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

ABRAHOSTING
São Paulo, SP | 8/9/20

PROGRAMA POR UMA INTERNET MAIS SEGURA

O FUTURO DA INTERNET DEPENDE DA SEGURANÇA DOS SEUS PARTICIPANTES

Gilberto Zorello | 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

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

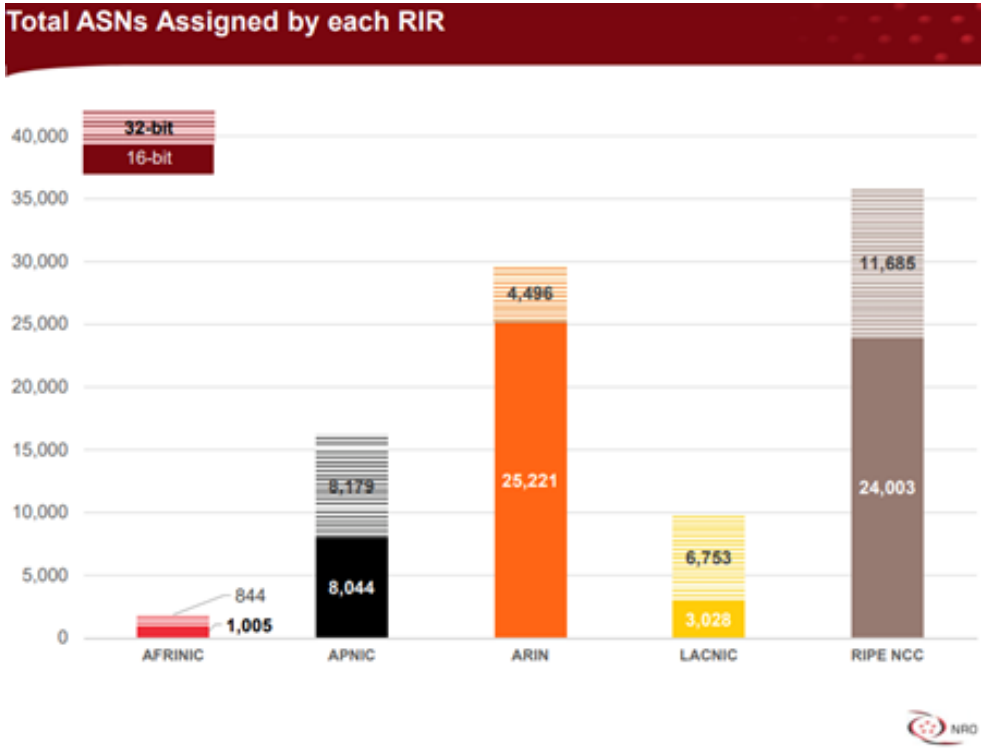
1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br

Panorama atual

Segurança e estabilidade da Internet
Estrutura da Internet atual

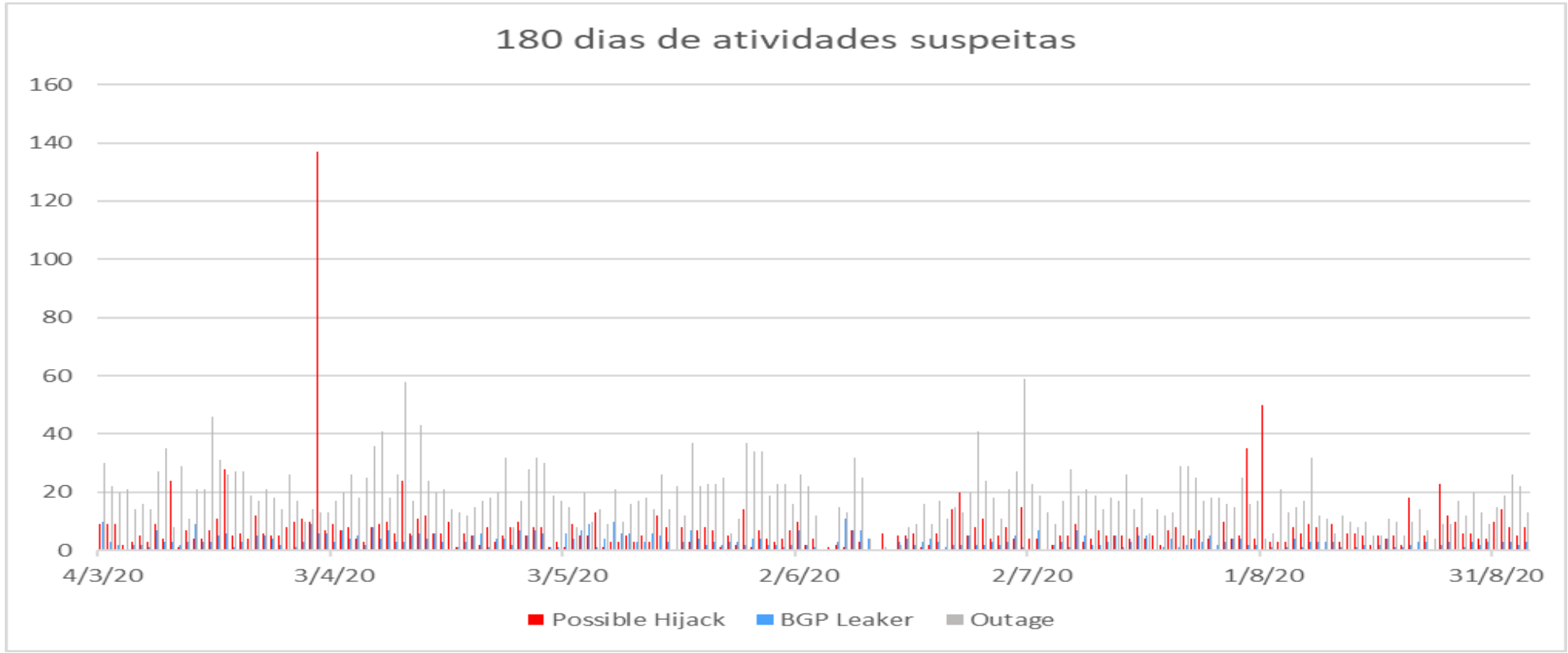
A Internet funciona com base na cooperação entre Sistemas Autônomos

