MELHORANDO A SEGURANÇA DE SEU PROVEDOR E DE TODA A INTERNET

Rodrigo Regis | rsantos@nic.br

registro.br nic.br cgi.br

Segurança e estabilidade da Internet
Querem saber?

Como...

RESOLVER DEFINITIVAMENTE

OS PRINCIPAIS PROBLEMAS DE SEGURANÇA

da INTERNET (e do seu provedor)**???**

Incluindo ataques DDOS, SPAM

e ‘roubo de prefixos’!

Segurança e estabilidade da Internet
Querem saber?

Isso tudo gastando praticamente

NADA, ZERO, NOTHING! ~~$$$$~~

Com apenas 4 ações muito simples…

Interessados?

Panorama atual

Segurança e estabilidade da Internet
Estrutura da Internet atual

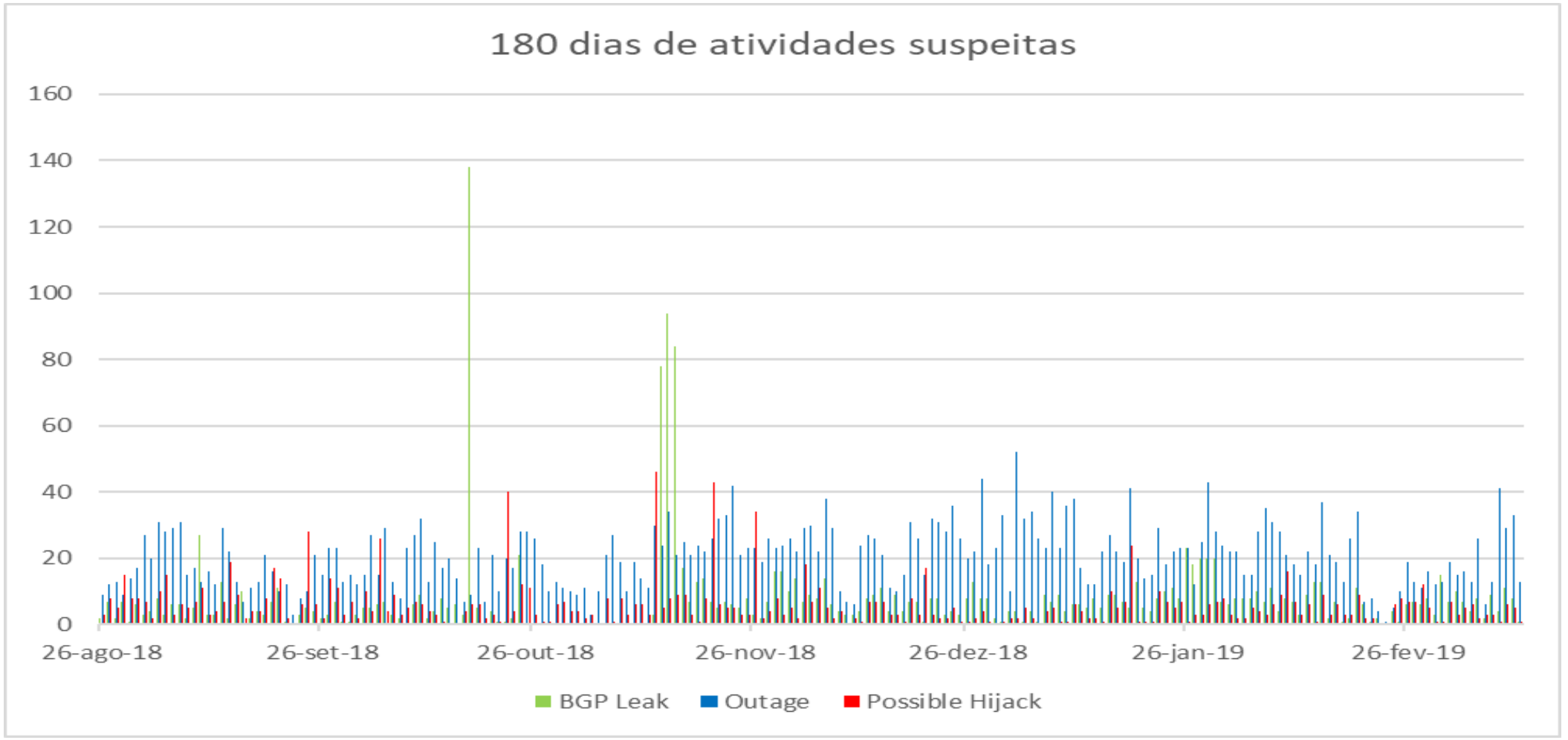
A Internet funciona com base na cooperação entre Sistemas Autônomos:

- 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

Segurança e estabilidade da Internet
Nenhum dia sem um incidente

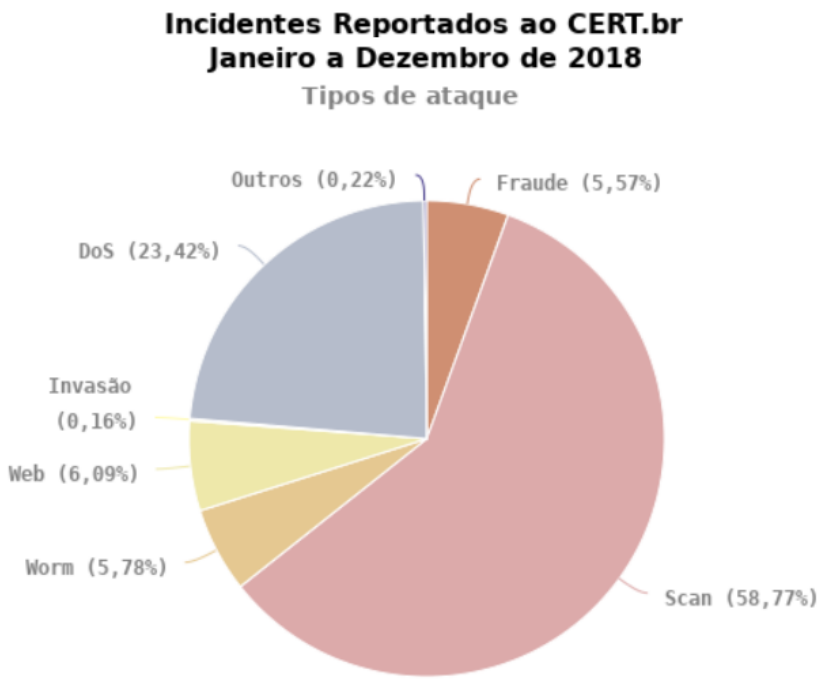


Segurança e estabilidade da Internet
Panorama Atual

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
- **Medições em "honeypots" distribuídos na Internet**
- Medições no IX.



