REISS ROMOLI

(Some) Best Practices for *Route Leaks* and *Prefix Hijacking* prevention

Tiziano TOFONI
Reiss Romoli srl
L'AQUILA
Tel. 0862.452401
Fax 0862.028308

info@ssgrr.com
www.reissromoli.com

REISS ROMOLI

What and to Whom You Should Advertise

Classifier (attached in ebgp-in)	ebgp-out to customer	ebgp-out to peer	ebgp-out to upstream
Learned from Customer	accept	accept	accept
Learned from Peer	accept	reject	reject
Learned from Upstream	accept	reject	reject
My own routes	accept	accept	accept
No Classifier	reject	reject	reject

Source: Melchior Aelmans, Niels Raijer - DAY ONE: DEPLOYING BGP ROUTING SECURITY, Juniper Networks, 2019

- Violations of these rules are considered route leaks
  - For a more formal definition and classification, see RFC 7908 - *Problem Definition and Classification of BGP Route Leaks*, June 2016

REISS ROMOLI

First Commandment

- Always use routing policies (inbound & outbound)
- Even better, use platforms that support RFC 8212
  - IOS XR: default
  - IOS XE: use command "**bgp safe-ebgp-policy**" under BGP process configuration
  - JunOS:

```
[edit protocols bgp defaults ebgp]
no-policy {
    advertise (accept | reject | reject-always);
    receive (accept | reject | reject-always);
}
```

For an update list of compliant BGP implementations: https://github.com/bgp/RFC8212

