



nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

cgib.br

Comitê Gestor da
Internet no Brasil



registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

nic.br cgi.br

ceptro.br

RPKI

Por que é importante para a segurança do seu provedor e como implantar.

ceptro.br nic.br cgi.br

Licença de uso do material

Esta apresentação está disponível sob a licença

Creative Commons

Atribuição – Não a Obras Derivadas (by-nd)

<http://creativecommons.org/licenses/by-nd/3.0/br/legalcode>



Você pode:

- **Compartilhar** — copiar, distribuir e transmitir a obra.
- **Fazer uso comercial da obra.**
- Sob as seguintes condições:

Atribuição — Ao distribuir essa apresentação, você deve deixar claro que ela faz parte do Curso de Formação para Sistemas Autônomos do CEPTR0.br/NIC.br, e que os originais podem ser obtidos em <http://ceptro.br>. Você deve fazer isso sem sugerir que nós damos algum aval à sua instituição, empresa, site ou curso.

Vedada a criação de obras derivadas — Você não pode modificar essa apresentação, nem criar apresentações ou outras obras baseadas nela..

Se tiver dúvidas, ou quiser obter permissão para utilizar o material de outra forma, entre em contato pelo e-mail: info@nic.br.

BGP Hijacking

- Anúncio de prefixos não autorizados
 - "Sequestro do prefixo"
- Motivos:
 - Erro de configuração
 - *Fat finger*
 - Proposital



Por que isso acontece?

- A Internet funciona com base na cooperação entre Sistemas Autônomos (ASes):
 - É uma “rede de redes”
 - São mais de **100.000 redes** diferentes, sob gestões técnicas independentes
 - A estrutura de **roteamento BGP** funciona com base em cooperação e confiança
 - O BGP **não** tem validação dos dados



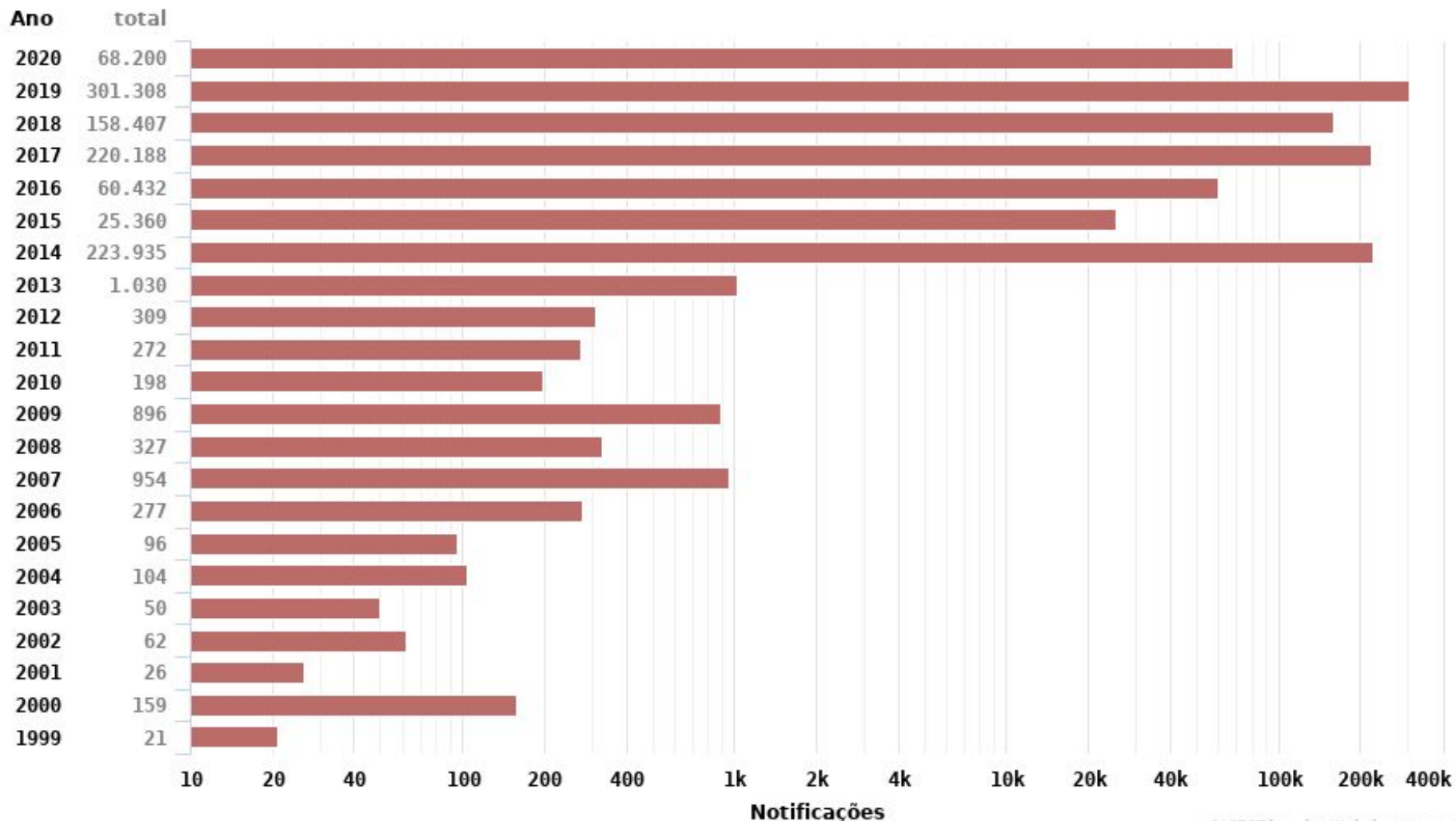
**Como resolver
esses problemas???**



MANRS

DDoS ao Longo do Tempo

Notificações sobre equipamentos participando em ataques DoS

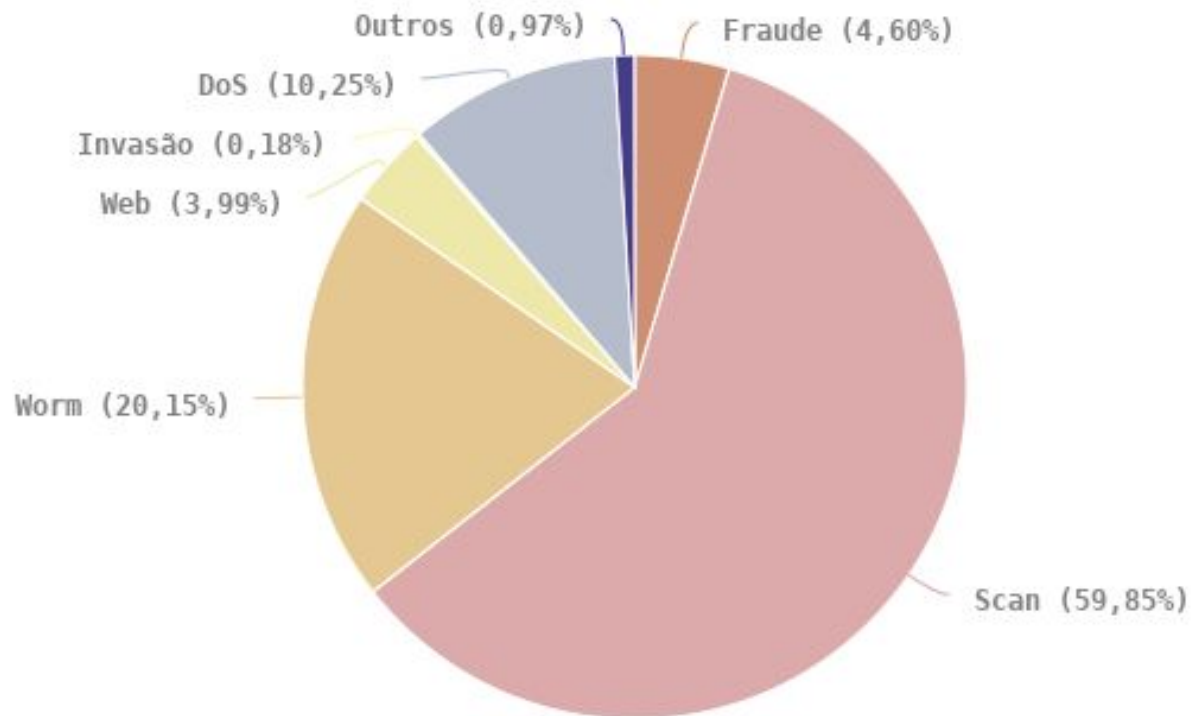


© CERT.br -- by Highcharts.com

Características dos Ataques

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2020

Tipos de ataque



© CERT.br – by Highcharts.com

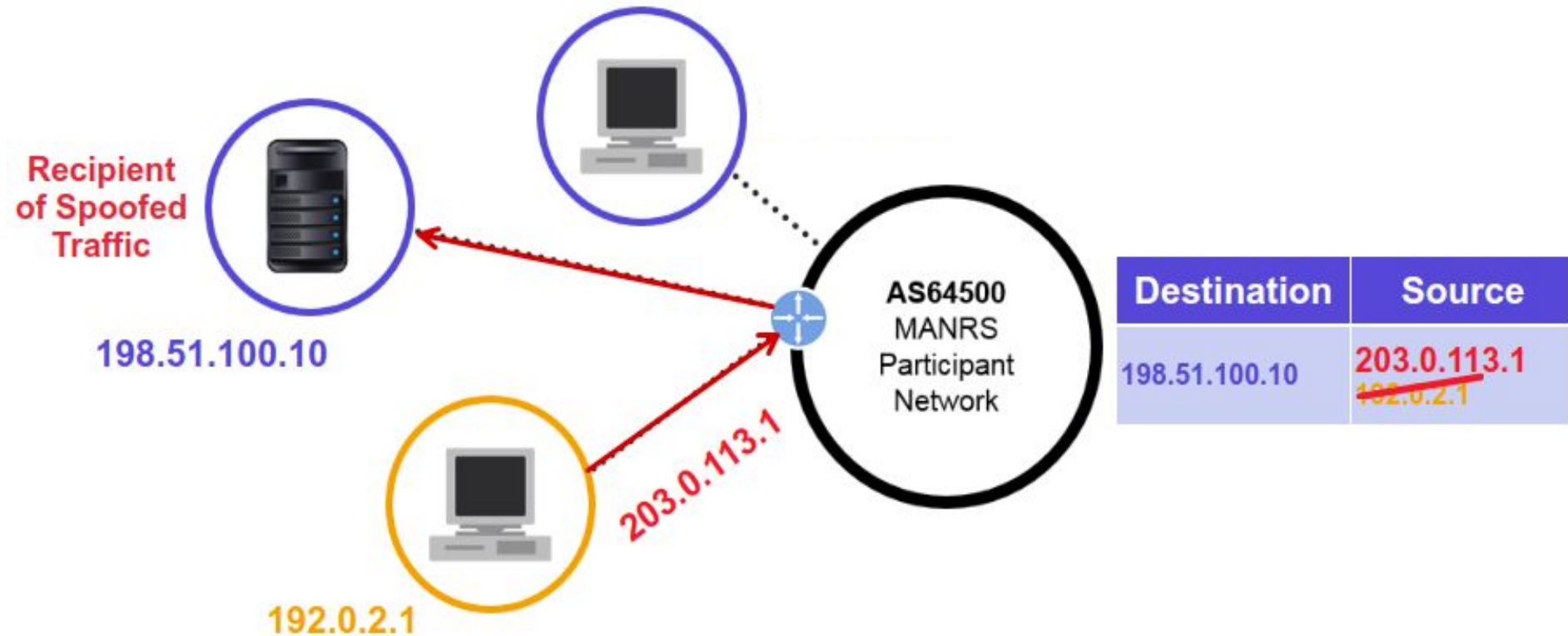
O que é MANRS?

