BOAS PRÁTICAS EM ROTEAMENTO DE BORDA PARA SISTEMAS AUTÔNOMOS PROVEDORES DE ACESSO À INTERNET EM PROCESSO DE *DUAL STACK*

João Alberto Barbosa de Oliveira[1]
Fábio Barbosa Rodrigues[2]

RESUMO

Considerando que o número de novos Sistemas Autônomos (SA) têm crescido em todo o mundo e, dentre as entidades que entram para esse grupo, temos outro nicho de grande importância, os provedores de acesso. De forma proporcional a esse crescimento, há a preocupação em propagar quesitos de boas práticas que são essenciais para o bom funcionamento do ativo de borda, suas políticas e a internet. O protocolo IPv6 está em crescimento exponencial entre os SA's do mundo, e já é fato que será o protocolo sucessor do IPv4. Este artigo tem como objetivo trazer o conjunto de práticas essenciais para mitigação de situações que possam causar possíveis problemas decorrentes à ausência de configurações essenciais em roteamento de borda do SA provedor de acesso.

Palavras-chave: Roteador de borda, Sistemas Autônomos, Provedor de Acesso, Boas práticas.

ABSTRACT

Considering that the number of new Autonomous Systems (SA) has grown all over the world, and among the entities that enter this group, we have another niche of great importance, the access providers. In proportion to this growth, there is a concern to propagate good practice requirements that are essential for the proper functioning of the edge asset, its policies and the Internet. The IPv6 protocol is in exponential growth among the SAs of the world, and already it is fact that will be the successor protocol of IPv4. This article aims to bring the set of practices essential to mitigation of situations that may cause possible problems due to the absence of essential configurations in the edge of the access provider SA.

Keywords: Border router, Autonomous Systems, Access Provider, Good practices.

1 INTRODUÇÃO

Este artigo aborda as principais práticas, voltadas para sistemas autônomos que provém acesso à internet à usuários finais, contudo, a maioria dos aspectos que serão tratados neste trabalho podem servir de referência para outros tipos de casos, como empresas e universidades que já são ou que estão prestes a tornar um novo SA. O trabalho apresenta o conjunto de práticas que visam métodos de se obter uma tabela global de roteamento mais segura e confiável, tendo como objetivo, o auxílio e colaboração em SA's já existentes, com

[1] Pós-graduando no curso *Lato Sensu* Gestão e Segurança em Redes de Computadores pela Universidade do Estado de Goiás (UEG). E-mail para contato: j.albertobsb@gmail.com.

[2] Tecnólogo em Redes de Comunicação IFG, Pós-graduado em Segurança de Redes de Computadores FATESG/Senai, Mestre em Engenharia Elétrica e Computação UFG, Doutorando em Engenharia Elétrica e de Computação UFG. E-mail para contato: prof.fabiobrodrigues@gmail.com.

foco em auxiliar administradores responsáveis por redes de provedores de acesso que estão atuando como um novo Sistema Autônomo.

O trabalho aborda cenários em comum aos protocolos BGP4[3], sob IPv4 e IPv6, o que torna híbridas as aplicações deste artigo para qualquer plataforma que tenha suporte a tais protocolos.

Apesar do BGP servir tanto para uso intra-SA como inter-SA, o uso do BGP é plenamente utilizado para conectar diferentes SA's que compõe a internet. Para a grande maioria dos cenários Intra-SA, protocolos como o OSPF (*Open Shortest Path First*) podem ser aplicados plenamente.

> Em um único SA, o protocolo de roteamento recomendado na Internet é o OSPF (embora este não seja o único em uso). Entre SAs é usado outro protocolo, o BGP (*Border Gateway Protocol*). É necessário um protocolo diferente entre SAs, porque os objetivos de um protocolo de gateway interior e os de um protocolo de gateway exterior não são os mesmos. Tudo o que um protocolo de gateway interior precisa fazer é movimentar pacotes da forma mais eficiente possível, da origem até o destino. Ele não precisa se preocupar com política. Tanenbaum (2003, p. 353)

Serão abordados cenários *fullrouting*[4] em processo de transição de IPv4 para IPv6 (*dual stack*[5]), cenário que muitos provedores estão passando (ou que passarão) até que o IPv6 seja plenamente difundido em toda a internet.

Importante ressaltar que, apesar das aplicações híbridas apresentadas neste artigo, é necessário que o administrador tenha ciência de que o roteador deva ter a capacidade de lidar com pelo menos um *fullrouting*, além de suportar o protocolo BGP com suas extensões Multiprotocolos (RFC 4760) e o IPv6.

2 DEFINIÇÕES E CONCEITOS

2.1 ENDEREÇAMENTO IP

[3] Border Gateway Protocol versão 4.

