

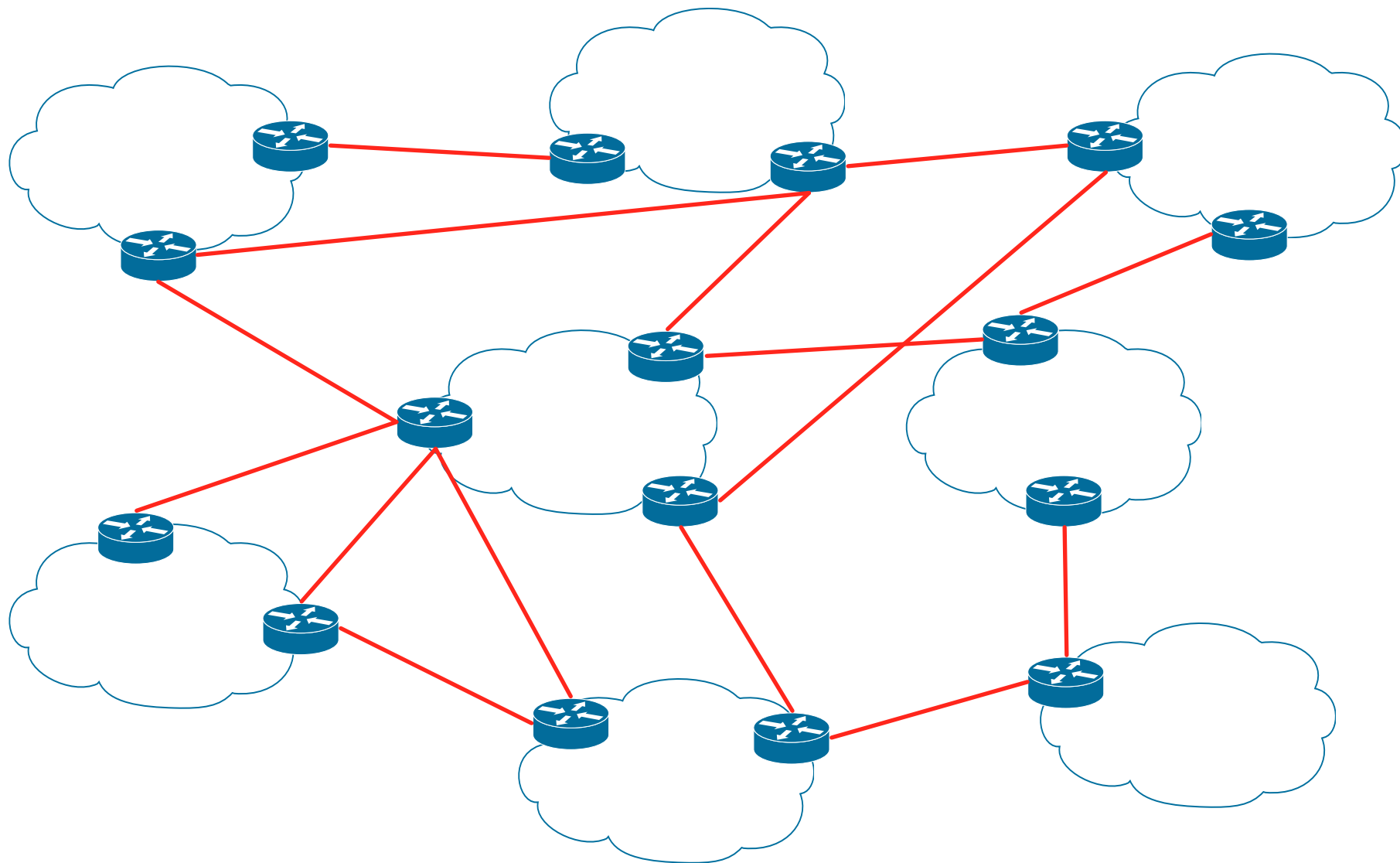


The world's most secure IXP

Internetworking security

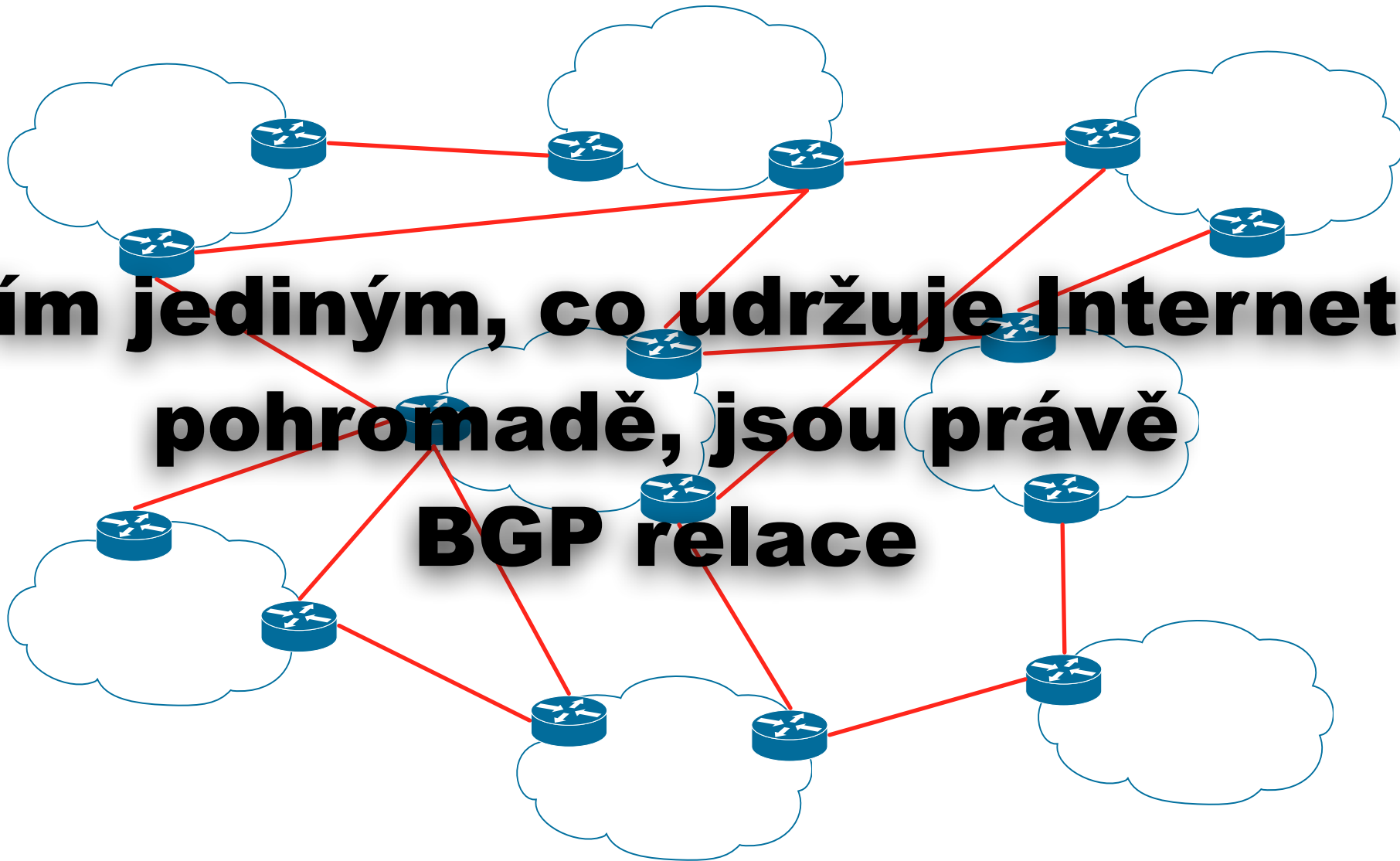
Zbyněk Pospíchal, 9/2017

Zabezpečení BGP relací



Zabezpečení BGP relací

**Tím jediným, co udržuje Internet
pohromadě, jsou právě
BGP relace**



Zabezpečení BGP relací

Ideální cílový stav: Rychle reagující relace (nezávisle na fyzickém médiu), zabezpečené proti spoofingu, zabezpečené proti utlučení CoP MD5 DoS útokem, zabezpečené proti route-hijackingu, proti podvržení cesty a s možností oznamování filtrovacích pravidel (ochrana před DDoS)



