Jak zabezpečit BGP verze 2026
ASPA

Marian Rychtecký

21.05.2026

NIX·CZ

Proč? aneb historické milníky

- Pakistan Telecom vs. YouTube (2008) – omylem zahladili globálně YouTube.
- China Telecom (2010) – přesměrování velké části globálního provozu.
- Route leak Telia – Level3 (2017) – globální výpadky.
- Roskomnadzor (2022) – pokus o přesměrování provozu k Telegramu.

Proč? aneb nechoďme daleko

- Kolik incidentů (BGP hijack) postihnuvších CZ sítě se událo za posledních 12 měsíců? Tipy?

360

NIX·CZ

Proč? aneb nechoďme daleko

BGP origin hijacks

Recent potential BGP hijack originated by or affecting ASes registered in the Czech Republic

Detected origin	Expected origin(s)	Start time (UTC)	Duration	BGP messages	Prefixes	Confidence	Tags
AS57608 (PL)	AS5588 (CZ)	05/19/2026, 23:41	—	120 msgs (23 peers)	45.9.233.0/24...4 more	Low	IRR invalid, IRR old origin invalid
AS8648 (DE)	AS29134 (CZ)	05/19/2026, 11:54	—	72 msgs (20 peers)	37.46.80.0/24...5 more	High	RPKI invalid, IRR invalid, RPKI old origin invalid
AS63113 (CZ)	AS56898 (NL)	05/14/2026, 22:06	2 minutes	12 msgs (3 peers)	185.75.76.0/24...3 more	Medium	IRR invalid

