síť + „Next-hop“



uRPF princip

- 2 módy
  - Strict – Existuje cesta ke zdrojové adrese a je přes stejné rozhraní jako příchozí paket?
  - Loose – Existuje cesta ke zdrojové adrese?
- „Null“ rozhraní
  - Obdoba /dev/null v Linuxu
  - RFP = nevyhovuje podmínce
  - ip route 10.0.0.0 255.0.0.0 Null0

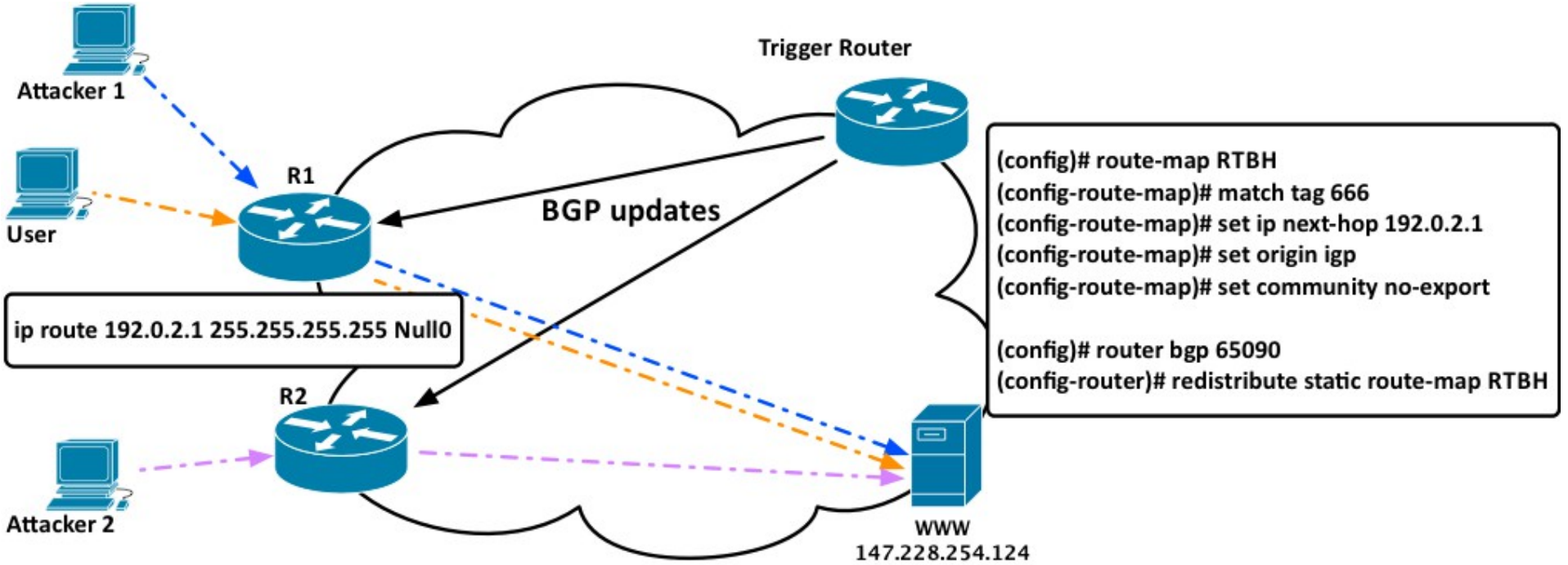
uRPF konfigurace

- Cisco
  - interface Gi1/1
    ip verify unicast source reachable-via {rx | any}
    [allow-default] [list]
  - Rx – „strict“ mód
  - Any – „loose“ mód
  - Allow-default – Bere v potaz „defaultní“ cestu
  - List – ACL s povolených seznamem IP
    - Lze využít pro logování, ale bude SW zpracováván

