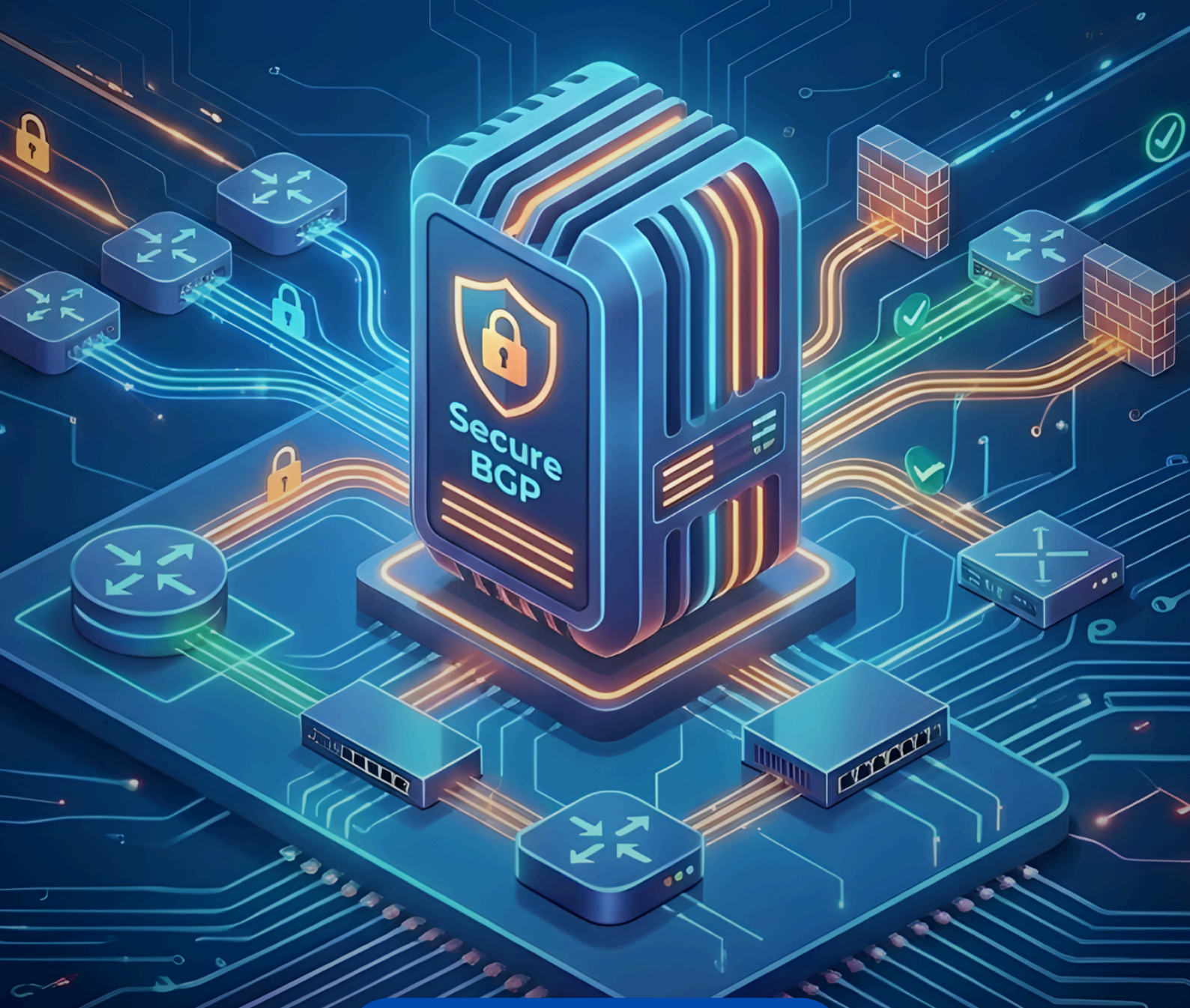
Roteamento Seguro com BGP

O que é, quais são suas principais ameaças e como proteger suas rotas



Lucas Rayan Guerra

Introdução

A estabilidade da Internet global depende da integridade das informações de roteamento trocadas entre dezenas de milhares de redes independentes. O Border Gateway Protocol (BGP), em sua versão 4, atua como o sistema nervoso central dessa infraestrutura, propagando informações de alcançabilidade entre Sistemas Autônomos (Autonomous Systems - AS) [1]. No entanto, o protocolo foi concebido em uma era de confiança implícita, desprovido de mecanismos nativos de validação de segurança, tornando-o suscetível a erros de configuração e ataques maliciosos que podem desviar tráfego em escala planetária.

O objetivo desta cartilha é fornecer um guia resumido sobre a operação segura do BGP, cobrindo desde os fundamentos teóricos até implementações práticas de mitigação de ataques. O documento alinha-se com as recomendações do NIST SP 800-189 e da iniciativa MANRS (Mutually Agreed Norms for Routing Security) [3] [4], abordando vetores de ameaça como sequestro de rotas (hijacking) e vazamentos de rotas (route leaks), e detalhando as tecnologias de defesa: RPKI, BGP Flowspec, RTBH e hardening de sessões.

O Básico do BGP e a Estrutura da Internet

Para proteger o BGP, primeiro precisamos entender como ele funciona na prática. Ao contrário de protocolos internos (IGP) como OSPF, que focam em encontrar o caminho mais rápido, o BGP é focado em políticas. Ele decide para onde o tráfego vai com base em regras de negócios e acordos entre empresas, não apenas velocidade [5].

O que é um Sistema Autônomo (AS)?