Čekáme na RFC a na implementaci (BGPSEC, Inter-AS FS, uRPFv3)



V zásadě umíme, vyžaduje širší deployment, mnohde nepodporováno (RPKI)



Umíme už teď, už málo systémů nepodporuje, relativně málo chyb v implementacích (BFD, GTSM)

Zabezpečení BGP relací

Ideální cílový stav: Rychle reagující relace (nezávisle na fyzickém médiu), zabezpečené proti spoofingu, zabezpečené proti utlučení CoP MD5 DoS útokem, zabezpečené proti route-hijackingu, proti podvržení cesty a s možností oznamování filtrovacích pravidel (ochrana před DDoS)



Čekáme na RFC a na implementaci (BGPSEC, Inter-AS FS, uRPFv3)

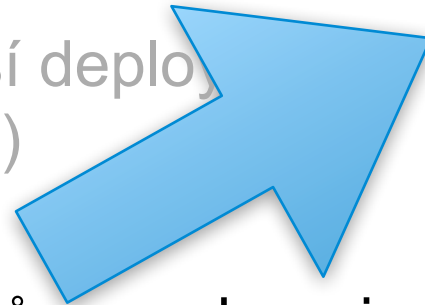


V zásadě umíme, vyžaduje širší deploy, mnohde nepodporováno (RPKI)

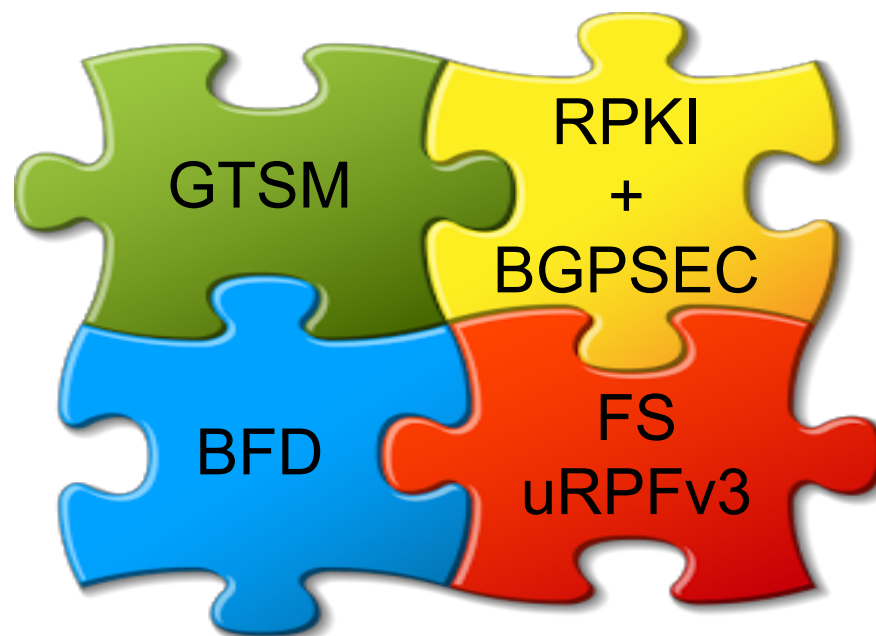


Umíme už teď, už málo systémů nepodporuje, relativně málo chyb v implementacích (BFD, GTSM)

Lze udělat
HNED!



Následně už budeme jen "doplňovat puzzle"...



