PROJEKT FENIX

Petr Jiran – NIX.CZ

EurOpen.CZ – VZ Měřín
20151005

NIX·CZ

IXP NIX.CZ v číslech

- Založen 1996
- 5x PoP v Praze
- 134 připojených ASN
- 215 připojených portů – 5x 100GE
- 1773 Gb/s připojené kapacity
- 360 Gb/s max. datový tok
- 7 .TLD operátorů
- L2 topologie – virtualizovaná dvojitá hvězda
- Veřejný peering, Privátní VLAN, .TLD housing, Partner Program a Fenix projekt
- Člen Euro-IX, RIPE a projektu Atlas

IXP NIX.SK v číslech

- Založen 2015 – převzetí SitelIX
- 2x PoP v Bratislavě
- 23 připojených ASN
- 27 připojených portů
- 144 Gb/s připojené kapacity
- 4.5 Gb/s max. datový tok
- 1 .TLD operátor
- L2 topologie
- Veřejný peering, Privátní VLAN, Multicast VLAN, .TLD housing

Vznik projektu FENIX

- Odpověď na DDoS útoky z 3/2013 trvající 4 dny
- Útoky zasáhly mnoho cílů v CZ – média, banky, ISP, CDN
- Zdroje útoků byly mimo CZ
- Útoky přicházely jak přes tranzitní ISP, tak přes NIX.CZ
- Žádná odpověď od ISP kde byly zdroje útoků

FENIX

NIX·CZ

Projekt FENIX

- Združení vzájemně si “důvěřujících” sítí
- CZ uživatelé se potřebují dostat na CZ zdroje
  – Internet banking, média, e-mail . . .
- Možnost fungování v ostrovním režimu
  - řešení poslední možnosti
- Dříve než přijde regulace
- Vysoká kritéria pro vstup

FENIX

NIX·CZ

FENIX - organizační pravidla

- Převedení pravidel až na koncového uživatele
  - SPAM, útoky, atd.
- 24x7 technický kontakt bez IVR
- CSIRT team – vedený v Trusted introducer, Terena
- Aktivní účast v NIX.CZ
- Doporučení od dvou členů – žádné veto

FENIX

NIX·CZ

FENIX – technická pravidla

- BCP-38/SAC004 – granularita IPv4 /24 a IPv6 /48
- RTBH využívající RS
- IPv6, DNSSEC – na důležitých doménách
- Plná redundance připojení do NIX.CZ
- Monitoring sítě (MRTG, NetFlow, ...)
- Control plane policy RFC6192
- DNS, NTP, SNMP amplification protection
- Reakční čas na bezpečnostní incident <30min.
- BGP – TCP MD5 zabezpečení

FENIX

NIX·CZ

FENIX - začátek

- 6 společností zakládá projekt
  - Active24, CESNET, CZ.NIC, Dial Telecom, Seznam.cz, Telefonica Czech Republic
- NIX.CZ funguje jako arbitr dodržování pravidel
- Spolupráce s CSIRT.CZ

FENIX

NIX·CZ

FENIX – členové v CZ

FENIX

NIX·CZ

FENIX - pokračování

- 6 kandidátů na vstup
- Prezentace projketu v zahraničí
- Zahájení diskuzí na Slovensku
- Spolupráce na technických standardech

FENIX

NIX·CZ

FENIX - SK

- Memorandum s CSIRT.SK
- Start diskuze s ISP
- Definice pravidel pro SK
- Červen – první NIX.SK WG
- Říjen – druhá NIX.SK WG