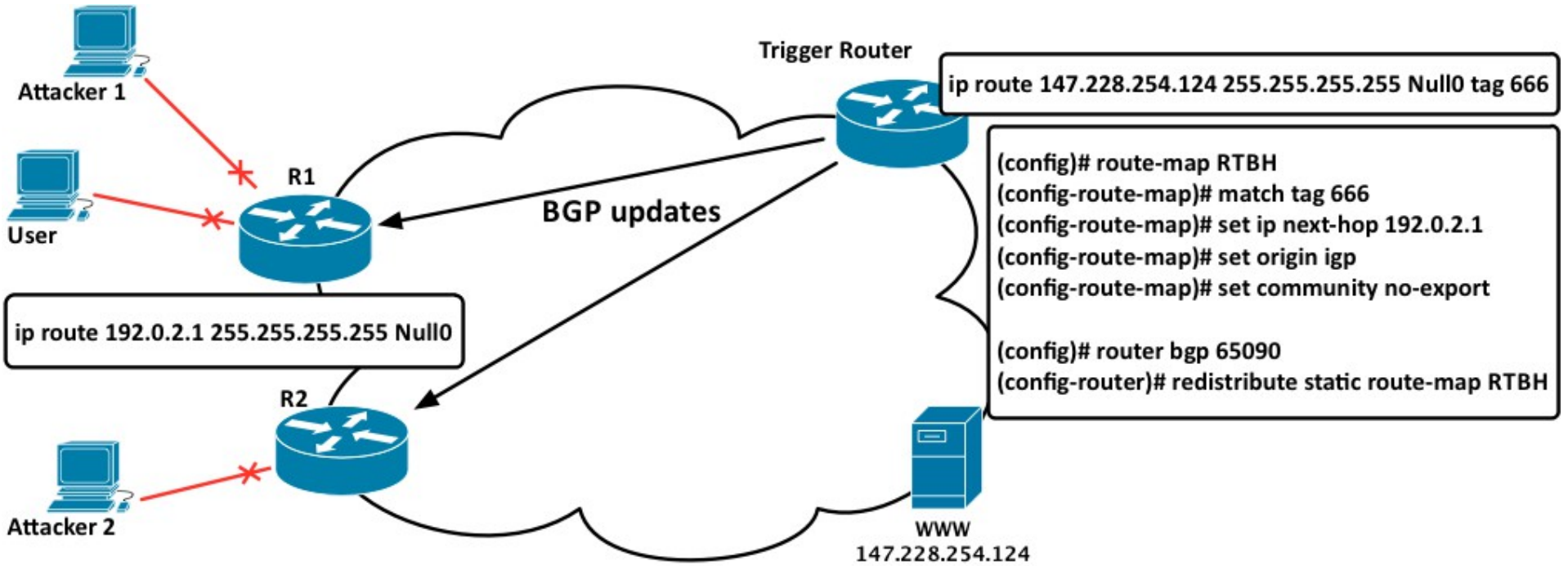
RTBH filtrování

- Remote Triggered Black Hole
- RFC 5635
- Filtrování dle cílové adresy
- Vhodné pro sítě s více směrovači
  - Založeno na BGP a redistribuci cest
    - „Pravidlo“ vloženo pouze na jeden prvek
  - Stejného výsledku lze dosáhnout pomocí ACL
    - Složité u velkého množství směrovačů
  - Lze automatizovat
  - Lze použít open-source nástroje pro směrování
    - Quagga, Bird, ...

