nic.br

Núcleo de Informação e Coordenação do Ponto BR

cgi.br

Comitê Gestor da Internet no Brasil

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

nic.br cgi.br | registro.br

Encontro Regional REDETELESUL
Londrina - PR | 16/8/19

MELHORES PRÁTICAS PARA CONFIGURAÇÕES DE SERVIÇOS E MANRS

PROGRAMA POR UMA INTERNET MAIS SEGURA

Gilberto Zorello | gzorello@gmail.com

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
- **MANRS**
- Hardening
- **Requisitos Mínimos para aquisição de CPEs**

cgi.br

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21

GOVERNO e SOCIEDADE CIVIL

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

Organograma do NIC.br

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

ASSEMBLEIA GERAL

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

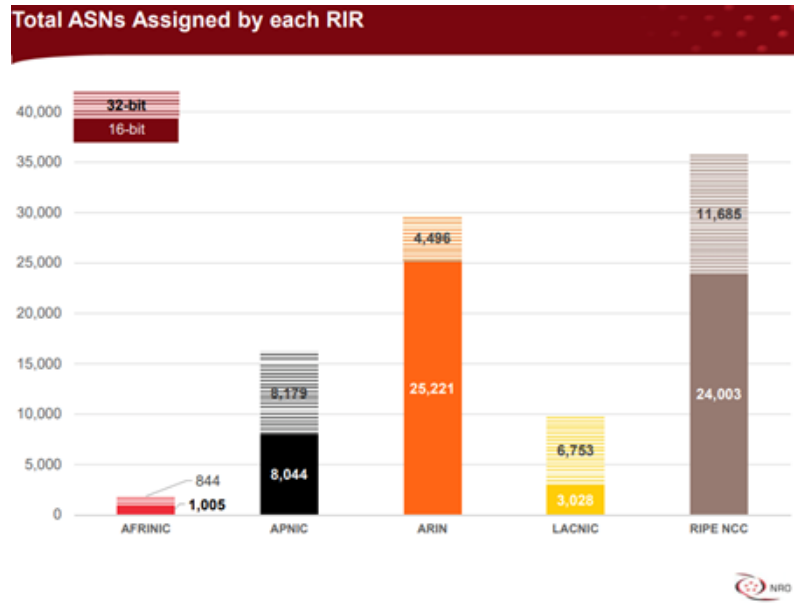
1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br

Panorama atual

Segurança e estabilidade da Internet
Estrutura da Internet atual

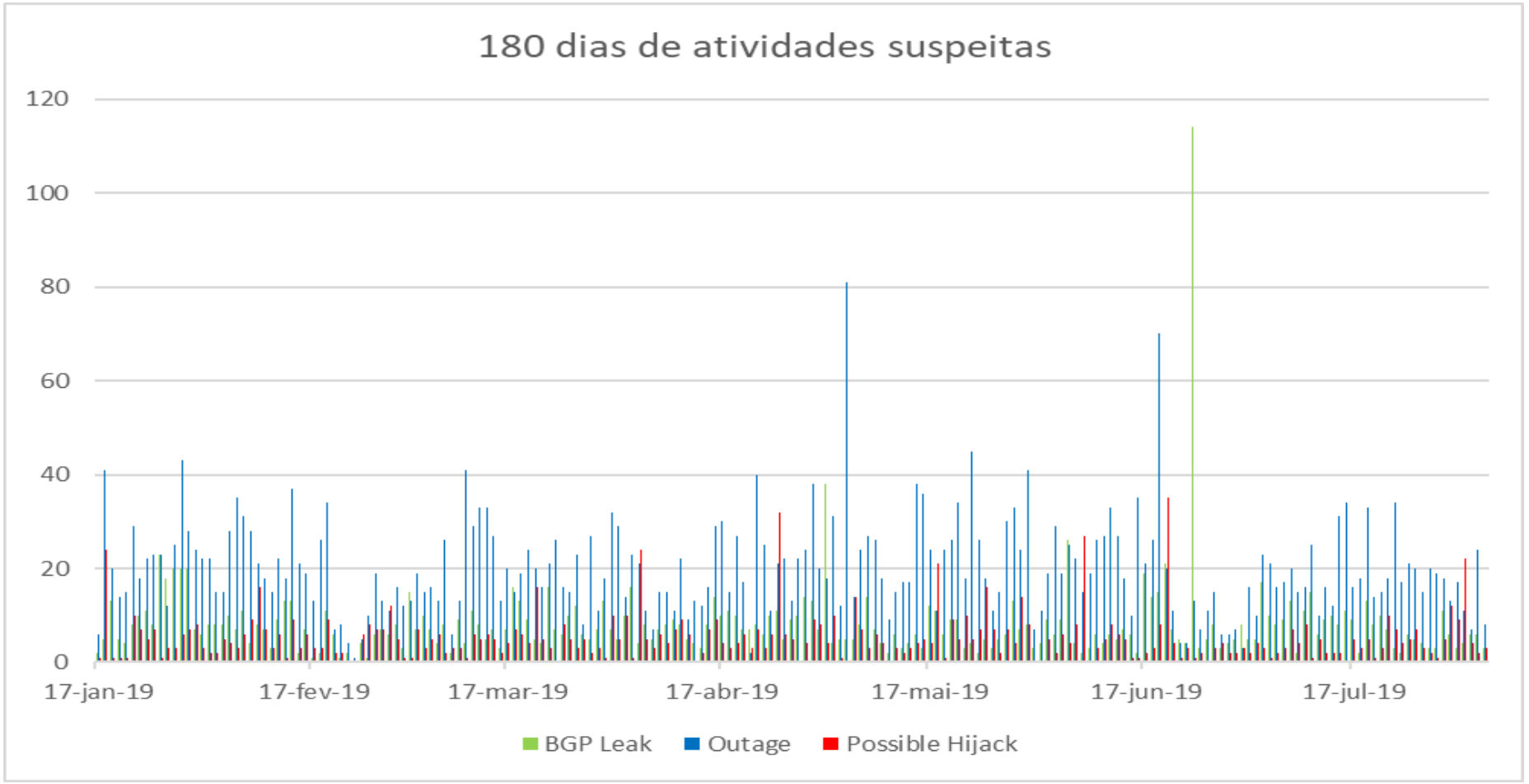
A Internet funciona com base na cooperação entre Sistemas Autônomos

- 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

Segurança e estabilidade da Internet
Nenhum dia sem um incidente



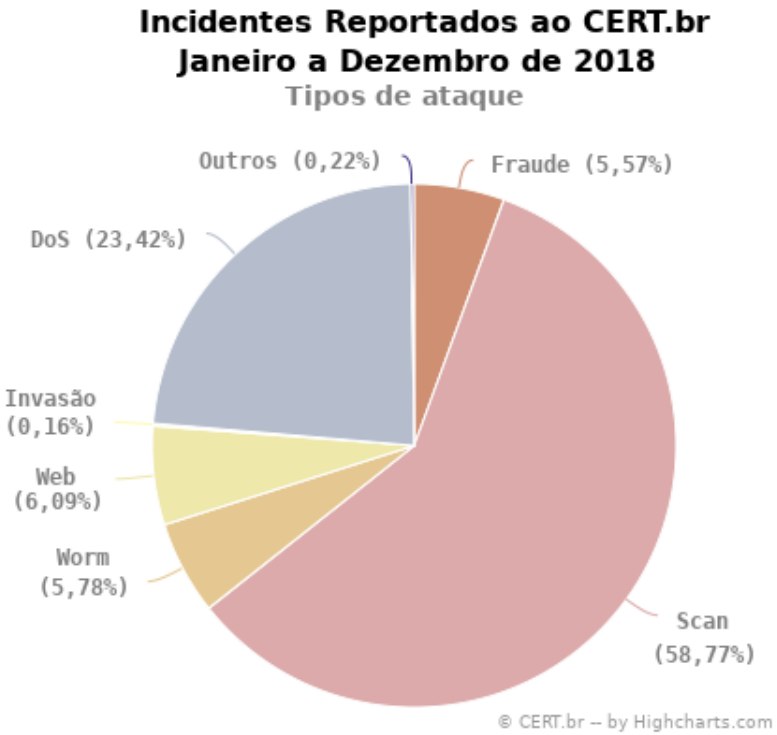
Fonte: https://bgpstream.com/

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

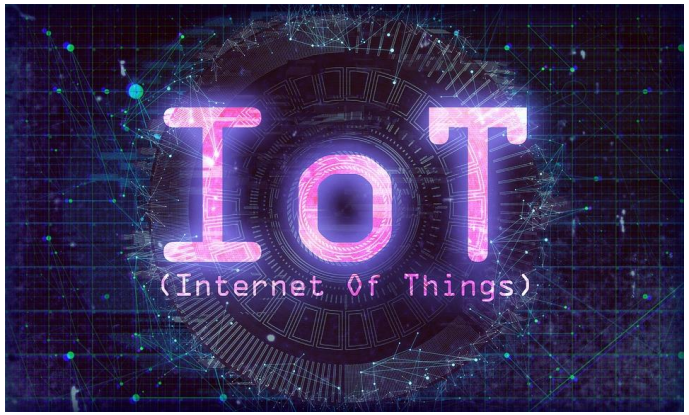


https://www.cert.br/stats/incidentes/2018-jan-dec/tipos-ataque.html

Constata-se um ritmo crescente de notificações de varreduras e DoS [4]

Segurança e estabilidade da Internet
IoT – Internet of Things

- Segundo a Cisco é esperado que 500 bilhões de dispositivos estejam conectados à Internet em 2030



- **Segundo a Gartner é esperado que 20 bilhões de coisas estejam conectadas à Internet em 2020**

- Nossas redes estão preparadas para esta tecnologia?

