セキュアアクセスIPプールサブネット割り当てとBGPルートアドバタイズメント

内容

お問い合わせ内容

/20サブネットで構成されたIPプールは、予期された2つの/21サブネットではなく、2つの/22サブネットがクラウドルートにインストールされていることを示しています。 この設定では、予想されるアドレス空間の半分しか提供されません。

環境

- テクノロジー：ソリューションサポート（SSPT – 契約が必要）
- サブテクノロジー：セキュアなアクセス
- 製品ファミリ：SECACCS
- ソフトウェアバージョン：すべて
- 設定：サブネット設定が/20のIPプール
- インフラストラクチャ：BGPルートアドバタイズメントを使用する2つのアクティブなVPNヘッドエンド

解決策

ユーザVPNプールサイジングとBGPアドバタイズメント

セキュアアクセスBGPは、/22より大きいプレフィクスをアドバタイズしません。 セキュアアクセスでリモートアクセスVPN(RAVPN)用のユーザVPNプールを設定すると、プラットフォームによってネットワークが適切に処理されます。

- 指定されたネットワークが/22（/20など）より大きい場合、プラットフォームは自動的にネットワークを複数の/22チャンクに内部的に分割します。

例： /20プールを指定します。 Secure Accessは、これを内部で4 × /22サブネットに分割します。 各/22は、地域のデータセンターによってオンデマンドでリースされます。 データセンターが/22をリースするとき、その/22（またはそれ以下）のみをBGP経由でアドバタイズし、完全な/20はアドバタイズしません。

- 提供されたネットワークが/22以下（/24など）の場合、プラットフォームはネットワークを少なくとも2つの小さなサブネットに分割し、地域の少なくとも2つのデータセンター間で高可用性をサポートします。

例： /24プールを提供します。 Secure Accessは、これを2 ×/25サブネットに分割します。 各/25は、地域の異なるデータセンターに割り当てられます。 各データセンターは、それぞれの

/25をBGP経由でアドバタイズします。

VPNプールサブネットは、同時にアドバタイズされません。 代わりに、RAVPNクライアント接続の数が増えるに従って、オンデマンドで割り当ておよびアドバタイズされます。

- 最初は、最初のサブネット（/20の最初の/22など）だけがリースされ、BGPを介してアドバタイズされます。
- 需要が高まるにつれて、追加のサブネットがデータセンターによってリースされ、アドバタイズされます。
- これは、クラウドリソースを動的に拡張する方法と一致しています。

例： /20の範囲をカバーする4つの× /22プールを設定します。 接続ボリュームが小さい場合、BGPは最初の/22だけをアドバタイズします。 RAVPN接続が増加すると、残りの/22プールが徐々にアクティブ化され、アドバタイズされます。

重要：設定したプールの1つだけがアドバタイズされているのであれば、これは正常な動作です。 追加のプールは、拡張要求に応じてアドバタイズされます。

要約

提供されたプールサイズ	内部分割	BGPアドバタイズメント	原因
/22より大きい（/20など）	複数の/22に分割(4 × /22など)	各/22以下、オンデマンド	アドバタイズされる最大プレフィックスは/22です。オンデマンドのスケーリング
/22	2つ以上の小さなサブネットに分割する	小さいサブネットごとにオンデマンド	≥2データセンター全体の高可用性
/22より小さい（/24など）	少なくとも2つのサブネットに分割する(2 × /25など)	各サブネット、オンデマンド	≥2データセンター全体の高可用性

- アドバタイズされる最大BGPプレフィックス： /22：セキュアアクセスは、BGP経由で/22を超えるネットワークをアドバタイズしません。
- 自動分割：ネットワークは内部的に分割され、ハイアベイラビリティ（地域ごとに2つ以上のデータセンター）と拡張性を実現します。
- オンデマンドアドバタイズメント：サブネットは、接続を処理するためにデータセンターによってアクティブにリースされた場合にのみ、BGPを介してアドバタイズされます。 すべてのプールが同時にBGPに表示されるわけではありません。
- 拡張は動的：クラウドネイティブのリソース拡張原則に従って、RAVPNクライアント接続の数が増加すると、追加のプールサブネットがアクティブ化されます。

原因

これは、Secure Access Systemのサブネット割り当てアルゴリズムの設計上の動作です。 このシステムは、設定されたサブネットをサイズの小さい同じサイズのサブネットに自動的に分割し、辞書編集上の並べ替えを使用して使用可能なVPNヘッドエンド全体に分散することで、一貫性の

ある予測可能な割り当てパターンを実現します。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。