REISS ROMOLI

Second Commandment

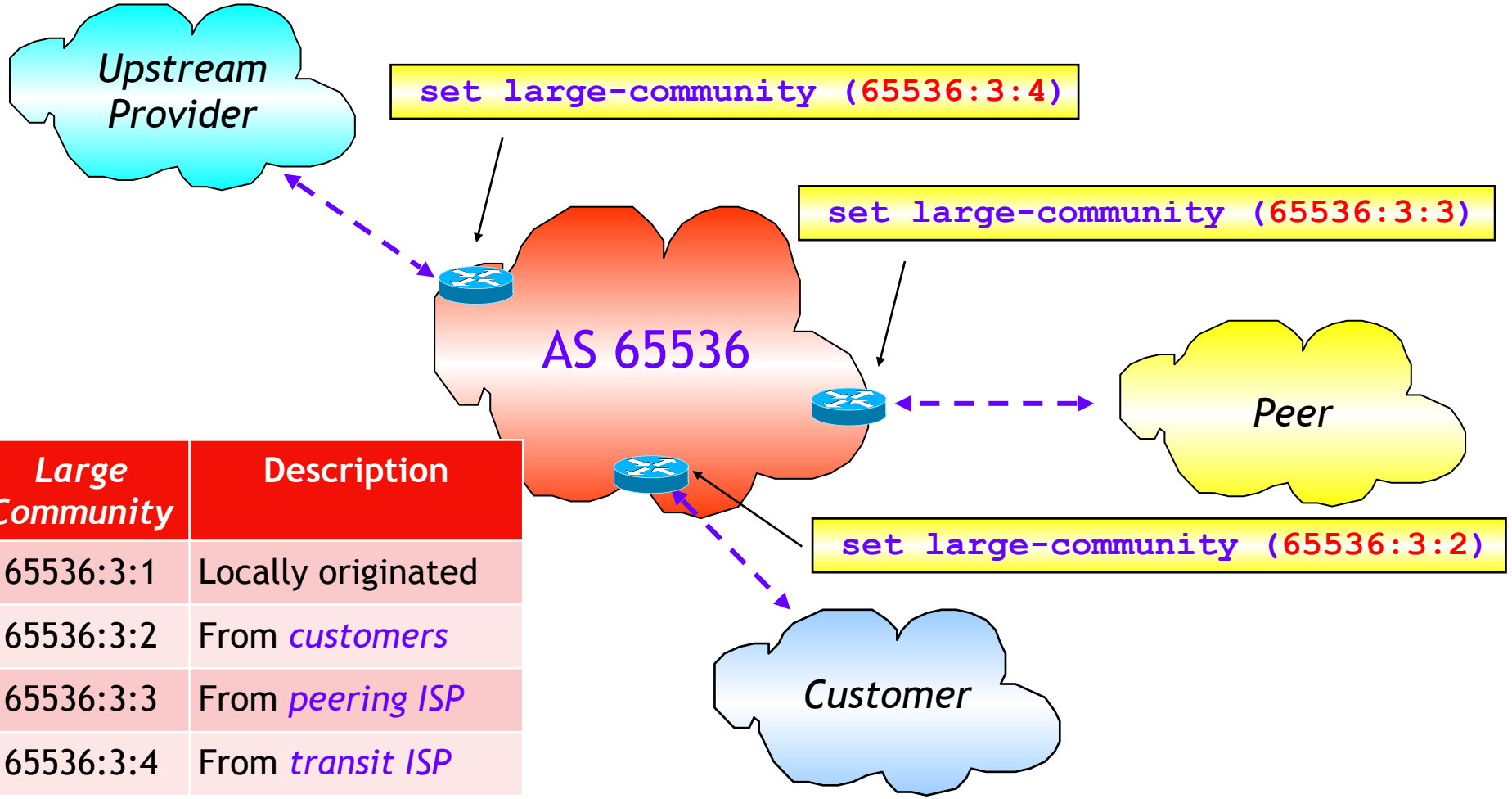
- To prevent Route Leaks

Filter, filter and … filter

Worth reading: https://www.manrs.org/isps/guide/filtering/

Best practice (1/2)

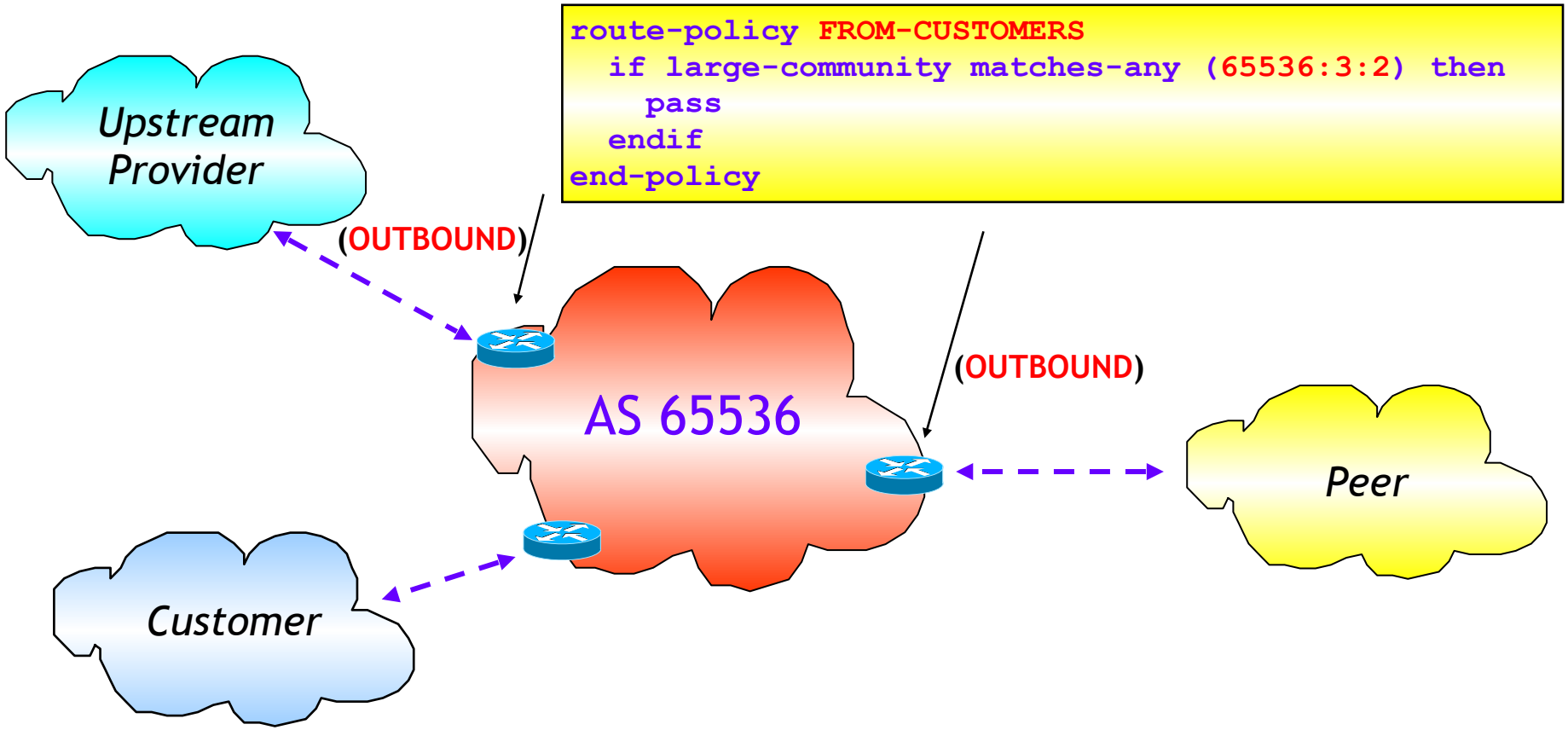
- First step: **tag routes**
  - Use BGP communities (standard/extended/large)