- Mutually Agreed Norms for Routing Security
- É uma iniciativa global
- Apoio da ISOC
- Consiste em 4 coisas básicas
 - Anti-Spoofing
 - Filtros
 - Coordenação
 - Validação Global

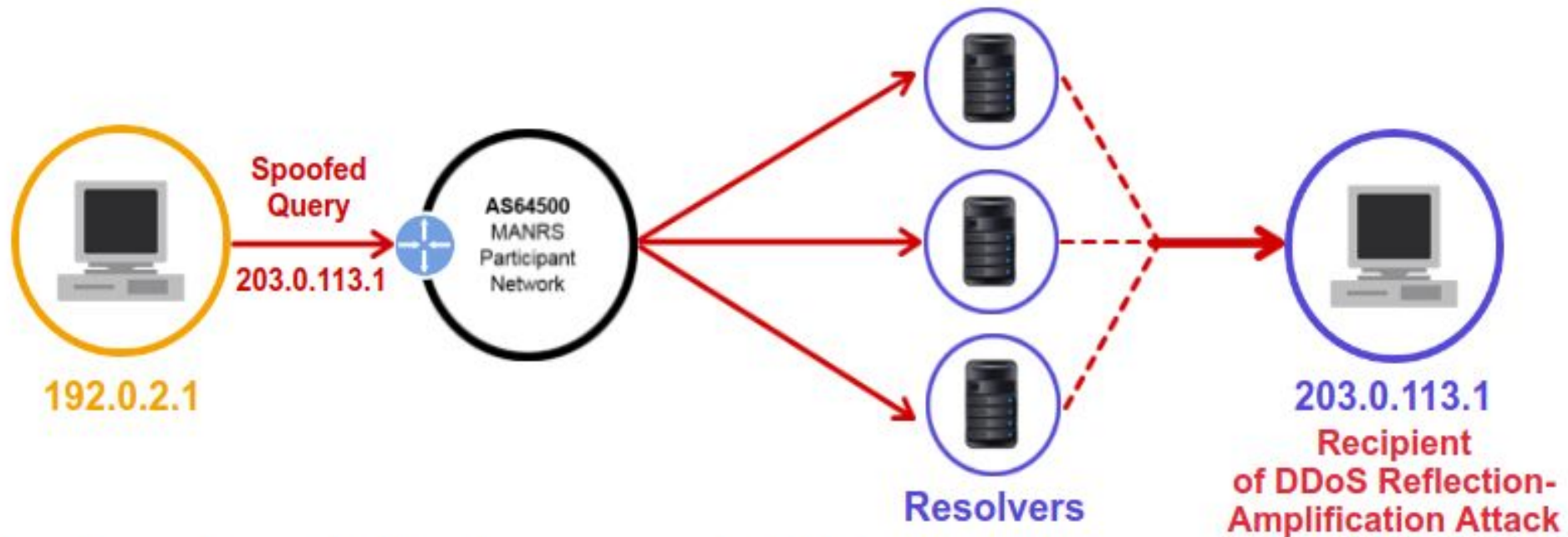
O que é spoofing?

- Pacotes IP com endereços de origem incorretos
 - **Erro de configuração**
 - Problema de Software
 - **Teste e Simulação**
 - Teste de Performance
 - **Atitude maliciosa**
 - Esconder a identidade do atacante
 - Fingir ser outro computador na rede
- O spoofing pode ser usado em ataques de negação de serviço e é um problema sério na Internet

Como funciona o ataque spoofing



Como funciona o ataque reflexão-amplificação



Fatores de amplificação

| Protocolo | Fator de Amplificação | Comando Vulnerável |
|--------------|-----------------------|------------------------------|
| DNS | 28 a 54 | Ver: TA13-088A |
| NTP | 556.9 | Ver: TA14-013A |
| SNMPv2 | 6.3 | GetBulk request |
| LDAP / CLDAP | 46 a 70 | Malformed request |
| SSDP | 30.8 | SEARCH request |
| Chargen | 358.8 | Character generation request |

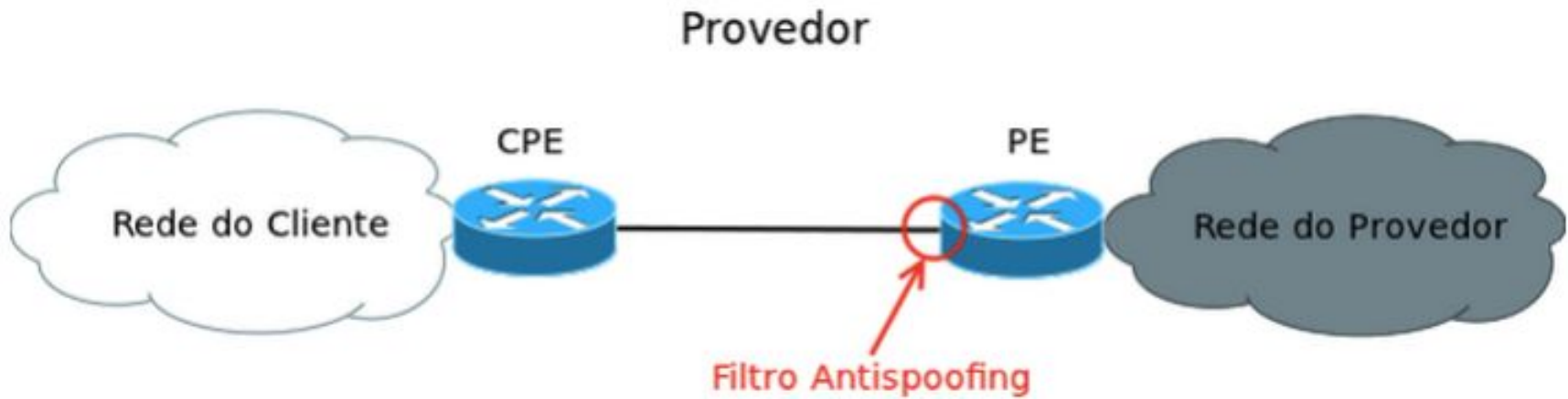
Total de ASNs e IPs Notificados pelo CERT.br

| mês | DNS | | SNMP | | NTP | | SSDP | | Portmap | | Ubiquiti | |
|---------|-------|--------|-------|--------|-------|--------|------|--------|---------|-------|----------|-------|
| | ASNs | IPs | ASNs | IPs | ASNs | IPs | ASNs | IPs | ASNs | IPs | ASNs | IPs |
| 2021-10 | 3.174 | 41.817 | 3.298 | 75.026 | 1.184 | 73.819 | 712 | 20.903 | 1.599 | 8.888 | 740 | 3.817 |
| 2021-11 | 3.197 | 44.549 | 3.402 | 73.792 | 1.215 | 71.992 | 685 | 17.132 | 1.724 | 8.957 | 720 | 4.015 |
| 2021-12 | 3.223 | 46.370 | 3.360 | 70.562 | 1.198 | 63.180 | 460 | 2.388 | 1.629 | 8.953 | 729 | 4.096 |
| 2022-01 | 3.218 | 46.246 | 3.377 | 75.092 | 1.216 | 72.576 | 442 | 2.258 | 1.602 | 8.323 | 714 | 3.682 |
| 2022-02 | 3.093 | 39.946 | 3.053 | 58.454 | 1.178 | 68.493 | 313 | 1.203 | 1.596 | 8.365 | 665 | 3.304 |
| 2022-03 | 3.221 | 46.560 | 3.396 | 74.557 | 1.176 | 67.549 | 283 | 1.000 | 1.585 | 7.868 | 663 | 3.428 |
| 2022-04 | 3.187 | 50.275 | 3.440 | 72.178 | 1.169 | 68.141 | 436 | 2.105 | 1.572 | 7.591 | 654 | 3.425 |
| 2022-05 | 3.186 | 52.248 | 3.372 | 72.007 | 1.219 | 71.229 | 417 | 2.040 | 1.714 | 8.212 | 624 | 2.889 |
| 2022-06 | 3.203 | 49.995 | 3.419 | 68.921 | 1.216 | 71.961 | 368 | 1.503 | 1.649 | 7.739 | 615 | 2.410 |
| 2022-07 | 3.203 | 47.594 | 3.426 | 69.697 | 1.218 | 71.649 | 556 | 12.623 | 1.586 | 7.459 | 591 | 2.362 |
| 2022-08 | 3.243 | 53.304 | 3.457 | 68.891 | 1.235 | 72.463 | 343 | 1.383 | 1.529 | 7.361 | 589 | 2.236 |
| 2022-09 | 3.205 | 50.239 | 3.463 | 69.177 | 1.239 | 71.610 | 327 | 1.270 | 1.492 | 7.421 | 542 | 2.079 |

Soluções propostas

- **Ingress Access Lists**
 - **Access Control List - ACLs**
- **Unicast Reverse Path Forward (uRPF)**
 - **Strict Mode**
 - **Loose Mode**
- **VRF (Virtual Routing and Forwarding) Mode**
- **Source Address Validation Improvement (SAVI)**

Filtro anti spoofing



uRPF



Porque utilizar filtros? Roubo de prefixos

Mutually Agreed Norms for Routing Security (MANRS) 27 April 2018

EN ES

What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets

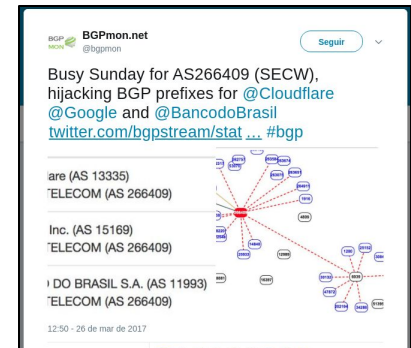
<https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/>

Mutually Agreed Norms for Routing Security (MANRS) 28 August 2017

EN FR ES

Google leaked prefixes – and knocked Japan off the Internet

<https://www.internetsociety.org/blog/2017/08/google-leaked-prefixes-knocked-japan-off-internet/>



<https://twitter.com/bgpmon/status/846087079763177472>

Mutually Agreed Norms for Routing Security (MANRS) 15 November 2018

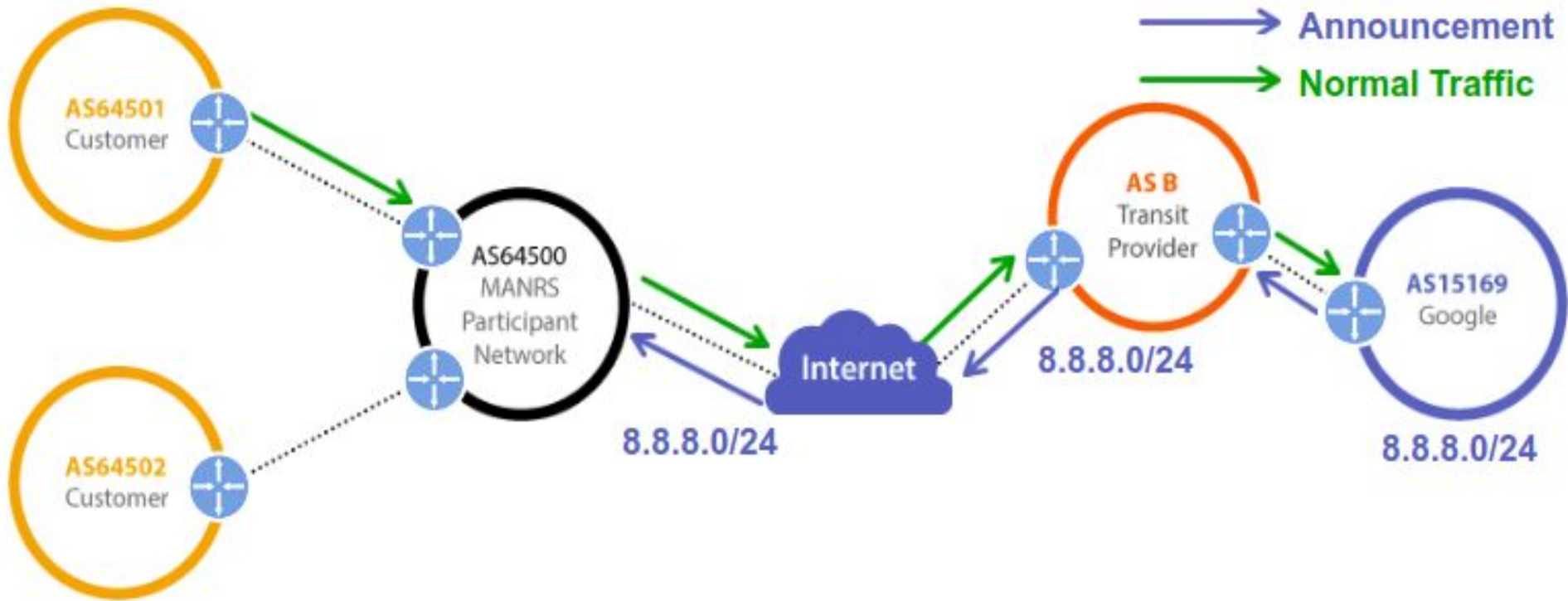
Route Leak Causes Major Google Outage

<https://www.internetsociety.org/blog/2018/11/route-leak-caused-a-major-google-outage/>

