



**nie.br**

Núcleo de Informação  
e Coordenação do  
Ponto BR

**egi.br**

Comitê Gestor da  
Internet no Brasil

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

nic.br egi.br

registro.br

IX Fórum Regional Edição Especial On-line  
São Paulo, SP | 20/3/20

# PROGRAMA POR UMA INTERNET MAIS SEGURA

**A segurança da sua rede depende da segurança de todos**

Gilberto Zorello | [gzorello@nic.br](mailto:gzorello@nic.br)

registro.br nic.br cgi.br

# Nossa Agenda

- **CGI.br e NIC.br**
- Panorama atual
- **Ataques à infraestrutura mais frequentes**
- Programa por uma Internet mais segura



1 2 3 4 5 6 7 8 9

GOVERNO

10 11 12 13 14 15 16 17 18 19 20 21

SOCIEDADE CIVIL

e

### Representantes do Governo:

- 1 Ministério da Ciência, Tecnologia e Inovação (coordenador)
- 2 Casa Civil da Presidência da República
- 3 Ministério das Comunicações
- 4 Ministério da Defesa
- 5 Ministério do Desenvolvimento, Indústria e Comércio Exterior
- 6 Ministério do Planejamento, Orçamento e Gestão
- 7 Agência Nacional de Telecomunicações
- 8 Conselho Nacional de Desenvolvimento Científico e Tecnológico
- 9 Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

### Representantes da Sociedade Civil:

- 10 Notório saber em assunto da Internet
- 11 a 14 Representantes do setor empresarial
  - provedores de acesso e conteúdo da Internet
  - provedores de infra-estrutura de telecomunicações
  - indústria de bens de informática, de bens de telecomunicações e de software
  - setor empresarial usuário
- 15 a 18 Representantes do terceiro setor
- 19 a 21 Representantes da comunidade científica e tecnológica

membros e ex-membros do CGI.br  
(somente os atuais membros têm direito a voto) ➡

# ASSEMBLEIA GERAL

## Organograma do NIC.br

7 membros eleitos pela Assembleia Geral ➡

**CONSELHO DE  
ADMINISTRAÇÃO**

**CONSELHO  
FISCAL**

ADMINISTRAÇÃO  
.....  
JURÍDICO  
.....  
COMUNICAÇÃO  
.....  
ASSESSORIAS:  
CGI.br e PRESIDÊNCIA

**DIRETORIA  
EXECUTIVA**

1 2 3 4 5

**registro.br**

Domínios

**cert.br**

Segurança

**cetic.br**

Indicadores

**ceptro.br**

Redes e Operações

**ceweb.br**

Tecnologias Web

**ix.br**

Troca de Tráfego

**W3C**  
Brasil

Padrões Web

- 1 Diretor presidente
- 2 Diretor administrativo e financeiro
- 3 Diretor de serviços e de tecnologia
- 4 Diretor de projetos especiais e de desenvolvimento
- 5 Diretor de assessoria às atividades do CGI.br

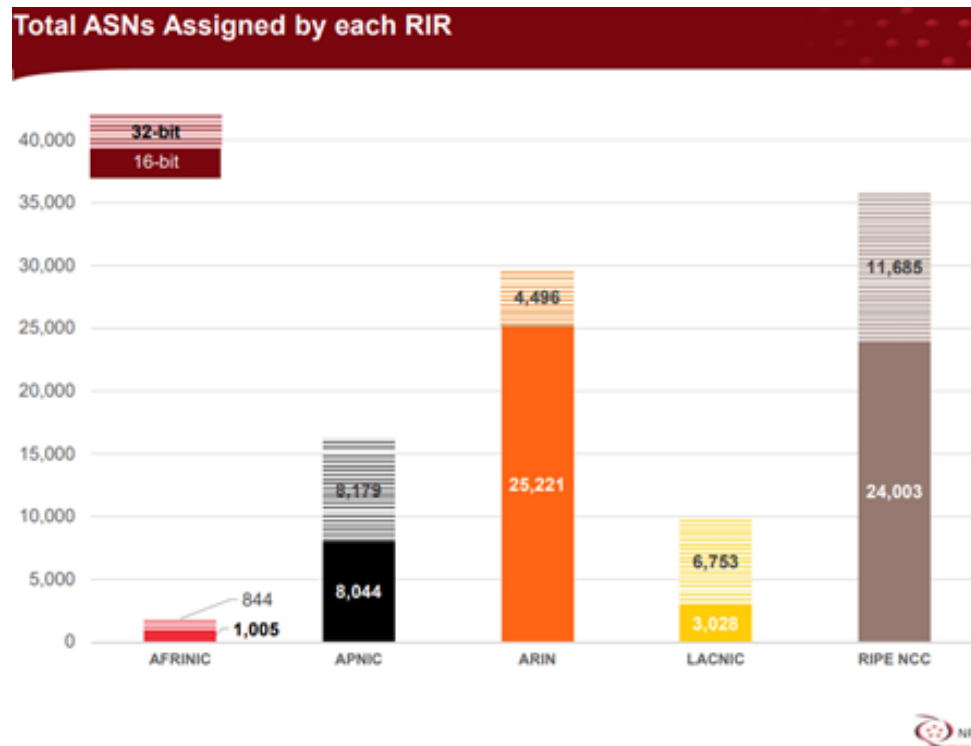
# Panorama atual

# Segurança e estabilidade da Internet

## Estrutura da Internet atual

A Internet funciona com base na cooperação entre Sistemas Autônomos

- É uma “rede de redes”
- São mais de **93.000 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
- **Resultado: não há um dia em que não ocorram incidentes de Segurança na Internet**



# O BGP não tem Validação para os dados

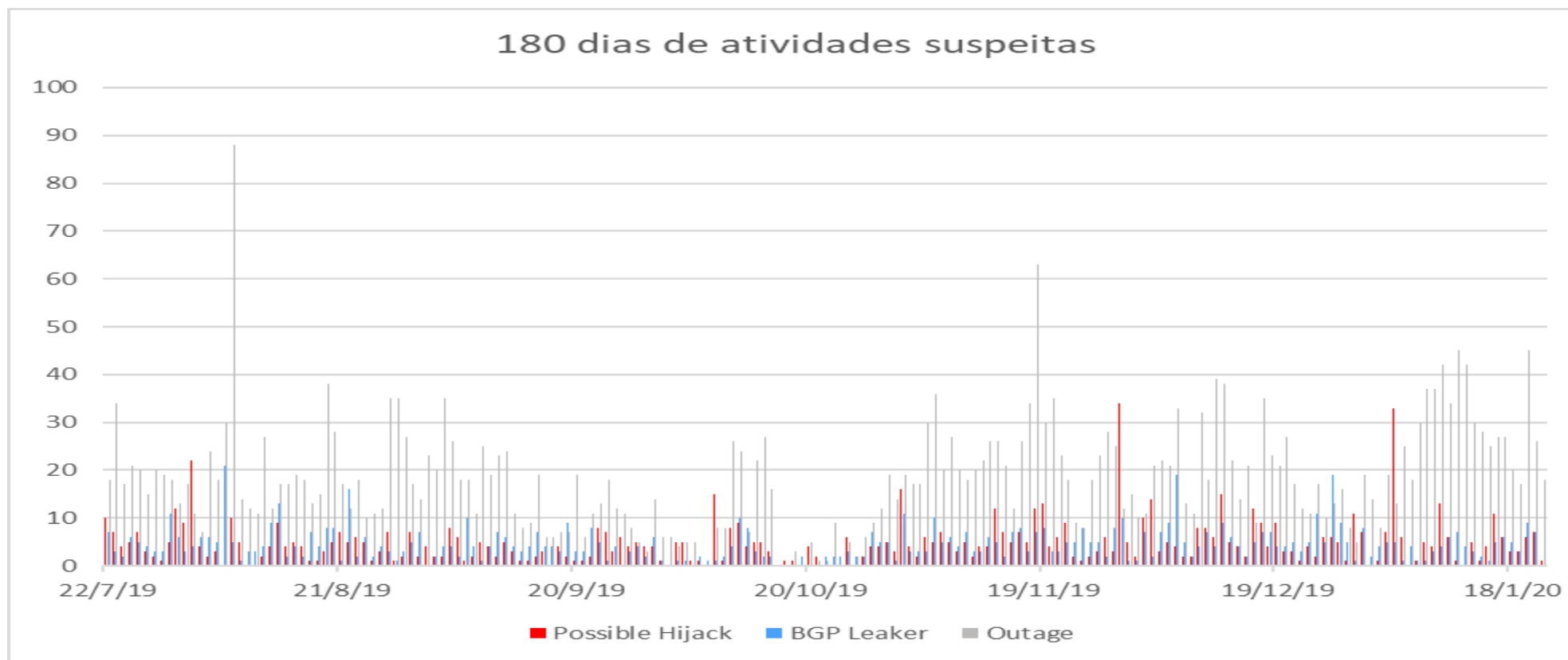
The collage features several news snippets from CNET and CSO:

- CNET Article:** "How Pakistan knocked YouTube offline (and how to make sure it never happens again)". Subtitle: "Large scale BGP hijack out of India".
- CNET Article:** "Routing Leak briefly takes down Google".
- CNET Article:** "Massive route leak causes internet slowdown".
- CNET Article:** "Global Collateral Damage of TMnet leak".
- CNET Article:** "DDoS Attacks Storm Linode Servers Worldwide".
- CNET Article:** "On-going BGP Hijack Targets Palestinian ISP".
- CNET Article:** "UK traffic diverted through Ukraine".
- CNET Article:** "BGP hijack incident by Syrian Telecommunications".
- CNET Article:** "The Vast World of Fraudulent Routing".
- Table:** "Global Impacts of Rece" (likely Receptions). It lists BGP Leak events with details on Origin AS, Leaker AS, and Start time.
- CSO Article:** "DDoS attack on BBC may have been biggest in history".

