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

APRONET

Florianópolis, SC | 23/02/19

AUMENTANDO A SEGURANÇA DOS PROVEDORES E DA INFRAESTRUTURA DA INTERNET

Gilberto Zorello

gzorello@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?

Nossa
Agenda

- CGI.br e NIC.br
- **Panorama atual**
- Ataques mais frequentes
- **Como resolver os problemas**
- MANRS
- **Desenvolvimento do Programa por uma Internet mais Segura**

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 **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**

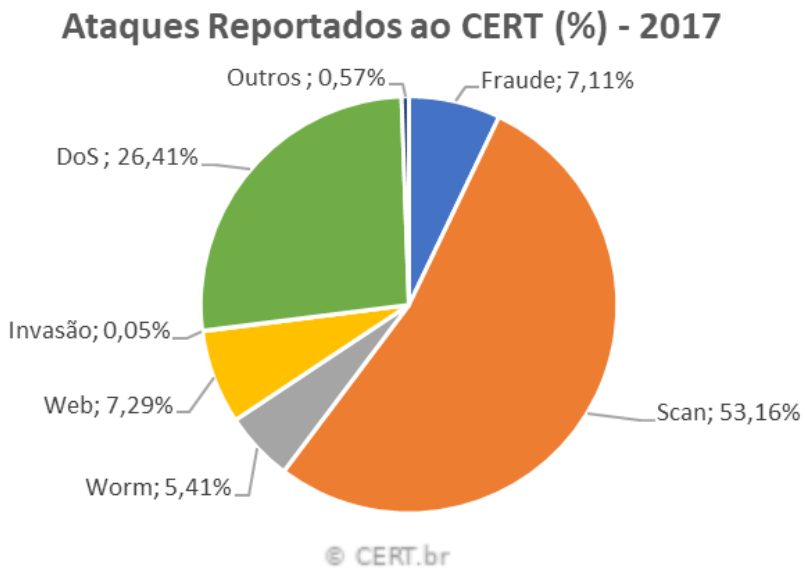
O BGP não tem
Validação para os dados

Segurança e estabilidade da Internet
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:

- Tratamento de incidentes de segurança
- **Medições em "honeypots" distribuídos na Internet**
- Medições no IX.

