

The background of the entire image is a dark grey circuit board pattern with white lines representing traces and components. The top and bottom sections of the image are framed by this pattern, while the middle section is a solid light grey gradient.

nic.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

Workshop TelComp - Lei de Proteção de Dados e Segurança de Redes
São Paulo | 25/6/19

MELHORES PRÁTICAS DE SEGURANÇA PARA A INFRAESTRUTURA DA INTERNET

PROGRAMA POR UMA INTERNET MAIS SEGURA

Gilberto Zorello | gzorello@gmail.com

registro.br nic.br cgi.br



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

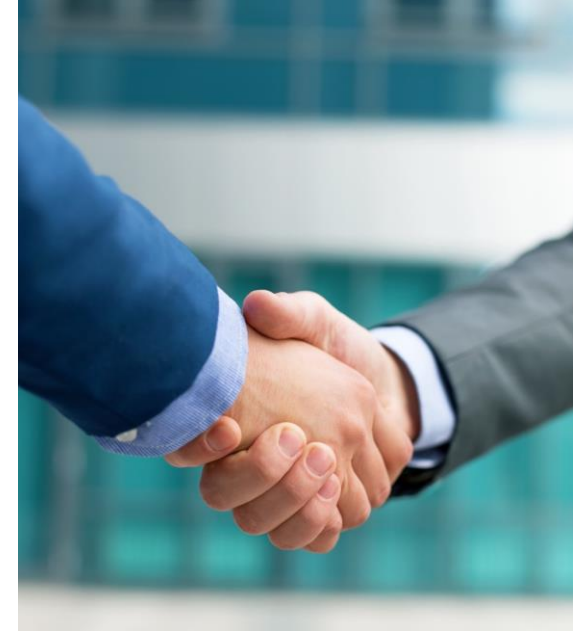
Panorama atual

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 **60.000 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

CNET > Tech Culture > How Pakistan knocked YouTube offline (and how to make sure it never happens again)

How Pakistan knocked YouTube offline (and how to make sure it never happens again)

Posted by Andree Toonk - November 6, 2015 - Hijack - 1 Comment

Large scale BGP hijack out of India

Massive route leak causes internet slowdown

Routing Leak briefly takes down Google

Global Collateral Damage of TMnet leak

DDoS Attacks Storm Linode Servers Worldwide

BY DOUGLAS BONDERUD • JANUARY 5, 2016

UK traffic diverted through Ukraine

Global Impacts of Rece

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

Un-going BGP Hijack Targets Palestinian ISP

BGP hijack incident by Syrian Telecommunication

The Vast World of Fraudulent Routing

CSO Most read: [v]

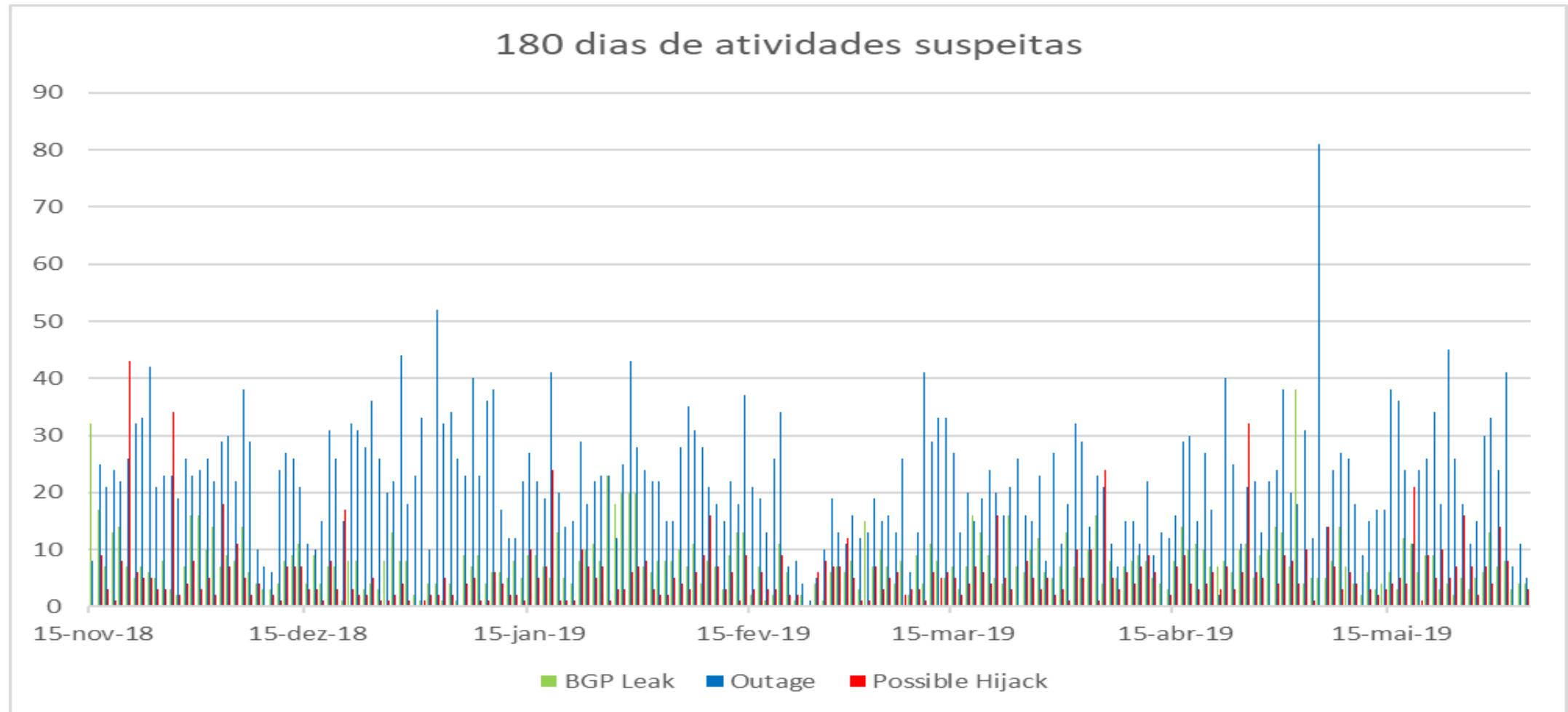
Home > Data Protection > Cyber Attacks/Espionage

TODAY'S TOP STORIES

DDoS attack on BBC may have been biggest in history

Segurança e estabilidade da Internet

Nenhum dia sem um incidente



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

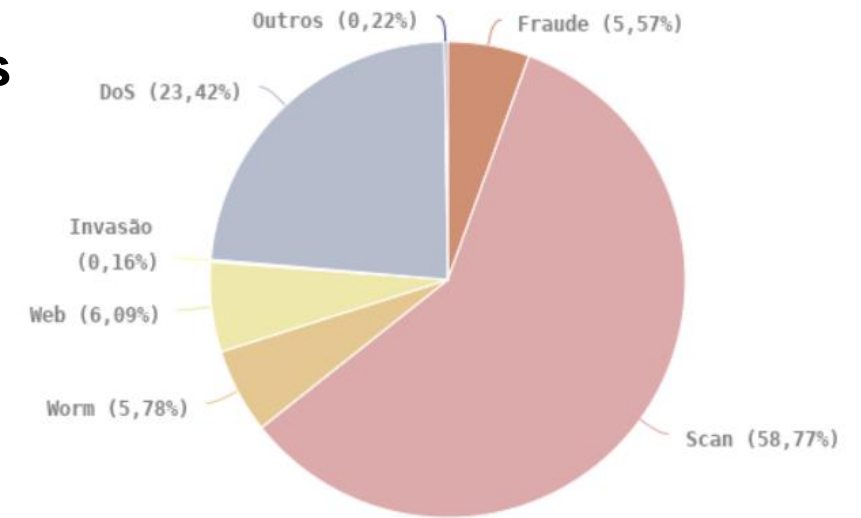
Segurança e estabilidade da Internet Panorama Atual