Cloudflare Radar
https://radar.cloudflare.com/routing/anomalies/cz?dateRange=52w

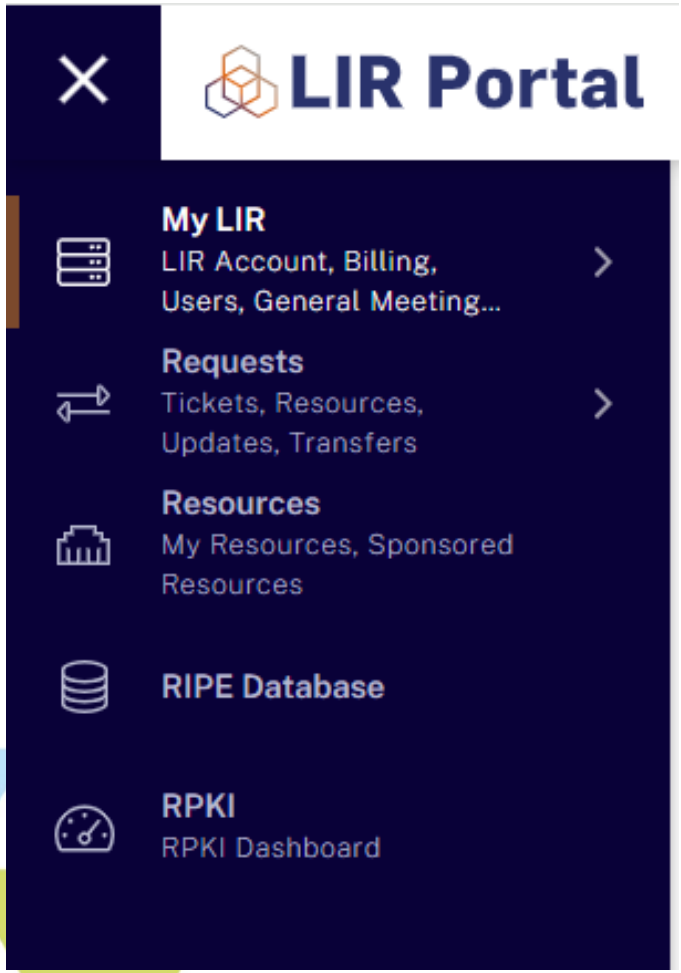
NIX·CZ

Jak? (se bránit) - vrstvy ochrany

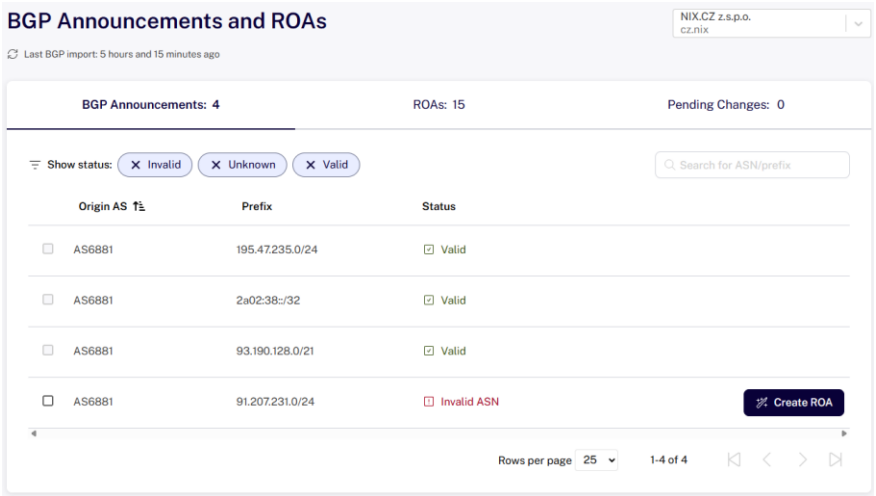
- RPKI
- ASPA
- BGP Roles (RFC 9234)

Jak? RPKI ROA

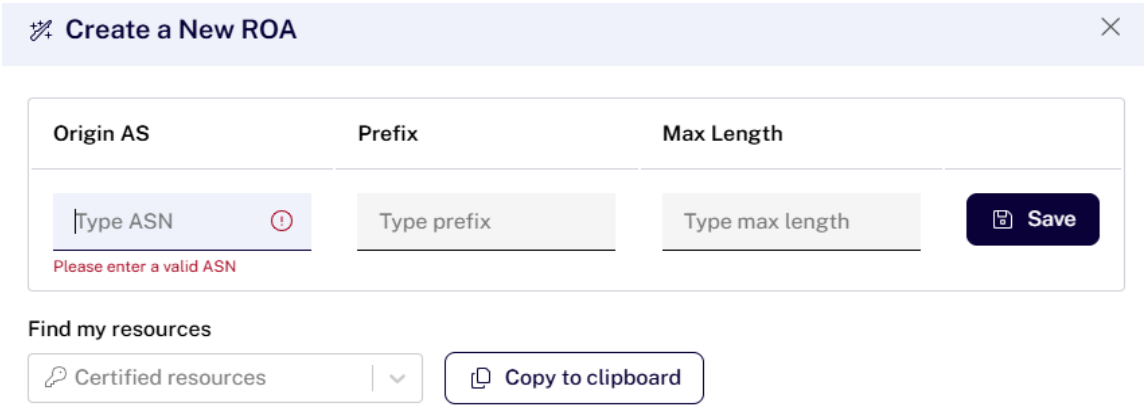
1.



2.



3.



Jak? RPKI ROV Cisco XR

```
! definice RPKI serveru (validátoru)
router rpki
 rpki server 192.0.2.10
  transport tcp port 3323
  refresh 600
  response-time 600
  expiration 7200

! aktivace validace na BGP
router bgp 65000
 address-family ipv4 unicast
  rpki origin-validation enable
  ! volitelně: invalid drop, unknown accept
  bgp bestpath origin-as use validity
```

NIX·CZ

Jak? RPKI ROV Juniper JunOS

```
set routing-options validation-group RPKI group 192.0.2.10 port 3323
set routing-options validation-group RPKI hold-time 600
set routing-options validation-group RPKI refresh-time 600
set routing-options validation-group RPKI response-time 600
set routing-options validation-group RPKI preference 1

set policy-options policy-statement RPKI-VALIDATION term VALID from validation-database valid
set policy-options policy-statement RPKI-VALIDATION term VALID then accept
set policy-options policy-statement RPKI-VALIDATION term INVALID from validation-database
invalid
set policy-options policy-statement RPKI-VALIDATION term INVALID then reject
set policy-options policy-statement RPKI-VALIDATION term UNKNOWN then accept

set protocols bgp group IBGP import RPKI-VALIDATION
```

NIX·CZ

Jak? RPKI ROV Huawei (VRP)

```
bgp 65000
 rpki enable
 rpki server 192.0.2.10 port 3323 refresh-time 600 expire-time 7200
 #
 ipv4-family unicast
  route-policy RPKI-VALIDATION import

route-policy RPKI-VALIDATION permit node 10
 if-match rpki validity valid
  apply accept
route-policy RPKI-VALIDATION permit node 20
 if-match rpki validity invalid
  apply reject
route-policy RPKI-VALIDATION permit node 30
 if-match rpki validity notfound
  apply accept
```

