

ZTNAクライアントレス送信元IPアドレスの制限

内容

お問い合わせ内容

ZTNAクライアントレスを介して公開されるブラウザベースのアプリケーションに対してアクセス制御を実装しようとする、特定の許可リストに掲載されたパブリックIPアドレスに基づいてアクセスを制限する機能が設定オプションとして利用できないことがわかります。要件は、カスタムドメインを使用してZTNA Clientless経由でアクセスするアプリケーションの他のすべての送信元IPをブロックしながら、指定された送信元IPアドレスからのアクセスのみを許可することです。

環境

- Cisco Secure Access - Zero Trust Network Access(ZTNA)
- ZTNAクライアントレス (ブラウザベースのアクセス)
- カスタムドメインを使用して公開されたアプリケーション
- すべてのソフトウェアバージョンが該当

解決策

ZTNAクライアントレスURLの送信元IPアドレスベースのアクセス制限は、Cisco Secure Accessプラットフォームではサポートされていません。この制限は、カスタムドメインまたは標準のZTNA URLのどちらを使用するかに関係なく、ZTNAクライアントレスを通じて公開されるすべてのアプリケーションに適用されます。

ZTNAクライアントレスアーキテクチャは、アプリケーションレベルでIPベースのアクセスコントロールリスト(ACL)または許可リスト機能を実装する機能を提供しません。アクセスコントロールは、ゼロトラストフレームワーク内の次のような他の認証および認可メカニズムによって管理

されます。

- ユーザIDの検証
- デバイスポスチャ評価
- 多要素認証
- アプリケーション固有のポリシー

発信元IPベースのアクセス制御を必要とする組織は、代替アプローチを検討するか、またはこの機能を含む可能性のある将来の製品拡張を待つ必要がある可能性があります。機能拡張要求を提出するために、シスコアカウントチームに連絡してください。

原因

ZTNAクライアントレスサービスアーキテクチャには、現在の機能セットの一部として、送信元IPアドレスのフィルタリング機能は含まれていません。これは、設定の問題ではなく、製品の制限です。

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。