Event type	Country	ASN	Start time
BGP Leak		Origin AS: PO box T511 Phonexay road - Xaysettha district (AS 131267) Leaker AS: Viettel Corporation (AS 7552)	2016-01-13 12:25:47
BGP Leak		Origin AS: Lirex net EOOD (AS 8262) Leaker AS: Traffic Broadband Communications Ltd. (AS 48452)	2016-01-13 12:11:26

# Segurança e estabilidade da Internet

## Nenhum dia sem um incidente



Fonte: <https://bgpstream.com/>

# Segurança e estabilidade da Internet

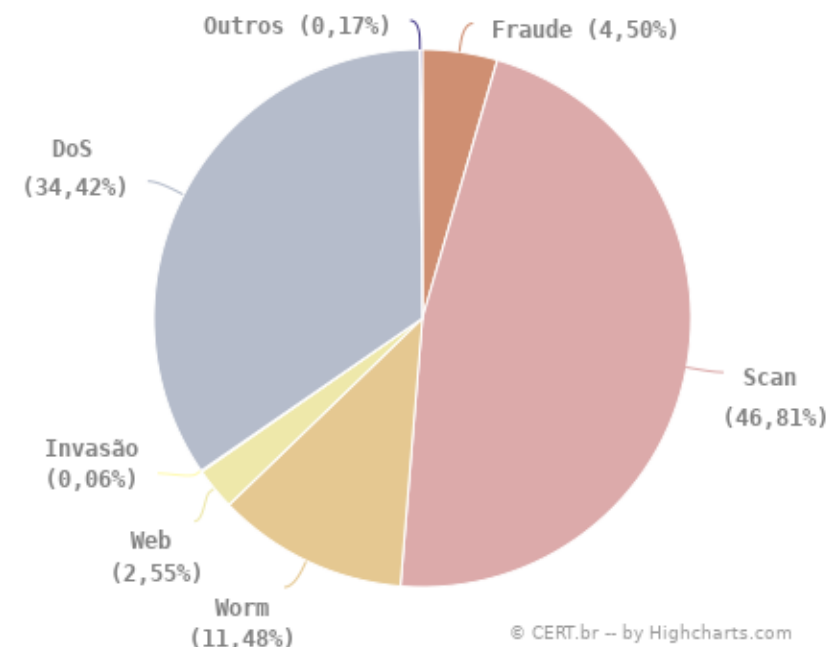
## Panorama Atual

Ataques à infraestrutura e aos serviços disponíveis na Internet estão cada vez mais comuns

O NIC.br analisa a tendência dos ataques com dados obtidos por:

- Incidentes de segurança reportados ao CERT.br
- **Medições em “honeypots” distribuídos na Internet**
- Medições no IX

**Incidentes Reportados ao CERT.br  
Janeiro a Dezembro de 2019**  
Tipos de ataque



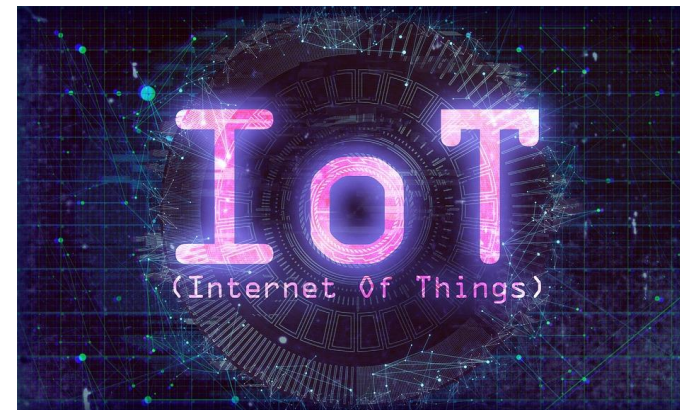
<https://www.cert.br/stats/incidentes/2019-jan-dec/tipos-ataque.html>

**Constata-se um ritmo crescente de notificações de varreduras e DoS [6]**

# Segurança e estabilidade da Internet

## IoT – Internet of Things

- Segundo a Gartner é esperado que 20 bilhões de coisas estejam conectadas à Internet em 2020
- **Segundo a Cisco é esperado que 500 bilhões de dispositivos estejam conectados à Internet em 2030**
- Nossas redes estão preparadas para esta tecnologia?
- **Como estamos em relação à segurança ?**

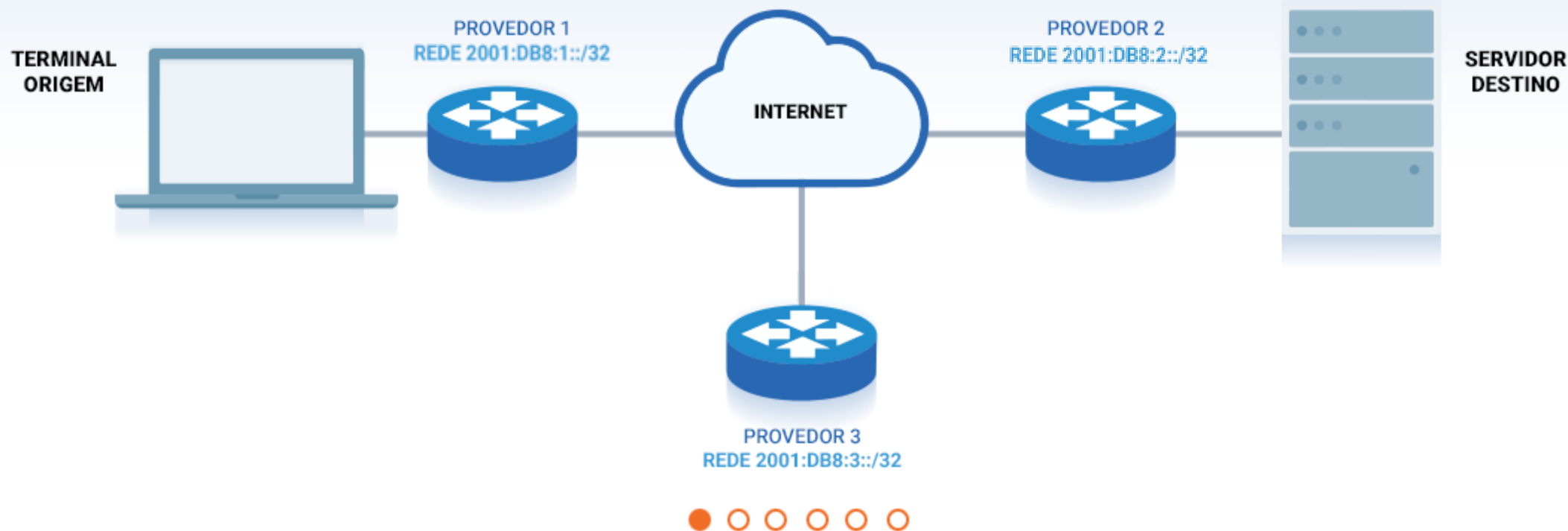


# Ataques mais frequentes na infraestrutura da rede

# Segurança e estabilidade da Internet

## Ataque DoS por reflexão

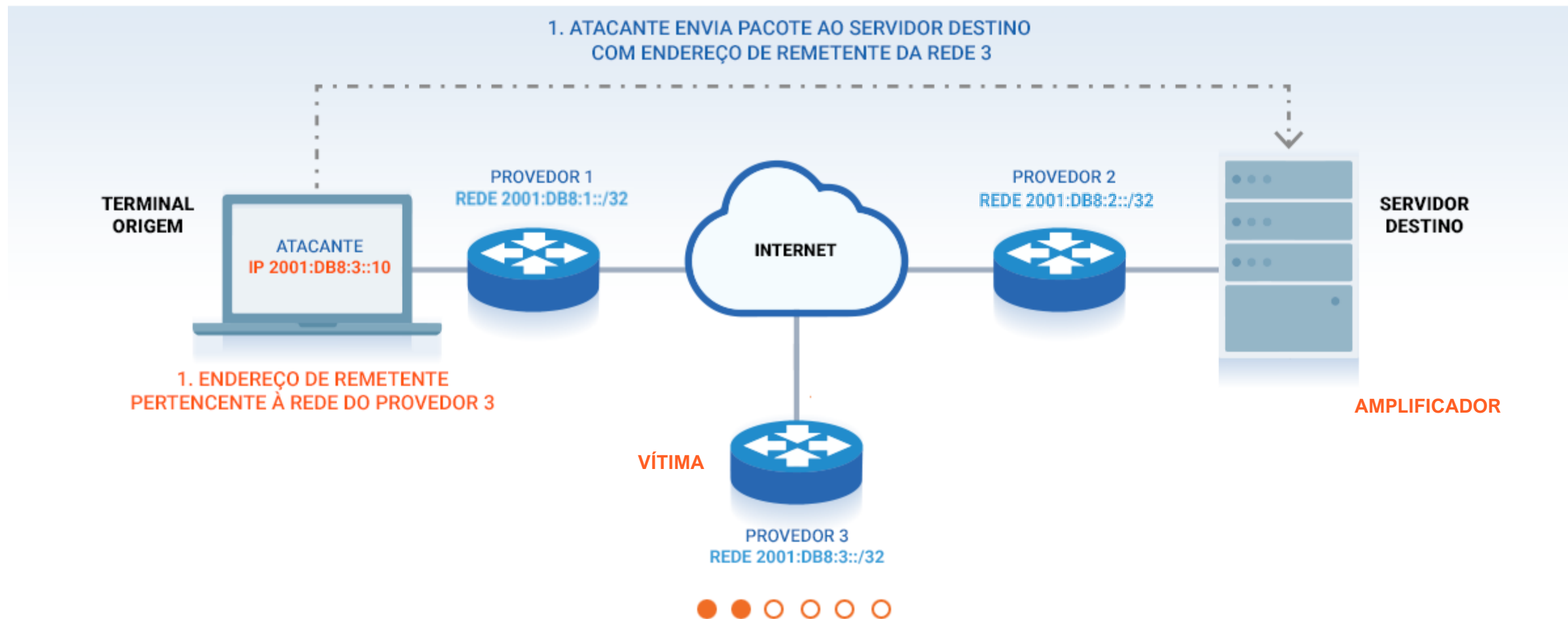
Topologia de rede sem filtros antispoofting [4]