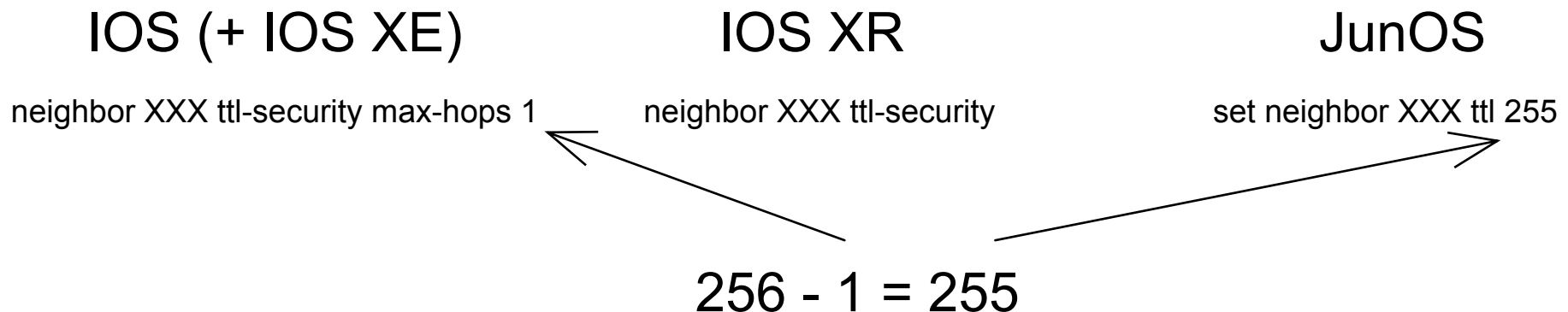
GTSM

Generalized TTL Security Mechanism

RFC 5082

router v BGP relaci přijme jen packety se stanoveným TTL

-> jsou zahozeny všechny packety z cizích zdrojů ještě před tím, než zatíží CoP CPU počítáním MD5 hashe



Zkušnosti: (skoro) všude funguje, problémy s platformou Arista

BFD

Bidirectional Forwarding Detection

RFC 5880 - 5884

protokol zajišťující rychlou detekci a konvergenci
v případě výpadků
není závislý na konkrétním protokolu, umí hlídat
kupříkladu i statické routy

IOS (+ IOS XE)

```
(interface)
bfd interval X multiplier Y
(router-bgp xyz)
neighbor XXX fall-over bfd (single-hop)
```

IOS XR

```
(router bgp xyz)
bfd interval X
bfd multiplier Y
neighbor XXX bfd fast-detect
```

JunOS

```
(edit protocols bgp group CCC)
set neighbor XXX bfd-liveness-detection
minimum-interval X
multiplier Y
```

BFD

Bidirectional Forwarding Detection

Praktické zkušenosti: o něco více problémů než u GTSM

Hardwarové problémy:

malý výkon CPU a málo jader na starších generacích routerů (typicky Cat6500/Cat6800/C7600), absence distribuce BFD do linecards

Softwarové problémy:

IOS XR 5.x.x se nespojí proti jinému IOS XR 5.x.x

BFD: Funguje to?

Po ~3/4 roce se stále zdá, že ano

NIX.CZ: 2x 21 IPv4 relací, 2x 20 IPv6 relací

NIX.SK: 1 IPv4 relace, 1 IPv6 relace

SIX.SK: 2 IPv4 relace, 3 IPv6 relace

```
RP/0/RSP0/CPU0:ASBR1-SITEL#sh bfd all session | i 91.210 | i UP
Thu May 31 12:12:57.319 CET
BE7.10      91.210.16.45      0s(0s*0)      5s(1s*5)      UP
BE7.10      91.210.16.46      0s(0s*0)      5s(1s*5)      UP
BE7.10      91.210.16.166     0s(0s*0)      1500ms(500ms*3) UP
BE7.10      91.210.16.230     0s(0s*0)      1665ms(333ms*5) UP
BE7.10      91.210.16.42      0s(0s*0)      5s(1s*5)      UP
BE7.10      91.210.16.60      0s(0s*0)      999ms(333ms*3) UP
BE7.10      91.210.16.93      0s(0s*0)      999ms(333ms*3) UP
BE7.10      91.210.16.152     0s(0s*0)      5s(1s*5)      UP
BE7.10      91.210.16.41      0s(0s*0)      5s(1s*5)      UP
BE7.10      91.210.16.73      0s(0s*0)      5s(1s*5)      UP
BE7.10      91.210.16.74      0s(0s*0)      5s(1s*5)      UP
BE7.10      91.210.16.77      0s(0s*0)      999ms(333ms*3) UP
BE7.10      91.210.16.78      0s(0s*0)      2250ms(750ms*3) UP
BE7.10      91.210.16.87      0s(0s*0)      5s(1s*5)      UP
BE7.10      91.210.16.88      0s(0s*0)      5s(1s*5)      UP
BE7.10      91.210.16.151     0s(0s*0)      5s(1s*5)      UP
BE7.10      91.210.16.165     0s(0s*0)      1500ms(500ms*3) UP
BE7.10      91.210.16.174     0s(0s*0)      2500ms(500ms*5) UP
BE7.10      91.210.16.190     0s(0s*0)      1665ms(333ms*5) UP
BE7.10      91.210.16.191     0s(0s*0)      1665ms(333ms*5) UP
BE7.10      91.210.16.229     0s(0s*0)      1665ms(333ms*5) UP
```