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

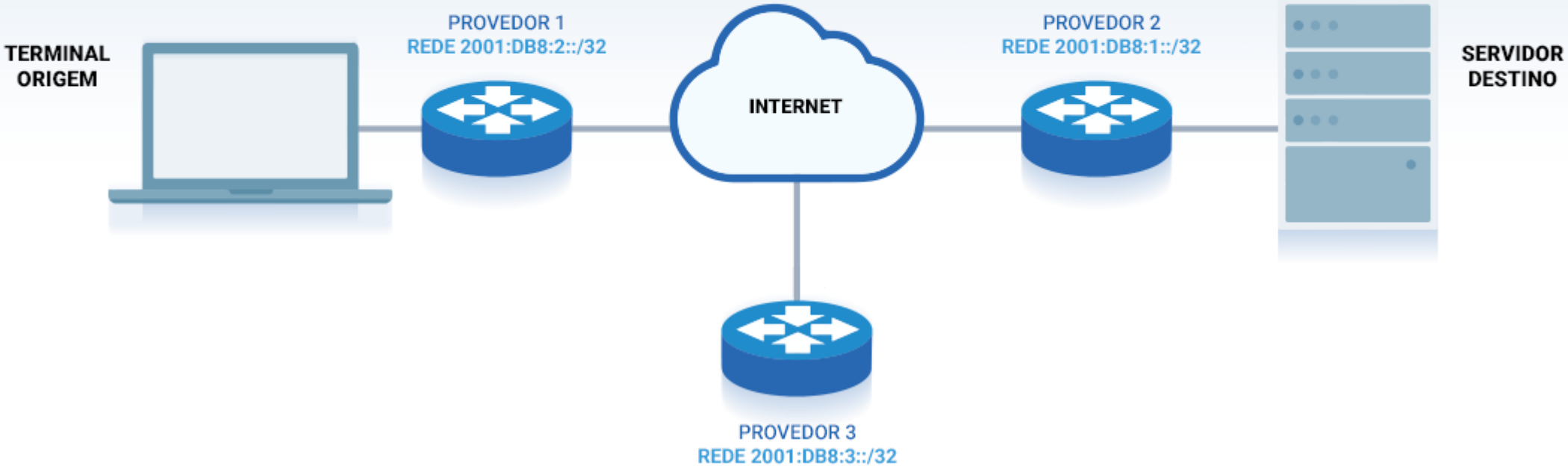
Constata-se um ritmo crescente de notificações de varreduras, fraudes e DoS [4]

Ataques mais frequentes

Segurança e estabilidade da Internet

Ataque DoS por reflexão

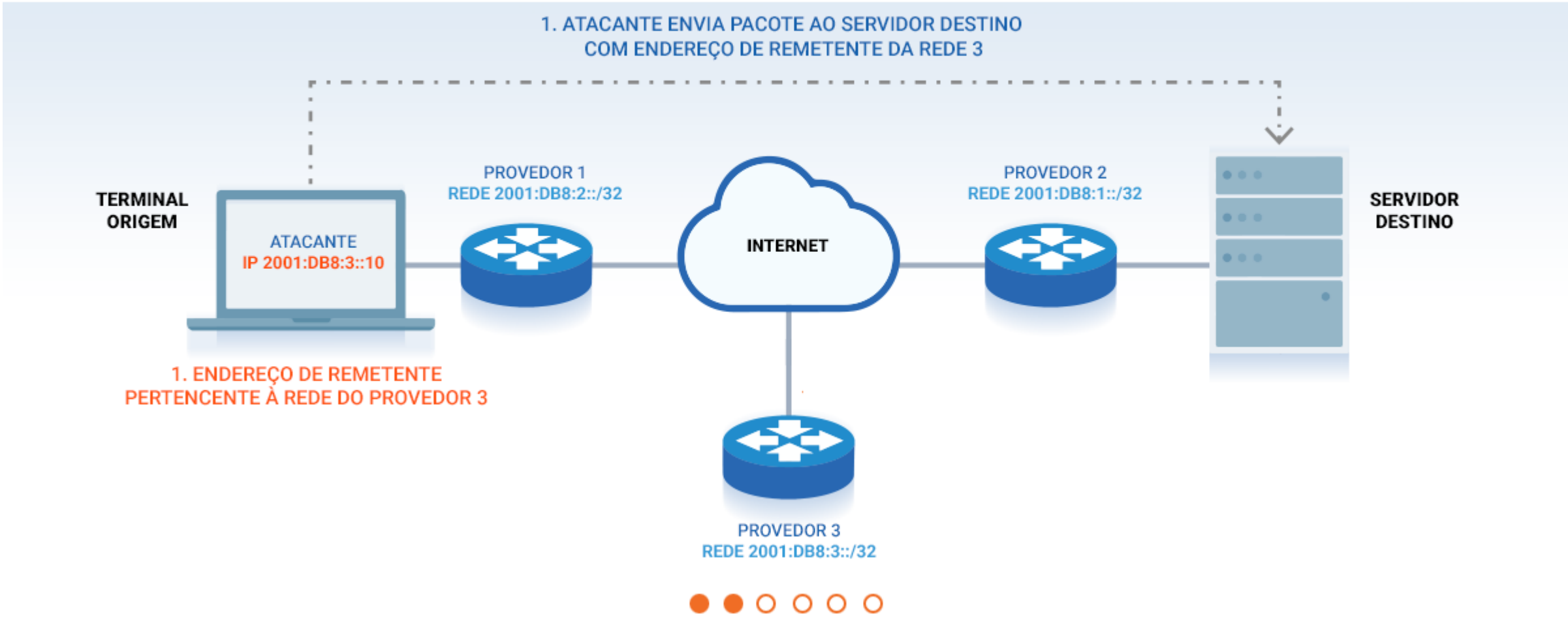
Topologia de rede sem filtros antispoofing



Segurança e estabilidade da Internet

Ataque DoS por reflexão

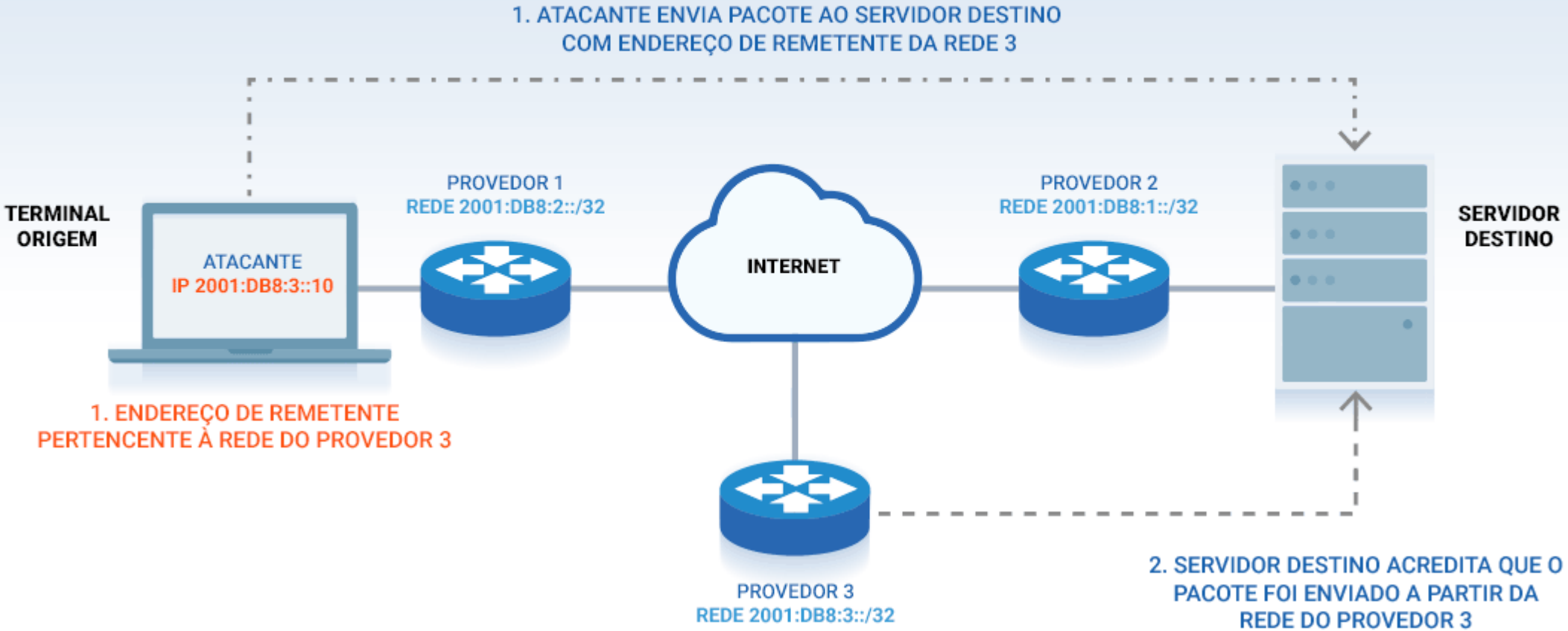
Ataque DoS utilizando endereço de remetente forjado (Spoofing)



