Secure Access IP Pool Subnet Allocation and BGP Route Advertisement

Contents

Issue

IP pool configured with a /20 subnet shows two /22 subnets installed in the Cloud routes instead of the expected two

Environment

- Technology: Solution Support (SSPT - contract required)
- Sub-technology: Secure Access
- Product Family: SECACCS
- Software Version: ALL
- Configuration: IP pools with /20 subnet configurations
- Infrastructure: Two active VPN headends with BGP route advertisement

Resolution

User VPN Pool Sizing and BGP Advertisement

Secure Access BGP does not advertise a prefix larger than /22. When you configure a user VPN pool for remote acc

- If the provided network is larger than /22 (such as /20), the platform automatically splits the network internally

    Example:

    You provide a /20 pool.

    Secure Access splits this into $4 \times$ /22 subnets internally.

    Each /22 is leased by a datacenter in the region on demand.

    When a data center leases a /22, it advertises only that /22 (or smaller) over BGP — not the full /20.

- If the provided network is /22 or smaller (such as /24), the platform splits the network into at least two smaller

    Example:

    You provide a /24 pool.

    Secure Access splits this into $2 \times$ /25 subnets.

    Each /25 is assigned to a different datacenter in the region.

    Each datacenter advertises its respective /25 over BGP.

VPN pool subnets are not all advertised simultaneously. Instead, they are allocated and advertised on demand as the

- Initially, only the first subnet (such as the first /22 of a /20) is leased and advertised via BGP.
- As demand grows, additional subnets are leased by data centers and subsequently advertised.
- This is consistent with how cloud resources are dynamically scaled.

  Example:

  You configure $4 \times$ /22 pools to cover a /20 range.

  At low connection volume, BGP advertises only the first /22.

  As RAVPN connections increase, the remaining /22 pools are activated and advertised incrementally.

Important: If you observe that only one of your configured pools is being advertised, this is expected behavior. Ad

Summary

Provided pool size	Internal split	BGP advertisement	Reason
Larger than /22 (such as /20)	Split into multiple /22s (such as $4 \times$ /22)	Each /22 or smaller, on demand	Max adv demand
/22	Split into 2 or more smaller subnets	Each smaller subnet, on demand	High av
Smaller than /22 (such as /24)	Split into at least 2 subnets (such as $2 \times$ /25)	Each subnet, on demand	High av

- **Maximum BGP advertised prefix:** /22 — Secure Access never advertises a network larger than /22 over BG
- **Automatic splitting** — Networks are split internally for high availability (minimum 2 data centers per region)
- **On-demand advertisement** — Subnets are advertised via BGP only when they are actively leased by a data cente
- **Scaling is dynamic** — Additional pool subnets are activated as RAVPN client connection counts increase, in native resource scaling principles.

Cause

This is the designed behavior of the Secure Access system subnet allocation algorithm. The system automatically sp sized subnets and distributes them across available VPN headends using lexicographical sorting to ensure consistent

Related Content

- [Cisco Technical Support & Downloads](#)