

Formação para Sistemas Autônomos

Boas Práticas BGP

Licença de uso do material

Esta apresentação está disponível sob a licença



Creative Commons

Atribuição – Não a Obras Derivadas (by-nd)

<http://creativecommons.org/licenses/by-nd/3.0/br/legalcode>

Você pode:

- **Compartilhar** — copiar, distribuir e transmitir a obra.
- **Fazer uso comercial da obra.**
- Sob as seguintes condições:

Atribuição — Ao distribuir essa apresentação, você deve deixar claro que ela faz parte do Curso de Formação para Sistemas Autônomos do CEPTRO.br/NIC.br, e que os originais podem ser obtidos em <http://ceptro.br>. Você deve fazer isso sem sugerir que nós damos algum aval à sua instituição, empresa, site ou curso.

Vedada a criação de obras derivadas — Você não pode modificar essa apresentação, nem criar apresentações ou outras obras baseadas nela..

Se tiver dúvidas, ou quiser obter permissão para utilizar o material de outra forma, entre em contato pelo e-mail: info@nic.br.

Estabelecendo uma sessão BGP

- As sessões BGP utilizam TCP, na porta 179
- Pode-se utilizar IPv4 ou IPv6
- Recomenda-se o uso de interfaces loopback
 - Loopbacks são interfaces lógicas
 - Elas não “caem”. São independentes de problemas com links.

Loopback no iBGP

- No iBGP devemos sempre usar interfaces loopback
 - Usando interfaces físicas, se o link for interrompido, a sessão BGP também será
 - Usando loopbacks temos uma estabilidade maior. Como as rotas para os IPs das loopbacks são aprendidos via IGP, se um enlace for interrompido, a sessão continua estabelecida, com os pacotes fazendo um caminho alternativo.

Loopbacks no eBGP

- No eBGP também é recomendado utilizar loopbacks
 - O IP na loopback é de responsabilidade do AS
 - Use um IP público/válido /32 e um IPv6 /128
 - Não deve ser utilizado um IP privado.
 - O IP na interface física é geralmente fornecido pelo provedor de trânsito (upstream)
 - Se o serviço for trânsito Internet, esse IP deve ser roteável
 - Se for um serviço de conexão privada (uma rede MPLS por exemplo) pode-se usar IPs privados
 - Cuidados
 - É necessário criar uma rota estática para o endereço da loopback do vizinho
 - É preciso usar também a funcionalidade de multihop
 - Caso se utilize o TTL Security Check, é preciso configurá-lo corretamente

Loopbacks no eBGP

- O loopback no eBGP facilita o balanceamento entre enlaces redundantes com outro AS
 - Com sessões estabelecidas pelas interfaces físicas, seriam necessárias duas. Com o loopback, apenas uma sessão é necessária.



Loopbacks no eBGP

- O uso de loopbacks no eBGP dificulta ataques
 - Estabelecendo uma sessão com interfaces físicas, os IPs utilizados são da mesma rede. Normalmente um /30 ou /31 IPv4 e um /127 IPv6.
 - Um desses IPs normalmente pode ser obtido via traceroute. O outro pode ser facilmente inferido.
 - A porta de destino da conexão é padrão, 179 TCP.
 - Dessa forma, das 4 variáveis da conexão TCP por meio da qual está estabelecida a sessão, 3 são descobertas trivialmente. Isso torna relativamente fáceis alguns tipos de ataque, como men in the middle.
 - Com o uso de loopbacks, os IPs utilizados são de redes diferentes, dificultando a descoberta dos parâmetros da conexão por alguém com más intenções.

Uma loopback por serviço

- Um dos benefícios do uso das loopbacks é a possibilidade de separar os serviços e protocolos em um dado roteador:
 - Cada qual usa uma loopback e IP próprios
 - A prática pode facilitar a migração de serviços entre diferentes roteadores
 - O lado negativo é o maior consumo de IPs na infraestrutura

Autenticando sessões BGP com MD5

- É recomendável usar autenticação MD5 para as sessões BGP
 - A configuração é simples: os roteadores vizinhos compartilham uma mesma chave (uma senha)
 - A cada pacote é adicionado um checksum codificado, que o outro roteador pode verificar utilizando sua chave MD5, ajudando a garantir sua autenticidade e integridade
 - A técnica dificulta ataques
 - neighbor "ip-address ou peer-group-name" password "senha" (Cisco)
 - authentication-key "senha" (Juniper)