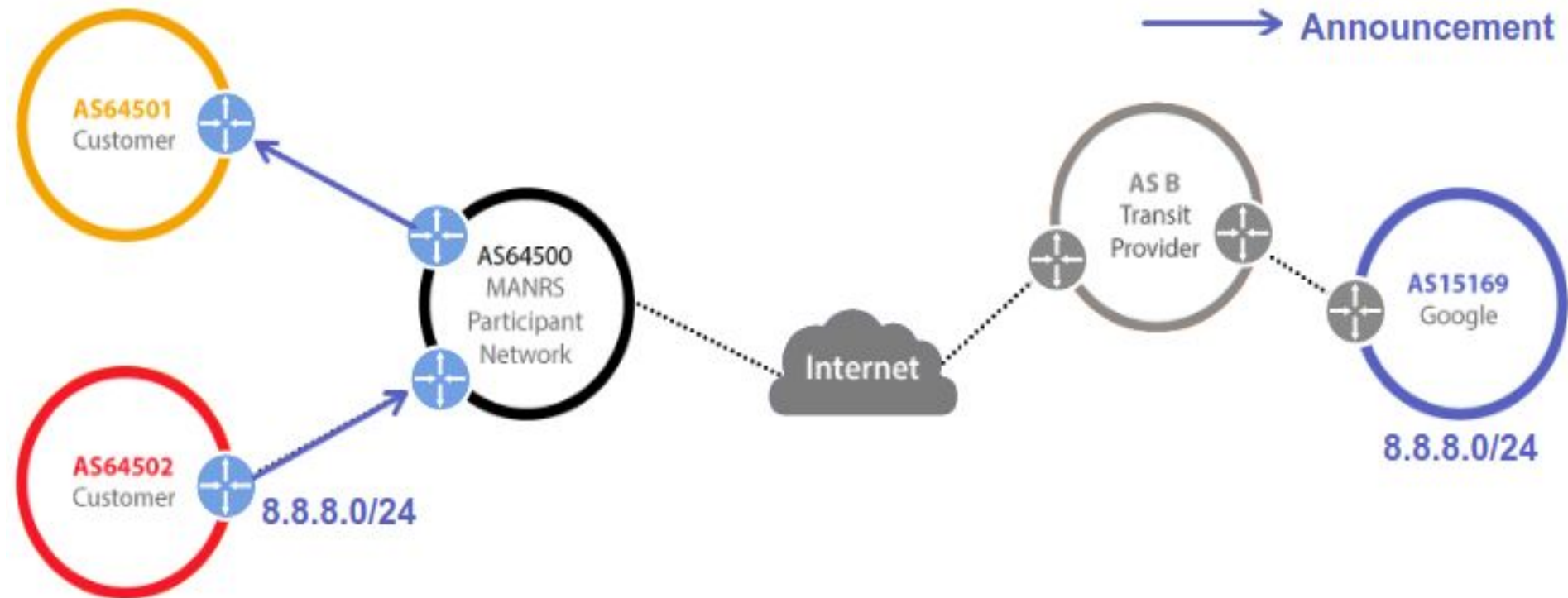


<https://dyn.com/blog/widespread-impact-caused-by-level-3-bgp-route-leak/>

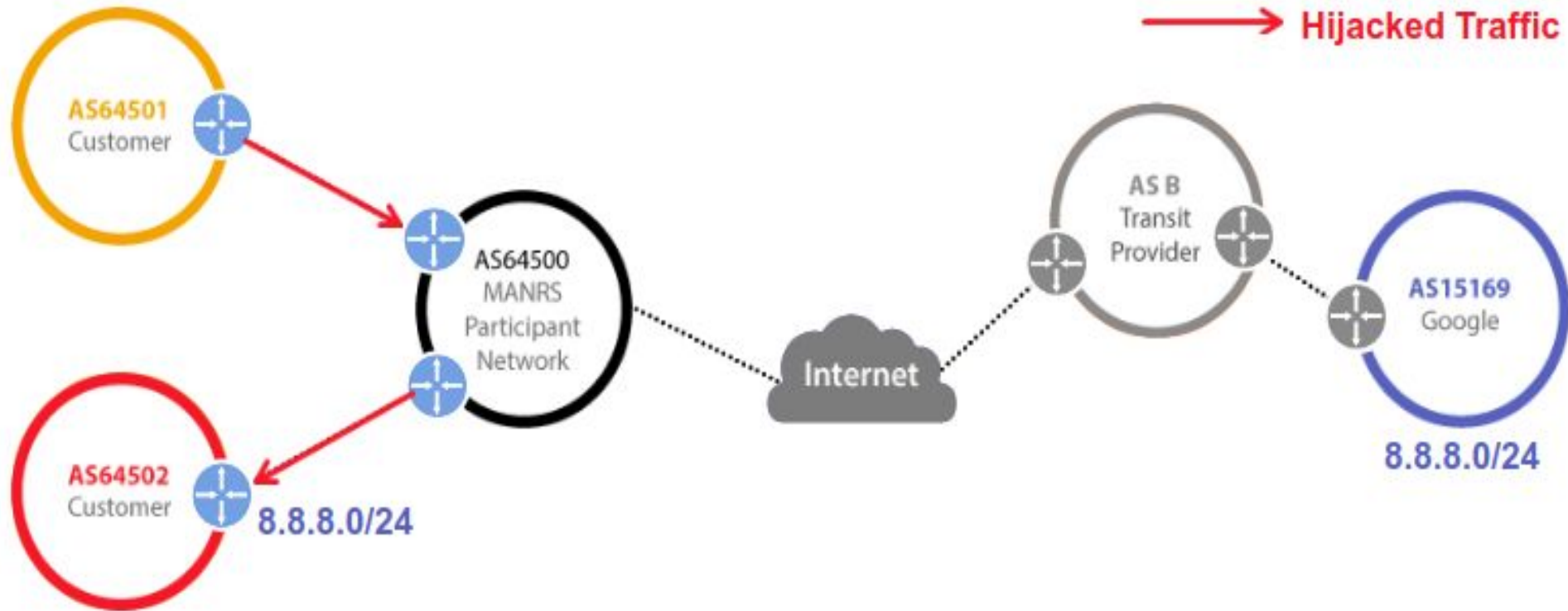
Porque utilizar filtros? Roubo de prefixos



Porque utilizar filtros? Roubo de prefixos



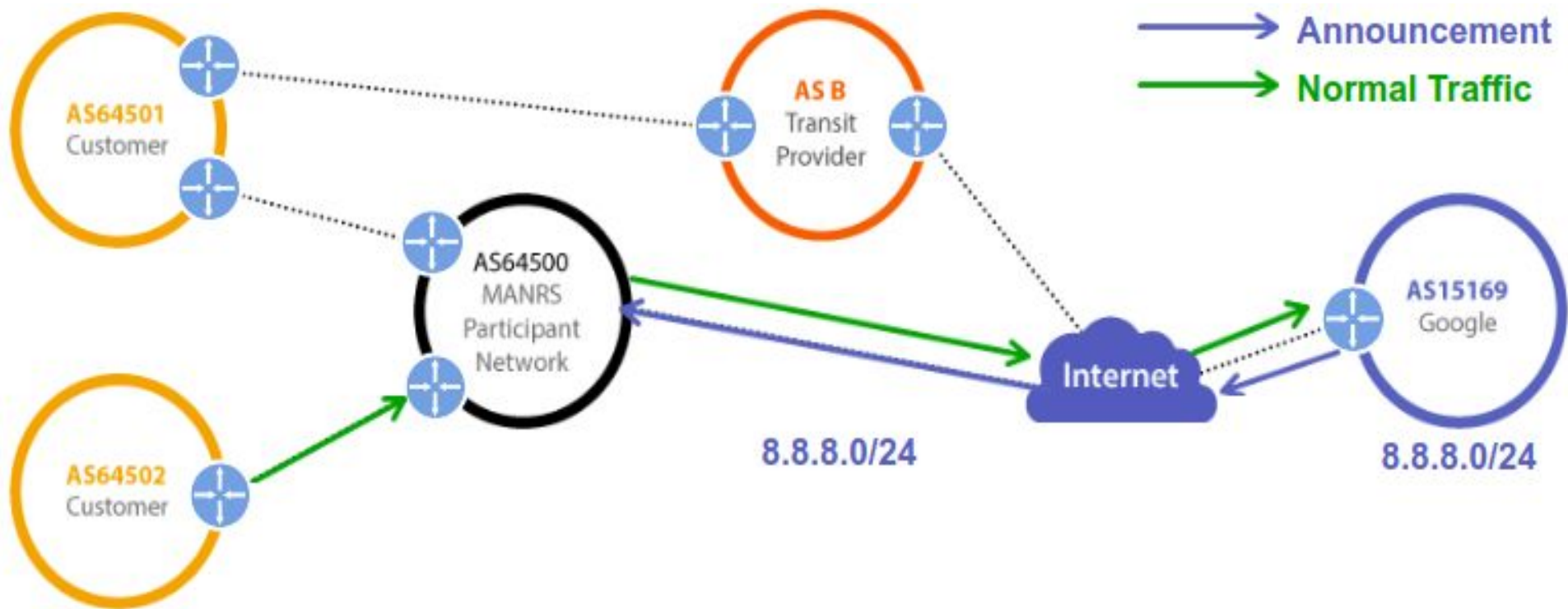
Porque utilizar filtros? Roubo de prefixos



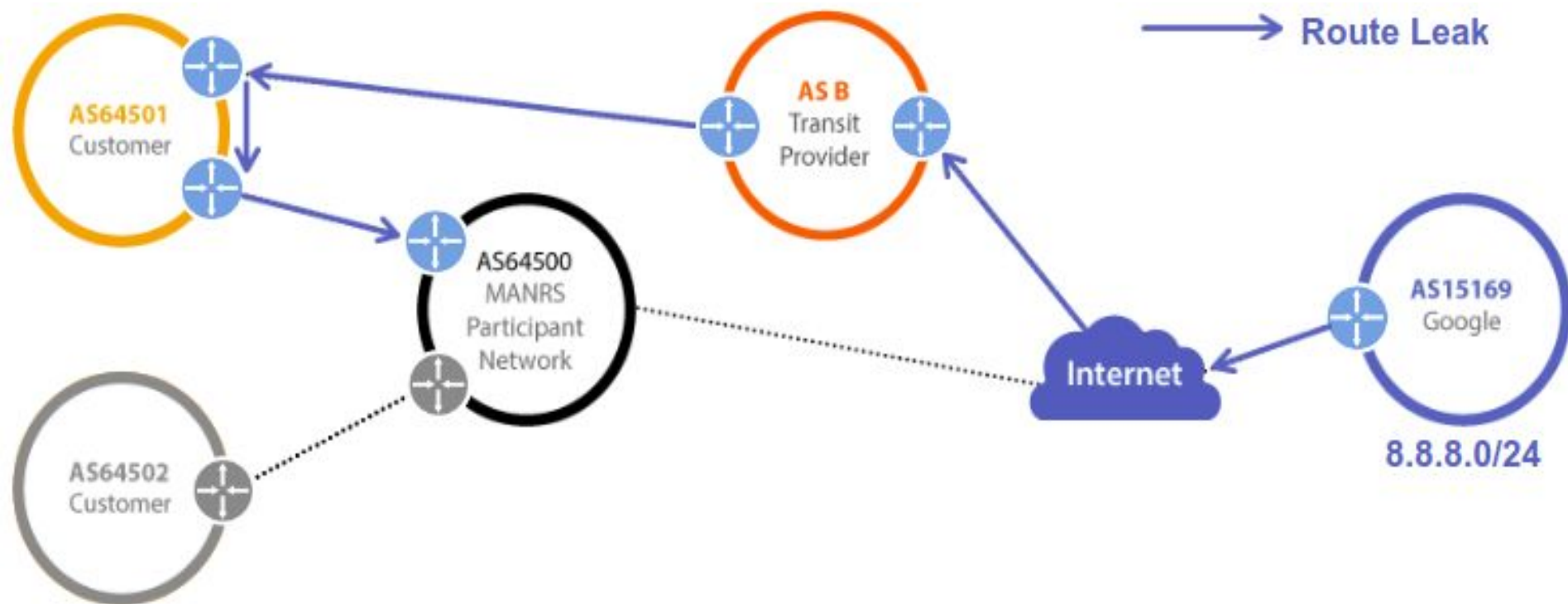
Porque utilizar filtros? Roubo de prefixos

- Rotas anunciadas
 - Monitorar todos os anúncios com origem em seu ASN
 - BGPmon
 - <https://bgpmon.net>
 - BGPStream
 - <https://twitter.com/bgpstream>
 - <http://bgpstream.caida.org>
 - Via scripts de consulta a servidores looking glass
 - Ex: <telnet://lg.saopaulo.sp.ix.br>
 - Monitorar anúncios internos