NIX·CZ

ASPA (Autonomous System Provider Authorization)

- „nový“ bezpečnostní mechanismus, který doplňuje RPKI.
- RPKI říká: „Tento prefix smí oznamovat jen tento ASN.“
- ASPA říká: „Tento ASN smí používat jako svého providera jen tyto ASN.“
- ASPA říká: „Cesta může být pouze nahoru nebo dolů.“

ASPA

- AS vytváří ASPA objekt (u svého RIR, podobně jako ROA)
- V objektu je: „Já (AS12345) mám jako **upstreamy** AS111, AS222, AS333.“
- Tento ASPA objekt se kryptograficky podepíše a publikuje do RPKI systému.
- Router validátoru si přes RTR stáhne ASPA data.
- Když přijde "BGP cesta", router ověří, jestli směrování odpovídá modelu provider–customer.

ASPA - validace

ASPA record - AS10 [20], AS20 [30]

Reálný AS PATH z BGP – AS30 AS20 AS10

Krok 1) AS20 <- AS10 – OK 20 Provider 10

Krok 2) AS30 <- AS20 – OK 30 Provider 20

Výsledek ASPA **valid**

ASPA - validace

ASPA record - AS10 [20,30], AS20 [30], AS30[-]

Reálný AS PATH z BGP – AS40 AS30 AS20 AS10

Krok 1) AS20 <- AS10 – OK Provider

Krok 2) AS30 <- AS20 – OK Provider

Krok 3) AS40 <- AS30 – nemá záznam

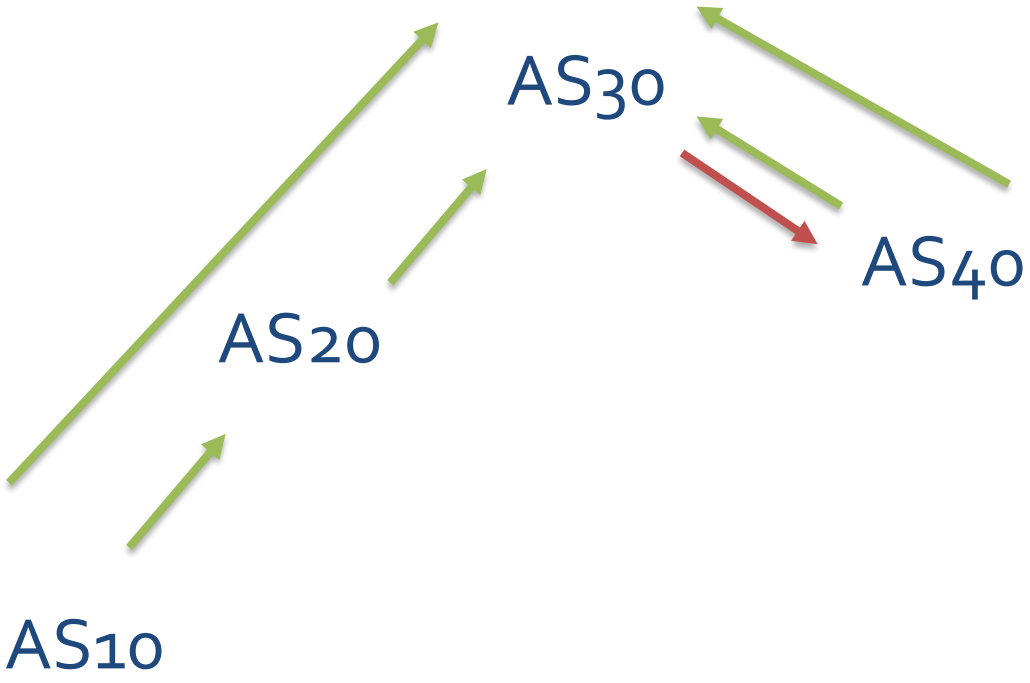
Výsledek ASPA **unknown**

NIX·CZ

ASPA – validace - valid

AS10 [20], AS20 [30], AS30[50], **AS40 [30]**

Reálný AS PATH z BGP – AS40 AS30 AS20 AS10

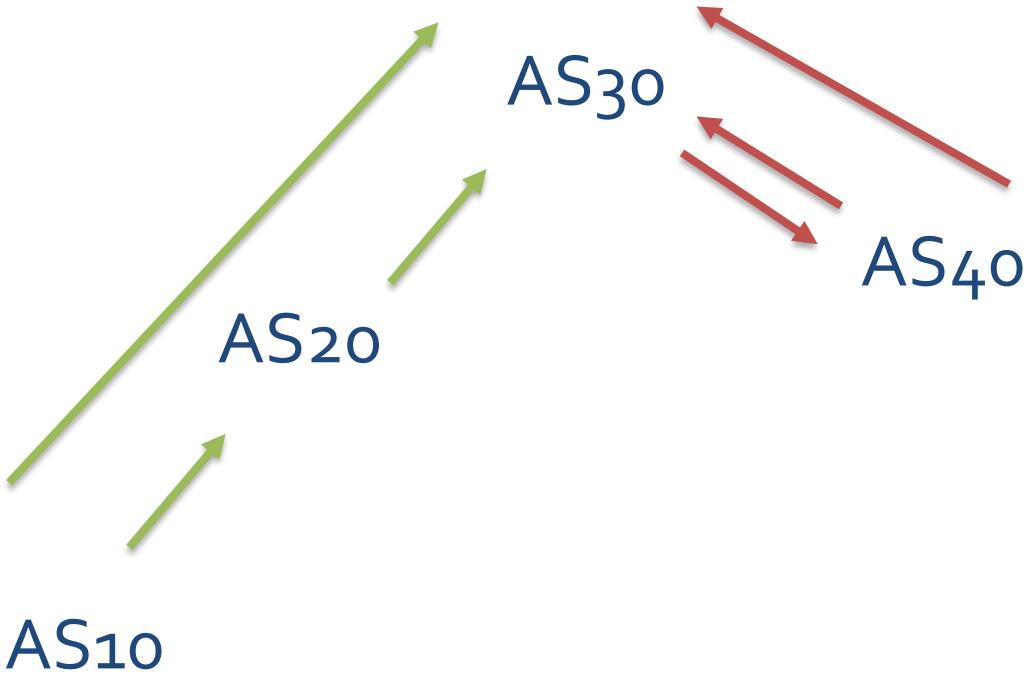


NIX·CZ

ASPA – validace - invalid

AS10 [20], AS20 [30], AS30[50], AS40 [60]

Reálný AS PATH z BGP – AS40 AS30 AS20 AS10



NIX·CZ

ASPA - validace

AS10 [20], AS20 [30], AS30[50], AS40 [30], AS50 [30]