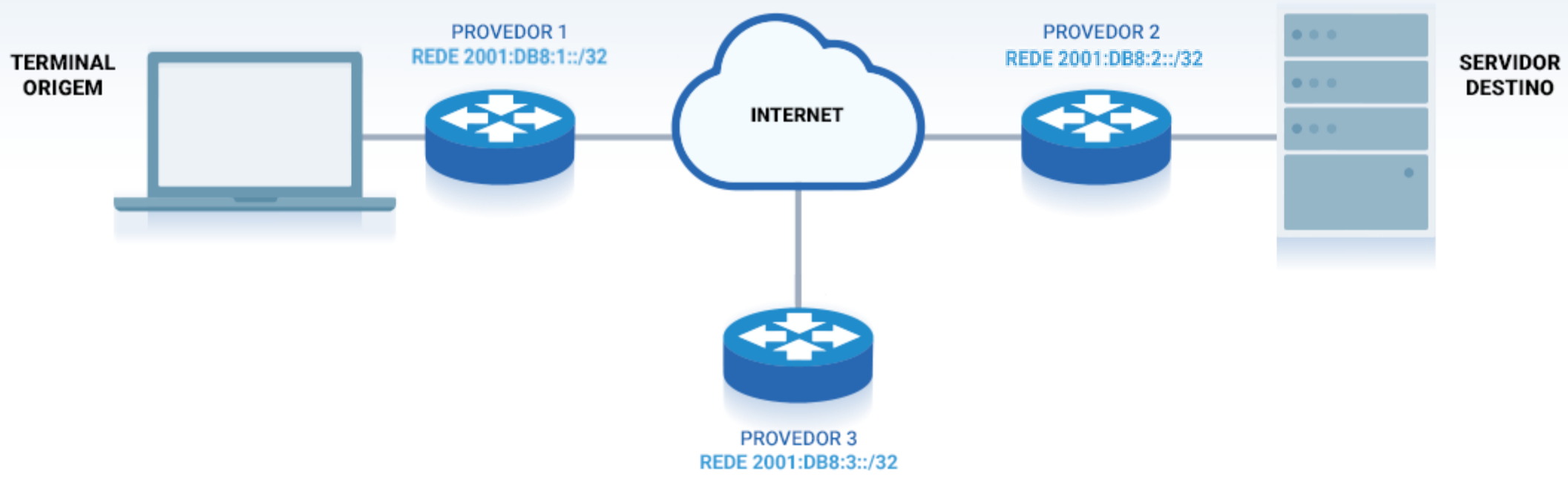
- **Como estamos em relação à segurança ?**

Ataques mais frequentes na infraestrutura da rede

Segurança e estabilidade da Internet

Ataque DoS por reflexão

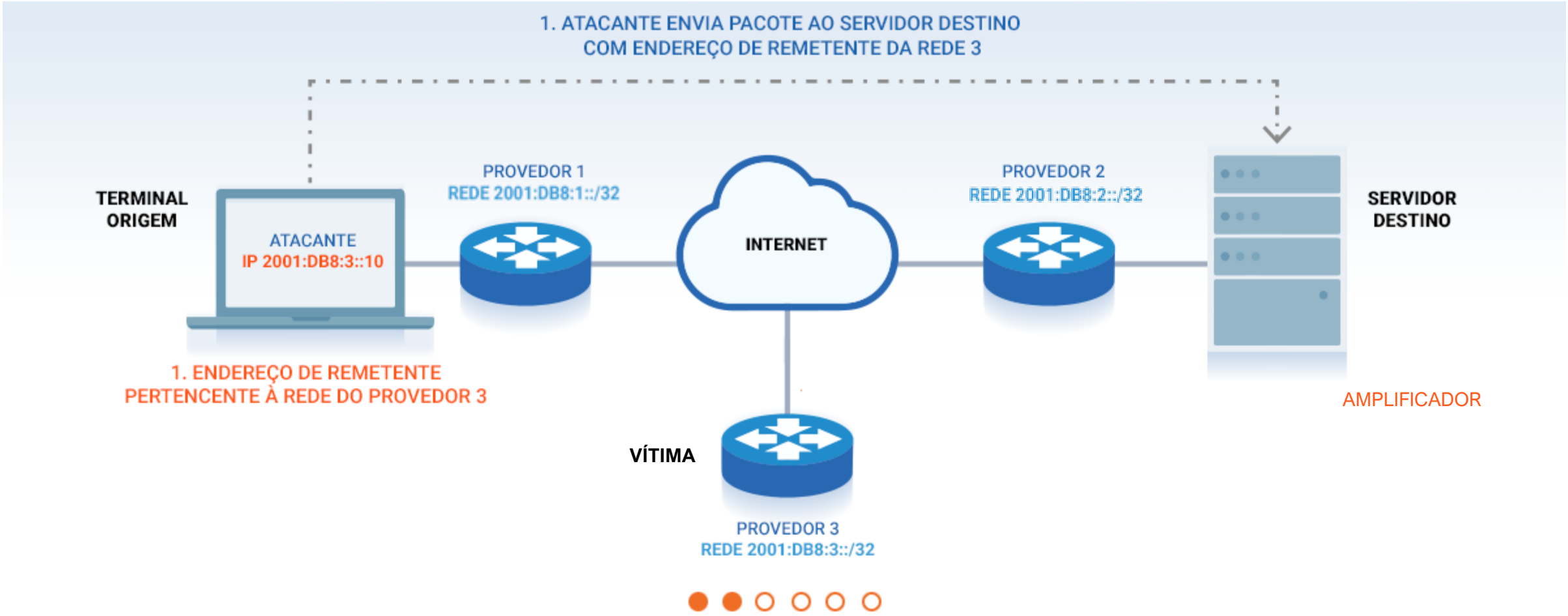
Topologia de rede sem filtros antispoofing



Segurança e estabilidade da Internet

Ataque DoS por reflexão

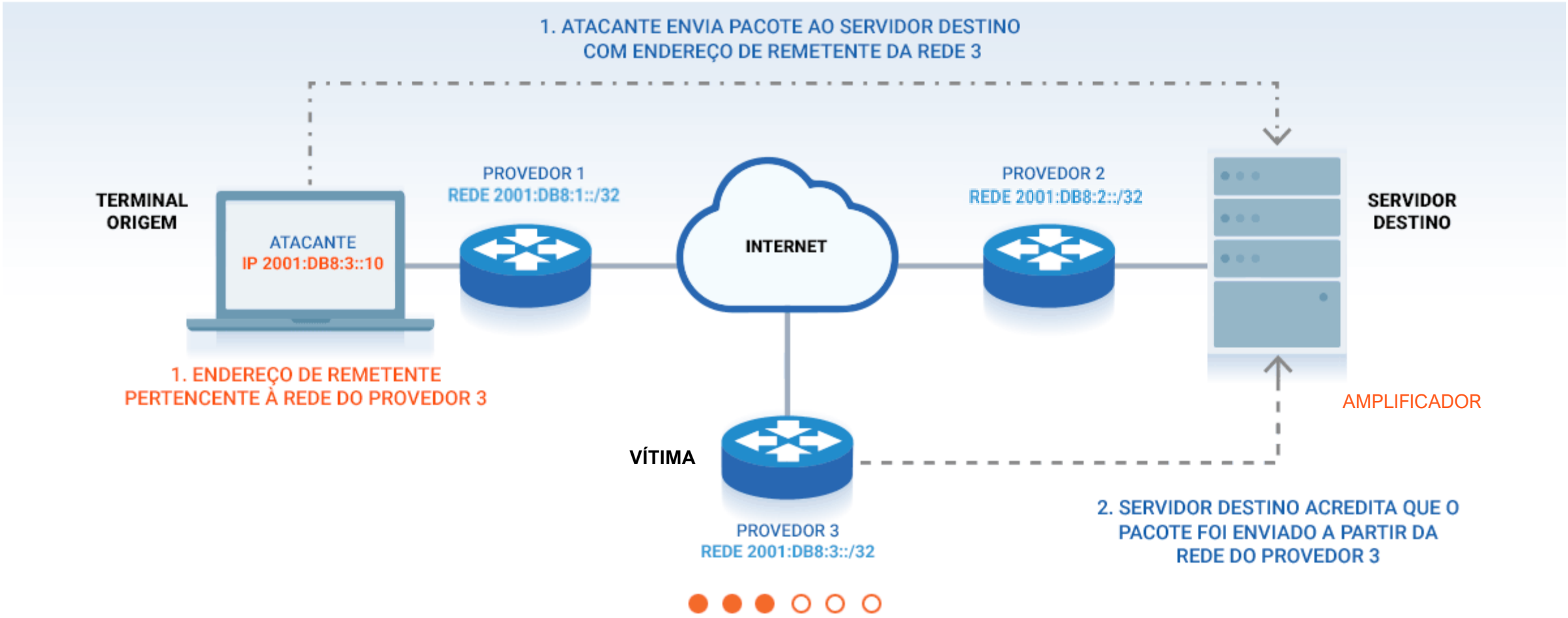
Ataque DoS utilizando endereço de remetente forjado (Spoofing)