Large Community	Description
65536:3:1	Locally originated
65536:3:2	From *customers*
65536:3:3	From *peering ISP*
65536:3:4	From *transit ISP*

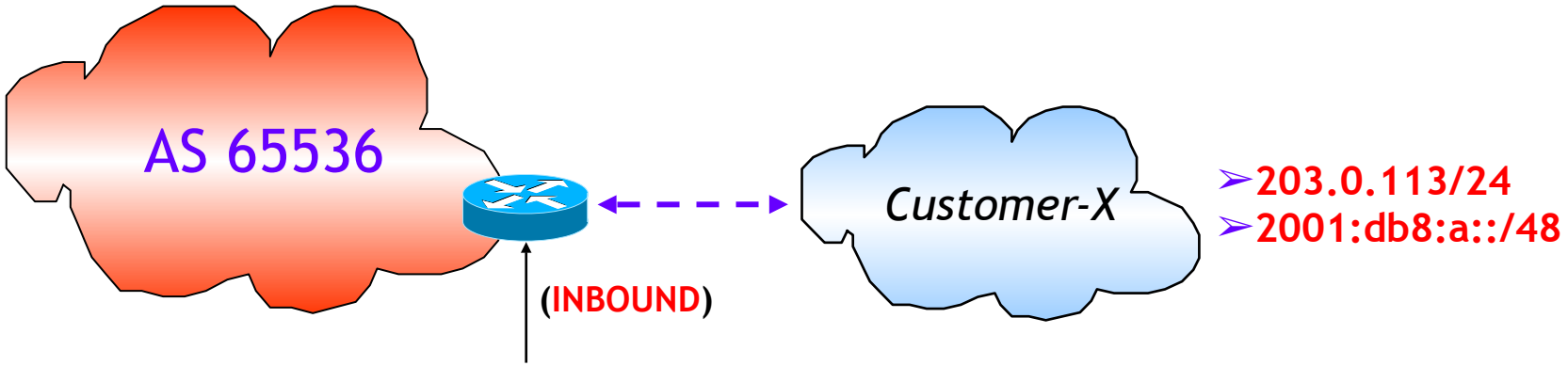
Best practice (2/2)

- Second step: **filter routes**
  - Use filters based on BGP communities (standard/extended/large)



Third Commandment (I)

- Filter customers routes
  - Accept only prefixes that your customers are allowed to advertise
  - Even better: automate prefix-list updates, i.e. apply a "whitelist" of prefixes a customer may announce on every customer session (ex. use bgpq3, IRRPT)