Segurança e estabilidade da Internet

Ataque DoS por reflexão

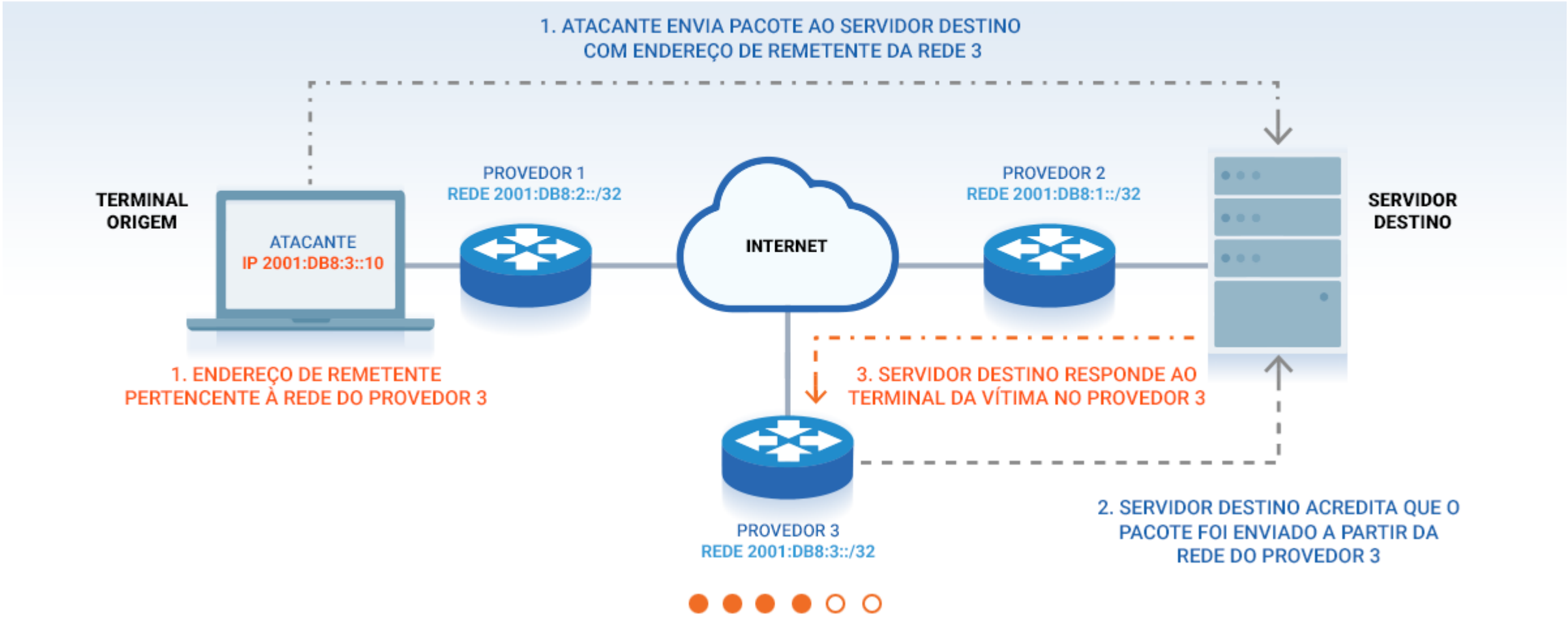
Ataque DoS utilizando endereço de remetente forjado (Spoofing)



Segurança e estabilidade da Internet

Ataque DoS por reflexão

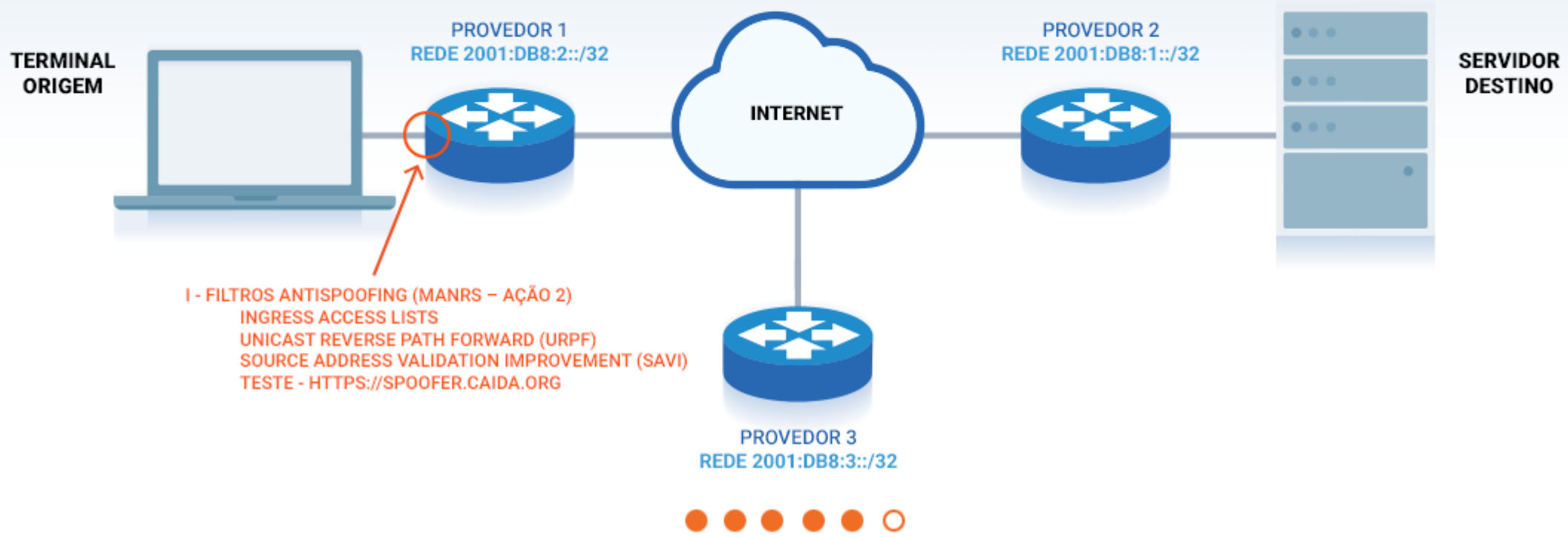
Ataque DoS utilizando endereço de remetente forjado (Spoofing)