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
- **Medições em “honeypots” distribuídos na Internet**
- Medições no IX

Incidentes Reportados ao CERT.br
Janeiro a Dezembro de 2018
Tipos de ataque



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

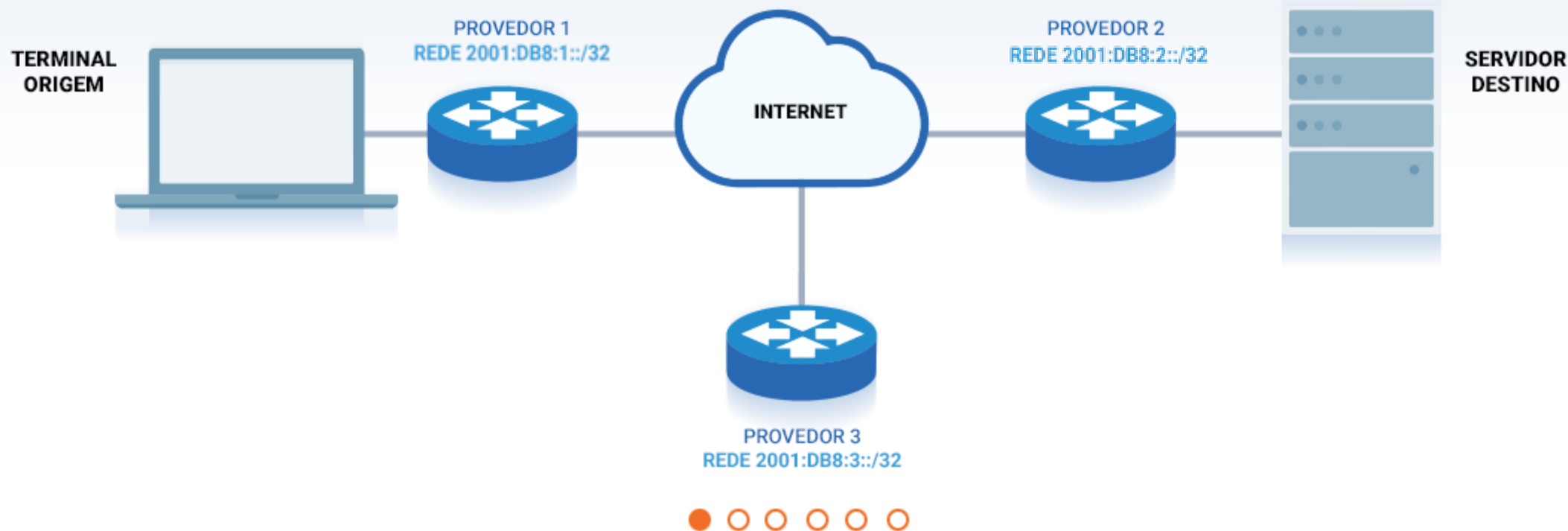
Constata-se um ritmo crescente de notificações de varreduras e DoS [4]

Ataques mais frequentes na infraestrutura da rede

Segurança e estabilidade da Internet

Ataque DoS por reflexão

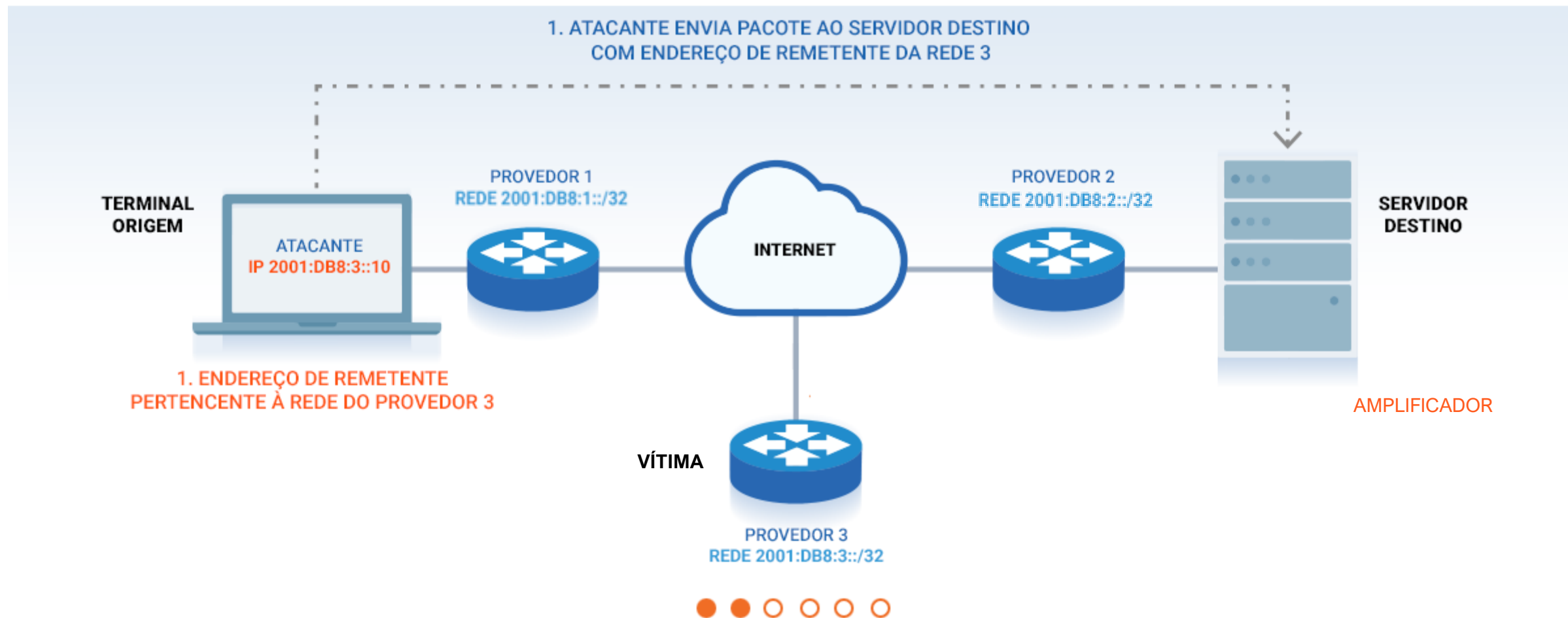
Topologia de rede sem filtros antispoofing