Příprava prostředí

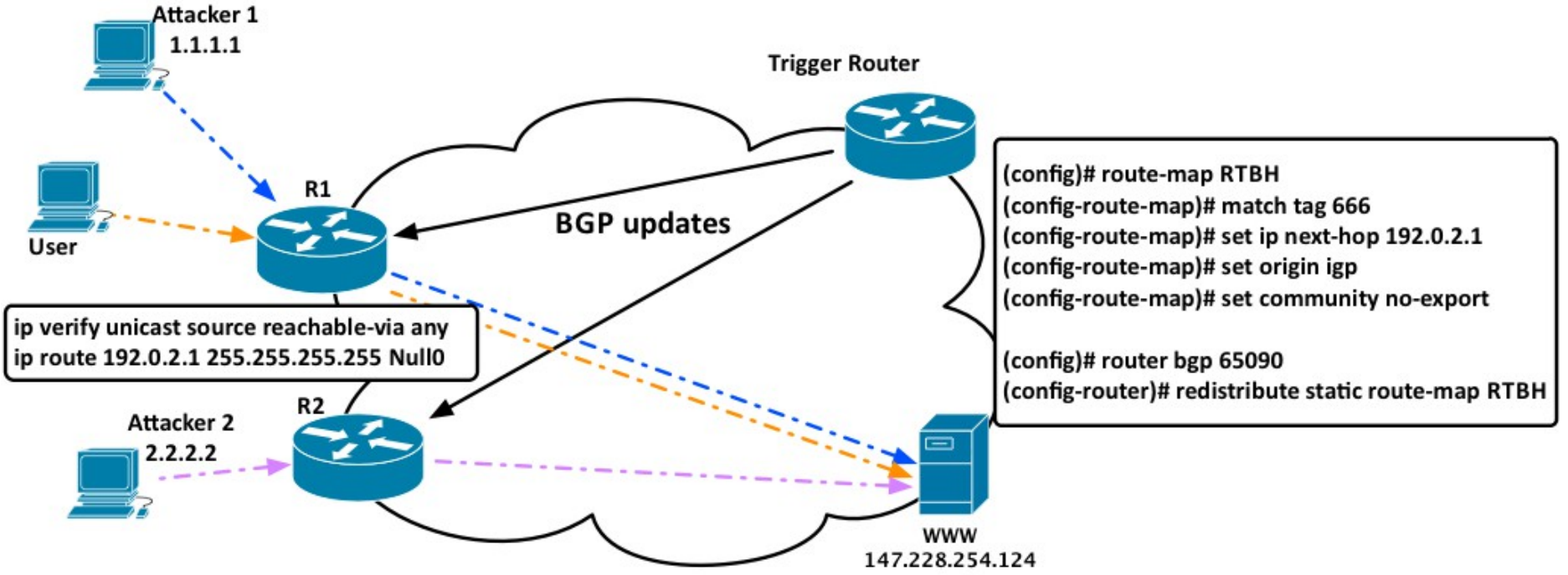


Filtrování dle cíle

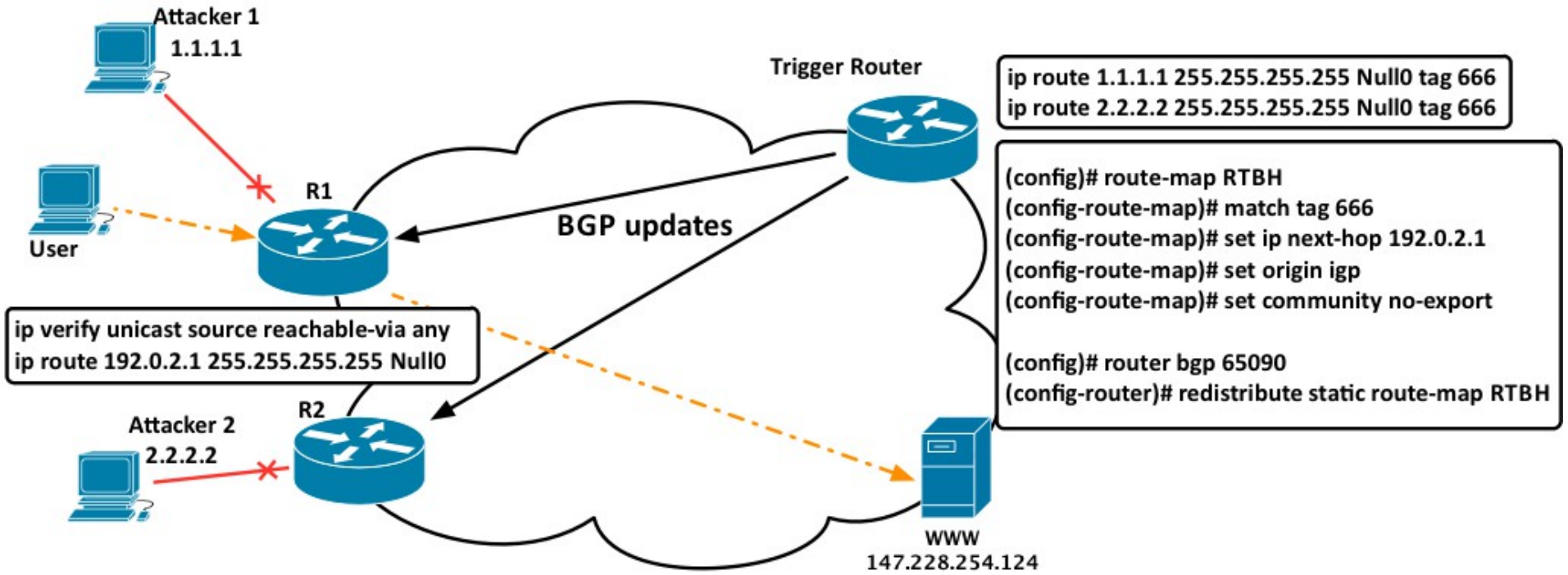


Příprava prostředí

- Bylo by vhodné blokovat i podle zdrojových IP
  - Stejný scénář + uRPF „loose“ mód