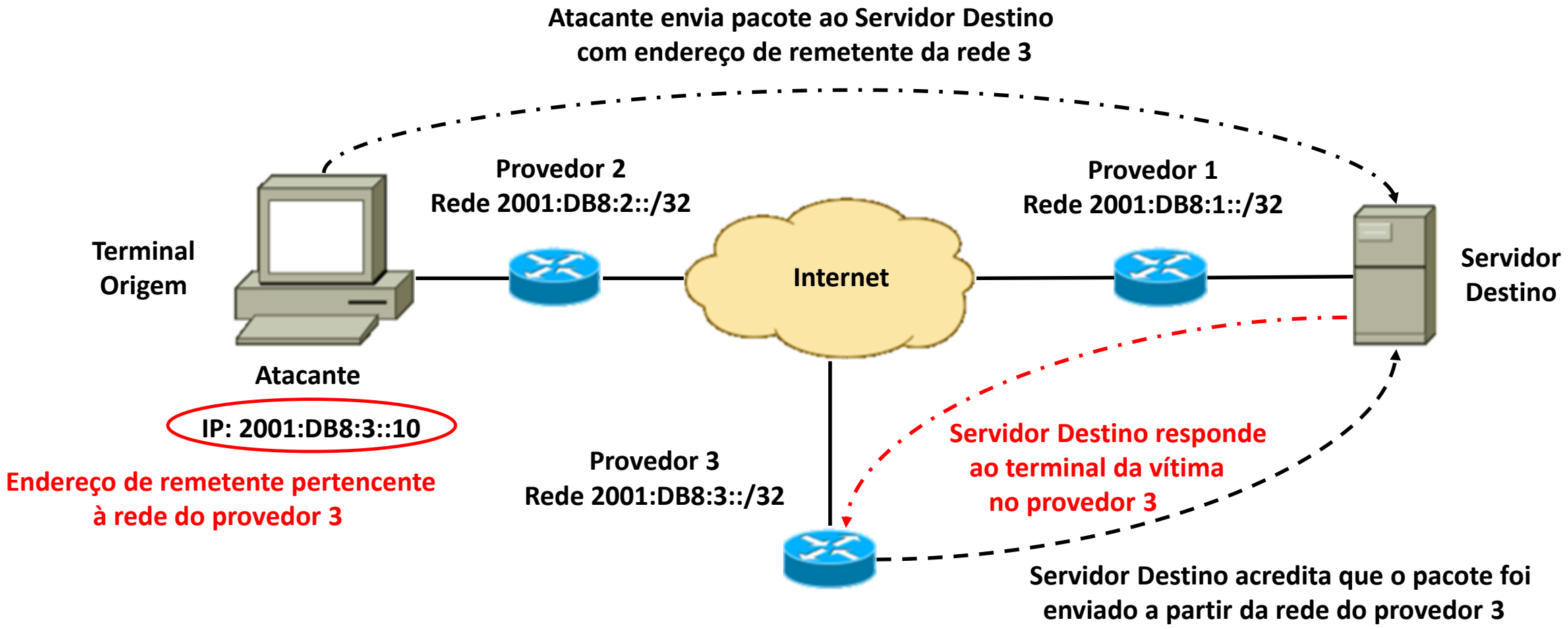


Constata-se um ritmo crescente de notificações de varreduras, fraudes e DDoS [4]

Ataques mais frequentes

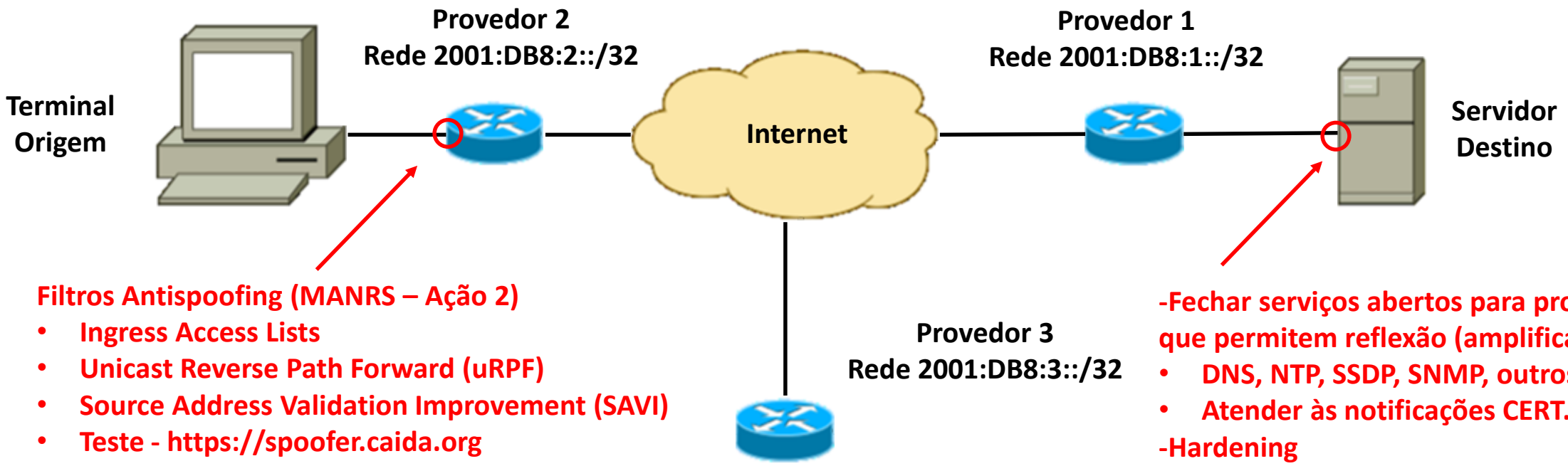
Segurança e estabilidade da Internet
Ataque DoS por reflexão

Ataque DoS utilizando endereço de remetente forjado (Spoofing)