uRPFv3

uRPF - unicast reverse path filtering

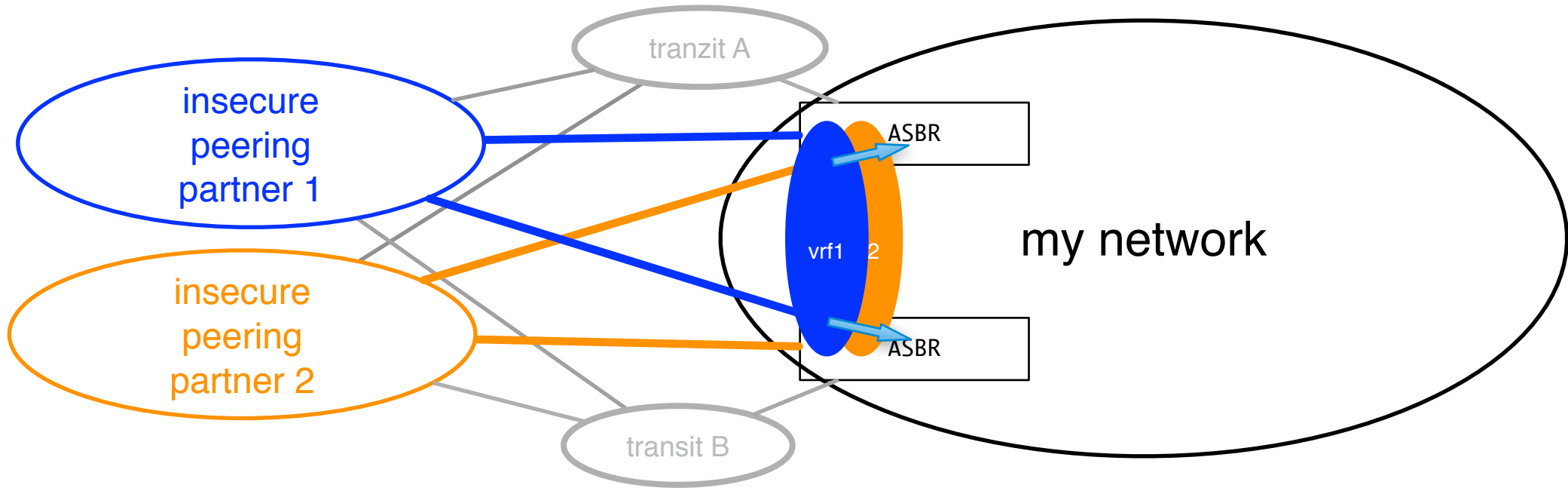
Nástroj pro filtrování příchozího spoofovaného provozu, popsán
v RFC 3704, BCP 38, BCP 84

Pro příchozí packet musí existovat odpovídající záznam ve FIB
(loose mode) - bohužel na boxu s plnou GRT nic moc neřeší

tento záznam navíc musí směřovat na příslušný interface
(strict mode) - použitelně funguje jen proti single-homed zákazníkům,
při použití ACL problémy se škálováním a debugem

uRPFv3

"uRPFv3" alias "uRPF vrf mode"



Routy ze specifické BGP relace se nejprve nasypou do speciální VRF, z níž se pak exportují do GRT

Proti FIB této VRF se provádí loose mode RPF check

Teprve pokud tento check projde, packet propadne do GRT

uRPFv3

"uRPFv3" alias "uRPF vrf mode"

Špatné zprávy:

Vyvinuto, naimplementováno před dvanácti lety do Cisco IOS

Od té doby nic, v IOS XR ani v IOS XE to není, v road map to taky není, konkurence taky nic



Pojďme společně zatlačit na vendory.

