
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 ptt.br


nic.br cgi.br
ceptro.br

MANRS

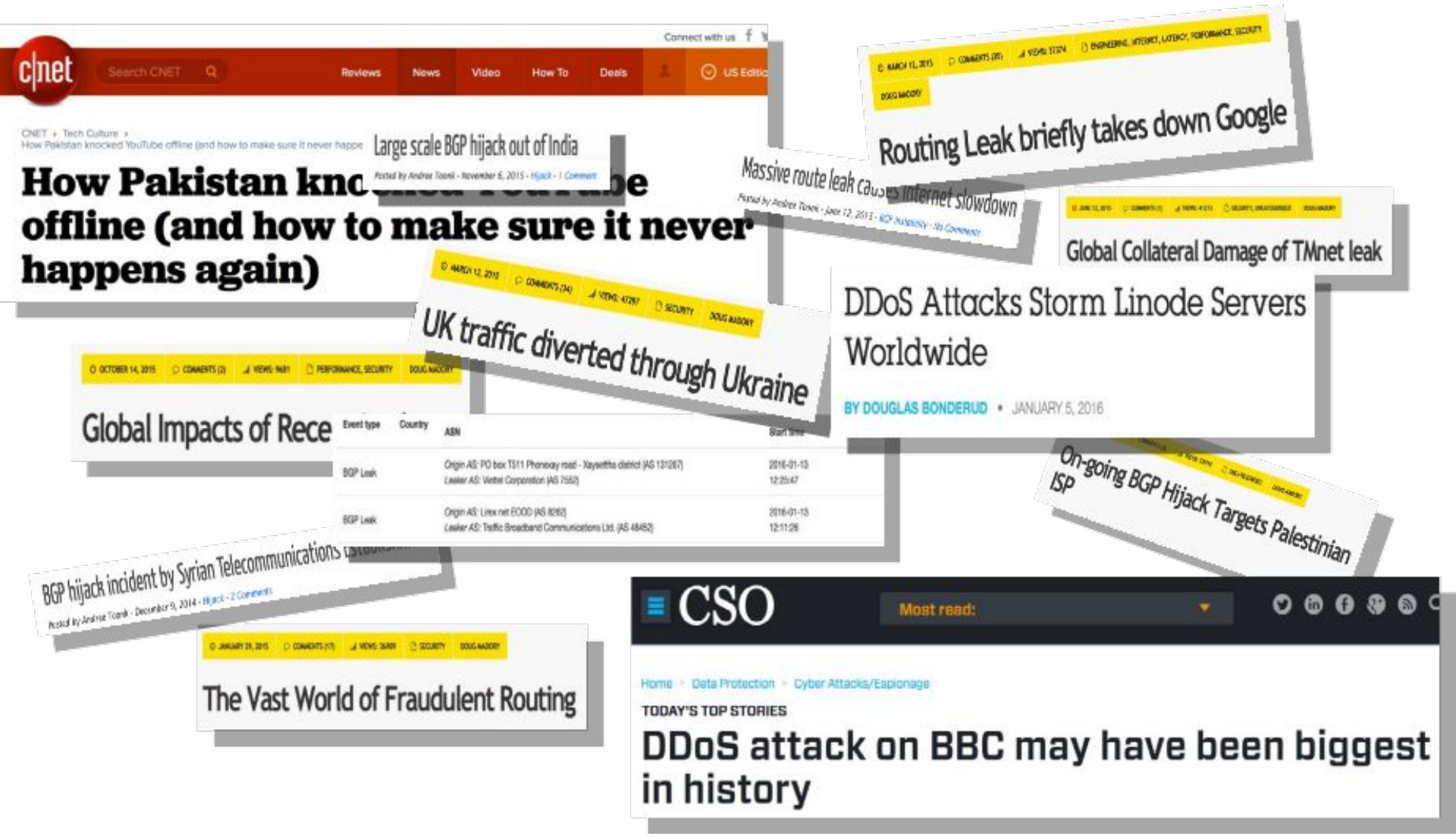
Mutually Agreed Norms for Routing Security

ceptro.br nic.br cgi.br

Como a Internet funciona?

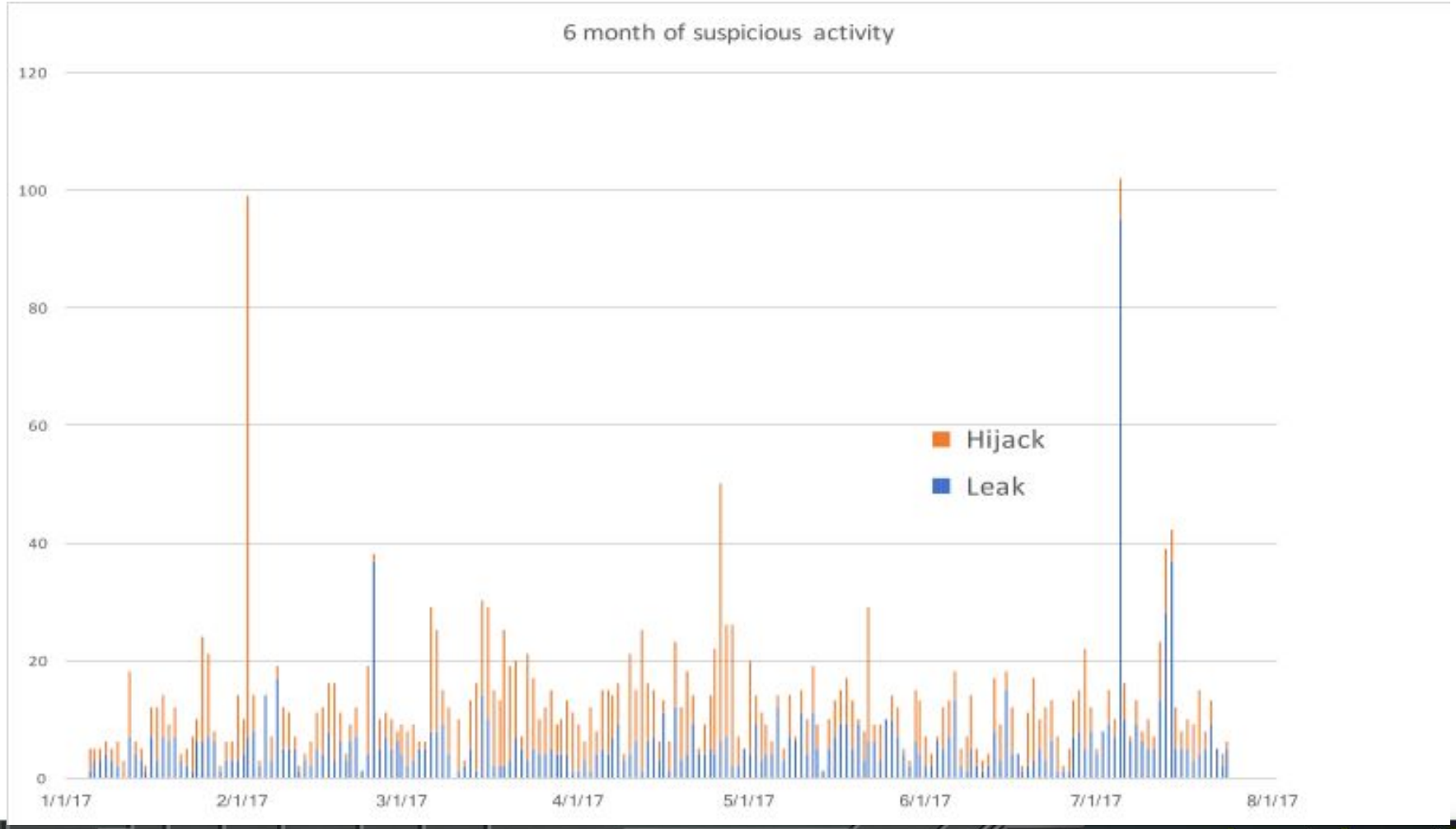
- A Internet é uma ’rede de redes’
- São quase 60.000 redes diferentes, sob gestões técnicas e administrativas diferentes.
- A estrutura de roteamento BGP funciona com base em cooperação e confiança.

