# Secure Access Split-Tunnelingの設定に関する課題

## 内容

## お問い合わせ内容

スプリットトンネルトラフィック用にCisco Secure Access(TIA)機能を設定する際に、設定プロセス中に次のような複数の複雑な問題が発生し、適切な導入が妨げられました。

- トラフィック識別の課題：スプリットトンネリング用にTIAを設定する場合、すべてのVPNトラフィックをインターネットセキュリティ検査から除外する必要があります。必要なトラフィックフローを特定することは困難であり、一部のリダイレクトURLは追跡と分類が特に困難でした。
- 認証トラフィックの制約：特定のスプリットトンネルシナリオでは、認証トラフィックをプロキシから除外する必要がありました。ただし、既存のポリシーに基づいて、認証関連のトラフィックがプロキシからバイパスできず、ポリシーの競合が発生します。
- VPNの切断に関するセキュリティリスク：スプリットトンネルトラフィックは、VPNの切断時にオープンインターネットに公開されるため、設定時に考慮する必要がある追加のセキュリティリスクとなります。

また、このプロセス中に追加の設定の問題も確認されたため、さらなる分析と解決が必要でした。

## 環境

- 製品ファミリ：SECACCS ( セキュアアクセス )
- テクノロジー：スプリットトンネリング機能を備えたCisco Secure Access(TIA)
- 設定：既存のポリシーを使用したスプリットトンネルトラフィックシナリオ
- 認証：プロキシベースの認証トラフィック処理

- ネットワークセキュリティ：VPNトラフィックのインターネットセキュリティ検査要件

# 解決策

Cisco Secure Accessスプリットトンネリングで特定された設定の課題に基づき、特定された制限とポリシーの競合に対処するための包括的な機能要求が提出されました。

## 機能要求の送信

次の設定の課題に対処するために、関連するエンジニアリングチームによるレビューのために、機能リクエスト(CSE-I-5636)がオープンされ、送信されました。

- インターネットセキュリティ検査からVPNトラフィックを除外するためのトラフィック識別機能の強化
- 追跡および分類が困難なリダイレクトURLの処理の改善
- 既存のポリシーによる認証トラフィックバイパスの制限の解決
- VPN切断時のスプリットトンネルのトラフィック漏洩に対するセキュリティリスクの軽減

# 原因

設定に関する課題は、Cisco Secure Access(TIA)スプリットトンネリング実装における現在の制限に起因しており、複雑なエンタープライズ導入シナリオに十分に対処できていません。具体的には、このシステムには、トラフィックの識別と分類に対する十分な細かい制御がなく、ポリシーが設定されているときは認証トラフィックをバイパスするという制約があり、VPN接続が中断された場合のスプリットトンネルトラフィックに対する適切なセキュリティ保護が提供されません。

# 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。