BGP FlowSpec

Primární cíl: škálovatelný nástroj pro distribuci filtrovacích pravidel v rámci sítě a také mezi sítěmi

Využívá BGP jako nosný protokol
address-family ipv4 flowspec, ipv6 flowspec, vpnv4 flowspec atd.
NLRI AFI = 1, SAFI = 133/134

RFC 5575

BGP FlowSpec

Reálný stav

Primární cíl: škálovatelný nástroj pro distribuci filtrovacích pravidel
v rámci sítě a také mezi sítěmi

Využívá BGP jako nosný protokol
address-family ipv4 flowspec, ipv6 flowspec, vpnv4 flowspec atd.
NLRI AFI = 1, SAFI = 133/134

RFC 5575

hezké, ale má nedostatky

draft-ietf-idr-rfc5575bis

real-world implementace jen podle RFC 5575

FlowSpec: Definice flow

Destination prefix (/netmask)

Source prefix (/netmask)

Protokol (TCP=6, UDP=17)

TCP nebo UDP: Source AND/OR destination port

ICMP type

TCP flags

Délka packetu

DSCP

Fragment

FlowSpec: filtrovací úkony

(traffic filtering actions)

Rate

Redirect (do jiné vrf)

Redirect (na jiný next-hop) (*)

Change community (*)

Marking (*)

Není explicitně Drop (používá se Rate na rychlost 0 Kbps)

(*) postaveno jen na draftech, někde neimplementováno

Je to v podstatě routa. Až na to, že...

Záznam v tabulce vypadá poněkud nezvykle:

```
RP/0/RSP0/CPU0:ASBR4#show bgp ipv4 flowspec
```

RIB

```
...
```

```
Status codes: s suppressed, d damped, h history, * valid, > best  
               i - internal, r RIB-failure, S stale, N Nexthop-discard
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network          Next Hop          Metric LocPrf Weight Path
```

```
*>iDest:31.13.0.0/16,Source:215.24.132.66/32,Proto:=6,DPort:=80|443/152
```

```
0.0.0.0          100          0 ?
```

```
*>iDest:77.167.2.26/32,Source:131.237.225.38/32,Proto:=6,DPort:=80,TCPFlags:=0x04/168
```

```
0.0.0.0          100          0 ?
```

```
RP/0/RSP0/CPU0:ASBR4#show flowspec ipv4 detail
```

```
Mon Jun 12 12:13:00.455 CET
```

FIB

```
AFI: IPv4
```

```
Flow              :Dest:31.13.0.0/16,Source:215.24.132.66/32,Proto:=6,DPort:=80|443
```

```
Actions           :Traffic-rate: 0 bps (bgp.1)
```

```
Statistics        (packets/bytes)
```

```
Matched           : 58/4080
```

```
Dropped           : 58/4080
```

```
Flow              :Dest:77.167.2.26/32,Source:131.237.225.38/32,Proto:=6,DPort:=80,TCPFlags:=0x04
```

```
Actions           :Traffic-rate: 200000 bps (bgp.1)
```

```
Statistics        (packets/bytes)
```

```
Matched           : 0/0
```

```
Dropped           : 0/0
```

Příkazy



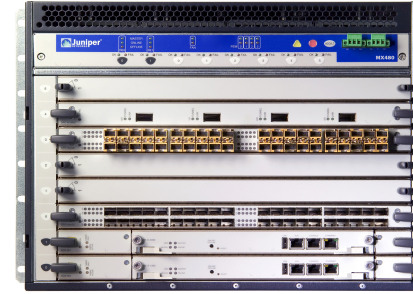
IOS XR:

show flowspec ipv4 detail

FIB

show bgp ipv4 flowspec

RIB



JunOS:

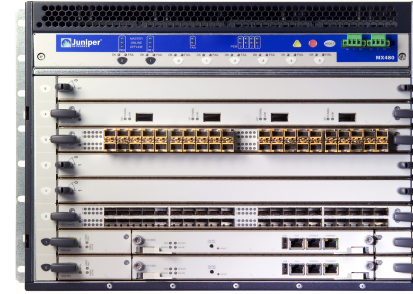
show policer
__flowspec_default_inet__

show firewall filter
__flowspec_default_inet__

show route table inetflow.0
extensive



Definice FS pravidel



IOS XR:

```
!  
class-map type traffic match-all cm1  
    match source-address ipv4 100.0.0.0/24  
    match ipv4 icmp-type 8  
!  
policy-map type pbr pm1  
    class type traffic cm1  
        drop  
!
```

JunOS:

```
[routing-options]  
flow {  
    term-order standard;  
    route block-100.0.0.0 {  
        match {  
            source 100.0.0.0/24;  
            protocol icmp;  
            icmp-type echo-request;  
        }  
        then discard;  
    }  
}
```

Definice FlowSpec pravidel

FlowSpec routa je narozdíl od rout v eBGP ~~netranzitivní~~
- platí do implementace draft-ietf-idr-rfc5575bis



nutno mít přímou BGP session s routery, na které
FS routy posíláme

(chová se tedy identicky jako iBGP)

Šedá je teorie, zelený strom života. Jak kde. Existují
errata k RFC 5575, která někteří vendori četli. Jiní ne.

FlowSpec v praxi

V intra-AS v odzkoušených scénářích funguje spolehlivě.

U neodzkoušených scénářů je nutná velká opatrnost (rozhodně se vyhnout všemu, na co je jen IETF draft)

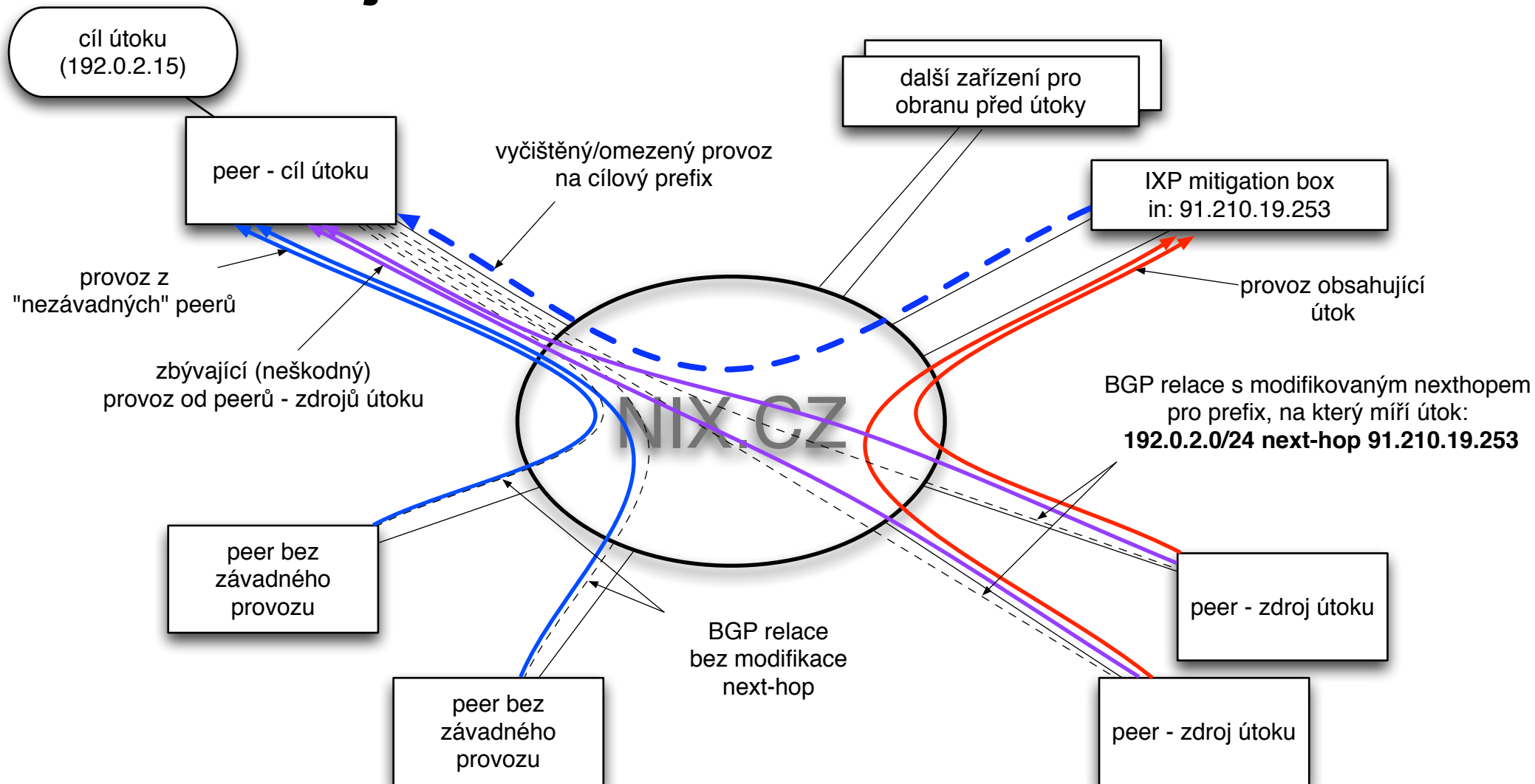
U inter-AS nasazení od 05/2017 žádný posun, zde bude zajímavé sledovat další vývoj.

