

Subnetzzuweisung für sicheren Zugriff auf IP-Pool und BGP-Routenankündigung

Inhalt

Problem

Der mit einem /20-Subnetz konfigurierte IP-Pool zeigt zwei /22-Subnetze, die in den Cloud-Routen installiert sind, anstelle der erwarteten zwei /21-Subnetze. Diese Konfiguration stellt nur die Hälfte des erwarteten Adressraums bereit.

Umwelt

- Technologie: Solution Support (SSPT - Vertrag erforderlich)
- Untertechnologie: Sicherer Zugriff
- Produktfamilie: SECACS
- Software-Version: ALLE
- Konfiguration: IP-Pools mit /20-Subnetzkonfigurationen
- Infrastruktur: Zwei aktive VPN-Headends mit BGP-Routenankündigung

Auflösung

Benutzer-VPN-Pool-Größe und BGP-Meldung

Das BGP für sicheren Zugriff kündigt kein Präfix an, das größer als /22 ist. Wenn Sie einen Benutzer-VPN-Pool für RAVPN (Remote Access VPN) in sicherem Zugriff konfigurieren, verarbeitet die Plattform das Netzwerk entsprechend:

- Wenn das bereitgestellte Netzwerk größer als /22 ist (z. B. /20), teilt die Plattform das Netzwerk automatisch intern in mehrere /22-Chunks auf.

Beispiel: Sie stellen einen /20-Pool bereit. Secure Access teilt dies intern in 4 × /22 Subnetze auf. Jeder /22 wird bei Bedarf von einem Rechenzentrum in der Region gemietet. Wenn ein Rechenzentrum einen /22 leaset, wird nur dieser /22 (oder kleiner) über BGP angekündigt, nicht der volle /20.

- Wenn das bereitgestellte Netzwerk /22 oder kleiner (z. B. /24) ist, teilt die Plattform das Netzwerk in mindestens zwei kleinere Subnetze auf, um eine hohe Verfügbarkeit in mindestens zwei Rechenzentren in der Region zu unterstützen.

Beispiel: Sie stellen einen /24-Pool bereit. Secure Access teilt dies in 2 × /25 Subnetze auf. Jeder /25 ist einem anderen Rechenzentrum in der Region zugewiesen. Jedes Rechenzentrum meldet seine jeweiligen /25-over-BGP-Verbindungen.

Die Subnetze des VPN-Pools werden nicht alle gleichzeitig angekündigt, sondern bei Bedarf zugewiesen und angekündigt, wenn die Anzahl der RAVPN-Clientverbindungen zunimmt:

- Zunächst wird nur das erste Subnetz (z. B. das erste /22 eines /20) geleast und via BGP angekündigt.
- Bei steigendem Bedarf werden zusätzliche Subnetze von Rechenzentren geleast und anschließend angekündigt.
- Dies entspricht der dynamischen Skalierung von Cloud-Ressourcen.

Beispiel: Sie konfigurieren 4 × /22 Pools, um einen /20-Bereich abzudecken. Bei geringem Verbindungsvolumen meldet BGP nur den ersten /22. Mit der Zunahme der RAVPN-Verbindungen werden die verbleibenden /22-Pools aktiviert und nach und nach bekannt gegeben.

Wichtig: Wenn Sie feststellen, dass nur einer Ihrer konfigurierten Pools angekündigt wird, wird dieses Verhalten erwartet. Zusätzliche Pools werden angekündigt, wenn Skalierungsanforderungen dies erfordern.

Zusammenfassung

Bereitgestellte Poolgröße	Interne Aufteilung	BGP-Anzeige	Grund
Größer als /22 (wie /20)	Aufteilen in mehrere /22s (z. B. 4 × /22)	Jeder/22 oder kleiner, je nach Bedarf	Das max. angekündigte Präfix ist /22; bedarfsgerechte Skalierung
/22	Aufteilung in zwei oder mehr kleinere Subnetze	Jedes kleinere Subnetz, auf Anfrage	Hohe Verfügbarkeit in ≥2 Rechenzentren
Kleiner als /22 (wie /24)	In mindestens 2 Subnetze aufteilen (z. B. 2 × /25)	Jedes Subnetz, On Demand	Hohe Verfügbarkeit in ≥2 Rechenzentren

- Maximales vom BGP bekanntes Präfix: /22 - Secure Access kündigt ein Netzwerk, das größer als /22 ist, nie über BGP an.
- Automatisches Splitting - Netzwerke werden intern aufgeteilt, um hohe Verfügbarkeit (mindestens 2 Rechenzentren pro Region) und Skalierbarkeit zu gewährleisten.
- On-Demand-Werbung - Subnetze werden nur dann über BGP angekündigt, wenn sie von einem Rechenzentrum aktiv geleast werden, um Verbindungen zu bedienen. Nicht alle Pools werden gleichzeitig in BGP angezeigt.
- Dynamische Skalierung: Bei zunehmender Anzahl von RAVPN-Client-Verbindungen werden zusätzliche Pool-Subnetze aktiviert. Dabei werden die Cloud-nativen Prinzipien der Ressourcenskalisierung befolgt.

Ursache

Dies ist das geplante Verhalten des Subnetz-Zuweisungsalgorithmus des Secure Access-Systems. Das System teilt konfigurierte Subnetze automatisch in kleinere Subnetze gleicher

Größe auf und verteilt sie mithilfe lexikografischer Sortierung auf verfügbare VPN-Headends, um konsistente und vorhersagbare Zuweisungsmuster zu gewährleisten.

Verwandte Inhalte

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.