O BGP não possui validação para os dados

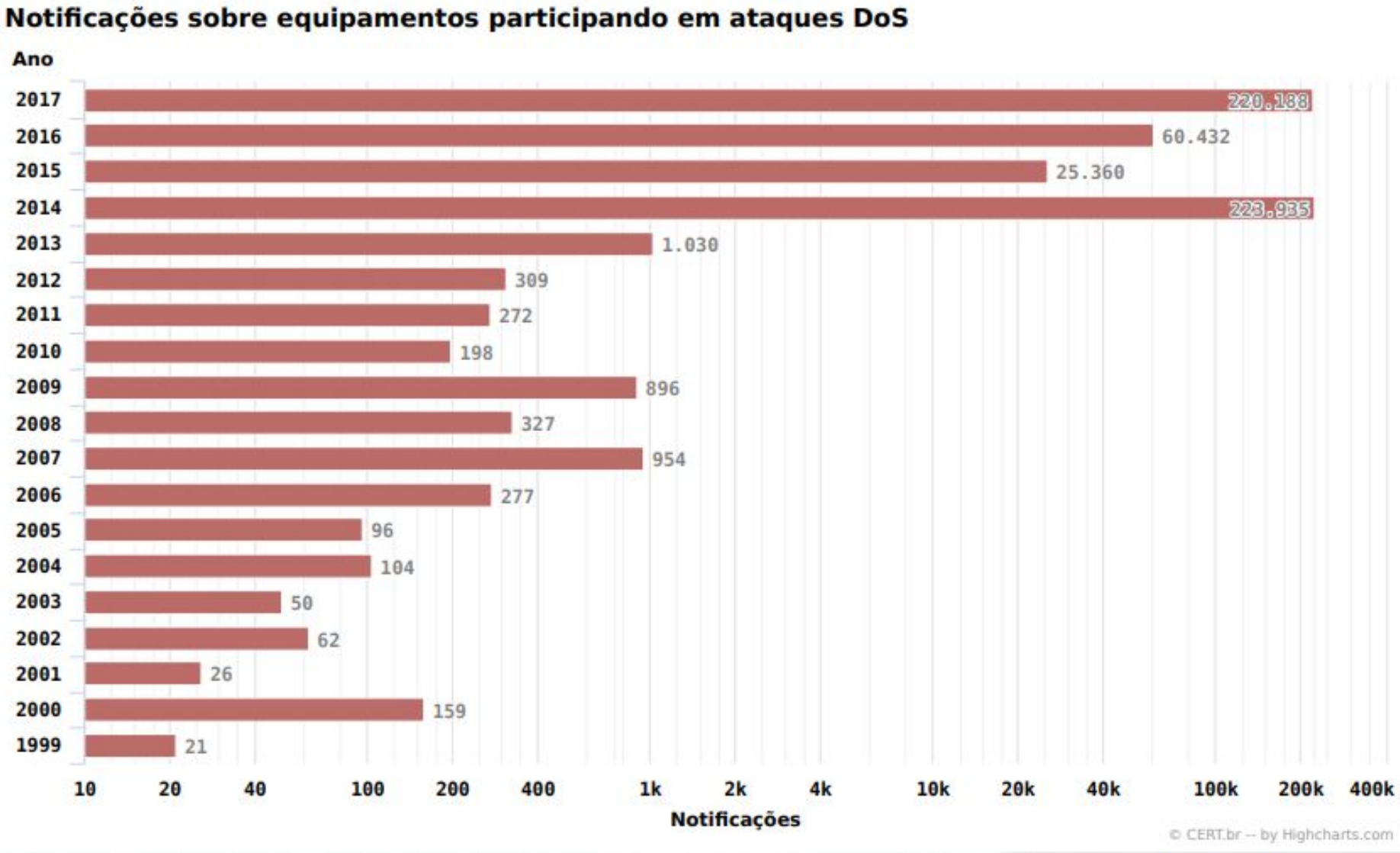


Segurança e estabilidade na Internet

- Nenhum dia sem incidente!!!



