Núcleo de Informação e Coordenação do Ponto BR

versão 2018-05-07-14-11

Solicitação de Comentários à Comunidade Técnica da Internet **Programa por uma Internet Segura** Ações no IX.br

Introdução

O IX.br está presente em 30 localidades no Brasil, por meio da instalação e operação de Pontos de Troca de Tráfego Internet (PTTs), sendo parte integrante da infraestrutura de rede da Internet do Brasil, onde Sistemas Autônomos (ASs) podem trocar tráfego nas regiões metropolitanas próximas.

Dois tipos de serviços são oferecidos aos participantes da troca de tráfego: (i) **o Acordo de Troca de Tráfego Multilateral** (ATM), chamado em inglês de *Multilateral Peering Agreement* (MPA) e (ii) a **Troca de Tráfego Bilateral**, em inglês *Bilateral Peering Agreement*. Os participantes do ATM trocam tráfego entre si: como regra geral, cada AS troca tráfego com todos os demais. Já na Troca de Tráfego Bilateral apenas dois ASs participam, utilizando-se ou não de um domínio de camada 2 exclusivo (uma VLAN bilateral).

O Acordo de Troca de Tráfego Multilateral (ATM), na prática, funciona com uma VLAN compartilhada para a troca de tráfego IPv4 (ATMv4) e outra para troca de tráfego IPv6 (ATMv6). Cada PTT possui dois ou mais *route servers,* que também são utilizados no Acordo de Troca de Tráfego Multilateral (ATM) para centralizar o recebimento de anúncios de rotas de todos os participantes da troca de tráfego, permitindo que, com uma única sessão BGP, a tabela de rotas da localidade seja carregada e mantida. O estabelecimento de sessões BGP com os *route servers* é condição necessária para participar do ATM. A maior parte dos participantes de um PTT participa da troca de tráfego multilateral, mas nem todos. Mesmo participantes que não estão no ATM podem estar presentes nas VLANs do ATMv4 ou ATMv6, para fins de monitoramento, ou outros fins.

Existem casos em que o participante está presente na VLAN do ATMv4 ou ATMv6 e não fecha sessão BGP com o *route server*, mas fecha sessões BGP diretamente com o roteador de outros participantes com os quais deseja trocar tráfego. Ou seja, acordos bilaterais de troca de tráfego podem se utilizar tanto da VLAN de uso comum (ATMv4 ou ATMv6), como de VLANs específicas (VLANs bilaterias)

Desta forma, neste cenário, temos em cada PTT do IX.br:

- um **ambiente privado**, formado pelos Acordos Bilaterais com troca direta de tráfego através VLANs, sejam VLANs bilaterais ou as VLANs do ATMv4 e/ou ATMv6, e
- um **ambiente compartilhado** formado pelos participantes presentes nas VLANs do ATMv4 e/ou ATMv6 e com sessões BGP com os route servers.

Dentro do **Programa por uma Internet Segura** que o NIC.br está desenvolvendo com a comunidade da Internet, **esta Solicitação de Comentários à Comunidade Técnica da Internet diz respeito a ações para aumentar a segurança dos *route servers***, onde a ocorrência de problemas em relação à tabela de rotas compartilhada pode afetar seriamente os ASs que participam ou não dos PTTs. **Trata-se de ações sobre o ambiente compartilhado.** Ocorrências no **ambiente privado não estão no escopo de atuação do NIC.br e do IX.br,** mas todas as recomendações feitas devem ser consideradas e aplicadas pelos gestores dos ASs envolvidos em relações privadas dentro do IX.br.