Filtrování dle zdrojové IP



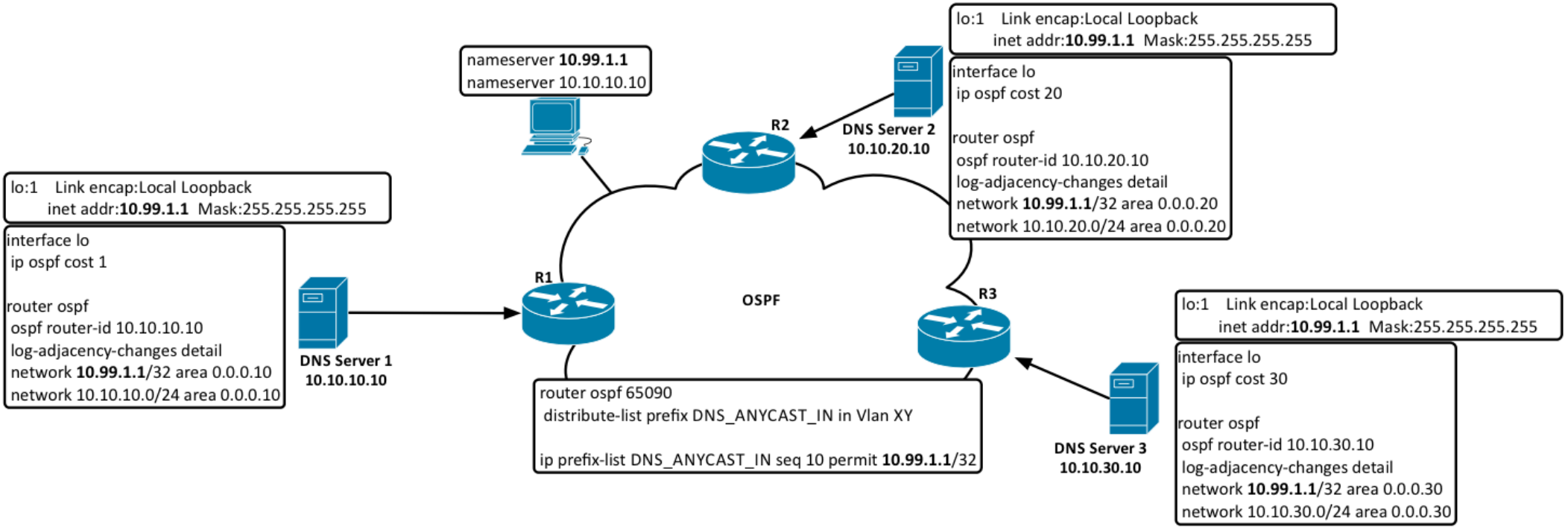
Anycast DNS

- Motivace
  - Jednoduchá konfigurace klientů – jedna položka
  - Rozložení zátěže
  - OS hůře pracují se sekundárním DNS
  - Odolnost proti DoS
- Spojení s dynamickým směrováním
  - Quagga, Bird
- Ověřené řešení
  - Kořenové DNS servery
  - 13 serverů (A-M), 10 anycastem ~ 300 reálných

Anycast DNS


Kalaallit Nunaat (Greenland)
Ísland (Iceland)
Россия (Russia)
Canada
Қазақстан (Kazakhstan)
Монгол Улс (Mongolia)
中国 (China)
North Pacific Ocean
North Atlantic Ocean
México (Mexico)
Venezuela
Perú (Peru)
Bolivia
Argentina
Brasil (Brazil)
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Niger
Tchad (Chad)
Nigeria
DR Congo
Tanzania
Angola
Namibia
Botswana
South Africa
Madagasikara (Madagascar)
Indonesia
Australia
New Zealand
Papua New Guinea

Anycast DNS prakticky



Anycast prakticky

- Testovací skripty
  - Pokud nejede „Bind“ démon, tak shodíme OSPF démona
- Podle priority OSPF lze definovat preferenci serverů
- Zabezpečení OSPF komunikace
- Zlepšení konvergence nastavením OSPF „timeoutů“
  - „Hello“, „Dead“
- Pomocí Netflow lze zjistit, kdo stále nepoužívá anycastovou adresu