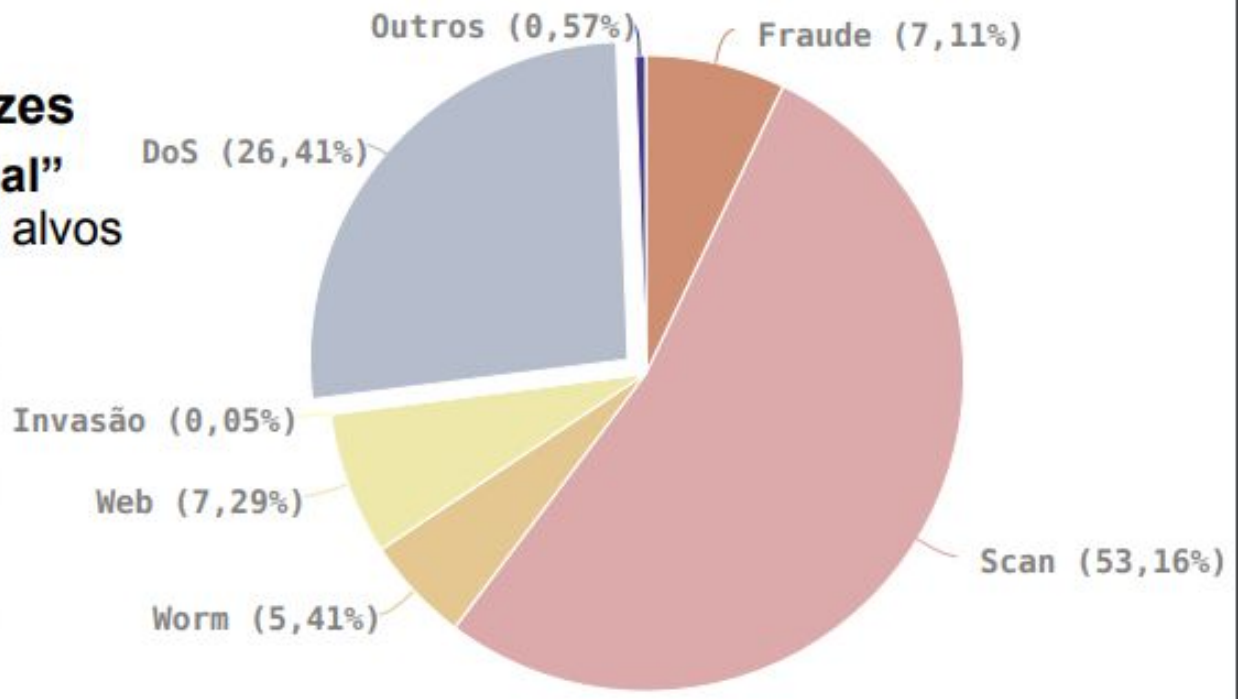
DDoS ao Longo do Tempo



Características dos Ataques DDoS

DDoS – aumento de 4 vezes

- **300Gbps é o novo "normal"**
  - Até 1Tbps contra alguns alvos
- **Tipos mais frequentes**
  - amplificação
  - *botnets* IoT



Como se proteger?

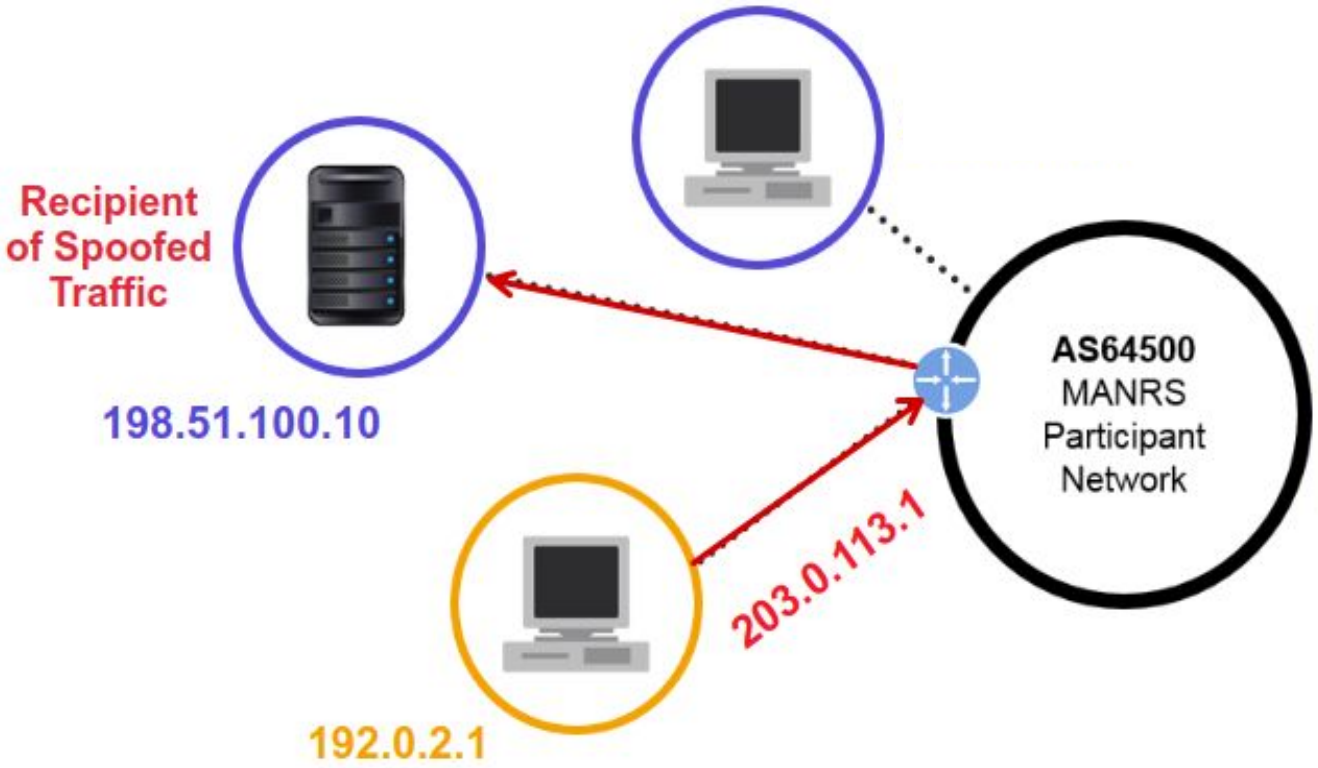
- Não basta se preocupar somente quando o problema acontece.
  - Isso é caro!
  - Pode requerer equipamentos e configurações complexas!
  - Não tem resolvido.

- É preciso se prevenir!
  - Hardening de equipamentos
  - MANRS
  - Evitamos que o ataque sai da nossa rede
  - É barato!

Entendendo o ataque: O que é spoofing?