[4] Tabela completa de roteamento da Internet, estimada conforme apresentado no item 4.5.

[5] Pilha Dupla, processo de transição de IPv4 para IPv6, descrito no Capítulo 3 deste artigo.

"Na internet, cada host e cada roteador tem um endereço IP que codifica seu número de rede e seu número de host. A combinação é exclusiva: em princípio, duas máquinas na Internet nunca têm o mesmo endereço IP". Tanenbaum (2003, p.464)

2.2 ROTEAMENTO

"Roteamento diz a respeito à maneira pela qual as tabelas de roteamento são criadas para auxiliar no encaminhamento. Os protocolos de roteamento são usados para atualizar continuamente as tabelas de roteamento que são consultadas para encaminhamento e roteamento". Furouzan (2008, p.647)

2.2.1 ROTEAMENTO INTERDOMÍNIO E INTRADOMÍNIO

"Uma sessão BGP que abranja dois ASs é denominada uma sessão BGP externa (eBGP) e uma sessão BGP entre dois roteadores no mesmo AS é denominada uma sessão BGP interna (iBGP)." Kurose (2009, p.291).

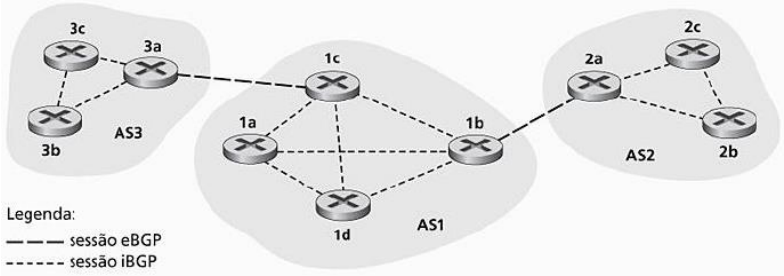


Figura 1 – Diferença entre iBGP e eBGP

Fonte: Kurose (2009, p.291)

2.3 SESSÃO BGP

Furouzan (2008, p.677) define como "Uma sessão é uma conexão estabelecida entre dois BGP roteadores apenas para fins de troca de informações de roteamento".

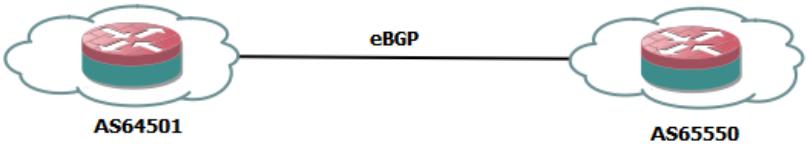


Figura 2 – Sessão BGP entre 2 AS's

Fonte: Autoria própria,2016

2.4 SISTEMA AUTÔNOMO

"Um sistema autônomo (SA) é um grupo de redes e roteadores sob a regência de uma única administração". Furouzan (2008, p.659).

2.4.1 HISTÓRICO DE ATRIBUIÇÕES DE SA's

O número de novos SA's está em constante crescimento, a figura 3 apresenta o crescimento do número total atribuído pelos RIR's (Regional Internet Number Registries)[6].