- 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



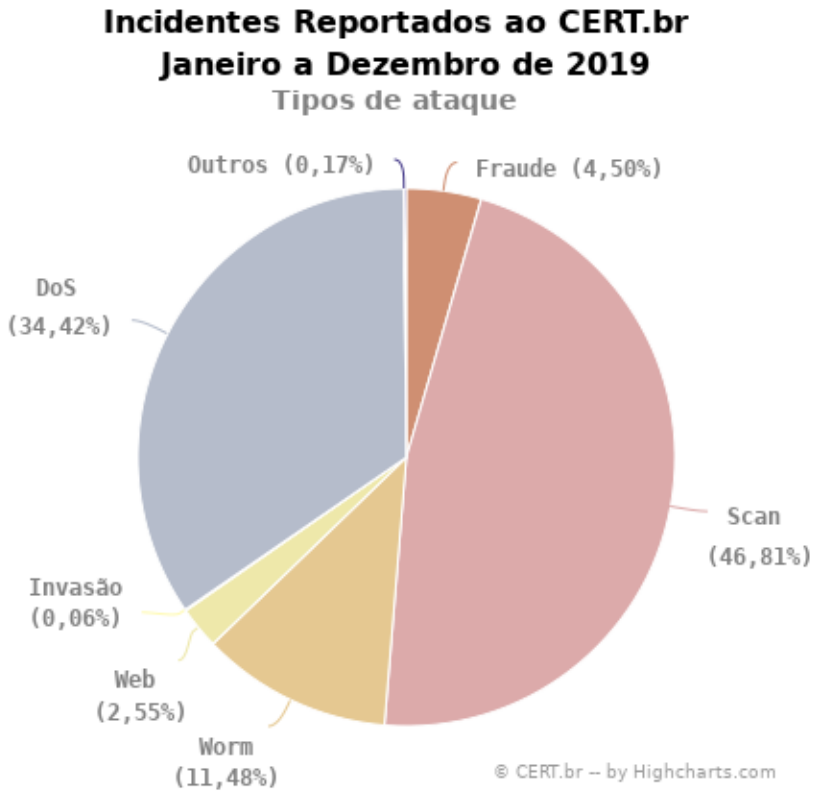
Fonte: https://bgpstream.com/

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

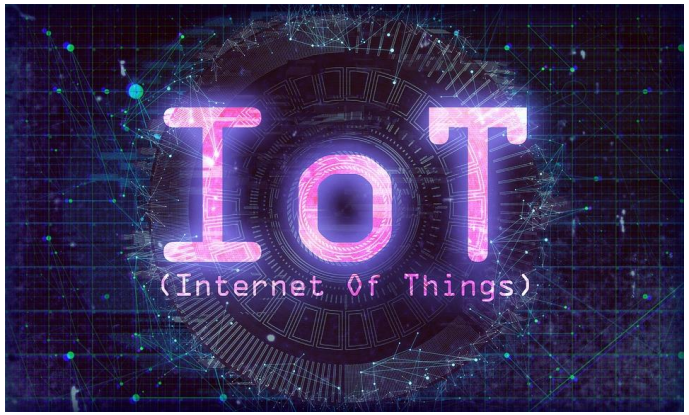


https://www.cert.br/stats/incidentes/2019-jan-dec/tipos-ataque.html

Constata-se um ritmo crescente de notificações de varreduras e DoS [5]

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?

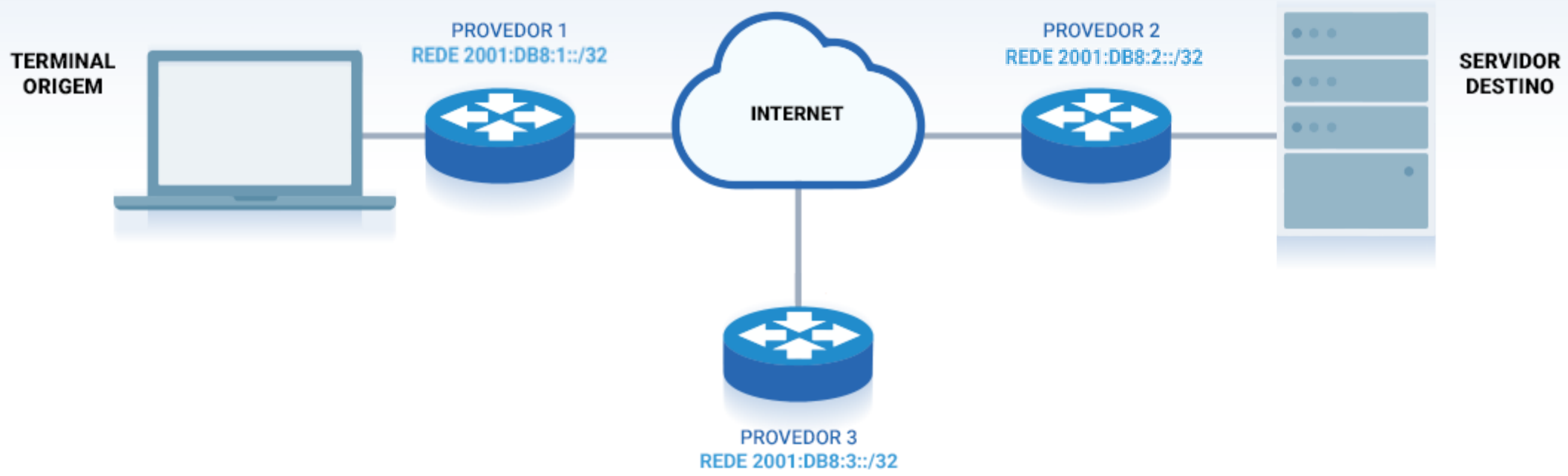
- **Como estamos em relação à segurança ?**

Ataques mais frequentes na infraestrutura da rede

Segurança e estabilidade da Internet

Ataque DoS por reflexão

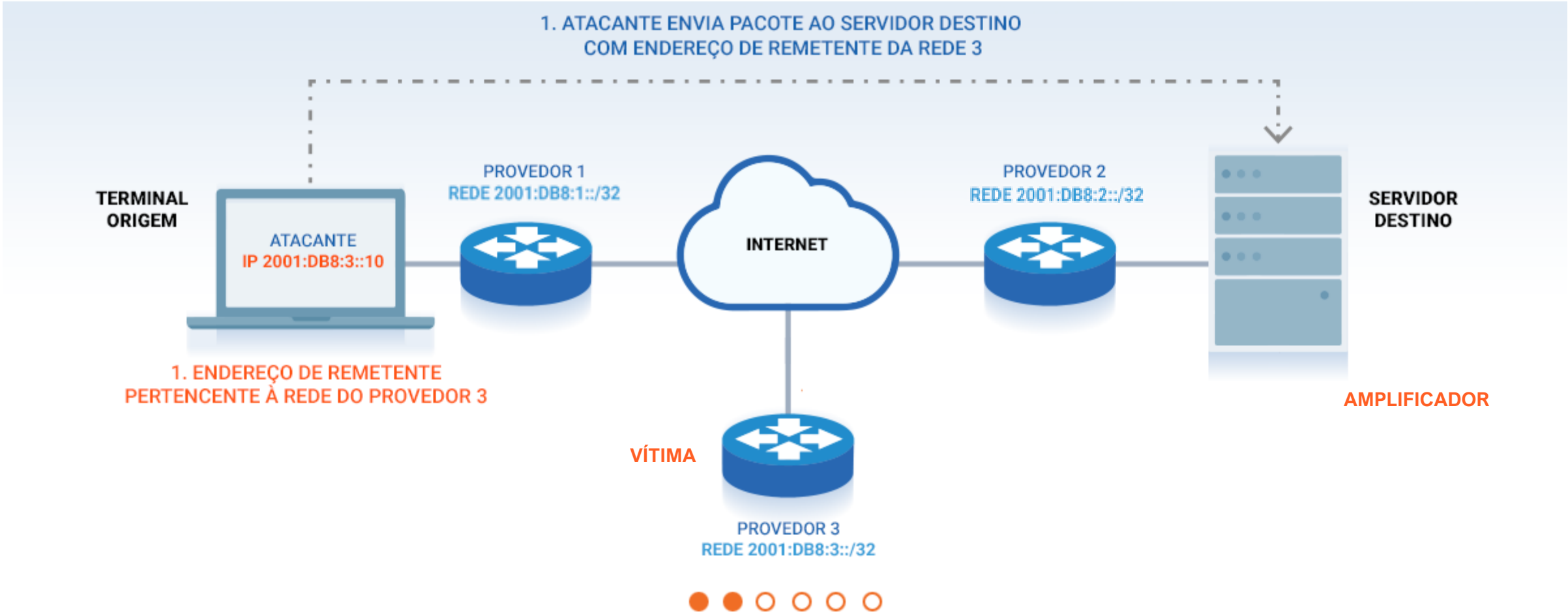
Topologia de rede sem filtros antispoofing [3]