Segurança e estabilidade da Internet

Ataque DoS por reflexão

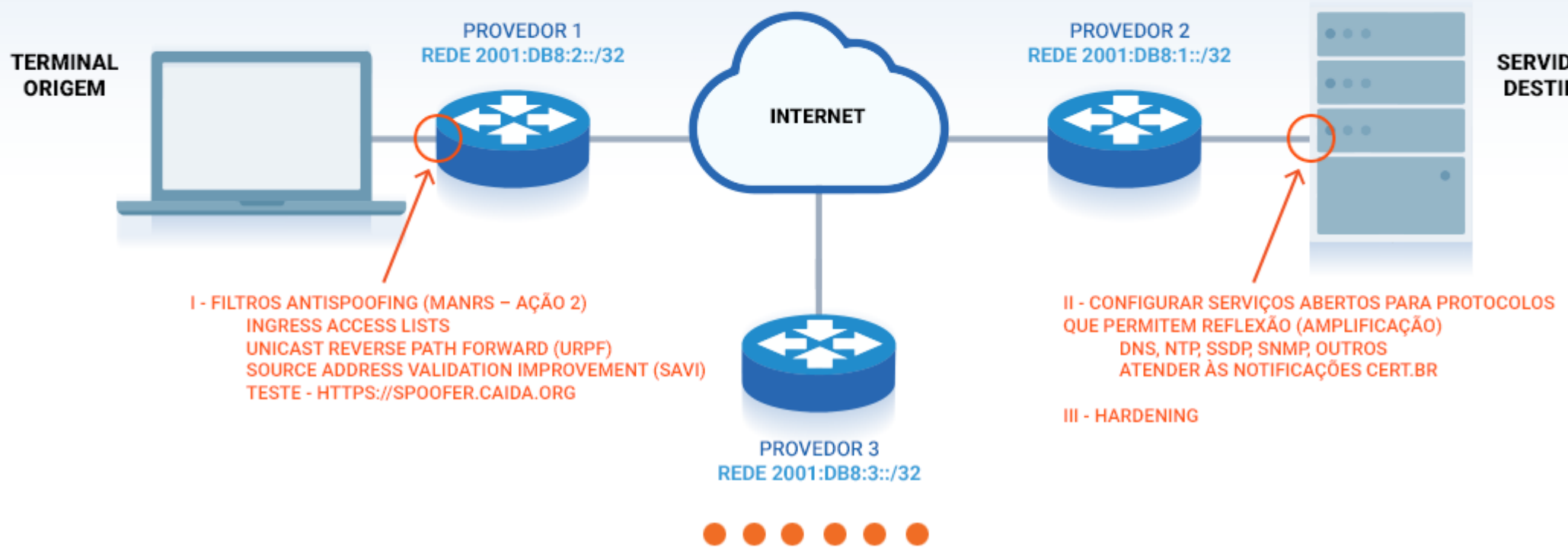
Solução: Aplicação de filtros antispoofing



Segurança e estabilidade da Internet

Ataque DoS por reflexão

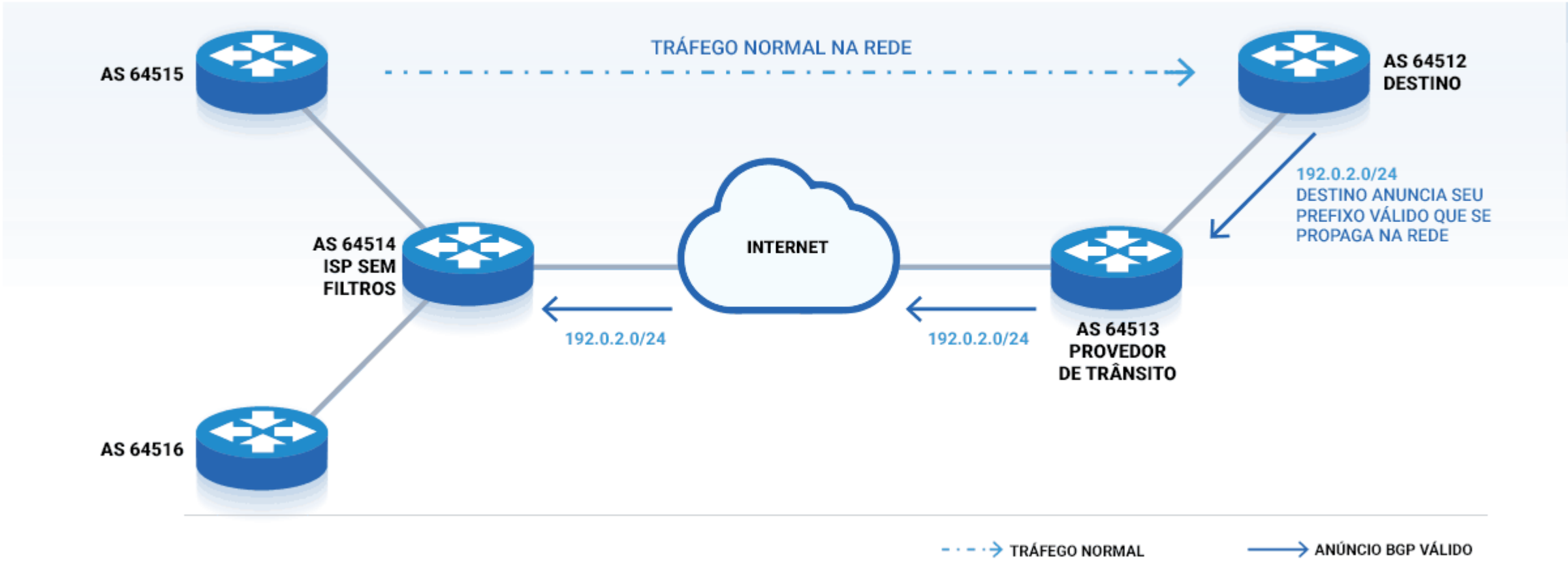
Solução: Aplicação de filtros antispoofing, configuração de serviços e Hardening



Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

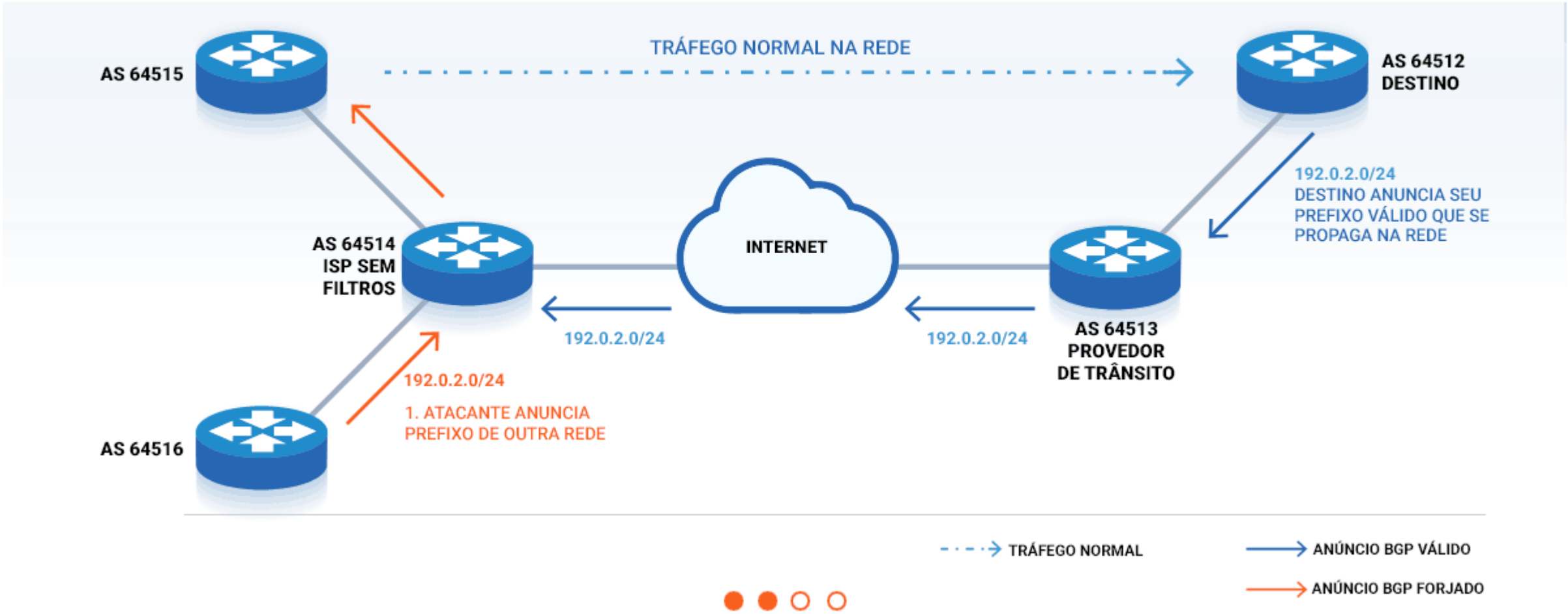
Topologia de rede sem filtros de anúncios



Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

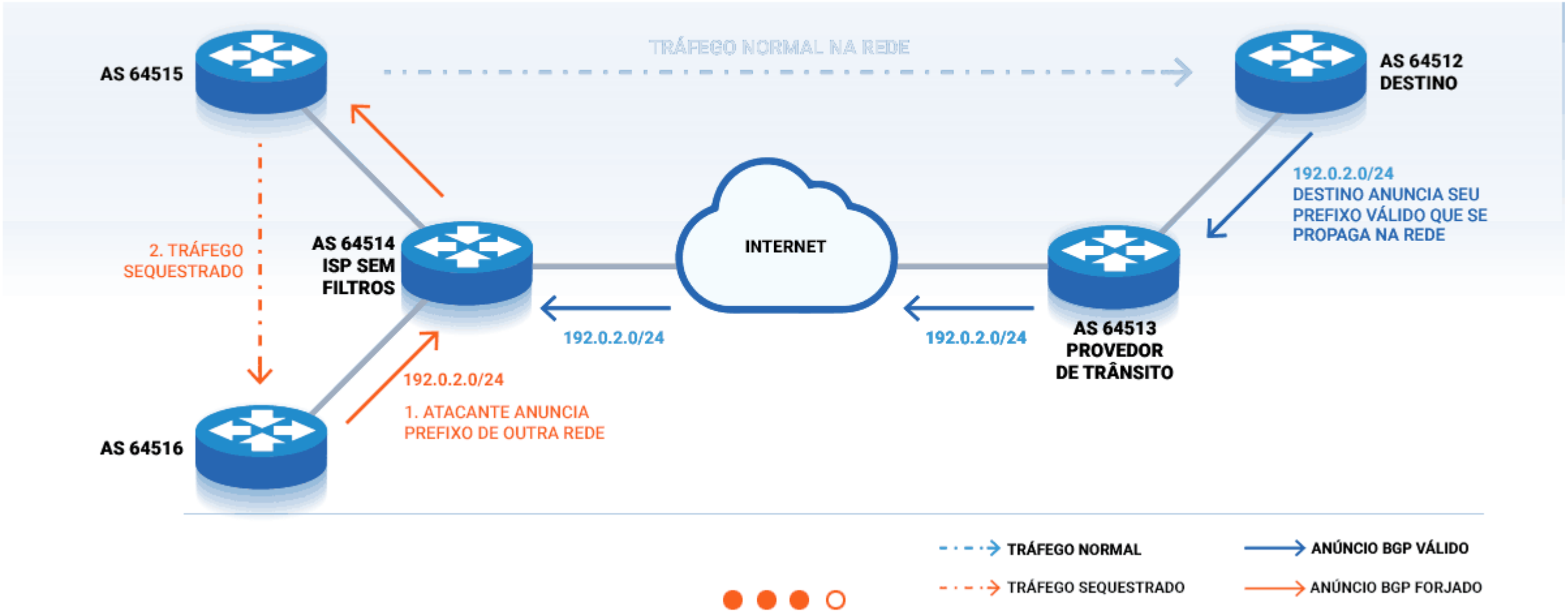
Ataque utilizando sequestro de prefixos



Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

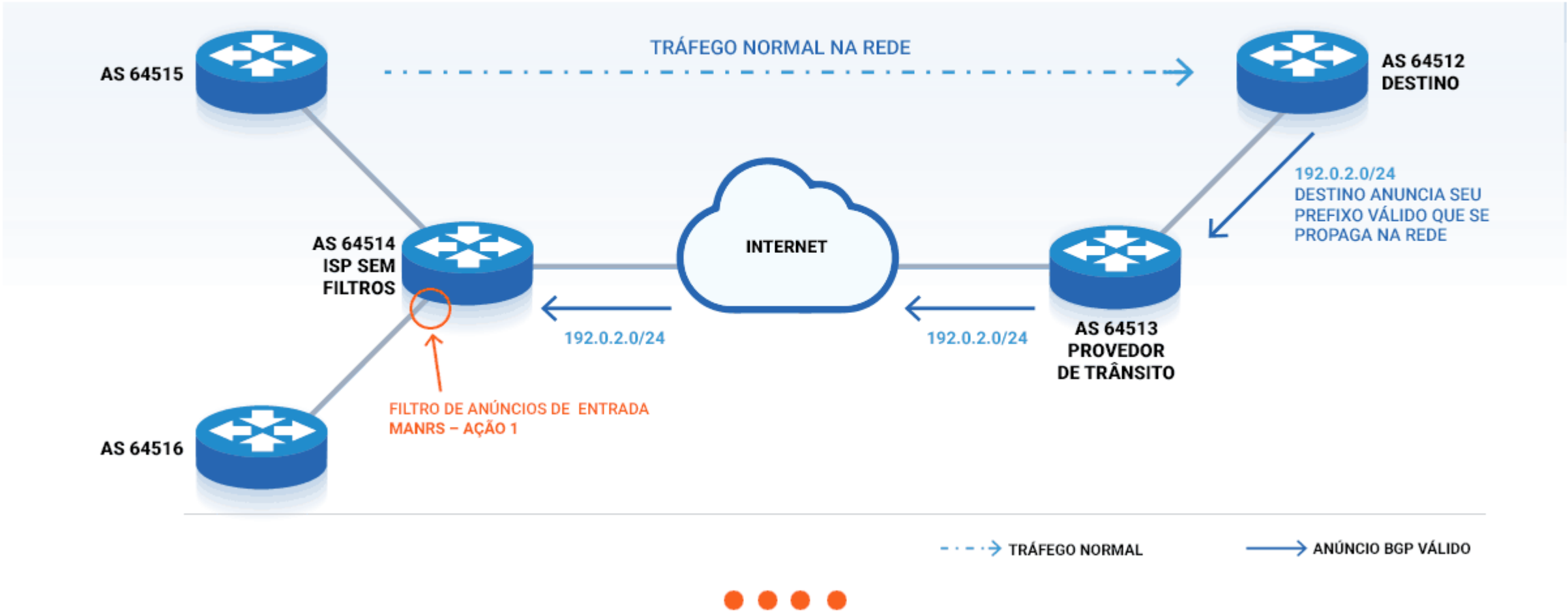
Topologia de rede sem filtros de anúncios



