

Allocazione subnet pool IP di accesso sicuro e annuncio route BGP

Sommario

Problema

Il pool IP configurato con una subnet /20 mostra due subnet /22 installate nelle route del cloud anziché le due subnet /21 previste. Questa configurazione fornisce solo metà dello spazio degli indirizzi previsto.

Ambiente

- Tecnologia: Supporto per la soluzione (SSPT - contratto obbligatorio)
- Sottotecnologia: Accesso sicuro
- Famiglia di prodotti: SECACS
- Versione del software: TUTTO
- Configurazione: Pool IP con configurazioni subnet /20
- Infrastruttura: Due headend VPN attivi con annuncio route BGP

Risoluzione

Dimensionamento pool VPN utente e pubblicità BGP

Secure Access BGP non annuncia un prefisso più grande di /22. Quando si configura un pool VPN per l'utente per la VPN ad accesso remoto (RAVPN) in Secure Access, la piattaforma elabora la rete di conseguenza:

- Se la rete specificata è più grande di /22 (ad esempio /20), la piattaforma suddivide automaticamente la rete internamente in più blocchi /22.

Esempio: Viene fornito un pool /20. Secure Access suddivide internamente queste subnet in 4 × /22. Ogni /22 viene concesso in leasing su richiesta da un centro dati dell'area. Quando un data center concede in leasing una /22, viene annunciata solo la /22 (o una versione inferiore) su BGP, non la /20 completa.

- Se la rete specificata è di dimensioni maggiori o uguali a /22 (ad esempio /24), la piattaforma suddivide la rete in almeno due subnet più piccole per supportare l'elevata disponibilità in almeno due centri dati della regione.

Esempio: Viene fornito un pool /24. Secure Access suddivide il pacchetto in 2 subnet × /25. Ogni /25 viene assegnato a un centro dati diverso nell'area. Ogni data center annuncia il proprio /25 su BGP.

Le subnet del pool VPN non vengono annunciate tutte contemporaneamente. Al contrario, vengono allocate e annunciate su richiesta con l'aumento del numero di connessioni client VPN:

- Inizialmente, solo la prima subnet (ad esempio la prima /22 di una /20) viene assegnata in leasing e pubblicizzata tramite BGP.
- Con l'aumento della domanda, le subnet aggiuntive vengono prese in leasing dai centri dati e successivamente pubblicizzate.
- Ciò è coerente con il modo in cui le risorse cloud vengono scalate dinamicamente.

Esempio: È possibile configurare pool $4 \times /22$ per coprire un intervallo /20. Con un volume di connessione basso, BGP annuncia solo la prima /22. Con l'aumento delle connessioni RAVPN, i pool /22 rimanenti vengono attivati e annunciati in modo incrementale.

Importante: se si osserva che solo uno dei pool configurati viene annunciato, si tratta del comportamento previsto. I pool aggiuntivi vengono annunciati come richieste di scalabilità.

Riepilogo

Dimensioni pool fornite	Divisione interna	Annuncio BGP	Motivo
Maggiore di /22 (ad esempio /20)	Divisione in più /22s (ad esempio $4 \times /22$)	Ogni /22 o meno, su richiesta	Il prefisso annunciato massimo è /22; il ridimensionamento su richiesta
/22	Dividi in 2 o più subnet più piccole	Ogni subnet più piccola, su richiesta	Elevata disponibilità in almeno 2 centri dati
Inferiore a /22 (ad esempio /24)	Dividere in almeno 2 subnet (ad esempio $2 \times /25$)	Ogni subnet, su richiesta	Elevata disponibilità in almeno 2 centri dati

- Prefisso BGP annunciato massimo: /2 — Secure Access non annuncia mai una rete più grande di /22 su BGP.
- Suddivisione automatica: le reti vengono suddivise internamente per garantire elevata disponibilità (almeno 2 centri dati per area) e scalabilità.
- Pubblicità su richiesta: le subnet vengono pubblicizzate tramite BGP solo quando vengono utilizzate attivamente da un centro dati per servire le connessioni. Non tutti i pool vengono visualizzati contemporaneamente in BGP.
- La scalabilità è dinamica: le subnet del pool aggiuntive vengono attivate all'aumentare del numero di connessioni client RAVPN, in conformità ai principi di scalabilità delle risorse native del cloud.

Causa

Questo è il comportamento progettato dell'algoritmo di allocazione delle subnet del sistema Secure Access. Il sistema divide automaticamente le subnet configurate in subnet più piccole di dimensioni uguali e le distribuisce sugli headend VPN disponibili utilizzando l'ordinamento

lessicografico per garantire modelli di allocazione coerenti e prevedibili.

Contenuto correlato

- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).