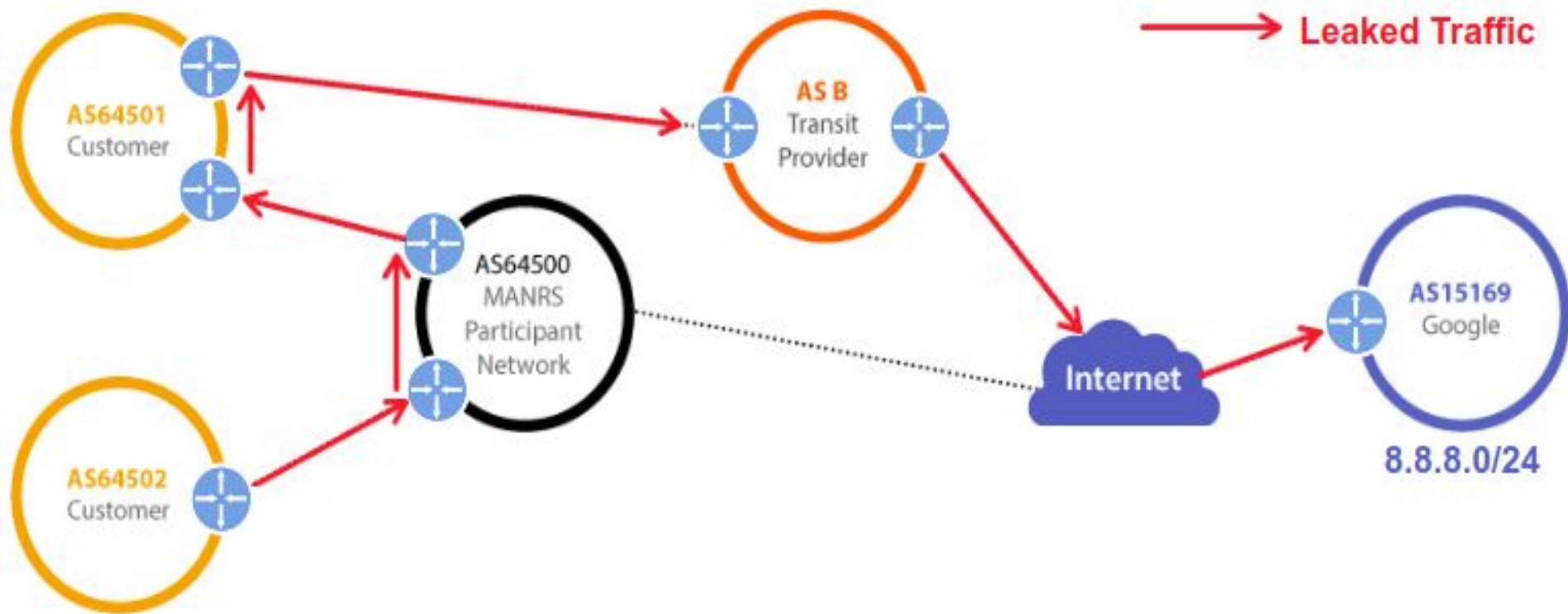
Porque utilizar filtros? Vazamento de rotas



Porque utilizar filtros? Vazamento de rotas



Porque utilizar filtros? Vazamento de rotas



Filtros

- Garanta que os seus anúncios BGP estejam corretos.
 - Publique suas informações de roteamento.
- Garanta que os anúncios BGP dos seus clientes estejam corretos.
 - Exija que eles publiquem suas informações de roteamento.
 - Aplique filtros de acordo com as informações publicadas por eles.
- Utilize WHOIS, IRR, RPKI e site da instituição para publicar e encontrar dados de roteamento.

Filtros

- Filtro de prefixos
 - Entrada: Só receba os prefixos que foram acordados previamente com o seu cliente.
 - Entrada: Em casos de peering (como ATM do PTT) aplique filtro de bogons.
 - Saída: Só envie os seus prefixos e de seus downstream.
- Filtro de AS-Path
 - Só receba as rotas que o seu cliente possui e dos downstreams dele.
- Evita problemas de prefix hijacking e route leaks.

Coordenação

- Ataques podem ser mitigados se tiver uma ação global e cooperativa
- Mantenha atualizada suas informações de contato
 - Administrativo
 - Técnico (NOC)
 - Abuso
- Publique sua informações
 - RIRs - Whois
 - IRRs
 - PeeringDB
 - Website

Validação Global

- Publique suas informações de Roteamento
 - Seu sistema autônomo
 - Suas políticas de roteamento
 - As rotas dos seus clientes
- Peça que seus clientes e seus upstreams também publique suas informações de roteamento
- Utilize ferramentas
 - RPKI
 - IRR

IRRs

- RADb
 - <http://www.radb.net/>
- NTTCOM
 - <https://www.us.ntt.net/support/policy/rr.cfm>
- TC IRR
 - <http://bgp.net.br/>

Programa Internet+Segura

- Redução dos ataques de Negação de Serviço
- Melhora da Segurança de Roteamento na rede
- Redução das vulnerabilidades e falhas de configuração
- **Incentivar o crescimento de uma cultura de segurança entre os operadores da rede**



<https://bcp.nic.br/i+seg/>

Programa Internet+Segura

- Reuniões com os ASes
- Relatório gerencial mensal para o acompanhamento da resolução dos problemas notificados pelo **CERT.br**
- Temas nas reuniões bilaterais:
 - Acompanhamento da correção dos serviços notificados pelo CERT.br
 - Adoção de Boas Práticas de roteamento (MANRS)
 - TOP – Teste os Padrões



<https://bcp.nic.br/i+seg/>

Dúvidas?



Resource Public Key Infrastructure (RPKI)

faz parte do  MANRS!!!

O que é RPKI?

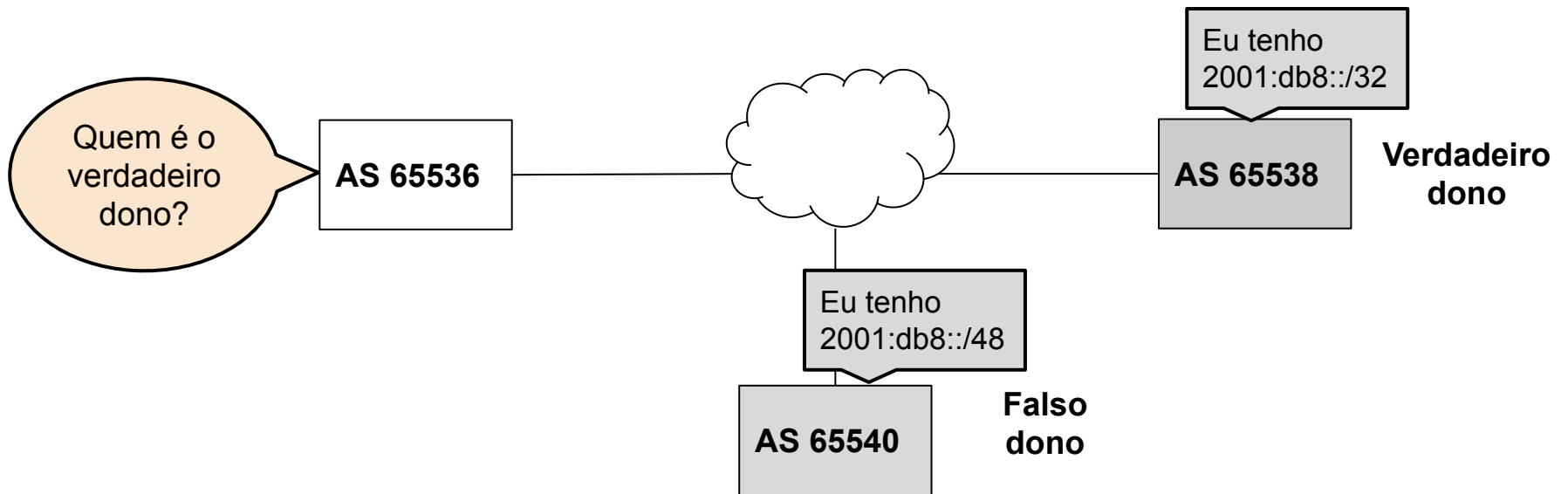
- Estrutura desenvolvida para validar recursos de numeração
 - ASN e Prefixos IPs
 - Alocados
 - Utilizado no BGP
- Previne os problemas de BGP *Hijacking*
- **A colaboração de todos os ASes é essencial!!!**

O que é RPKI?

ROTAS:

2001:db8::/32 ... 65538 i

2001:db8::/48 ... 65540 i

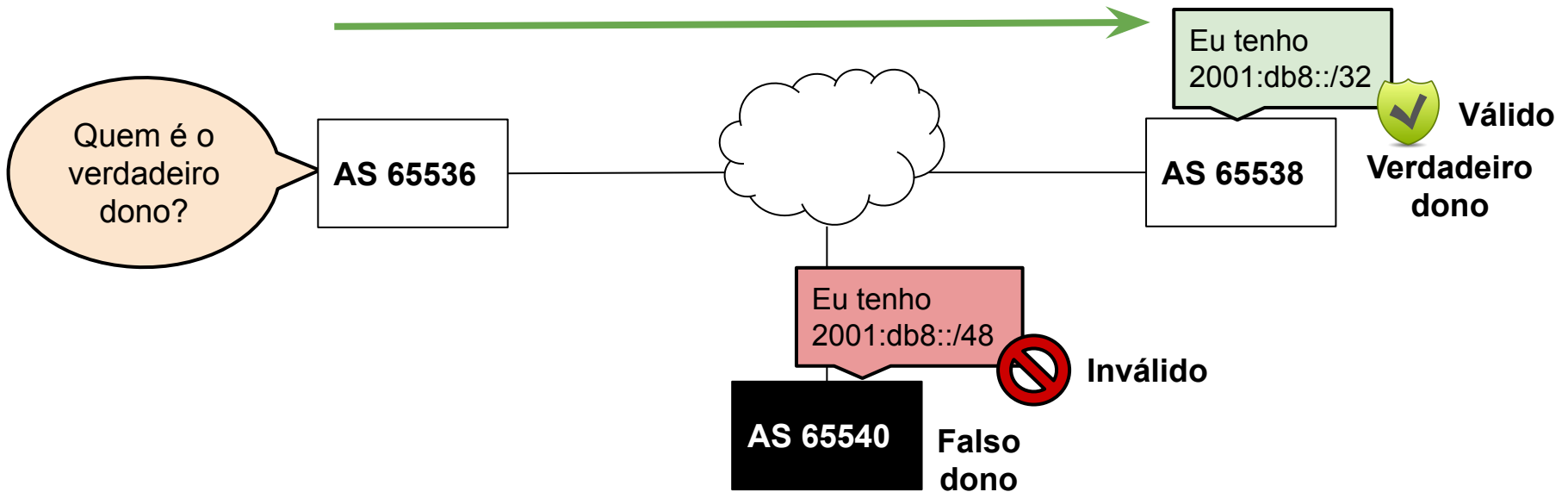


O que é RPKI?

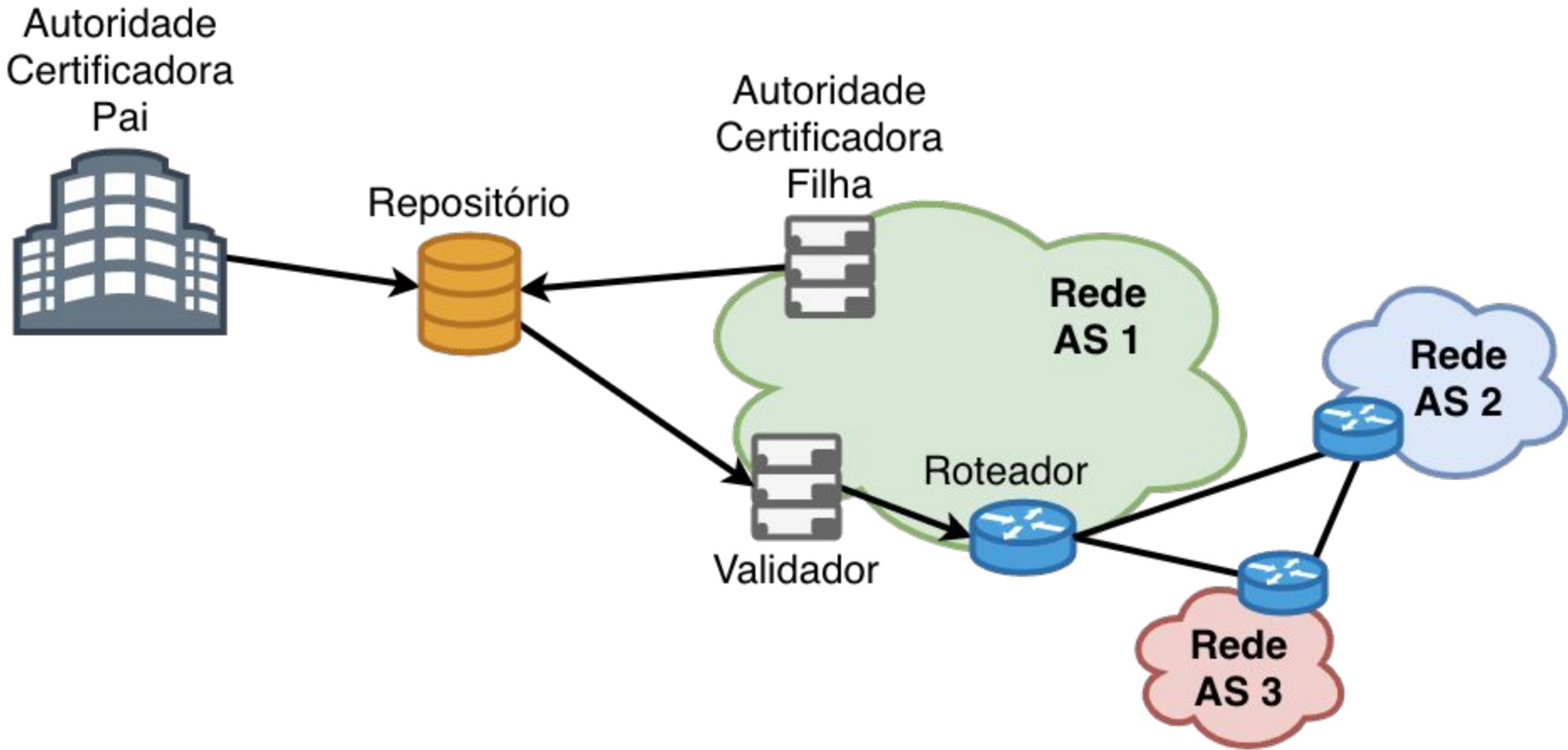
ROTAS:

2001:db8::/32 ... 65538 i

2001:db8::/48 ... 65540 i



Estrutura do RPKI



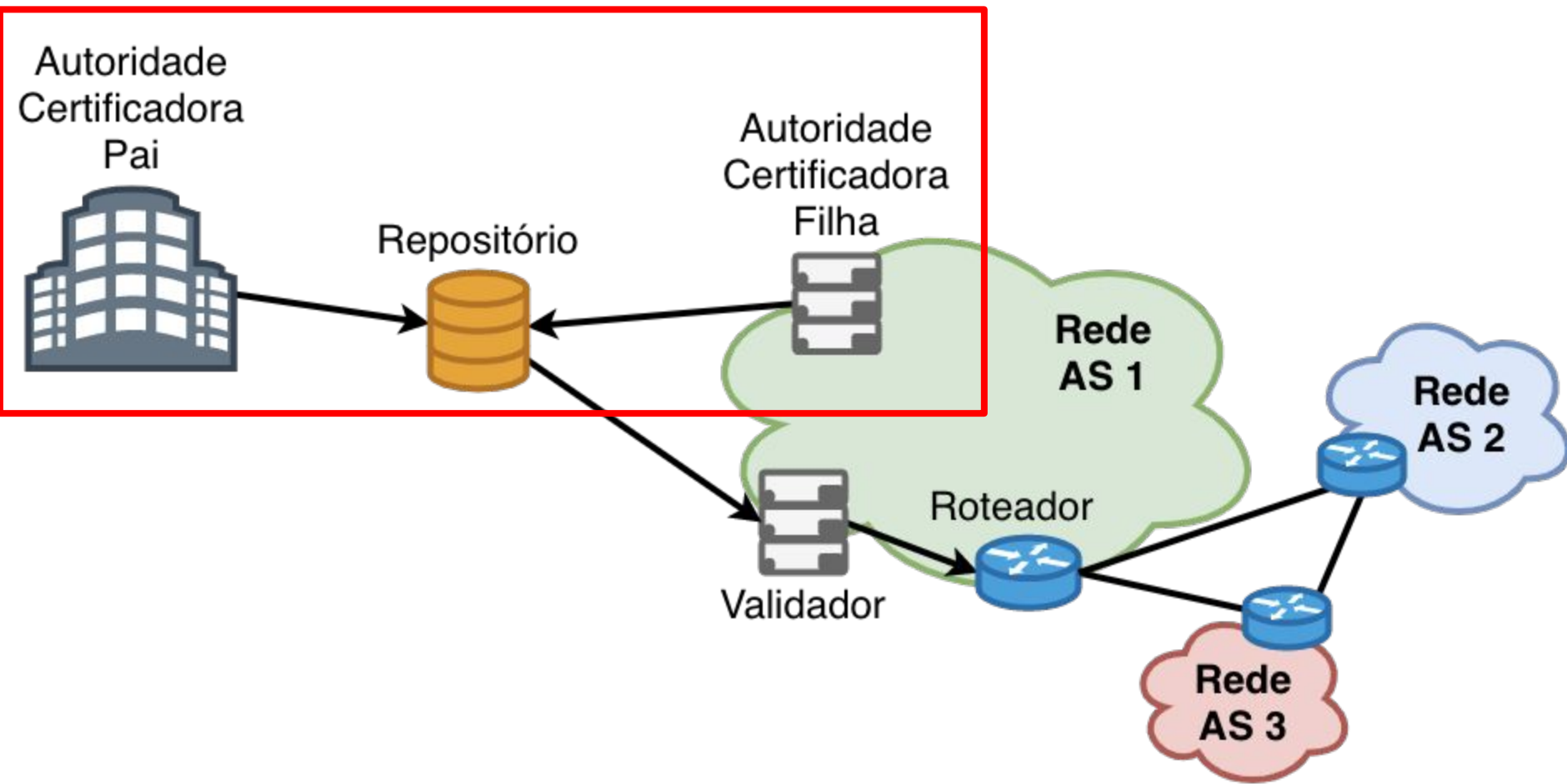
Estrutura do RPKI

Duas partes:

- **Certificação de recursos**
 - Anunciar os prefixos no RPKI
 - Qualquer um que possuir recursos de IP pode aderir
- **Validação da Origem**
 - Consultar prefixos anunciados no RPKI
 - Necessita uso de roteador compatível

Parte I: Certificação de Recursos

Certificação de Recursos

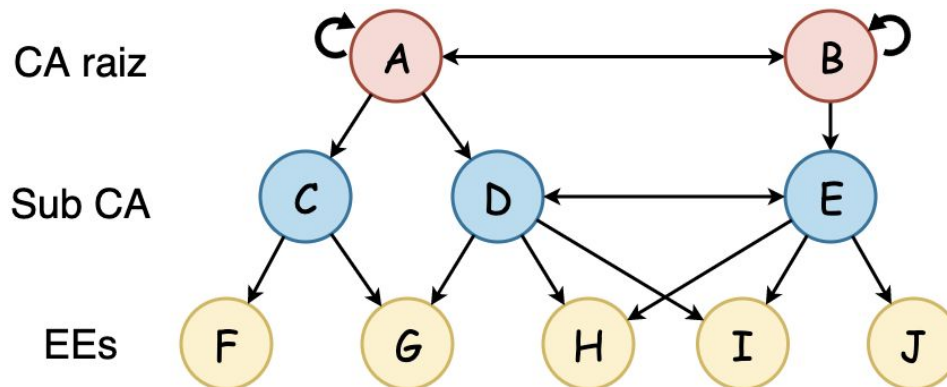


Certificação

- Certificação digital
 - Associa a chave pública com o seu dono
- Modelo **PKI** (***Public Key Infrastructure***)
 - certificado contém chave pública assinada por uma **Autoridade Certificadora** ou **Certificate Authority (CA)**.
 - Ex.: ICP-Brasil
- **RPKI**
 - Certificação de recursos
 - *Associa a chave pública com os recursos*

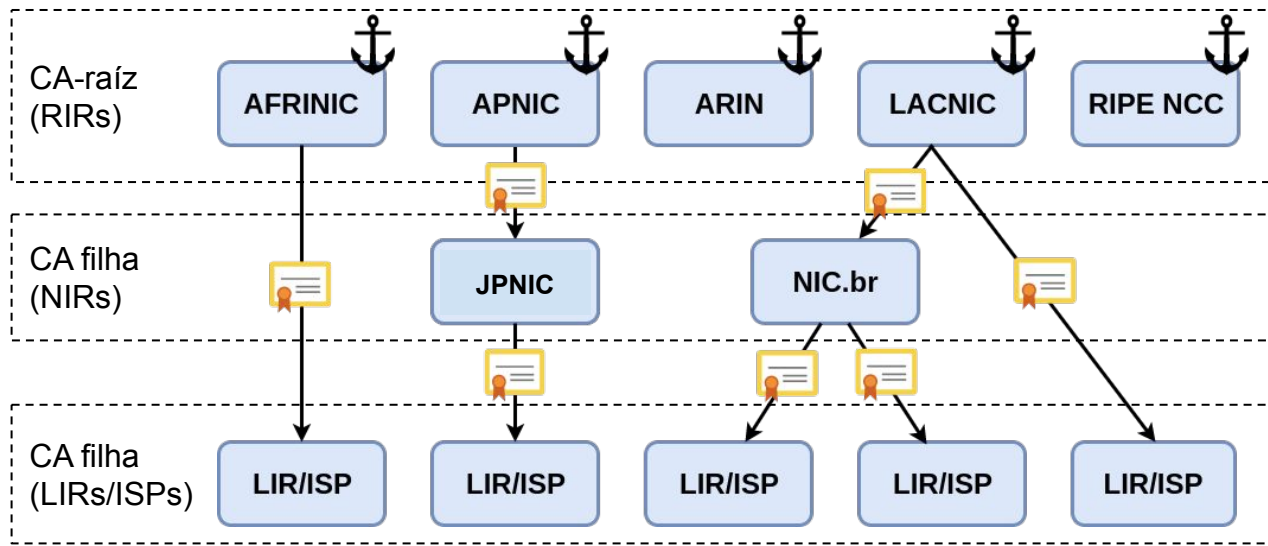
Modelo PKI

- Cadeias de certificação
 - **CA (Certificate Authority)** são entidades **confiáveis** e sua chaves públicas são **amplamente conhecidas!**
 - Usa-se a chave da CA raiz (auto-assinado) para assinar outras chaves na cadeia até as entidades finais ou *End Entities* (EEs).
 - Importante a proteção das chaves mais críticas (mais próximas da raiz).



Cadeia de certificação do RPKI

- RIRs
 - *Trust Anchor*
 - Confiabilidade implícita
 - Certificados auto-assinados
 - Certificam somente os recursos de sua própria hierarquia



Cadeia de certificação do RPKI

Cada **RIR** pode ser uma fonte autoritativa para a alocação de recursos:

- Delegação de endereços IPs (IPv4 e IPv6)
- Delegação de ASNs

Funcionam como CA do par IPs-ASN e da chave pública do AS

ROAs

- *Route Origin Authorisation*
 - Objeto assinado


“Eu autorizo o ASN XXXX a originar esse prefixo”.

Elementos principais:

- Nome da ROA
- Número do AS (ASN)
- Prefixo alocado e máximo permitido
- Tempo de validade
- Assinatura da organização

Responsável pelos recursos

ROA da organização

| | |
|---|---------------|
| ROA | |
| Prefixo | 2001:db8::/32 |
| ASN | 65538 |
| Prefixo Max | /48 |
| Tempo de validade | 1 ano |
| Assinatura da organização | |
|  | |

ROAs

- Todos os prefixos anunciados devem estar cadastrados em um ou mais ROAs
- Assinados e guardados em um repositório RPKI
 - Certificado contendo recursos de numeração
 - Declarações da origem das rotas para esses recursos
- Cada ROA contém apenas um ASN
 - Prefixos podem possuir mais de um ROA

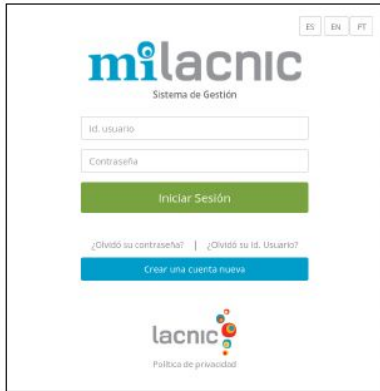
ROAs

- E se uma organização quiser alocar seus recursos para outros ASes?
- Duas opções:
 1. Gerar a ROA para os próprios anúncios do seu ASN
 2. Gerar um certificado CA para outra organização (e.g. AS cliente), então essa gera a própria ROA
- Se existir ROA para o prefixo, a origem da rota é validada
- Publicar ROA incorreta é pior do que não publicar!