TTL Security Check

- Por padrão, os pacotes das sessões eBGP são enviados com valor de TTL/Hop-Limit igual a 1, buscando garantir que quem está enviando o pacote é um vizinho diretamente conectado. Porém um atacante externo pode facilmente conseguir inserir um pacote com TTL/Hop-Limit igual a 1 no enlace.
- O TTL Security Check é uma ideia bastante simples e engenhosa:
 - O roteador envia pacotes com TTL/Hop-Limit igual a 255 (valor máximo desse campo).
 - No próximo roteador, o valor será decrementado, e igual a 254 (255-1).
 - Verificando esse valor é possível garantir que o pacote de origem está a 1 salto de distância, ou seja, veio do roteador vizinho
 - Um atacante em outra rede não conseguirá inserir um pacote com TTL/Hop-Limit igual a 255 no enlace onde foi estabelecida a sessão BGP, pois o TTL/Hop-Limit será decrementado antes, em outros roteadores.

```
neighbor 2001:DB8:200:FFFF::255 ttl-security hops 1 (Cisco)
```

- Quando as sessões BGP são estabelecidas entre loopbacks, há um hop extra:

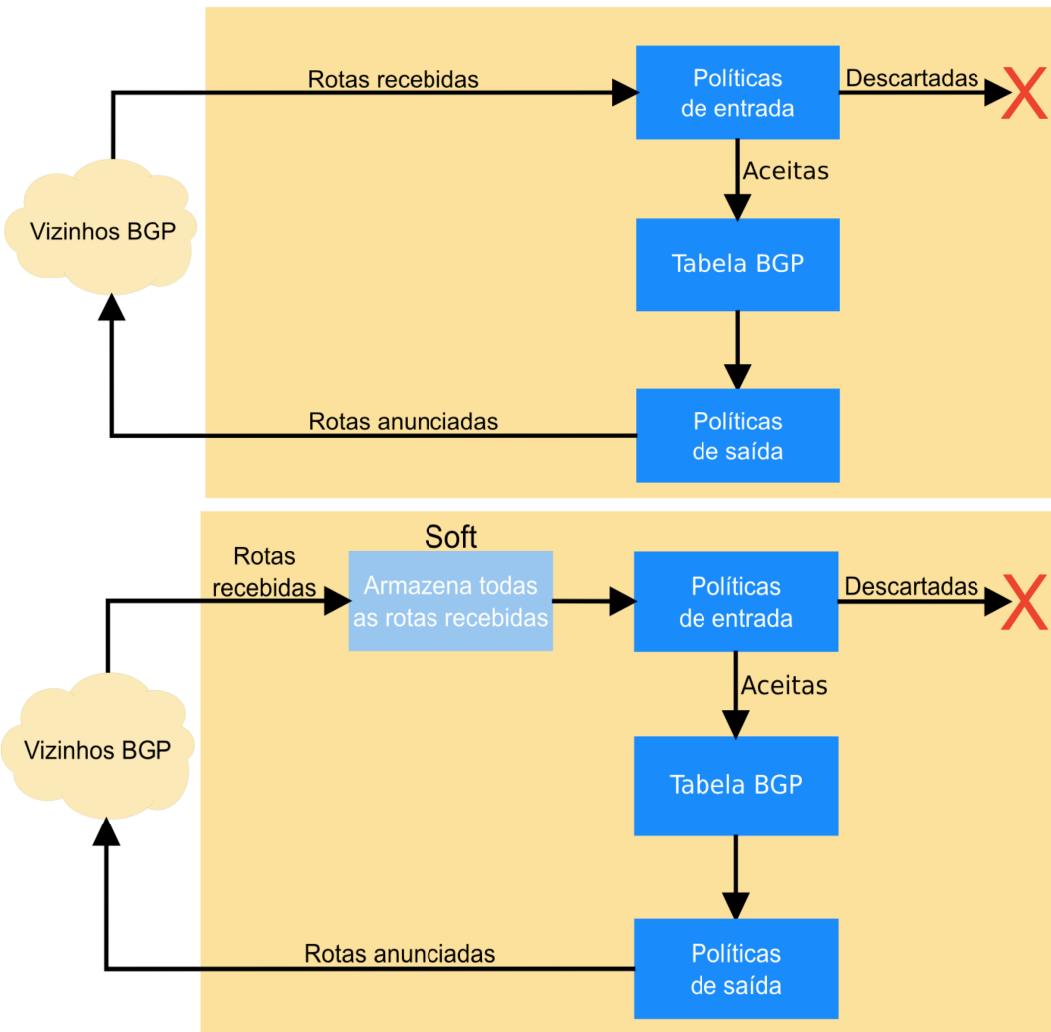
```
neighbor 2001:DB8:200:FFFF::255 ttl-security hops 2 (Cisco)
```

Desabilitando serviços e protocolos

- Nas interfaces onde são estabelecidas sessões eBGP é fundamentalmente que todos os serviços e protocolos desnecessários estejam desabilitados, de forma particular:
 - IGP (OSPF)
 - Router Advertisement (RA) no IPv6

Soft Reconfiguration Inbound

- A tabela BGP de um roteador é populada após a aplicação de filtros.
 - Informações podem ser descartadas e não são armazenadas nessa tabela
 - Se os filtros são mudados, não há como reaplicá-los sobre a informação original
- Habilitando a “soft reconfiguration” é criada uma nova tabela, com a informação original.
 - Isso consome mais memória
 - Permite que filtros sejam modificados facilmente
- Para Cisco e Mikrotik é recomendado habilitar a função. Para o Juniper, é automático.