# Segurança e estabilidade da Internet

## Ataque DoS por reflexão

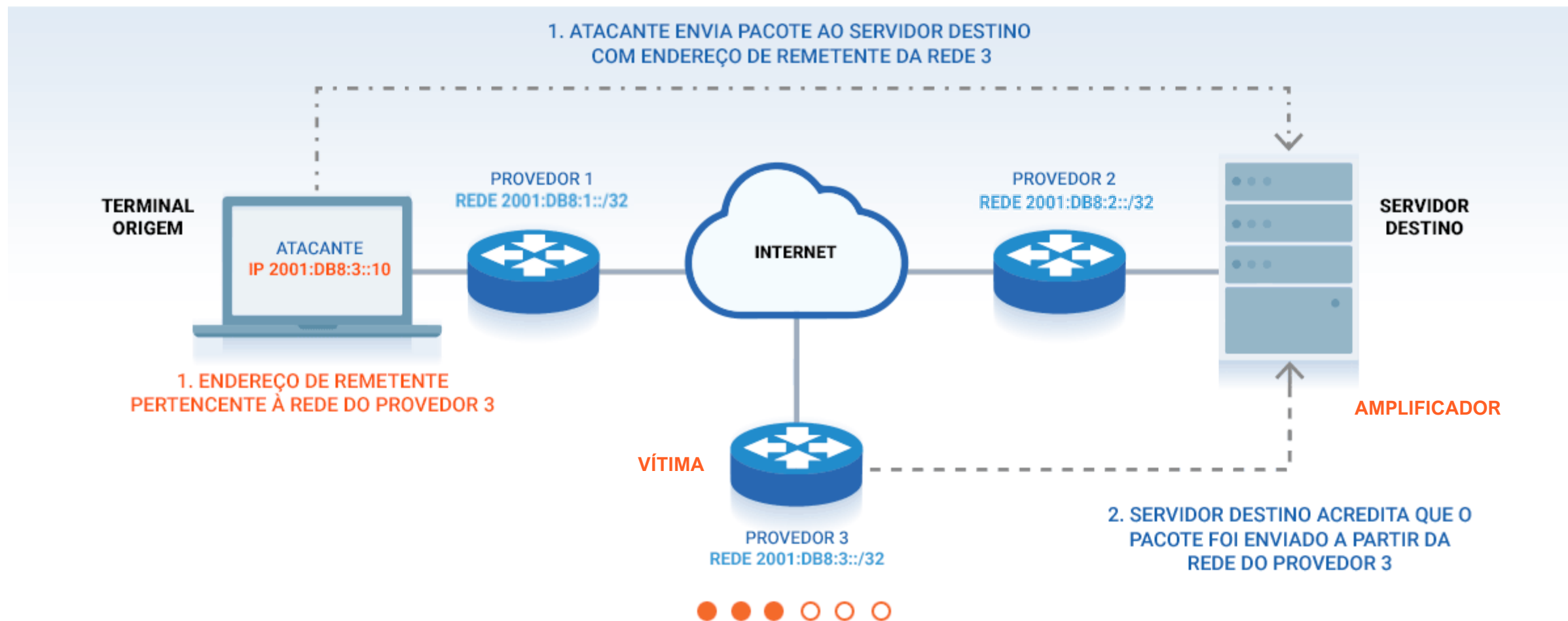
Ataque DoS utilizando endereço de remetente forjado (Spoofing) [4]



# Segurança e estabilidade da Internet

## Ataque DoS por reflexão

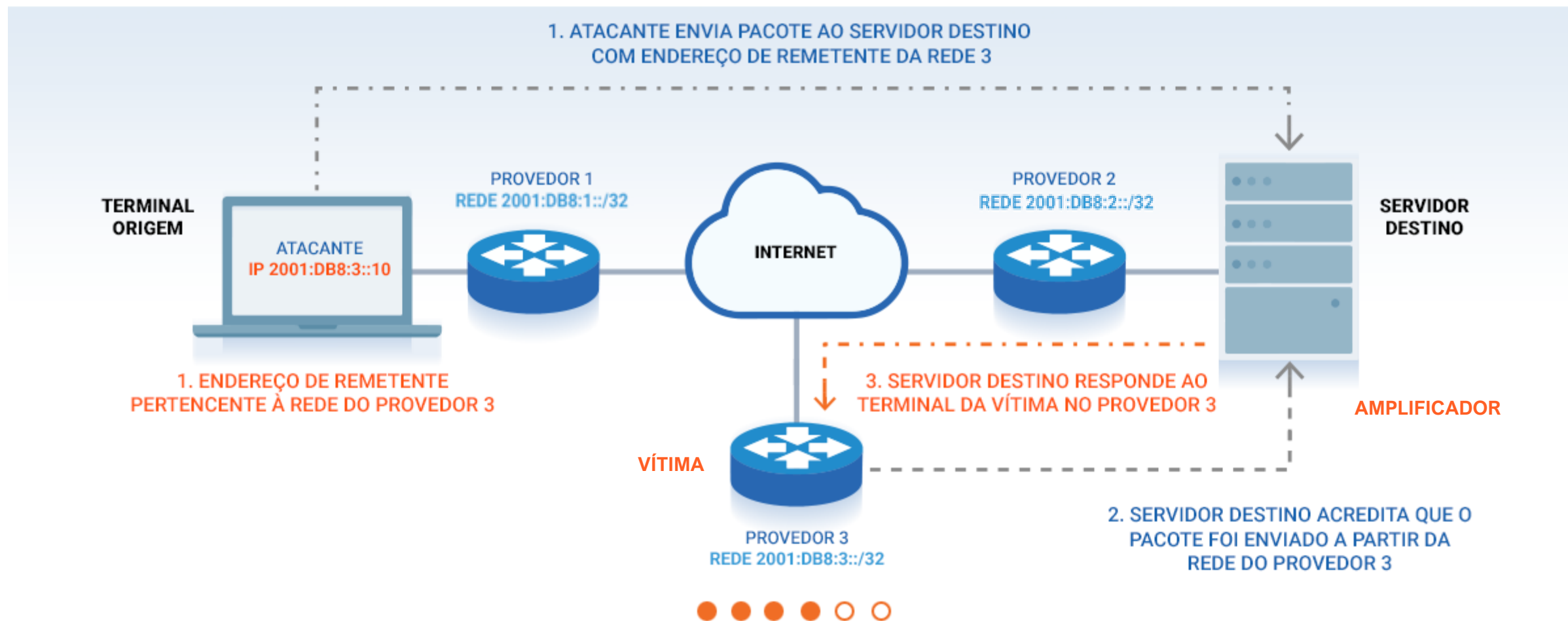
Ataque DoS utilizando endereço de remetente forjado (Spoofing) [4]



# Segurança e estabilidade da Internet

## Ataque DoS por reflexão

Ataque DoS utilizando endereço de remetente forjado (Spoofing) [4]



# Segurança e estabilidade da Internet

## Servidor Destino

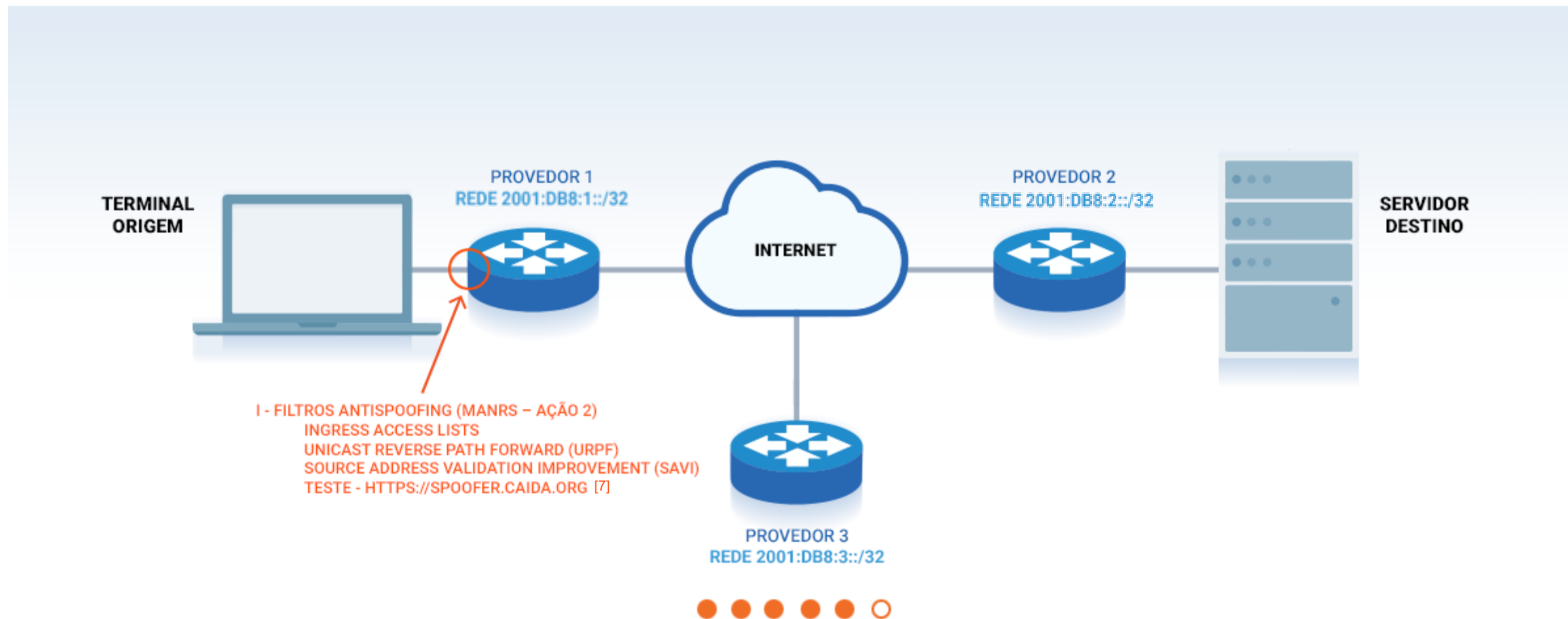
Os protocolos usados nos ataques fazem parte legítima da infraestrutura pública da Internet, porém em alguns equipamentos, como CPEs, são instalados por padrão e abusados por atacantes.

