ゼロトラストアクセスおよびVPN接続のための地理的アクセス制限

内容

お問い合わせ内容

ゼロトラストアクセス(ZTA)およびVPN接続に地理的なアクセス制限を必要とする組織では、国ベースのアクセス制御を実装しようとする際に、既存のZTAおよびVPNポリシーを無効にする必要があります。Secure SSE製品のインターフェイス内でネイティブの地理的制限オプションを見つけられないためにポリシーが無効になっていると、必要なリソースへのアクセスが完全に失われます。特定の国内からのみの接続へのアクセスを制限する特定の要件は、組み込みの製品機能を使用して設定することができません。そのため、このような制限を実装しようとして既存のポリシーを無効にした場合、ユーザに広範な影響が生じます。

環境

- Cisco Secure Access Service Edge(SASE)/Secure SSE製品
- ゼロトラストアクセス(ZTNA)の実装
- 地理的なアクセス制御を必要とするVPNサービス
- プライベートリソースアクセスポリシー
- 国別のアクセス制限が必要な組織

解決策

現在、Cisco Secure SSE製品には、ユーザの地理的な場所または国に基づいてプライベートリソースへのアクセスを制限するネイティブ機能がありません。次のセクションで説明するアプローチは、この制限に対処するものと考えることができます。

機能要求の送信

ZTAおよびVPNアクセスの地理的制限機能を追加するには、機能要求をシスコに送信する必要があります。この機能拡張要求は、今後のリリースに含まれる可能性について製品チームによって評価されます。組織は、シスコアカウントマネージャと連携して、ビジネス要件に基づいてこのような機能のリクエストに優先順位を付けることができます。

手動による回避策の検討

手動による回避策としては、アクセスポリシーでネットワークオブジェクトグループとして国固有のパブリックIPアドレス範囲を追加することが考えられます。

ステップ1：適切な地域インターネットレジストリ(RIR)から国のパブリックIPアドレス範囲を取得します。

手順2：指定されたIP範囲を含むネットワークオブジェクトグループを作成します。アクセスポリシー設定内でネットワークオブジェクトグループを設定し、ターゲット国に割り当てられた特定のIPアドレス範囲を含めます。

ステップ3：ネットワークオブジェクトグループをアクセスポリシーに適用します。作成されたネットワークオブジェクトグループを参照するように既存のアクセスポリシーを変更し、指定されたIP範囲から発信された接続へのアクセスを効果的に制限します。

重要な制限

この手動のアプローチは、静的なIP範囲の定義に依存し、地理的な制限をバイパスする可能性のある動的なIP割り当て、モバイルユーザ、またはVPNサービスを考慮できないため、非常に制限があります。また、この方法では、IP範囲の精度を確保するために継続的なメンテナンスが必要です。

一時的なポリシー管理

恒久的なソリューションが利用可能になるまで、組織はすべてのZTAポリシーとVPNポリシーを

同時に無効にすることを避ける必要があります。その代わりに、別の手段を使用して、または製品の拡張を待っている間も重要なアクセスポリシーをアクティブに保ちながら、地理的な制限の要件に対処する段階的アプローチの実装を検討してください。

原因

Cisco Secure SSE製品のアーキテクチャには、プライベートリソースアクセス用のネイティブな地理的アクセス制御機能は含まれていません。製品アクセスポリシーフレームワークは、ユーザID、デバイスポスチャ、およびネットワークベースの制御を中心に設計されていますが、ポリシー適用パラメータとして地理的な場所は組み込まれていません。これは、設定の問題やソフトウェアの不具合ではなく、製品の機能のギャップを表しています。

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。