

Alocação de Sub-rede do Pool IP de Acesso Seguro e Anúncio de Rota BGP

Contents

Problema

O pool IP configurado com uma sub-rede /20 mostra duas sub-redes /22 instaladas nas rotas de Nuvem em vez das duas sub-redes /21 esperadas. Essa configuração fornece apenas metade do espaço de endereço esperado.

Ambiente

- Tecnologia: Suporte à solução (SSPT - contrato necessário)
- Subtecnologia: Acesso seguro
- Linha de produtos: SECACCS
- Versão de software: TODOS
- Configuração: Pools IP com configurações de sub-rede /20
- Infraestrutura: Dois headends de VPN ativos com anúncio de rota BGP

Resolução

Dimensionamento do pool de VPN do usuário e anúncio de BGP

O BGP de Acesso Seguro não anuncia um prefixo maior que /22. Quando você configura um pool de VPN de usuário para VPN de acesso remoto (RAVPN) no Acesso Seguro, a plataforma processa a rede de acordo:

- Se a rede fornecida for maior que /22 (como /20), a plataforma automaticamente divide a rede internamente em vários blocos /22.

Exemplo: Você fornece um pool /20. O Secure Access divide isso em 4 ×/22 sub-redes internamente. Cada /22 é alugado por um data center na região sob demanda. Quando um data center aluga um /22, ele anuncia apenas esse /22 (ou menor) sobre o BGP — não o /20 completo.

- Se a rede fornecida for /22 ou menor (como /24), a plataforma dividirá a rede em pelo menos duas sub-redes menores para suportar alta disponibilidade em um mínimo de dois data centers na região.

Exemplo: Você fornece um pool /24. O Secure Access divide isso em 2 ×/25 sub-redes. Cada /25 é atribuído a um datacenter diferente na região. Cada datacenter anuncia seu respectivo /25 sobre o BGP.

Nem todas as sub-redes do pool VPN são anunciadas simultaneamente. Em vez disso, elas são alocadas e anunciadas sob demanda à medida que o número de conexões de cliente VPN aumenta:

- Inicialmente, somente a primeira sub-rede (como a primeira /22 de um /20) é alugada e anunciada via BGP.
- À medida que a demanda aumenta, as sub-redes adicionais são alugadas por data centers e anunciadas subsequentemente.
- Isso é consistente com a maneira como os recursos de nuvem são dinamicamente escalados.

Exemplo: Você configura 4 pools × /22 para cobrir um intervalo de /20. No volume de conexão baixo, o BGP anuncia somente o primeiro /22. Conforme as conexões RAVPN aumentam, os pools /22 restantes são ativados e anunciados incrementalmente.

Importante: Se você observar que apenas um dos seus pools configurados está sendo anunciado, esse é o comportamento esperado. Pools adicionais são anunciados conforme as demandas de dimensionamento exigem.

Summary

Tamanho do pool fornecido	Divisão interna	anúncio de BGP	Razão
Maior que /22 (como /20)	Dividido em vários /22s (como 4 × /22)	Cada /22 ou menor, sob demanda	O prefixo máximo anunciado é /22; escalonamento sob demanda
/22	Dividido em 2 ou mais sub-redes menores	Cada sub-rede menor, sob demanda	Alta disponibilidade em data centers ≥2
Menor que /22 (como /24)	Dividido em pelo menos 2 sub-redes (como 2 × /25)	Cada sub-rede, sob demanda	Alta disponibilidade em data centers ≥2

- Prefixo máximo anunciado pelo BGP: /22 — O Secure Access nunca anuncia uma rede maior que /22 pelo BGP.
- Divisão automática — as redes são divididas internamente para alta disponibilidade (mínimo de 2 data centers por região) e escalabilidade.
- Anúncio sob demanda — As sub-redes são anunciadas via BGP somente quando são alugadas ativamente por um data center para servir conexões. Nem todos os pools aparecem no BGP de uma vez.
- O dimensionamento é dinâmico — As sub-redes de pool adicionais são ativadas à medida que as contagens de conexões de clientes RAVPN aumentam, em conformidade com os princípios de dimensionamento de recursos nativos da nuvem.

Causa

Este é o comportamento projetado do algoritmo de alocação de sub-rede do sistema Secure

Access. O sistema divide automaticamente as sub-redes configuradas em sub-redes menores e de mesmo tamanho e as distribui entre os headends VPN disponíveis usando classificação lexicográfica para garantir padrões de alocação consistentes e previsíveis.

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.