- DNS (53 / UDP): fator de amplificação de 28 até 54 vezes
- NTP (123 / UDP): fator de amplificação de 556.9 vezes
- SNMPv2 (161 / UDP): fator de amplificação de 6.3 vezes
- NetBIOS (137–139 / UDP): fator de amplificação de 3.8 vezes
- SSDP (1900 / UDP): fator de amplificação de 30.8 vezes
- CHARGEN (19 / UDP): fator de amplificação de 358.8 vezes

# Segurança e estabilidade da Internet

## Ataque DoS por reflexão

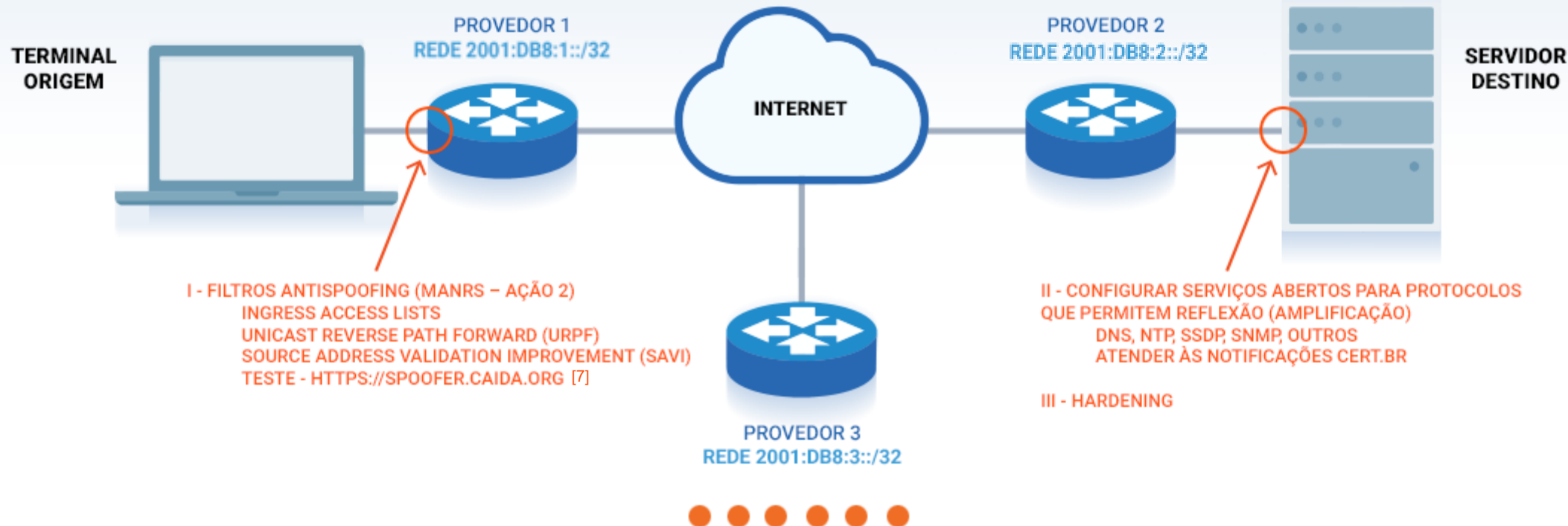
Solução: Aplicação de filtros antispoofing BCP38 [4]



# Segurança e estabilidade da Internet

## Ataque DoS por reflexão

Solução: Aplicação de filtros antispoofing, configuração de serviços e Hardening [4]



# Segurança e estabilidade da Internet

## Ataques DDoS – Distributed Deny of Service

Principais características dos ataques DDoS:

- Aumentou de patamar a partir de 2014
- O reporte de incidentes recebidos pelo CERT.br sobre computadores que participaram de ataques DDoS cresceu 90% em relação ao ano anterior
- 300 Gbps é o “normal”, até 1 Tbps contra alguns alvos
- Tipos mais frequentes:
  - Botnets IoT, ataques do tipo UDP flood
  - Ataque DDoS por reflexão com amplificação de tráfego

Fonte: CERT.br [13]

# Segurança e estabilidade da Internet

## Ataques DDoS – Distributed Deny of Service

Serviços mais abusados para ataques de amplificação no Brasil:

- SNMP (161/UDP), DNS (53/UDP), NTP (123/UDP)

Principais malwares por trás das botnets responsáveis por ataques DDoS:

- Mirai, BASHLITE e respectivas variantes

Dispositivos mais utilizados nos ataques utilizando botnets:

- Modems e roteadores de banda larga mal configurados com serviços abertos
- DVR de câmeras de segurança e câmeras IP
- TVs conectadas e caixas de TV via Internet
- Dispositivos IoT

# Segurança e estabilidade da Internet

## Ações de Hardening



Para proteger suas infraestruturas, os operadores das redes devem adotar medidas para **analisar suas vulnerabilidades, mapear as ameaças, mitigar ou minimizar os riscos e aplicar medidas corretivas**

- **Autenticação**

- Usuário, contas, senhas

- **Autorização**

- Permissão de acesso

- **Acesso**

- Protocolo seguro, criptografado
- Mudar porta padrão, log, interface específica para configuração
- Logout forçado, Port Knocking

- **Sistema**

- Desative interfaces e serviços não utilizados
- Manter os sistemas e equipamentos atualizados

- **Configurações**

- Backup seguro, script de configuração

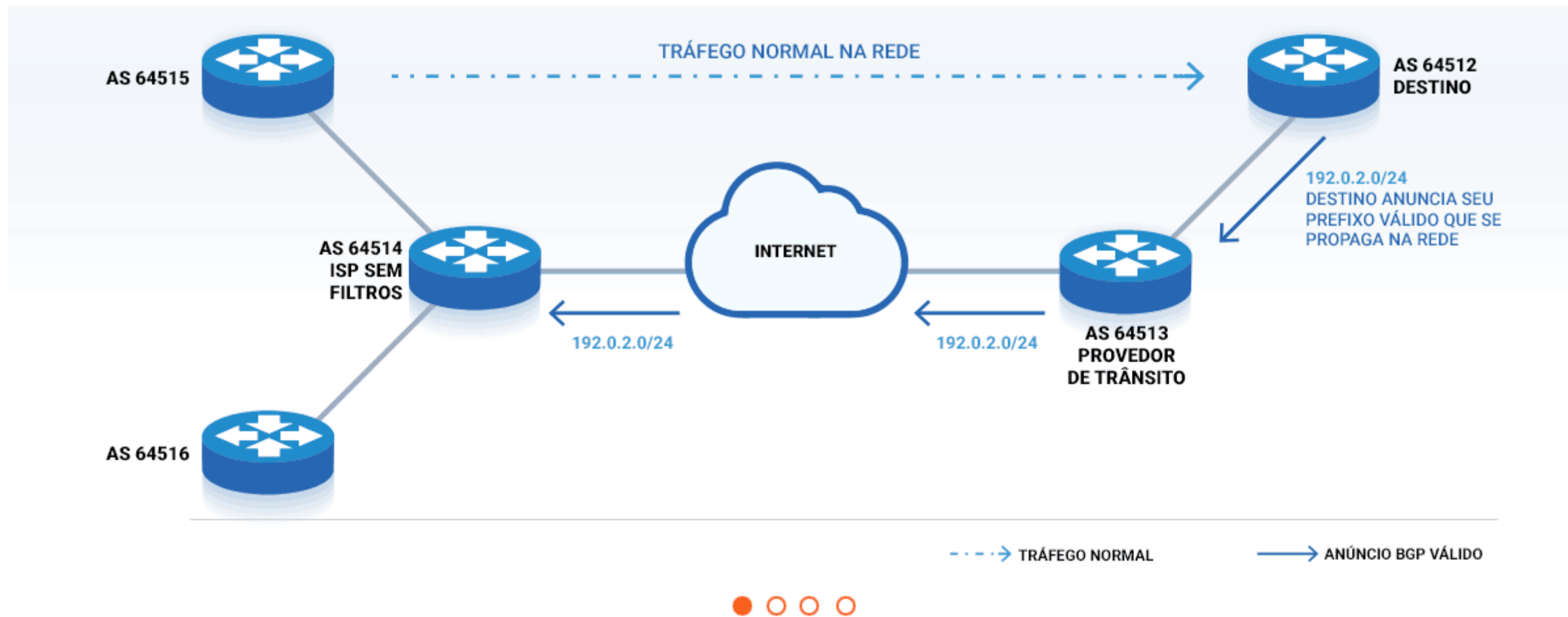
- **Registros e Auditoria**

- Nível criticidade, armazenado em local seguro, hora correta (NTP)
- Registro de ações