Segurança e estabilidade da Internet

Ataque DoS por reflexão

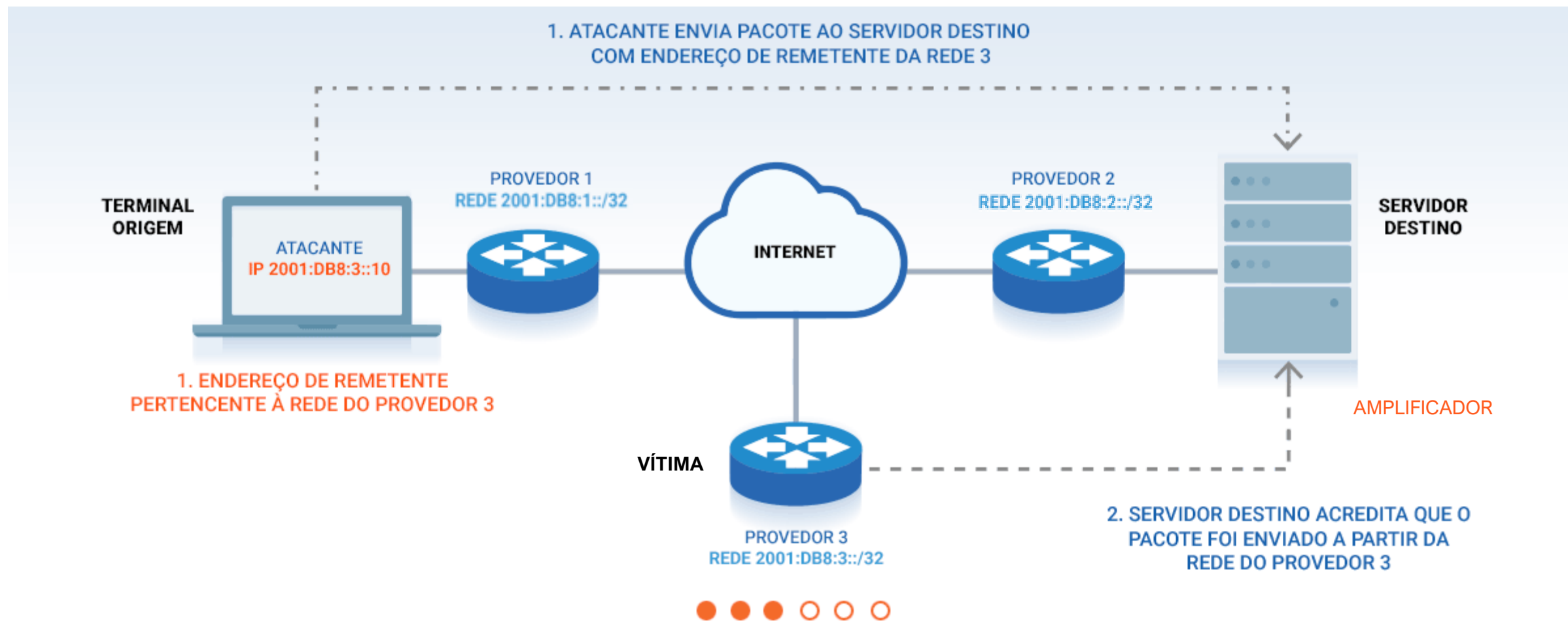
Ataque DoS utilizando endereço de remetente forjado (Spoofing)



Segurança e estabilidade da Internet

Ataque DoS por reflexão

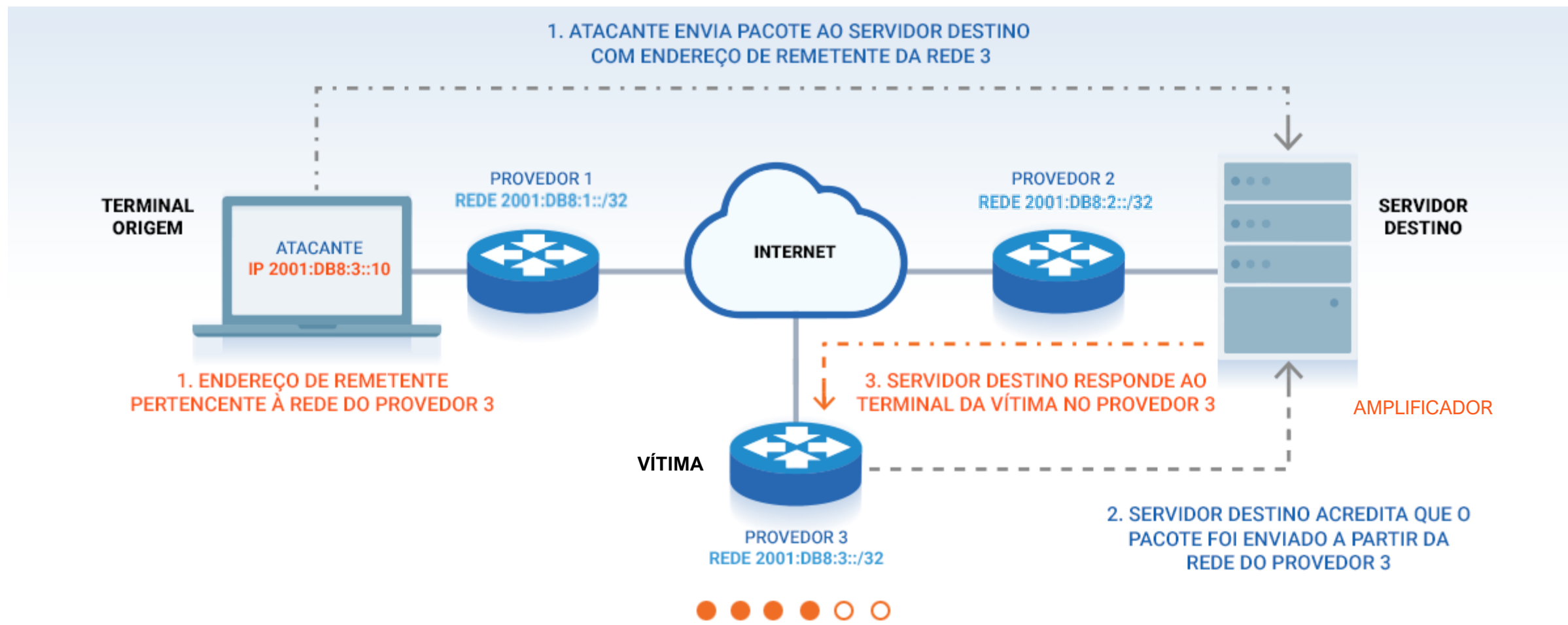
Ataque DoS utilizando endereço de remetente forjado (Spoofing)