Reálný AS PATH z BGP – AS50 AS40 AS30 AS20 AS10

Krok 1) AS20 <- AS10 – OK 20 Provider 10

Krok 2) AS30 <- AS20 – OK 30 Provider 20

Krok 3) AS40 <- AS30 – Není záznam v 30 – Not-Provider

Krok 4) AS50 <- AS40 – OK 50 Provider 40

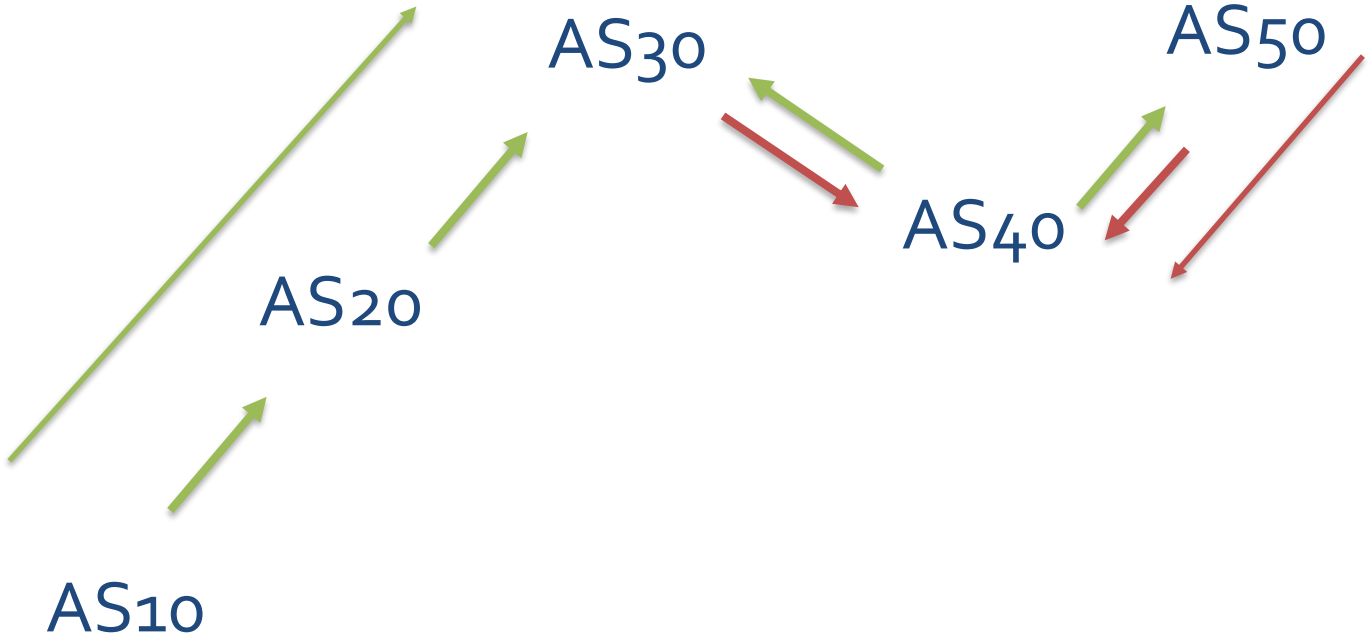
Výsledek ASPA invalid (cesta vede od zákazníka zpět)

NIX·CZ

ASPA – validace - leak

AS10 [20], AS20 [30], AS30[50], AS40 [30,50], AS50 [30]

