

Formação para Sistemas Autônomos

Anti Spoofing (BCP 38)

Licença de uso do material

Esta apresentação está disponível sob a licença



Creative Commons

Atribuição – Não a Obras Derivadas (by-nd)

<http://creativecommons.org/licenses/by-nd/3.0/br/legalcode>

Você pode:

- **Compartilhar** — copiar, distribuir e transmitir a obra.
- **Fazer uso comercial da obra.**
- Sob as seguintes condições:

Atribuição — Ao distribuir essa apresentação, você deve deixar claro que ela faz parte do Curso de Formação para Sistemas Autônomos do CEPTRo.br/NIC.br, e que os originais podem ser obtidos em <http://ceptro.br>. Você deve fazer isso sem sugerir que nós damos algum aval à sua instituição, empresa, site ou curso.

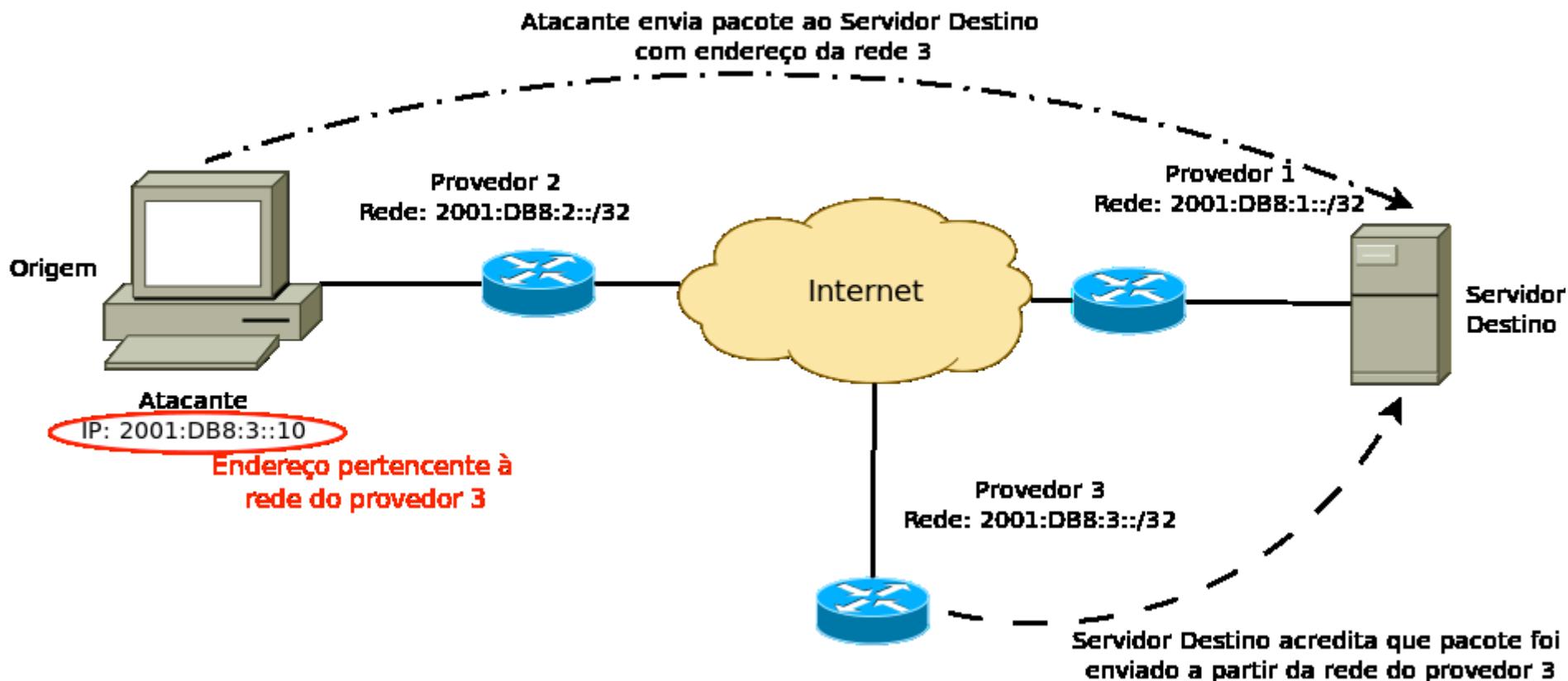
Vedada a criação de obras derivadas — Você não pode modificar essa apresentação, nem criar apresentações ou outras obras baseadas nela..

Se tiver dúvidas, ou quiser obter permissão para utilizar o material de outra forma, entre em contato pelo e-mail: info@nic.br.

O que é spoofing?

- Pacotes IP com endereços de origem incorretos podem ser gerados e utilizados
 - Endereços reservados ou de redes de terceiros
- Isso é spoofing, ou falsificação de pacotes
- O spoofing pode ser usado em ataques de negação de serviço e é um problema sério na Internet
- Qualquer rede na Internet pode ser vítima desse tipo de ataque

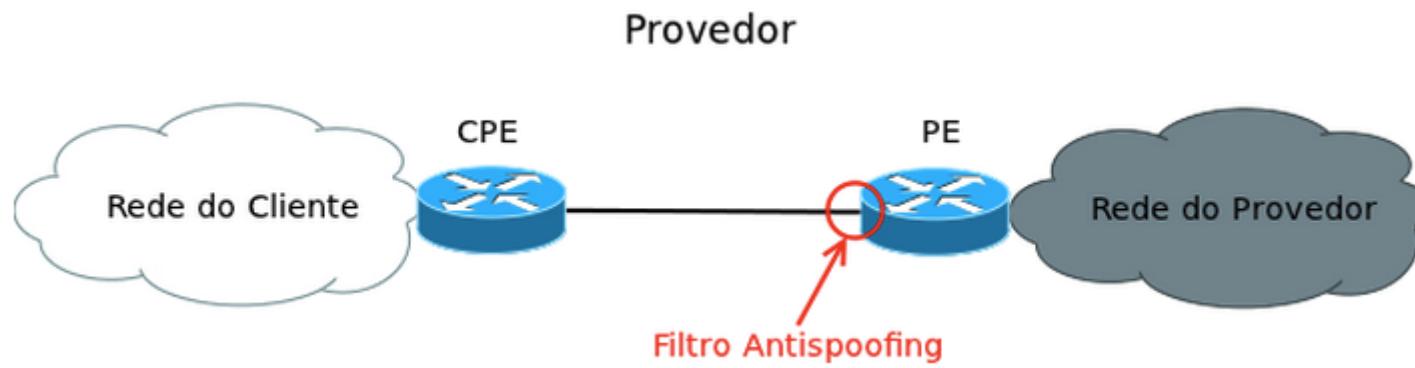
Ataque usando spoofing



Solução

- A BCP 38 (RFC 2827) recomenda que se filtrem pacotes na interface de entrada da rede do provedor, de forma a permitir somente aqueles cujo endereço de origem seja parte da rede conectada àquela interface.
- Os filtros devem ser aplicados também nos servidores de acesso remoto ou agregadores.
- A BCP 84 (RFC 3704) recomenda o uso do RPF (Reverse Path Forwarding).

Filtro antispoofing



uRPF



Exemplos de filtros

- <http://bcn.nic.br>
- Cisco e Juniper: uRPF
- O MikroTik RouterOS só passou a suportar uRPF a partir da sua versão 6.0rc3 (11/2012)

Dúvidas?



br