Segurança e estabilidade da Internet

Ataque DoS por reflexão

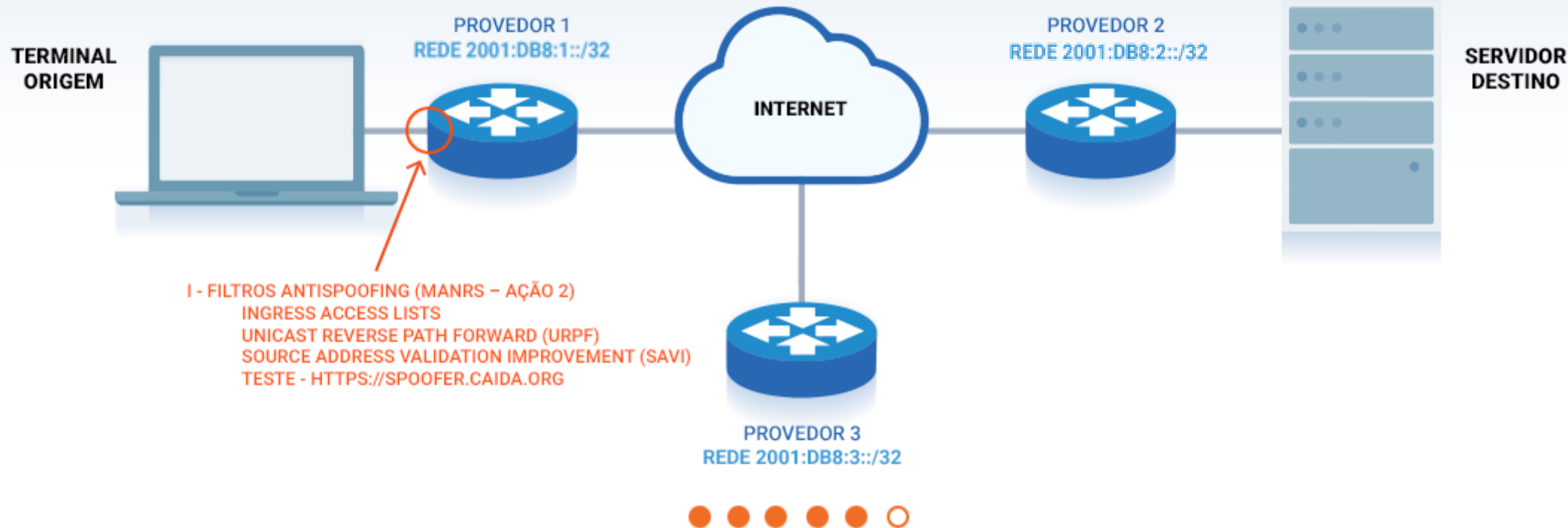
Ataque DoS utilizando endereço de remetente forjado (Spoofing)



Segurança e estabilidade da Internet

Ataque DoS por reflexão

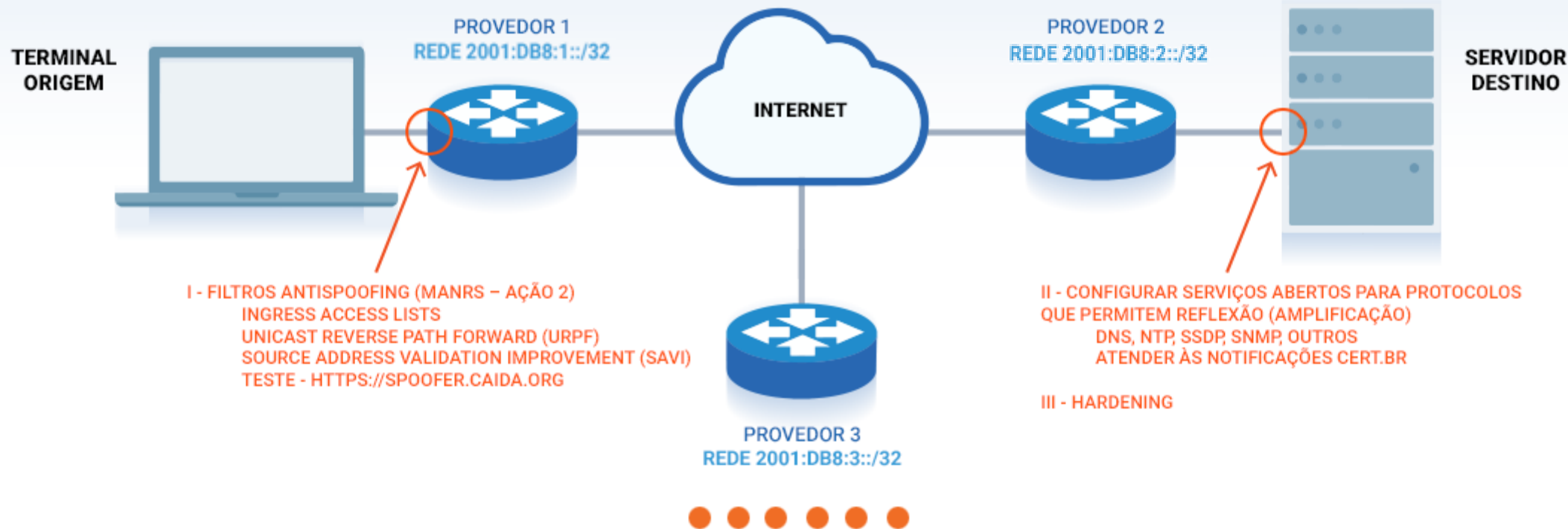
Solução: Aplicação de filtros antispoofing



Segurança e estabilidade da Internet

Ataque DoS por reflexão

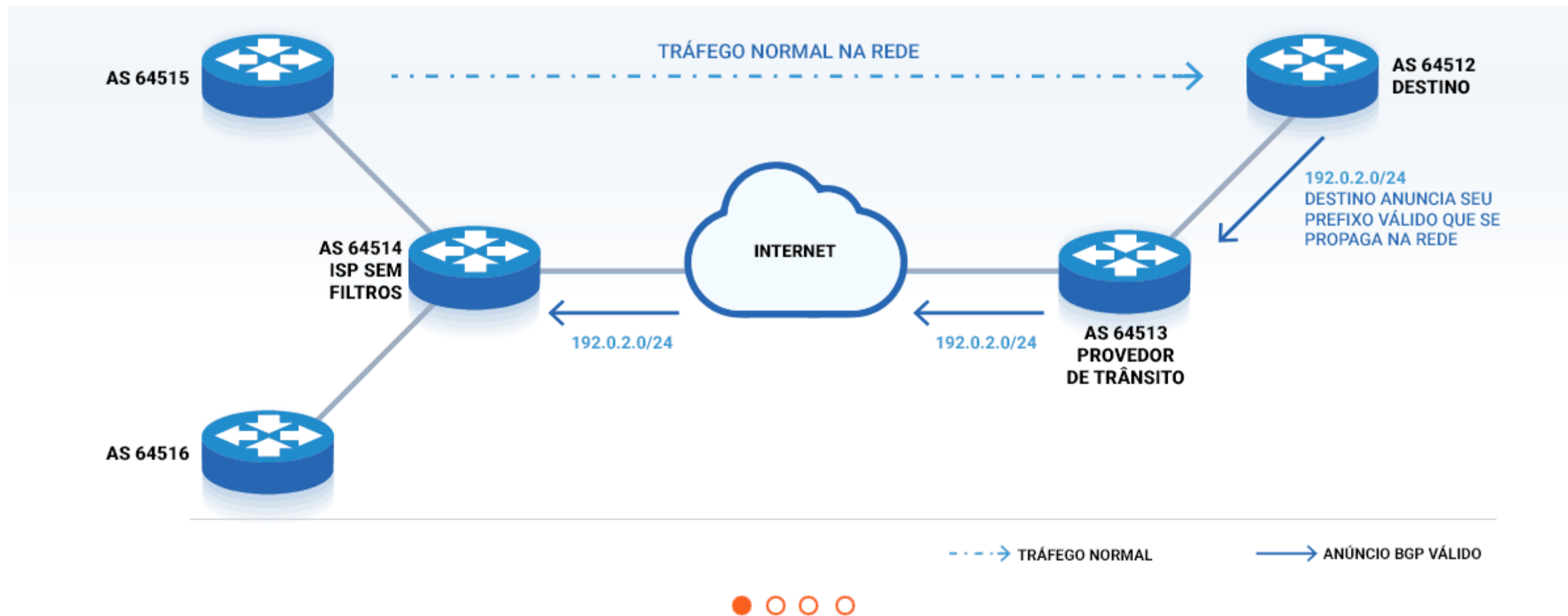
Solução: Aplicação de filtros antispoofing, configuração de serviços e Hardening



Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

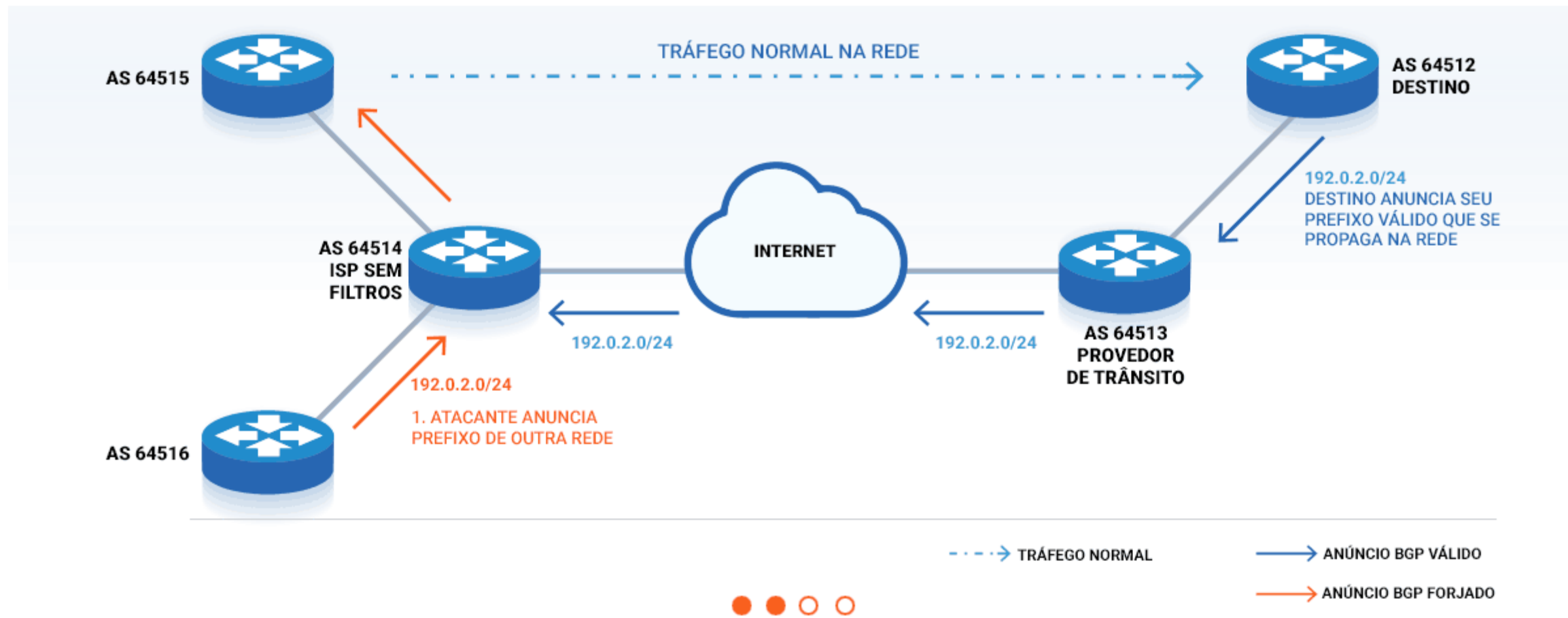
Topologia de rede sem filtros de anúncios



Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

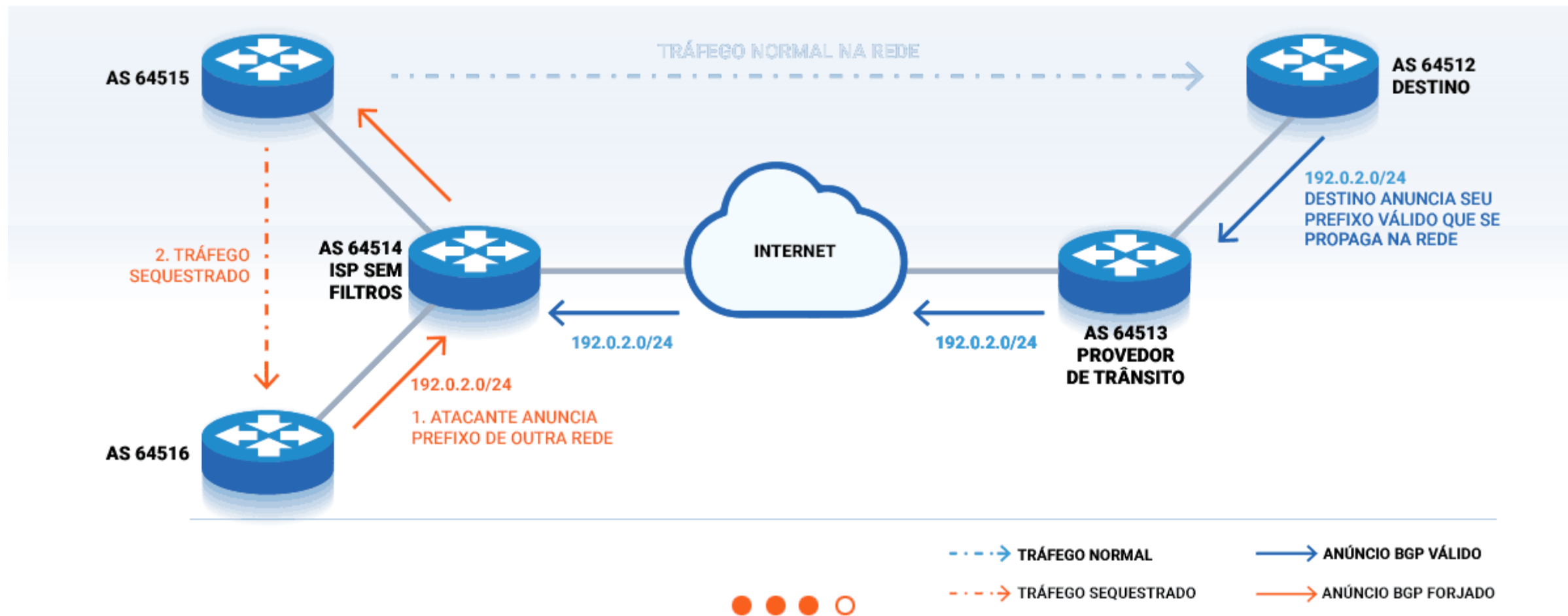
Topologia de rede sem filtros de anúncios



Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

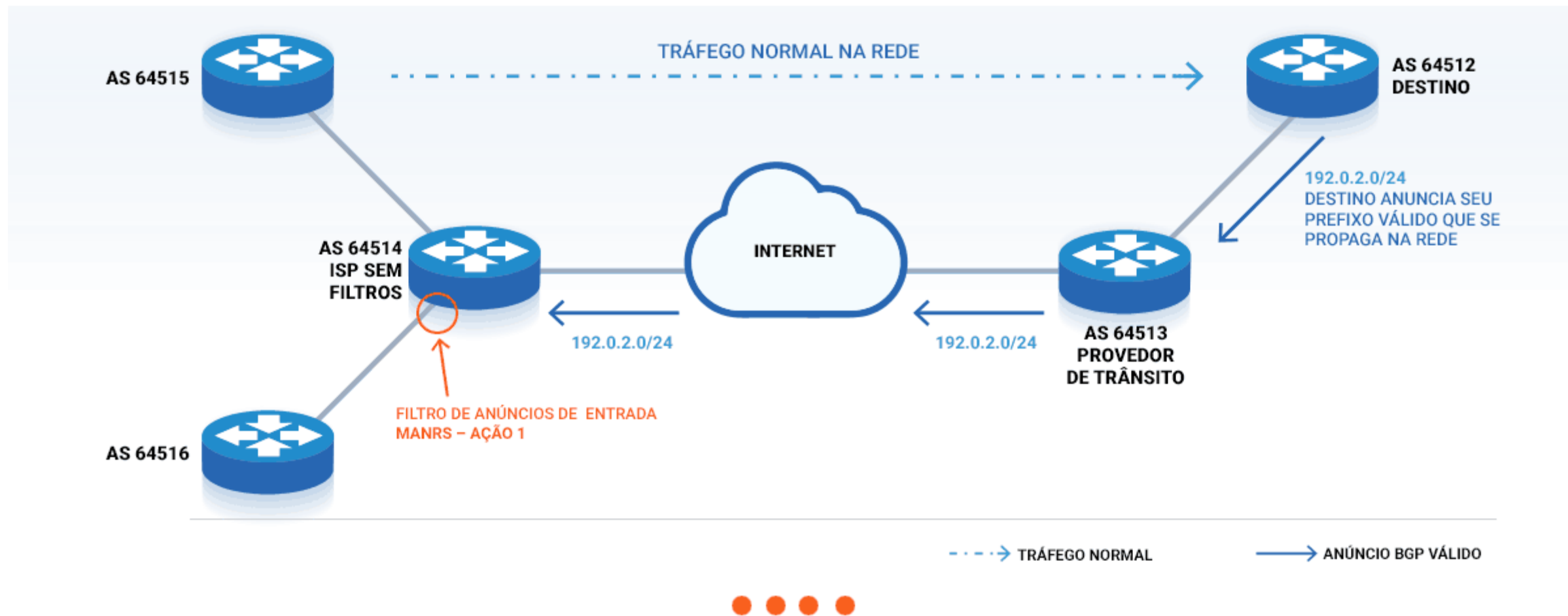
Topologia de rede sem filtros de anúncios



Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

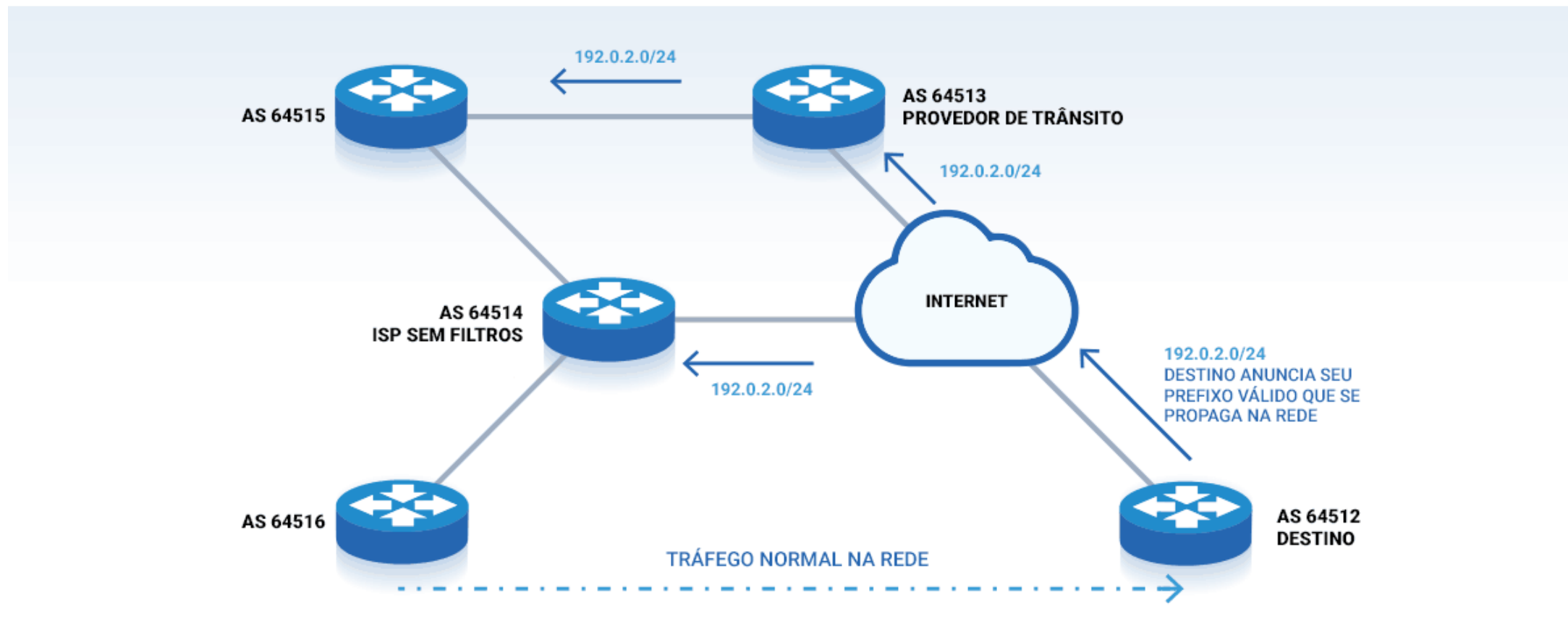
Solução: Filtro de anúncios de entrada (clientes) – MANRS - Ação 1



Segurança e estabilidade da Internet

Ataque por Vazamento de Rotas (Leak)