A Internet não é uma "nuvem" única, mas sim uma colcha de retalhos de redes independentes conectadas umas às outras. A peça básica desse quebra-cabeça é o Sistema Autônomo (AS). Um AS é um conjunto de endereços IP controlados por uma única organização (como um provedor de internet, um banco ou uma universidade) que tem uma política de roteamento própria [2] [6].

Cada AS tem um identificador global chamado ASN (Autonomous System Number). Antigamente eram números de 16 bits (até 65.536), mas como estavam acabando, hoje usamos 32 bits, o que permite mais de 4 bilhões de identificadores [7] [8].

Quem fala com quem? (Tipos de Relacionamento)

No BGP, a forma como as rotas se espalham depende de quem está pagando a conta. Entender isso é crucial para evitar vazamentos de rota (route leaks) [9] [10].

Tipos de Relacionamento		
Relação	**Descrição Econômica e Técnica**	**Política de Exportação Típica**
Trânsito (Provider-Customer)	O Cliente (Customer) paga ao Provedor (Transit) pela conectividade global.	O Provedor anuncia todas as rotas da tabela global ao Cliente (ou rota default). O Cliente anuncia apenas seus prefixos e de seus clientes ao Provedor.
Peering (Peer-to-Peer)	Troca de tráfego bilateral, geralmente sem custo (settlement-free), para beneficiar a latência e reduzir custos de trânsito.	O AS A anuncia apenas seus prefixos e de seus clientes ao AS B. O AS B faz o mesmo. Rotas aprendidas de outros provedores ou peers não são trocadas.
Sibilings (Irmãos)	Conexão entre dois AS pertencentes à mesma empresa, muitas vezes resultado de fusões/aquisições.	Política flexível, muitas vezes permitindo trânsito mútuo completo.

A maioria dos problemas acontece quando alguém quebra essas regras de exportação, anunciando rotas que não deveria.

Como o BGP Opera

O BGP roda em cima do protocolo TCP na porta 179. Isso é bom porque garante que as mensagens cheguem na ordem certa, mas também traz os riscos do TCP. Se alguém conseguir atacar a sessão TCP, derruba o BGP [11] [12].

