安全访问IP池子网分配和BGP路由通告

目录

问题

使用/20子网配置的IP池显示在云路由中安装了两个/22子网，而不是预期的两个/21子网。此配置仅提供预期地址空间的一半。

环境

- 技术：解决方案支持（SSPT — 需要合同）
- 子技术：安全访问
- 产品系列：SECACCS
- 软件版本:全部
- 配置:具有/20子网配置的IP池
- 基础设施:两个具有BGP路由通告的活动VPN前端

分辨率

用户VPN池大小和BGP通告

安全访问BGP不会通告大于/22的前缀。在安全访问中为远程访问VPN(RAVPN)配置用户VPN池时，平台将相应地处理网络：

- 如果提供的网络大于/22（例如/20），平台会自动将网络内部拆分为多个/22数据块。

示例： 提供/20池。 Secure Access在内部将其拆分×4个/22子网。 每个/22都由该区域内的数据中心按需租用。 当数据中心租用/22时，它仅通过BGP通告/22（或更小），而不是完整的/20。

- 如果提供的网络是/22或更小（例如/24），平台会将网络拆分为至少两个较小的子网，以支持该区域中至少两个数据中心的高可用性。

示例： 提供/24池。 Secure Access将此划分为2 × /25子网。 每个/25都分配到该区域中的不同数据中心。 每个数据中心都通过BGP通告其各自的/25。

VPN池子网并非全部同时通告。相反，随着RAVPN客户端连接数量的增加，将会按需分配和通告子网：

- 最初，只有第一个子网（如/20的前/22）通过BGP租用和通告。
- 随着需求的增长，数据中心会租用更多子网，并随后进行通告。
- 这与云资源的动态扩展方式一致。

示例： 您配置4个× /22池以覆盖/20范围。 在连接量较低时，BGP仅通告第一个/22。 随着

RAVPN连接的增加，剩余的/22池将被激活并以增量方式通告。

重要信息：如果您发现仅通告一个已配置的池，这是预期行为。其他池将通告为所需的扩展需求。

摘要

提供的池大小	内部拆分	BGP通告	原因
大于/22（例如/20）	拆分为多个/22s(例如4 × /22)	每个/22或更小，按需	最大通告前缀为/22；按需扩展
/22	划分为2个或更多更小的子网	每个更小的子网，按需	跨2个数据中心≥高可用性
小于/22（例如/24）	拆分为至少2个子网(例如2 × /25)	每个子网按需分配	跨2个数据中心≥高可用性

- 最大BGP通告前缀: /22 — 安全访问绝不会通过BGP通告大于/22的网络。
- 自动拆分 — 网络在内部拆分，以实现高可用性（每个区域至少2个数据中心）和可扩展性。
- 按需通告 — 只有当子网由数据中心主动租用以服务连接时，才会通过BGP通告子网。并非所有池同时出现在BGP中。
- 扩展是动态的 — 根据cloud-native resource scaling principles，随着RAVPN客户端连接计数增加，会激活额外的池子网。

原因

这是Secure Access系统子网分配算法的设计行为。系统会自动将已配置的子网拆分为较小且大小相等的子网，并使用字典排序将它们分配到可用的VPN头端，以确保一致和可预测的分配模式。

相关内容

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。