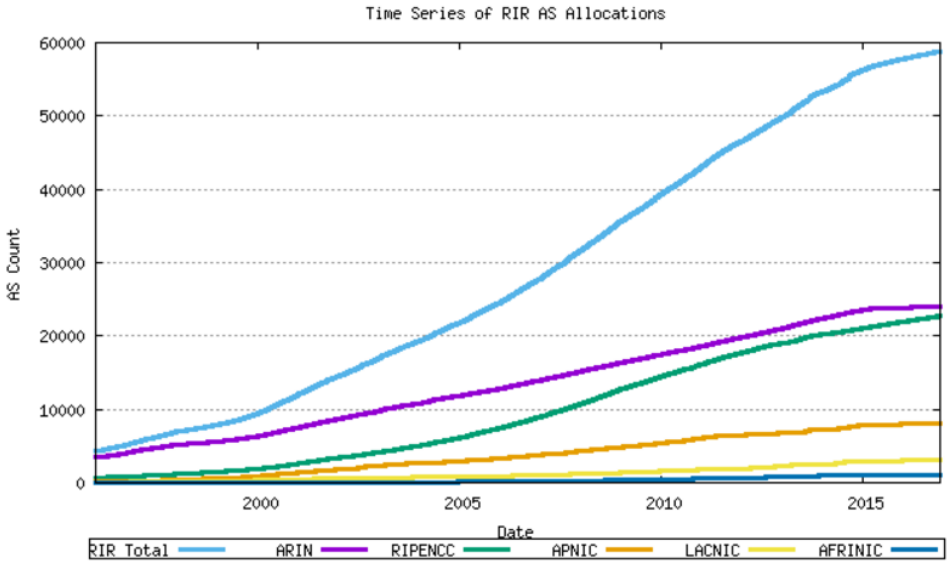


Figura 3 – Gráfico do histórico de alocação de SA's / AS's no mundo

Fonte: http://www.potaroo.net/tools/asns/

3 O PROCESSO DE TRANSIÇÃO "DUAL STACK"

O processo de transição entre os protocolos IPv4 e IPv6 na internet, não pode ser feito de forma brusca, desativando de vez uma versão do protocolo e ativando a outra. Como cita Furouzan (2008, p.603): "Em razão do número enorme de sistemas na Internet, a transição do IPv4 para o IPv6 não pode acontecer repentinamente. Levará um tempo

[6] *Regional Internet Number Registries*, organização responsável pela atribuição de números na Internet.

considerável antes que todos os sistemas na Internet possam mudar do IPv4 para o IPv6. A transição deve ser suave para evitar quaisquer problemas entre os sistemas IPv4 e IPv6.”

3.1 DUAL STACK OU PILHA DUPLA

“Recomenda-se que todos os hosts, antes de migrarem completamente para a versão 6, implementem a pilha dupla de protocolos. Em outras palavras, uma estação deve rodar o IPv4 e o IPv6 simultaneamente até que toda a Internet passe a usar o IPv6”. Furouzan (2008, p.604).

Os roteadores trabalharão com duas tabelas individuais de roteamento, sendo uma para o IPv4 e outra para o IPv6, isso de forma coexistente no mesmo equipamento, para que pacotes com destinos em suas respectivas versões de protocolos tenham sucesso no processo de encaminhamento até o seu destino.

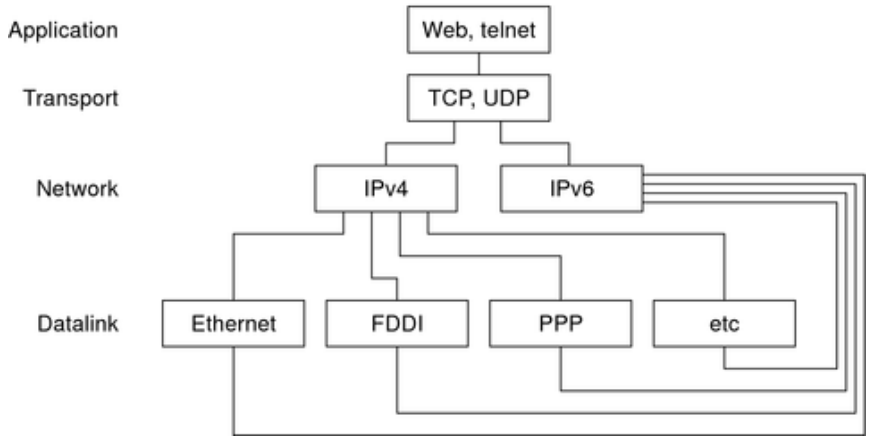


Figura 4 – Pilha dupla na camada de Rede (IP)

Fonte: https://docs.oracle.com/cd/E23823_01/html/816-4554/figures/dual.png

4 AS BOAS PRÁTICAS EM ROTEAMENTO

As boas práticas visam o conjunto de implantações cujo objetivo é tornar a rede e seus ativos mais tolerantes a situações adversas, resultando em mais segurança, estabilidade e resiliência em sua operação.