FENIX

NIX·CZ

FENIX – podobné projekty

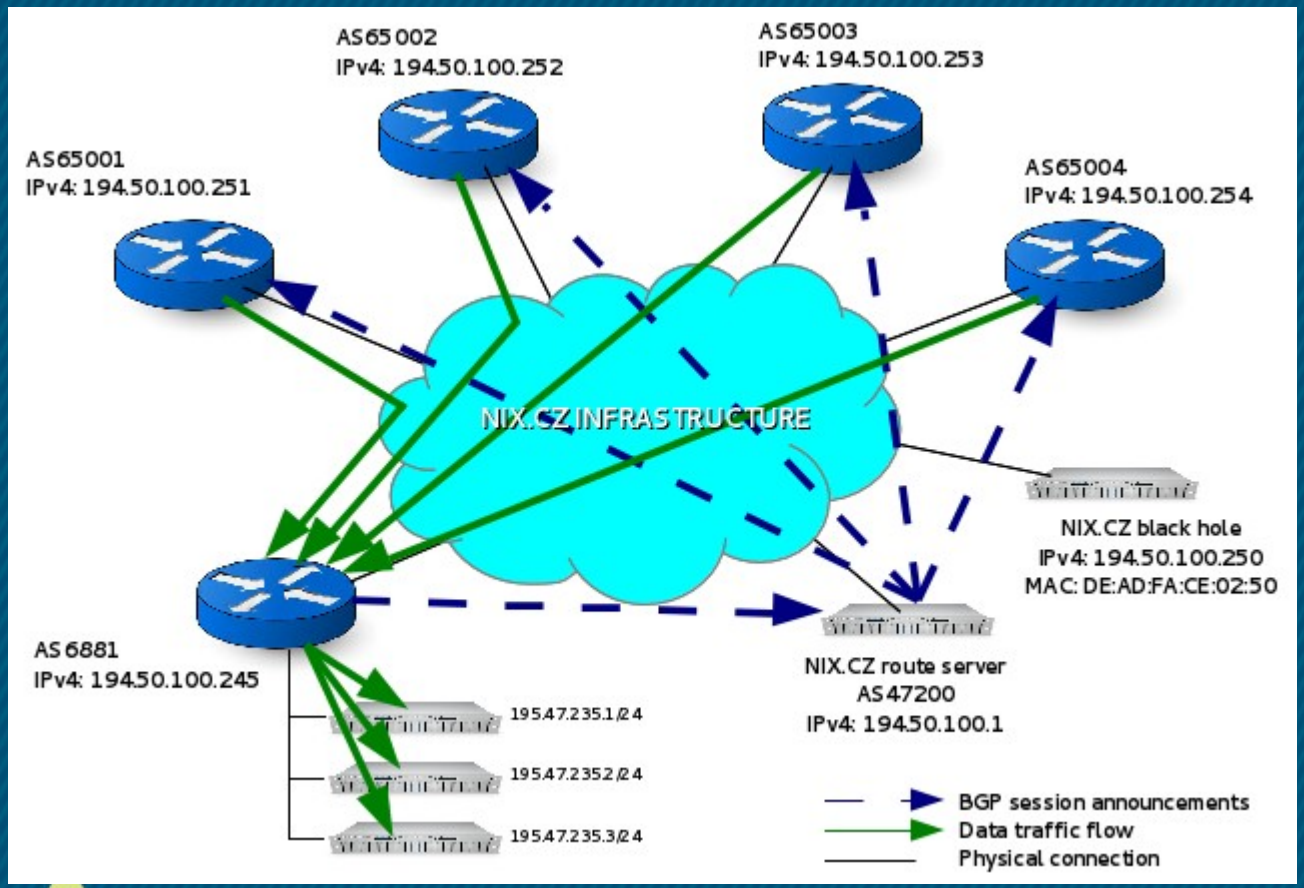
- **Trusted networks initiative**
  - www.tn-init.nl
- **Routing manifesto**
  - www.routingmanifesto.org

FENIX

NIX·CZ

FENIX – RS peering

- **Jak funguje peering s route servery**



FENIX

NIX·CZ

Co je RTBH?

- RTBH = Remotely Triggered Black Hole filtering
- RTBH v praxi znamená, přesměrování toku dat na jiný next-hop (black hole), kde je zahozen
- Výsledkem je, že provoz směrovaný na původní cíl ho nedosáhne a tím jsou prefixy těchto hostitelů chráněny
- Takto rešený blackholing je účinný způsob, jak zmírnit dopady Distributed Denial of Service (DDoS) útoků, atd.

FENIX

NIX·CZ

RTBH @ FENIX – Jak to funguje?