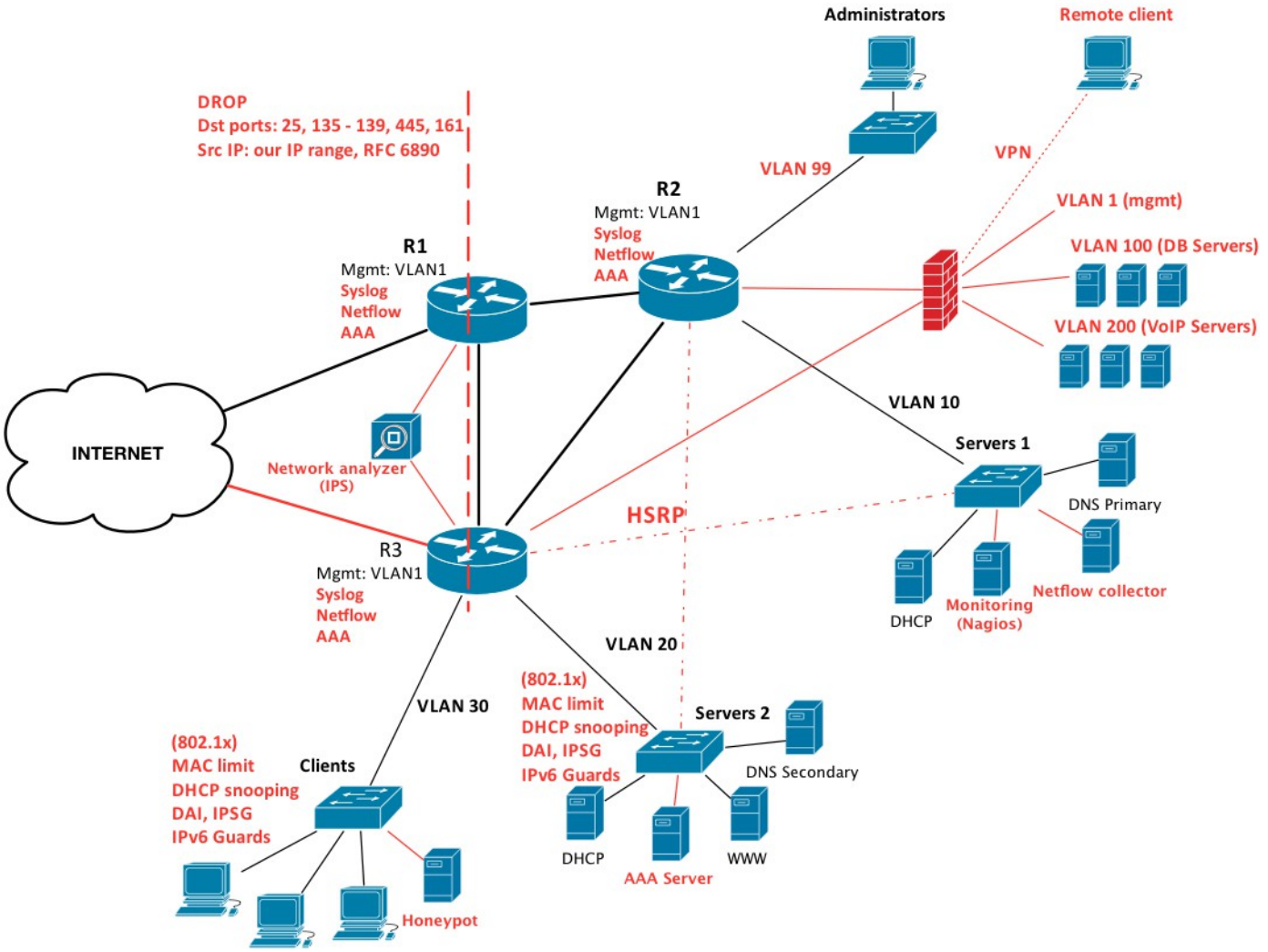
Kippo

- SSH honeypot se střední mírou interakce
- Jednoduchá instalace
  - Python
  - MySQL databáze
  - Výborný HP pro začátek
- Loguje útoky hrubou silou
- Virtuální prostředí
- Zaznamenává kompletní spojení (session)
  - Po odhlášení neodhlásí :-)