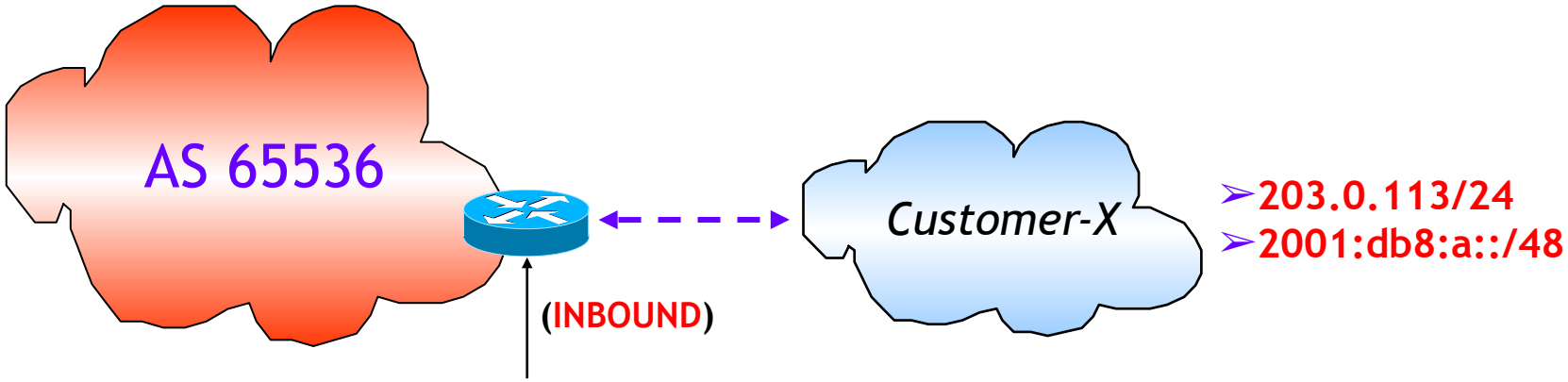



```
route-policy V4-FROM-CUSTOMER-X
 if destination in (203.0.113.0/24) then
   set large-community (65536:3:2)
 endif
end-policy
```

```
route-policy V6-FROM-CUSTOMER-X
 if destination in (2001:db8:a::/48) then
   set large-community (65536:3:2)
 endif
end-policy
```

Third Commandment (II)

- Filter customers routes: allow subnets for BGP traffic Engineering
  - Tag subnets with well-known community **no-export** to avoid leaking subnets outside your AS