- Tuto službu poskytují route servery (RS) NIX.CZ secrs1.nix.cz a secrs2.nix.cz pro IPv4 a IPv6 prefixy
- V případě útoku, může ISP propagovat své prefixy se speciální BGP black hole komunitou směrem k RS
- Když RS dostane tuto speciálni BGP komunitu, automaticky tomuto prefixu změní next-hop IP na black hole IP
- Black hole next-hop (BN) má unikátní MAC adresu
- Všechny rámce s cílovou BN MAC adresou jsou filtrovány pomocí L2 ACL na vstupních portech NIX.CZ infrastruktury
- V tomto případě je veškerý provoz směrovaný na black hole prefixy zahozen dříve, než zasáhne vlastní zdroje napadeného ISP

FENIX

NIX·CZ

RTBH @ FENIX - podmínky

- secrs1.nix.cz = 194.50.100.1 / 2001:7F8:14:5EC::11
- secrs2.nix.cz = 194.50.100.2 / 2001:7F8:14:5EC::12
- RS provádí standardní bezpečnostní kontroly jednotlivých ISP prefixů
- ISP musí akceptovat délku prefixů <=/32 IPv4 a <=/128 IPv6
- Black hole MAC adresa = DE:AD:FA:CE:02:50
- Black hole IPv4 adresa = 194.50.100.250
- Black hole IPv6 adresa = 2001:7F8:14:5EC::250
- Black hole komunita = 65511:<ASN>
- Black hole extended komunita = rt:65511:<ASN>

FENIX

NIX·CZ

RTBH @ FENIX – RTBH komunity

Example	Include community(ies)
Change next-hop to all RS clients	65511:47200
Change next-hop to RS clients A, B, C ASNs, to other clients send normal next-hop	65511:A 65511:B 65511:C
Change next-hop to RS clients A, B, C ASNs only, do not send this prefix to other RS clients	65511:A 65511:B 65511:C 0:47200

Example	Include ext. community(ies)
Change next-hop to all RS clients	rt:65511:47200
Change next-hop to RS clients A, B, C ASNs, to other clients send normal next-hop	rt:65511:A rt:65511:B rt:65511:C
Change next-hop to RS clients A, B, C ASNs only, do not send this prefix to other RS clients	rt:65511:A rt:65511:B rt:65511:C rt:0:47200

FENIX

NIX·CZ

RTBH @ FENIX – standardizace

- RTBH BGP komunity nejsou nijak standardizované
- Každý ISP a IXP používá jiné tvary RTBH BGP komunit
- Snaha o standardizaci tzv. well-known BGP community [RFC1997]
- Spolupráce na RFC se světovými IXP, ISP a výrobci (DE-CIX, NTT, Alcatel-Lucent) při IETF.
- IETF Internet-Draft: BLACKHOLE BGP Community for Blackholing draft-ymbk-grow-blackholing-01