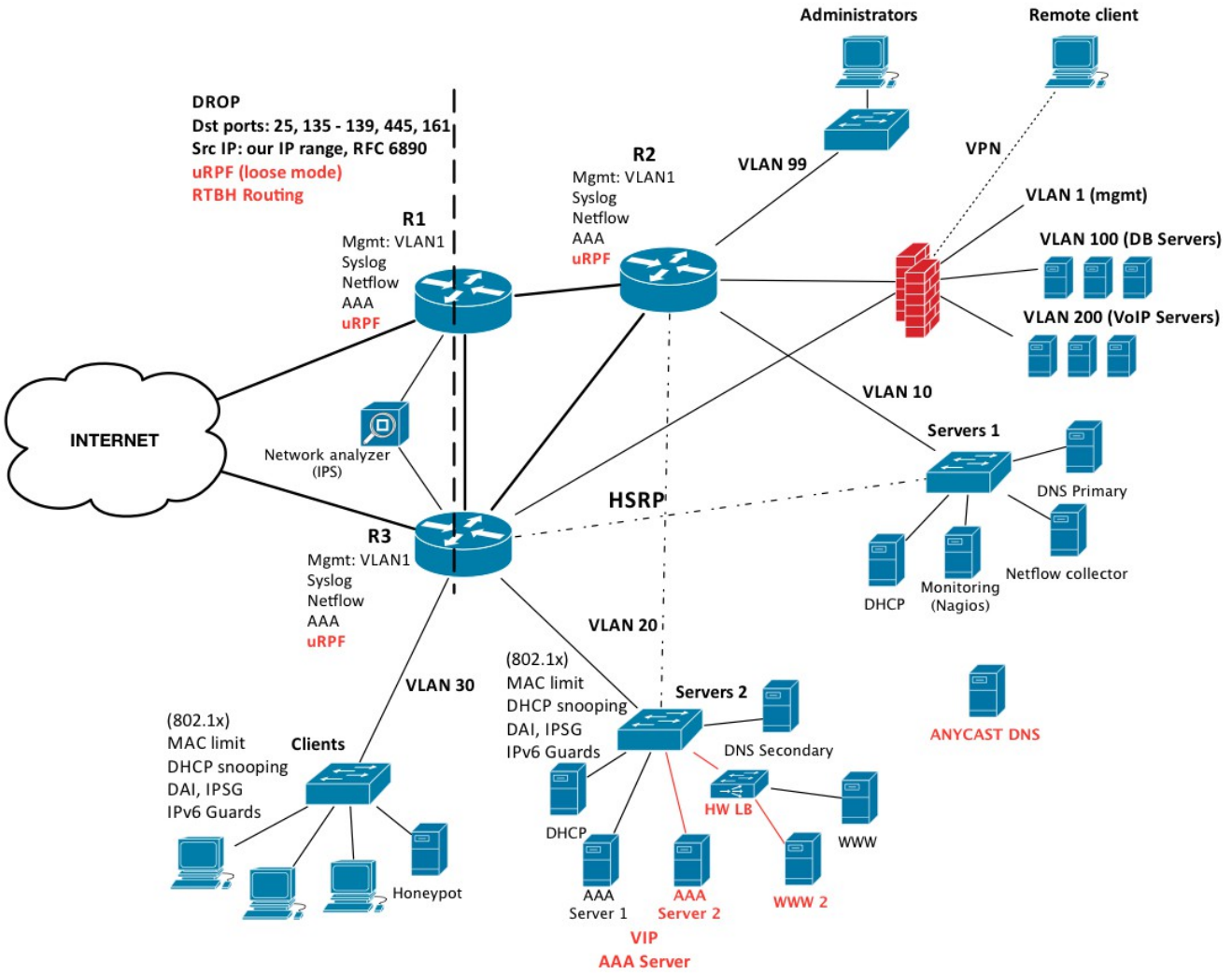
Kippo uvnitř

- Vizuální kopie Debianu
  - Útočník má pocit přítomnosti v reálném systému
    - Může spouštět systémové příkazy
  - Lze stahovat soubory (lze je zobrazit)
  - „Pingnout“ IP adresy
- Systémové příkazy
  - Předdefinované
    - Pouze výpis statického souboru (ifconfig, dmesg)
  - Dynamické
    - Statická část + dynamická (ping, ssh, wget)
    - Python moduly

Původní vylepšená síť



Další vylepšení



Aktualizujte!

- Aktualizace vylepší funkčnost systému
- Aktualizace nejsou jen pro zlepšení uživatelova pohodlí, ale pro odstranění zranitelností
- Pokud je chyba v aplikaci, tak ani dobrý FW nepomůže

- Aktualizujte.

Forenzní laboratoř

- Zjištění vektoru útoku (šíření malware)
- Prokázání porušování směrnic a provozních řádů uživatelem
- Monitoring nakládání se specifikovanými dokumenty
- https://csirt.cesnet.cz/FLAB/

Děkuji za pozornost.