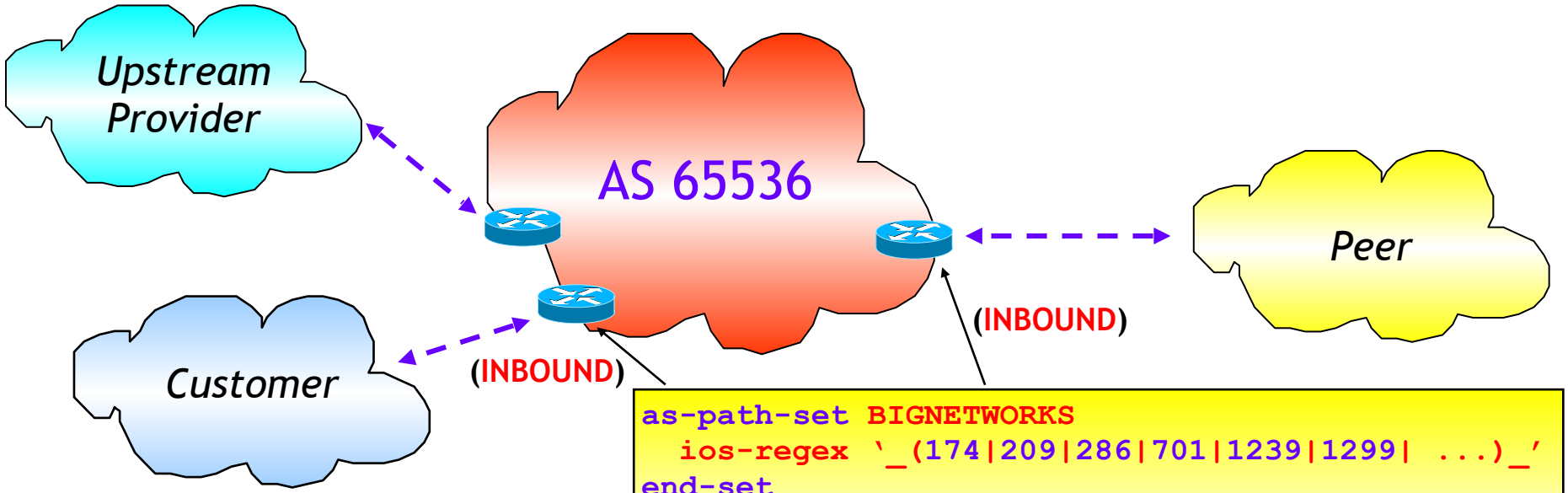



```
route-policy V4-FROM-CUSTOMER-X
 if destination in (203.0.113.0/24 ge 25 le 26) then
   set large-community (65536:3:2)
   set community (no-export)
 endif
end-policy
```

```
route-policy V6-FROM-CUSTOMER-X
 if destination in (2001:db8:a::/48 ge 48 le 56) then
   set large-community (65536:3:2)
   set community (no-export)
 endif
end-policy
```

Third Commandment (III)

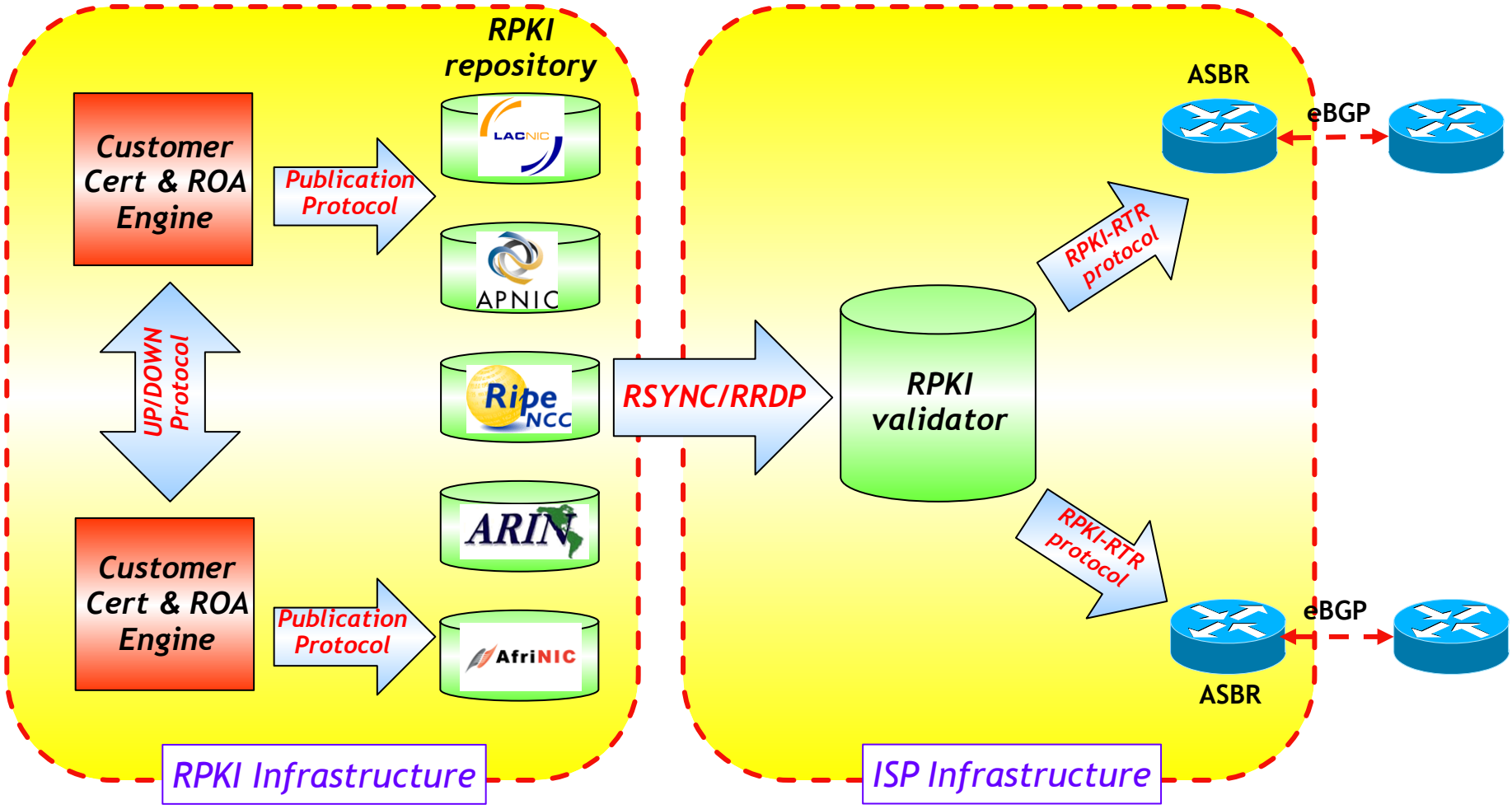
- Filter "**transits**" (i.e. Tier-1) and "**bignetworks**" (i.e. Facebook, Google, Cloudflare, ...) from your customers and peers
  - To get a list of "**transits**" and "**bignetworks**": **https://api.asrank.caida.org/v2/docs**




```
as-path-set BIGNETWORKS
  ios-regex '_(174|209|286|701|1239|1299| ...)_'
end-set
!
route-policy NO-BIGNETWORKS
   if as-path in BIGNETWORKS then drop
     else pass
   endif
 end-policy
```