4.1 PROCESSO DE AUTENTICAÇÃO EM SESSÕES BGP

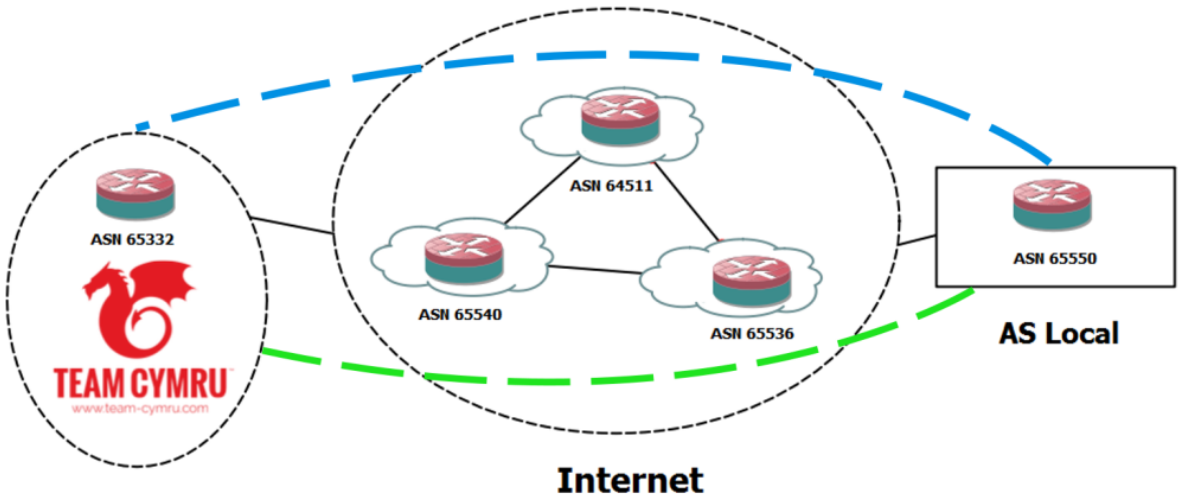
Para obter uma sessão mais confiável entre os vizinhos BGP, é importante fazer o uso de autenticação, isso, de forma criptografada. O uso de chaves MD5, descrito na RFC

2385 é, atualmente, a forma mais utilizada, “MD5 é ainda o mecanismo mais utilizado devido às suas disponibilidades de equipamentos dos fornecedores” (BCP 194, 2015, p. 5).

4.2 FILTRO DE BOGONS

No geral, os Bogons são blocos de IP’s aos quais não devem estar instalados na tabela de roteamento da Internet, tais são definidos nas RFC’s 1918, 6598 e 6890. São constituídos por endereços IP de uso privado, reservados ou não alocados pela IANA. Como o 192.168.0.0/16 (uso privado IPv4) e fe80::/10 (link local IPv6). Em muitos casos pacotes com IP’s de origem contidos nesses blocos são formados por *spoofing*[7] com o propósito de ataques de negação de serviço, o que torna difícil o rastreamento da origem em um momento de ataque, isso justifica a importância de não ter esses prefixos na tabela de roteadores de borda.

Um método que pode ser feito para receber esses prefixos dinamicamente é estabelecendo uma sessão *multihoping*[8] com a *Team CYMRU*[9] eles oferecem este serviço de forma gratuita. A Figura 5 apresenta 2 sessões *multihoping*, sendo 1 para receber prefixos bogons em IPv4 e outro em IPv6. As numerações de AS representadas pelo AS local e Internet são de uso genéricos, para documentação (RFC5398). Já o AS 65332 Representado pela Team CYMRU é o real.



[7] Pacotes cujo IP’s de origem foram falsificados.

[8] Sessão BGP não alcançável diretamente.

[9] Detalhes em: www.team-cymru.org

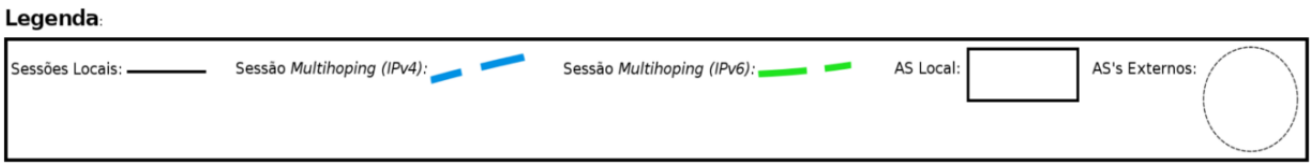


Figura 5 – Sessões com a Team CYMRU

Fonte: Autoria própria,2016

Os prefixos recebidos devem ser filtrados, conforme indicado no próximo tópico, para que sejam descartados, tais políticas são aplicáveis tanto para IPv6 como em IPv4.

4.3 FILTRAGEM DE PREFIXOS DE ENTRADA

Conforme BCP[10] 194, onde em um provedor *upstream*[11] podemos aceitar toda a tabela de rotas normalmente, com exceção de prefixos do próprio SA, prefixos mais específicos que /24 para IPv4 e /48 para IPv6, e prefixos que não podem estar na tabela global de roteamento, como os privados e não alocadas pela IANA.

É possível combinar essa tabela de acordo com a filtragem de descarte à prefixos dinâmicos recebidos via tabela *full Bogons*[12], conforme citado no item 4.2.

4.4 FILTRAGEM DE PREFIXOS DE SAÍDA

Segundo a BCP 194, anunciar prefixos que são apropriados, como pertencentes ao próprio AS em questão, e descartar todo o resto já é o suficiente. Evitando assim, por exemplo, de se tornar provedor de trânsito de forma indesejável.