A Máquina de Estados (Fases da Conexão)

Para saber se seu BGP está saudável, fique de olho nos estados da conexão [11]:

- **Idle:** O roteador está parado, recusando conexões.
- **Connect/Active:** O roteador está tentando ativamente abrir a porta TCP com o vizinho. Se ficar preso aqui, verifique se não há firewall bloqueando a porta 179 ou se a rota para o IP do vizinho existe.
- **Established:** Sucesso! A sessão está de pé e as rotas estão sendo trocadas.

Como o BGP escolhe o melhor caminho?

O BGP é um pouco teimoso. Ele não olha apenas a "velocidade". Ele segue uma lista rigorosa de critérios para decidir qual rota usar [13]:

- **Weight:** Critério proprietário (Cisco). Se configurado, ganha de tudo.
- **Local Preference:** O mais importante para decidir por onde o tráfego SAI da sua rede. Maior é melhor.
- **AS Path:** O caminho mais curto (menos saltos entre ASs). É aqui que os atacantes tentam enganar o roteador, fingindo ter um caminho curtinho.
- **MED:** Uma sugestão para o vizinho sobre por onde entrar na sua rede.

As Principais Ameaças

O grande defeito de fábrica do BGP é a confiança. Ele assume que, se um vizinho te mandou uma rota, ela é verdadeira. Isso cria duas grandes dores de cabeça:

BGP Hijacking (Sequestro de IP)

Acontece quando alguém anuncia IPs que não são dele. Isso pode desviar o tráfego da Internet inteira para o lugar errado [1] [14].

- **O ataque mais perigoso (More-Specific):** Se você anuncia o bloco 192.0.2.0/24, e um atacante anuncia 192.0.2.0/25 (uma metade desse bloco), a Internet vai preferir a rota do atacante, porque a regra do roteamento é sempre preferir o prefixo mais específico. Isso rouba todo o tráfego, não importa onde o atacante esteja no mundo [15].

Por que fazem isso?

- **Erro Humano (Fat Finger):** Alguém digitou o IP errado na configuração. Foi o que aconteceu quando o Paquistão tentou bloquear o YouTube e acabou derrubando o site no mundo todo [15].

- **Crime:** Para interceptar dados, roubar senhas, criptomoedas ou informações sensíveis [14].

Route Leaks (Vazamento de Rotas)

Diferente do sequestro, aqui a rota até existe, mas ela foi anunciada para quem não devia. É como contar um segredo para a pessoa errada [9] [16].

- **O Clássico (Tipo 1 - Hairpin):** Imagine que sua empresa tem dois links de internet (ISP A e ISP B). Se você não configurar direito, pode acabar recebendo as rotas do ISP A e anunciando para o ISP B.

O resultado é que o ISP B vai achar que você é um caminho ótimo para chegar no ISP A. De repente, o tráfego da Internet começa a passar por dentro do seu roteadorzinho, entupindo seu link e derrubando sua rede [9] [10].

Isso já aconteceu com grandes empresas, como a Google e provedores na Malásia, causando lentidão global [17] [18].

Hardening (Protegendo a Caixa)

Antes de olhar para fora, vamos proteger o roteador (Plano de Controle).

GTSM (Segurança via TTL)

Essa é uma técnica simples e genial para impedir que alguém longe de você tente derrubar sua sessão BGP. O truque é configurar o BGP para enviar pacotes com TTL (Time to Live) = 255. Você diz ao seu roteador: "Só aceite pacotes BGP se o TTL for 255 ou 254". Se um atacante estiver longe, o pacote vai passar por vários roteadores até chegar em você, e o TTL vai diminuindo (253, 250, 240...). Seu roteador vai ver o TTL baixo e descartar o pacote direto no hardware, sem nem incomodar o processador [19] [20].

Autenticação: Esqueça o MD5

Precisamos de senha na sessão BGP para garantir que o vizinho é quem diz ser.

- **MD5 (O Velho):** Era o padrão (RFC 2385). O problema é que, se você precisar trocar a senha, tem que derrubar a sessão BGP. Ninguém quer derrubar a Internet para trocar senha [12].