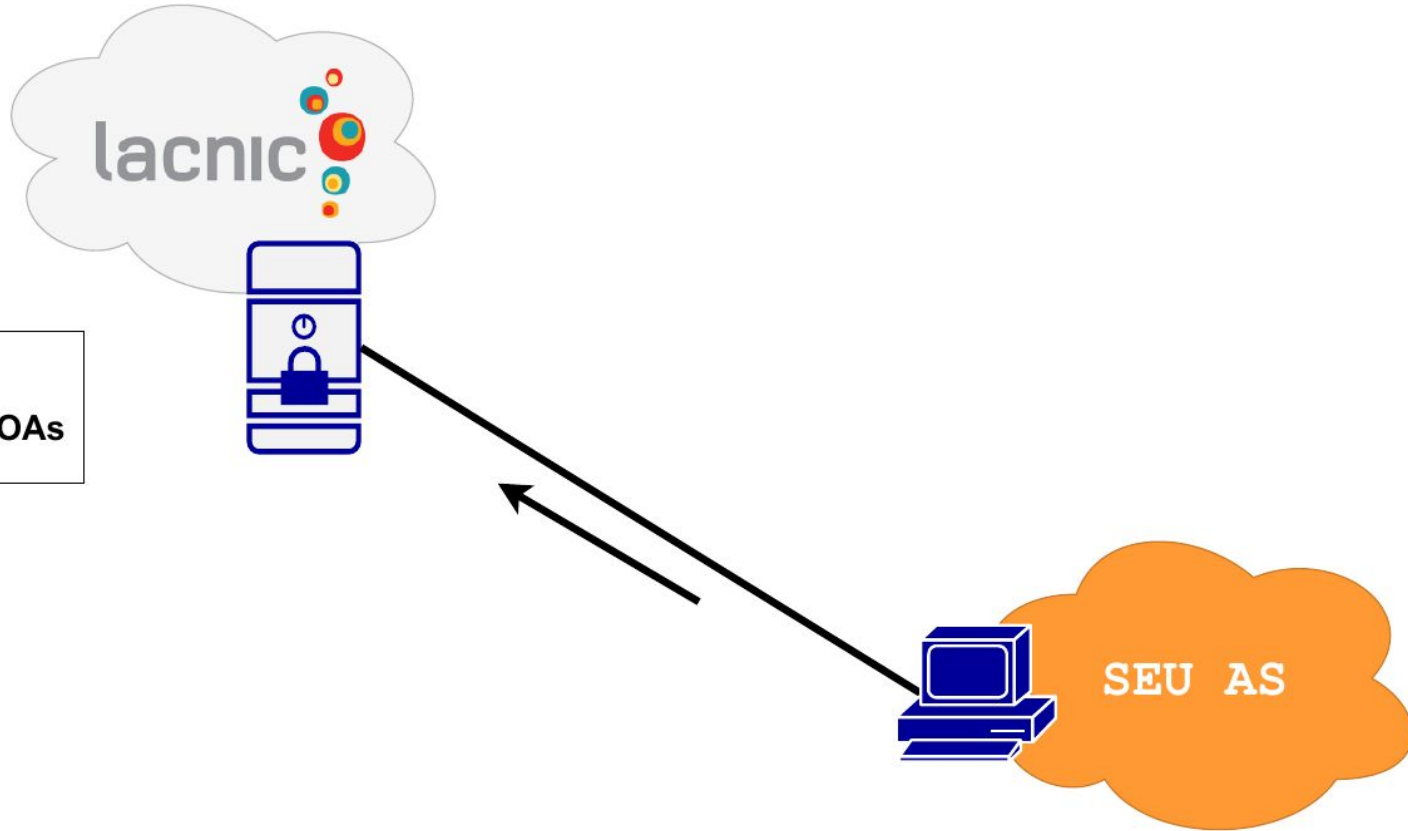
Modos de operação no RPKI

- Existem dois modos de operação no RPKI:
 - **Modo hospedado**
 - LACNIC
 - **Modo delegado**
 - NIC.br

Modo Hospedado



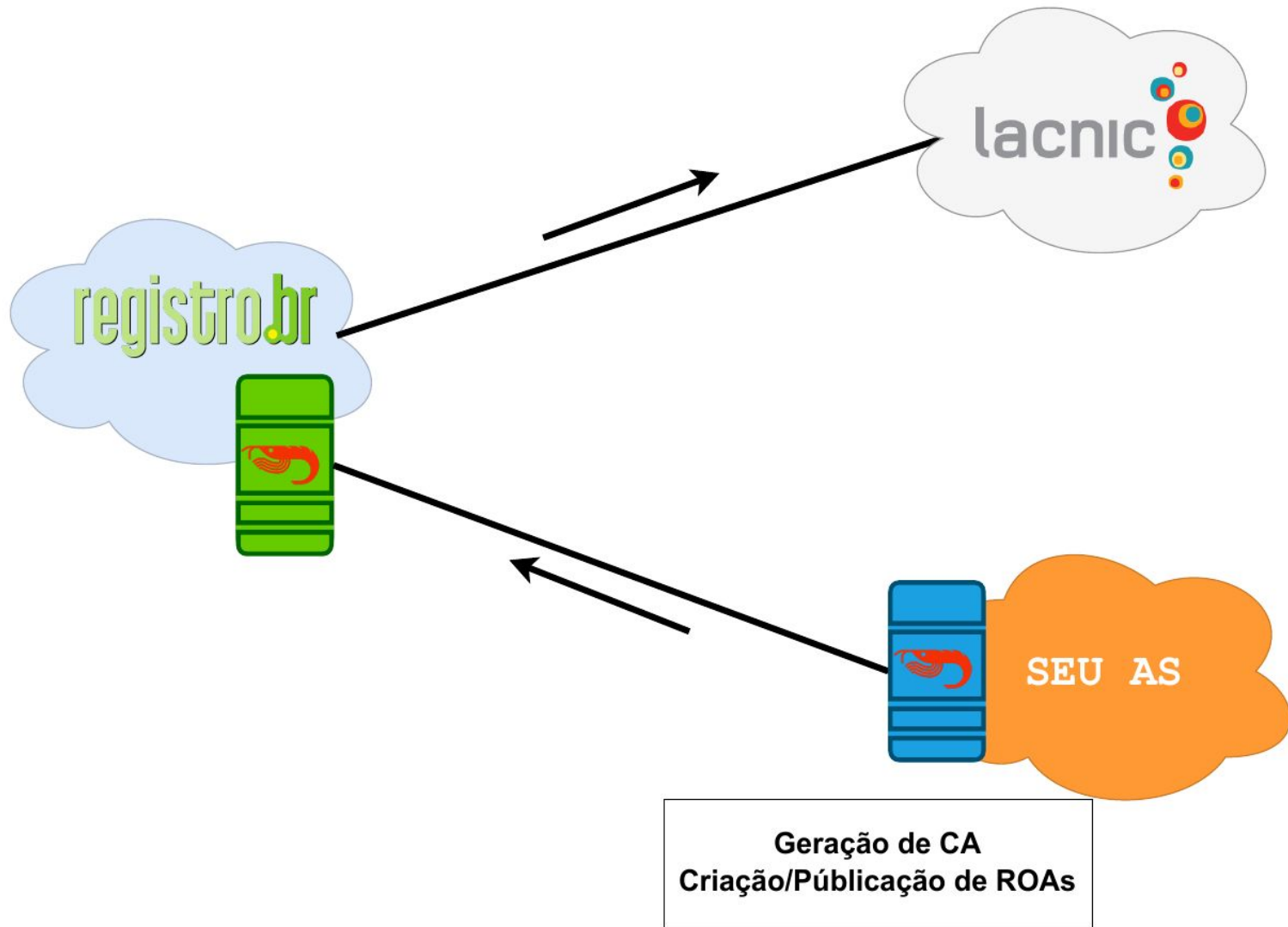
**Geração de CA
Criação/Publicação de ROAs**



Modo Hospedado

- Incentivar a adoção do RPKI
- RIRs
 - Emitem e armazenam os certificados de recursos
 - Armazenam as chaves públicas e privadas
 - Oferecem interface web para os participantes
- AS depende do RIR para realizar suas ações no RPKI

Modo Delegado



Modo Delegado

- Sistema distribuído de CAs
 - Foi desenhado para ser assim
- Facilita a automatização
- Centraliza o gerenciamento das ROAs na organização dona dos recursos
- Controle da chave privada pelo AS
- Permite delegar CAs filhos para clientes
- AS tem mais autonomia no RPKI

Modo Delegado

- **Protocolo UpDown**

- Geração e validação do repositório
- Cada CA armazena a própria chave privada
- Envia seus certificados para assinatura da CA pai
- Publicação de certificados e ROAs
 - Repositório próprio ou de terceiros

Modo Delegado

O que eu preciso?

- **Software CA**
 - Krill - NLnet Labs
- **Servidor de publicação**
 - Servidor proprio (alta disponibilidade)
 - Servidor de terceiros (NIC.br)

O que é o Krill ?

- *Software open source*
 - Criação, gerenciamento, publicação de CAs e ROAs
- Possui repositório próprio, mas permite a utilização de repositório de terceiros
- Funciona por linha de comando e por interface gráfica para usuário

Servidor Krill ?

- **É de extrema importância manter seu servidor Krill sempre ativo!**
 - Documentos do RPKI possuem prazo de validade
 - Atualizações automáticas e periódicas desses documentos são feitas pelo protocolo UpDown
 - Se o servidor Krill ficar inacessível e os documentos expirarem, as rotas **válidas** podem passar a ser consideradas **desconhecidas**

Repositório RPKI

- Armazenam
 - **Resource Certification** -
 - Certificados X.509 + extensão para IPs e ASNs (RFC 3779)
 - **Certificate Revocation List (CRL) - RFC 5280**
 - **Manifests (RFC 6486)**
 - Lista de documentos assinados por um AS
 - **Route Origin Authorisation (ROA) - RFC 6482**
 - Contém a lista de prefixos que podem ser anunciados por um ASN

Manutenção é essencial!

Não esqueça do RPKI!

**Atualize as ROAs
quando mudar os
anúncios!**



nusenu
@nusenu_

On 2018-11-12 @Orange_France AS3215 replaced multiple /16 BGP announcements with /17s, unfortunately they didn't update their #RPKI ROAs causing big junks of IP space to become RPKI-unreachable.

This increases the RPKI unreachable IP space to >10k /24s

nusenu.github.io/RPKI-Observato...



11:18 AM - 16 Nov 2018

Como verificar existencia de ROAs

```
$ whois -h whois.bgpmon.net 200.160.0.0
```

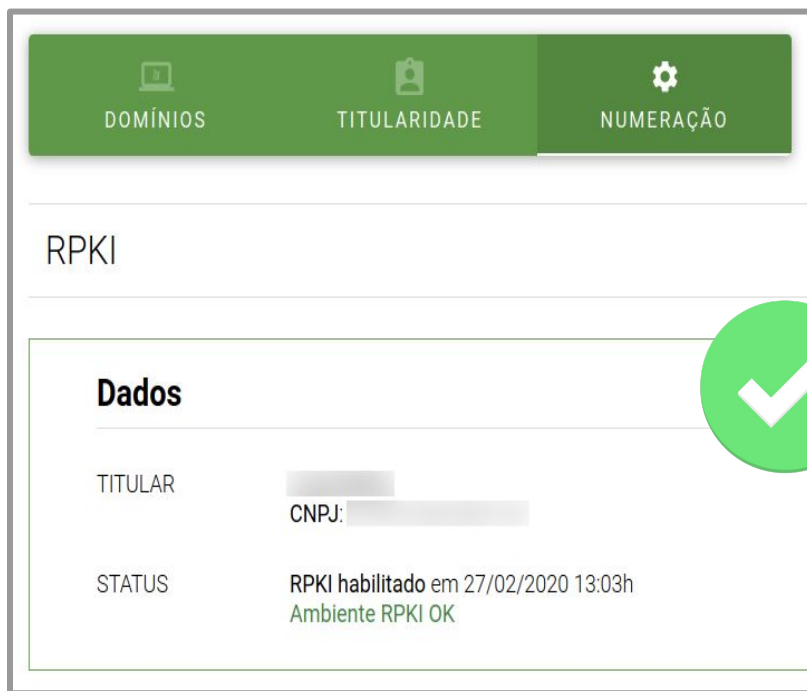
```
Prefix:                200.160.0.0/20
Prefix description:    Registro.BR Network
Country code:         BR
Origin AS:             22548
Origin AS Name:        N?cleo de Inf. e Coord. do Ponto BR
- NIC., BR
RPKI status:           ROA validation successful
First seen:            2011-10-19
Last seen:             2019-12-11
Seen by #peers:        66
```

Visualizando uma ROA

```
$ whois -h whois.bgpmon.net " --roa 22548
200.160.0.0/22"
0 - Valid
-----
ROA Details
-----
Origin ASN:          AS22548
Not valid Before:    2019-12-12 17:20:05
Not valid After:     2020-12-12 17:25:05 Expires in
1y14h24m2.60000000149012s
Trust Anchor:        rpki-repo.registro.br
Prefixes:            200.160.0.0/20 (max length /24)
```

Monitoramento do RPKI pelo Registro.br

Para ajudar nessa fase inicial da implantação do RPKI, o Registro.br disponibilizou um serviço de monitoramento que informa se suas configurações de RPKI estão corretas.



The screenshot shows the 'NUMERAÇÃO' tab selected in the top navigation bar. Below the navigation bar, the text 'RPKI' is displayed. Under the 'Dados' section, the following information is shown:

| | |
|---------|--|
| TITULAR | [Redacted] |
| CNPJ: | [Redacted] |
| STATUS | RPKI habilitado em 27/02/2020 13:03h Ambiente RPKI OK |

A large green checkmark icon is overlaid on the right side of the screenshot, indicating a successful configuration.