4.5 LIMITAÇÃO DE PREFIXOS RECEBIDOS POR UM PERING

Conforme propõe a BCP 194, onde, em um *upstream fullrouting*, deve-se limitar o número máximo de prefixos recebidos, com a finalidade de proteger a memória dos roteadores. Recomenda-se ajustar esse valor de forma que sempre seja superior ao número de rotas na internet, já o limite, pode ser ajustado com a finalidade de alertar o administrador

[10] *Best Current Pratice*.

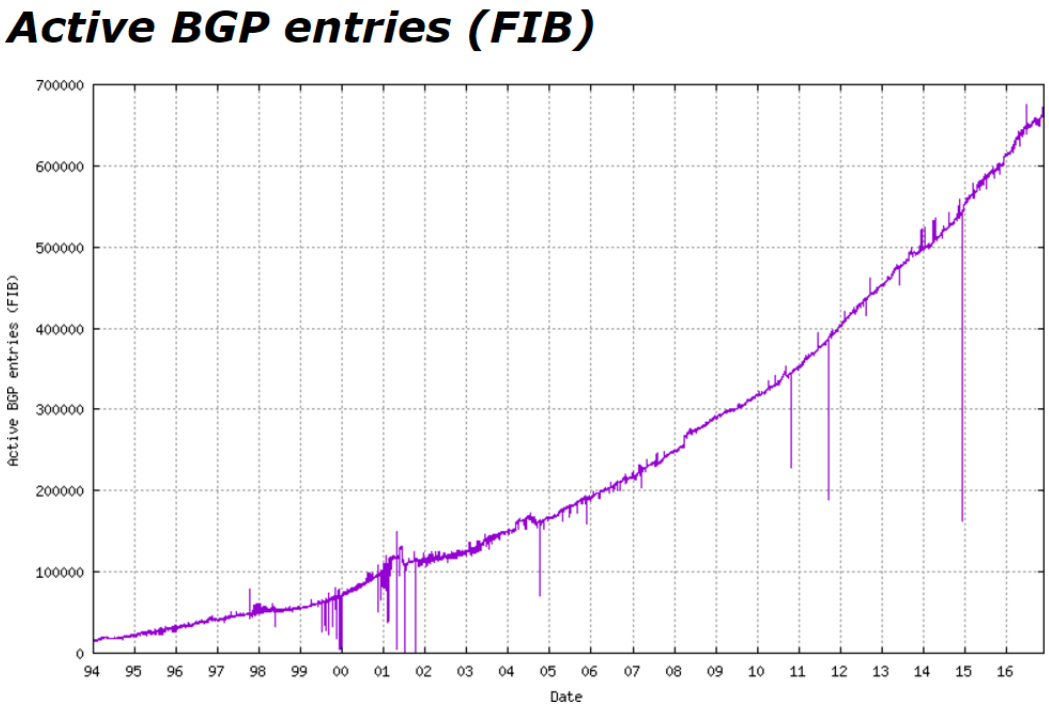
[11] Sessão com operadora de trânsito contratada pelo AS em questão.

[12] Combinação completa de prefixos reservados para uso especial e não alocados pela IANA.

sobre um determinado valor extrapolado, podendo variar até no valor máximo baseado no número de rotas reais que podem ser manipuladas pelo roteador.

Segundo o site potaroo.net, o número de rotas globais IPv4 (FIB[13]) obtidos pelo AS 6447 em 26 de novembro de 2016, foi de 674050 rotas e, em IPv6 no dia 27 de novembro de 2016 foi de 36682 rotas.

BGP data obtained from *AS6447*
Report last updated at Sat Nov 26 16:40:00 2016 (UTC+1000).