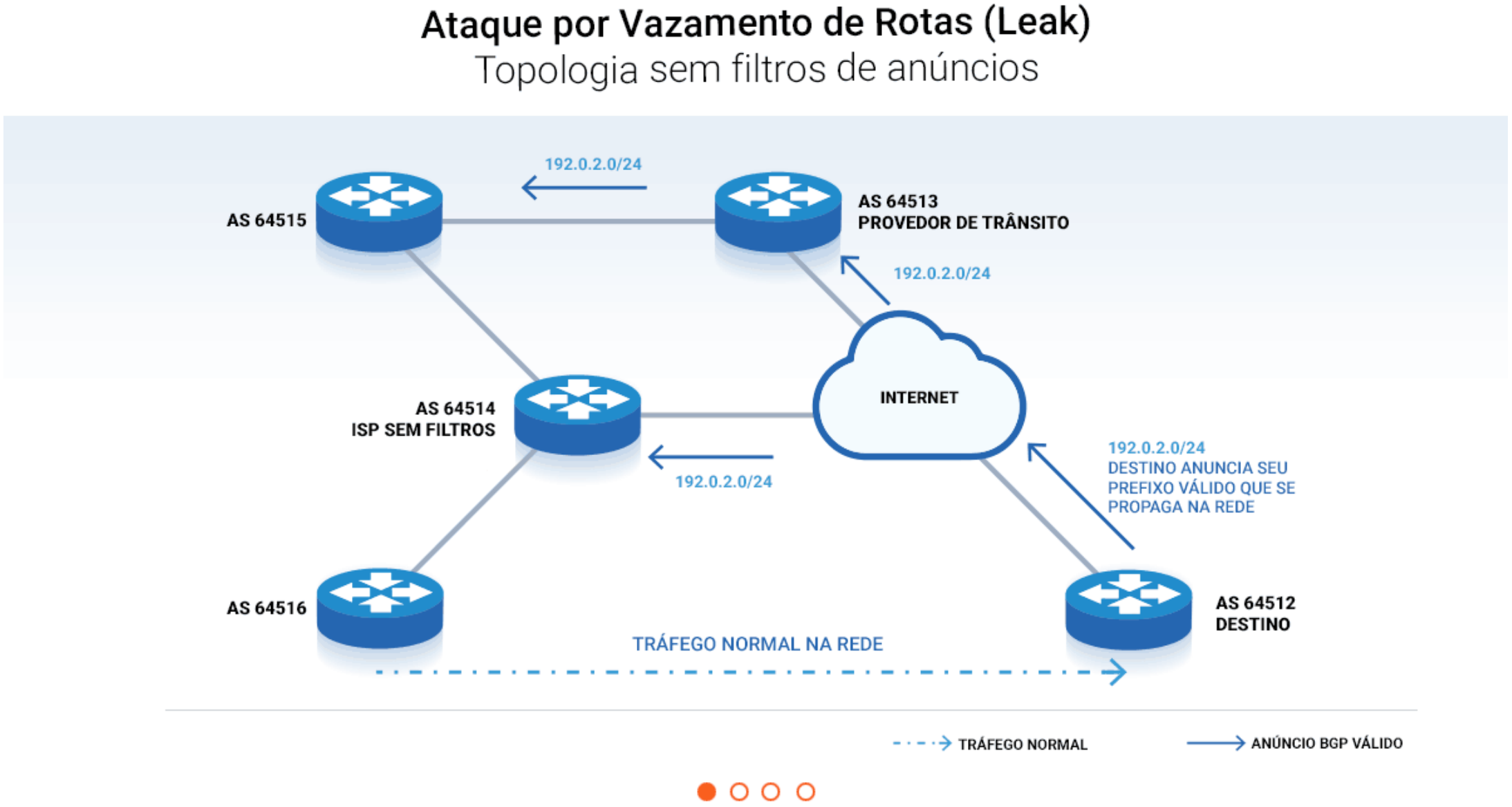
Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

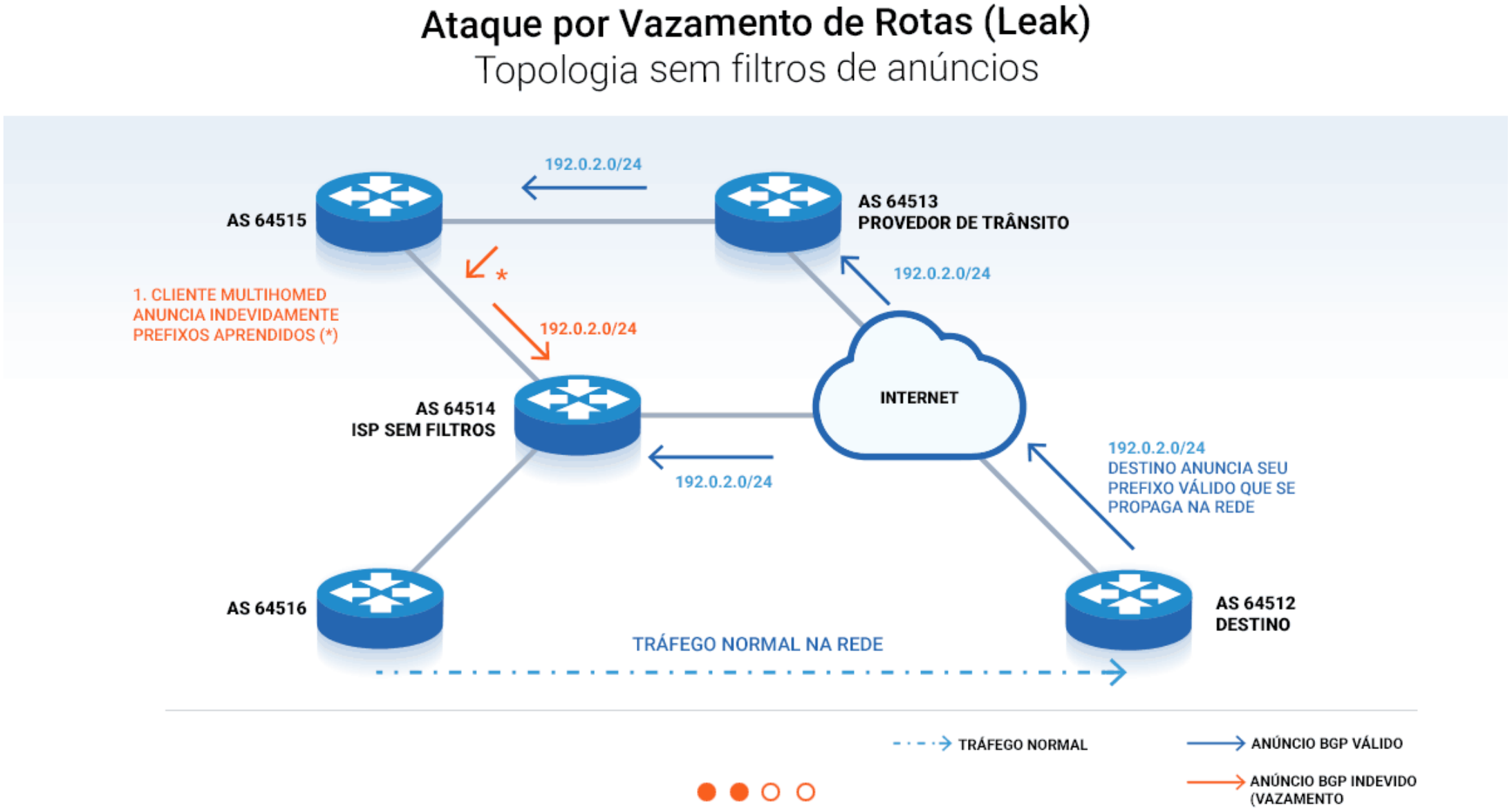
Solução: Filtro de anúncios de entrada (clientes) – MANRS - Ação 1