  https://tools.ietf.org/html/draft-ymbk-grow-blackholing-01

FENIX

NIX·CZ

RTBH @ FENIX – příklad DDoS

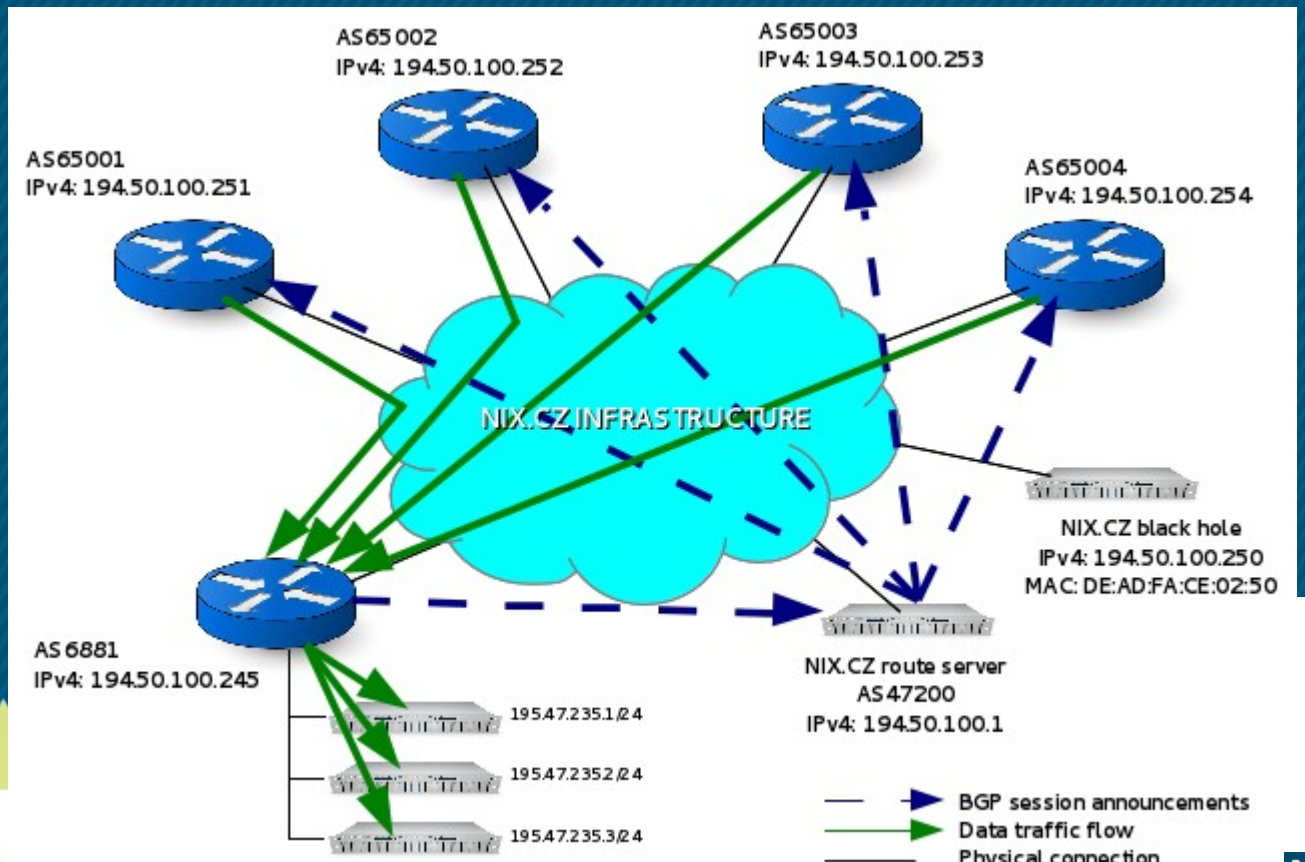
1. Standardní situace

→ AS6881 propaguje pfx. 195.47.235.0/24 směrem k RS bez BGP komunit.

→ RS propaguje tento pfx. všem klientům → prefix je přijímán/akceptován a zvolen jako best-path.

→ Odpovídající next-hop IP (194.50.100.245) a MAC jsou naučeny pomocí ARP.

→ Zákaznický provoz teče přes NIX.CZ infrastrukturu do AS6881.



FENIX

NIX·CZ

RTBH @ FENIX – příklad DDoS

2. DDoS útok

→ AS65001-3 jsou zdroje zákeřného (“dirty”) provozu útočícího na server 195.47.235.1 v AS6881

→ AS65004 je zdroj norlmálního (“clean”) provozu proudícího na server 195.47.235.1 v AS6881

→ Server 195.47.235.1 je přetížen
→ jeho služby jsou nedostupné pro všechny klienty