Segurança e estabilidade da Internet

Ataque DoS por reflexão

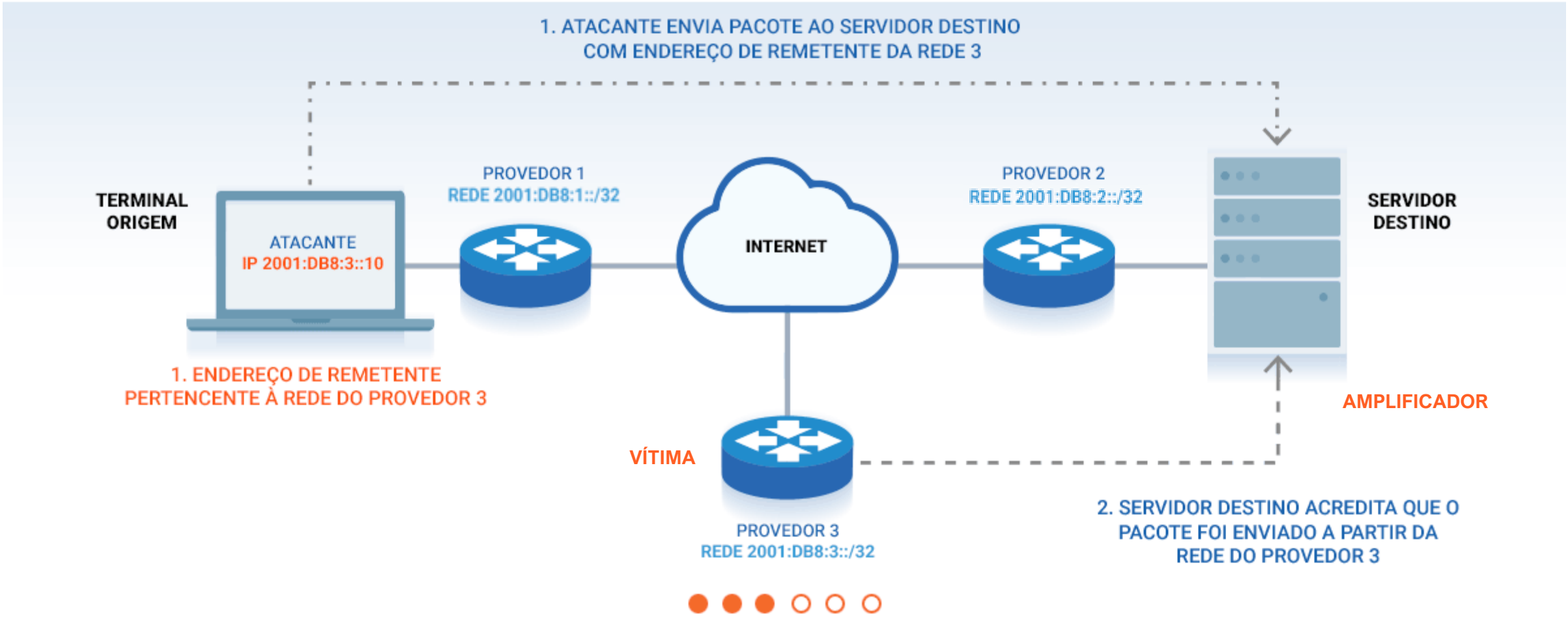
Ataque DoS utilizando endereço de remetente forjado (Spoofing) [3]



Segurança e estabilidade da Internet

Ataque DoS por reflexão

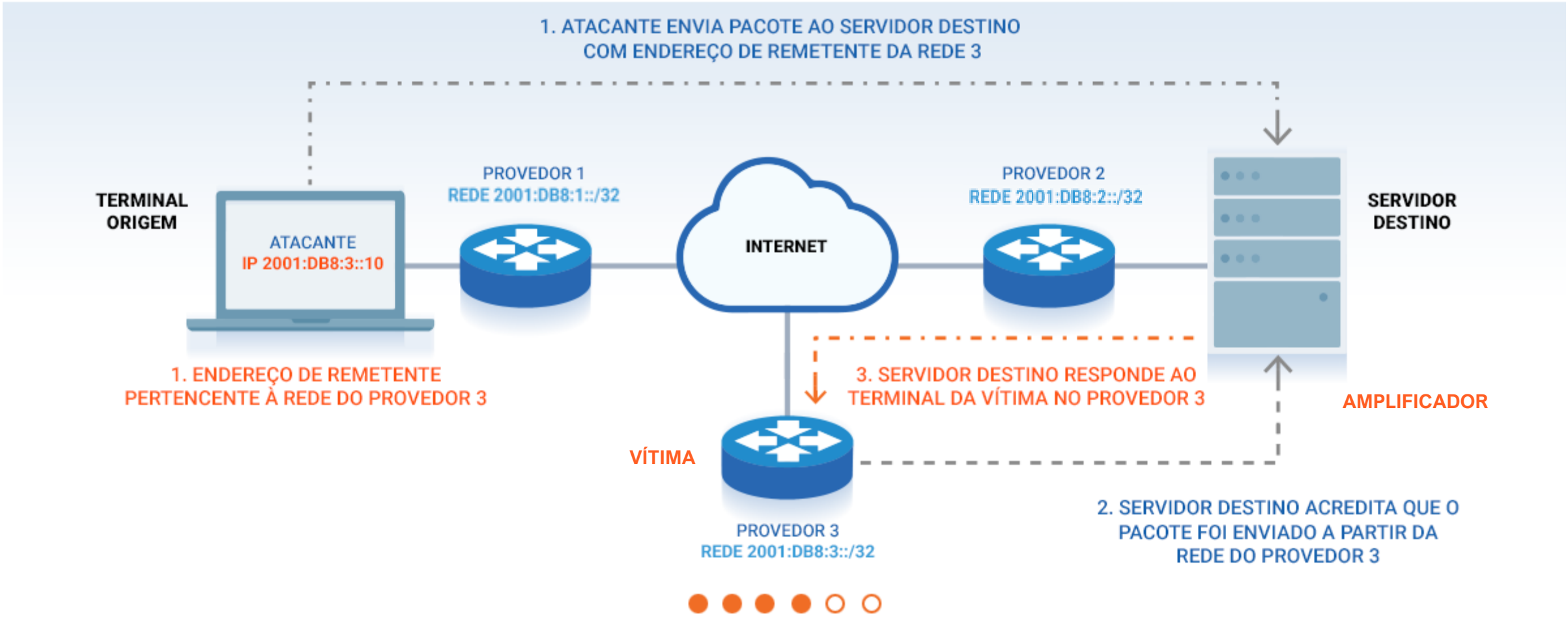
Ataque DoS utilizando endereço de remetente forjado (Spoofing) [3]



Segurança e estabilidade da Internet

Ataque DoS por reflexão

Ataque DoS utilizando endereço de remetente forjado (Spoofing) [3]



