セキュアアクセスVPN:Jabberにアクセスできない

内容

お問い合わせ内容

プライベートアクセスポリシーの使用時に、セキュアアクセスVPNトンネル経由でJabberやEpicなどの内部アプリケーションとプライベートアプリケーションにアクセスできませんでした。ユーザがVPN接続を介してこれらの重要なビジネスアプリケーションにアクセスしようとすると、接続障害が発生します。トラブルシューティングの際、Epicリソースで単一方向トラフィックが観測されました。このリソースでは、セキュアアクセスVPNトンネルからpingおよびTCP SYNトラフィックが出力されていましたが、Palo Altoファイアウォールでリターントラフィック検証の問題が見つかりました。さらに、トラフィックステアリングがIPベースルーティング用に設定されている間にCUCM FQDNが内部DNSを介して解決され、トラフィックフローの不一致が発生するJabber到達可能性の問題が文書化されました。

環境

- VPNトンネルを使用したCisco Secure Accessの設定
- VPN接続用のセキュアクライアント
- プライベートアクセスポリシーの実装
- Cisco Unified Communications Manager(CUCM)for Jabberサービス
- Epicアプリケーションリソース
- Palo Altoファイアウォールによるネットワークセキュリティ
- CUCM FQDNの内部DNS解決

解決策

この問題を解決するには、複数の設定変更と、セキュアアクセスVPNトンネルを介して内部アプリケーションへの接続を復元するトラブルシューティング手順が必要でした。

サブネットの設定とトンネルの変更

ステップ1:VPNトンネルにサブネットを追加する

影響を受けるリソースのVPNトンネル設定にサブネットが追加されました。この変更を実装した後、以前はアクセスできなかったリソースのロードが正常に開始されました。

CUCM IPアドレスのステアリング設定

ステップ2:CUCM IP Steeringの設定

トラフィックのステアリングがIPベースの場合にCUCM FQDNが内部DNSを介して解決されるJabber接続の問題を解決するために、CUCM IPアドレスがセキュアクライアントにステアリングされました。この設定変更により、DNS解決とトラフィックステアリングメカニズムが調整されました。

ステップ3：アクセスポリシールールの作成

アクセスポリシールールが作成され、CUCM IPアドレスへの到達可能性が許可されました。このルールにより、CUCMインフラストラクチャへの適切な接続が復元され、VPNトンネル経由でのJabber機能が有効になりました。

スタティック ルーティングの設定

ステップ4:CUCMサブネットのスタティックルーティングを設定します。

CUCM IPアドレスとCUCMサブネット全体がネットワークトンネルのスタティックルーティングテーブルに含まれていることを確認します。この設定により、セキュアクライアントユーザプールとCUCMインフラストラクチャ間のトラフィックが適切にルーティングされます。

リターントラフィックの検証

ステップ5：パケットフローとリターントラフィックの検証

パケットフローの設定を検証して、リターントラフィックがセキュアクライアントユーザプールに到達できることを確認します。これには、すべての内部リソース、特に単方向トラフィックが観測されたEpic接続に対して適切なリターンパス検証を保証するためのPalo Altoファイアウォール設定のレビューが含まれます。

原因

接続の問題は、セキュアアクセスVPNの実装における複数の設定ギャップが原因で発生しました。

- VPNトンネルでサブネット設定が欠落しているため、内部アプリケーションリソースへの適切なルーティングが妨げられている
- CUCMサービスのDNS解決（FQDNベース）とトラフィックステアリング設定（IPベース）の間で不一致が発生し、Jabber接続障害が発生しました
- CUCM IPアドレスへのトラフィックを許可しなかったアクセスポリシールールが不完全です。
- ネットワークトンネル設定にCUCMサブネットのスタティックルーティングエントリがない
- 双方向通信に影響を与えるPalo Altoファイアウォールでのリターントラフィックパス検証の問題

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。