- **TCP-AO (O Novo):** É o padrão moderno (RFC 5925). Ele é mais seguro e permite usar "chaves" com data de validade. Você configura a chave nova para começar a valer amanhã, e os roteadores trocam sozinhos, sem derrubar a conexão. Use sempre que o equipamento suportar (Cisco, Juniper e Nokia modernos já suportam) [22] [23].

Limite de Rotas (Max-Prefix)

Essa é sua rede de segurança. Se seu vizinho errar e te mandar a tabela da Internet inteira (900 mil rotas) em vez de apenas as 10 rotas dele, seu roteador pode travar por falta de memória. Configure um Max-Prefix Limit. Se o vizinho passar do limite combinado (com uma margem de segurança), a sessão cai automaticamente para proteger seu equipamento [24] [25].

RPKI (O "Certificado Digital" das Rotas)

O RPKI é a solução definitiva para saber se a origem da rota é verdadeira, sem depender de bancos de dados desatualizados [3] [26].

O que é ROA?

Pense na ROA (Route Origin Authorization) como uma procuração assinada digitalmente. O dono do IP assina um documento dizendo: "Autorizo o AS X a anunciar meu bloco IP".

Cuidado com o Max Length: Um erro comum ao criar a ROA é ser muito permissivo no campo "Max Length". Se você tem um bloco /22 mas cria uma ROA permitindo até /24, um atacante pode anunciar os /24 e roubar seu tráfego, e o RPKI vai dizer que é válido!

Dica: O Max Length deve bater exatamente com o que você anuncia no BGP [27].

ROV (Validando na Entrada)

No seu roteador, você configura a validação (ROV - Route Origin Validation). O roteador baixa a lista de ROAs válidas e compara com o que recebe via BGP:

- **Valid:** Tudo certo. O dono autorizou esse AS.
- **Invalid:** Problema! Ou o AS está errado, ou o prefixo é mais específico do que o permitido. A recomendação é descartar (drop) essas rotas.

- **NotFound:** Ninguém criou ROA para isso ainda. Aceite normalmente (por enquanto) [25] [28].

Segurando Ataques DDoS

Quando o ataque é grande e entope seu link, não adianta tentar bloquear no seu firewall, porque o link já está cheio. Você precisa pedir ajuda para o provedor acima de você (upstream).

RTBH (Blackhole Remoto)

É o método mais "bruto". Você avisa seu provedor (usando uma Community BGP especial) que um IP específico da sua rede está sob ataque. O provedor descarta todo o tráfego para aquele IP na borda dele, antes de entrar no seu link [29] [30].

Lado ruim: Você completa o ataque. O IP atacado fica fora do ar para todo mundo. Mas pelo menos o resto da sua rede (e os outros clientes) continua funcionando [31].

BGP Flowspec (O Bisturi)

O Flowspec é muito mais elegante. Em vez de "matar" o IP, você envia uma regra de firewall via BGP. Exemplo: "Bloqueie apenas o tráfego UDP na porta 123 (NTP) vindo para o meu servidor". Isso segura o ataque sem tirar o servidor do ar para o tráfego legítimo (como o site HTTP na porta 80).

Atenção: Exige roteadores mais modernos e cuidado para não estourar a memória TCAM do equipamento [29] [32].

Boas Práticas (MANRS)

Segurança no BGP é um esporte coletivo. O MANRS é um compromisso global dos operadores de rede para limpar a Internet [4]. As 4 ações básicas que você deve fazer:

Filtragem: Não aceite lixo. Filtre o que seus clientes te mandam.

Anti-Spoofing: Não deixe sair da sua rede pacotes com IP de origem falsificado (use uRPF ou ACLs) [3].

Coordenação: Mantenha seus contatos atualizados no PeeringDB e Whois. Se der problema, as pessoas precisam te achar.

Validação Global: Crie suas ROAs. Diga ao mundo quais são seus IPs legítimos.

O Futuro: ASPA

O RPKI resolve a origem, mas e o caminho? O ASPA é a nova tecnologia que está chegando para validar se a sequência de ASs na rota faz sentido, impedindo aqueles vazamentos de rota onde o tráfego faz curvas estranhas (leaks tipo 1) [33] [34].