Topologia sem filtros de anúncios



---> TRÁFEGO NORMAL

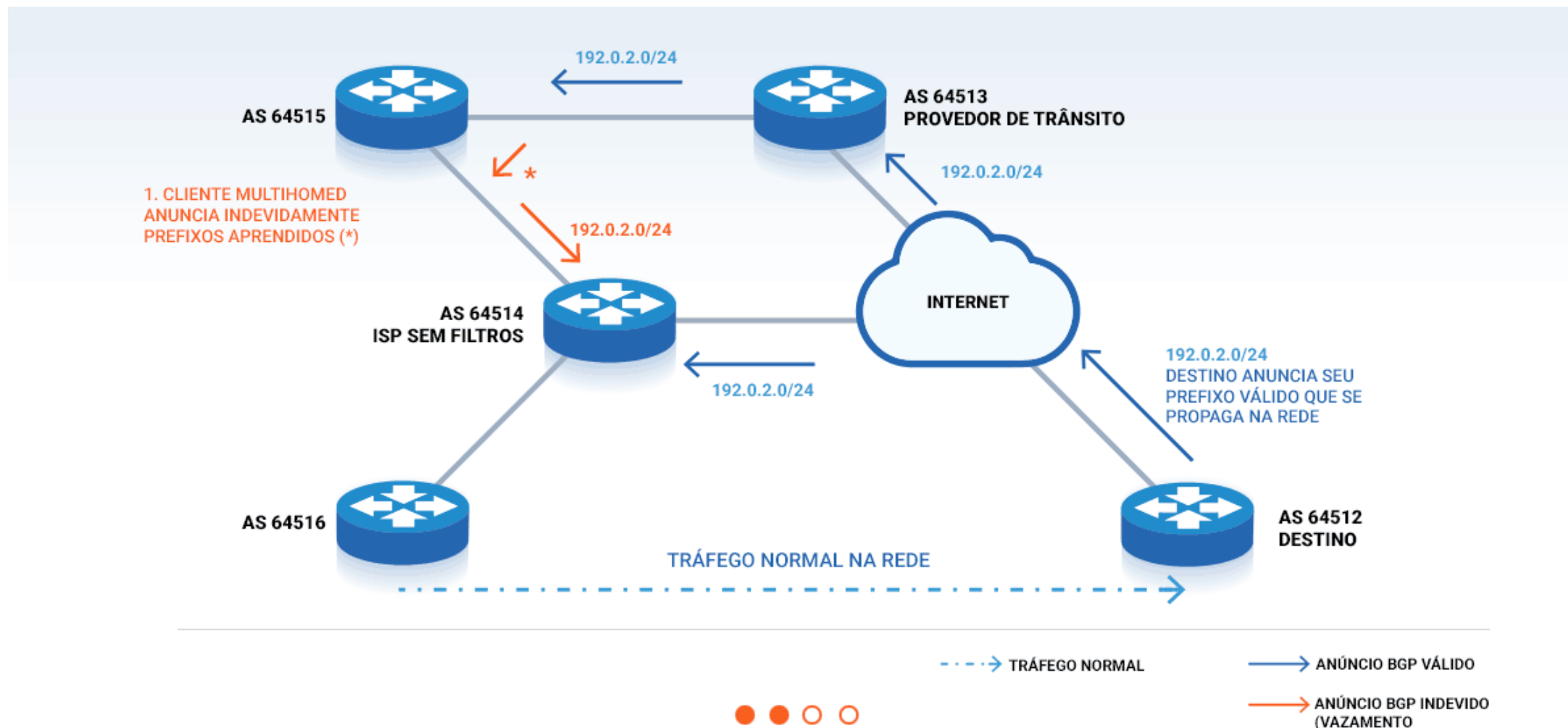
—> ANÚNCIO BGP VÁLIDO



Segurança e estabilidade da Internet

Ataque por Vazamento de Rotas (Leak)

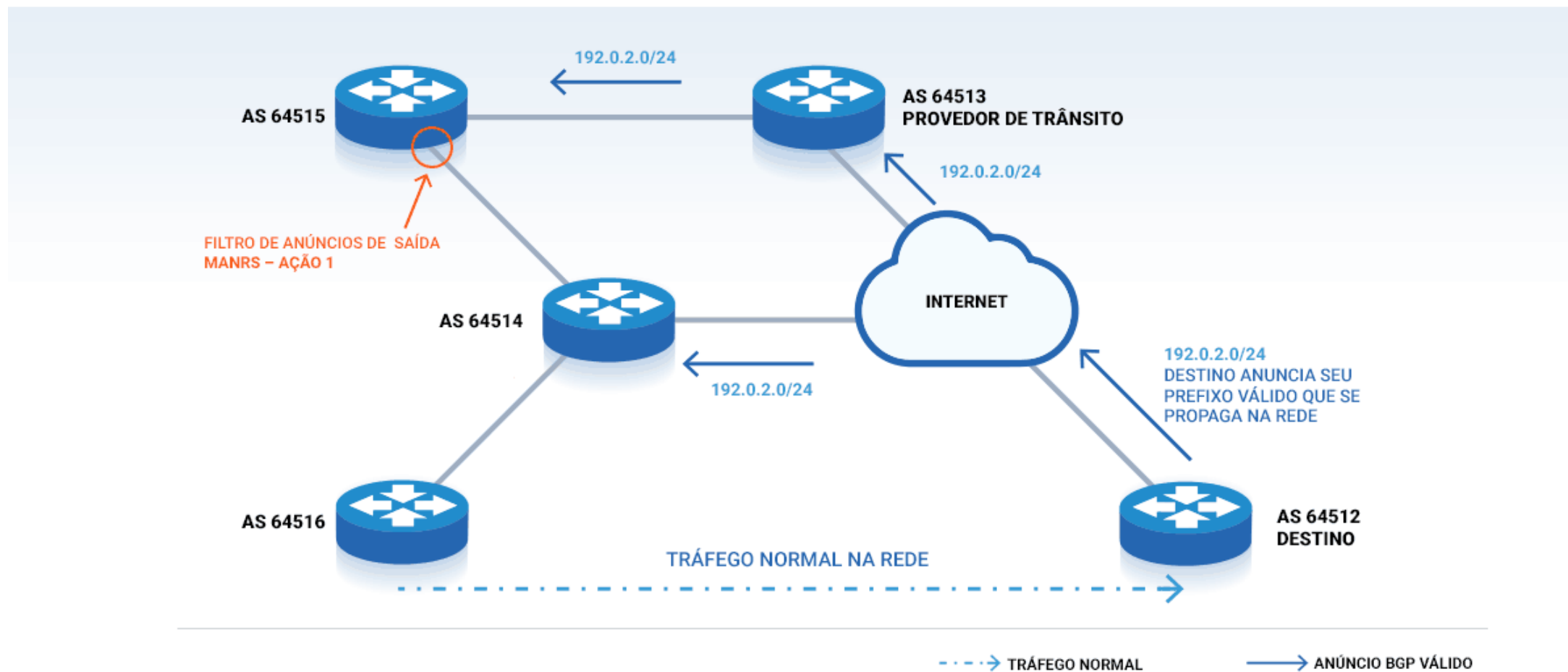
Topologia sem filtros de anúncios



Segurança e estabilidade da Internet

Ataque por Vazamento de Rotas (Leak)

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



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
- Interação com grandes operadoras: redução de endereços IP mal configurados que permitem amplificação
 - Em mar/18: **581k** grandes operadoras // **144k** ISP e AS corporativos
 - Hoje: **154k** grandes operadoras // **209k** ISP e AS corporativos.
- Ações com as maiores Associações de Provedores de Internet
- Ações com a indústria



PROGRAMA
**INTERNET
+SEGURA**

<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.