Route refresh

- Uma alternativa ao uso do Soft Reconfiguration, é solicitar, numa mudança de filtros, que o vizinho cujas rotas são afetadas reenvie toda a informação pertinente.
 - Isso se chama Route Refresh
 - Economiza memória que seria utilizada para manter a tabela extra do Soft Reconfiguration
 - Nem todos os roteadores suportam
- Alguns roteadores suportam a função de route refresh. Essa capacidade é informada no estabelecimento de uma sessão BGP e é possível verificar-la olhando as informações do vizinho.
- Após uma mudança em um filtro é preciso solicitar o refresh para o roteador vizinho, com um comando. Isso não é automático.

Filtros

- Alguns roteadores são permissivos e, se nenhum filtro for aplicado, aceitam tudo que os vizinhos enviam.
- É uma boa prática aplicar filtros de entrada e saída para cada vizinho, ANTES de estabelecer qualquer sessão eBGP.

Filtros de entrada

- Clientes
 - Deve-se aceitar apenas os prefixos que foram designados (por você mesmo) ao cliente, ou alocados a ele pelo NIC.br ou por um RIR.
- Fornecedores de trânsito (upstreams)
 - Você paga seu fornecedor de trânsito para que ele forneça acesso à toda a Internet. É possível trabalhar com rotas default nesse caso.
 - Você só deve receber prefixos de seu upstream, caso necessite deles para fazer engenharia de tráfego.
- Peers (com quem realizamos troca de tráfego)
 - Deve-se combinar antes que prefixos serão anunciados ou aceitos.
 - No caso sessões BGP em um acordo de troca de tráfego multilateral no PTT, deve-se receber todos os prefixos anunciados, com as seguintes exceções:
 - Se você têm clientes de trânsito no PTT, deve-se filtrar os prefixos deles. Assim evita-se que o tráfego na direção do cliente passe pelo PTT, no lugar de passar no link de trânsito
 - Se você têm upstreams no PTT, pode ser desejável filtrá-los, forçando o tráfego a fluir pelo link de trânsito em ambas as direções, e evitando assimetrias.

Filtros de entrada

- Verifique a lista do bogons (prefixos que não deveriam aparecer no BGP), do Team Cymru:
 - www.team-cymru.org/Services/Bogons/http.html
- Para IPv4
 - É preciso lembrar que não há mais endereços reservados para alocações futuras. Deve-se remover todos os filtros baseados no status dos blocos nos RIRs. Ver:
 - <http://tools.ietf.org/html/rfc6441>
- Para IPv6
 - Você pode bloquear tudo por padrão e permitir apenas o 2000::/3, ou os prefixos mais específicos /12 e /23 sob responsabilidade de cada RIR. Alguns bogons podem estar dentro do espaço dos RIRs, então também devem ser bloqueados explicitamente.
- Feed automático de bogons:
 - <http://www.team-cymru.org/Services/Bogons/routeserver.html>

Filtros de entrada

- Aplicando corretamente os filtros, você ajuda a:
 - Garantir a integridade da sua própria rede
 - Garantir a integridade de toda a Internet
- É responsabilidade de cada Sistema Autônomos ser um bom cidadão da Internet.

Prefixos no iBGP e eBGP

- O iBGP deve ser usado para transportar os prefixos de seus clientes / usuários. Não use OSPF ou outro IGP para isso.
 - Crie uma rota estática para a interface do cliente (ou agregador).
 - Use “bgp network” para originar o prefixo no iBGP
 - O prefixo existirá enquanto a rota estática existir e a interface estiver ativa.
- Esses prefixos não são exportados no eBGP. No eBGP devem estar presentes apenas os prefixos agregados, mais aqueles necessários para engenharia de tráfego.
 - Os prefixos usados para engenharia de tráfego não dependem daqueles presentes no iBGP. Os prefixos presentes no iBGP não devem ser exportados para o eBGP.
 - Os prefixos usados para engenharia de tráfego devem ser gerados na borda da rede, com rotas estáticas para null e comandos do tipo “bgp network”.

Dúvidas?