Bezpečnostní projekty sdružení NIX.CZ

Projekt FENIX: společenství důvěryhodných sítí

The logo for SEZNAM.CZ, featuring a red stylized 'S' followed by the text 'EZNAM.CZ' in black.The logo for cz.nic, with 'cz.' in blue and 'nic' in a darker blue.The logo for Casablanca, with a blue square icon followed by the text 'Casablanca' and 'INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE' in smaller text below.The logo for O2, featuring the text 'O2' in a blue serif font.The logo for Dial Telecom, featuring a red circular icon with a white 'D' and the text 'Dial Telecom' in black.The logo for cesnet, with 'cesnet' in a grey sans-serif font and a series of blue dots below it.The logo for NIX.CZ, featuring a stylized 'X' made of blue and green triangles followed by the text 'NIX.CZ' in blue.The logo for ČD-Telematika, featuring a stylized 'D' with a red and blue swoosh and the text 'ČD-Telematika' in blue.The logo for COOL HOUSING.NET, featuring three blue dots above the text 'COOL HOUSING.NET' in a black sans-serif font.The logo for merit, featuring a green circular icon with two white dots and the text 'merit' in a black sans-serif font.The logo for WEB4U, featuring a blue 'E' icon followed by the text 'WEB4U' in a bold blue sans-serif font, with 'SERVERY HOSTING DOMÉNY' in smaller text below.The logo for ISP Alliance, featuring a stylized star icon and the text 'ISP Alliance networking together' in blue.The logo for kara, featuring the text 'kara' in a blue sans-serif font with a yellow smiley face replacing the 'a'.The logo for 2connect, featuring a blue circular icon with a white '2' and the text '2connect' in a blue sans-serif font.The logo for itself, featuring the text 'itself' in a green sans-serif font.The logo for CETIN, featuring a red triangle icon followed by the text 'CETIN' in a bold blue sans-serif font, with 'ČESKÁ TELEKOMUNICAČNÍ INFRASTRUKTURA' in smaller text below.The logo for TELCO PRO SERVICES, featuring a red square icon with a white 'E' and the text 'TELCO PRO SERVICES' in a red sans-serif font.The logo for T.., featuring a stylized 'T' in a purple sans-serif font followed by two dots.The logo for master data in motion, featuring a stylized 'm' icon and the text 'master data in motion' in a black sans-serif font.The logo for HOSTING, featuring a green square icon with a white 'H' and the text 'HOSTING' in a green sans-serif font.

Projekt TANK: Anti-DDoS řešení v IXP



Dotazy

