ZTNAクライアント – ネットワークインターセプターエラー

内容

お問い合わせ内容

Cisco Secure Access Zero Trust Access(ZTNA)を介してプライベートリソースにアクセスしようとすると、ネットワークインターセプタエラーが発生する。 このエラーにより、ゼロトラストアクセス環境内で設定されたプライベートリソースへの接続が正常に行われず、内部アプリケーションおよびサービスへのアクセスが完全に失われます。

環境

- テクノロジー：Cisco Secure Access - Zero Trust Access(ZTNA)
- ソフトウェアバージョン：5.1.14
- 製品ファミリ：SECACCS
- エラータイプ：ネットワークインターセプターエラー
- 影響：重大 – プライベートリソースへのアクセスが完全に失われる
- 最近の変更：レポートされていません

解決策

これはDARTログで確認できます。

++次のログが見つかりました：

E/ ZtnaKdfConfigurator.cpp:208 ZtnaKdfConfigurator::StartIntercept() IZtnaApi::SetParametersがエラーコード=BadParameterで失敗しました

2026-03-02 11:33:30.933701 csc_zta_agent[0x000020fc/config_enforcer, 0x00001994] E/ ZtnaConfigEnforcer.cpp:444 ZtnaConfigEnforcer::applyActiveSteeringPolicy()がZTNAインターセプトを開始/更新できませんでした

2026-03-02 11:33:30.933701 csc_zta_agent[0x000020fc/config_enforcer, 0x00001994] I/ ZtnaConfigEnforcer.cpp:145 ZtnaConfigEnforcer::reportInterceptorConnectivityChange()レポートKDF到達可能性： ConfigFailed

DARTのキャッシュされた構成

この問題の原因となる末尾のスペース(cisco.com)が導入されています。

- さらにテストを行った結果、プライベートリソース構成のリモート到達可能アドレスオプシ

ョンとリモート到達可能アドレスフィールドの選択が変更されていないか、内部的に到達可能なアドレスと同じ値であることが判明しました。この設定は保存時に無効になります。
- ただし、リモート到達可能アドレスフィールドがチェックされたときに、リモート到達可能なアドレスのFQDNに余分な空白があり（たとえば、「cisco.com」と「cisco.com」の対比）、設定を保存できたと思われます。
- デフォルトのゼロトラストプロファイルが使用されていたため、新しく作成されたプライベートリソース設定または既存のプライベートリソース設定が組織内のすべてのユーザにプッシュされ、この空白文字を含む設定が同期されました。 この空白が原因で、クライアントに表示されていた「Network Interceptor」エラーが発生します。
- この問題を当分の間、解決するには、プライベートリソースに移動し、リモートで到達可能なアドレスのFQDNに空白文字が含まれていないことを確認します。

原因

Cisco Secure Access Zero Trust Accessのネットワークインターセプタエラーは、通常、ZTNA環境内のプライベートリソース定義の設定ミスまたは問題が原因で発生します。 リモートで到達可能なアドレスフィールドがチェックされたとき、リモートで到達可能なアドレスのFQDNに余分な空白が含まれていました（たとえば、「cisco.com」と「cisco.com」の比較）。

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。