Segurança e estabilidade da Internet
Ataque DoS por reflexão

Solução: Filtros Antispoofing e Fechar portas para serviços abusáveis



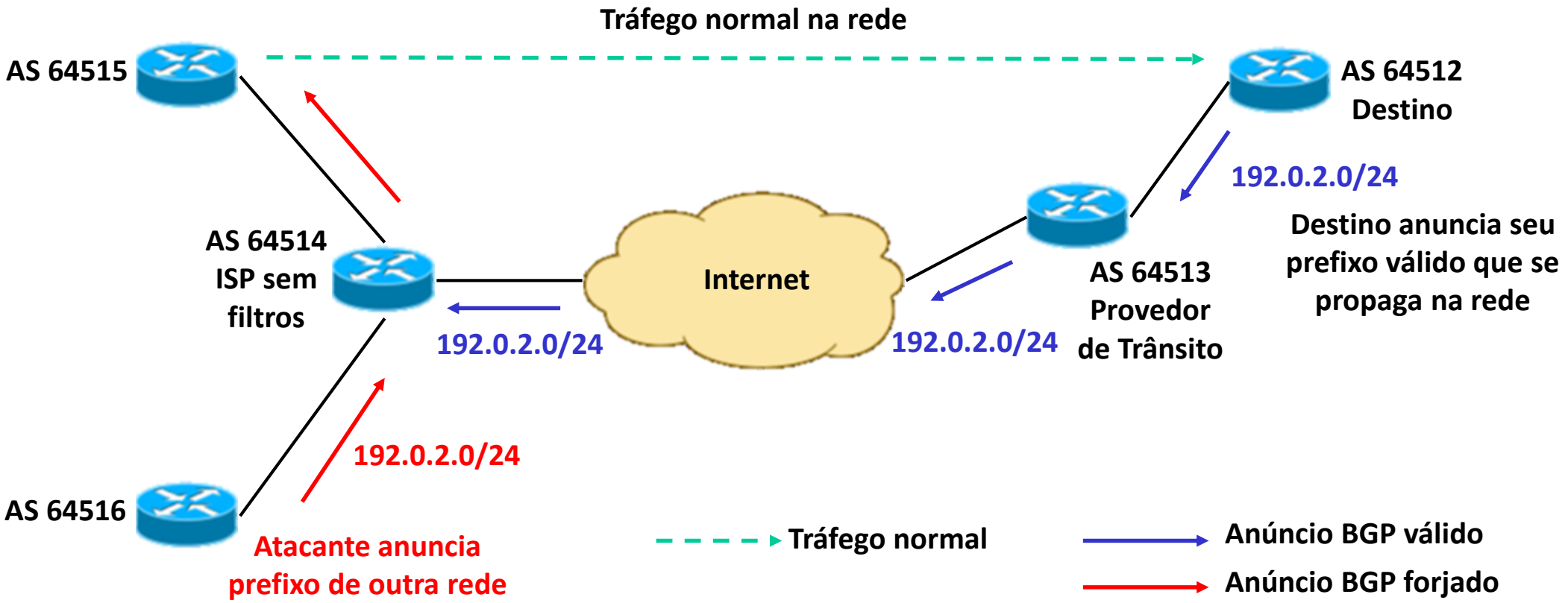
Filtros Antispoofing (MANRS – Ação 2)
- **Ingress Access Lists**
- **Unicast Reverse Path Forward (uRPF)**
- **Source Address Validation Improvement (SAVI)**
- **Teste - https://spoofer.caida.org**

-Fechar serviços abertos para protocolos que permitem reflexão (amplificação)
- **DNS, NTP, SSDP, SNMP, outros**
- **Atender às notificações CERT.br**

