ANEXO IV – TERMO DE REFERÊNCIA INFOVIA NACIONAL

Especificação técnica do Trânsito IP seguro

Especificação do trânsito IP para o AS1916

A RNP aceitará a oferta de trânsito IP como parte da pontuação para equilíbrio da permuta na oferta de canais ópticos e/ou capacidade, ou ainda na oferta conjunta com colocation.

A oferta de trânsito deve possuir uma qualificação mínima, de acordo com as premissas da RNP:

No exterior:

Provedor Tier 1, reconhecido publicamente como tal, que tenha conectividade direta com todos os outros Tier 1. Deve ter relação de peering privado (PNI) com ao menos dois outros provedores Tier 1 no Brasil, preferencialmente em mais de uma localidade.

Deve demonstrar via ferramentas públicas da CAIDA e Hurricane Electric sua conectividade BGP com outras redes, sendo que para a conectividade com outros provedores Tier 1, será necessária a conexão direta com todos eles conforme exemplos abaixo:

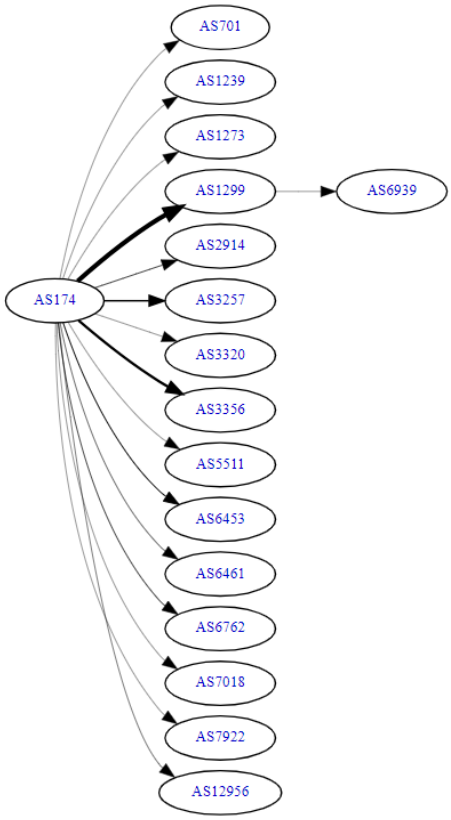

Figura 1: Gráfico de propagação de rotas da ferramenta da Hurricane Electric

AS Rank ▽	AS neighbors ▽	Organization		AS customer cone ▽	number of paths	relationship ▲	
1	3356	Level 3 Parent, LLC		53330	175011	provider	✗
2	1299	Arelion Sweden AB		41747	105417	provider	✗
10	3491	PCCW Global, Inc.		12078	32755	provider	
225	4761	PT. INDOSAT Tbk		217	4355	provider	
4	6762	Telecom Italia S.p.A.		23029	66043	peer	✓
7	3257	GTT Communications Inc.		19644	32	peer	✓
8	6453	TATA COMMUNICATIONS (A...		19537	60572	peer	✓
9	6461	Zayo Bandwidth		19034	46830	peer	
11	9002	RETN Limited		9802	26430	peer	
12	5511	Orange S.A.		8963	17536	peer	
13	4637	Telstra International Limited		7881	15358	peer	

Figura 2: AS rank da CAIDA com informação do tipo de relacionamento com o AS neighbor e destaque para a conexão com provedores Tier 1

Deve possuir plena capacidade de conexão nacional e internacional, tanto nas suas conexões de backbone/core, quanto nas interconexões com outras redes. preferencialmente possuindo conexões escaláveis em múltiplos cabos para os EUA. Deverá ser demonstrada sua conectividade do backbone mundial, tanto do ponto de vista nacional, sua interconexão para outros países a partir do Brasil e a capilaridade do backbone nos principais mercados (EUA e Europa). A conexão direta com outros países da América Latina será considerada um diferencial.

Também deve possuir e disponibilizar para uso da RNP BGP *communities* para engenharia de tráfego e anúncios IP blackhole.

Quando a permuta for por capacidade, é desejável porta 100GbE no padrão 100GBASE-LR4, 10GBASE-LR. Qualquer outro padrão proposto precisará de avaliação pela RNP. No caso dos datacenters comerciais indicados abaixo, o custo de *cross-connect* será do proponente.

Tabela 1. Especificação da conectividade para ofertar de trânsito IP à RNP

Localidade	Interface física	Commitment rate (oferta inicial)	Burst rate (90th or 95th percentile)
Equinix MI1, em Miami/FL	100G LR4 ou 40G LR4	12 Gb/s	30 Gb/s
NIC.br-JD, em São Paulo/SP Ou Equinix SP4	100G LR4 ou 40G LR4	12 Gb/s	30 Gb/s
PoP-RJ (CBPF) Ou Cirion RJ (São Cristóvão)	100G LR4 ou 40G LR4	12 Gb/s	30 Gb/s

A especificação do trânsito IP seguro, no contexto deste Termo de Referência, refere-se a oferta adicional de serviço agregado de proteção a ataques DDoS.

A oferta mínima considerada será a de recebimento de anúncios de BGP flow-spec. Contudo, será preferido aquele proponente que demonstrar que possui solução de detecção e mitigação inteligente, principalmente com workflow de mitigação automática.

Não deverá existir limitação quanto ao tamanho do ataque, seja em bps ou pps. A limitação deverá ser dada pelo *troughput* do tráfego limpo que deve respeite o *burst-rate* acordado.

O suporte a BGP flow-spec será considerado um diferencial, assim como permitir a instalação de regras estáticas de filtragem stateless (ACL, firewall-filters etc.).

O proponente também deverá informar suporte aos recursos de segurança tanto para IPv4, quanto para IPV6, informando também possíveis diferenças no tratamento dos ataques em v4/v6.

Tabela 2.Especificação do serviço agregado de detecção e/ou mitigação de ataques DDoS

Serviço de proteção contra ataques DDoS	**Informações adicionais**
Solução de mitigação inteligente (especificar a solução atualmente em uso)	Como se dará a limitação no uso do serviço. Exemplos: número de prefixos simultâneos ou tempo de uso mensal de mitigação. Se for por tempo, será cumulativo por algum período?
BGP Flow-spec	Número de prefixos simultâneos. Tamanhos de prefixos aceitos. Política dos anúncios e granularidade (SRC/DST IP, Protocol, SRC/DST Port etc)
ACLs (ou filtros de firewall stateless)	Número de regras simultâneas. Como será realizada a atualização? Qual o SLA para aplicação? Especificação das regras.
IP Blackhole	Limitação de número de prefixos, tamanho de prefixos aceitos, regionalização da aplicação dos anúncios.