セキュアなアクセスによるOmnissaのクライアント接続に関する問題

内容

お問い合わせ内容

Omnissaフルクライアントは、Cisco Secure Access経由で接続すると仮想デスクトップをロードできません。完全なクライアントアプリケーションを使用して仮想環境への接続を確立しようとすると、接続エラーが発生する。ただし、HTML/Webクライアント経由のアクセスは引き続き正常に動作します。これは、基盤となる仮想デスクトップインフラストラクチャは機能しているが、Cisco Secure Accessソリューション経由で接続を確立するクライアントの機能に影響を与える特定の問題があることを示しています。

環境

- テクノロジー：ソリューションサポート（SSPT – 契約が必要）
- サブテクノロジー：Cisco Secure Access
- 製品ファミリ：SECACCS
- ソフトウェアバージョン：該当するすべてのバージョン
- クライアントアプリケーション：Omnissaフルクライアント
- 仮想デスクトップ環境：オムニッサの仮想デスクトップ
- ネットワークインフラストラクチャ：IPsecトンネルおよびFTD(Firepower Threat Defense)

解決策

この問題を解決するには、Cisco Secure Accessを介してOmnissaフルクライアントの適切なルー

ティングを有効にするために、特定のネットワーク設定を変更する必要があります。接続の問題を解決するために、次の手順が実行されました。

- スプリットトンネルの設定を行います。Omnissaフルクライアントが必要な宛先ホストへの直接接続を確立できるように、スプリットトンネル設定を追加します。この設定により、特定の仮想デスクトップクライアント宛てのトラフィックが適切なネットワークパスを介して適切にルーティングされるようになります。
- スタティックルートの設定を実装する。仮想デスクトップへの接続を確立する必要がある特定のクライアントのスタティックルートを設定します。主な要件は、集約サーバのダウンストリームへのルートだけでなく、仮想デスクトップクライアントが到達する必要がある宛先ホストへのルートを直接設定することです。
- IPSecトンネルをクリアします。設定変更を実装した後、FTDでIPsecトンネルをクリアし、新しいルーティング設定が正しく有効であることを確認します。
- 接続を検証します。変更を実装した後にOmnissaのフルクライアント接続をテストし、Cisco Secure Accessを介して仮想デスクトップ接続が正常に確立できることを確認します。

実装スケジュール

設定変更は、ユーザへの影響を最小限に抑えるために、スケジュールされたメンテナンスの時間帯に実施する必要があります。実装後に、到達可能性とOmnissaの完全なクライアント接続の両方を検証し、解決が成功することを確認します。

原因

この接続の問題は、Cisco Secure Access環境でのルーティング設定が不十分であることが原因で発生しました。具体的には、ネットワークには集約サーバのダウンストリームへのルートのみが設定されていますが、Omnissaフルクライアントが接続を確立するために必要な特定のクライアントに対するスプリットトンネルとスタティックルートの設定が不足していました。このルーティングギャップにより、クライアント全体が仮想デスクトップホストに適切に到達できませんでしたが、HTML/Webクライアントは、適切に設定されたさまざまな接続パスを使用したため、機能し続ける可能性があります。

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。