

ZTAブラウザベースのプライベートリソース TLSハンドシェイクの失敗

内容

問題

ユーザは、Cisco Secure Accessを介してブラウザベースのプライベートリソースにアクセスできません。

接続しようとする、次の症状が発生します。

- TCP 3ウェイハンドシェイクは正常に完了するが、Client Helloの後、TLSネゴシエーションが失敗する。
- SSEでマッピングされたパブリックURL(<https://example-orgid.ztna.sse.cisco.io>)への接続がCisco認証に到達しますが、HTTP 404エラーが返されます。
- FQDNをプライベートリソース設定に追加すると、トラフィックは認証プロンプトにリダイレクトされますが、認証後に空白のページが表示されます。
- HARファイルにはHTTP 200応答が表示されますが、TLSハンドシェイクは完了しません。
- ブロックの理由は、「Private Access: fetched posture data for device is too old/needs to be refreshed」と表示されます。

環境

- シスコセキュアアクセス(SSE)
- Secure Access組織ID:xxxx
- ブラウザベースのゼロトラストネットワークアクセス(ZTNA)
- プライベートリソース : example.net

- 比較のための作業プライベートリソース : abc.net
- ワイルドカード証明書の設定

解決方法

この問題は、プライベートリソースを設定して、動作中のプライベートリソースと同じ証明書の設定を使用することで解決されました。

次のセクションで説明する手順を実行しました。

ステップ1 : 動作している設定の分析

障害が発生したプライベートリソース(example.net)と動作しているプライベートリソース(abc.net)を比較して、設定の違いを特定します。

使用される作業リソース :

- ドメインオプションでURLを使用する
- 既存のワイルドカード証明書/キーペアへの参照

ステップ2 : パケットキャプチャ分析

Wiresharkを使用してパケットキャプチャ分析を実行し、TLSハンドシェイクの失敗を確認します。

- TCP 3ウェイハンドシェイクが正常に完了することを確認します。
- Client Helloの後、TLSネゴシエーションが失敗することを確認します。
- 診断アーティファクト (HARファイル、DARTバンドル、パケットキャプチャ) の収集

ステップ3：証明書の検証

RAVPN接続経由でアプリケーションにアクセスし、証明書の表示を確認します。

- Webサイトexample.netがワイルドカード証明書を提示していることを確認します。
- 設定の参照用に証明書の詳細を文書化します。

ステップ4：プライベートリソースの設定

稼働中のプライベートリソースと同じ設定方法を適用します。

- Use a URL in your domainオプションを使用するように、プライベートリソースを設定します。
- 既存のワイルドカード証明書/キーペアを参照します。
- プライベートリソースフィールドでFQDNが正しく設定されていることを確認します。

ステップ5：検証

ブラウザベースのアクセスをテストして、設定が問題を解決したことを確認します。

- TLSハンドシェイクが正常に完了したことを確認します。
- 適切な認証フローを確認します。
- 認証後にアプリケーションのアクセシビリティを検証します。

原因

根本的な原因は、プライベートリソースのセットアップでの設定の不一致でした。失敗したプライベートリソースは、ターゲットアプリケーションが提示していたワイルドカード証明書を正しく参照するように構成されていませんでした。プライベートリソースの構成が、アプリケーション

ンサーバーで使用される証明書の構成と一致しなかったため、TLSハンドシェイクに失敗しました。「Use a URL in your domain」オプションを使用するようにプライベートリソースを設定し、既存のワイルドカード証明書/キーペア（実際の設定と一致）を参照することで、TLSネゴシエーションは正常に完了します。

関連コンテンツ

- [セキュアアクセスに関するシスコリファレンスガイド](#)
- [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。