FIB / RIB Table Reports (plots)	Data Sets(txt)
Active BGP entries (FIB)	674050

Figura 6 – Tabela de roteamento IPv4 global

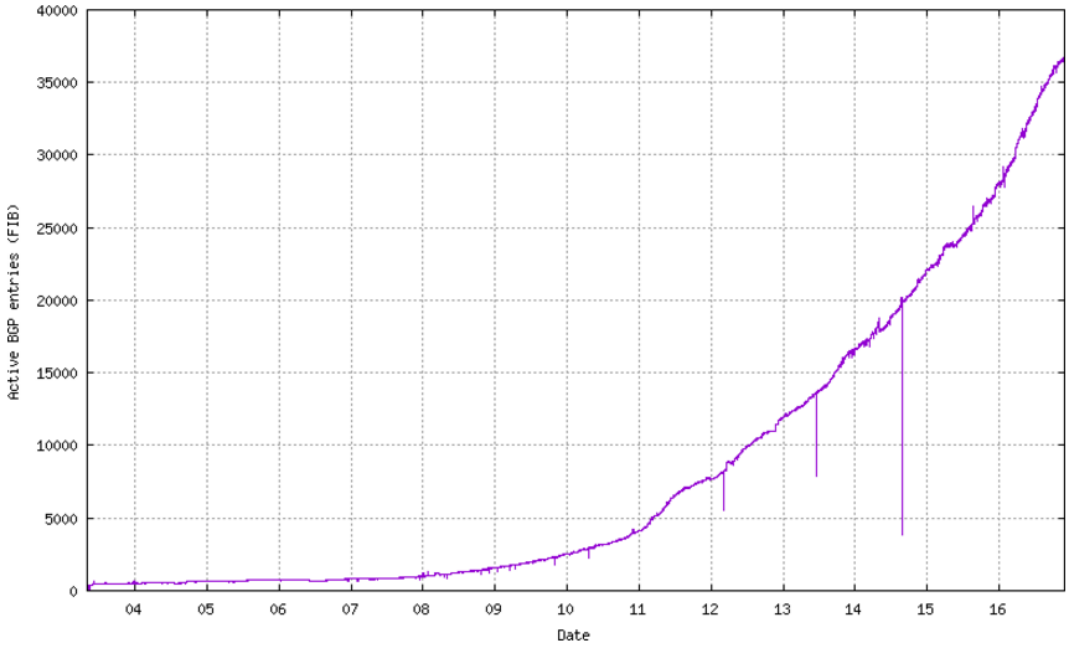
Fonte: http://bgp.potaroo.net/as6447/

[13]*Fowarding Information Base*, tabela ativa de encaminhamento

AS6447 IPv6 BGP Table Data

BGP data obtained from *AS6447*.
Report last updated at Sun Nov 27 16:00:00 2016 (Australian Eastern Time).

Active BGP entries (FIB)



FIB / RIB Table Reports (plots)	Data Sets(txt)
Active BGP entries (FIB)	36682

Figura 7 –Estatísticas de tabela (FIB) de roteamento IPv6 global

Fonte: http://bgp.potaroo.net/v6/as6447/

Ajustado tal valor, o roteador, verificando que o número limite foi extrapolado, imediatamente há um desligamento da sessão BGP. Baseado nisso, pode-se, por exemplo gerar um log, para que o administrador saiba o real motivo da sessão ter parado. A imagem a seguir demonstra uma simulação onde o limite de prefixos IPv6 foi estimado em 5000 rotas.

Nov/22/2016 15:15:57	memory	route, bgp, error	Terminating connection, too much routes received
Nov/22/2016 15:15:57	memory	route, bgp, error	RemoteAddress=2804:3[redacted]
Nov/22/2016 15:15:57	memory	route, bgp, error	RoutesReceived=5001

Figura 8 – Log de encerramento da sessão BGP sob atributo de limitação de prefixos

Fonte: Autoria própria, 2016

5 BOAS PRÁTICAS PARA O ROTEADOR DE BORDA

Considerando a importância do ativo responsável pelo roteamento de borda, é importante citar algumas práticas. Essa seção menciona de forma breve, questões mínimas ao software do ativo.

5.1 GERAÇÃO DE LOGS

Os logs são extremamente importantes para alertar o administrador sobre eventos anormais para o cenário em questão, como um login inválido ou a queda de uma sessão BGP, os logs podem ser gerados localmente, contudo é altamente recomendável o uso de um loghost centralizado. “Sempre que possível, o uso de loghosts centralizados é fortemente recomendado”. NIC BR Security Office (2003, p.20).

5.2 OTIMIZAÇÕES DE SERVIÇOS E SISTEMA OPERACIONAL

É imprescindível que o administrador realize otimizações no sistema operacional além dos serviços que rodam no roteador de borda. Vale ressaltar, que este ativo deve estar plenamente configurado com ênfase em sua principal função. Basicamente precisamos ter sessões BGP, tabelas de roteamento e ACL’s[14] básicas neste ativo. A presença de serviços ou pacotes extras ativos como DHCP[15], DNS[16], OSPF, FTP[17] dentre outros diversos não são nem um pouco necessários para um roteador de borda.

Por quesito de necessidade e segurança, sempre é necessário desativar este serviços e / ou pacotes dos mesmos. “A redução no número de pacotes instalados diminui a chance de que o sistema possua uma vulnerabilidade que possa vir a ser explorada por um atacante.” NIC BR Security Office (2003, p.14)

5.5.1 O ACESSO

[14] *Access Control Lists* lista de controle de acesso, são definidas por políticas de segurança.
[15] Dynamic HotsControl Protocol, protocolo de atribuição de IP’s de forma dinâmica.
[16] Domain Name System, protocolo responsável pela resolução de nomes em redes.
[17] File Transfer Protocol, protocolo para transferência de arquivos entre hots em rede.