# Segurança e estabilidade da Internet

## Ataque por Sequestro de Prefixos (Hijacking)

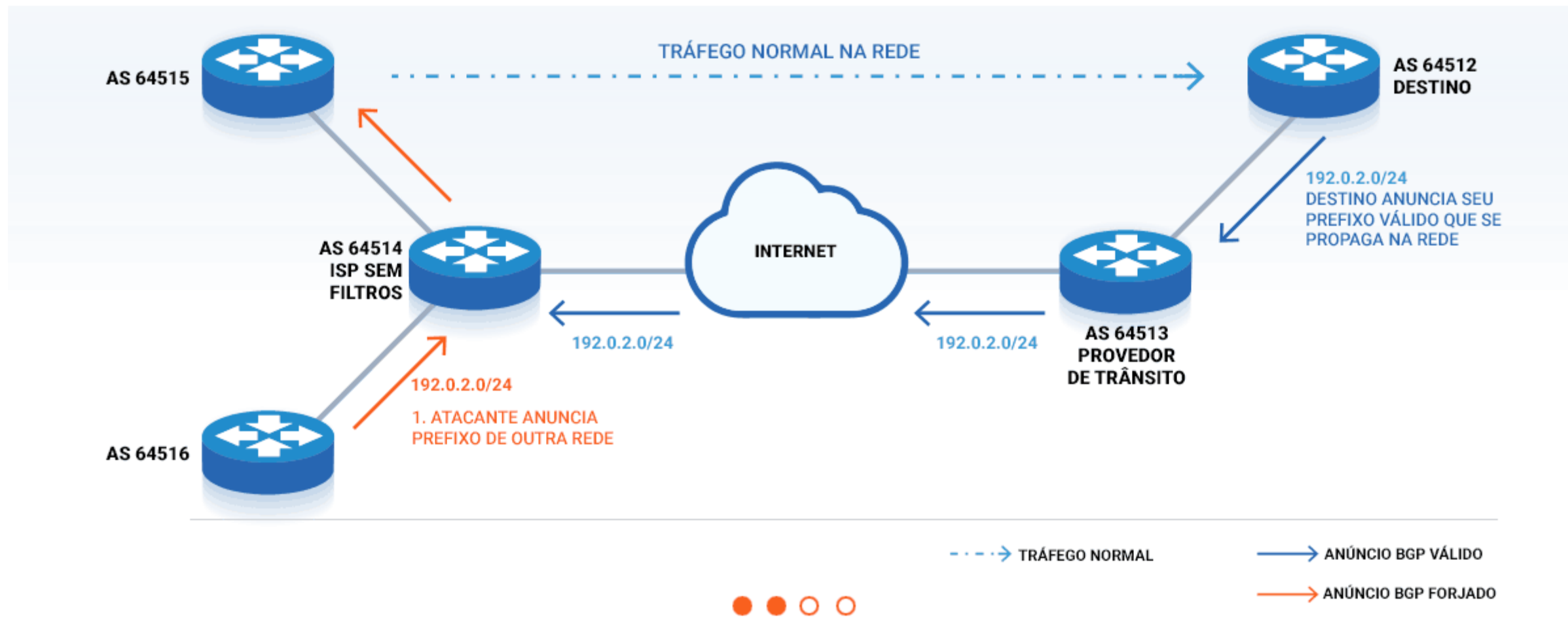
Topologia de rede sem filtros de anúncios



# Segurança e estabilidade da Internet

## Ataque por Sequestro de Prefixos (Hijacking)

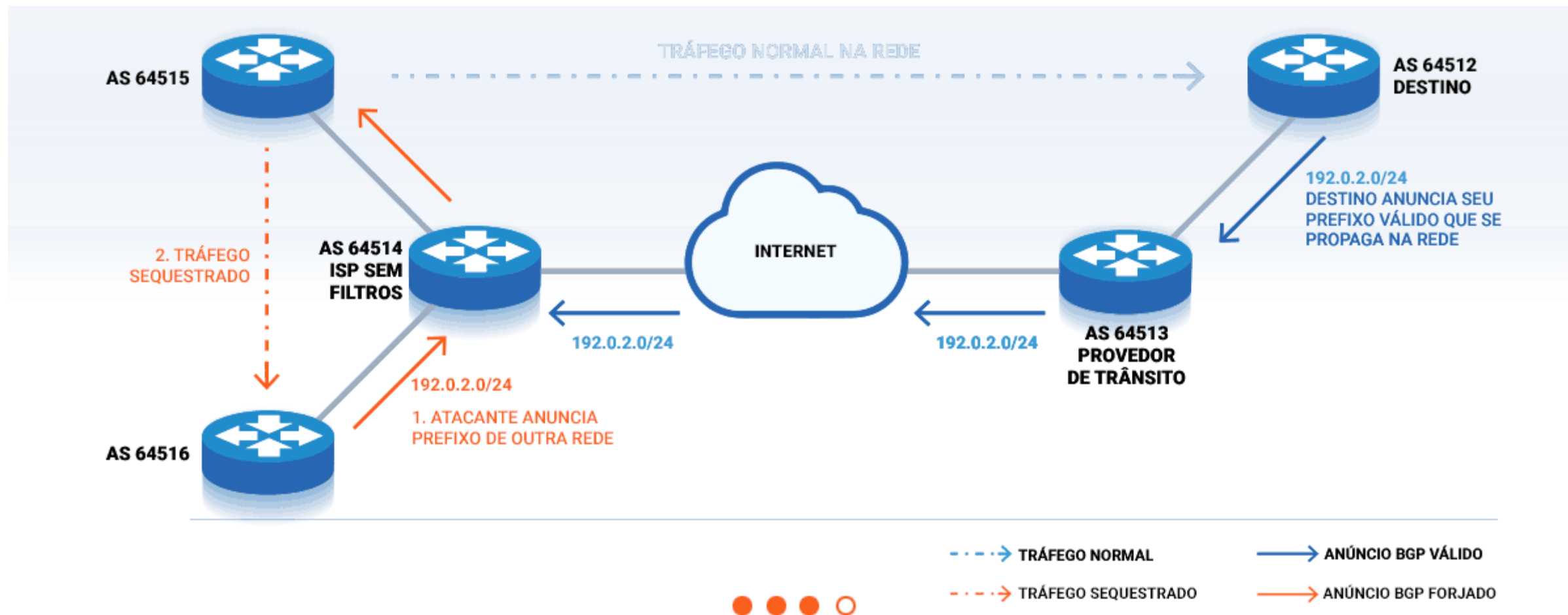
Topologia de rede sem filtros de anúncios



# Segurança e estabilidade da Internet

## Ataque por Sequestro de Prefixos (Hijacking)

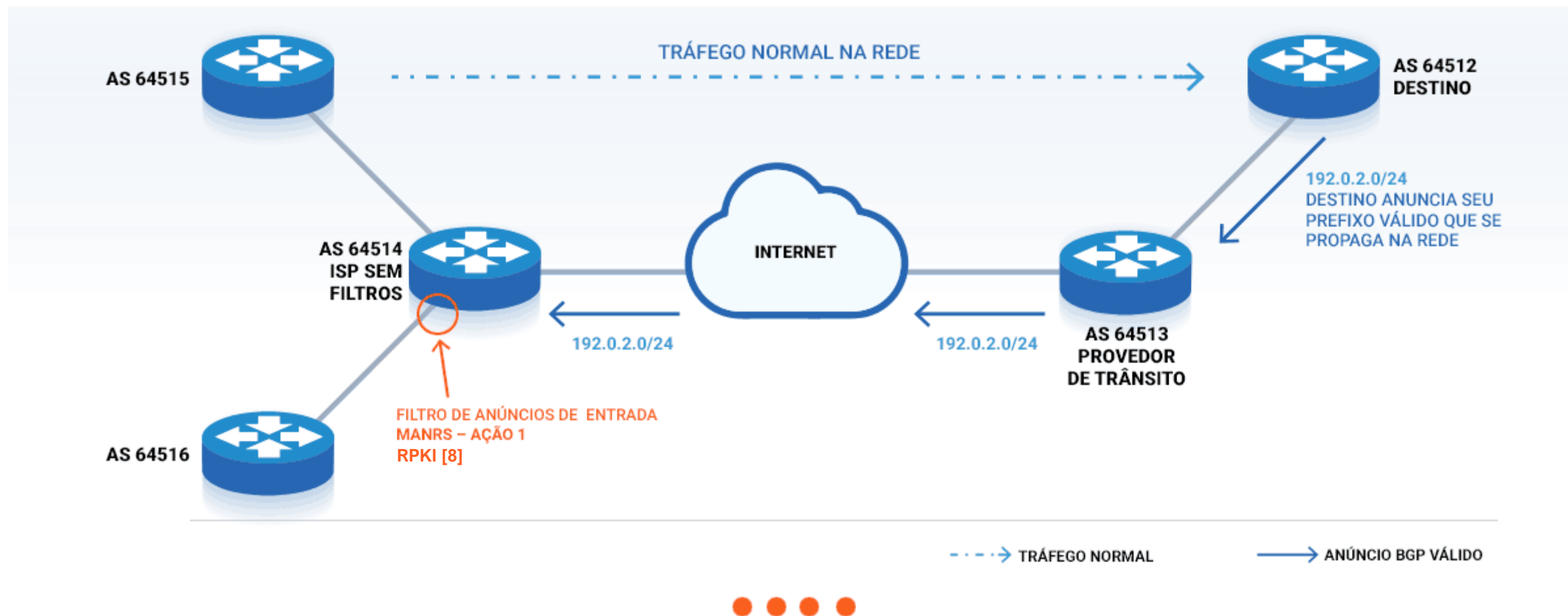
Topologia de rede sem filtros de anúncios



# Segurança e estabilidade da Internet

## Ataque por Sequestro de Prefixos (Hijacking)

Solução: Filtro de anúncios de entrada (clientes) – MANRS - Ação 1



# Segurança e estabilidade da Internet

RPKI → Certificado de chaves públicas para Recursos Internet  
(Resource Public Key Infrastructure)

- Permite emissão de Certificados Digitais de Chaves Públicas (PKI) associados a às alocações de blocos de endereços IP e ASNs
- **As empresas que recebem alocações demonstram que são os reais titulares dos recursos → melhora a segurança dos anúncios**
- Permite a emissão de Certificados Digitais e assinatura dos ROAs
- **As ROAs possuem uma lista prefixos e um ASN autorizado a gerar anúncios**
- Este objeto é assinado digitalmente com a chave privada associada à chave pública do Certificado Digital → disponível publicamente