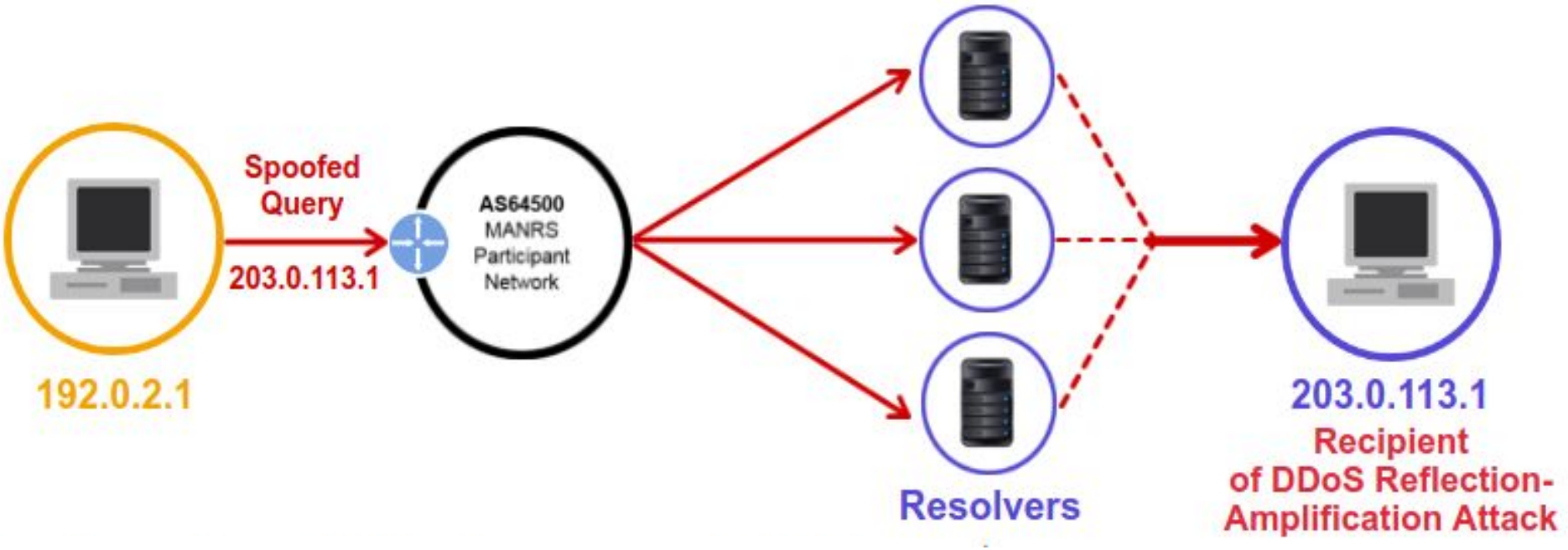
- Pacotes IP com endereços de origem incorretos
  - **Erro de configuração**
    - Problema de Software
  - **Teste e Simulação**
    - Teste de Performance
  - **Atitude maliciosa**
    - Esconder a identidade do atacante
    - Fingir ser outro computador na rede
- O spoofing pode ser usado em ataques de negação de serviço e é um problema sério na Internet

Como funciona o ataque spoofing



Destination	Source
198.51.100.10	203.0.113.1 ~~192.0.2.1~~

Como funciona o ataque reflexão-amplificação



Fatores de amplificação

Protocolo	Fator de Amplificação	Comando Vulnerável
DNS	28 a 54	Ver: TA13-088A
NTP	556.9	Ver: TA14-013A
SNMPv2	6.3	GetBulk request
LDAP / CLDAP	46 a 70	Malformed request
SSDP	30.8	SEARCH request
Chargen	358.8	Character generation request

Total de ASNs e IPs Notificados pelo CERT.br

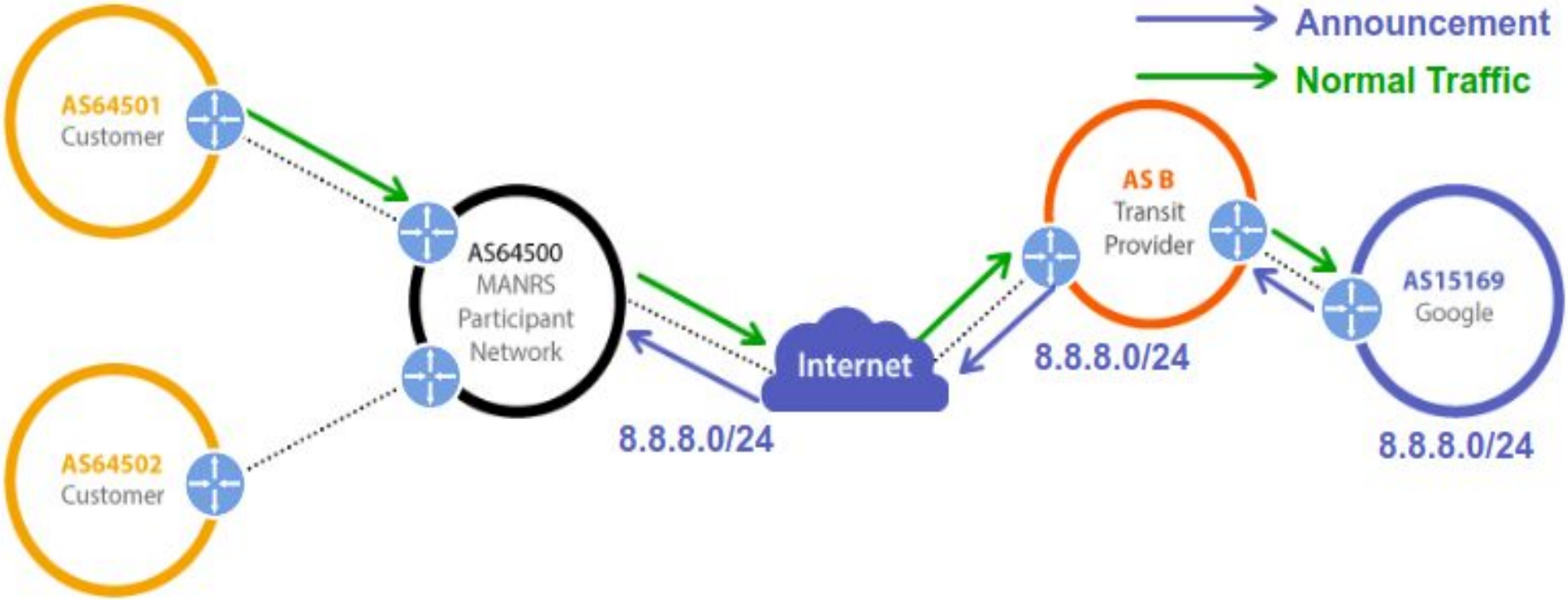
	DNS		SNMP		NTP		SSDP	
2017	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
Janeiro	2.133	87.953	–	–	981	97.423	–	–
Fevereiro	2.066	67.159	1.681	573.373	–	–	805	37.459
Março	–	–	1.805	604.805	915	104.665	–	–
Abril	2.191	72.124	–	–	861	92.120	812	27.233
Maio	2.280	69.957	1.869	573.400	–	–	839	40.814
Junho	2.183	64.179	1.948	596.348	860	91.257	812	33.805
Julho	–	–	1.963	551.953	841	107.097	–	–
Agosto	2.347	72.677	2.018	554.457	872	108.168	891	27.209
Setembro	2.307	62.283	1.791	406.015	800	89.603	–	–
Outubro	2.328	67.066	1.886	343.674	845	108.605	902	32.056
Novembro	2.279	61.281	–	–	–	–	863	26.999
Dezembro	2.436	62.758	2.001	460.519	–	–	845	27.828
2018	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
Janeiro	2.412	61.875	2.130	479.247	823	97.075	888	25.982
Fevereiro	2.438	72.185	2.324	559.784	849	93.801	778	20.210
Março	2.476	63.811	2.278	515.345	844	84.483	544	11.431

Legenda: "–" significa que não foi realizada notificação desta categoria no referido mês