Segurança e estabilidade da Internet

Servidor Destino

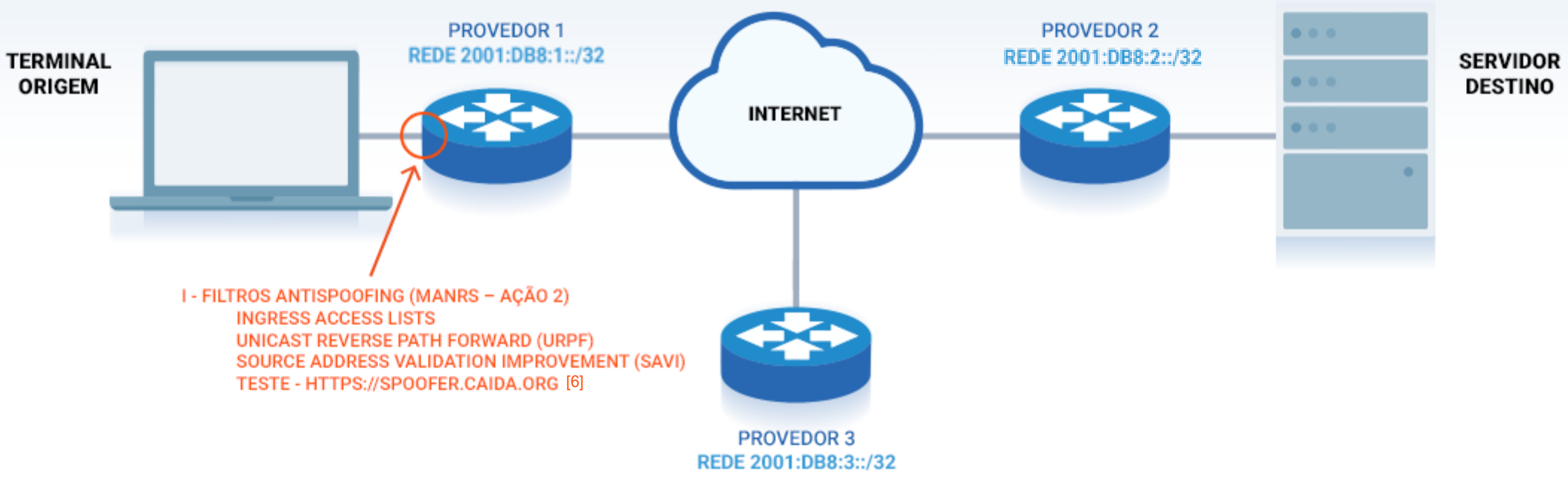
Os protocolos usados nos ataques fazem parte legítima da infraestrutura pública da Internet, porém em alguns equipamentos, como CPEs, são instalados por padrão e abusados por atacantes.

- 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

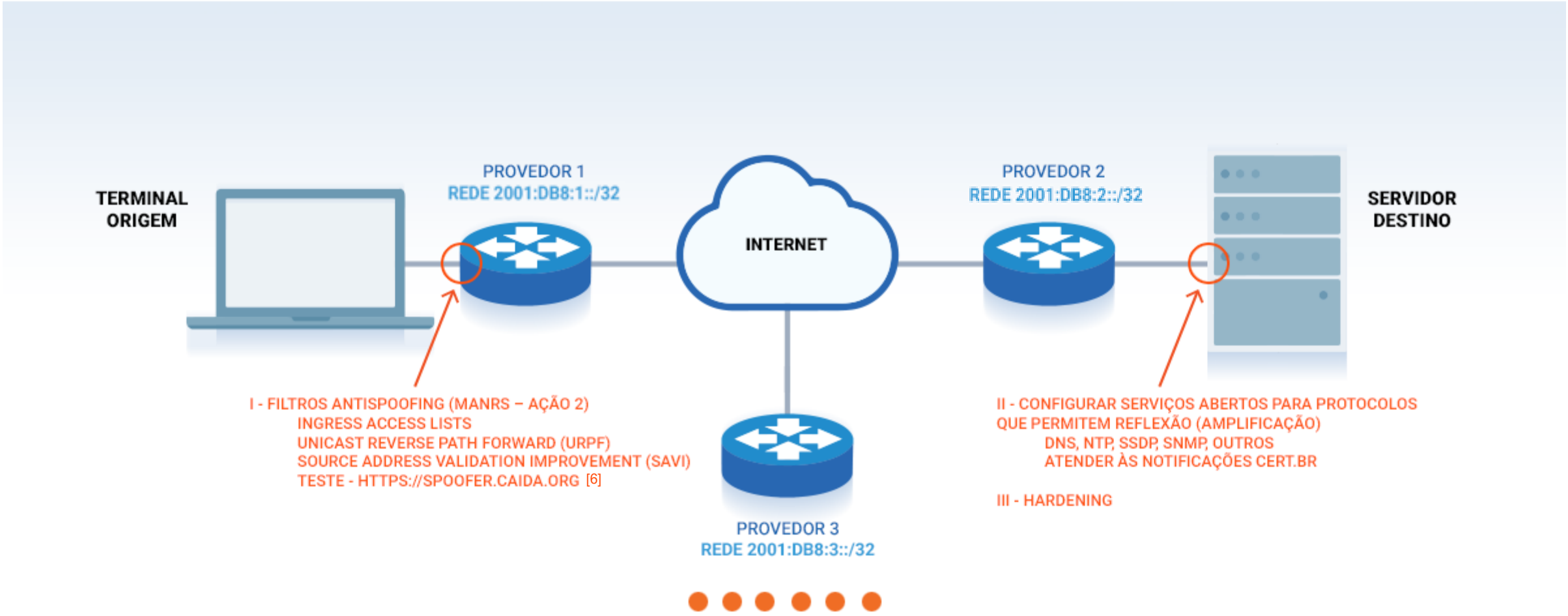
Solução: Aplicação de filtros antispoofing BCP38 [3]



Segurança e estabilidade da Internet

Ataque DoS por reflexão

Solução: Aplicação de filtros antispoofing, configuração de serviços e Hardening [3]



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 [8]

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

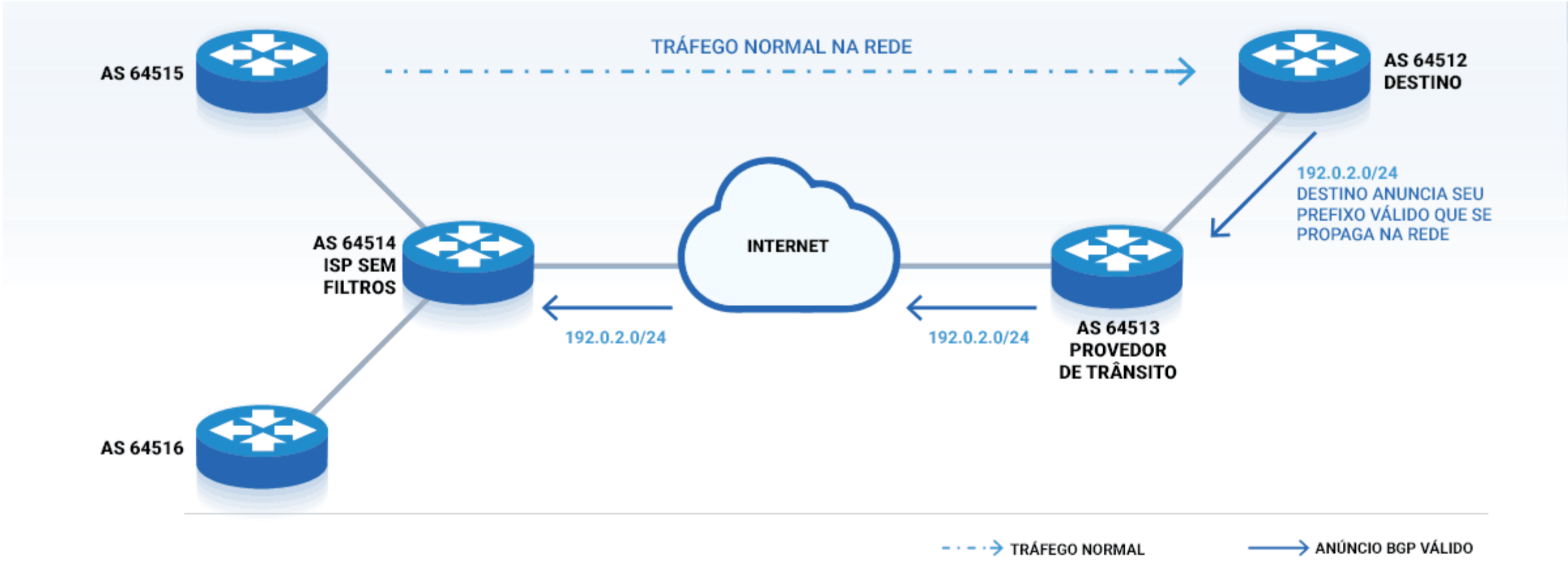
Dispositivos mais utilizados nos ataques utilizando botnets:

- Modens 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

Ataque por Sequestro de Prefixos (Hijacking)

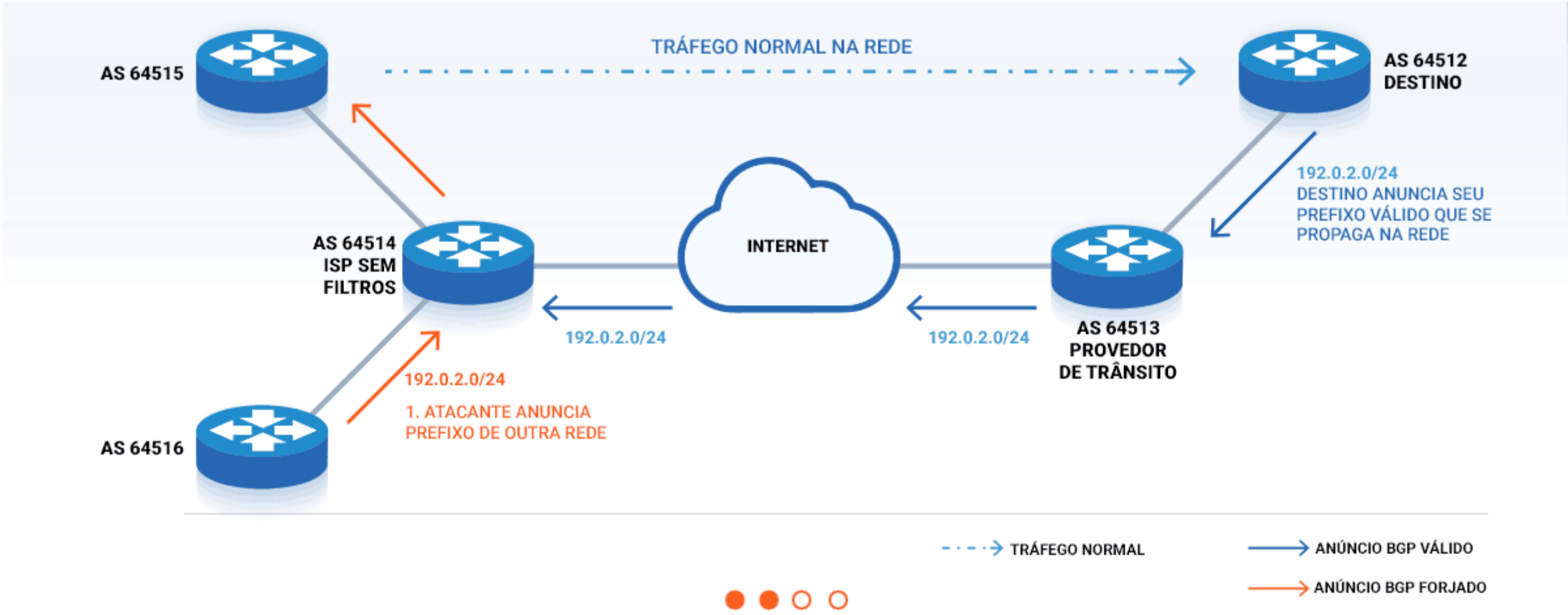
Topologia de rede sem filtros de anúncios



Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

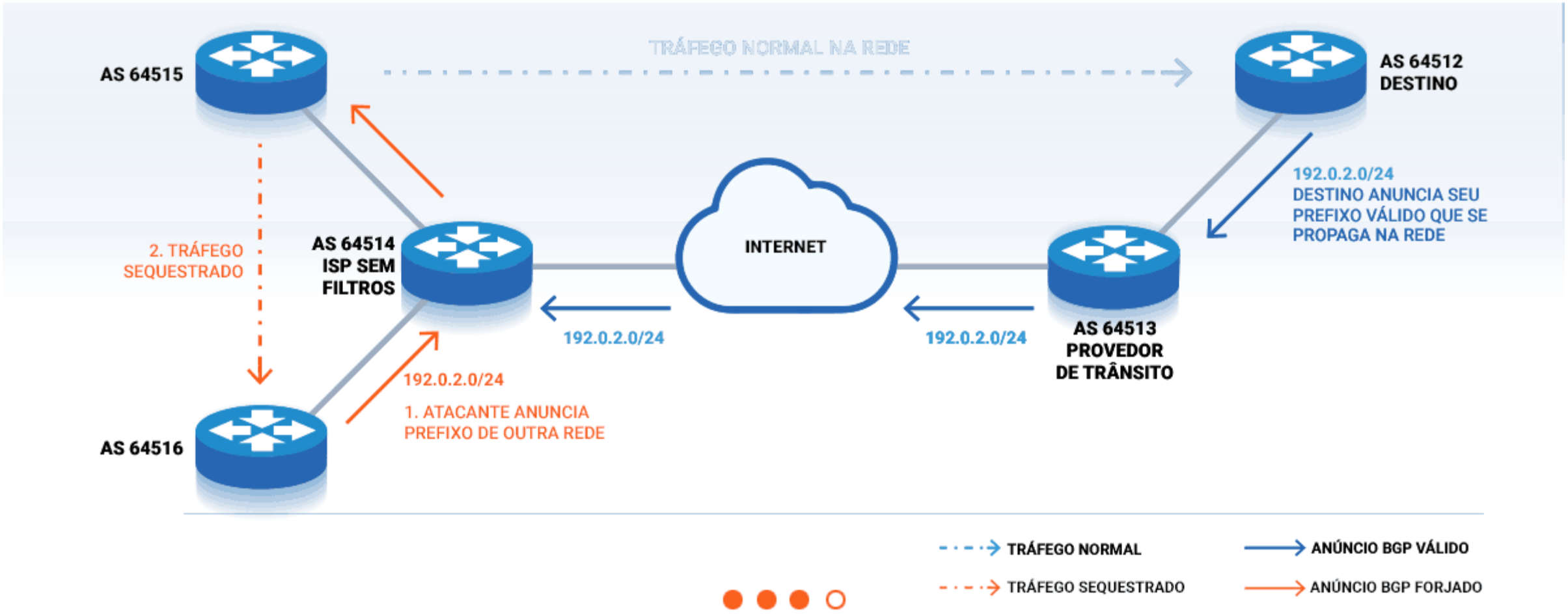
Topologia de rede sem filtros de anúncios



Segurança e estabilidade da Internet

Ataque por Sequestro de Prefixos (Hijacking)