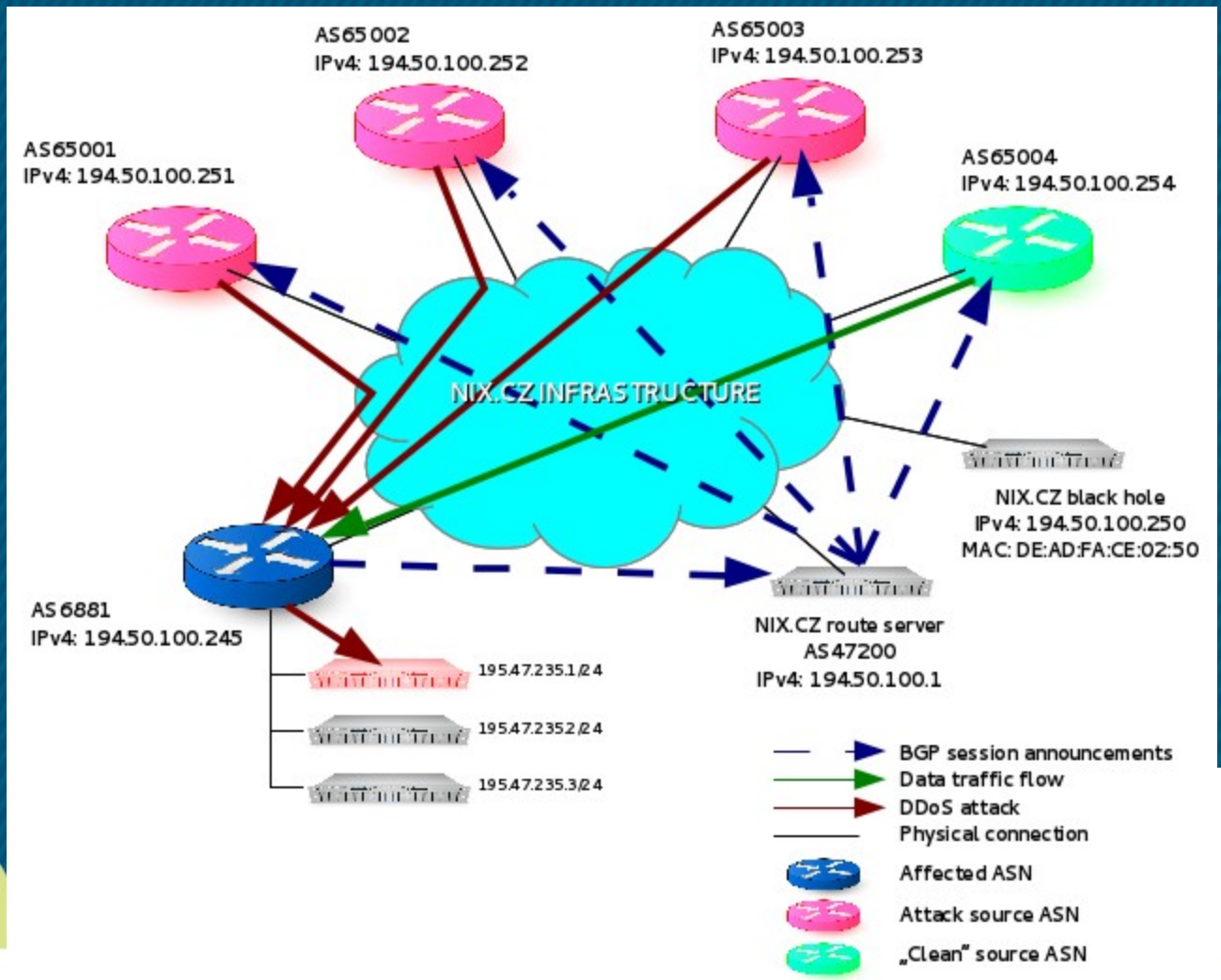
→ Ostatní IP AS6881 mohou být tímto útokem postiženy také
→ zahlcení portů, přetížení CPU routeru, “flapování” BGP relací, atd.

FENIX

NIX·CZ

RTBH @ FENIX – příklad DDoS

2. DDoS útok



FENIX

NIX·CZ

RTBH @ FENIX – příklad DDoS

3. Obrana proti DDoS útoku

→ AS6881 začne propagovat pfx. 195.47.235.1/32 s BGP komunitou 65511:65001 65511:65002 65511:65003 směrem k RS

→ RS přijme tuto komunitu a změní next-hop pro tento pfx. 195.47.235.1/32 na black hole IP (194.50.100.250) pouze pro klienty AS65001-3

→ AS65001-3 přijmou/akceptují a zvolí prefix 195.47.235.1/32 jako best-path

→ AS65001-3 se naučí odpovídající black hole next-hop IP a MAC via ARP

→ AS65001-3 začnou směrovat svůj provoz na black hole IP (194.50.100.250)

→ Provoz směrovaný na cílovou black hole MAC je pomocí vstupního L2 ACL zahozen již na vstupu do infrastruktury NIX.CZ

→ AS65004 posílá “čistý” provoz na 195.47.235.1 bez problémů, jelikož RS nezměnil tomuto klientovi next-hop