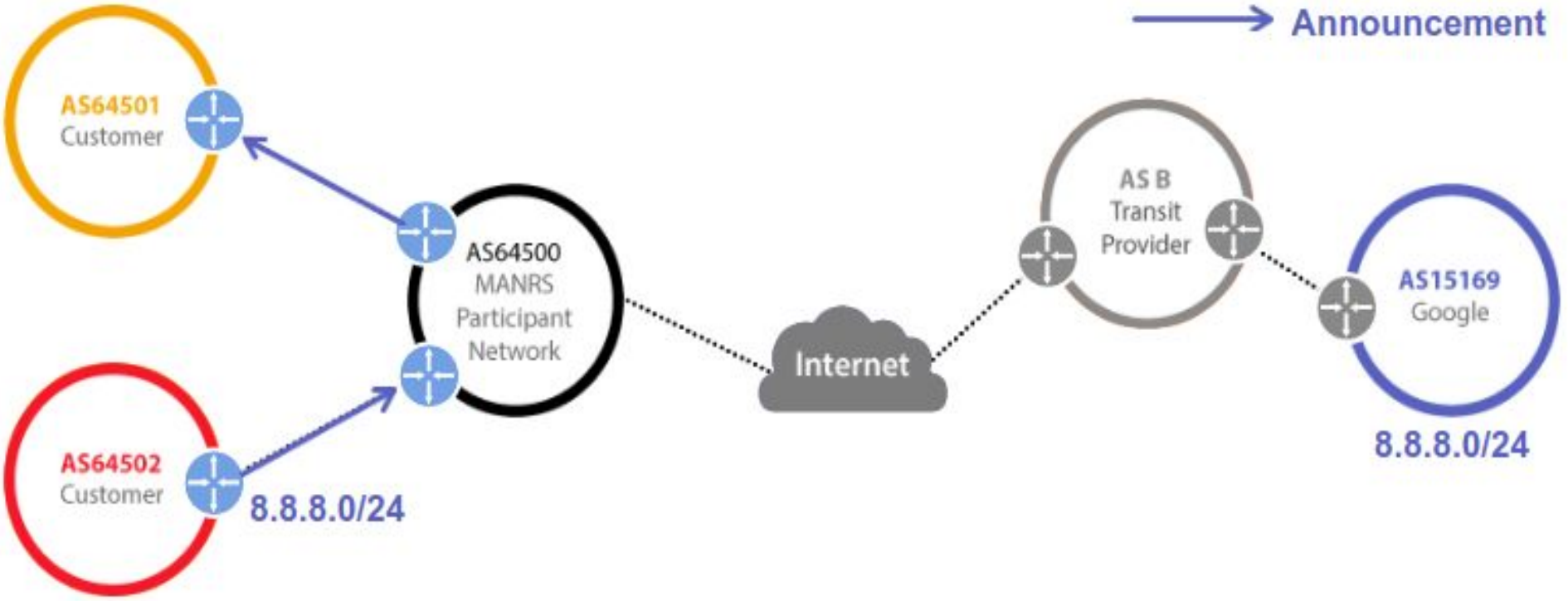
O que é MANRS?

- Mutually Agreed Norms for Routing Security
- É uma iniciativa global
- Apoio da ISOC
- Consiste em 4 coisas básicas
  - Filtros
  - Anti-Spoofing
  - Coordenação
  - Validação Global

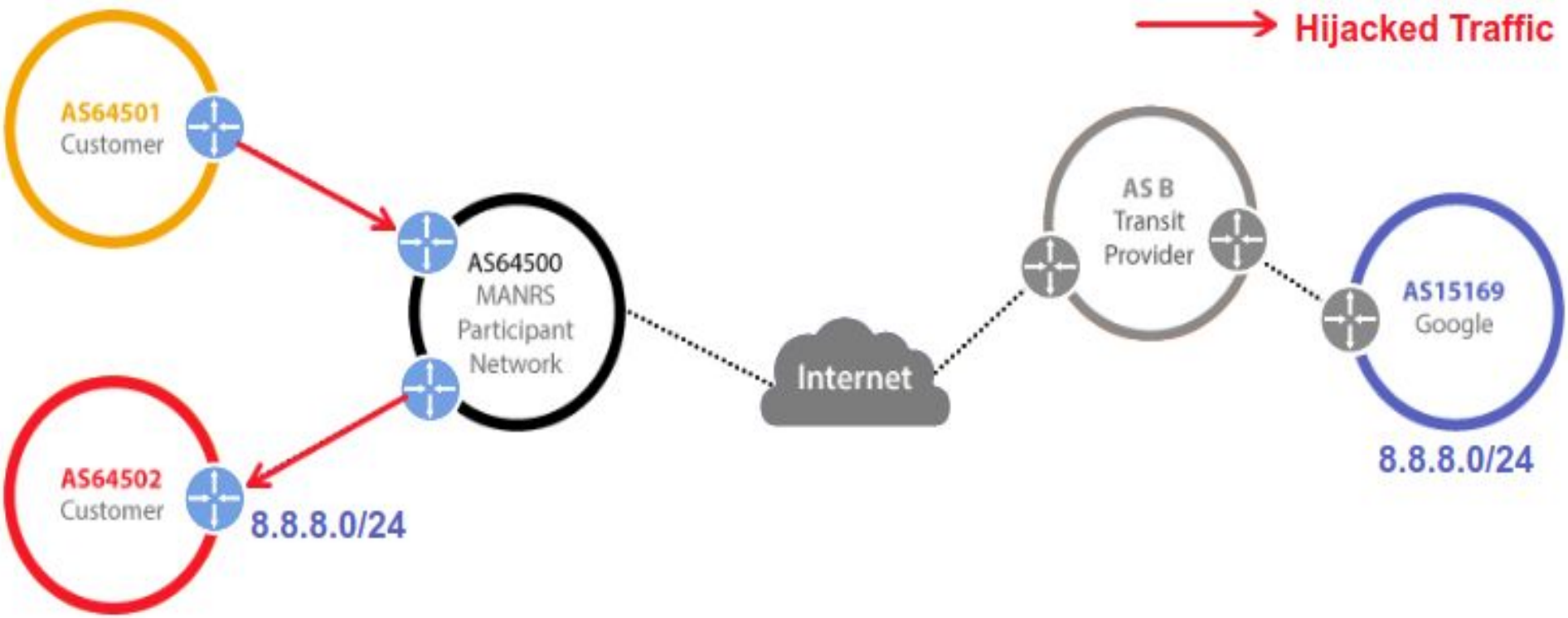
Porque utilizar filtros? Roubo de prefixos



