リモートアクセスVPN用のiOS上のCisco Secure ClientでのDNSロギングおよびデバイス登録動作

内容

お問い合わせ内容

iOS(iPad)でCisco Secure Clientを使用し、Microsoft Entra IDによるSAML認証を使用してCisco Secure Accessとのリモートアクセスvpnを確立する場合、ファイアウォールとWebログが正しく生成されていても、VPN接続が成功した後にDNSログがSecure Accessに表示されません。また、VPN接続を確立した後、セキュアアクセスダッシュボードのRoaming Devices > Mobile Devicesの下にiPadが表示されません。

確認された具体的な症状は次のとおりです。

- リモートアクセスログに、セキュアアクセスで成功した「接続」イベントが表示される
- ファイアウォールおよびWebログが生成され、SAML認証されたユーザIDが表示されます
- DNSログがセキュアアクセスロギングから完全に欠落している
- iPadデバイス情報は、セキュアアクセスローミングデバイスセクションには入力されません
- すべてのトラフィックフローがVPNトンネルを通過する（スプリットトンネリングは設定されない）

環境

- iOS 26.2を実行しているiPad
- Cisco Secure Client
- アイデンティティプロバイダー： Microsoft Entra ID
- セキュリティコネクタ：インストールされていません

- SSO認証が設定されたCisco Secure Access
- SAML認証の実装
- DNSモードがデフォルトに設定されたVPNプロファイル
- スプリットトンネリングが設定されていない（すべてのトラフィックがVPN経由でルーティングされる）
- プロファイル配信に使用されるMobile Device Management(MDM)

解決策

文書化された設定では、確認された動作が予想されます。iOS上のCisco Secure ClientはVPNクライアント（AnyConnectと同等）として機能し、デフォルトではRSMと同等の機能を含みません。セキュリティコネクタは、iOS上のRSMと同等のコンポーネントで、エンドポイントIDの入力と包括スタイルのDNS制御に必要です。

アーキテクチャについて

DNSログおよびデバイス登録が存在しないのは、次の理由によります。

- Cisco Secure Clientは単独でVPN接続を提供しますが、DNSの可視性に必要なエンドポイントエージェント機能がありません
- セキュリティコネクタ（WindowsのRSMに相当）は、セキュアアクセスでのDNS制御およびデバイス登録に必要です
- Security Connectorを使用しない場合、DNSクエリはVPNで取得されたDNSサーバで処理され、Umbrella/Secure Accessは表示されません

トラフィック操作によるDNSロギングソリューション

セキュリティコネクタをインストールせずにDNSロギングを有効にするには、DNSクエリをUmbrella DNSサーバに送信するようにトラフィックステアリングを設定します。

ステップ1：セキュアアクセスでトラフィックステアリングを設定します。

Traffic Steering > Add > Add a sourceの順に移動し、送信元としてDNSサーバのIPを指定します。

ステップ2:DNSトラフィックをUmbrellaサーバに送信する

Umbrella DNSサーバ（208.67.222.222および208.67.220.220）を使用してDNSクエリがセキュアアクセスに表示されるようにVPNプロファイルを設定します。

手順3: DNSログを検証する

トラフィックステアリングの設定を実装すると、VPNセッションのDNSログがセキュアアクセスダッシュボードに表示されるようになります。

VPNプロファイルのDNSモード設定

VPNプロファイルの「DNS Mode」設定は、この設定にDNSログが存在しないことに関係しません。RAVPN（リモートアクセスVPN）セッションでは、この設定に関係なく、VPNで取得されたDNSサーバが使用されます。ロギングの可視性は、DNSトラフィックが監視対象のDNSインフラストラクチャに送信されるかどうかによって異なります。

セキュリティコネクタのインストールオプション

Security ConnectorをiOSにインストールすると、次のことが可能になります。

- Secure AccessでのDNSロギングの可視性
- 強化されたエンドポイントIDおよびデバイス登録機能
- 包括的なDNS制御と保護

セキュリティコネクタはSecure Clientと組み合わせて使用できますが、2つのコンポーネント間の競合を防ぐには、トラフィックの除外と設計に関する適切な考慮事項が必要です。

原因

根本的な原因はアーキテクチャにあります。iOS上のCisco Secure ClientはVPN接続を提供しますが、Secure AccessでのDNSの可視性とデバイス登録に必要なエンドポイントエージェント機能は含まれていません。この機能を使用するには、セキュリティコネクタをインストールするか、トラフィックステアリングを設定して、監視対象のインフラストラクチャを通じてDNSクエリを送信する必要があります。これらのコンポーネントがない場合、DNSクエリはセキュアアクセスモニタリングをバイパスし、デバイスID情報はローミングデバイスセクションに取り込まれません。

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。