The screenshot shows the 'NUMERAÇÃO' tab selected in the top navigation bar. Below the navigation bar, the text 'RPKI' is displayed. Under the 'Dados' section, the following information is shown:

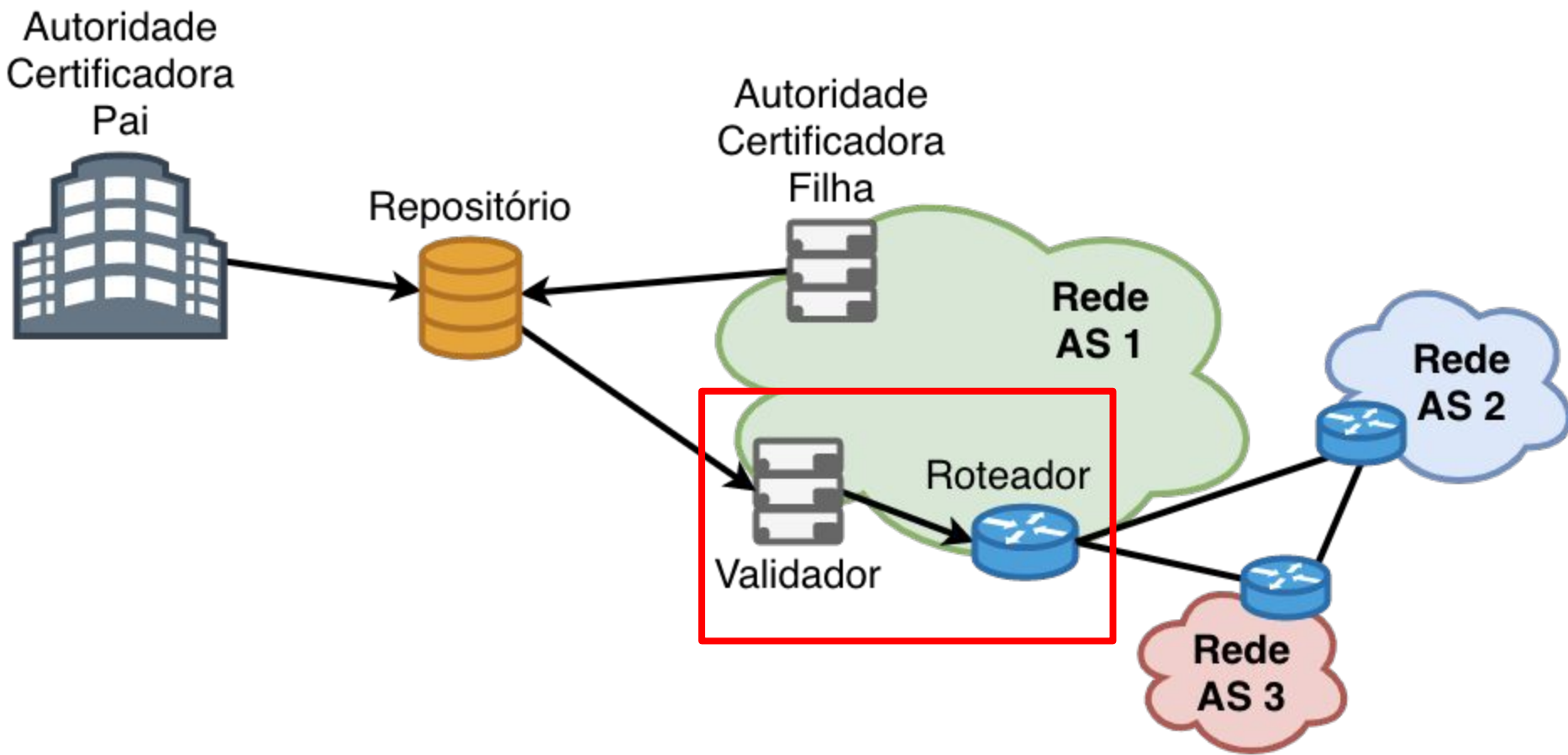
| | |
|---------|--|
| TITULAR | [Redacted] |
| CNPJ: | [Redacted] |
| STATUS | RPKI habilitado em 27/02/2020 13:03h ⚠ Ambiente RPKI com inconsistências* desde 03/03/2020 15:50h • Publicação RPKI em atraso. <small>*Última verificação em 03/03/2020 15:50h</small> |

A large yellow warning triangle icon with a black exclamation mark is overlaid on the right side of the screenshot, indicating an issue with the RPKI configuration.

Laboratório I: **Instalação e Configuração** **Krill**

Parte II: Validação da Origem

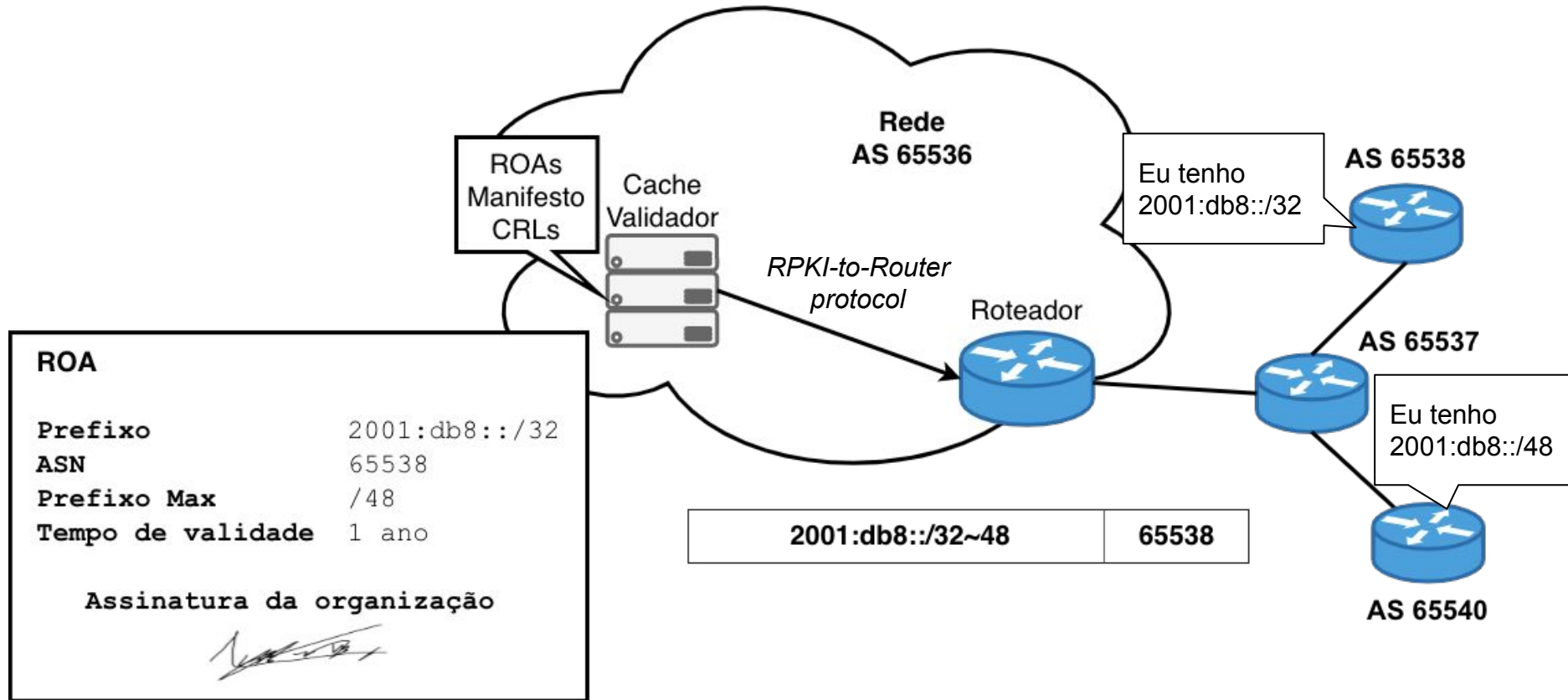
Validação da Origem



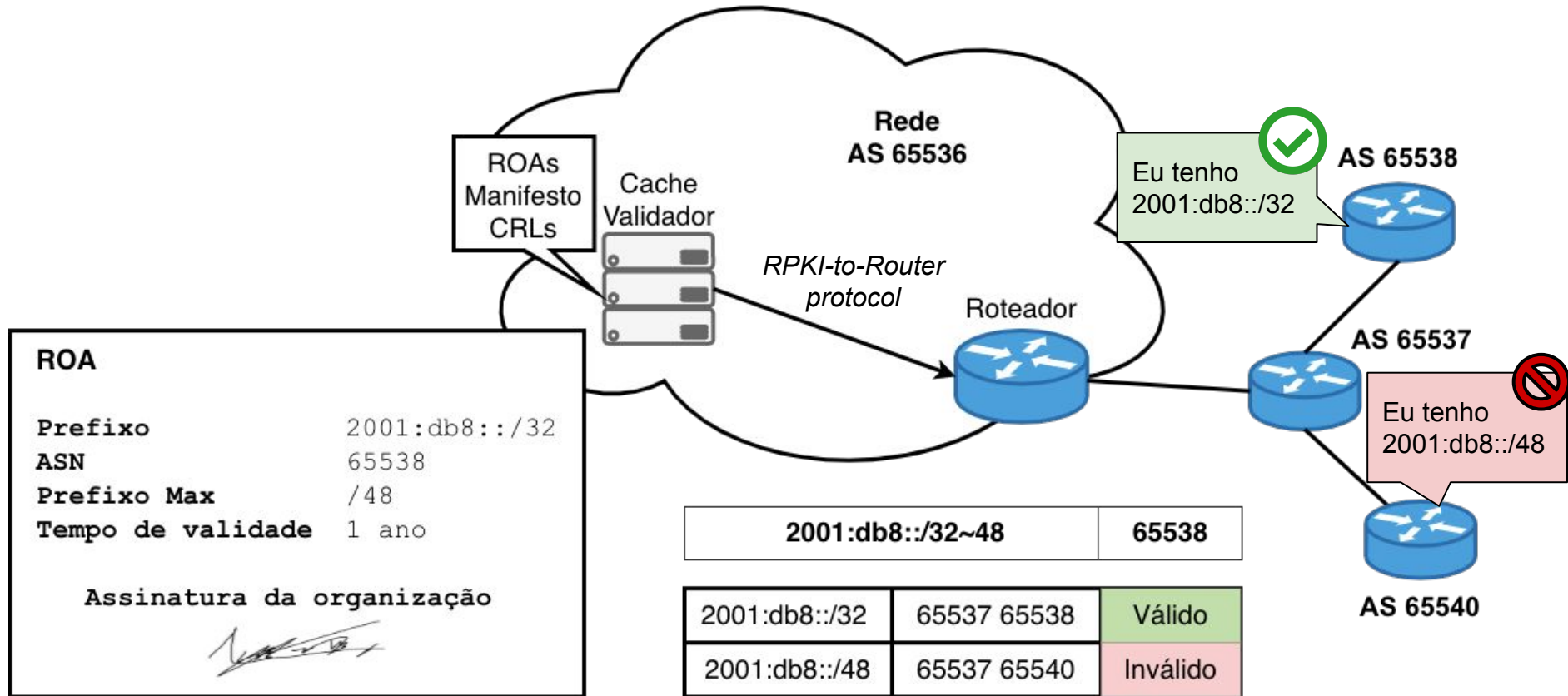
Validação da Origem

- **Validador**
 - Validação dos objetos certificados
 - Software que acessa fontes confiáveis e cria um cache da informação validada
- **Roteador**
 - Validação das rotas
 - BGP habilitado para usar o RPKI
 - Obtém informações do validador e utiliza para influenciar o roteamento

Validação da Origem



Validação da Origem



Roteador

Exemplo:

| | AS de Origem | Prefixo | Prefixo Max. |
|-----|---------------------|----------------|---------------------|
| ROA | 65536 | 10.0.0.0/16 | /18 |

| | | |
|--------------|-------|---------------|
| Válida | 65536 | 10.0.128.0/17 |
| Inválida | 65536 | 10.0.0.0/24 |
| Desconhecido | 65540 | 10.0.0.0/8 |

Validador

- Conexão com repositórios confiáveis (RIPE, LACNIC,...)
 - Rsync ou RPKI Repository Delta Protocol (RRDP)
- Cache
 - Atualizações periódicas
- Validação
 - Verificação das assinaturas dos ROAs e certificados
 - Geração de **Verified ROA Payloads (VRP)**
- Envia **VRPs** para o roteador usando o protocolo **RPKI-to-Router (RTR)**

Validador

- Existem vários softwares disponíveis:
 - **ROUTINATOR**
 - FORT (LACNIC)
 - **RIPE validator**
 - RTRlib (bird, FRR, Quagga...)
 - **OctoRPKI & GoRTR (Cloudflare)**
- *Trust Anchor Locator* (TAL) já vem incorporados
 - Localizador para os 5 RIRs

Roteador

- Recebem VRPs do validador e utilizam para tomar decisões de roteamento
- Uma rota pode ser classificada como:
 - **Válida**: A origem e o prefixo máximo estão de acordo com a informação do ROA
 - **Inválida**: A informação não está de acordo com o ROA
 - **Desconhecido**: Não existe ROA para o prefixo verificado

Roteador

- Suporte a validação na origem
- Hardware
 - Juniper
 - Junos versão 12.2 e superiores
 - Cisco
 - IOS release 15.2 e superiores
 - Cisco IOS/XR desde a 4.3.2
 - Nokia
 - Release R12.0R4 e superiores rodando no 7210 SAS, 7750 SR, 7950 XRS ou VSR.