Fourth Commandment

- Use RPKI architecture to prevent BGP prefix hijacking



REISS ROMOLI

Fifth Commandment (for future use …)

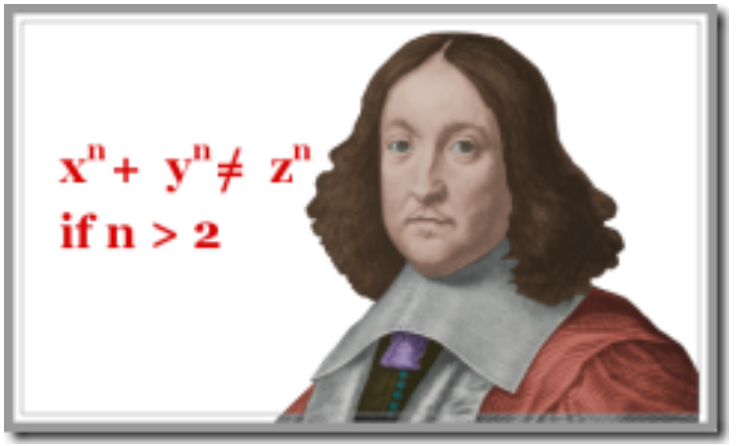
- RPKI architecture does not protect from forged AS_PATH
- Use BGP Path Validation (a.k.a. BGPsec): RFC 8205 - BGPsec Protocol Specification, september 2017
- Commercial vendor implementations not widely available yet
  - Some open source prototype implementations are available (NIST, GoBGP, BIRD, Quagga)

REISS ROMOLI

Time is over …

Thank you for your kind attention

I have 5 other commandments and dozens of best practices but the space granted me does not allow to set them out



But you have a great friend: MANRS (https://www.manrs.org/).

Joining MANRS means joining a community of security-minded organizations committed to making the global routing infrastructure more robust and secure