Como resolver os problemas

Proposta de Ações

Programa por uma Internet mais Segura

Ações necessárias da comunidade técnica



PROGRAMA
**INTERNET
+SEGURA**

- **Configurar corretamente serviços que podem ser abusados em ataques de amplificação [5]**
 - **Conforme as notificações do CERT**
 - <https://bcp.nic.br/i+seg/acoes/amplificacao/>
- **Implementar as ações preconizadas pelo MANRS**
 - **Filtragem de rotas e de endereços de origem falsos (antispoofing) e informações para ações colaborativas entre os operadores da rede**
 - <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/>

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

Programa por uma Internet mais Segura

Notificações de IPs amplificadores

- O CERT.br envia mensalmente notificações aos contatos dos Sistemas Autônomos do Brasil
- As notificações possuem uma lista com endereços IP que possuem serviços mal configurados e que podem permitir o abuso para amplificação de tráfego
- São analisados 12 protocolos com maior incidência de ataques de amplificação: DNS, SNMP, NTP, SSDP, Chargen, LDAP, mDNS, MemCached, Netbios, Portmap, qotd, Ubiquiti discovery service
- Fonte inicial dos dados é da Fundação ShadowServer:
<https://www.shadowserver.org>



Programa por uma Internet mais Segura

Endereços IP e ASN notificados pelo CERT.br



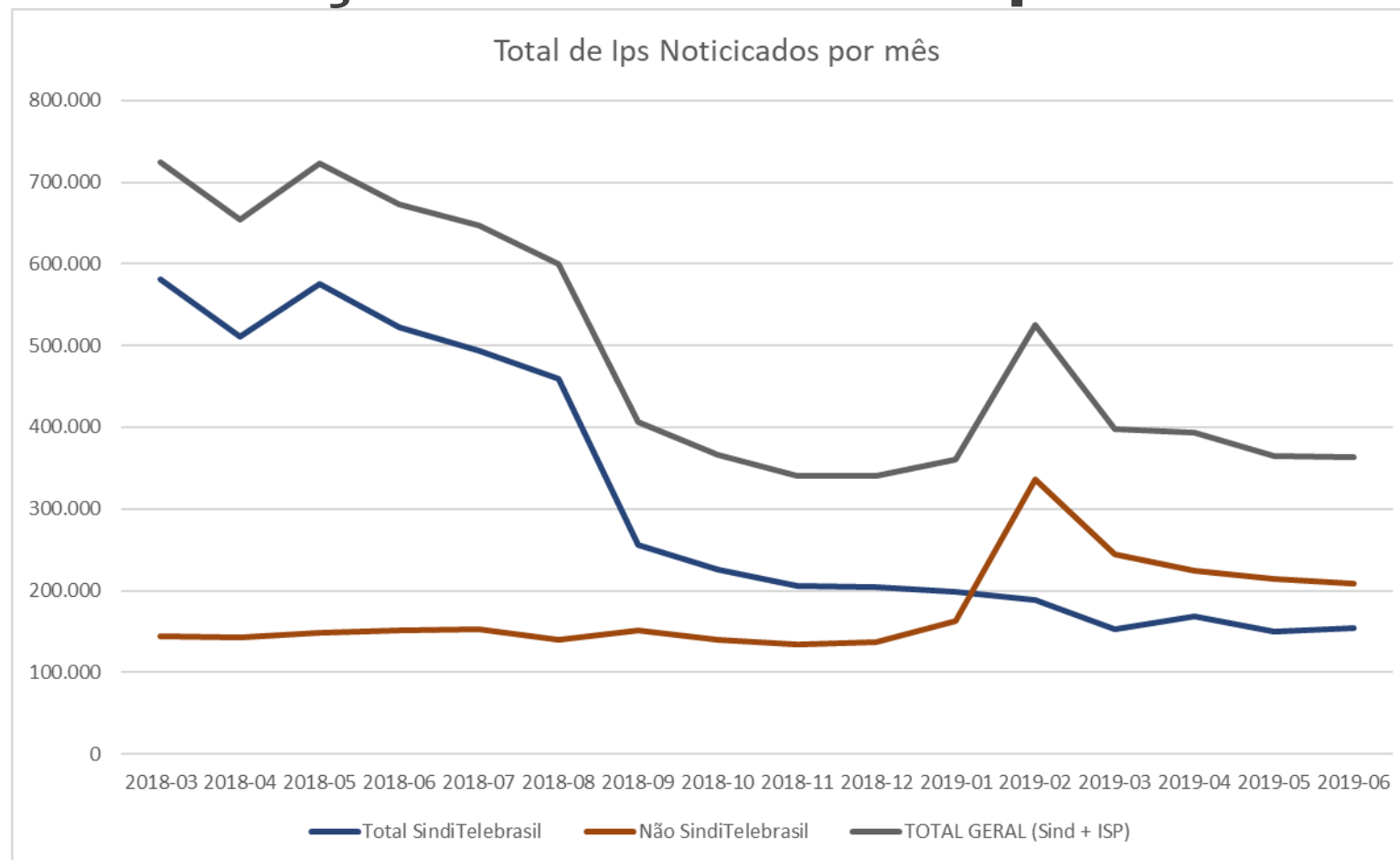
Brasil	DNS		SNMP		NTP		SSDP		UBNT	
	ASNs	IP	ASNs	IP	ASNs	IP	ASNs	IP	ASNs	IP
2018-05	2.343	65.270	2.390	502.861	870	88.788	846	23.174	0	0
2018-06	2.629	70.188	2.284	447.411	805	87.408	817	23.340	0	0
2018-07	2.721	68.415	2.436	431.907	881	89.484	787	17.255	0	0
2018-08	2.459	56.555	2.411	397.622	895	89.353	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

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

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

Programa por uma Internet mais Segura

Total de endereços IP notificados por mês



Hoje são notificados mais endereços IP de ISPs do que operadoras

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



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)**
- **Dezoito empresas brasileiras já participam da iniciativa MANRS**
- **Inscreva-se no programa MANRS, diferencie-se num mercado competitivo...**



MANRS



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/>

Programa por uma Internet mais Segura

Exemplo de problema com sistemas não atualizados



- **Situação:**
- Mensalmente o CERT.br notifica os responsáveis por ASNs cujos endereços IP possivelmente são de dispositivos Mikrotik em sua rede que foram comprometidos e que estão sendo abusados para o envio de spam.
- **Esse comprometimento habilita o serviço SOCKS na porta 4145/tcp que pode ser abusado para diversas atividades, principalmente para o envio de spam.**
- Essas atividades estão consumindo recursos da rede dos ASNs e provavelmente incluindo seus endereços IP em listas de bloqueio.
- **Mais de 3.000 endereços IP estão sendo notificados mensalmente.**

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 por 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

Requisitos especificados pelo documento:

- Gerais (GR)
- Segurança de software (SSR)
- Atualização e gerenciamento (MR)
- Funcionais (FR)
- Configurações iniciais (IR)
- Fabricante e distribuição (VR)

The logo for nic.br, featuring the text "nic.br" in a bold, sans-serif font. The "nic" is in black and the ".br" is in a light green color.The logo for lacnog, featuring the text "lacnog" in a bold, sans-serif font. To the right of the text is a stylized graphic consisting of several overlapping, curved shapes in red, blue, and yellow, resembling a globe or a network diagram.The logo for M3AAWG, featuring the text "M3AAWG" in a bold, sans-serif font. The "M3" is in a blue box, and "AAWG" is in blue. Below the main text, it reads "MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP" in a smaller, blue, sans-serif font.

Minimum security requirements for CPEs acquisition

Em geral, as vulnerabilidades 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

The logo for nic.br, featuring the text "nic.br" in a bold, sans-serif font. The "nic" is in black and the ".br" is in a bright green color.The logo for lacnog, featuring the text "lacnog" in a bold, sans-serif font. To the right of the text is a stylized graphic consisting of several overlapping, curved shapes in red, blue, and yellow, resembling a globe or a network diagram.The logo for M3 AAWG, featuring the text "M3 AAWG" in a bold, sans-serif font. The "M3" is in blue with a red outline, and "AAWG" is in blue. Below the main text, the words "MESSAGING MALWARE MOBILE" and "ANTI-ABUSE WORKING GROUP" are written in smaller, blue and red text respectively.

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

25 de junho de 2019

nic.br egi.br

www.nic.br | www.cgi.br