A segurança da Internet depende fundamentalmente da participação de todos os ASNs. A segurança do ambiente de um Ponto de Troca de Tráfego Internet - PTT (*Internet Exchange Point* - IX) reflete o cuidado que cada rede participante adota internamente. Se todas as redes adotarem as melhores práticas recomendadas na configuração de suas redes, com certeza teríamos um ambiente mais saudável no PTT. Configurar uma rede para evitar a propagação de problemas, ou seja, controlar o que sai de uma rede, é muito mais simples e econômico do que proteger a entrada da rede contra tudo o que existe no exterior. Se todos protegerem as saídas de suas redes, não haverá problemas na entrada do PTT. Esta é a filosofia do MANRS (Mutually Agreed Norms for Routing Security - https://www.manrs.org/), que é uma iniciativa global, apoiada pela Internet Society, que fornece recomendações cruciais para eliminar ameaças causadas pelos problemas de roteamento mais comuns e tem como objetivos:

- Aumentar a conscientização e incentivar ações, com o compromisso dos apoiadores.
- Promover a cultura de responsabilidade coletiva para a resiliência e segurança do sistema de roteamento global da Internet.
- Demonstrar a capacidade do setor para abordar as questões de resiliência e segurança com espírito de responsabilidade coletiva.
- Fornecer uma estrutura para que os provedores de serviços de acesso à Internet (ISP) compreendam melhor e ajudem a solucionar os problemas relacionados à resiliência e segurança do roteamento da Internet.

O que é muito preocupante é o fato de que **nos PTTs não há como atuar em todos os possíveis problemas causados por redes configuradas sem as devidas proteções, por restrições técnicas nos equipamentos de rede**. Contudo, **podemos atuar na segurança dos *route servers***, com medidas que diminuam a possibilidade da ocorrência de sequestro de prefixos (*prefix hijack*) ou vazamento de rotas (*route leaks*) que têm causado tanto prejuízo e preocupação aos usuários da Internet brasileira.

O objetivo desta solicitação de comentários é ouvir da comunidade sua opinião sobre ações já em uso e outras sugeridas, além de abrir um canal para a recepção de mais sugestões para aumentar a segurança dentro do ambiente dos PTTs do IX.br.

Aumento da Segurança dos Route Servers

Para aumentar a confiabilidade da tabela local de rotas do ATM de um PTT, validações devem ser executadas na entrada do route server para mitigar eventuais erros, ações maliciosas ou imperícia na configuração dos roteadores dos participantes da troca de tráfego.

Apresentamos a seguir uma série de medidas executadas ou a serem executadas a nível dos route servers, onde classificamos cada uma como EM USO e de possibilidade de implementação a CURTO (45 dias), MÉDIO (120 dias) e LONGO (12 a 18 meses) prazos. O tempo para implementação não necessariamente está ligado a questões técnicas, mas também para que a tecnologia atinja maturidade suficiente para ser considerada relevante no processo.

Existe um certo grau de redundância no resultado de cada uma das ações, mas o objetivo final é alcançar uma maior abrangência e eficiência.

- **Ação 1 (filtro de prefixos bogons):**

  Rejeição de anúncios com prefixos indevidos (Bogon Prefixes): os anúncios recebidos que contenham blocos de endereços utilizando espaço de endereçamento reservado são descartados.

  Anúncios com os seguintes prefixos IPv4 são rejeitados:

```
0.0.0.0/8 prefixlen >= 8          # 'this' network [RFC1122]
10.0.0.0/8 prefixlen >= 8         # private space [RFC1918]
100.64.0.0/10 prefixlen >= 10     # CGN Shared [RFC6598]
127.0.0.0/8 prefixlen >= 8        # localhost [RFC1122]
169.254.0.0/16 prefixlen >= 16    # link local [RFC3927]
172.16.0.0/12 prefixlen >= 12     # private space [RFC1918]
192.0.2.0/24 prefixlen >= 24      # TEST-NET-1 [RFC5737]
192.168.0.0/16 prefixlen >= 16    # private space [RFC1918]
198.18.0.0/15 prefixlen >= 15     # benchmarking [RFC2544]
198.51.100.0/24 prefixlen >= 24   # TEST-NET-2 [RFC5737]
203.0.113.0/24 prefixlen >= 24    # TEST-NET-3 [RFC5737]
224.0.0.0/4 prefixlen >= 4        # multicast
240.0.0.0/4 prefixlen >= 4        # reserved for future use
```