Reálný AS PATH z BGP – AS50 AS40 AS30 AS20 AS10

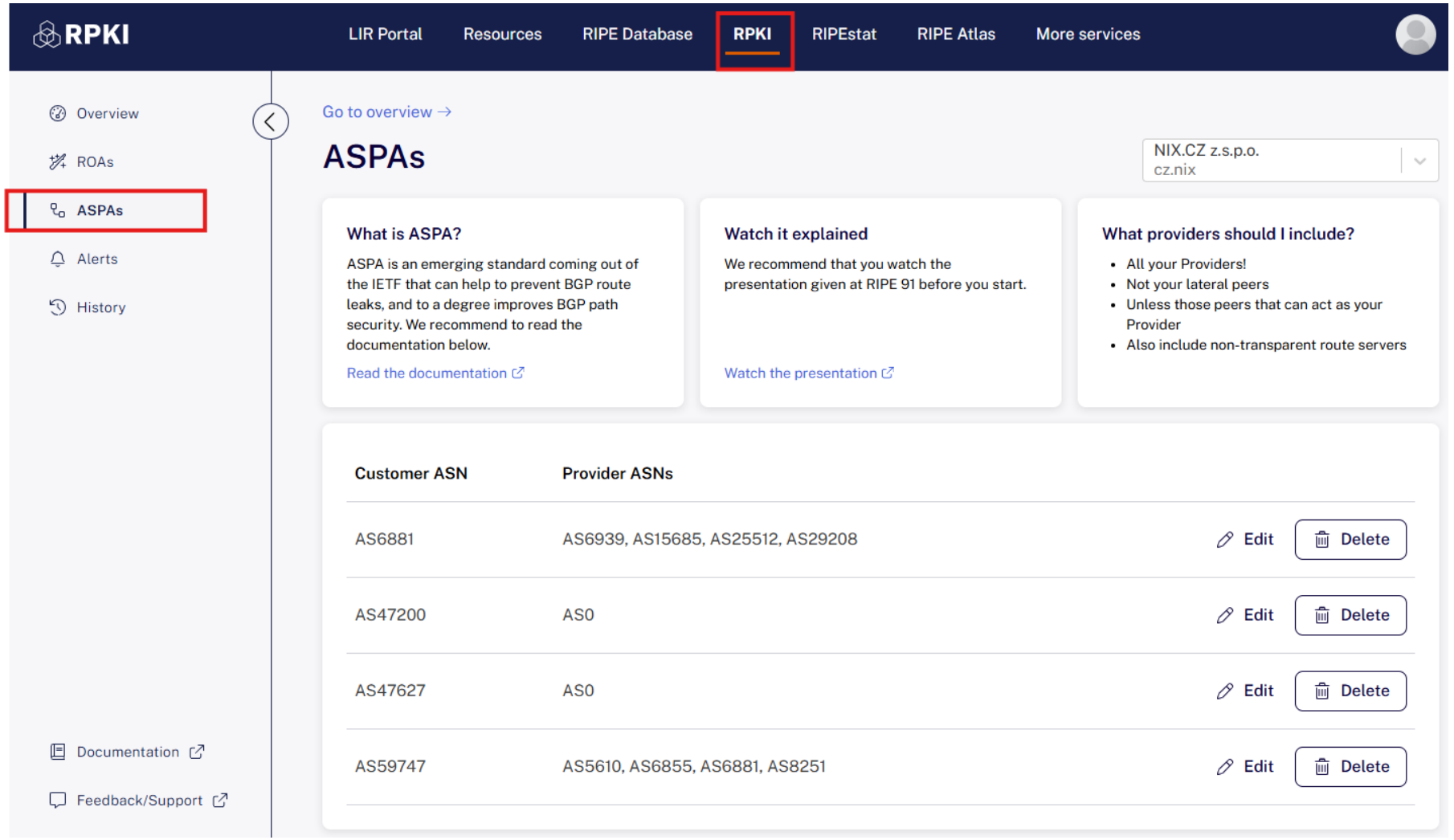


NIX·CZ

ASPA prakticky pro ISP

1. Příprava dat
   - Seznam všech upstream poskytovatelů (transit AS). To bude obsah ASPA objektu.
2. Vytvoření ASPA objektu (jakmile bude podporováno)
   - V RIPE NCC portálu (nebo jiném RIR) – podobně jako dnes se vytváří ROA.
3. Validace v síti (jakmile bude podporováno)
   - Je nutný router nebo route server s podporou ASPA (Bird, Cisco, Juniper – zatím testovací implementace).
4. Politika
   - Stejně jako u RPKI: nastaví se, že invalidní trasy se dropují nebo dávají nižší prioritu.

ASPA prakticky pro ISP - RIPE



RFC 9234 - BGP Roles

1. Rozšíření BGP. Sousedi při navazování session řeknou, jaký je jejich vztah:
   - Provider – dává transit.
   - Customer – přijímá transit.
   - Peer – výměna jen vlastních prefixů.
   - RS/RS-Client – pro Internet Exchange.
2. Router podle role ví, jaké typy cest přijmout nebo odmítnout.
3. Funguje i bez RPKI – je to čistě konfigurační, vyžaduje podporu obou stran.

RFC 9234 - BGP Roles – allowed pairs

Local AS Role	Remote AS Role
Provider	Customer
Customer	Provider
RS	RS-Client
RS-Client	RS
Peer	Peer

Table 2: Allowed Pairs of Role Capabilities

NIX·CZ

RFC 9234 - BGP OTC

1. Only-To-Customer (OTC, RFC 9234)
   - Nový BGP atribut, automaticky se přidává k prefixům, které AS šíří svému zákazníkovi.
   - Pokud se takový prefix objeví u peera nebo providera, je jasné, že jde o route leak.
2. OTC = jednoduchý atribut, kterou routery využijí ke kontrole správného toku cest.