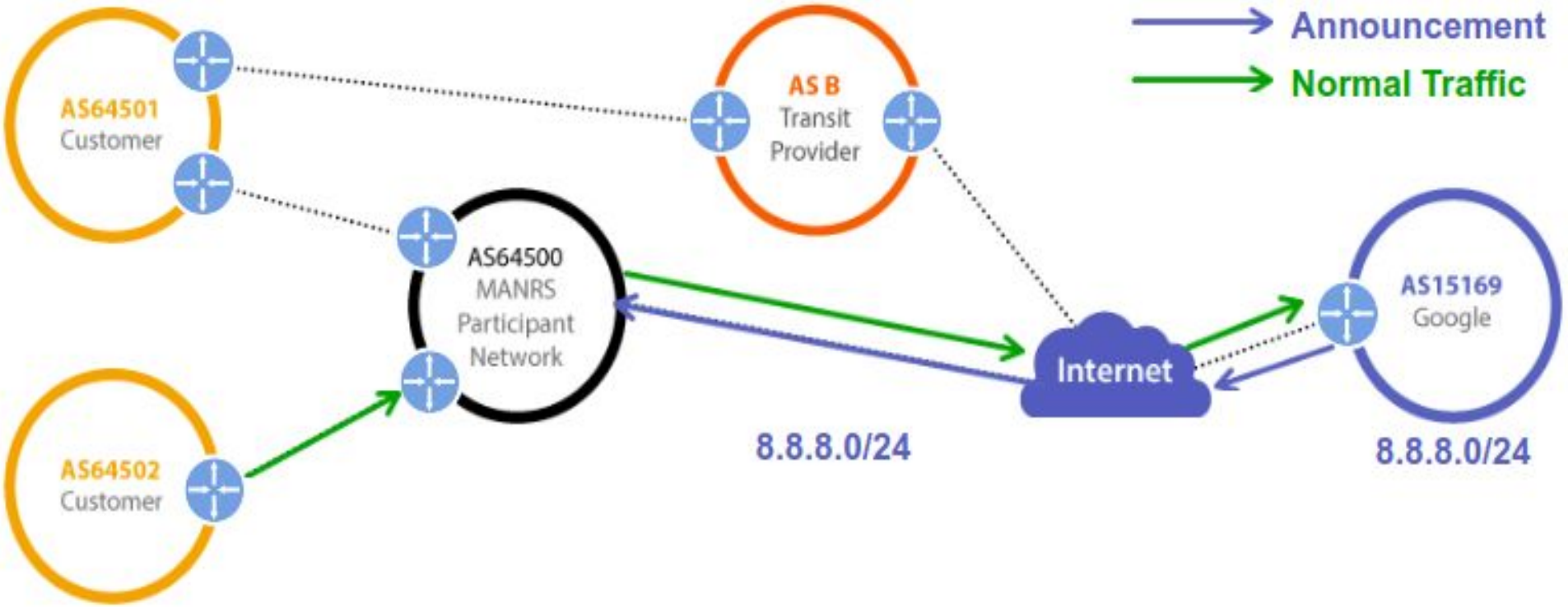
Porque utilizar filtros? Roubo de prefixos



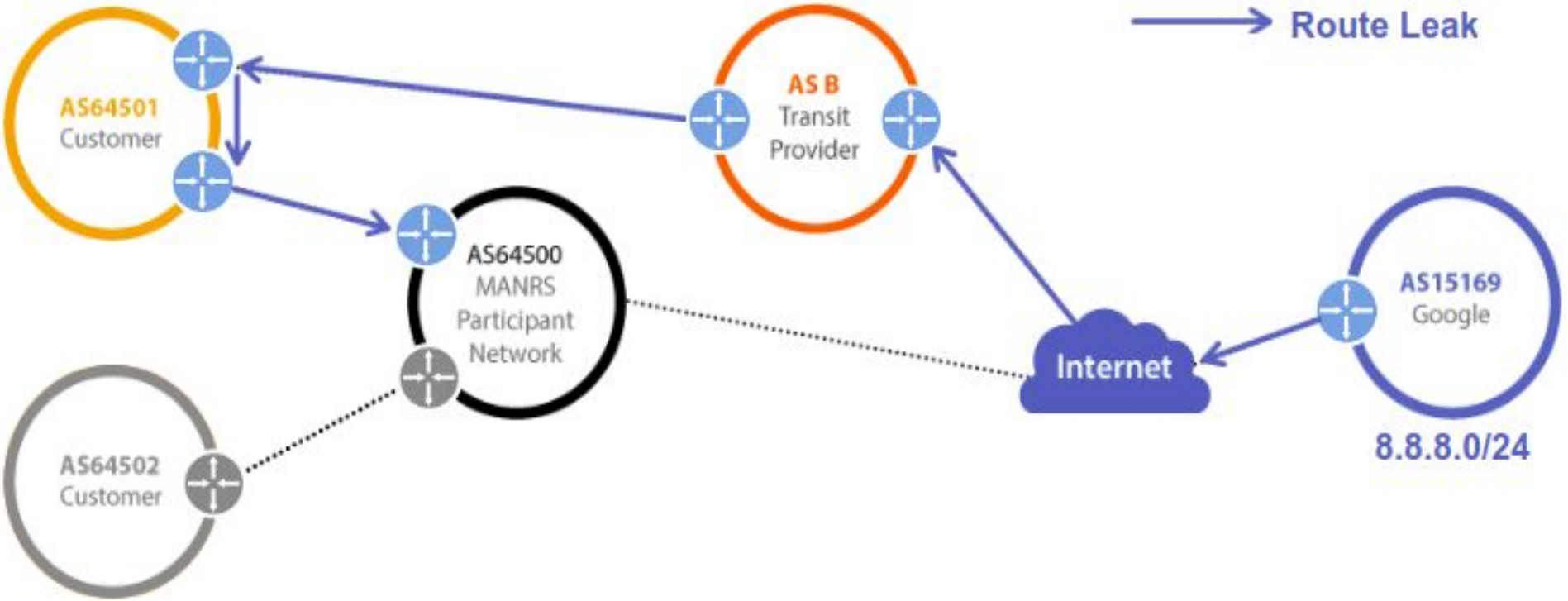
Porque utilizar filtros? Roubo de prefixos