  Anúncios com os seguintes prefixos IPv6 são rejeitados:

```
::/8 prefixlen >= 8
0100::/64 prefixlen >= 64         # Discard-Only [RFC6666]
2001:2::/48 prefixlen >= 48       # BMWG [RFC5180]
2001:10::/28 prefixlen >= 28      # ORCHID [RFC4843]
2001:db8::/32 prefixlen >= 32     # docu range [RFC3849]
3ffe::/16 prefixlen >= 16         # old 6bone
fc00::/7 prefixlen >= 7           # unique local unicast
```

```
fe80::/10 prefixlen >= 10          # link local unicast
fec0::/10 prefixlen >= 10          # old site local unicast
ff00::/8 prefixlen >= 8            # multicast
```

Tempo para implementação/status: EM USO.

- **Ação 2 (filtro dos prefixos do IX.br):**

Rejeição de anúncios que contenham o espaço de endereçamento utilizados para o IX.br para endereçar os roteadores que participam da troca de tráfego da localidade. Mesmo utilizando blocos de endereços válidos, a rede do IX.br NÃO DEVE ser anunciada. Endereços válidos são utilizados para facilitar o trabalho de investigação de problemas de conectividade e/ou roteamento (*troubleshooting*).

Tempo para implementação/status: EM USO.

- **Ação 3 (filtro de ASNs bogons):**

Rejeição de anúncios que contenham ASNs (número de identificação dos Sistemas Autônomos) reservados (Bogon ASNs) em qualquer parte do AS-PATH.

Anúncios com os seguintes ASNs serão rejeitados:

0 - RFC 7607
23456 - RFC 4893 AS_TRANS
64496 a 64511 - RFC 5398 and documentation/example ASNs
64512 a 65534 - RFC 6996 Private ASNs
65535 - RFC 6996 Last 16 bit ASN
65536 a 65551 - RFC 5398 and documentation/example ASNs
65552 a 131071 - IANA reserved ASNs
4200000000 a 4294967294 - RFC 6996 Private ASNs
4294967295 - RFC 6996 Last 32 bit ASN

Tempo para implementação/status: CURTO.

- **Ação 4: (filtro de Tier-1s no AS PATH):**

Rejeição de anúncios que contenham no AS-PATH, após o ASN do participante o ASN de redes conhecidas como tendo trânsito livre, tipicamente os principais Tier-1:

174 - Cogent
209 - Centurylink
701 - Verizon
702 - Verizon
1239 - Sprint
1299 - Telia
2914 - NTT

3257 - GTT Communications
3320 - Deutsche Telekom
3356 - Level 3
3549 - Level 3
3561 - Centurylink
4134 - China Telecom
5511 - Orange
6453 - Tata Communications
6461 - Zayo
6762 - Telecom Italia Sparkle
7018 - AT&T
12956 - TIWS

A presença destes ASNs no AS-PATH é um indicativo de má configuração em roteador de participante da troca de tráfego. Ninguém fornece trânsito a um Tier-1, por definição. Os Tier-1 fazem peering entre si. A presença do ASN de um Tier-1 no AS-PATH indica que o participante, ou um cliente de trânsito do participante está 'fornecendo trânsito' ao Tier-1, o que indica provavelmente um erro de configuração.

Obs: em 28/03/2018 no IX.br SP foram encontrados 90 anúncios contendo os ASNs listados acima, com um tráfego diário de 36.8 Tb e uma média de 3.5 Gbps.

Tempo para implementação/status: CURTO.

- **Ação 5 (proteção aos ASs stubs):**

Essa ação visa oferecer proteção aos ASs stubs registrados no Brasil.

ASNs conectados ao IX.br podem ser classificados em duas categorias: stub ou trânsito. Um ASN stub é aquele que está conectado diretamente ao IX.br, anunciando apenas os seus próprios prefixos, não existindo outro ASN no AS-PATH. Já um ASN trânsito é aquele que anuncia prefixos de outros ASNs, além dos seus, com AS-PATH podendo conter múltiplos ASNs.