-Hardening

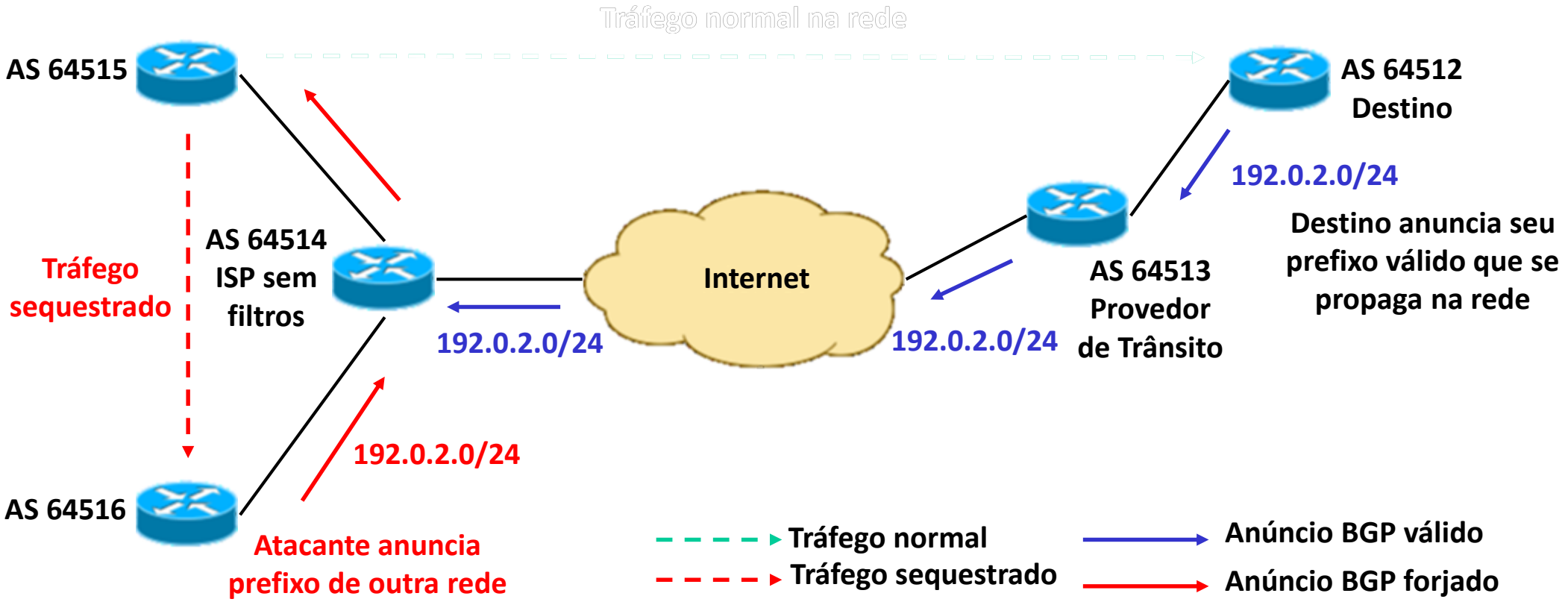
Segurança e estabilidade da Internet
Ataque por Sequestro de Prefixos (Hijacking)

Ataque utilizando sequestro de prefixos



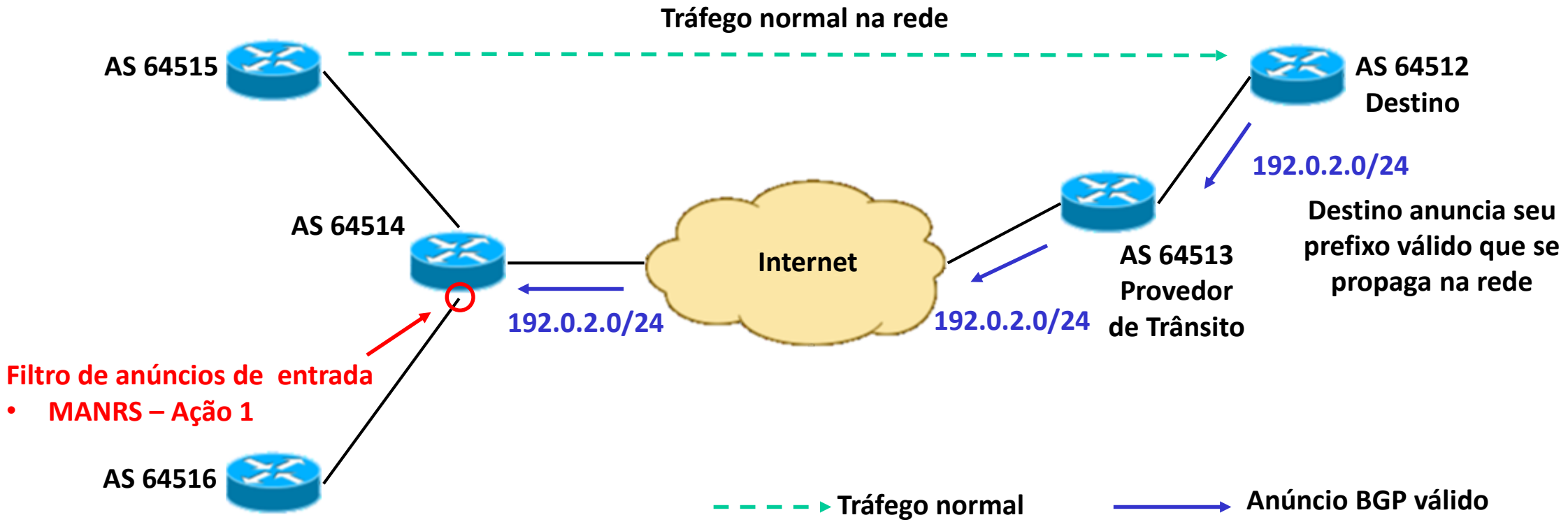
Segurança e estabilidade da Internet
Ataque por Sequestro de Prefixos (Hijacking)

