BGP-sessieflappen vanwege limieten voor routeprefix in beveiligde toegang tot AWS Direct Connect-integratie

Inhoud

uitgeven

BGP-sessies worden ervaren flappen op een site-to-site tunnel tussen Cisco Secure Access en AWS Direct Connect. De instabiliteit treedt op omdat het aantal routevoorvoegsels dat wordt geadverteerd vanuit Secure Access de AWS Direct Connect-limieten overschrijdt, waardoor stabiele routeuitwisseling wordt voorkomen en de mogelijkheid om consistente connectiviteit tot stand te brengen tussen Secure Access en AWS wordt beïnvloed.

milieu

- Cisco Secure Access (CSA)
- AWS Direct Connect met BGP-routering
- Site-to-site tunnelconfiguratie tussen Secure Access en AWS
- AWS Direct Connect BGP prefix limiet van 100 routes

resolutie

De resolutie omvat meerdere benaderingen om de BGP prefix limiet beperking aan te pakken.

Analyse van netwerkpakketten onthult BGP NOTIFICATION-berichten die aangeven dat het maximum aantal voorvoegsels is bereikt:

```
Border Gateway Protocol - NOTIFICATION Message
    Length: 28
    Type: NOTIFICATION Message (3)
    Major error Code: Cease (6)
    Minor error Code (Cease): Maximum Number of Prefixes Reached (1)
```

Onmiddellijke tijdelijke oplossingen

Optie 1: routefiltering aan de AWS-zijde

Evalueer AWS-opties om binnenkomende routevoorvoegsels van Secure Access te negeren of te filteren om binnen de limiet van 100 voorvoegsels te blijven die door AWS Direct Connect wordt opgelegd.

Optie 2: Implementatie van AWS Transit Gateway

Overweeg de migratie naar een AWS Transit Gateway als alternatief connectiviteitsmodel. Deze aanpak kan meer flexibele routeringsopties bieden en kan helpen de prefix-beperkingen van Direct Connect te omzeilen.

langetermijnoplossing

Implementatie van functieaanvraag

Er is een aanvraag voor een functie (CSE-I-4783) ingediend om routefiltering of samenvattingsmogelijkheden op Secure Access mogelijk te maken. Deze verbetering zou het mogelijk maken:

- Route-samenvatting om het aantal geadverteerde voorvoegsels te verminderen
- Routefiltering om te bepalen welke voorvoegsels worden geadverteerd in AWS Direct

Connect

- Betere controle over BGP-advertenties vanaf de Secure Access-kant

Implementatiestappen

1: Bekijk de beperkingen van AWS Direct Connect. Raadpleeg de documentatie van AWS Direct Connect-limieten om de specifieke beperkingen te begrijpen.

2: Evalueer actuele routeadvertenties. Analyseer het huidige aantal routes dat wordt geadverteerd vanuit Secure Access om te bepalen hoeveel de 100-prefix AWS-limiet overschrijden.

3: Implementeer een onmiddellijke oplossing. Kies tussen AWS-filtering of Transit Gateway-implementatie op basis van netwerkarchitectuurvereisten en zakelijke behoeften.

4: Voortgang van het verzoek om functies controleren. Werk samen met de toepasselijke Cisco-accountteams om de haalbaarheid en impact van het voorgestelde verzoek voor routefiltering/samenvattende functies te beoordelen.

Oorzaak

De hoofdoorzaak is een fundamentele beperking in AWS Direct Connect, die BGP-routeadvertenties beperkt tot maximaal 100 voorvoegsels. Cisco Secure Access adverteert meer dan 100 routevoorvoegsels, waardoor AWS Direct Connect BGP NOTIFICATION-berichten met foutcode "Maximum aantal bereikte voorvoegsels" verzendt en vervolgens de BGP-sessie afbreekt. Dit creëert een cyclus van sessie-instelling en afbraak, resulterend in het waargenomen BGP-sessieflappergedrag.

Verwante inhoud

- Documentatie over beperkingen van AWS Direct Connect
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.