VPN Client Unable to Successfully Verify IP Forwarding Table Modification」エラー( ):Secure Client RAVPN Split-Tunnel/Default DNS

内容

お問い合わせ内容

Cisco Secure Client VPNに接続しているときに、Macユーザが内部アプリケーションに対してCLI認証を試行すると、断続的な障害が発生します。 この障害は、CLI認証中および`curl`などのコマンドの使用時に、「host not found」エラーとして表示されます。 ただし、`nslookup`や`dig`などのDNS解決コマンドは成功します。 この問題はランダムに発生し、VPNを再接続することで一時的に解決できます。その後、接続は問題が再発する前に短期間機能します。 スプリットトンネルVPNが使用されており、Cisco Umbrellaがアクティブです。 Palo Alto GlobalProtect VPNを使用している場合は、この問題は発生しません。

- CLI認証および`curl`コマンドのエラーメッセージ：「host not found」
- エラーメッセージ：VPN client unable to successfully verify IP forwarding table modifications. プライベートリソースの接続中のドメインネームサーバ(DNS)解決の問題
- `nslookup`コマンドと`dig`コマンドが成功する
- VPN再接続後の断続的な接続
- スプリットトンネルリモートアクセスVPNおよびUmbrellaモジュールが有効
- MacOSデバイス上のCisco Secure Client VPNでのみ再現可能な問題

環境

- 製品：Cisco Secure Client(CSC)と複数のモジュール
- プラットフォーム：企業のMacデバイス
- VPNプロファイルの設定：リモートアクセスVPNプロファイル：セキュアアクセスのバイパス：スプリットトンネルモードとDNSモードが「Default DNS」として選択されている
- DNSフィルタリング：Cisco Umbrella対応
- モジュールバージョン：
  - クラウド管理v1.0.0.23
  - AnyConnect VPN v5.1.13.177
  - 包括v5.1.13.177
  - DART v5.1.13.177
  - セキュアファイアウォールポスチャv5.1.13.177
  - Network Visibility Module v5.1.13.177
- 診断データ：分析用に収集されたDARTバンドル
- Cisco Secure Client VPNでのみ確認（Palo Alto GlobalProtectでは未確認）

解決策

- VPNプロファイル(naic.org)スプリットトンネル設定とクライアント側のAnyConnect VPNルーティングテーブルのデバッグ中に、次の動作が見られました。
  - 作業シナリオ：Vaultの非実稼働ローカルドメインに対してnslookupを実行すると、VPNプロファイル内に設定されたDNSサーバによって処理されるDNS要求は、10.xアドレスに正しく解決されました。 これに応じて、ルーティングテーブルは、セキュリティで保護されていないルートの解決済みIP（たとえば、10.59.130.193）で更新されました。
  - 動作しないシナリオ：ただし、同じDNS要求が、VPNプロファイルで定義されたDNSサーバではなく、untun4およびen0アダプタ上で設定されたmacOSシステムのローカルDNS(192.168.x.x)で処理された場合、この動作は問題が認識されている間にパケットキャプチャから明確に観察されました。
  - プライベートドメインは34.x.x.xのIP範囲に解決され、これが接続の問題を引き起こした。 Wiresharkのキャプチャは、この問題の根本的な原因を特定するのに役立ちました。
- 設計および設定の観点から、スプリットトンネルVPNプロファイル設定では、ローカルシステムのDNS/デフォルトDNSに依存するのではなく、スプリットDNSを使用することを推奨します。
- また、us-east-eks-amazonaws.comエントリが追加されたため、このEKSクラスタのトラフィックがリモートトンネルインターフェイスを通じて正しく転送されます。
- また、RAVPNインターフェイスはUmbrellaモジュールよりも優先される必要があり、Umbrella組織IDを含むOrgInfo.jsonファイルと競合しないようにする必要があることについても説明しました。
- トラブルシューティングプロセス中に、UmbrellaモジュールなしでCSCクライアントの新規インストールを実行しましたが、そのシナリオでは問題を確認できませんでした。 Umbrellaの観点からも確認できました。内部ドメインリストでUmbrellaをバイパスするように設定されたルートドメインnaic.orgです。これは、カーネルレベルのループバックインターフェイスでUmbrella DNSモジュールによって代行受信されない、macOSが設定されたシステムDNSにローカルドメインの解決が転送されることを意味します。

これは、Umbrellaモジュールが取り付けられていない場合の問題の解決と一致します。 トラフィックステアリングルールとスプリットDNS設定に正しいドメインを含む適切なVPNプロファイル設定を使用すると、Umbrellaモデルがオンになっていても問題が発生しないはずです。

ユーザは、DNSモードをスプリットトンネルに変更し、VPNプロファイル設定を編集した後、問題が解決されたことを確認しました。

原因

VPNプロファイル – セキュアアクセスのバイパス – DNSモードはスプリットトンネル（ユースケースのシナリオで最もよく見られるオプション）に設定され、すべてのプライベート/内部アプリケーションドメインをスプリットDNS設定の下に含めることで問題を解決します。

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。