Ataque utilizando sequestro de prefixos



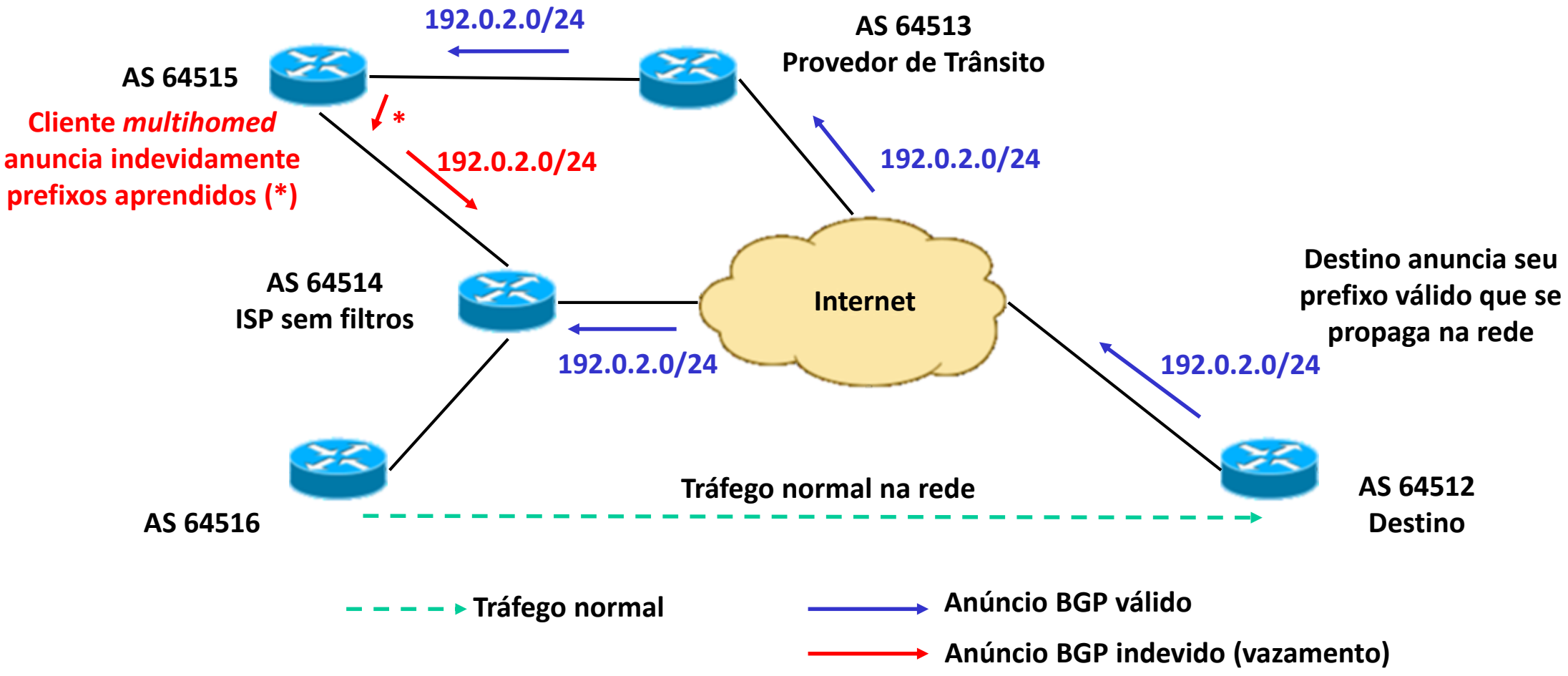
Segurança e estabilidade da Internet
Ataque por Sequestro de Prefixos (Hijacking)