Segurança e estabilidade da Internet

Ataque DoS por reflexão

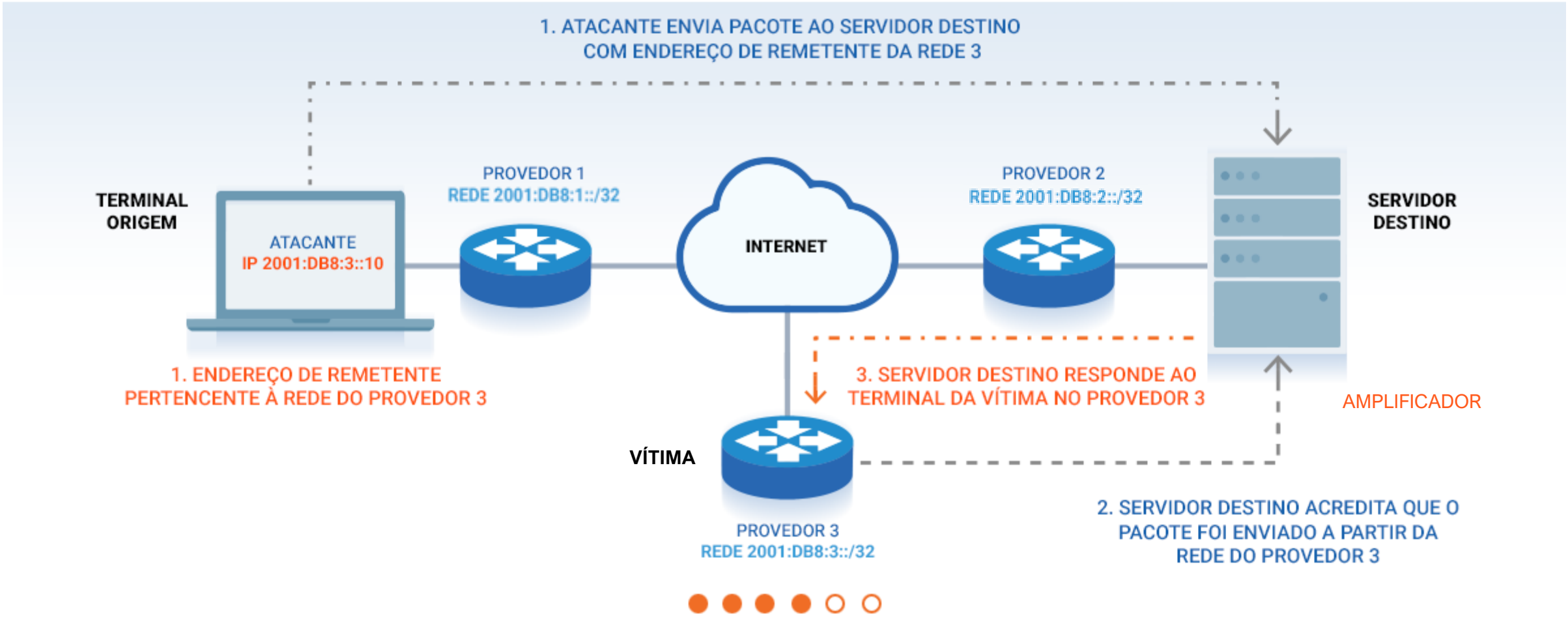
Ataque DoS utilizando endereço de remetente forjado (Spoofing)



Segurança e estabilidade da Internet

Ataque DoS por reflexão

Ataque DoS utilizando endereço de remetente forjado (Spoofing)



Segurança e estabilidade da Internet
Servidor Destino

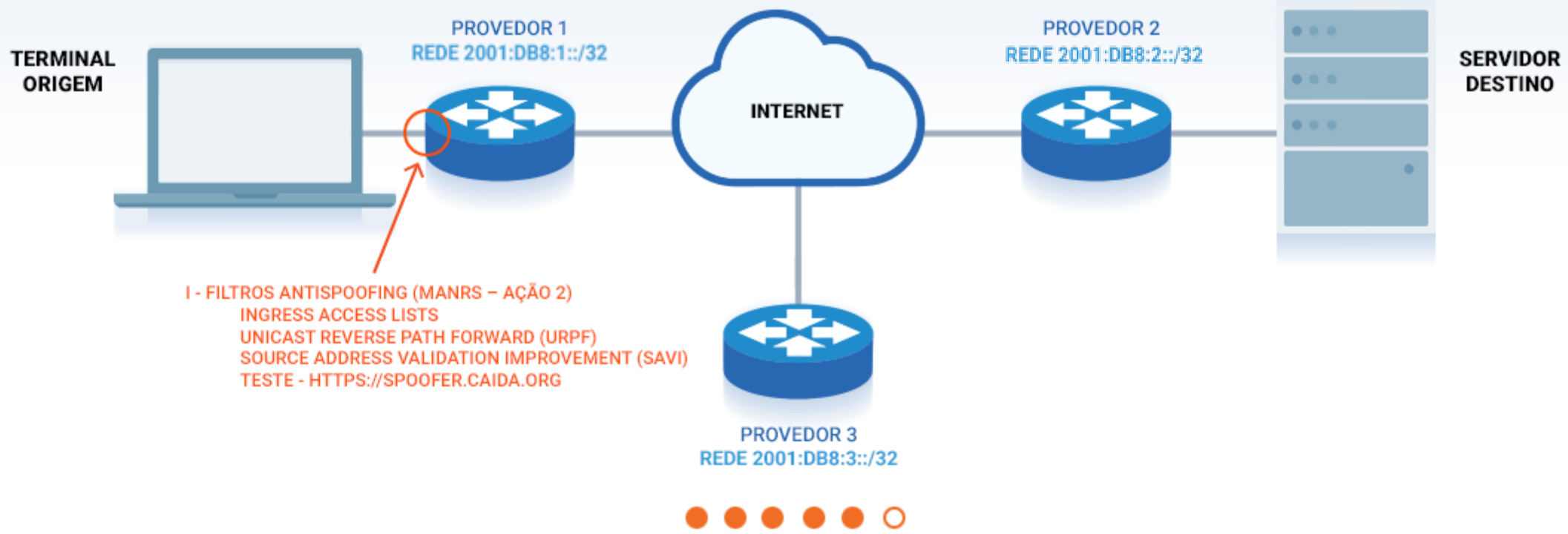
Os protocolos usados nos ataques fazem parte legítima da infraestrutura pública da Internet, porém em alguns equipamentos, como CPEs, são instalados por padrão e abusados por atacantes.

- **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

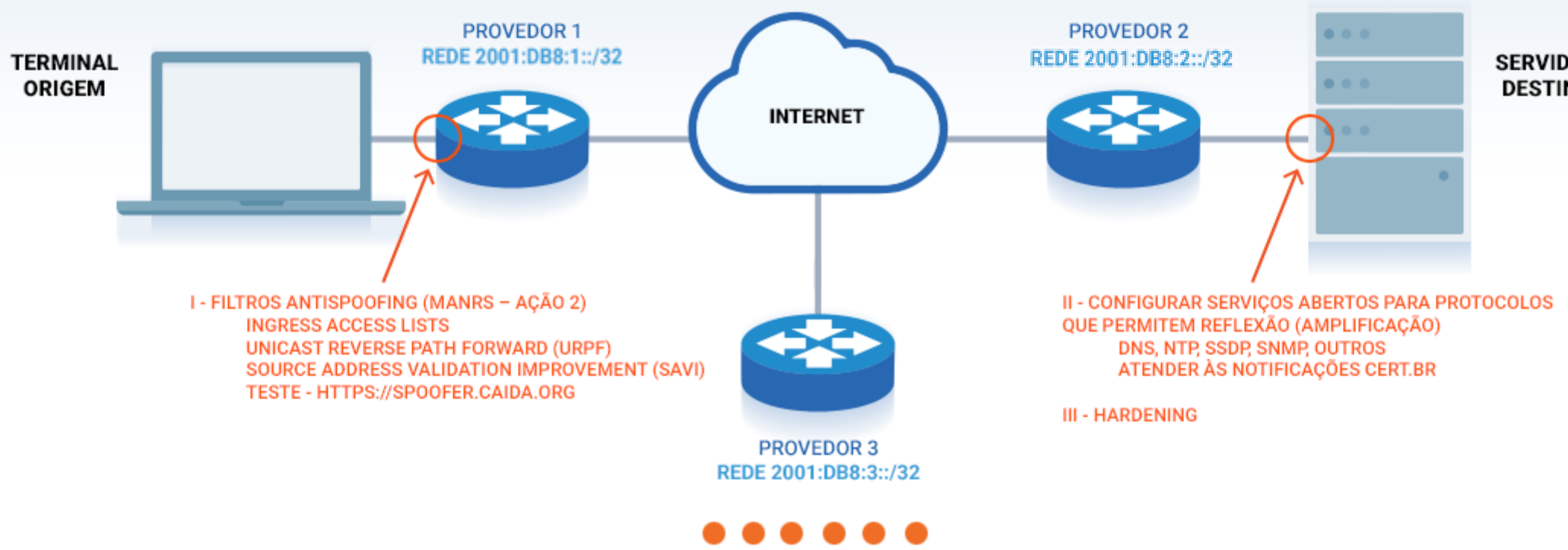
Solução: Aplicação de filtros antispoofing