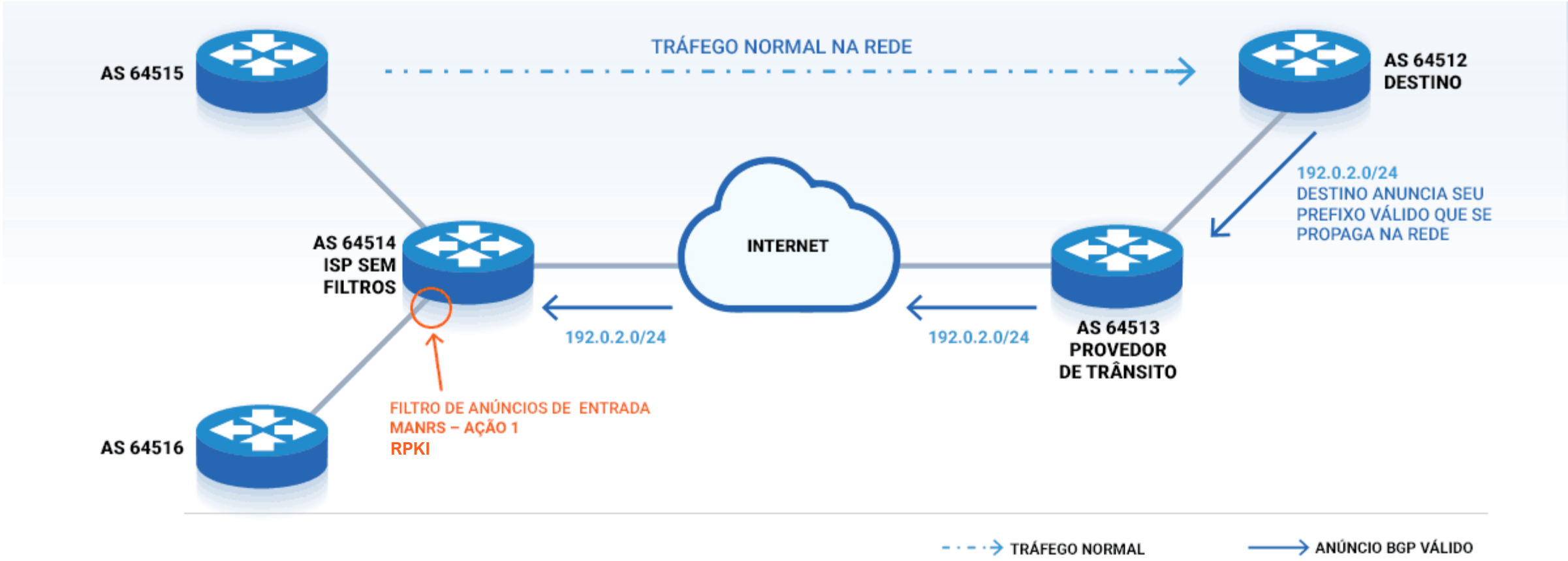
Topologia de rede sem filtros de anúncios



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
Problemas de segurança

- A falta de preocupação com a segurança da infraestrutura impacta as redes e os negócios
- **Redes mal configuradas são mais vulneráveis a ataques e podem ser utilizadas para atacar outras redes**
- Seus recursos são comprometidos: links de conexão e equipamentos
- **Pode levar a empresa ser envolvida em ataques : um único problema pode manchar a reputação de uma companhia frente a clientes e potenciais parceiros**
- A adoção de procedimentos de segurança adiciona um valor competitivo num mercado em que todos oferecem serviços semelhantes e direcionados ao preço
- **Mostra também competência e comprometimento com a segurança dos serviços prestados aos seus clientes**
- “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

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

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**
- 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 INTERNET +SEGURA

Programa por uma Internet mais Segura
Interação com Associações

Atividades com Operadoras e Provedores com apoio das Associações

- Reuniões bilaterais
  - Correção de pontos de contato para notificação (Ação 3 MANRS) [2]
    - 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) [4]
  - Adoção de Boas Práticas de roteamento (MANRS) [2]

Nome da Empresa	ASN	DNS	SNMP	NTP	SSDP	PORTMAP	MEMCACHED	NETBIOS	QOTD	CHARGEN	LDAP	MDNS	UBNT	WS-DICOVERY	TFTP	CoAP	ARMS	2020-06	2020-07	2020-08	Mais Recente	MT4145
Empresa 1	ASN1	7	12	1	0	0	0	2	0	0	0	2	0	0	0	0	0	221	211	204	24	0
Empresa 2	ASN2	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	8	9	9	3	0
Empresa 3	ASN3	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	1	1	1	0
Empresa 4	ASN4	6	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	2	2	7	9	0
																		229	**220**	**213**	**27**	

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: 106k grandes operadoras // 163k ISP e ASN corporativos (novos protocolos analisados – UBNT, WS-DISCOVERY, TFTP (39/61)**
  - Redução total dos IPs notificados de 62% desde o início do Programa
    - **Segmentação dos IPs notificados: 59% ISPs, 1% corporativos, 40% operadoras**
  - Segmentação dos ASNs (Brasil): 90,7% ISPs, 9,0% 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
2019-10	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	3.143	64.219	3.021	81.009	1.015	71.864	721	9.326	1.305	20.780
2020-04	3.051	64.224	3.044	81.169	1.050	71.528	720	8.703	1.290	20.134
2020-05	3.217	69.588	3.121	86.097	1.080	70.097	749	9.624	1.475	21.312
2020-06	3.248	59.613	3.119	87.996	1.063	69.523	705	5.859	1.388	18.746
2020-07	3.270	65.856	3.201	86.097	1.120	69.026	699	9.380	1.339	17.531
2020-08	3.261	63.398	3.191	83.327	1.131	69.764	770	15.579	1.274	15.503
2020-09	na	na	3.172	81.526	1.143	70.447	na	na	1.208	12.596

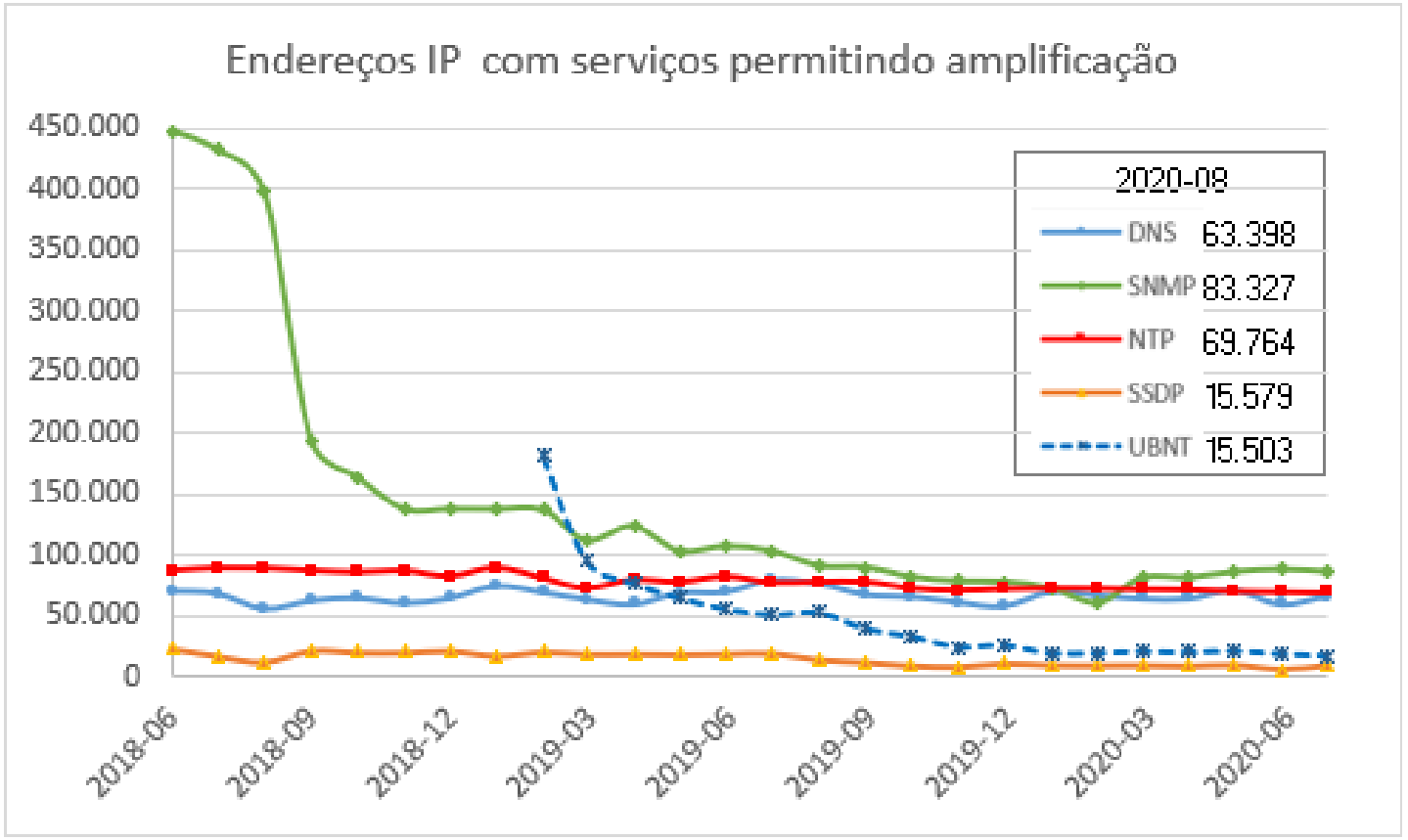
O Brasil está em **quinto** lugar entre os endereços IPs com serviços SNMP mal configurados

