Roteamento BGP Seguro e Eficiente

O Border Gateway Protocol (BGP) é um recurso fundamental da Internet, que essencialmente ajuda a unir a infinidade de redes que compõem a web e transporta a enorme quantidade de tráfego que cruza o globo a cada dia.

Como uma peça crucial do quebracabeça da Internet, é imperativo que o BGP funcione sem problemas e evite vulnerabilidades, interrupções e problemas de segurança.

A Internet depende muito que os operadores de rede façam a coisa certa para garantir que as informações corretas cheguem às partes corretas. No entanto, o fornecimento de uma filtragem de rota BGP robusta e à prova de falhas representa um desafio para muitas organizações.

O protocolo BGP funciona muito bem, mas existe desde muito antes dos problemas de segurança específicos de hoje e funciona em coordenação com redes espalhadas por todo o globo — deixando a rede potencialmente aberta a sequestros e vazamentos. A Internet Society estimou, como exemplo, que houve mais de 5.000 vazamentos e sequestros de rotas em 2017.

As informações coletadas pela divisão Global IP Network (GIN) da NTT sobre esse fenômeno mostraram alguns padrões nos EUA: a maioria desses vazamentos parece acontecer no meio da semana, por volta de terça-feira, e também há um pico nas sextasfeiras, pouco antes do fim de semana começar. Portanto, é necessário estar extremamente atento nesses períodos.

Os vazamentos de rota BGP envolvem a configuração incorreta acidental ou anúncio ilegítimo de prefixos, ou blocos de endereços IP, que se propagam pelas redes e resultam em roteamento deficiente (suboptimal routing) ou sequestro de tráfego.

Esses tipos de vazamentos vêm ocorrendo na última década, ano após ano — então, vale a pena implementar filtros para neutralizar os problemas que isso pode causar.

E há vários desses mecanismos que podem ajudar a proteger contra esses vazamentos — métodos com os quais a NTT e a Global IP Network estão bem preparadas para ajudar.

Peerlock “Lite”

Uma forma de filtragem, usando um método que a NTT se refere como “Peerlock Lite”, é rejeitar prefixos que passaram por redes Tier 1 recebidos de clientes ou peers (veja o link para as redes comumente consideradas neste nível).

Por exemplo, a NTT só pode ser acessada por meio de peering gratuito (settlement-free peering). Portanto, quaisquer rotas para a NTT que você receber de um cliente ou peer serão vazamentos. Usando mecanismos de proteção implementados em peering privado ou pontos de troca Internet para negar essas redes Tier 1, é possível bloquear facilmente muitos problemas potenciais, antes mesmo que eles ocorram.

> “Usando mecanismos de proteção implementados em peering privado ou pontos de troca Internet ... é possível **bloquear facilmente muitos problemas potenciais,** antes mesmo que eles ocorram.

A desvantagem desse método é que ele requer uma lista estática de Números de Sistema Autônomo (ASNs), que são números que identificam redes específicas. A sua natureza estática significa que se a função de uma dessas redes for modificada ou deixar de ser trânsito gratuito, a lista necessitará de atualização.

Assim, torna-se crucial garantir que uma revisão semestral ou anual seja realizada para manter a lista fidedigna. Também requer um conhecimento inferido ou explícito das relações de trânsito dos ASNs bloqueados. No entanto, esse método é uma das maneiras mais eficazes de eliminar vazamentos de rota.

Comunidades BGP

Outro método para bloquear vazamentos é garantir que os prefixos recebidos de parceiros de peering gratuitos nunca sejam anunciados a outros parceiros de peering. Uma maneira de fazer isso é etiquetar rotas com comunidades BGP ou rótulos para rotas que compartilham uma propriedade comum. Os filtros podem então ser configurados para que os prefixos sem as comunidades apropriadas sejam rejeitados na saída de um roteador de borda.

Além disso, se não houver nenhuma comunidade associada a determinadas rotas, seria aconselhável que não fossem anunciadas a outra parte. Isso garantirá que, se esses prefixos de alguma forma entrarem em sua rede, sua rede nunca os propagará. Desta forma, o uso de comunidades BGP pode ser uma ferramenta chave na prevenção de vazamentos de rota.

Entre as comunidades BGP mais conhecidas estão “no-export” e “no-advertise”. A primeira delas está associada a rotas que não devem ser anunciadas além do ASN próprio da empresa e a segunda está associada com aquelas rotas que não devem ser anunciadas além do roteador receptor. É importante entender o comportamento dessas comunidades antes de usá-las, ajudando assim a garantir que o nível exigido de disponibilidade seja mantido nas rotas.

As comunidades podem ser especificadas para categorias, incluindo onde as rotas foram aprendidas — como um cliente de trânsito ou parceiro de peering — ou para locais como Europa ou uma cidade específica. No entanto, a gama de possibilidades para as comunidades BGP é ampla e essa flexibilidade fornece um escopo significativo para aproveitá-las.

Como exemplo do uso de tais comunidades, a NTT tem uma comunidade que pode ser aplicada para suprimir anúncios aos parceiros de peering da operadora. Um cliente pode usar isso se, por exemplo, quiser desviar o tráfego de um peer, que tem congestionamento em sua rede ou está sofrendo uma interrupção, para outro peer. Uma outra opção permite que o tráfego seja desviado, mas os anúncios de rota para o peer devem ser deixados como um backup de último recurso no caso de problemas ocorrerem também nas conexões com os outros peers.