# Segurança e estabilidade da Internet

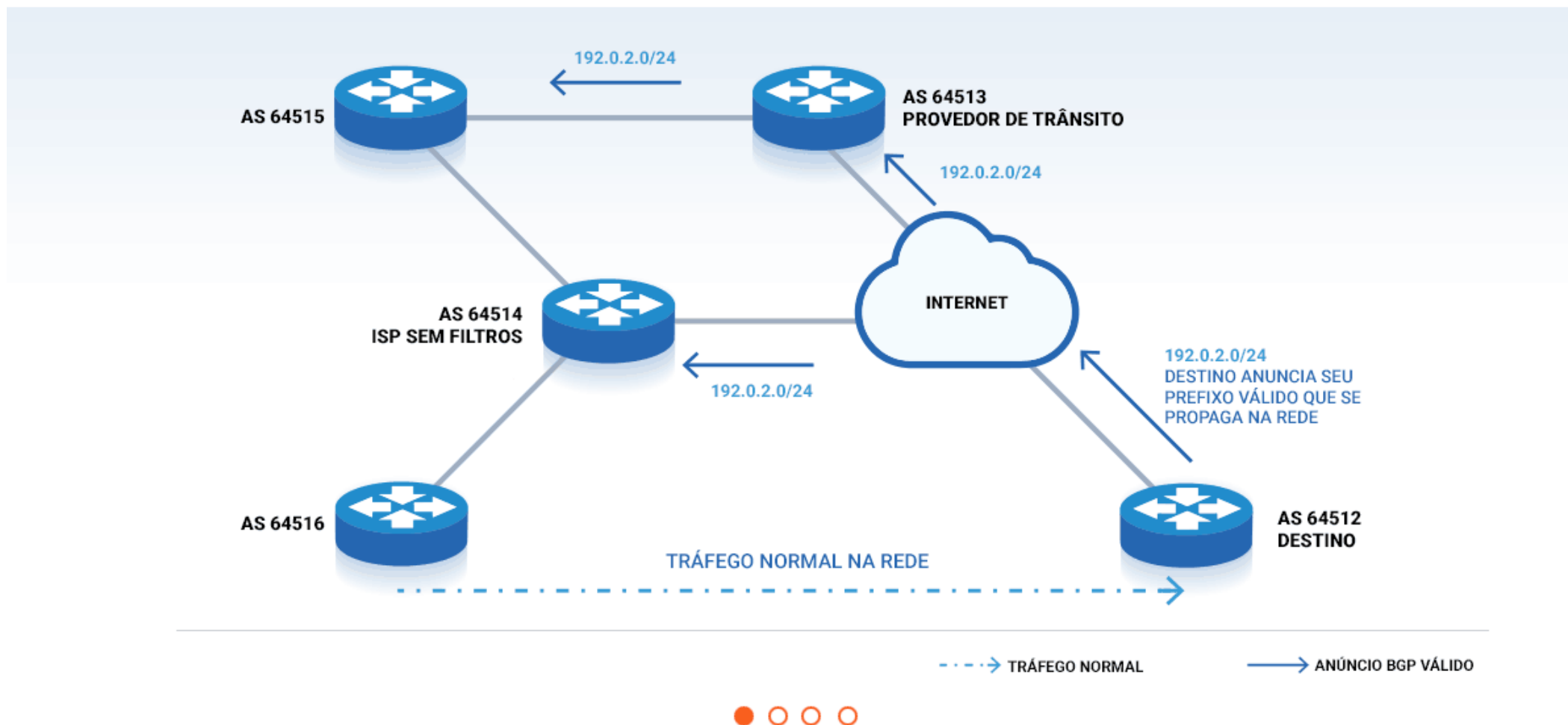
RPKI → Certificado de chaves públicas para Recursos Internet  
(Resource Public Key Infrastructure)

- A segurança do sistema de rotas é garantida com o uso dos sistemas de validação que verificam se para uma determinada rota para um bloco IP há uma ROA que indique permissão do anúncio
- **A validação de uma ROA é feita a partir de uma verificação criptográfica**
- Mais detalhes sobre o sistema RPKI e passo a passo para implementação e ativação: <https://registro.br/rpki> [8] [9]

