BGP-Sitzungsflapping aufgrund von Grenzwerten für Routenpräfixe beim sicheren Zugriff auf AWS Direct Connect-Integration

Inhalt

Problem

Bei BGP-Sitzungen kommt es zu Flapping in einem Site-to-Site-Tunnel zwischen Cisco Secure Access und AWS Direct Connect. Die Instabilität tritt auf, weil die Anzahl der von Secure Access angekündigten Routen-Präfixe die AWS Direct Connect-Grenzwerte überschreitet, wodurch ein stabiler Routenaustausch verhindert und die Fähigkeit beeinträchtigt wird, eine konsistente Verbindung zwischen Secure Access und AWS herzustellen.

Umwelt

- Cisco Secure Access (CSA)
- AWS Direct Connect mit BGP-Routing
- Site-to-Site-Tunnelkonfiguration zwischen Secure Access und AWS
- BGP-Präfixlimit für AWS Direct Connect von 100 Routen

Auflösung

Bei der Auflösung sind mehrere Ansätze erforderlich, um die Einschränkung des BGP-Präfixes zu erfüllen.

Bei der Netzwerkpaketanalyse werden BGP-BENACHRICHTIGUNGSNACHRICHTEN angezeigt, die darauf hinweisen, dass die maximale Anzahl an Präfixen erreicht wurde:

```
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)
```

Sofortige Problemumgehungen

Option 1: AWS-seitige Routenfilterung

Evaluieren Sie die AWS-seitigen Optionen, um eingehende Routenpräfixe von Secure Access zu ignorieren oder zu filtern und so innerhalb der durch AWS Direct Connect vorgegebenen 100-Präfixgrenze zu bleiben.

Option 2: AWS Transit Gateway-Implementierung

Ziehen Sie die Migration auf ein AWS Transit-Gateway als alternatives Verbindungsmodell in Betracht. Dieser Ansatz bietet flexiblere Routing-Optionen und kann dazu beitragen, die Beschränkungen des Direct Connect-Präfix zu umgehen.

Langfristige Lösung

Implementierung von Funktionsanforderungen

Es wurde eine Funktionsanforderung (CSE-I-4783) eingereicht, um eine Routenfilterung oder Zusammenfassungsfunktionen für sicheren Zugriff zu ermöglichen. Diese Erweiterung würde Folgendes ermöglichen:

- Routenzusammenfassung zur Reduzierung der Anzahl angekündigter Präfixe

- Routenfilterung, um zu steuern, welche Präfixe AWS Direct Connect angekündigt werden
- Bessere Kontrolle über BGP-Meldungen auf der Seite für sicheren Zugriff

Implementierungsschritte

1: Überprüfen Sie die Einschränkungen von AWS Direct Connect. Verweisen Sie auf die Dokumentation zu den AWS Direct Connect-Beschränkungen, um die spezifischen Einschränkungen zu verstehen.

2: Aktuelle Routenankündigungen auswerten. Analysieren Sie die aktuelle Anzahl der Routen, die von Secure Access angekündigt werden, um zu ermitteln, wie viele Routen den AWS-Grenzwert mit 100 Präfixen überschreiten.

3: Sofortige Problemumgehung Wählen Sie zwischen AWS-seitiger Filterung und Transit-Gateway-Implementierung basierend auf den Anforderungen der Netzwerkarchitektur und den geschäftlichen Anforderungen.

4: Überwachung des Fortschritts bei Featureanforderungen. Arbeiten Sie mit den zuständigen Cisco Account Teams zusammen, um die Machbarkeit und die Auswirkungen der Anfrage für die angebotene Routenfilterung/Zusammenfassung zu prüfen.

Ursache

Die Ursache liegt in einer grundlegenden Einschränkung in AWS Direct Connect, die BGP-Routenankündigungen auf maximal 100 Präfixe beschränkt. Cisco Secure Access meldet mehr als 100 Routenpräfixe, was dazu führt, dass AWS Direct Connect BGP-BENACHRICHTIGUNGSNACHRICHTEN mit dem Fehlercode "Maximum Number of Prefixes Reached" sendet und anschließend die BGP-Sitzung beendet. Dadurch wird ein Zyklus aus Sitzungsaufbau und -abbruch erstellt, der zu dem beobachteten Flapping-Verhalten der BGP-Sitzung führt.

Verwandte Inhalte

- AWS Direct Connect-Limitdokumentation
- 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.