リモートアクセスユーザがRAVPN経由で内部サービスにアクセスできない

内容

お問い合わせ内容

セキュアアクセスを使用しているリモートアクセスユーザは、インターネットアクセスが正常に機能している間に、本社のドメインコントローラを含む内部サービスにアクセスできませんでした。ユーザはインターネットを正常に閲覧できましたが、RAVPN（リモートアクセスVPN）経由でドメインコントローラなどの内部リソースにアクセスできませんでした。

環境

- Cisco Secure Access – セキュアクライアントリモートアクセス（VPN、ポスチャ、プライベートリソース）
- アップ状態で正常であると報告されたRAVPN（リモートアクセスVPN）トンネル
- 使用中のSD-WANインフラストラクチャ
- 本社の内部DNSサーバ
- 本社ロケーションのドメインコントローラサービス
- インフラストラクチャ経由で接続された複数のブランチネットワーク

解決策

リモートアクセス接続の問題に対処するために、次のトラブルシューティング手順と解決手順を実行しました。

ステップ1：パケットキャプチャの分析

クライアントとエッジデバイスから同時パケットキャプチャ（双方向）を収集し、トラフィックフローパターンを分析します。

Flow:

RA VPNクライアント----------Cisco Secure Access --------Ipsecトンネル----------エッジデバイス--------プライベートリソース

- クライアントからのDNSクエリがエッジデバイスに正常に到達し、DNSサーバに送信されているかどうかを確認します。
- ローカルDNSサーバからクライアントにDNS応答が返されないことが確認される
- ローカルDNSサーバは応答を送信しましたが、これらの応答はトンネルインターフェイスに返されませんでした。

ステップ2：根本原因の特定

パケットキャプチャ分析に基づいて、この問題はリターンパスルーティングの問題として特定されました。トラフィック分析では、DNSクエリがCisco Secure Accessインフラストラクチャを介してローカルDNSサーバに正常に到達しているのに対し、DNS応答を含むリターントラフィックは、インフラストラクチャのルーティングまたは設定の問題が原因でリモートアクセスクライアントに到達していないことが示されました。

ステップ3：設定のレビューと修復

内部ネットワーク設定と内部ネットワーク設定をレビューして修正します。特に、次の点に重点を置きます。

- DNS設定とリターントラフィックルーティング
- VPNリターントラフィックの内部ルーティングポリシー
- 内部ネットワークルーティングの設定

- エッジデバイス側で構成要素が欠落している

ステップ4：サービス復旧の検証

設定のレビューと修正を行った後、セキュアアクセス機能が大幅に復元されました。ほとんどのリモートアクセスユーザは、本社のドメインコントローラを含む内部サービスに再びアクセスできるようになりました。

原因

根本原因は、内部ネットワークインフラストラクチャ内のリターンパスルーティングの問題として特定されました。リモートアクセスクライアントからのDNSクエリがCisco Secure Access Infrastructureを介してローカルDNSサーバに正常に到達する一方、DNS応答を含むリターントラフィックがクライアントに正しくルーティングされませんでした。これは、内部ネットワークインフラストラクチャ側の設定が欠落しているか正しくないため、VPN接続を介してDNS応答とTCP応答がリモートアクセスクライアントに到達できないことが原因です。

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。