# Segurança e estabilidade da Internet

## Ataque por Vazamento de Rotas (Leak)

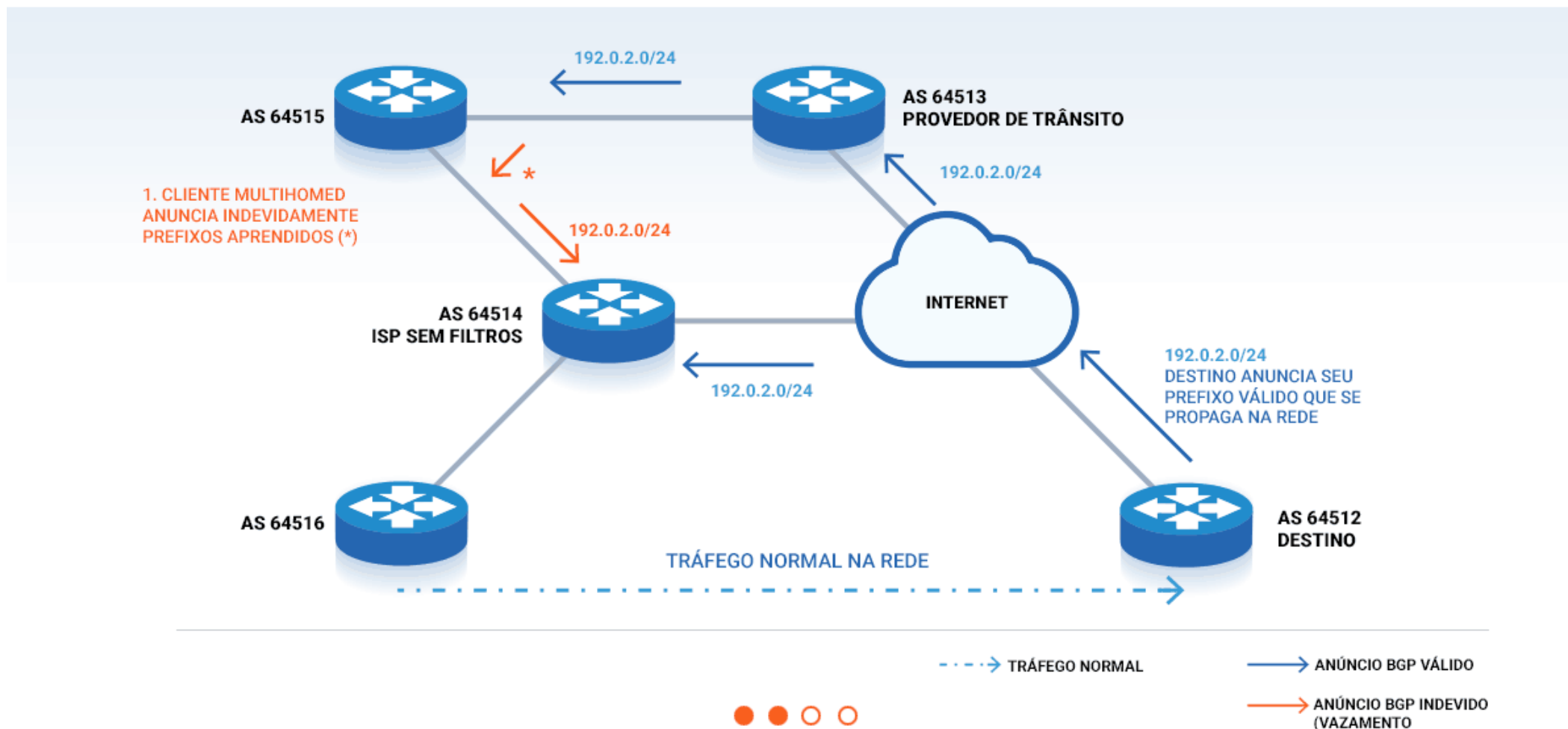
Topologia sem filtros de anúncios



# Segurança e estabilidade da Internet

## Ataque por Vazamento de Rotas (Leak)

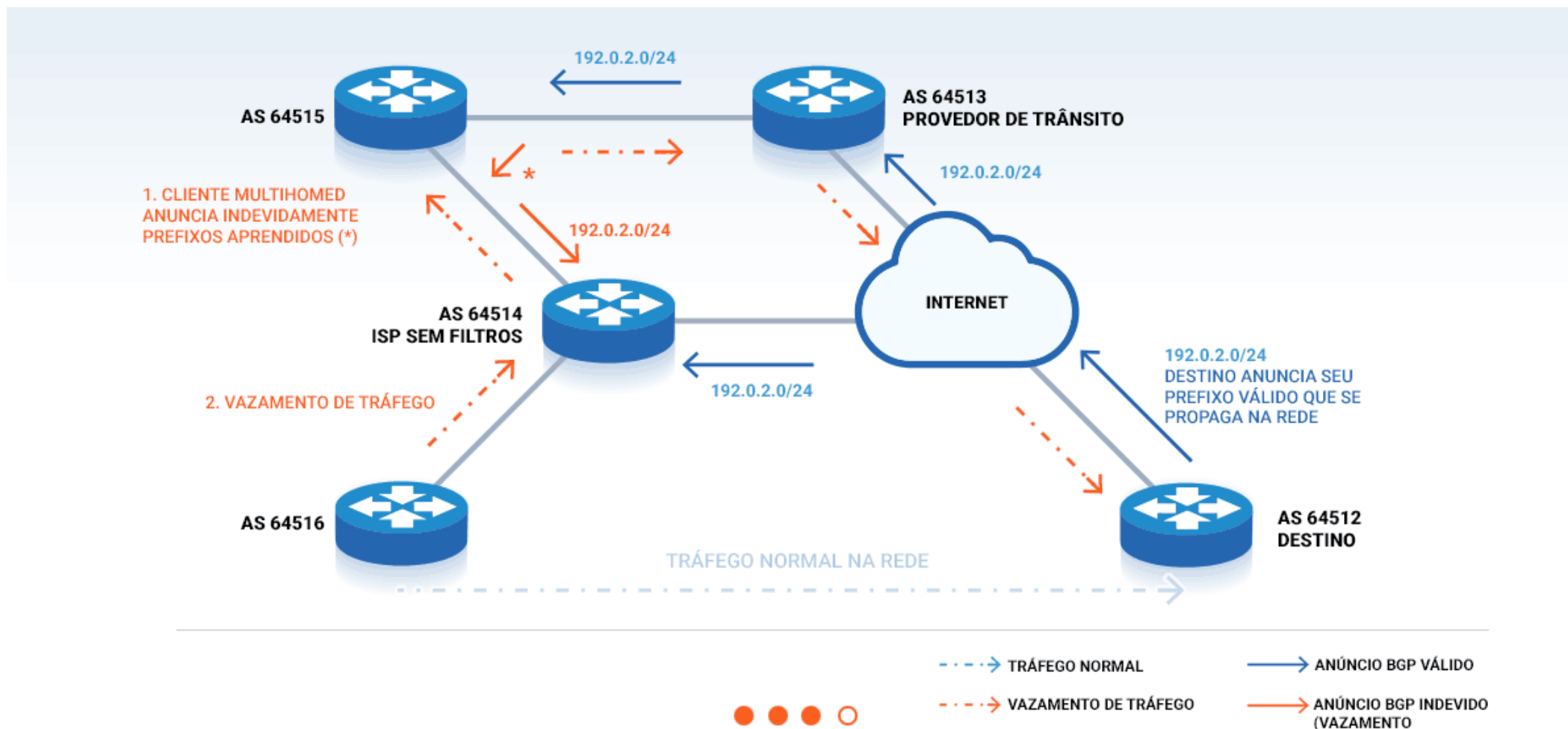
Topologia sem filtros de anúncios



# Segurança e estabilidade da Internet

## Ataque por Vazamento de Rotas (Leak)

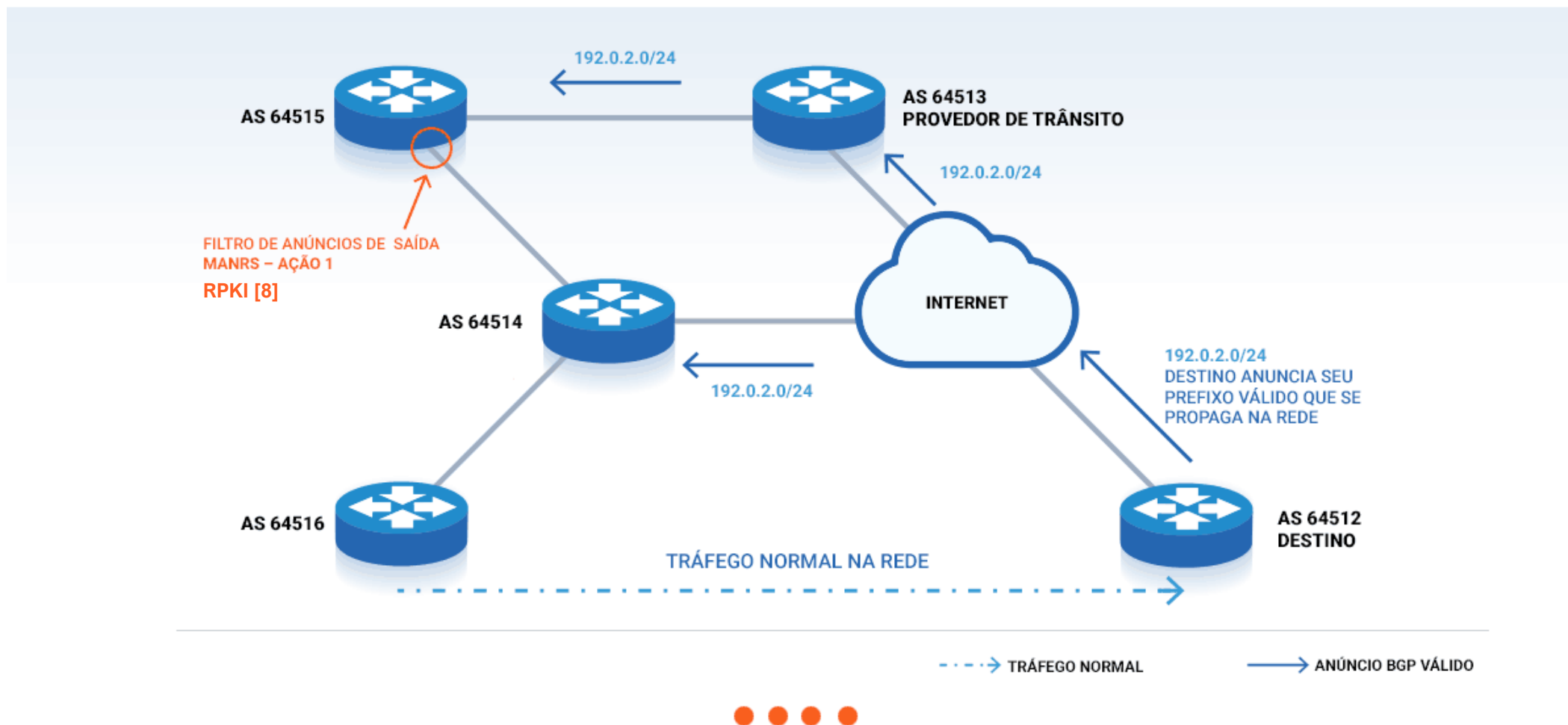
Topologia sem filtros de anúncios



# Segurança e estabilidade da Internet

## Ataque por Vazamento de Rotas (Leak)

Solução: Filtro de anúncios de saída – MANRS – Ação 1



# BGP Hijacking e Leak

- Anúncio de prefixos não autorizados
  - “Sequestro do Prefixo”
- Motivos:
  - Erro de configuração
  - *Fat Finger*
  - Proposital





# MANRS

## Mutually Agreed Norms for Routing Security

Saiba mais em:

<http://manrs.org> (site completo do MANRS em inglês)

<http://bcp.nic.br> (recomendação do MANRS em português)

# Como Resolver os problemas

Todos devem implementar estas recomendações:

1. **Garantir que seus anúncios BGP sejam de seus próprios blocos IP e de seus clientes: definição de políticas de roteamento e implantação de filtros (RPKI) [8]**
  - Dificulta sequestro de blocos IP e redirecionamento de tráfego.
2. **Garantir que os IP de origem que saem da rede não sejam falsificados: antispoofing [3] [6]**
  - Impede que os computadores infectados de seus usuários iniciem ataques de amplificação.
3. **Garantir que seus contatos estejam atualizados e acessíveis por terceiros de maneira global: Whois do Registro.br, PeeringDB e Site da Empresa**
  - Permite que equipes de segurança de outras redes te avisem sobre problemas que detectam na sua rede.
4. **Publicar suas políticas de roteamento em bases de dados externas: IRR (RADb, TC, NTTCOM) e RPKI [8]**
  - Facilita a validação de roteamento em escala global.



# Programa por uma Internet mais segura

# Programa por uma Internet mais Segura

## Problemas de segurança



- Todos tentam proteger sua própria rede. Olham apenas o que está entrando!
- **Isso é caro! Requer equipamentos e configurações complexas! Não tem resolvido!**
- Poucos olham o que sai da sua rede!
- **Isso é simples. Fácil. Barato.**



# Programa por uma Internet mais Segura

## Problemas de segurança



- A falta de preocupação com a segurança das redes pode gerar dor de cabeça sem fim.
- **As redes mal configuradas podem ser utilizadas para a geração de ataques a outras redes, DDoS, sequestro de prefixos (hijacking) e vazamento de rotas (leak).**
- Seus recursos são comprometidos: links de conexão com a Internet e equipamentos.
- **Além de levar o nome da empresa a ser envolvido em ataques devido às suas vulnerabilidades.**
- Um único problema pode manchar a reputação de uma companhia frente a clientes e potenciais parceiros.
- A adoção de procedimentos de segurança em suas redes adiciona um valor competitivo num mercado em que todos oferecem serviços semelhantes e direcionados ao preço. Mostra também competência e comprometimento com a segurança de seus serviços.
- “Quando o cliente adquire um serviço de rede, ele espera que essa ponte entre a casa dele e a Internet seja segura”.

# Programa por uma Internet mais Segura Iniciativa

Lançado pelo CGI.br e NIC.br

**Painel do IX Fórum 11 em dez/17 [1]**

Apoio: Internet Society, Abrint, Abranet, SindiTelebrasil

**Objetivo** - atuar em apoio à comunidade técnica da Internet para:

- **Redução de ataques de Negação de Serviço originados nas redes brasileiras**
- Reduzir **Sequestro de Prefixos, Vazamento de Rotas e Falsificação de IP de Origem**
- **Redução das vulnerabilidades e falhas de configuração presentes nos elementos da rede**
- Aproximar as diferentes equipes responsáveis pela segurança e estabilidade da rede
- **Criar uma cultura de segurança**



# Programa por uma Internet mais Segura

## Plano de Ação

Para solucionar os problemas de segurança, as ações devem ser realizadas pelos operadores dos Sistemas Autônomos, com apoio do NIC.br

### Ações coordenadas a serem executadas pelo NIC.br:

- Conscientização por meio de palestras, cursos e treinamentos
- **Criação de materiais didáticos e boas práticas [11]**
- Interação com **Associações de Provedores** e seus afiliados para disseminação da **Cultura de Segurança**, adoção de **Melhores Práticas** e **mitigação** de problemas existentes
- **Implementação de filtros de rotas no IX.br, que contribui para a melhora do cenário geral**
- Estabelecimento de métricas e acompanhamento da efetividade das ações



# Programa por uma Internet mais Segura

## Interação com Operadoras e Provedores



### Atividades com **Operadoras e Provedores** com apoio das **Associações**

- Reuniões bilaterais
  - Correção de pontos de contato para notificação (**Ação 3 MANRS**) [3]
    - Validar a permissão para recebimento de e-mails com origem **cert@cert.br**
  - Acompanhamento da correção de serviços mal configurados que podem ser abusados para fazer parte de ataques DDoS (**recomendação do CERT.br**) [5]