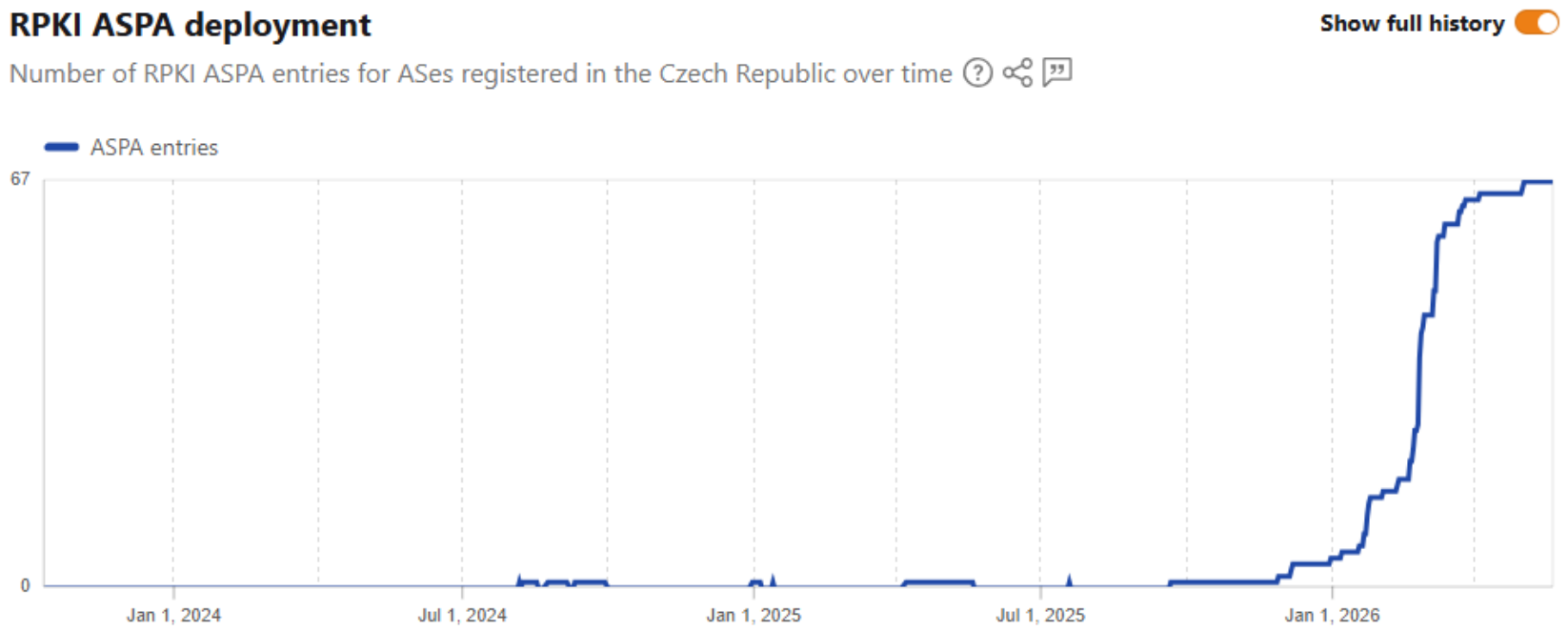
RFC 9234 - BGP OTC

```
Frame 42: 87 bytes on wire
Ethernet II, Src: 00:11:22:33:44:55, Dst: 66:77:88:99:aa:bb
Internet Protocol, Src: 192.0.2.1, Dst: 192.0.2.2
Transmission Control Protocol, Src Port: 45231, Dst Port: 179
Border Gateway Protocol
    Marker: ffffffffffffffffffffffffffffffff
    Length: 47
    Type: OPEN (1)
        Version: 4
        My AS: 65001
        Hold Time: 90
        BGP Identifier: 192.0.2.1
        Optional Parameters (1)
            Optional Parameter, Type: BGP Role (9), Length: 1
                Role: Provider (1)
```

```
Frame 45: 121 bytes on wire
Ethernet II, Src: 00:11:22:33:44:55, Dst: 66:77:88:99:aa:bb
Internet Protocol, Src: 192.0.2.1, Dst: 192.0.2.2
Transmission Control Protocol, Src Port: 45231, Dst Port: 179
Border Gateway Protocol
    Marker: ffffffffffffffffffffffffffffffff
    Length: 81
    Type: UPDATE (2)
        Withdrawn Routes Length: 0
        Total Path Attribute Length: 44
        Path attributes
            ORIGIN: IGP
            AS_PATH: 65001
            NEXT_HOP: 192.0.2.1
            LOCAL_PREF: 100
            OTC: 0x00000001    (Only-To-Customer attribute present)
        NLRI
            203.0.113.0/24
```

Závěr - statistika

- **RPKI – 79.7% / 980 ASNs - (SK 62.4% / 278)**
- **ASPA – 67 ASNs - (SK 13)**



Závěr - zabezpečte své BGP

- **RPKI** = kryptograficky potvrzený zdroj
- **ASPA** = kryptograficky potvrzený seznam providerů (v RPKI)
- **BGP Roles** = deklarace vztahu už při BGP session (protokolová vrstva)
- **OTC** = technický mechanismus, který roli propaguje dál do sítě