"na" – significa que ainda não houve notificação para o serviço

Fonte: https://snmpscan.shadowserver.org/ [7]

Notificações encaminhadas pelo CERT.br

Resultados: redução de serviços mal configurados



Fonte dos dados: CERT.br

01/09/20

Redução de 62% do total de serviços mal configurados desde o início do Programa

ISPs e ASes corporativos

2018-06 → 20%

2020-08 → 60%

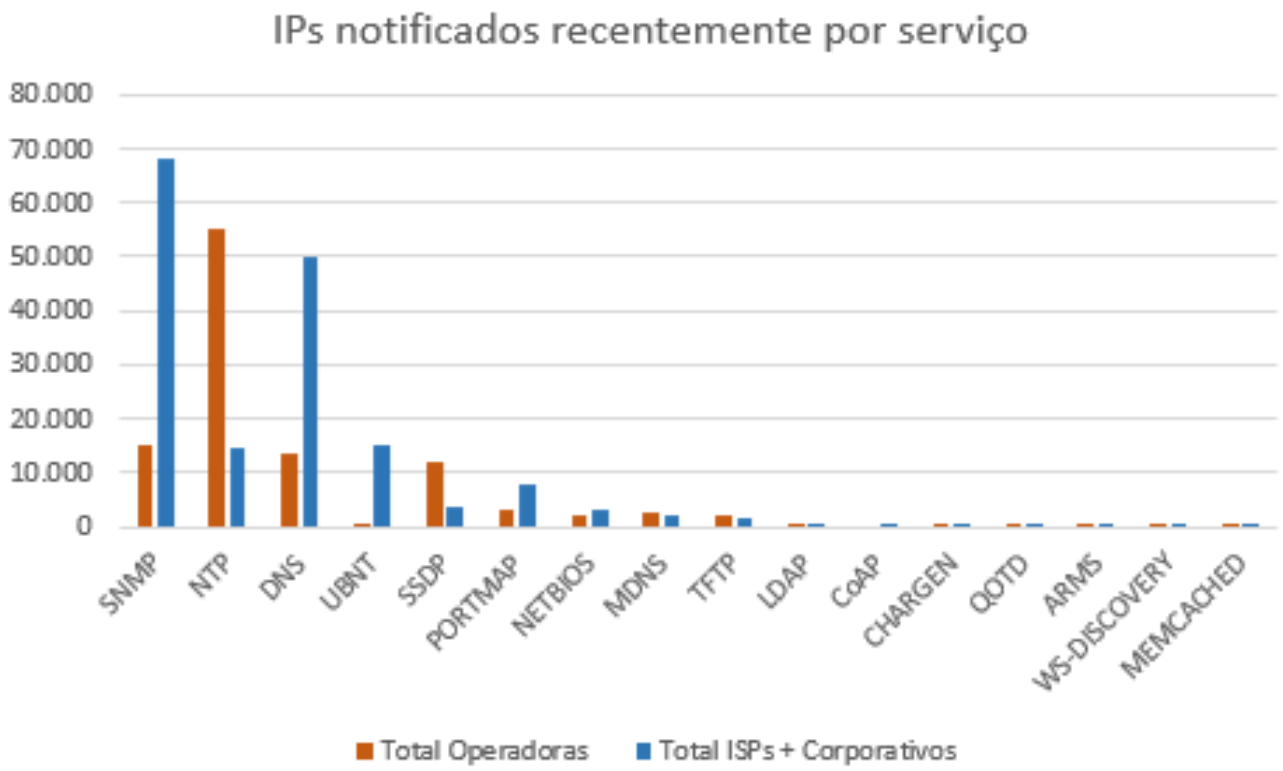
Grandes operadoras

2018-06 → 80%

2020-08 → 40%

Notificações encaminhadas pelo CERT.br

Status atual dos serviços mal configurados



***Share* dos serviços mal configurados**

ISPs e ASes corporativos →

SNMP, DNS, UBNT e NTP (60%)

Grandes operadoras →

NTP, SNMP, DNS e SSDP (40%)

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

Programa por uma Internet mais Segura
Página WEB

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

Notificações de serviços amplificadores: Sobre os dados notificados

Os números são relativos a IPs notificados pelo CERT.br

Notificações periódicas enviadas aos contatos dos Sistemas Autônomos (AS)

- Contém uma lista com endereços IP que possuem serviços mal configurados que permitam o abuso para amplificação de tráfego
- São notificados apenas aqueles que foram testados pelo CERT.br para confirmação do problema
- Logs do teste possuem horário sincronizado e fuso horário do momento da realização do teste

Fonte inicial da lista de serviços e IPs testados pelo CERT.br

Dados da Fundação ShadowServer

- O CERT.br, como CERT Nacional, tem acesso a todos os dados de redes brasileiras
- Os testes são realizados para eliminar falsos positivos

Artigo do *ShadowServer* sobre os testes de amplificadores:

https://www.shadowserver.org/news/the-scannings-will-continue-until-the-internet-improves/

Esta ação é importante para mitigar ataques volumétricos reflexivos que utilizam amplificação de tráfego na rede

Programa por uma Internet mais Segura
Parceria com a *Internet Society*

MANRS

Mutually Agreed Norms for Routing Security

http://manrs.org

Parceria: NIC.br e Brasil lideram a participação no MANRS (Blog)

Implementação de filtros de anúncios

- Destacamos a importância da implantação dos filtros de anúncios preconizados pela Ação 1 do MANRS (https://bcp.nic.br/i+seg/acoes/manrs/#filtragem-de-rotas): é importante que o administrador do AS garanta a correção dos próprios anúncios e de seus clientes.