Nome da Empresa	ASN	DNS	SNMP	NTP	SSDP	PORTMAP	MEMCACHED	NETBIOS	QOTD	CHARGEN	LDAP	MDNS	UBNT	WS-DISCOVERY	TFTP	2019-10	2019-11	2019-12	2020-01	MT4145
																			#	
Empresa 1	ASN 1	17	4	1	10	2	0	2	0	0	0	0	0	0	0	512	49	37	36	0
Empresa 2	ASN 2	0	5	9	0	0	0	1	0	0	0	0	1	0	0	16	11	12	16	0
Empresa 3	ASN 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	3	0	0
																529	60	52	52	

# Programa por uma Internet mais Segura

## Desenvolvimento do Programa



- Interação com as operadoras e provedores: redução de endereços IP mal configurados que permitem amplificação
  - Em mai/18: **575k** grandes operadoras // **148k** ISP e ASN corporativos (**80/20**)
  - Hoje: **103k** grandes operadoras // **174k** ISP e ASN corporativos (novos protocolos analisados – UBNT, WS-DISCOVERY, TFTP (**37/63**))
  - Redução total dos IPs notificados de **62%** desde o início do Programa
    - Segmentação dos IPs notificados: **37%** operadoras, **62%** ISPs, **1%** corporativos
  - Segmentação dos ASNs (Brasil): **90,3%** ISPs, **9,4%** corporativos, **0,3%** operadoras

# Programa por uma Internet mais Segura

## Endereços IP e ASNs notificados pelo CERT.br



	DNS		SNMP		NTP		SSDP		Ubiquiti	
mês	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
2019-04	2.898	59.865	2.662	123.241	997	79.698	886	18.919	1.909	76.666
2019-05	3.045	68.764	2.633	103.204	1.019	77.979	953	18.564	1.797	64.729
2019-06	2.960	69.473	2.744	107.090	961	82.372	928	19.048	1.679	55.732
2019-07	3.012	78.879	2.777	103.289	990	77.374	827	19.597	1.640	50.811
2019-08	3.068	76.143	2.808	90.960	998	78.058	795	14.071	1.625	52.598
2019-09	3.072	67.420	2.833	89.740	1.025	78.037	745	11.746	1.478	39.561
2019-10	3.113	65.922	2.861	81.781	991	72.720	695	8.811	1.442	33.160
2019-11	3.040	61.723	2.824	78.277	985	70.950	659	7.787	1.320	24.565
2019-12	2.962	58.453	2.900	77.952	1.003	72.235	736	10.791	1.374	25.964
2020-01	3.144	69.680	2.881	72.806	1.013	72.862	705	9.386	1.251	19.407
2020-02	3.086	66.958	2.545	60.678	1.013	72.591	680	9.134	1.315	19.726
2020-03	na	na	3.021	81.009	1.015	71.864	721	9.326	1.305	20.780

O Brasil está em **quinto** lugar entre os endereços IPs com serviços SNMP mal configurados

"na" significa que o protocolo ainda não foi notificado no mês

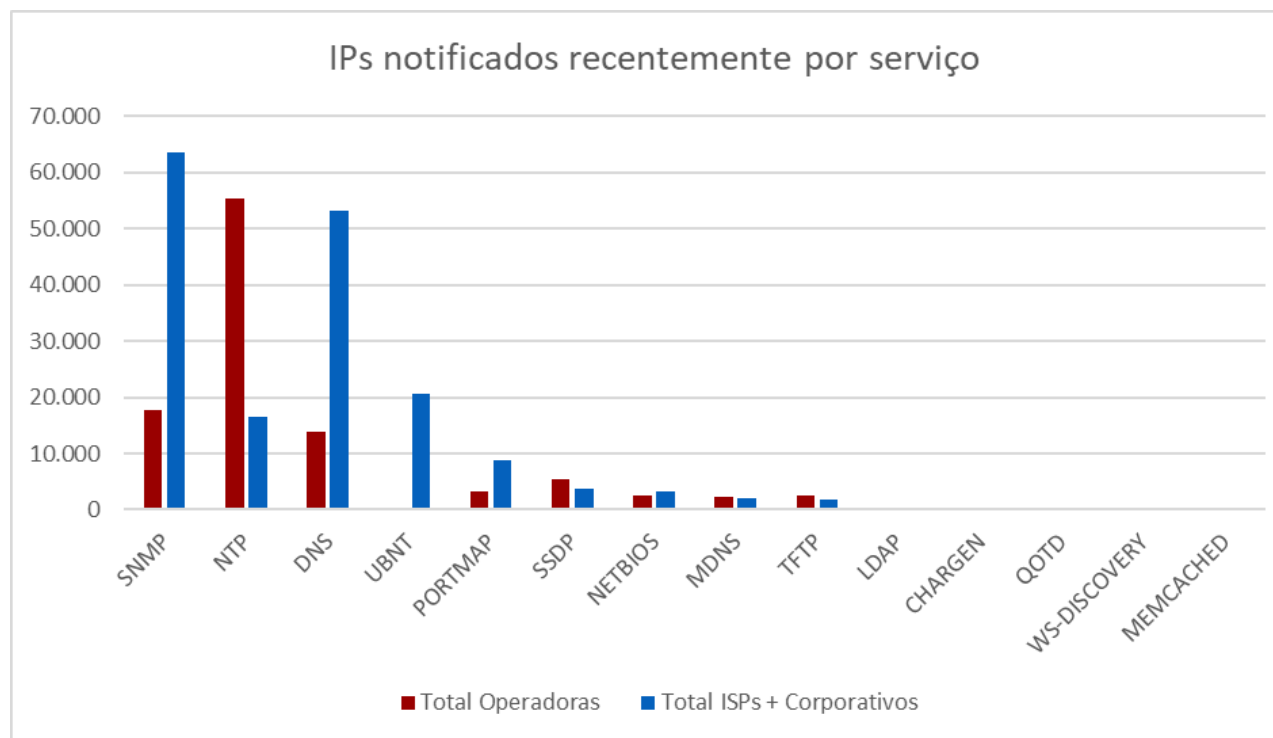
Fonte: <https://snmpscan.shadowserver.org/> [12]

# Programa por uma Internet mais Segura

## Desenvolvimento do Programa



- Endereços IP notificados recentemente por serviço mal configurado



Principais ofensores: **ISPs e ASes corporativos** → **SNMP, DNS, UBNT e NTP**

**Grandes operadoras** → **NTP, SNMP e DNS**



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

# Programa por uma Internet mais Segura

## Página WEB



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

### Ações necessárias



#### Contra ataques de Amplificação

Configurar corretamente serviços que podem ser abusados em ataques de amplificação.



MANRS

#### Configurações de Roteamento

Implementar as ações de segurança de roteamento preconizadas pelo MANRS.



#### Melhores Práticas de Hardening

Mapear ameaças, mitigar riscos e adotar ações corretivas.



# Minimum security requirements for CPEs acquisition

O LACNOG BCOP WG e LAC-AAWG, em parceria com M<sup>3</sup>AAWG e LACNIC, e coordenação NIC.br, desenvolveram um documento que tem como objetivo identificar um conjunto mínimo de requisitos de segurança que devem ser especificados no processo de compra de CPEs pelos ISPs



**Visa a aquisição de equipamentos que permitam gerenciamento remoto e que sejam nativamente mais seguros, permitindo:**

- Redução dos riscos de comprometimento da rede do provedor e da Internet como um todo
- Redução dos custos e perdas resultantes do abuso dos equipamentos por invasores: degradação ou indisponibilidade de serviços, suporte técnico e retrabalho

**O documento foi lançado no LACNIC 31 (maio/19) e está disponível em**

<https://www.m3aawg.org/sites/default/files/lac-bcop-1-m3aawg-v1-portuguese-final.pdf> - Documento conjunto LACNOG-M3AAWG: Melhores Práticas Operacionais Atuais sobre Requisitos Mínimos de Segurança para Aquisição de Equipamentos para Conexão de Assinante (CPE) LAC-BCOP-1

# Programa por uma Internet mais Segura

## Referências

- [1] <https://youtu.be/TIVrx3QoNU4?t=7586> - Painel sobre Programa para uma Internet mais Segura, IX (PTT) Fórum 11, São Paulo, SP
- [2] <https://bcp.nic.br/i+seg/> - Programa por uma Internet mais segura
- [3] <https://www.manrs.org/manrs/> - MANRS for Network Operators
- [4] <https://bcp.nic.br/antispoofing> - Boas Práticas de Antispoofing
- [5] <https://bcp.nic.br/ddos#5> - Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)
- [6] <https://bcp.nic.br/notificacoes> - Recomendações para Notificações de Incidentes de Segurança
- [7] <https://www.caida.org/projects/spoofers/> - Tool to access and report source address validation
- [8] <https://registro.br/tecnologia/numeracao/rpki/> - RPKI – Descrição e passo a passo para implementação e ativação junto ao Registro.br
- [9] <https://registro.br/tecnologia/numeracao/faq/rpki/> - RPKI - Perguntas frequentes
- [10] <http://www.nic.br/videos/ver/como-resolver-os-problemas-de-seguranca-da-internet-e-do-seu-provedor-ou-sistema-autonomo/>
- [11] <https://www.m3aawg.org/sites/default/files/lac-bcop-1-m3aawg-v1-portuguese-final.pdf> - Documento conjunto LACNOG-M3AAWG: Melhores Práticas Operacionais Atuais sobre Requisitos Mínimos de Segurança para Aquisição de Equipamentos para Conexão de Assinante (CPE) LAC-BCOP-1
- [12] <https://www.shadowserver.org/news/the-scannings-will-continue-until-the-internet-improves/> - Artigo do ShadowServer sobre os testes de amplificadores
- [13] <https://cert.br/docs/palestras/certbr-fiesp-deinfra-2019.pdf> - Apresentação do CERT.br na Reunião de Telecomunicações do DEINFRA FIESP 23 de outubro de 2019 – São Paulo/SP

# Obrigado

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

@ [gzorello@nic.br](mailto:gzorello@nic.br)

20 de março de 2020

**nic.br** **cgi.br**

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)