Recomendações e boas práticas

O anúncio dos prefixos IPv6, assim como dos blocos IPv4, deve ser feito levando em consideração importantes aspectos de segurança. É altamente recomendável prestar atenção aos aspectos de segurança na implementação das sessões eBGP4+. Situações decorrentes de erros de configuração, ataques de tipo *spoofing* e DDOS em roteadores de borda, não validação RPKI ou TIR de anúncio de prefixos de clientes, entre outros, comprometem a segurança do roteamento da Internet, tanto para IPv4 quanto para IPv6. Portanto, é importante que ações sejam projetadas e implementadas para mitigar os riscos e aumentar a segurança.

Além disso, é importante entender que o anúncio dos prefixos de uma operadora ISP faz parte do Sistema Global de Roteamento da Internet. Iniciativas novas como a do projeto **MANRS 'https://www.manrs.org/'**, em sua seção sobre MANRS para Operadores de Rede **'https://www.manrs.org/isps/'** propõem ações muito concretas como boas práticas a seguir na implementação do Roteamento da Internet pelas operadoras ISP. Da mesma forma, o Grupo de Networking da IETF apresenta em seus documentos BCP38 (https://tools.ietf.org/html/bcp38) e BCP84 (https://tools.ietf.org/html/bcp84), boas práticas para controle seguro dos prefixos anunciados e recebidos em sessões eBGP.
A seguir, o resumo das boas práticas mais destacadas dessas recomendações e documentos:

- Anunciar aos Upstream Providers SOMENTE o ASN e os prefixos IPv6 da operadora e dos seus clientes. Se a operadora ISP vai anunciar os prefixos IPv6 dos clientes finais, deve fazer as validações de autenticação correspondentes.
- Manter as informações de roteamento atualizadas no RIR/NIR correspondente e no PeeringDB se fizer Peering.
- Documentar e manter as informações de roteamento atualizadas perante o RIR correspondente e perante o IRR, se estiver associado. Isto, em nível do RPKI e IRR.
- Implementar os mecanismos necessários para uma proteção de rede eficaz e mitigar ataques DDOS, Spoofing, entre outros. Da mesma forma, prevenir o tráfego "spoofing" para a Internet.
- Implementar uma arquitetura adequada e um bom design de filtros BGP para controlar os prefixos que são anunciados e recebidos. Especificamente, evitar o anúncio de prefixos ilegítimos, não autorizados e errôneos.
- Uso de filtragem Bogons. Existem até mesmo provedores públicos da Internet que oferecem sessões eBGP Multihop para o anúncio de rotas Bogons e Full Bogons, a fim de suprimir o tráfego de Internet dessas rotas.
- Para o design dos filtros: filosofia de design 'denegar tudo e aceitar SOMENTE o que é conveniente'.
- Não anunciar ou aceitar rotas IPv6 com comprimento de prefixo maior que /48.
- Não anunciar o Default Gateway aos Upstream Providers.
- Não aceitar dos Upstream Providers os prefixos IPv6 da operadora ISP que estão sendo publicados.
- Usar como router-id endereços IPv4 configurados em interfaces de redes estáveis e sem possibilidade de flapping. Por exemplo, interfaces loopback ou interfaces bridge.

- Desenhar a configuração dos filtros BGP que sejam escalonáveis e que o sistema não seja afetado pelas mudanças necessárias.
- Usar a autenticação MD5 na configuração de sessões eBGP4+ para maior segurança.
- Configurar as sessões eBGP4+ com TTL 255 para evitar Spoofing e DDOS provenientes de além de um salto.
- Implementar técnicas de Filtragem e Limitação de Tráfego TCP/179 para denegar tudo e aceitar SOMENTE o tráfego proveniente dos Peers eBGP4+ conectados diretamente, conhecendo seus IPv6 de conexão.