Durante a etapa de quarentena do processo de ativação do participante no IX.br, serão analisados os anúncios recebidos e apresentada a classificação do ASN como stub ou trânsito. A classificação inicial poderá ser alterada a qualquer momento através do portal do participante do IX.br.

Quando da implantação do processo, para os participantes já conectados faremos a análise e a classificação baseada na tabela de rotas em vigor.

Para os ASNs stubs registrados no Brasil, ou seja, através do Registro.br, será aplicado um filtro que aceitará apenas os blocos de endereço IP alocados para o ASN, limitados a prefixos mais específicos de /24 em IPv4 e /48 em IPv6. Este filtro será atualizado uma vez

por dia, onde serão aplicadas eventuais mudanças nos dados referentes ao ASN, seja por configuração no portal ou em relação às informações encontradas no Registro.br.

O ASN stub que eventualmente passe a dar trânsito a outros ASNs, deverá especificar no portal do participante do IX.br que sua classificação deverá mudar para trânsito.

Tempo para implementação/status: MÉDIO.

- **Ação 6: (validação via bases de dados externas)**

Essa ação promove a utilização de bases de dados externas para a validação de anúncios.

Conforme já anunciado anteriormente no documento em que tratamos da "Proposta para mudança nos servidores de rotas e nas políticas de tratamento de communities BGP no IX.br", os anúncios recebidos pelos route servers serão marcados como Válidos, Inválidos ou Desconhecidos de acordo com pesquisas realizadas em 3 tipos de serviços/bases de dados: RDAP, IRR e RPKI.

RDAP (Registration Data Access Protocol): o serviço RDAP pode ser encarado como uma API para acesso a uma base de dados Whois, como a do Registro.br, com a qual se poderá validar os prefixos atribuídos a um determinado ASN. A atualização desta base de dados é feita pelo Registro.br no processo de atribuição dos recursos de numeração, não sendo necessário qualquer tipo de cadastro por parte do ASN. Por outro lado, é fundamental que delegações ou transferência de blocos entre ASNs sejam devidamente informadas e registradas no Registro.br, sem o que poderá haver rejeição de anúncios.
Duas formas de utilização poderão ser verificadas para a implementação dos filtros no IX.br:

- Consulta online: ao receber os anúncios, os route servers consultam a base de dados do Registro.br ou de outros RIRs na tentativa de validar o prefixo recebido de um determinado ASN.
- Consulta a uma base de dados própria ou um cache atualizados uma vez ao dia, contendo os prefixos de todos os ASNs presentes no IX.br.

Tempo para implementação: CURTO.

IRR (Internet Routing Registers): Os IRRs são bases de dados que armazenam políticas de roteamento descritas em uma linguagem denominada Routing Policy Specification Language (RPSL). Estas bases de dados são distribuídas e operadas por diversas organizações como RIRs (Regional Internet Registry), empresas de telecom, etc. Existem serviços que tem cópias (espelhos) das diversas bases existentes, de modo a oferecer a visão mais completa sobre as bases IRR existentes. Para aprimorar as informações obtidas sobre a política de roteamento de um ASN, é fundamental que todo ASN informe sua política de roteamento em uma ou mais das bases existentes, como o RADB, ARIN, APNIC, RIPE, TC ou outras, e se o fizer, informar qual usuário (mnt-by) e base foram

utilizadas. Quanto mais precisa for a informação utilizada na consulta, menor será a possibilidade da obtenção de resultados incorretos que possam vir a prejudicar o AS.

O uso deste tipo de base de dados implicará no seguinte processo diário no IX.br:

- Obter as informações dos ASs que informaram base/usuário no portal do participante. (Base Prioritária)
- Obtenção de diversas bases de dados IRR que serão sintetizadas em um cache a ser consultado pelos route servers. Sempre que houver a sinalização que uma base foi alterada, o processo de atualização do cache será iniciado.
- Uma vez ao dia a configuração dos filtros a serem aplicados nos route servers será atualizada (Prefix-list).

