# Cisco Secure Access Traffic Steeringの設定とクライアントの同期

## 内容

## お問い合わせ内容

Cisco Secure Access Traffic Steeringの設定を確認すると、VPNプロファイル設定とXMLファイルに、トラフィックのステアリング制御用に設定されている宛先IPアドレスまたはドメインが表示されません。このため、Secure Accessクライアントがステアリング決定のトラフィックの宛先を決定する方法や、管理ポータルで行われた設定変更がクライアントとどのように同期されるかについて、混乱が生じます。

具体的には、VPNプロファイル管理インターフェイスを使用してトラフィックステアリング設定を構成する一方で、対応するVPNプロファイルXMLファイルに、トラフィックステアリング制御の対象となる宛先アドレスまたはドメインの可視エントリが含まれていないことを確認します。

## 環境

- Cisco Secure Accessソリューション
- トラフィックステアリングが有効なVPNプロファイル設定
- セキュアアクセスクライアントの導入

## 解決策

Cisco Secure Accessのトラフィックステアリングは、VPNプロファイルXMLのスタティックエントリではなく、ダイナミックルール配信メカニズムを介して動作します。次に、このプロセスの仕組みと設定の検証方法を説明します。

## トラフィックステアリングルールの配信プロセス

トラフィックステアリングルールは、管理者が表示できるVPNプロファイルXMLファイルには保存されません。その代わり、VPN接続の確立中に、これらのルールがセキュアアクセスヘッドエンドからクライアントに動的にプッシュされます。このプロセスは次のように動作します。

1. VPN接続が確立されると、セキュアアクセスヘッドエンドは接続クライアントに現在のトラフィックステアリング（スプリットトンネル）ルールをプッシュします
2. クライアントはこれらのルールを受信し、ローカルクライアントルーティングテーブルに直接書き込みます
3. トラフィックステアリングの決定は、VPNプロファイルXMLに表示される情報からではなく、クライアントルーティングテーブルのエントリに基づいて行われます

## 設定変更の同期

管理ポータルのトラフィックステアリング設定に加えられた変更は、特定の同期パターンに従います。

- 管理ポータルで行った設定変更は、アクティブなVPNセッション中は有効になりません
- 次のVPN接続確立時に新しいトラフィックステアリングルールが適用される
- トラフィックステアリングの設定を変更した後で動作を検証するには、VPN接続を切断して再接続する必要があります

## 検証手順

トラフィックステアリングの設定変更を検証するには、次の手順を実行します。

1. Secure Access管理ポータルで、トラフィックステアリング設定に必要な変更を加えます
2. クライアント上の既存のVPN接続を切断します。
3. VPNを再接続して、更新されたトラフィックステアリングルールを受信します
4. クライアントルーティングテーブルを調べて、新しいルールが適用されたことを確認します

# 原因

VPNプロファイルXMLにトラフィックのステアリングの宛先が存在しないのは、設計上の問題です。Cisco Secure Accessは、ダイナミックルール配信システムを使用します。このシステムでは、トラフィックステアリングルールが、プロファイルXMLの可視的な構成要素として保存されるのではなく、接続時にクライアントにプッシュされ、ルーティングテーブルのエントリを通じて実装されます。このアーキテクチャにより、セキュリティとパフォーマンスを維持しながら、リアルタイムのポリシー更新と集中制御が可能になります。

## 関連コンテンツ

- ASAスプリットトンネリング設定ガイド
- 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。