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



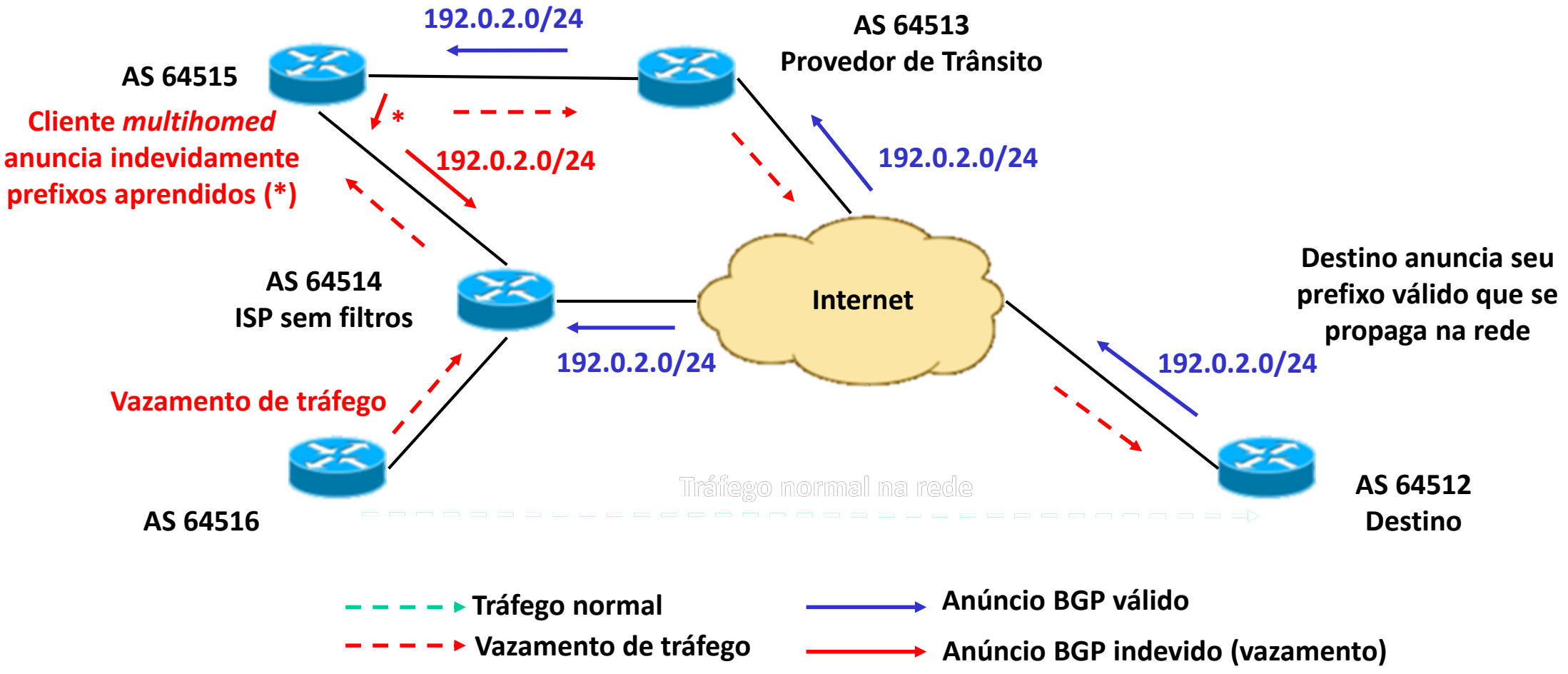
Segurança e estabilidade da Internet
Ataque por Vazamento de Rotas (Leak)