Segurança e estabilidade da Internet

Ataque DoS por reflexão

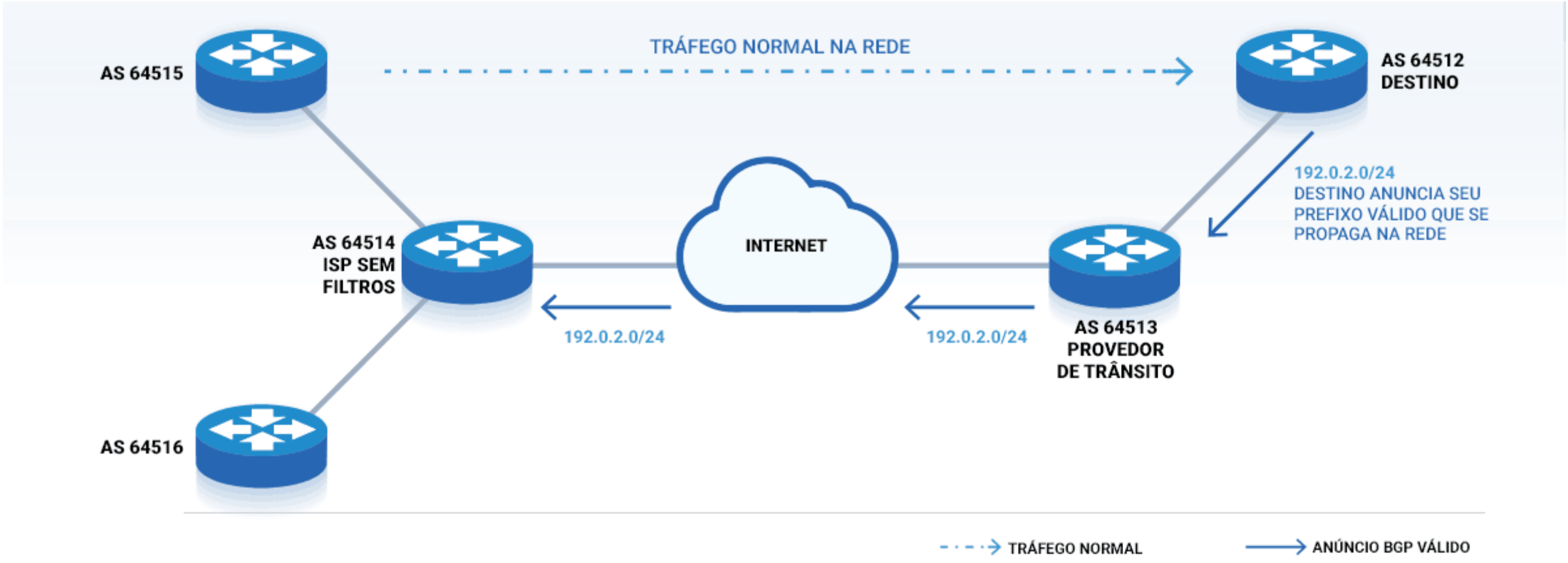
Solução: Aplicação de filtros antispoofing, configuração de serviços e Hardening



Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

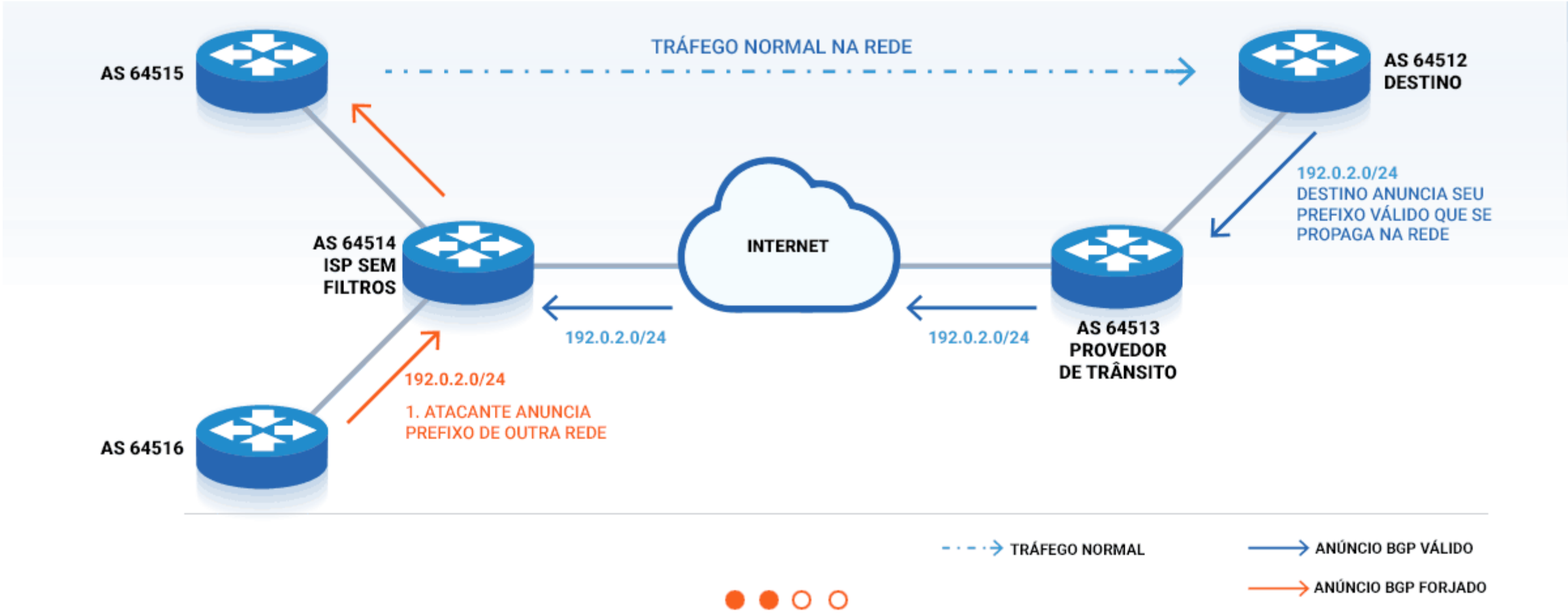
Topologia de rede sem filtros de anúncios



Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

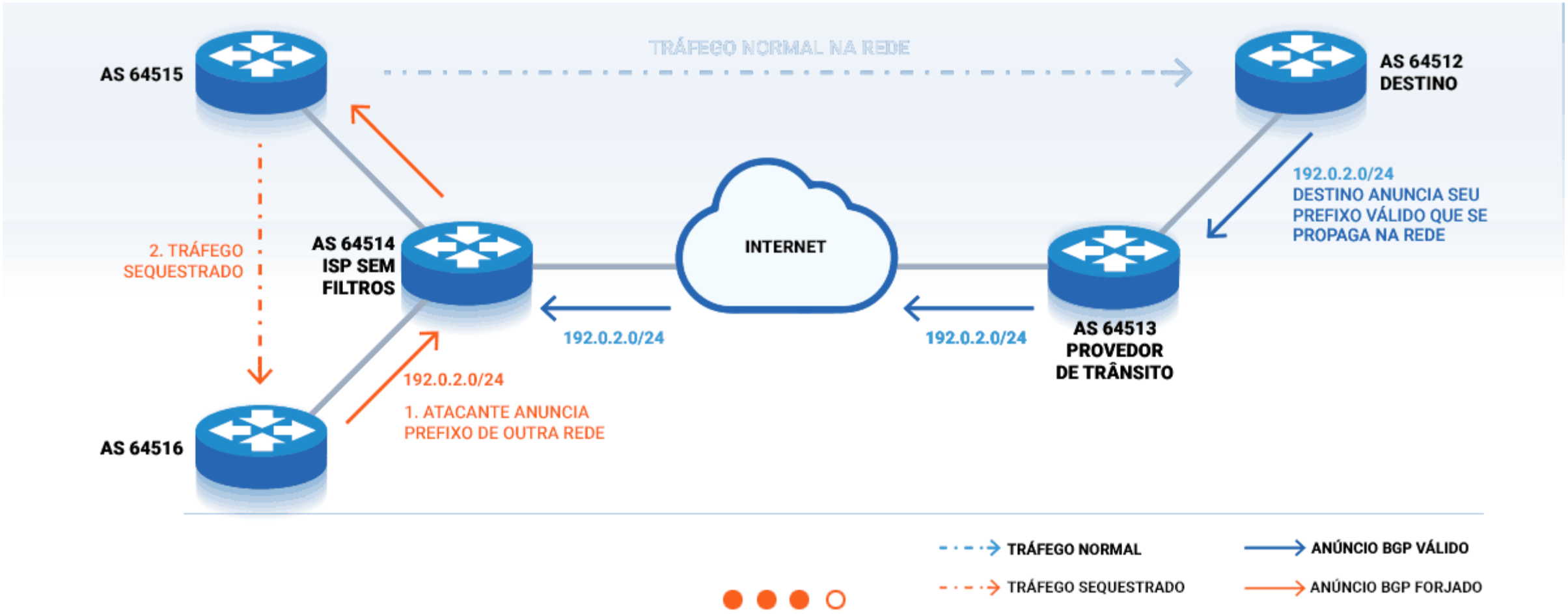
Topologia de rede sem filtros de anúncios



Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

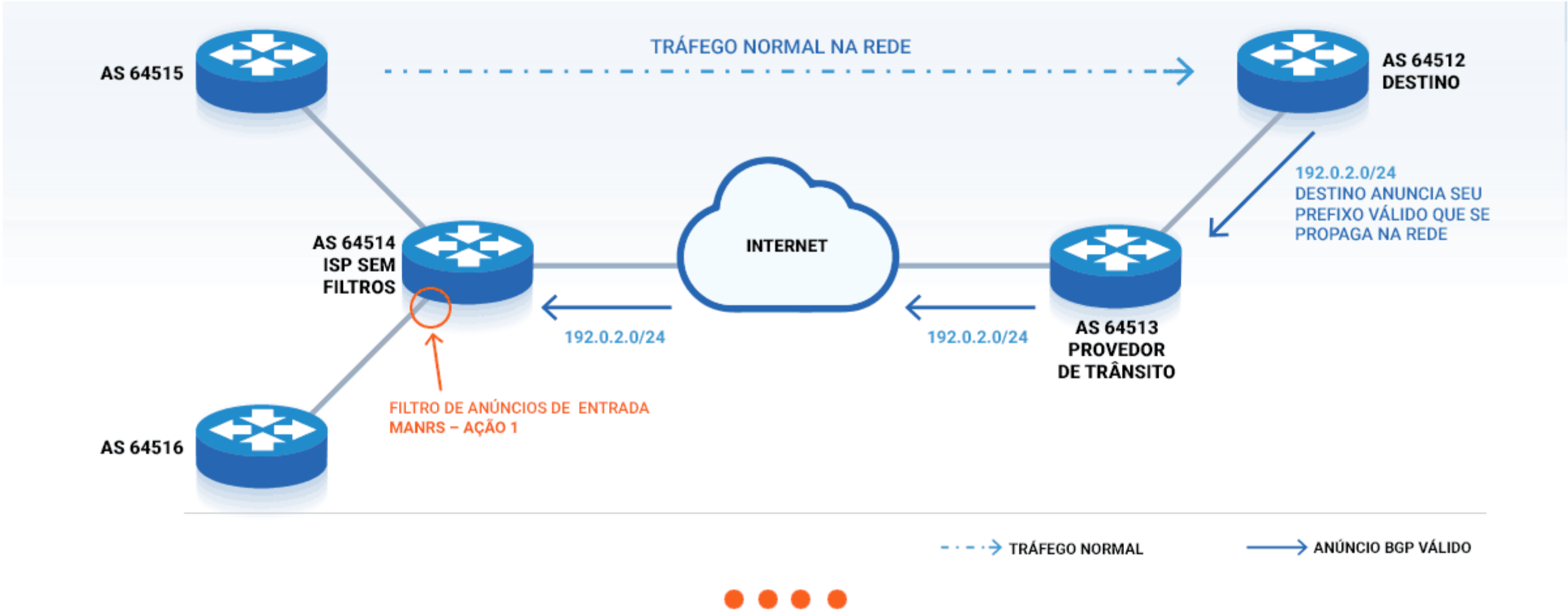
Topologia de rede sem filtros de anúncios



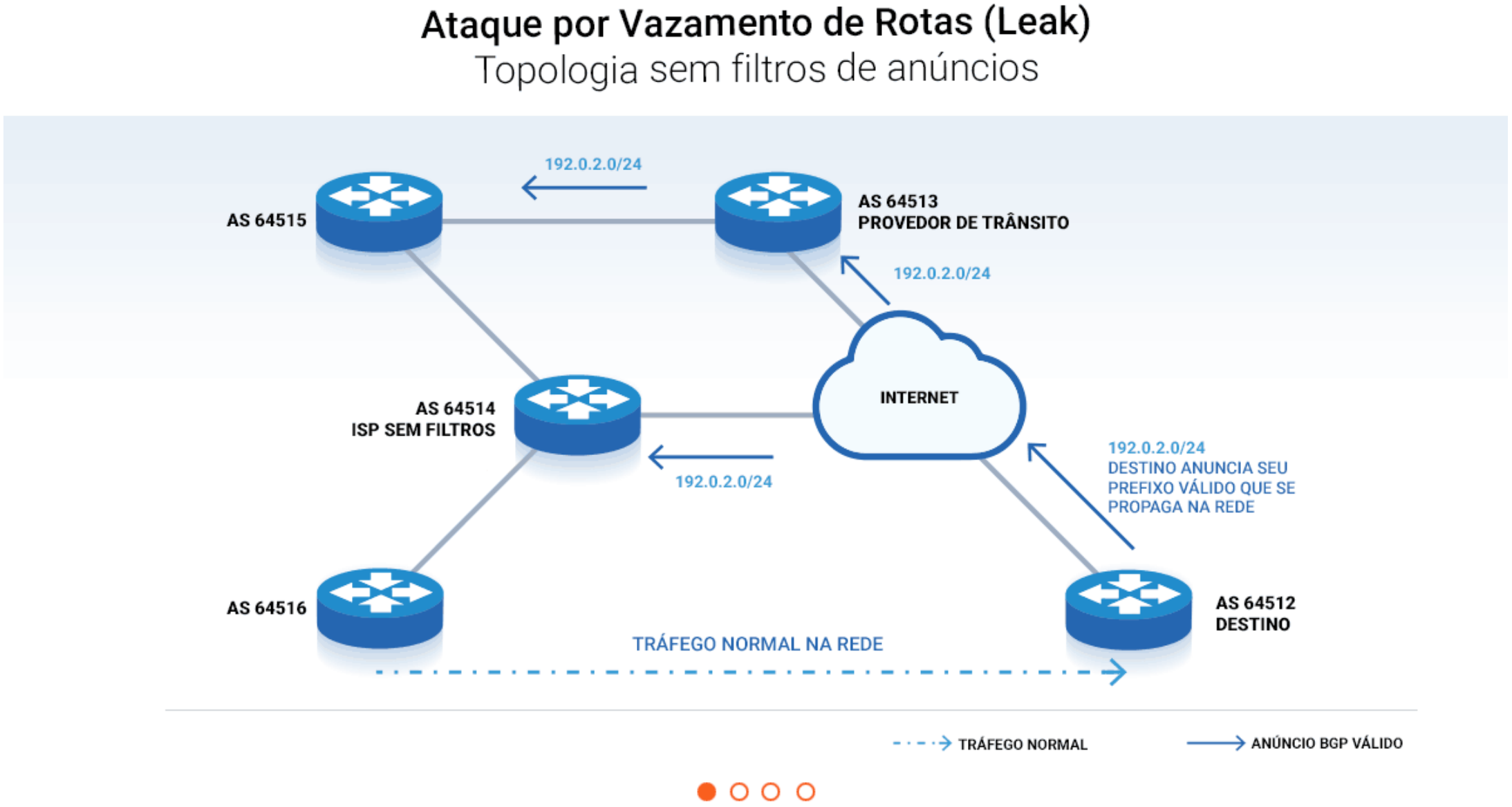
Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

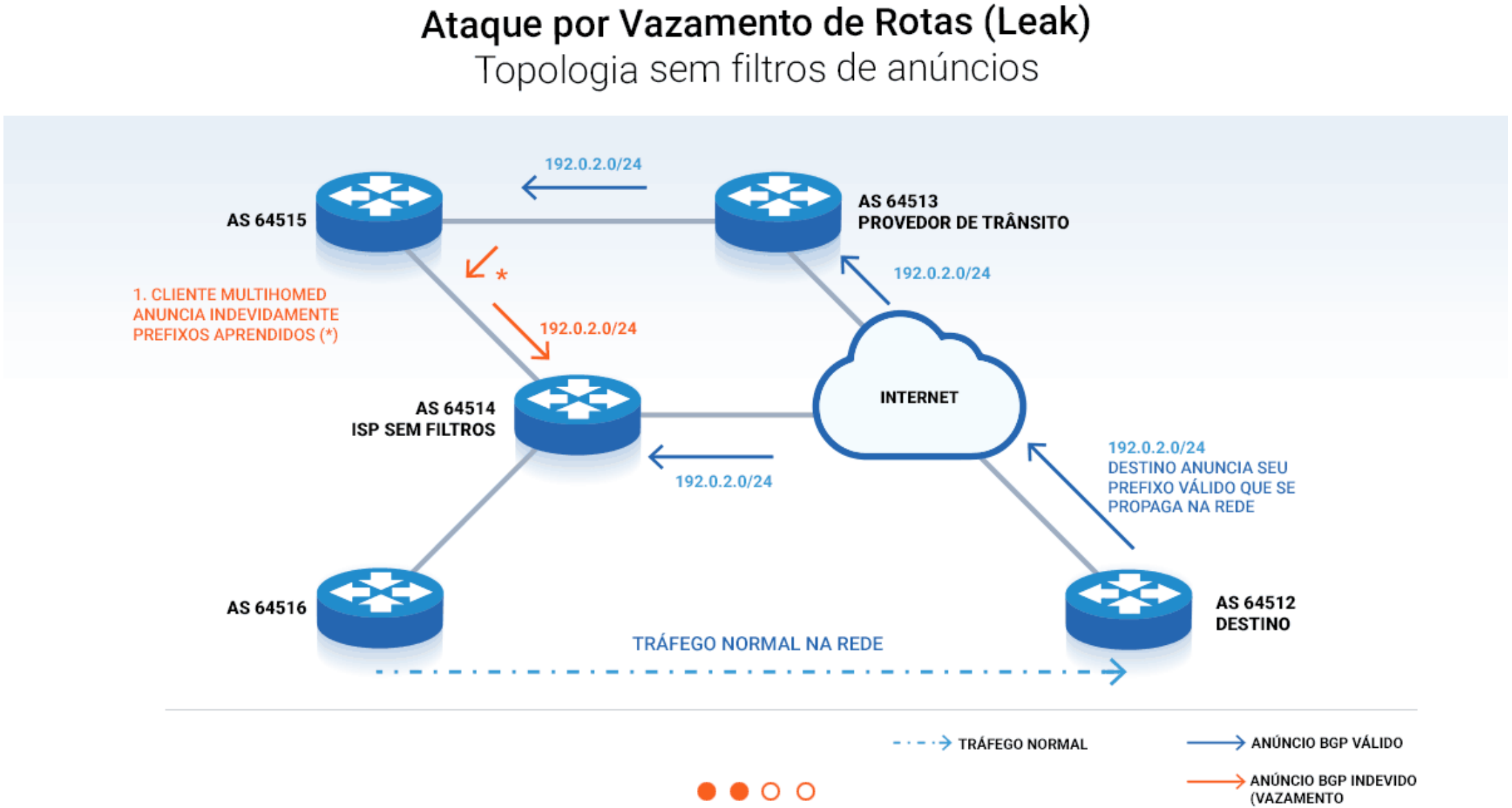
Solução: Filtro de anúncios de entrada (clientes) – MANRS - Ação 1