Uma prática importante, é adoção de protocolos que troquem informações com o ativo de forma criptografada, assim podemos evitar por exemplo, a captura de informações sensíveis trafegadas, como senhas. Ao contrário do Telnet (RFC854), o protocolo SSH, determinado pela RFC 4253 oferece essa vantagem, fazendo com que todas as informações transportadas possuam criptografia. NIC BR Security Office (2003, p.26) "Essa substituição, além de fazer com que o tráfego entre cliente e servidor passe a ser criptografado, traz ainda outras vantagens, como proteção da sessão contra ataques tipo *man-in-the-middle* e seqüestro de conexões TCP."

6 FILTRO ANTISPOOFING PARA O SA

Esta prática está relacionada ao SA como um todo, tem grande colaboração em mitigação de ataques como negação de serviço, e devido a sua importância, foi necessário citá-la. A prática do filtro *antispoofing* no SA, em associação com as demais apresentadas, acabam sendo grandes responsáveis para o bom funcionamento do ISP e da Internet.

Para mais detalhes, o leitor deve consultar a BCP 38, BCP 84, e também o portal de boas práticas para a internet no Brasil[18].

7 CONCLUSÕES E SUGESTÕES DE TRABALHOS FUTUROS

As práticas citadas neste artigo demonstram execuções essenciais em políticas de roteamento de borda, além uma sessão dedicada à práticas para o ativo em si, que é o principal responsável pela troca e armazenamento de tabelas de rotas e tráfego.

Conclui-se que tais práxis são de uso essencial, devem ser consideradas e aplicadas sempre que possíveis em cenários de SA's. As documentações de referências deste artigo, podem ser exploradas pelo administrador e adaptadas ao cenário. Como responsável pelo AS262880, fazendo o uso de boas práticas, tenho notado como resultado índices extremamente baixos de incidentes relacionados à instabilidade de protocolos, além de itens do ativo, como uso de processamento anormal e sua segurança. Segundo o analisador *Radar*

[18] Detalhes em: http://bcp.nic.br

byQrator[19], em 26/11/2016 o AS em questão obteve pontuação de 9.98 de 10 no quesito segurança.

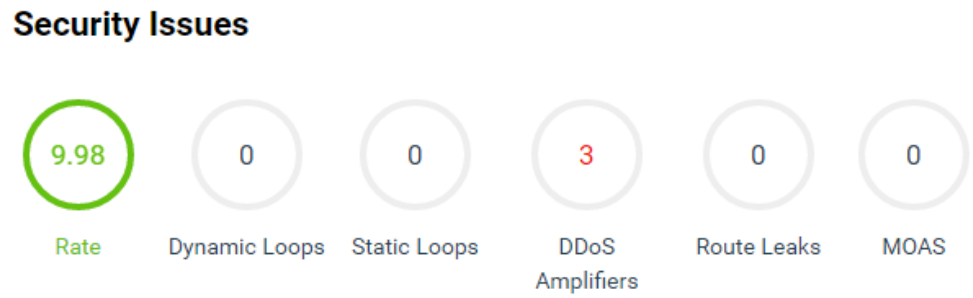


Figura 5 –Resultados do AS262880 segundo análise do site *Radar byQrator (26/11/2016)*