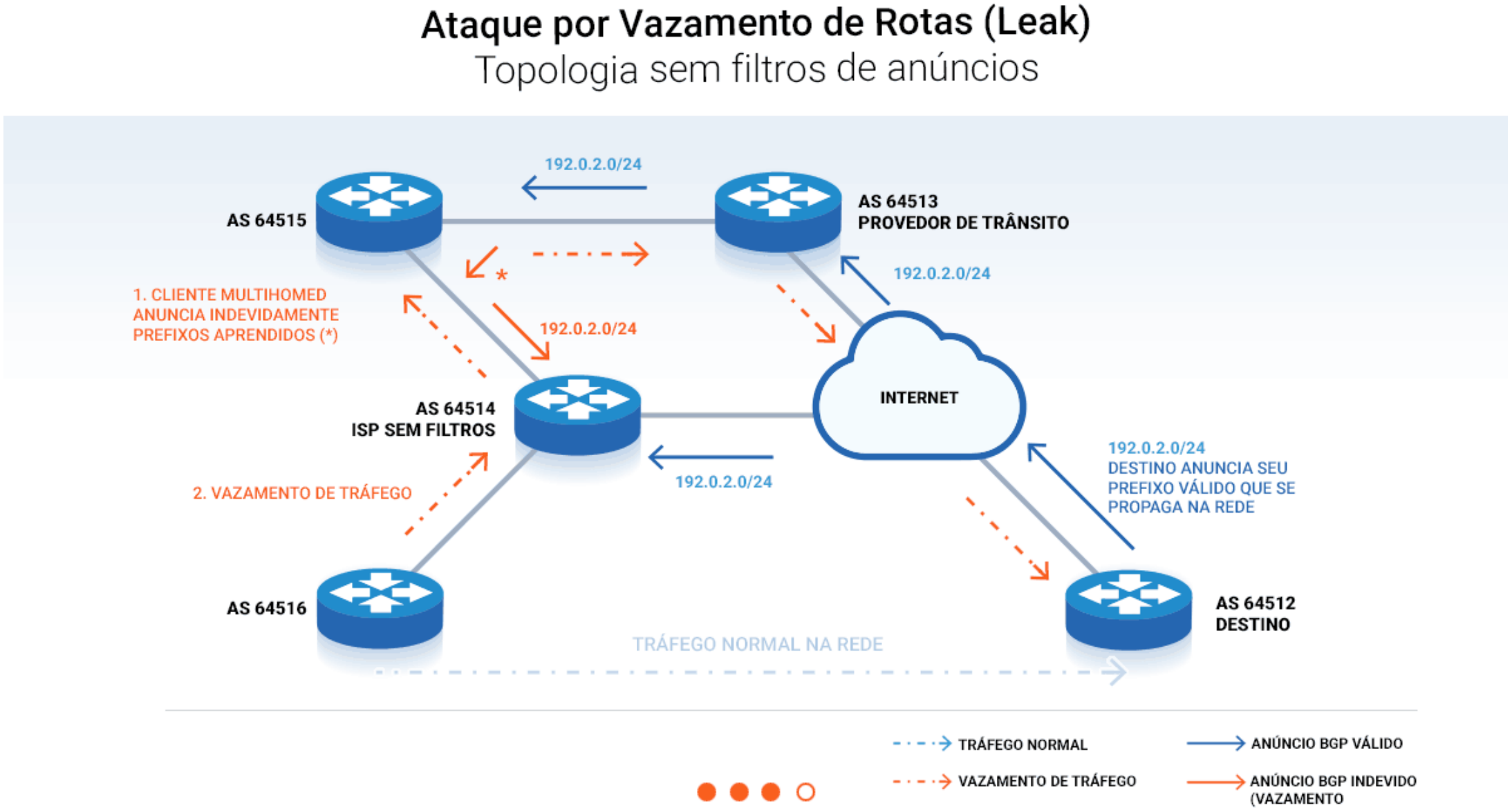
Segurança e estabilidade da Internet



Segurança e estabilidade da Internet



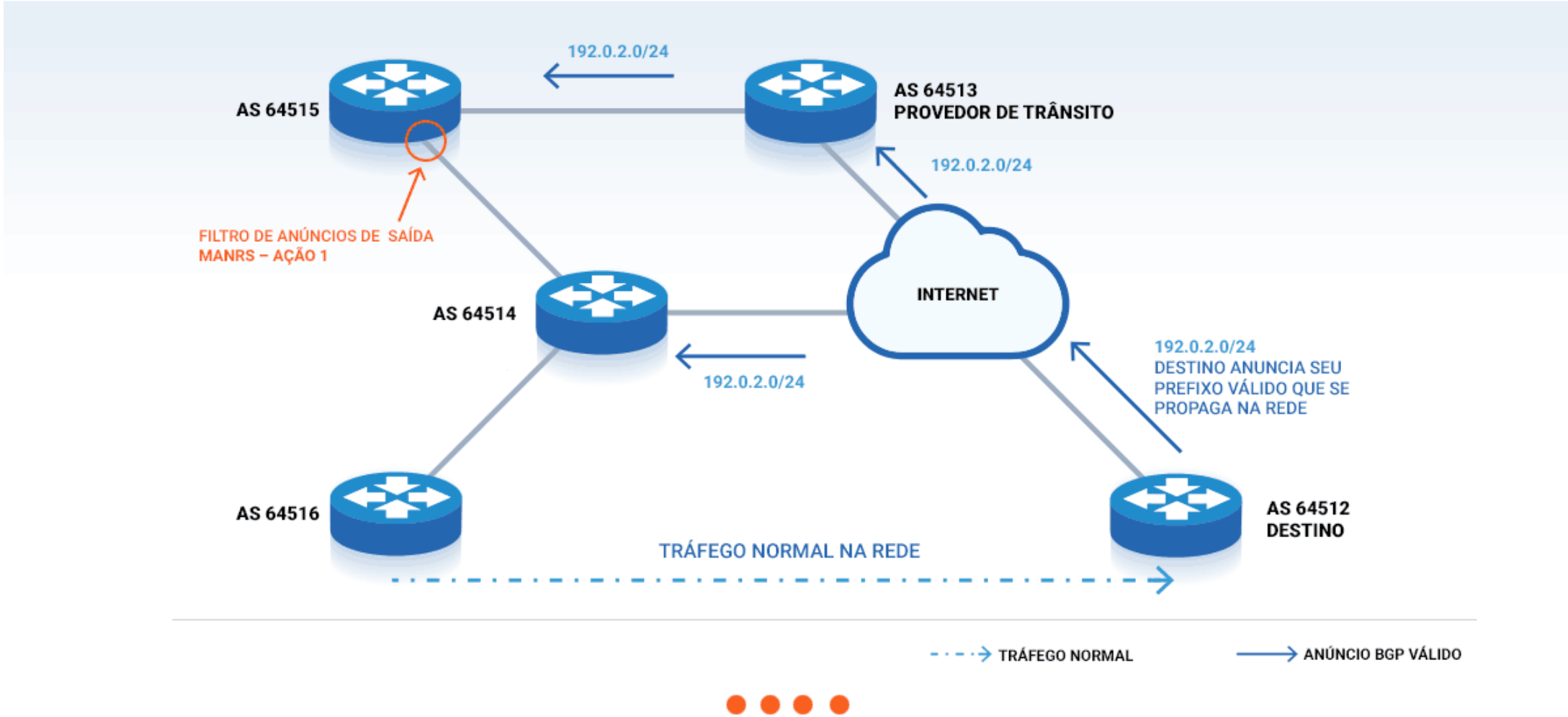
Segurança e estabilidade da Internet



Segurança e estabilidade da Internet

Ataque por Vazamento de Rotas (Leak)

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



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)

Apoiado pela Internet Society

Programa por uma Internet mais Segura

Problemas de segurança

MANRS

- 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!**

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)**

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

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:

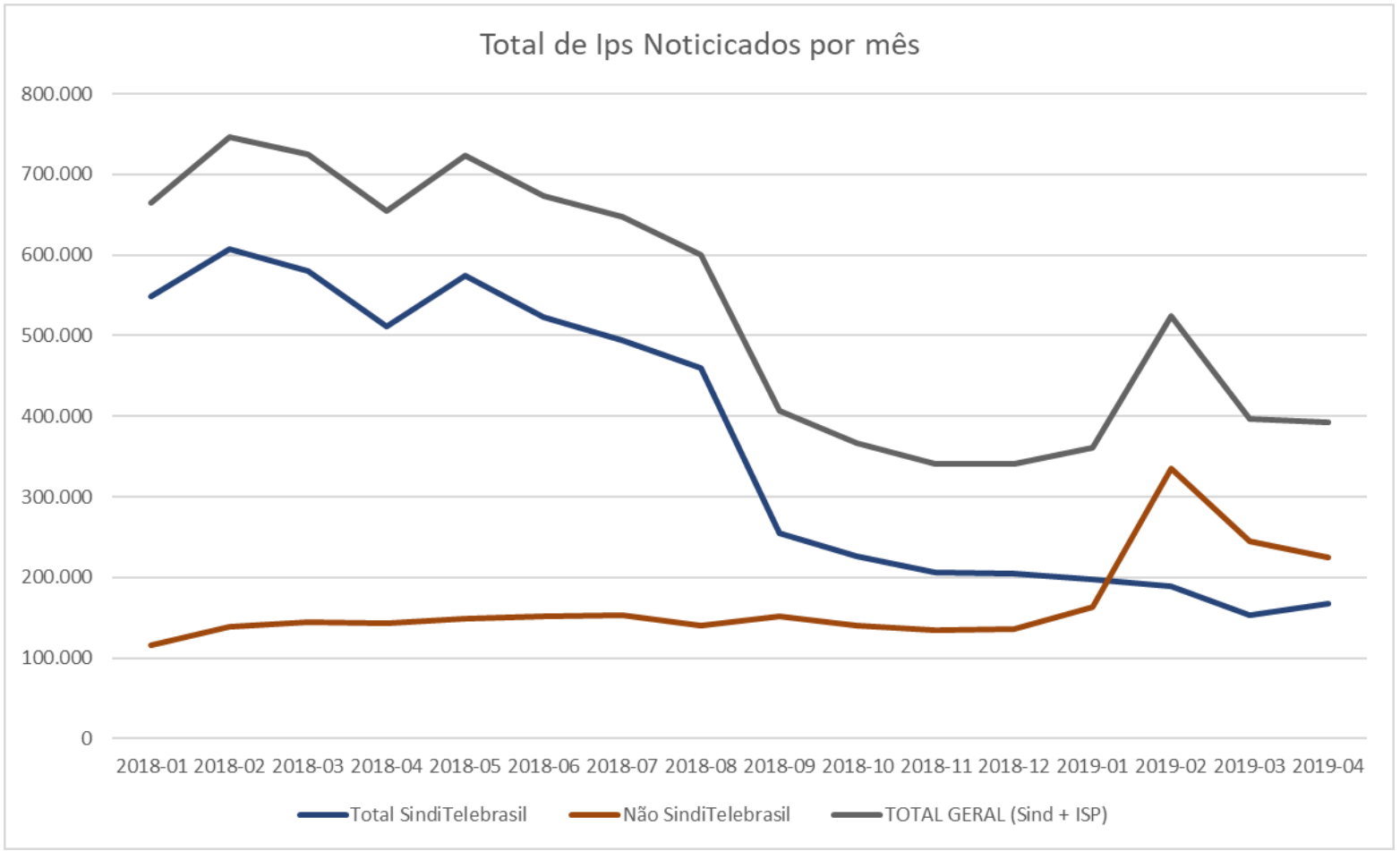
- Conscientização por meio de palestras, cursos e treinamentos
- **Criação de materiais didáticos e boas práticas**
- Interação com **Associações de Provedores** e seus afiliados para disseminação da **Cultura de Segurança**, adoção de **Melhores Práticas** e **mitigação** de problemas existentes
- **Implementação 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
  - Em mar/18: 581k grandes operadoras // 144k ISP e AS corporativos
  - Hoje: 168k grandes operadoras // 224k ISP e AS corporativos.
- Ações com as maiores Associações de Provedores de Internet
- Ações com a indústria

Programa por uma Internet mais Segura

Total de endereços IP notificados por mês



Hoje são notificados mais endereços IP de ISPs do que operadoras

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

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

rsantos@nic.br

10 de junho de 2019

nic.br cgi.br

www.nic.br | www.cgi.br