安全存取IP池子網分配和BGP路由通告

目錄

問題

使用/20子網配置的IP池顯示在雲路由中安裝了兩個/22子網，而不是預期兩個/21子網。此配置僅提供預期地址空間的一半。

環境

- 技術：解決方案支援（SSPT — 需要合約）
- 子技術：安全訪問
- 產品系列：SEACACS
- 軟體版本:ALL
- 組態:具有/20子網配置的IP池
- 基礎設施：具有BGP路由通告的兩個活動VPN前端

解析

使用者VPN池大小和BGP通告

Secure Access BGP不會通告大於/22的字首。在Secure Access中為遠端訪問VPN(RAVPN)配置使用者VPN池時，平台將相應地處理網路：

- 如果提供的網路大於/22（如/20），平台會自動將網路內部拆分為多個/22塊。

範例： 您提供了/20池。 Secure Access在內部將此子網分×為4個/22子網。 每個/22均由該區域內的資料中心按需租用。 當資料中心租用/22時，它只在BGP上通告/22（或更小），而不是完整的/20。

- 如果提供的網路為/22或更小（如/24），平台會將網路拆分為至少兩個較小的子網，以支援該區域中至少兩個資料中心的高可用性。

範例： 提供/24池。 Secure Access將此劃分為2個×/25子網。 每個/25都分配給該區域中的不同資料中心。 每個資料中心通過BGP通告其各自的/25。

VPN池子網並非全部同時通告。相反，隨著RAVPN客戶端連線數量的增加，它們會按需分配和通告：

- 最初，只有第一個子網（如/20的第一個/22）通過BGP租用和通告。
- 隨著需求的增長，資料中心會租用更多的子網，並隨後進行通告。
- 這與雲資源的動態擴展方式一致。

範例： 配置4個× /22池以覆蓋/20範圍。 在低連線量時，BGP僅通告第一個/22。 隨著RAVPN連線的增加，剩餘的/22池將啟用並增量通告。

重要資訊：如果您觀察到僅有一個已配置的池被通告，則這是預期行為。其他池被通告為擴展需求所需。

摘要

提供的池大小	內部拆分	BGP通告	原因
大於/22（例如/20）	拆分為多個/22s(如4 × /22)	每個/22或更小，按需	最大通告字首為/22；按需擴展
/22	分割為2個或更多更小的子網	每個較小的子網（按需）	跨2個資料中心≥高可用性
小於/22（例如/24）	拆分為至少2個子網(如2 × /25)	每個子網（按需）	跨2個資料中心≥高可用性

- 最大BGP通告字首: /22 — 安全訪問絕不會通過BGP通告大於/22的網路。
- 自動分隔 — 網路在內部進行拆分以實現高可用性（每個區域至少2個資料中心）和可擴充性。
- 按需通告 — 僅當資料中心主動租用子網為連線服務時，才會通過BGP通告子網。並非所有池同時出現在BGP中。
- 擴展是動態的 — 根據雲原生資源擴展原則，隨著RAVPN客戶端連線數量的增加，啟用額外的池子網。

原因

這是Secure Access系統子網分配演算法的設計行為。系統會自動將已配置的子網分割為大小相等的較小子網，並使用詞典排序將它們分配到可用的VPN前端，以確保一致和可預測的分配模式。

相關內容

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。