Fonte: https://radar.qrator.net

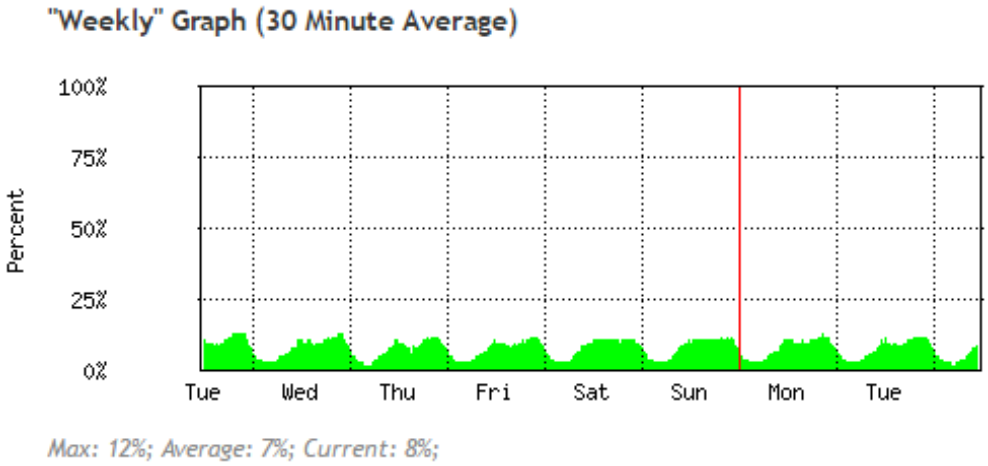


Figura 6 – Amostra do gráfico de processamento semanal - ativo de borda

Fonte: Autoria própria, 2016

Para trabalhos futuros, considerando a ampliação da abordagem deste artigo, seguem como sugestões do autor alguns títulos relevantes como: “O uso de novos métodos de autenticação como IPsec e TCP AO (Authentication Options) para sessões BGP”, “Políticas de firewall para sistemas autônomos” e “Segurança em OSPFv3”, tais títulos podem ter valores colaborativos no meio científico e tecnológico das comunicações, segurança e redes de computadores.

[19] https://radar.qrator.net

REFERÊNCIAS

Baker, F. and P. Savola, **"Ingress Filtering for Multihomed Networks"**, BCP 84, RFC 3704, DOI 10.17487/RFC3704, March 2004, <http://www.rfc-editor.org/info/rfc3704>.

Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "**Multiprotocol Extensions for BGP-4**", RFC 4760, DOI 10.17487/RFC4760, January 2007, <http://www.rfc-editor.org/info/rfc4760>.
Cotton, M., Vegoda, L., Bonica, R., Ed., and B. Haberman, "**Special-Purpose IP Address Registries**", BCP 153, RFC 6890, DOI 10.17487/RFC6890, April 2013, <http://www.rfc-editor.org/info/rfc6890>.

Durand, J., Pepelnjak, I., and G. Doering, **"BGP Operations and Security"**, BCP 194, RFC 7454, DOI 10.17487/RFC7454, February 2015, <http://www.rfc-editor.org/info/rfc7454>.

Ferguson, P. and D. Senie, **"Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing"**, BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <http://www.rfc-editor.org/info/rfc2827>.

FOROUZAN, BehrouzA..**Comunicação de dados e redes de computadores.**4 ed. [S.L.]: McGraw Hill, 2008. 1168 p.

Heffernan, A., "**Protection of BGP Sessions via the TCP MD5 Signature Option**", RFC 2385, DOI 10.17487/RFC2385, August 1998, <http://www.rfc-editor.org/info/rfc2385>.

Huston, G., "**Autonomous System (AS) Number Reservation for Documentation Use**", RFC 5398, DOI 10.17487/RFC5398, December 2008, <http://www.rfc-editor.org/info/rfc5398>.

OFFICE, NIC BR Security. "**Práticas de Segurança para Administradores de Redes de Internet**", 2002. <https://www.cert.br/docs/seg-adm-redes/seg-adm-redes.pdf>.

OLIVEIRA, J. A. B. de. Curso de Lato Sensu em Gestão e Segurança de Redes de Computadores. 2016. 12f. Trabalho de Conclusão – Universidade Estadual de Goiás, 2016.

Postel, J. and J. Reynolds, "**Telnet Protocol Specification**", STD 8, RFC 854, DOI 10.17487/RFC0854, May 1983, <http://www.rfc-editor.org/info/rfc854>.

Potaroo.net, "**Active BGP Entries"**. Disponível em: <http://bgp.potaroo.net>. Novembro, 2016.

Radar by Qrator, **"Security Issues".** Disponível em: <https://radar.qrator.net/>. Novembro 2016.

Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "**Address Allocation for Private Internets**", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <http://www.rfc-editor.org/info/rfc1918>.

ROSS, Keith W.; KUROSE., James F. **Redes de computadores e a internet:** Uma abordagem Top-Down. 5 ed. [S.L.]: Addison Wesley Bra, 2010. 576 p.

Tanenbaum, Andrew S., 1944 - **Redes de computadores** / Andrew S. Tanenbaum ; tradução Vanderberg D. de Souza – Rio de Janeiro : Elsevier, 2003 – 17º reimpressão.

Weil, J., Kuarsingh, V., Donley, C., Liljenstolpe, C., and M. Azinger, "**IANA-Reserved IPv4 Prefix for Shared Address Space**", BCP 153, RFC 6598, DOI 10.17487/RFC6598, April 2012, <http://www.rfc-editor.org/info/rfc6598>.

Ylonen, T. and C. Lonvick, Ed., "**The Secure Shell (SSH) Transport Layer Protocol**", RFC 4253, DOI 10.17487/RFC4253, January 2006, <http://www.rfc-editor.org/info/rfc4253>.

NOTAS PARA PUBLICAÇÃO

Esta versão se trata de uma submissão à revista "Anápolis Digital", contudo já foi publicado em outra revista: REVISTA MIRANTE (ONLINE), v. 11, p. 44-57, 2018.