Topologia sem filtros de anúncios



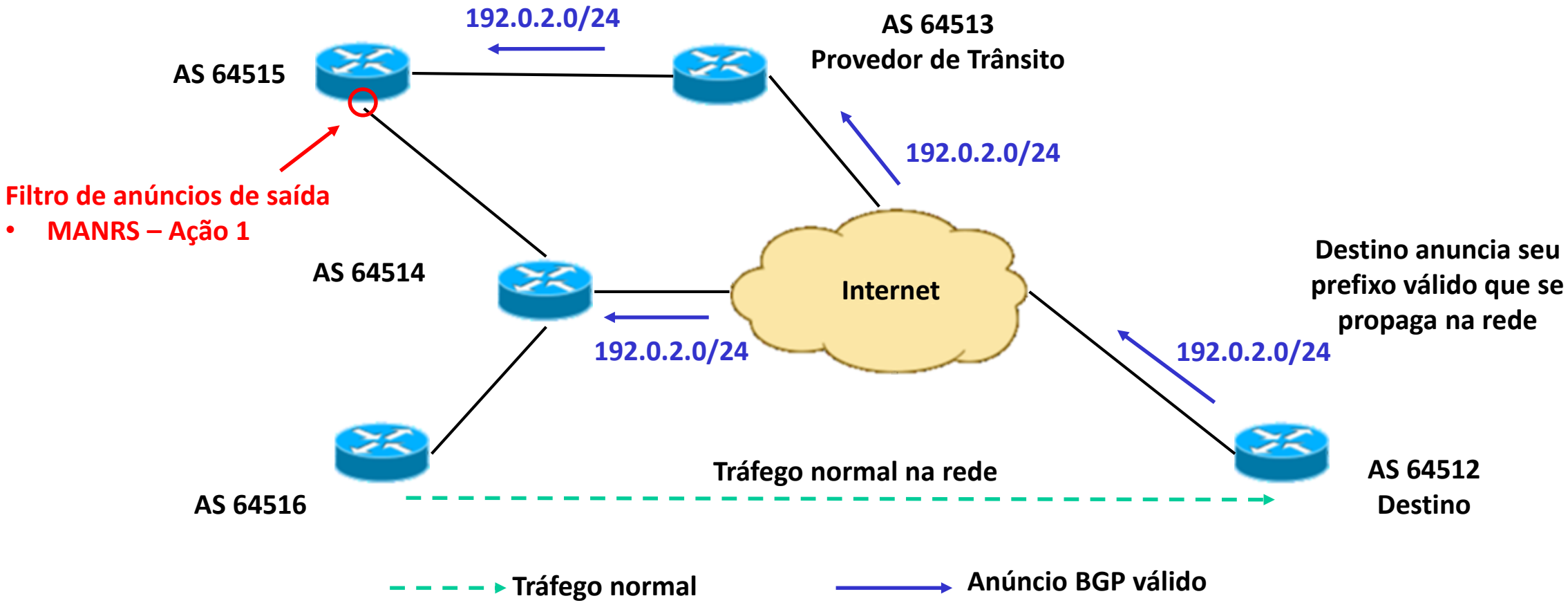
Segurança e estabilidade da Internet
Ataque por Vazamento de Rotas (Leak)

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



Como resolver os problemas

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

MANRS

Mutually Agreed Norms for Routing Security

Apoiado pela Internet Society

Segurança e estabilidade da Internet
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)**

MANRS

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

Desenvolvimento do Programa

Programa por uma Internet mais Segura
Desenvolvimento do Programa - Cursos

- 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 Ips vulneráveis
  - Em mar/18: 581k grandes operadoras // 144k ISP e AS corporativos
  - Hoje: 198k grandes operadoras // 162k ISP e AS corporativos.
- Ação com as maiores Associações de Provedores de Internet
- Ação com a indústria

Panorama Atual
Endereços IP e ASN notificados pelo CERT.br

Brasil	DNS		SNMP		NTP		SSDP	
mês	ASNs	IP	ASNs	IP	ASNs	IP	ASNs	IP
2018-01	2.412	61.875	2.130	479.247	823	97.075	888	25.982
2018-02	2.438	72.185	2.324	559.784	849	93.801	778	20.210
2018-03	2.476	63.811	2.278	515.345	844	84.483	544	11.431
2018-04	2.509	66.371	2.280	436.702	850	85.549	794	21.686
2018-05	2.343	65.270	2.390	502.861	870	88.788	846	23.174
2018-06	2.629	70.188	2.284	447.411	805	87.408	817	23.340
2018-07	2.721	68.415	2.436	431.907	881	89.484	787	17.255
2018-08	2.459	56.555	2.411	397.622	895	89.353	613	11.855
2018-09	2.767	62.942	2.366	193.432	772	87.378	836	21.836
2018-10	2.806	64.912	2.383	163.987	856	85.911	789	20.233
2018-11	2.604	60.937	2.376	137.331	851	87.155	814	20.124
2018-12	2.849	64.649	2.361	137.463	719	82.610	832	21.704
2019-01	2.960	74.257	2.583	137.253	923	89.567	840	17.348
2019-02	2.905	69.093	2.556	136.401	944	80.838	868	20.689

O Brasil está em **terceiro** lugar entre os endereços IPs abertos para abuso utilizando o protocolo SNMP

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

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

www.site.br

gzorello@nic.br

23 de fevereiro de 2019

nic.br cgi.br

www.nic.br | www.cgi.br