Estas opções podem ser aplicadas a todos os peers ou apenas aos peers selecionados, com o objetivo de dar o máximo de flexibilidade aos clientes para determinar como os anúncios de rota são tratados da forma que melhor se adapta às suas necessidades de negócio.

Enquanto isso, a NTT oferece comunidades mais amplas para escolhas baseadas em regiões e também blackholing acionado por comunidade — incluindo blackholing seletivo e regional, que fornece ferramentas para os clientes com opções ainda mais granulares.

Whitelists

Outra abordagem é aplicar a chamada “Whitelist” (lista branca) de prefixos que um cliente pode anunciar em cada sessão BGP externa (eBGP) voltada para o cliente, tornando as operações mais seguras.

Este é um método que a NTT emprega para todas essas sessões, usando dados dos Internet Routing Registries (IRRs). Na verdade, a empresa usa uma Whitelist exclusiva para cada cliente, reduzindo drasticamente as chances e a extensão dos danos e dando a ela um controle rígido sobre as rotas que a empresa aceita dos clientes.

Além dos mecanismos oferecidos pela NTT para lidar com isso, há uma série de ferramentas open-source que podem ser úteis para aplicar filtros de prefixo e podem ser convertidos no formato adequado para plataformas específicas de roteador, como BGPQ3.

> “A NTT usa uma Whitelist **exclusiva para cada cliente,** reduzindo drasticamente as chances e a extensão dos danos.

Limites Máximo de Prefixo

Ainda, outro método para evitar vazamentos de rota é a aplicação de Limites Máximo de Prefixo. Por exemplo, um limite de 1.000 rotas pode ser aplicado a uma sessão eBGP para que a sessão seja encerrada automaticamente se essa quantidade for excedida.

Esses limites de prefixo fornecem uma medida de segurança importante para ajudar a rede a responder de uma forma que cause danos mínimos ao sistema de roteamento global e proteja contra vazamentos, fornecendo proteção para roteadores e redes. Eles podem atuar como uma forma altamente eficaz de proteger a rede se houver de fato um vazamento de rota, pois impede que isso seja propagado.

Os Limites Máximos de Prefixo podem ser aplicados tanto como pré-política quanto como pós-política, embora o efeito máximo possa ser obtido ao fazer como pré-política para ajudar a evitar quaisquer problemas significativos antes que eles aconteçam, em vez de correr o risco que alguns prefixos vazados sejam permitidos. No entanto, as políticas de filtragem de prefixo variam de acordo com a plataforma de roteamento, com algumas permitindo que isso seja feito somente como pós-política.

Peerlocking

A NTT implementou com sucesso uma forma mais abrangente de Peerlocking. Usar isso pode, em uma escala global, reduzir enormemente o risco de prefixos sendo aceitos por rotas não autorizadas.

A essência dessa abordagem é “colocar na rede o que as pessoas te disseram”. Em termos básicos, depende dos parceiros de peering dizendo à NTT quais redes, se houver, são provedores de trânsito autorizados — com os parceiros que fornecem essas informações, conhecidos como “ASNs protegidos”. As rotas podem ser “bloqueadas” se vierem de provedores de trânsito não autorizados.

É altamente recomendável que as redes que você está tentando proteger sejam informadas e concordem com a implementação desses filtros, para que não haja surpresas inesperadas no futuro — novamente contando com a comunicação com os peers. Os parceiros sempre precisam estar cientes do que está acontecendo com a rede e o envolvimento é fundamental para isso.

> “O mecanismo de Peerlocking da NTT pode, portanto, **reduzir significativamente o impacto** e a proliferação de vazamentos de rota.

Também é essencial que esses filtros Peerlock sejam aplicados a todas as sessões eBGP, sejam as sessões voltadas para o cliente ou as sessões de peering, para garantir que esse mecanismo de proteção de chave seja totalmente utilizado.

Em suma, o Peerlocking da NTT oferece um método altamente eficiente para interromper vazamentos de rota e a empresa percebeu melhorias significativas para as redes que concordaram em se tornar ASNs protegidos.

Flexibilidade

A NTT oferece expectativas regionais, dando flexibilidade aos peers gratuitos globais que operam de maneira diferente em continentes diferentes. A NTT também tem um manual que gera para cada peer, para o qual habilita o bloqueio. Isso é útil para definir a documentação sobre os prós e contras da tecnologia e como ela funciona, bem como para a empresa reter esse conhecimento à medida que os funcionários deixam a empresa.

Resumindo, o mecanismo Peerlocking da NTT pode, portanto, reduzir significativamente o impacto e a proliferação de vazamentos de rota, ajudando por meio do monitoramento ativo da zona default-free.

Uma chave para o sucesso da NTT na implementação dessas tecnologias é seu controlador SDN líder da indústria chamado GIN Unified Management System (GUMS). O uso do GUMS permite que a NTT implemente alterações nas Whitelists, comunidades, Peerlocking e políticas BGP em geral de maneira programática. Isso leva a configurações implementadas de forma consistente e taxas de erro de configuração muito mais baixas.

Os operadores fazem alterações na interface Web do GUMS e implementam suas alterações no servidor GUMS, em vez de fazer login nos roteadores e fazer alterações manualmente. A capacidade de fazer isso torna o processo mais eficiente, melhorando a eficácia do sistema como um todo.

Para mais informações ou feedback, entre em contato conosco:

gin@ntt.net
gin.ntt.net
@GinNTTnet #globalipnetwork #AS2914