Tempo para implementação/status: MÉDIO.

RPKI (Resource Public Key Infrastructure): sistema que utiliza uma infraestrutura de certificados de chaves públicas para dar segurança ao roteamento da Internet, através da geração de atestados chamados Route Origination Authorization (ROAs), que informa qual Sistema Autônomo (AS) está autorizado a originar determinados prefixos, bem como o tamanho máximo do prefixo que o AS está autorizado a anunciar.

Este é um serviço ainda com pouca adesão dos ASNs, que devem registrar seus recursos para assegurar o sistema de roteamento da Internet.

O RPKI poderá ser utilizado no processo de importação de anúncios dos route servers, que irão consultar um serviço RPKI para validar a origem dos anúncios recebidos.

Tempo para implementação: LONGO.

Filtragem pelo Route Server:

Após a inclusão das Communities indicando o resultado da pesquisa em cada uma das três fontes de informações acima, o prefixo passará por um processo de filtragem. Qualquer anúncio marcado em qualquer dos métodos como inválido será rejeitado. No portal do participante do IX.br será informada qual a política escolhida pelo ASN para tratar os prefixos marcados como Desconhecidos. As opções são:

- Descartar IRR desconhecido (S/N) ?
- Descartar RPKI desconhecido (S/N) ?
- Descartar RDAP desconhecido (S/N) ?

Dependendo da dificuldade em se validar informações de ASNs estrangeiros, o processo de marcação de anúncios classificando cada um como brasileiro ou estrangeiro, e para cada caso novos valores de Communities informando o resultado das pesquisas. Com isso poderemos ter mais flexibilidade na definição da política de filtragem de prefixos nos route servers.

- **Ação 7: Visibilidade do processo de filtragem de anúncios.**

  Conforme descrito anteriormente, o processo de análise dos anúncios antes da efetiva filtragem, onde pode efetivamente ocorrer o descarte, vai inserir uma série de Communities informando o resultado de cada verificação. Todos estes anúncios, inclusive os descartados, deverão ser enviados para o serviço Looking Glass Web acessível através do portal do participante do IX.br onde o ASN poderá verificar a situação dos seus anúncios.

  Tempo para implementação/status: CURTO.

- **Ação 8: Análise do AS-SET.**

  Ao declarar sua política de roteamento a um IRR utilizando a linguagem RPSL, o administrador do AS pode informar uma lista de ASNs por onde seus prefixos podem ser anunciados. Com estas informações, pode ser criada uma lista de ASNs autorizados a anunciar os prefixos no IX.br.

  Durante o processo de importação de anúncios, os route servers consultam esta lista e verificam se o ASN anunciante está autorizado pelo ASN dono do prefixo. O resultado desta verificação resultará na inclusão de uma Community no anúncio (Válido, Inválido, Desconhecido).

  No portal do participante do IX.br será possível autorizar ou não o descarte de prefixos quando o administrador do ASN não definiu a lista.

  A lista de ASNs autorizados será atualizada uma vez ao dia.

  O PeeringDB tem um campo denominado IRR Record onde pode ser informado o AS-SET.
  .

  Tempo para implementação/status: LONGO.

Cronograma de atividades da Solicitação de Comentários

1) Publicação no site do IX.br da primeira versão do documento: 04/05/18.
2) Apresentação à comunidade: no IX Fórum Regional de São Paulo, no dia 17/05/2018, e na reunião GTER 45, em 22/05/2018.
3) Recepção de comentários através da lista de e-mails da GTER: até 04/06/18.
4) Análise, preparação e publicação no site do IX.br da segunda versão do documento, com a inclusão de sugestões da comunidade: 11/06/18.
5) Recepção de comentários através da lista de e-mails da GTER: até 25/06/18.
6) Publicação da versão final do documento com as ações a serem implementadas: 02/07/18.