Roteador

- Existem vários softwares com suporte a RPKI:
 - BIRD
 - OpenBGPD
 - FRRouting
 - GoBGP
 - VyOS

Fonte: <https://rpki.readthedocs.io/en/latest/rpki/router-support.html>

Roteador

- Políticas de roteamento podem ser estabelecidas em cima da validação das rotas
 - Alterar preferências
 - Atribuir *communities*
 - Aplicar filtros

Colaboração é essencial: Adoção do RPKI



% valid Prefix/Origin AS pairs

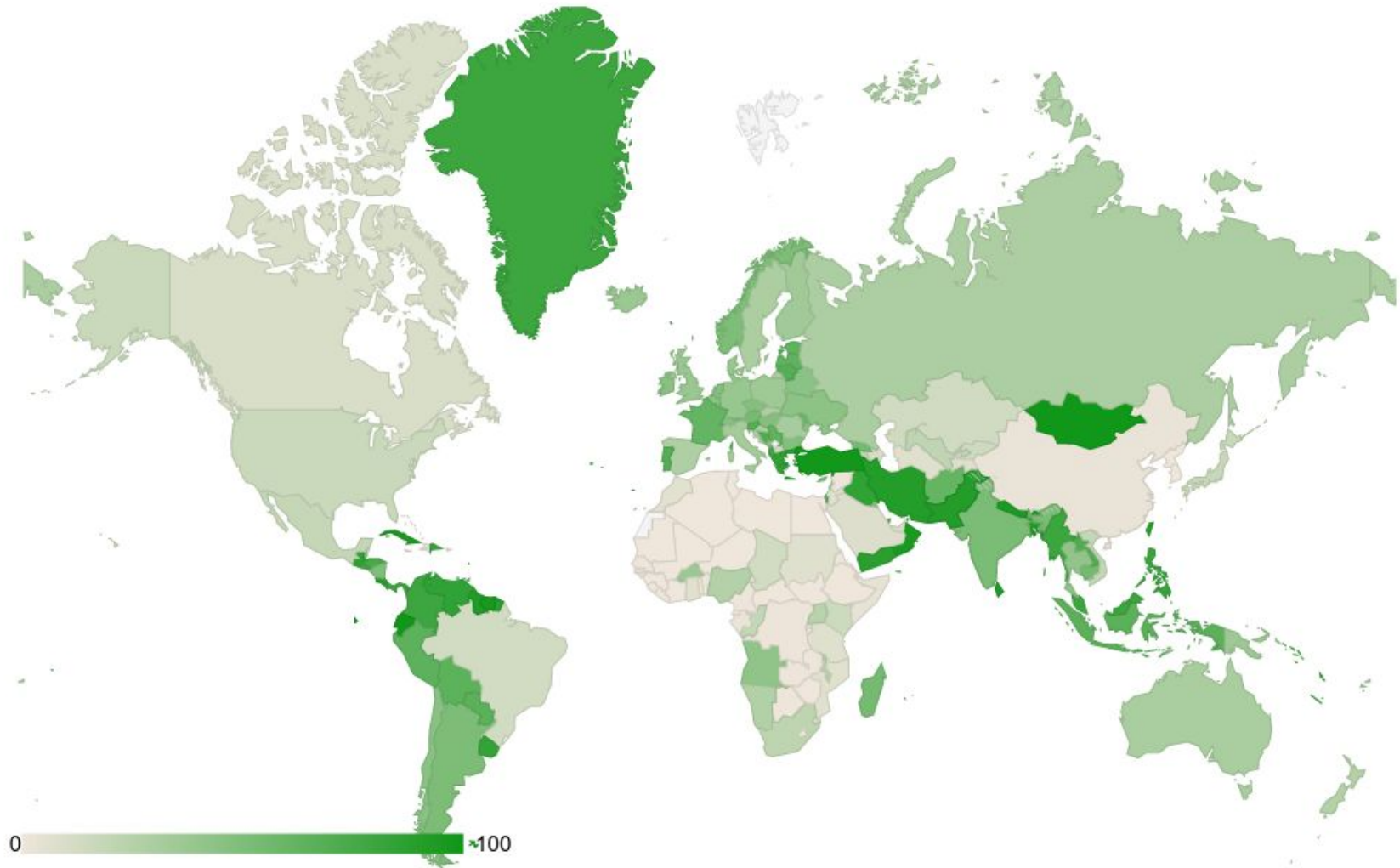


0 20 40 60

Highcharts.com © Natural Earth

Fonte: https://monitor.fortproject.net/en/rpki_map

Colaboração é essencial: Adoção do RPKI

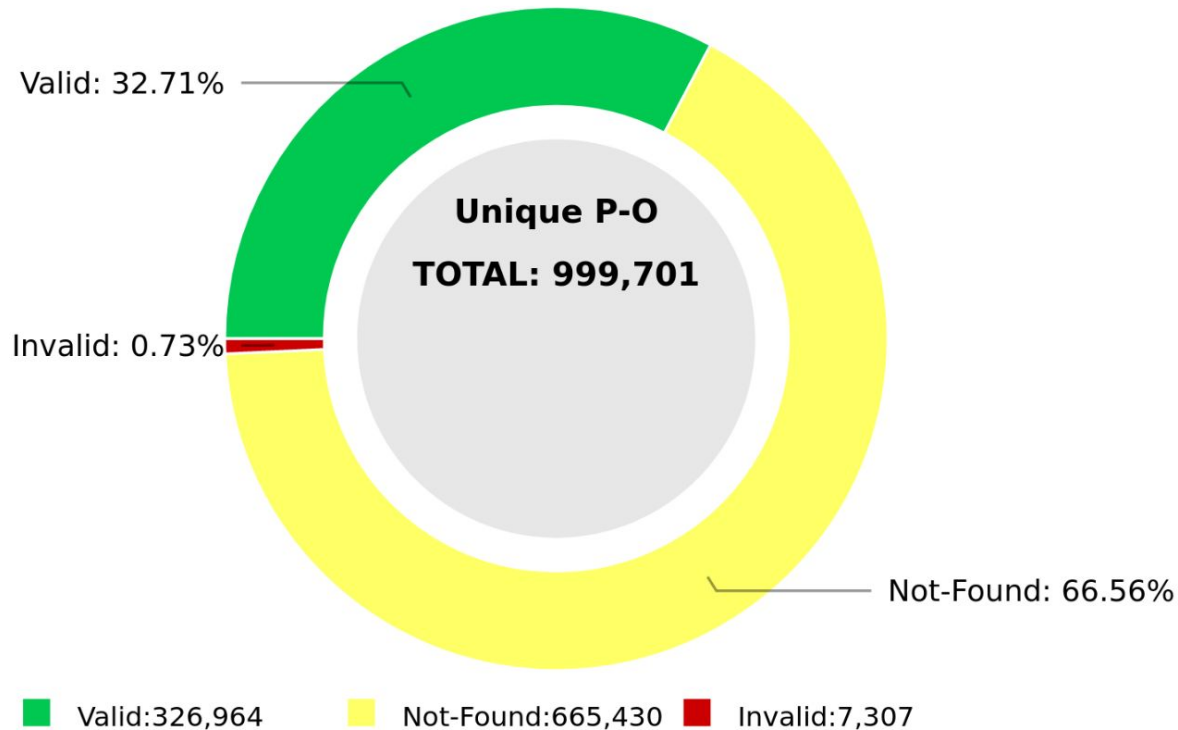


Fonte: <https://lirportal.ripe.net/certification/content/static/statistics/world-roas.html>

Validação de Rotas

Análise da tabela completa do BGP em relação aos prefixos anunciados nos RPKIs

RPKI-ROV Analysis of Unique Prefix-Origin Pairs (IPv4)



NIST RPKI Monitor RPKI-ROV Analysis

Protocol: IPv4

RIR: All

Date: 2021-11-11 06:00

Fonte: <https://rpki-monitor.antd.nist.gov/?p=0&s=0>

Laboratório II:
Instalação e Configuração
Routinator

Saiba mais



<https://www.youtube.com/watch?v=A6F3OswNyh8>

Saiba mais



<https://www.youtube.com/watch?v=jSvMCjPoFME>

Saiba mais

SEMANA DE CAPACITAÇÃO 3
EDIÇÃO ON-LINE

RPKI: APRENDA COM QUEM DESENVOLVEU OS VALIDADORES

1º DE OUTUBRO, ÀS 9H (UTC -3)
semanacap.bcp.nic.br

ceptro.br nic.br cgi.br

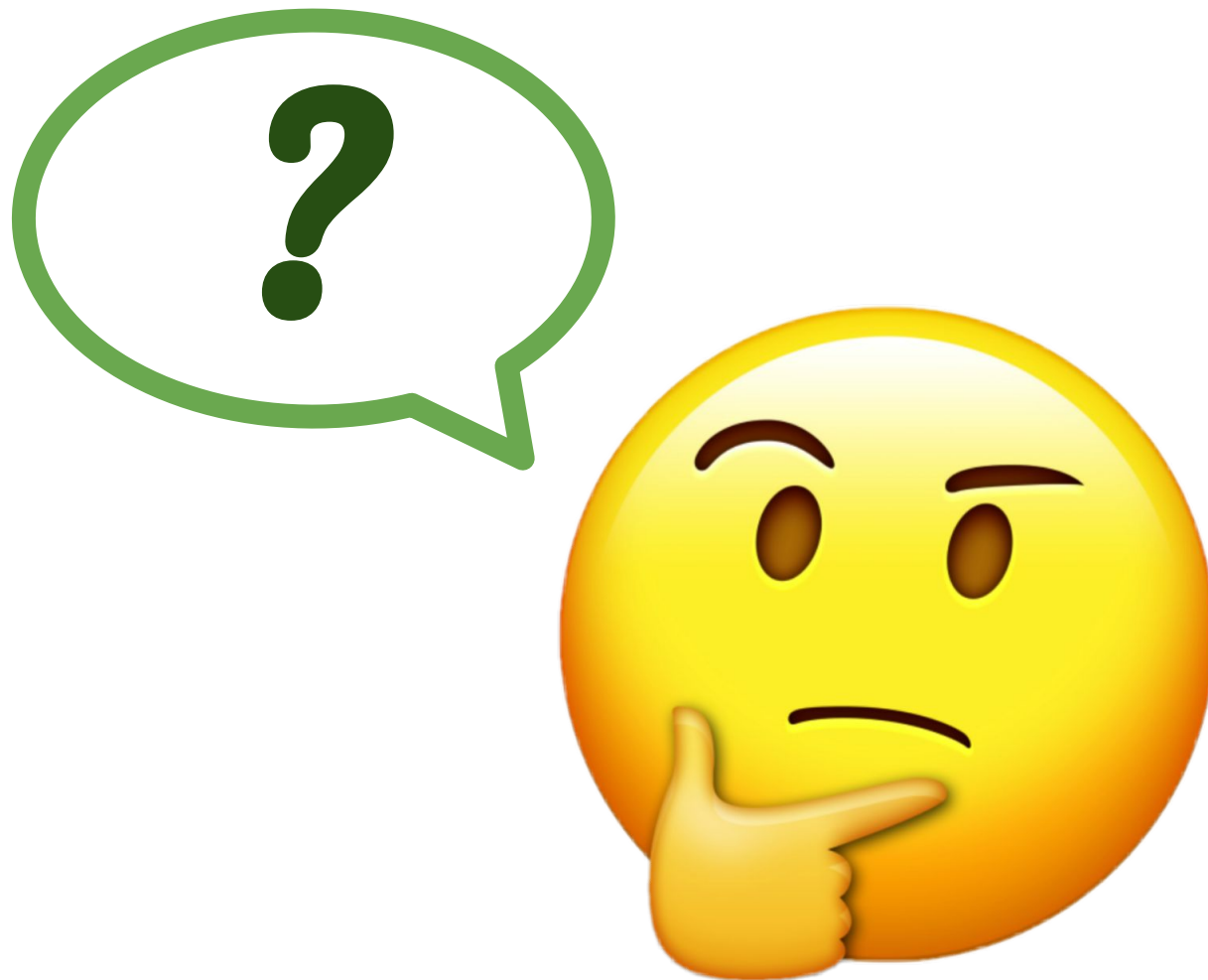
nic.br

0:00 / 3:30:47 • Abertura >

YouTube player controls: play, next, volume, settings, full screen, and share icons.

<https://www.youtube.com/watch?v=mvQ2GxslhKo>

Dúvidas??



Obrigado !!!

Equipe de cursos do CEPTRO.br

@cursosceptro@nic.br

@hostmaster@registro.br

nic.br **cgi.br**

www.nic.br | www.cgi.br