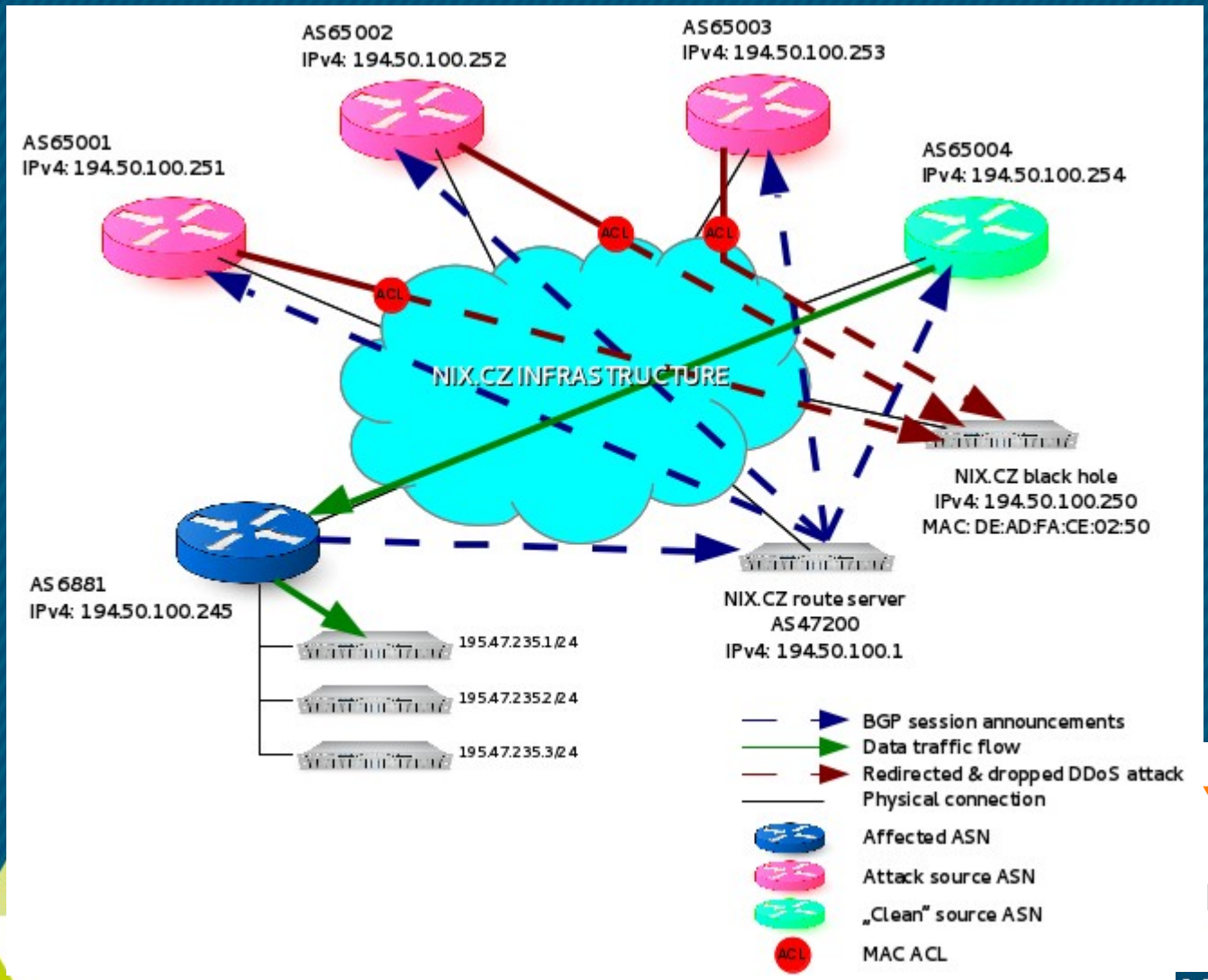
→ Veškerý provoz + DDoS z AS65001-3 na IP 195.47.235.1 je zahozen před tím, než dosáhne AS6881

FENIX

NIX·CZ

RTBH @ FENIX – příklad DDoS

3. Obrana proti DDoS útoku



FENIX

NIX·CZ

RTBH @ FENIX – příklad DDoS

3. Obrana proti DDoS útoku – příkladová konfigurace peeringu

(Cisco – IPv4)

```
!
ip prefix-list RTBH seq 5 permit <blackholed prefix/32>
!
router bgp <your ASN>
no bgp enforce-first-as
neighbor <RS> remote-as <NIX.CZ RS ASN>
!
address-family ipv4
network <blackholed prefix/32>
neighbor <RS> route-map RTBH-MAP out
exit-address-family
!
route-map RTBH-MAP permit 10
match ip address prefix-list RTBH
set community 65511:65001 65511:65002 65511:65003
!
```

FENIX

NIX·CZ

¿ DOTAZY ?

www.nix.cz
pj@nix.cz

NIX·CZ