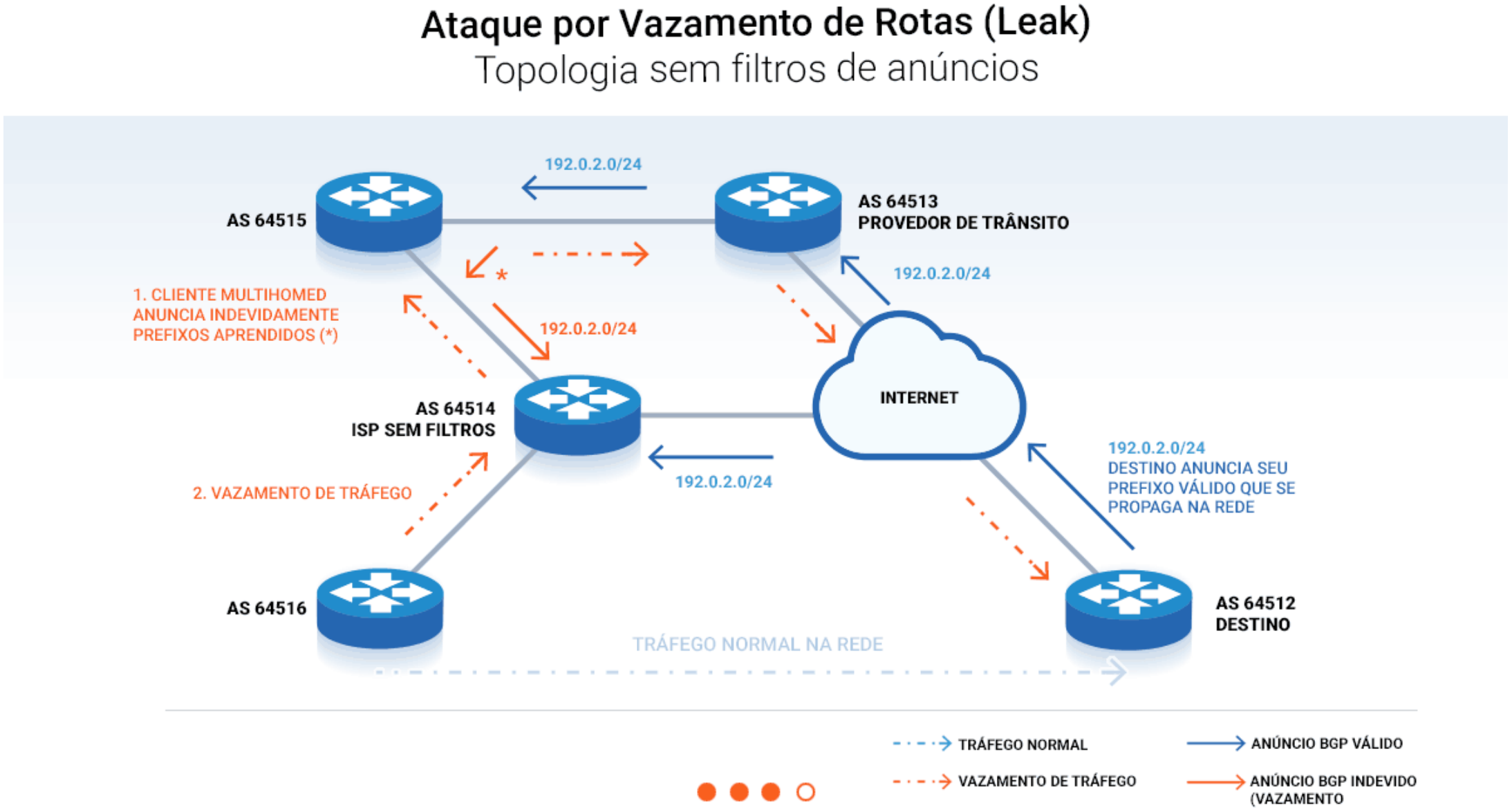
Segurança e estabilidade da Internet



Segurança e estabilidade da Internet



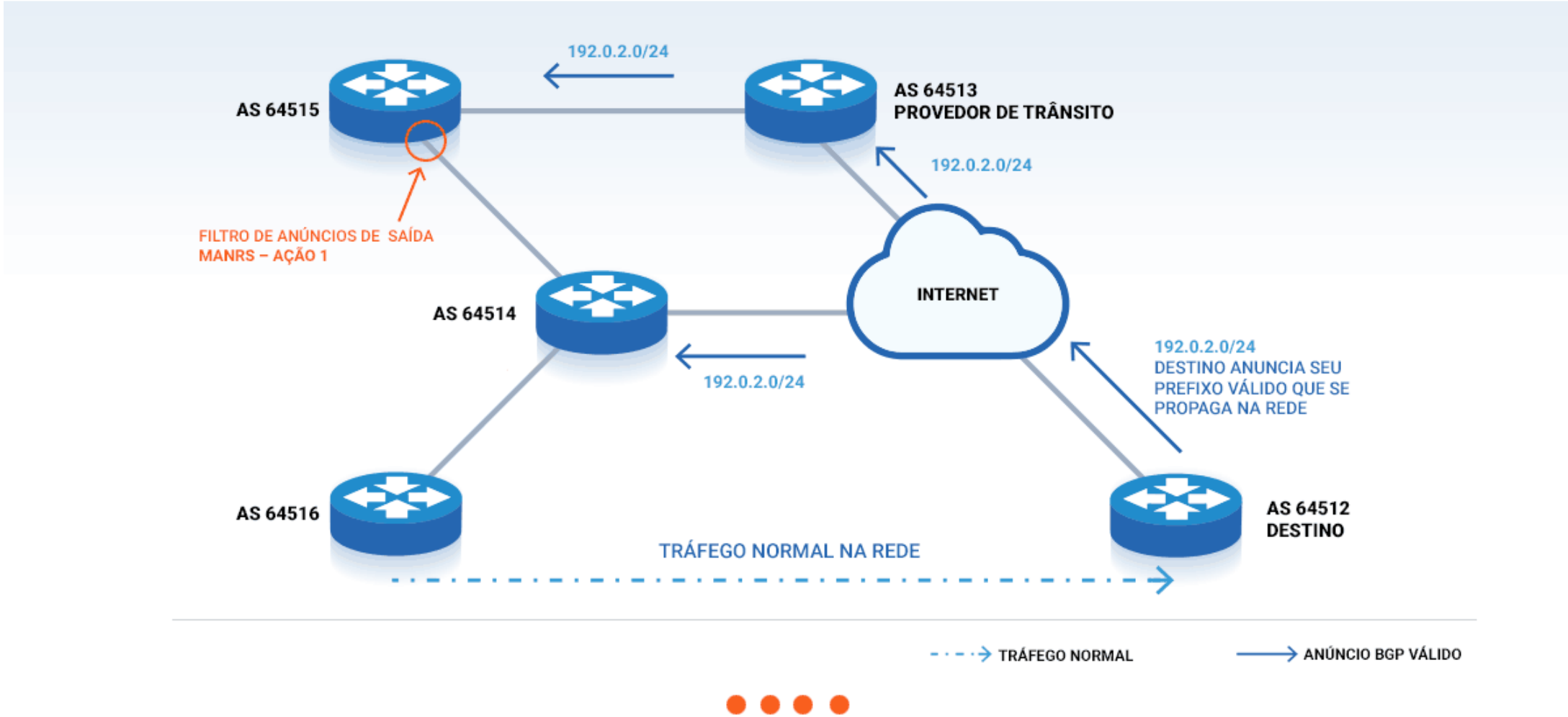
Segurança e estabilidade da Internet



Segurança e estabilidade da Internet

Ataque por Vazamento de Rotas (Leak)

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



Programa por uma Internet mais 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, ABRANET, SindiTelebrasil, ABRINT