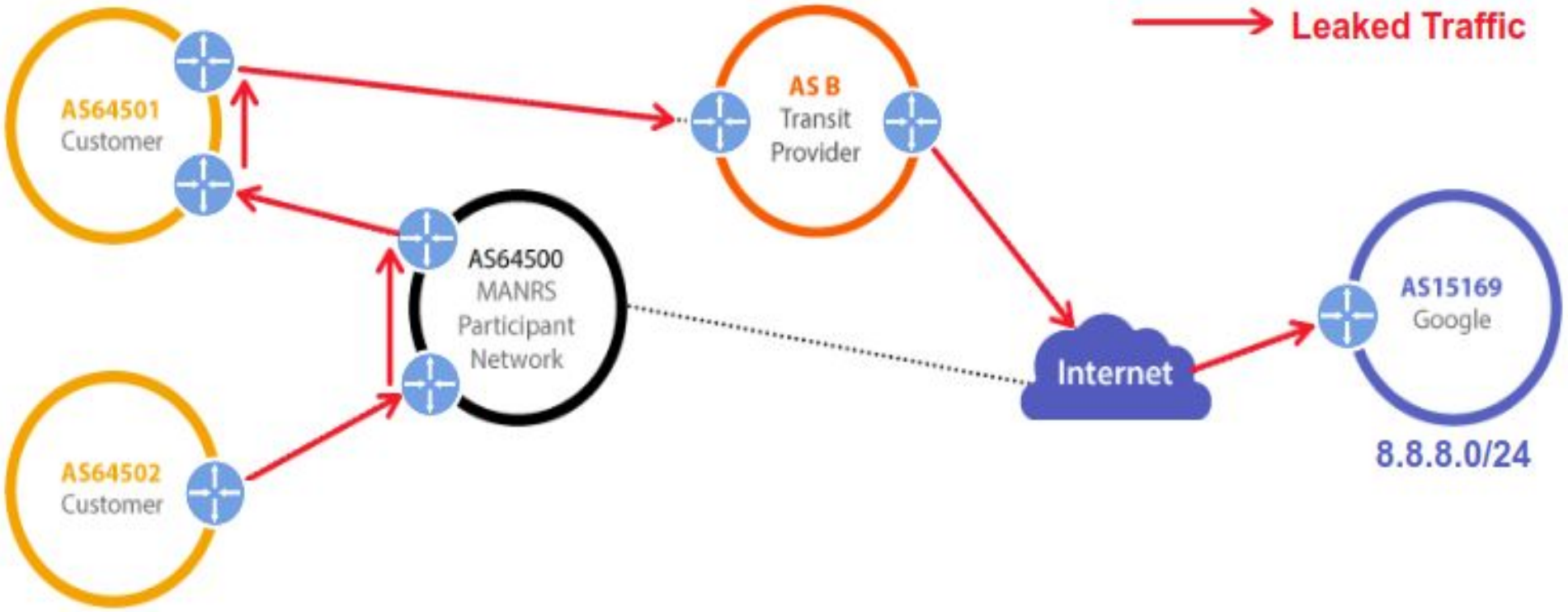
Porque utilizar filtros? Vazamento de rotas



Porque utilizar filtros? Vazamento de rotas



Porque utilizar filtros? Vazamento de rotas



Filtros

- Garanta que os seus anúncios BGP estejam corretos.
  - Publique suas informações de roteamento.

- Garanta que os anúncios BGP dos seus clientes estejam corretos.
  - Exija que eles publiquem suas informações de roteamento.
  - Aplique filtros de acordo com as informações publicadas por eles.

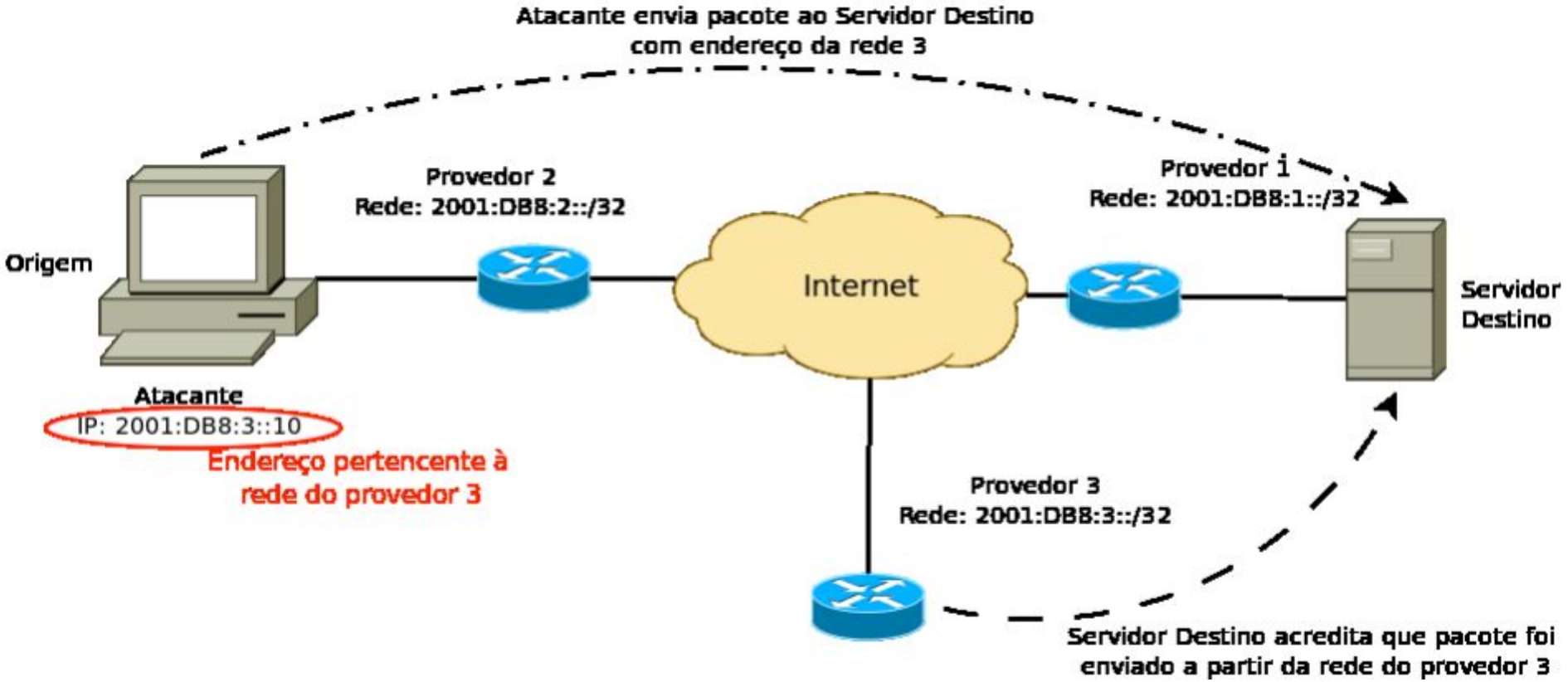
- Utilize WHOIS, IRR, RPKI e site da instituição para publicar e encontrar dados de roteamento.

Filtros

- Filtro de prefixos
  - Entrada: Só receba os prefixos que foram acordados previamente com o seu cliente.
  - Entrada: Em casos de peering (como ATM do PTT) aplique filtro de bogons.
  - Saída: Só envie os seus prefixos e de seus downstream.
- Filtro de AS-Path
  - Só receba as rotas que o seu cliente possui e dos downstreams dele.

- Evita problemas de prefix hijacking e route leaks.