Conclusão

Proteger o BGP não é algo que se resolve apertando um único botão; é uma construção em camadas. Nenhuma ferramenta sozinha faz milagre: o RPKI valida a origem, mas não o caminho; o Flowspec segura o ataque, mas exige hardware compatível. A chave do sucesso é a Defesa em Profundidade.

Comece pelo básico (filtros e senhas), avance para o RPKI e deixe o RTBH pronto para emergências. Ao adotar essas práticas e seguir as normas do MANRS, você não está apenas protegendo o seu negócio contra quedas e sequestros, mas está ajudando a "limpar" a Internet global, tornando a rede mais estável e confiável para todos nós, pois o trabalho real começa agora no seu roteador.

Referências

[1] IETF. (2006). RFC 4271 - A Border Gateway Protocol 4 (BGP-4).

[2] Huston, G. (2006). Anatomy of a Route Leak.

[3] NIST. (2019). SP 800-189 - Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation.

[4] Internet Society. (2017). Mutually Agreed Norms for Routing Security (MANRS).

[5] Rekhter, Y., et al. (2006). RFC 4271 - A Border Gateway Protocol 4 (BGP-4) - Path Vector Attributes.

[6] Hawkinson, J., & Bates, T. (1996). RFC 1930 - Guidelines for creation, selection, and registration of an Autonomous System (AS).

[7] Vohra, Q., & Chen, E. (2012). RFC 6793 - BGP Support for Four-Octet Autonomous System (AS) Number Space.

[8] NRO. (2024). Internet Number Resource Status Report.

[9] Sriram, K., et al. (2016). RFC 7908 - Problem Definition and Classification of BGP Route Leaks.

[10] Dickson, B. (2012). Route Leaks in the Internet.

[11] IETF. (2006). RFC 4271 - BGP Finite State Machine.

[12] Heffernan, A. (1998). RFC 2385 - Protection of BGP Sessions via the TCP MD5 Signature Option.

[13] Cisco. (2023). BGP Best Path Selection Algorithm.

[14] Butler, K., et al. (2010). A Survey of BGP Security Mechanisms.

[15] RIPE NCC. (2008). YouTube Hijacking: A RIPE NCC RIS case study.

[16] Mauch, J. (2016). BGP Route Leaks and Mitigation.

[17] Toonk, A. (2015). Massive Route Leak Causes Internet Slowdown.

[18] Cloudflare. (2017). The Google Route Leak.

[19] Gill, V., et al. (2007). RFC 5082 - The Generalized TTL Security Mechanism (GTSM).

[20] Gill, V. (2004). RFC 3682 - The Generalized TTL Security Mechanism (GTSM).

[21] Juniper Networks. (2023). Configuring the TTL Security Mechanism.

[22] Touch, J., et al. (2010). RFC 5925 - The TCP Authentication Option.

[23] Eastwood, M. (2023). TCP-AO: A Better Way to Protect BGP Sessions.

[24] Cisco. (2022). Configuring BGP Maximum Prefix Limits.

[25] MANRS. (2021). MANRS Implementation Guide.

[26] Lepinski, M., & Kent, S. (2012). RFC 6480 - An Infrastructure to Support Secure Internet Routing (RPKI).

[27] Gilad, Y., et al. (2017). Maxlength Considered Harmful to the RPKI.

[28] NIC.br. (2020). Implementando RPKI e ROV.

[29] Marques, P., et al. (2009). RFC 5575 - Dissemination of Flow Specification Rules.

[30] Cisco. (2020). Remotely Triggered Black Hole (RTBH) Filtering.

[31] FastNetMon. (2025). Filtering L3/L4 DDoS attacks with BGP Flow Spec and RTBH.

[32] Loibl, C., et al. (2020). RFC 8955 - Dissemination of Flow Specification Rules.

[33] Azimov, A., et al. (2023). BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA).

[34] NIST. (2023). BGP Security and Resilience - ASPA Implementation.