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

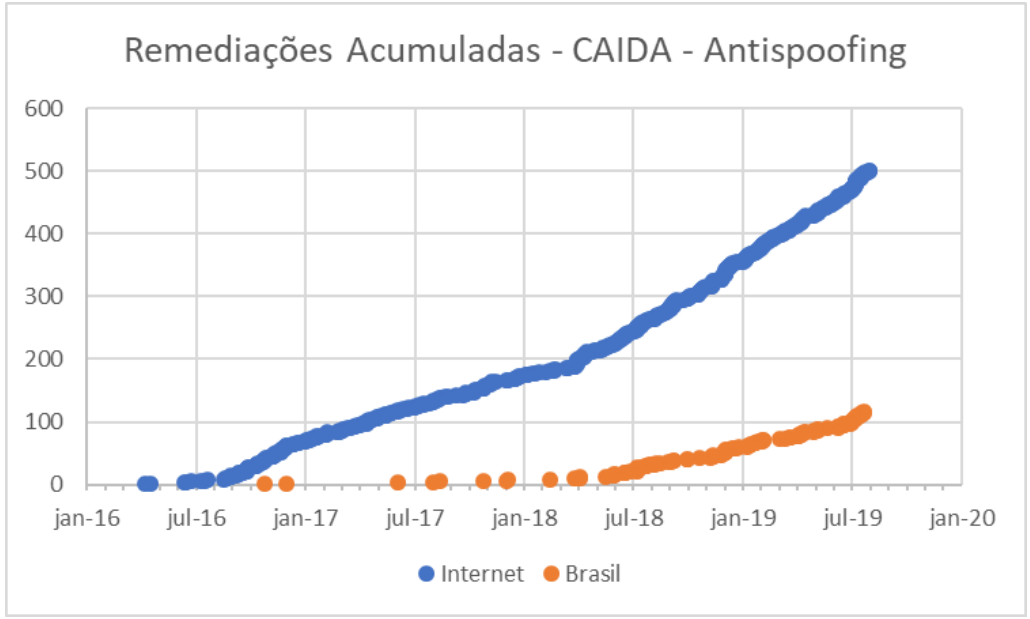
Para solucionar os problemas de segurança, as ações devem ser realizadas pelos operadores dos Sistemas Autônomos, com apoio do NIC.br

Ações coordenadas a serem executadas pelo NIC.br:

- Conscientização por meio de palestras, cursos e treinamentos
- **Criação de materiais didáticos e boas práticas**
- 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
Desenvolvimento do Programa

- Curso de Boas Práticas Operacionais p/ Sistemas Autônomos – BCOP
- Tutoriais sobre melhores práticas de roteamento e hardening
- Palestras sobre o Programa e o MANRS nos eventos do NIC.br e Associações parceiras



https://spoofer.caida.org/remedy.php

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- Interação com as maiores operadoras: redução de endereços IP mal configurados que permitem amplificação
  - Em mar/18: 581k grandes operadoras // 144k ISP e AS corporativos
  - Hoje: 147k grandes operadoras // 208k ISP e AS corporativos

Programa por uma Internet mais Segura
Endereços IP e ASN notificados pelo CERT.br

Brasil	DNS		SNMP		NTP		SSDP		UBNT	
mês	ASNs	IP	ASNs	IP	ASNs	IP	ASNs	IP	ASNs	IP
2018-08	2.459	56.555	2.411	397.622	895	89.353	613	11.855	0	0
2018-09	2.767	62.942	2.366	193.432	772	87.378	836	21.836	0	0
2018-10	2.806	64.912	2.383	163.987	856	85.911	789	20.233	0	0
2018-11	2.604	60.937	2.376	137.331	851	87.155	814	20.124	0	0
2018-12	2.849	64.649	2.361	137.463	719	82.610	832	21.704	0	0
2019-01	2.960	74.257	2.583	137.253	923	89.567	840	17.348	0	0
2019-02	2.905	69.093	2.556	136.401	944	80.838	868	20.689	2.690	180.756
2019-03	2.933	63.895	2.661	111.561	914	72.873	847	18.837	2.042	95.974
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	na	na	2.808	90.960	998	78.058	795	14.071	1.625	52.598

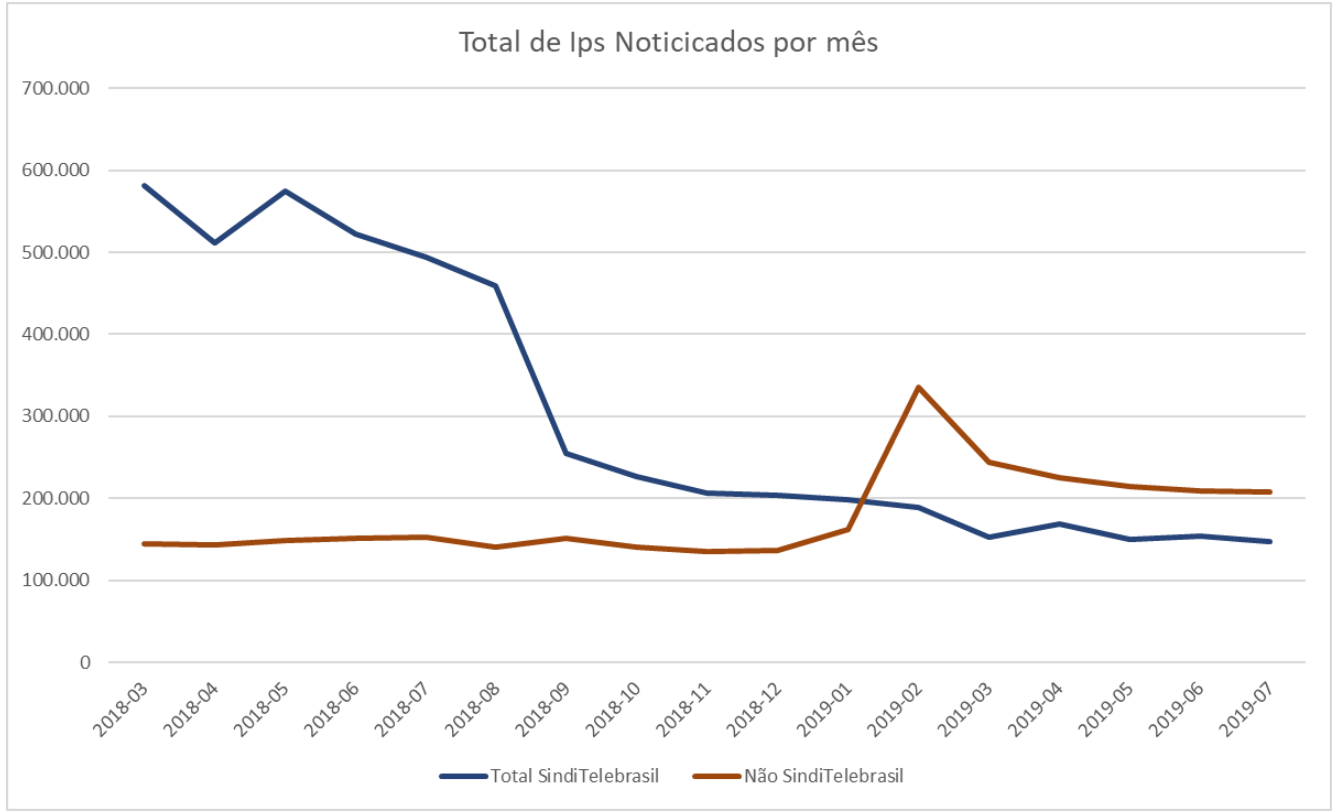
O Brasil está em **quarto** lugar entre os endereços IPs com serviço SNMP aberto

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

Fonte: https://snmpscan.shadowserver.org/

Programa por uma Internet mais Segura
Desenvolvimento do Programa

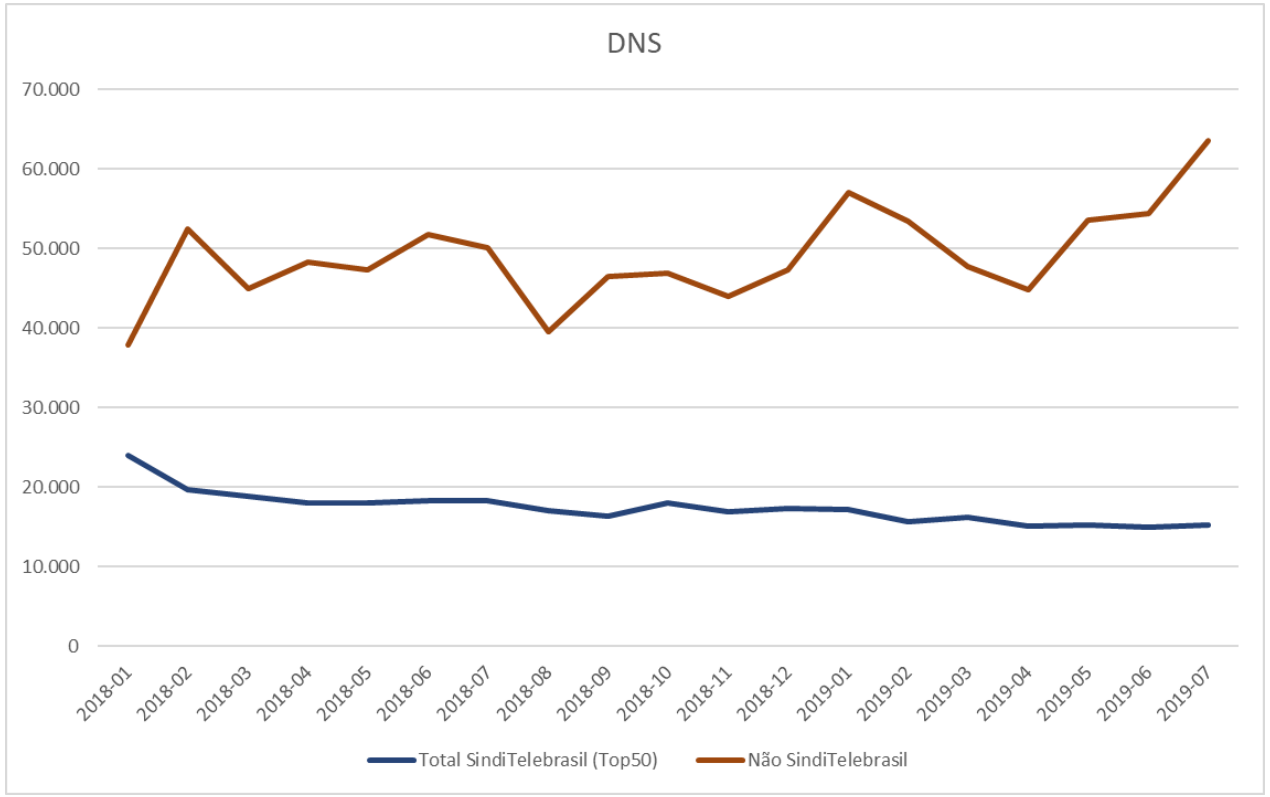
- Ações com as Associações e Provedores de Internet



