

Secure Clientを使用したクライアントベースのZTNAトラフィックステアリングの問題

内容

お問い合わせ内容

クライアントベースのゼロトラストネットワークアクセス(ZTNA)では、FQDNまたは直接IPアドレスでアクセスされた場合に内部アプリケーションへのアクセスを提供できませんが、同じアプリケーションにはVPN接続を介して到達できます。

確認された具体的な症状は次のとおりです。

- VPNが切断されると、セキュアクライアントZTNAはFQDNまたは直接IPで内部アプリケーションに到達できません。
- ブラウザベースのZTNAアクセスは、同じアプリケーションに対して正しく機能します。
- VPNがダウンしている場合、アクティビティログにZTNAイベントは表示されません。これは、クライアントトラフィックがZTNAパス経由でルーティングされていないことを示します。
- プライベートアプリケーション定義は、VPNでルーティング可能なリソースと正しいIP/ポート/FQDN設定が一致することが確認されています。
- ZTNAポリシーは、テストユーザとグループの割り当てに一致することが確認されています。

この問題は、特にセキュアクライアントZTNAトラフィックのステアリングまたは適用メカニズムを分離します。ブラウザベースのZTNAが、バックエンドの公開と適用が正常に機能していることを検証するためです。

環境

- テクノロジー：セキュアアクセス – ゼロトラストネットワークアクセス(ZTNA)

- コンポーネント：クライアントベースのZTNA、ポスチャ、登録、プライベートリソースアクセス
- VPNプロファイルが共存するセキュアクライアント
- FQDNと直接IPアドレッシングの両方を使用してアクセス可能なプライベートアプリケーション
- ブラウザベースのZTNA機能が動作していることを確認
- Most Specific Match Enforcementモードで設定されたポリシーの適用

解決策

この問題を解決するには、ZTAプロファイルの設定を調整し、ポリシーを検証する必要があります。次のセクションで説明する手順は、クライアントベースのZTNA機能を復元するために実行されたものです。

ステップ1:ZTAプロファイルへのプライベートリソースの追加

プライベートリソースがZTAプロファイル設定に追加されました。この変更の後、ブロックされたイベントがアクティビティログとスクリーンショットに表示され始め、クライアントトラフィックがZTNAパスを正しくルーティングされていることを示します。

ステップ2：ポリシーの検証とテスト

一時的な「permit any」ルールが追加され、トラフィックフローが検証されました。このルールがアクティブである間、クライアントベースのZTNAアクセスは正しく機能し、トラフィックのステアリングメカニズムは機能しているが、ポリシーを適用するには調整が必要であることを確認しました。

ステップ3：ポリシーの絞り込み

一時的なpermit-anyルールが削除され、特定のアクセスポリシーが検証されました。プライベ

トリソースは、プラットフォームのMost Specific Match Enforcement Modeを使用して、Private Resources_Cyrilという名前のアクセスポリシーでアクセス可能であることが確認されました。

ステップ4：設定の検証

ユーザは、クライアントベースのZTNAアクセスが、設定の変更後に一貫して機能し始めたことを確認しました。この問題は、追加のポリシー変更やシステム変更を必要とせずに解決されました。

原因

根本的な原因は、ZTAプロファイルのプライベートリソース設定が不完全であることでした。ZTAプロファイルで適切なプライベートリソースが定義されていないと、クライアントトラフィックはZTNA強制パスを通じて転送されず、ローカルルーティングメカニズムにフォールバックされます。これにより、トラフィックがZTNAポリシーを完全にバイパスすることになり、VPNが切断されたときにアクティビティログにZTNAイベントが表示されない理由が説明されました。

この問題は、クライアントベースのZTNAトラフィックステアリング設定に特有のもので、ブラウザベースのZTNAは、適切に設定された別のトラフィック処理メカニズムを使用するため、引き続き機能します。

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。