- **BGP Stream é uma ferramenta "*free*" que recebe alertas de *hijacking*, vazamento de rotas (*leak*) e outages do protocolo BGP na Internet e disponibiliza relatório para os últimos 180 dias de eventos.**

  - https://bgpstream.com/

  - Radar QRator

- É importante implantar filtros de anúncios na ativação dos clientes de trânsito e filtros de anúncios de saída

Validação de endereço IP de origem
Filtros Antispoofing – Testes pelo *Spoofer* do CAIDA

Ação 2 do MANRS - Impedir tráfego com endereços IP de origem falsificados

Implementação de filtro *antispoofing* o mais próximo do cliente – uRPF (*Unicast Reverse Path Forwarding*) - *Strict Mode, Loose Mode, Vrf Mode*

CAIDA: Center for Applied Internet Data Analysis

Conduz pesquisas de rede e constrói infraestrutura para dar suporte à coleta, curadoria e distribuição de dados para a comunidade de pesquisa científica

Projeto: ferramenta Spoofer disponibilizado pelo CAIDA

Site: https://www.caida.org/projects/spoofer/

Ferramenta de software de código aberto para avaliar e relatar a implantação das melhores práticas para validação de endereço de origem

Busca minimizar a suscetibilidade da Internet a ataques DDoS com endereços de origem falsificados

O projeto Spoofer é patrocinado pela Diretoria de Ciência e Tecnologia do Departamento de Segurança Interna dos EUA e pelo Governo de Reino Unido da Grã-Bretanha e Irlanda do Norte. Projeto originado no MIT ANA

Apresentação de dados referentes às últimas medições realizadas por software cliente instalado em máquina de usuário final que acessa servidores do Projeto CAIDA ao redor do mundo

Contatos utilizados para notificações

Ação 3 do MANRS - Facilitar a comunicação operacional global e a coordenação entre os operadores de rede.

E-mails indicados no Whois:

AS	Titular
	Roteamento
	Abuse

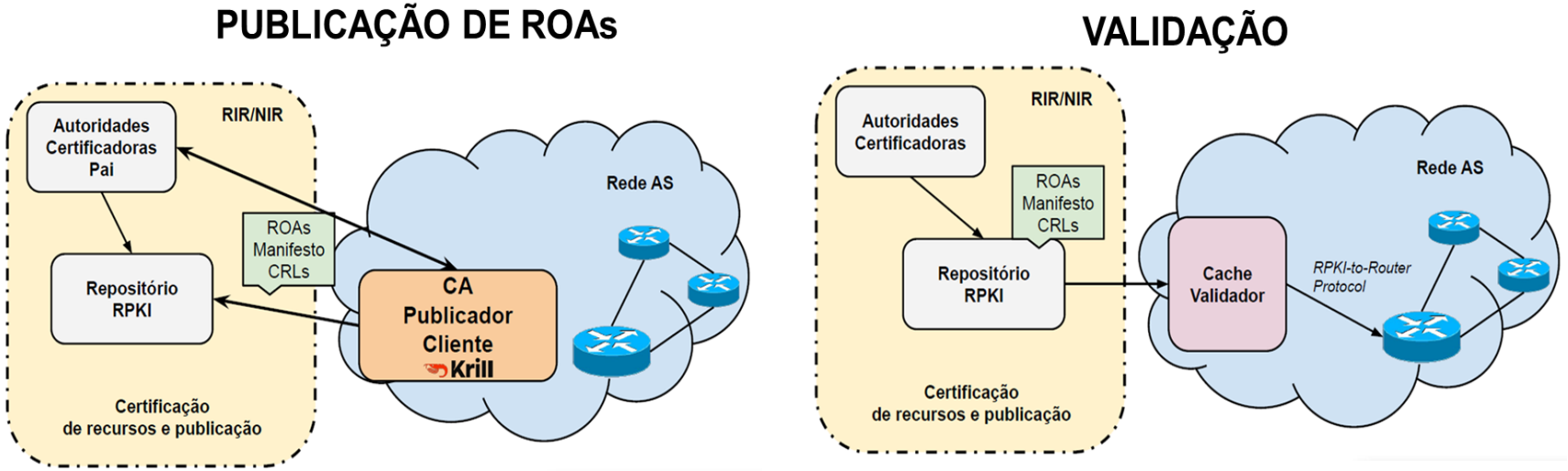
Pontos de contato no PeeringDB:

- Além do *Whois* do Registro.br o *MANRS* recomenda a disponibilização dos pontos de contato no PeeringDB.

Validação Global

Ação 4 do *MANRS*

- **Cadastro da política da política de Roteamento no IRR (RADB)**
- **Avaliar a implantação de *RPKI* para certificar alocações de endereços IP e ASN (processo automático)**
  - Publicação de *ROAs* (*Route Origin Authorisation*)
  - Filtro automático de anúncios
  - https://bcp.nic.br/rpki



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, backup seguro, script de configuração
- Registros e Auditoria
  - Nível criticidade, armazenado em local seguro, hora correta (NTP)
  - Registro de ações

Minimum security requirements for CPEs acquisition

Publicação conjunta:

- *M³AAWG - Messaging, Malware and Mobile Anti-Abuse Working Group*
- *LACNOG - Latin American and Caribbean Network Operators Group*
- Editora*:* Lucimara*, LAC-AAWG Chair / CERT.br*

Um *checklist* de referência para aquisição de equipamentos que permitam atualização e gerenciamento remoto, e que sejam nativamente mais seguros, visando:

- 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 trabalho de reparo

https://www.m3aawg.org/CPESecurityBP

https://www.m3aawg.org/CPESecurityBP-Portuguese

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

Maio 2019

Este documento está disponível no site do LACNOG em www.lacnog.net/docs/lac-bcop-1

Este documento está disponível no site do M3AAWG em www.m3aawg.org/CPESecurityBP-Portuguese

A versão original em Inglês está disponível no site do M3AAWG em www.m3aawg.org/CPESecurityBP

Este é um documento conjunto de Melhores Práticas Operacionais Atuais (*Best Current Operational Practices*, BCOP) desenvolvido pelo LACNOG[1] (Grupo de Operadores de Redes da América Latina e o Caribe) e pelo M3AAWG[2] (Messaging, Malware and Mobile Anti-Abuse Working Group). É o produto das versões originais do LACNOG por seus grupos de trabalho LAC-AAWG[3] (Grupo de Trabalho Antiabuso da América Latina e o Caribe) e Grupo de Trabalho BCOP[4], em cooperação com membros do M3AAWG, Assessores Técnicos Sêniores e o Comitê Técnico do M3AAWG.

Índice

1 Grupo de Operadores de Redes da América Latina e o Caribe (LACNOG), https://www.lacnog.net/
2 Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), https://www.m3aawg.org/
3 Grupo de Trabalho Antiabuso da América Latina e o Caribe (LAC-AAWG), https://www.lacnog.net/lac-aawg/
4 Grupo de trabalho BCOP, https://www.lacnog.net/wg-bcops/

LACNOG
Grupo de Operadores de Redes da América Latina e o Caribe
Departamento de Montevidéu, República Oriental do Uruguai
www.lacnog.net

M3AAWG
Messaging, Malware and Mobile Anti-Abuse Working Group
781 Beach Street, Suite 302
San Francisco, California 94109 U.S.A. – www.m3aawg.org

Programa por uma Internet mais Segura
Referências

[1] https://youtu.be/TIVrx3QoNU 4?t=7586 - Painel sobre Programa para uma Internet mais Segura, IX (PTT) Fórum 11, 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#5 - 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] https://www.shadowserver.org/news/the-scannings-will-continue-until-the-internet-improves/ - Artigo do *ShadowServer* sobre os testes de amplificadores

[8] 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

8 de setembro de 2020

nic.br cgi.br

www.nic.br | www.cgi.br