Hoje são notificados mais endereços IP de ISPs do que operadoras

Programa por uma Internet mais Segura
Desenvolvimento do Programa

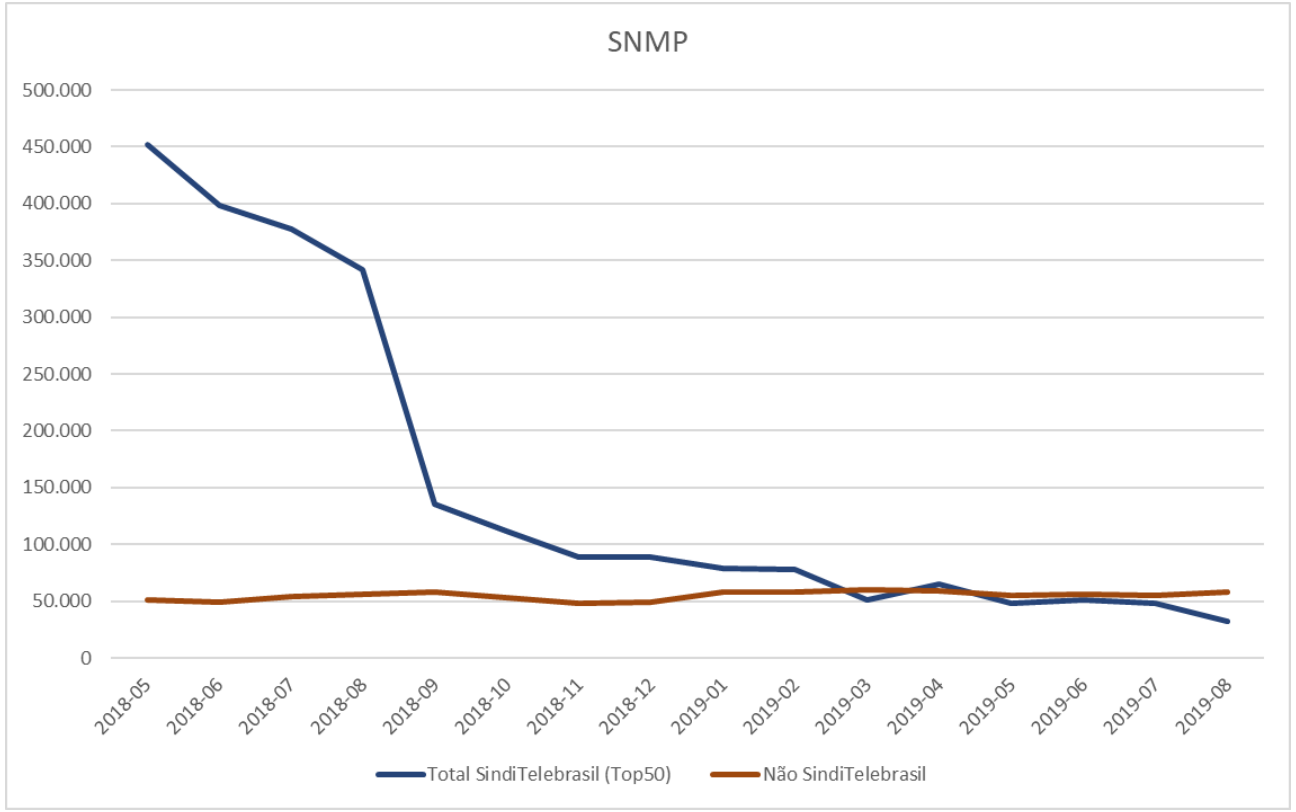
- Ações com as Associações e Provedores de Internet



Está em ritmo crescente as notificações de serviços DNS recursivos abertos em redes de ISPs

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- Ações com as Associações e Provedores de Internet



Hoje são notificados mais serviços SNMP habilitados de ISPs do que de operadoras

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

Programa por uma Internet mais Segura

Página WEB

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

Programa por uma Internet mais Segura
Ações necessárias da comunidade técnica

- **Configurar corretamente serviços que podem ser abusados em ataques de amplificação [5]**
  - **Conforme as notificações do CERT.br**
    - **https://bcp.nic.br/i+seg/acoes/amplificacao/**
- **Implementar as ações preconizadas pelo MANRS**
  - **Filtragem de rotas e endereços de origem falsos (antispoofing) e informações para ações colaborativas entre os operadores**
    - **https://bcp.nic.br/i+seg/acoes/manrs/**
- **Realizar o hardening de equipamentos e redes**
  - **Mapear ameaças, mitigar riscos e adotar ações corretivas**
    - **https://bcp.nic.br/i+seg/acoes/hardening/**

MANRS

MANRS

Mutually Agreed Norms for Routing Security

Apoiado pela Internet Society

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

MANRS

O Programa MANRS [2], apoiado pela Internet Society, preconiza a Segurança e Estabilidade na Internet

- **Estamos todos juntos nisso!!**
- Os operadores de rede têm a responsabilidade em assegurar uma infraestrutura de roteamento robusta, confiável!
- **A segurança da sua rede depende das demais redes!**
- A segurança das outras redes depende da sua rede!
- **Implemente as ações do MANRS e junte-se à iniciativa**
- **Quanto mais operadores de rede trabalharem juntos menos problemas todos terão!**

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)

Programa por uma Internet mais Segura

Como Resolver os problemas

Todos devem implementar estas recomendações [9]:

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**
   - 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**
   - Facilita a validação de roteamento em escala global

Programa por uma Internet mais Segura

Benefícios

Os Provedores se beneficiam com a implantação do MANRS:

- Adiciona um **valor competitivo** em um mercado onde todos oferecem serviços semelhantes e direcionado ao **preço**
- **Mostra aos seus clientes competência e comprometimento na área de segurança**
- Ajuda a resolver problemas de rede
- **Empresas indicam que pagariam mais por serviços efetivamente seguros (Pesquisa 451 Research)**

- **Vinte e uma empresas brasileiras já participam da iniciativa MANRS**
- **Inscreva-se no programa MANRS, diferencie-se num mercado competitivo…**

Hardening

Programa por uma Internet mais Segura
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**
- Autorização
- **Acesso**
- Auditoria

- **Sistema**
- Registros
- **Configurações**

https://bcp.nic.br/i+seg/acoes/hardening/

Requisitos Mínimos para aquisição de CPEs

Minimum security requirements for CPEs acquisition

O LACNOG BCOP WG e LAC-AAWG, em parceria com M³AAWG 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.lacnog.net/wp-content/uploads/2019/05/LAC-BCOP-1-M3AAWG-v1.pdf

O documento será disponibilizado em português pelo site https://bcp.nic.br

- **Utilize...**

Minimum security requirements for CPEs acquisition

As vulnerabilidades abordadas no documento incluem:

- **credenciais padrão para vários dispositivos**
- credenciais que não podem ser modificadas
- **uso de protocolos e algoritmos obsoletos e inseguros**
- acessos não documentados (backdoors)
- **falta de atualizações e correções de segurança**
- serviços desnecessários e / ou inseguros habilitados por padrão
- **serviços que não podem ser desativados**
- ausência de gerenciamento remoto e mecanismos seguros de atualização

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, dia 1, parte 1, São Paulo, SP

[2] https://www.manrs.org/manrs/ - MANRS for Network Operators

[3] https://bcp.nic.br/antispoofing - Boas Práticas de Antispoofing

[4] https://bcp.nic.br/ddos - Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)

[5] https://bcp.nic.br/notificacoes - Recomendações para Notificações de Incidentes de Segurança

[6] https://www.caida.org/projects/spoofer/ - Tool to access and report source address validation

[7] Ataques Mais Significativos e Como Melhorar o Cenário, IX Fórum Regional, 10/2017

https://www.cert.br/docs/palestras/certbr-ix-forum-sp-2017-10-20.pdf

https://youtu.be/R55-cTBTLcU?t=2h36m25s

[8] Problemas de Segurança e Incidentes com CPEs e Outros Dispositivos, 20º Fórum de Certificação para Produtos de Telecomunicações, Anatel, 11/2016, Campinas, SP

https://www.cert.br/docs/palestras/certbr-forum-anatel2016.pdf

[9] http://www.nic.br/videos/ver/como-resolver-os-problemas-de-seguranca-da-internet-e-do-seu-provedor-ou-sistema-autonomo/

Obrigado

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

gzorello@nic.br

16 de agosto de 2019

nic.br cgi.br

www.nic.br | www.cgi.br