Ataque usando spoofing



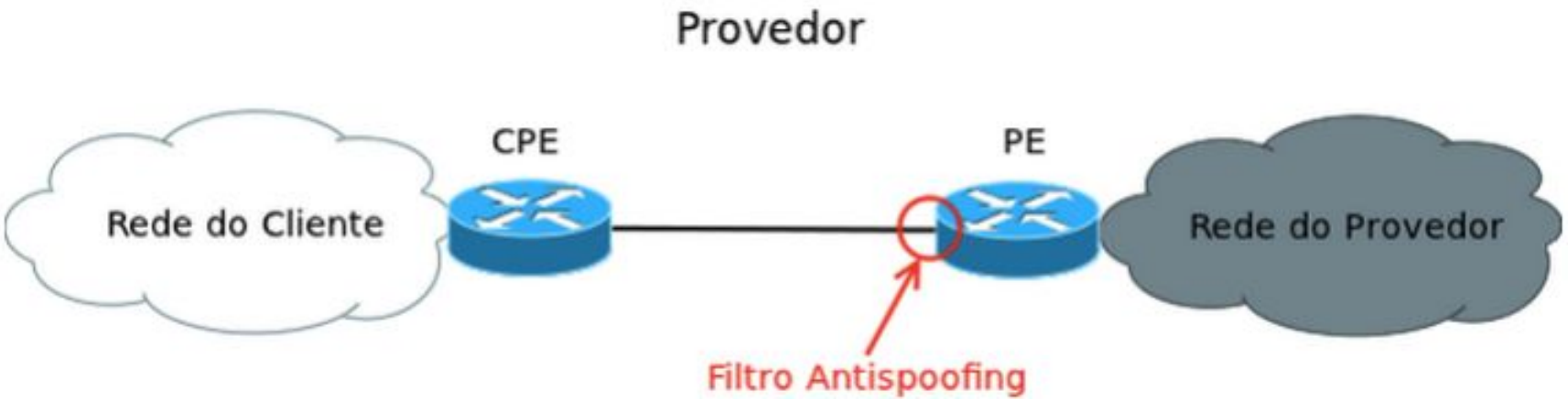
Soluções propostas

- **Ingress Access Lists**
  - **Access Control List - ACLs**

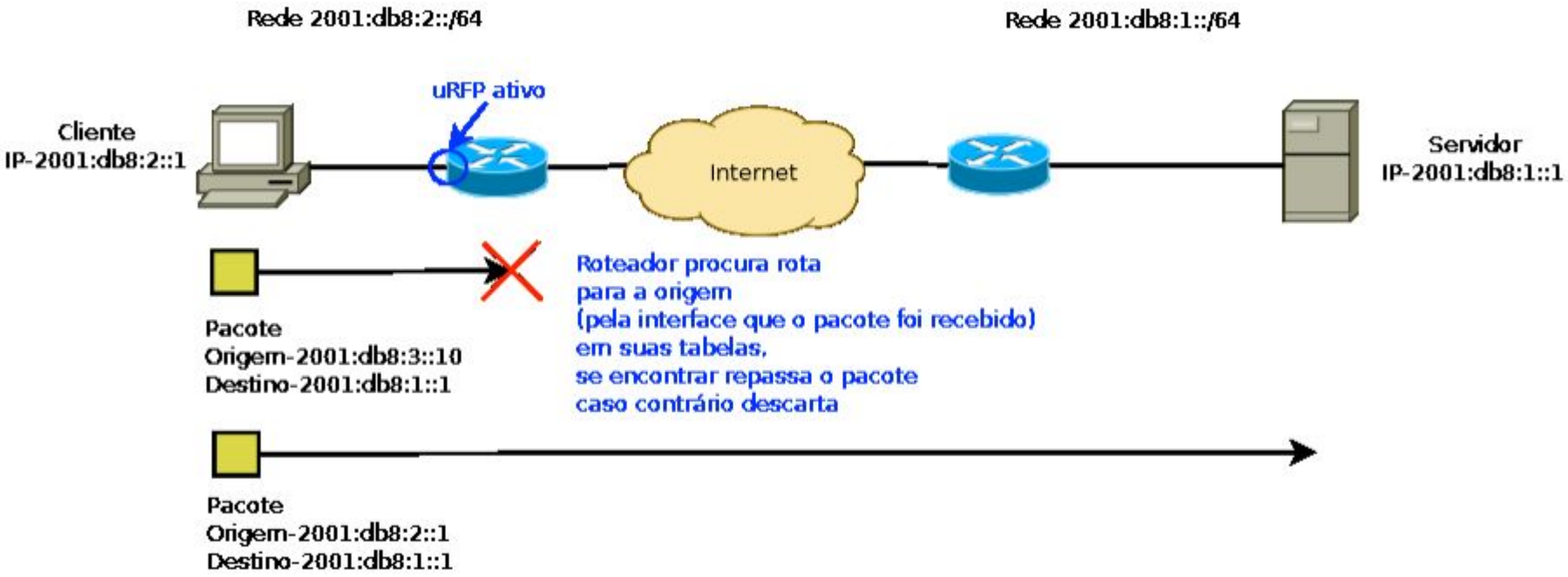
- **Unicast Reverse Path Forward (uRPF)**
  - **Strict Mode**
  - **Loose Mode**
  - **Feasible Path**
  - **VRF Mode**

- **Source Address Validation Improvement (SAVI)**

Filtro antispoofing



uRPF


Rede 2001:db8:2::/64
Rede 2001:db8:1::/64
uRFP ativo
Cliente
IP-2001:db8:2::1
Internet
Servidor
IP-2001:db8:1::1
Roteador procura rota
para a origem
(pela interface que o pacote foi recebido)
em suas tabelas,
se encontrar repassa o pacote
caso contrário descarta
Pacote
Origem-2001:db8:3::10
Destino-2001:db8:1::1
Pacote
Origem-2001:db8:2::1
Destino-2001:db8:1::1

Coordenação

- Ataques podem ser mitigados se tiver uma ação global e cooperativa
- Mantenha atualizada suas informações de contato
  - Administrativo
  - Técnico (NOC)
  - Abuso
- Publique sua informações
  - RIRs - Whois
  - IRRs
  - PeeringDB
  - Website

Validação Global

- Publique suas informações de Roteamento
  - Seu sistema autônomo
  - Suas políticas de roteamento
  - As rotas dos seus clientes

- Peça que seus clientes e seus upstreams também publique suas informações de roteamento

- Utilize ferramentas
  - RPKI
  - IRR

Projeto MANRS

- Site do Projeto
  - https://www.manrs.org/
  - https://bcp.nic.br/manrs (Em Português)

- Você pode assinar o projeto.
- Solicite que seus clientes e upstreams também assinem o projeto
  - https://www.manrs.org/participants/

- Faça o tutorial
  - https://www.manrs.org/tutorials/

Dúvidas?

Obrigado !!!

nic.br cgi.br

www.nic.br | www.cgi.br