Secure Access Decryption and Intrusion Prevention System(IPS)のトラブルシューティングワークフロー

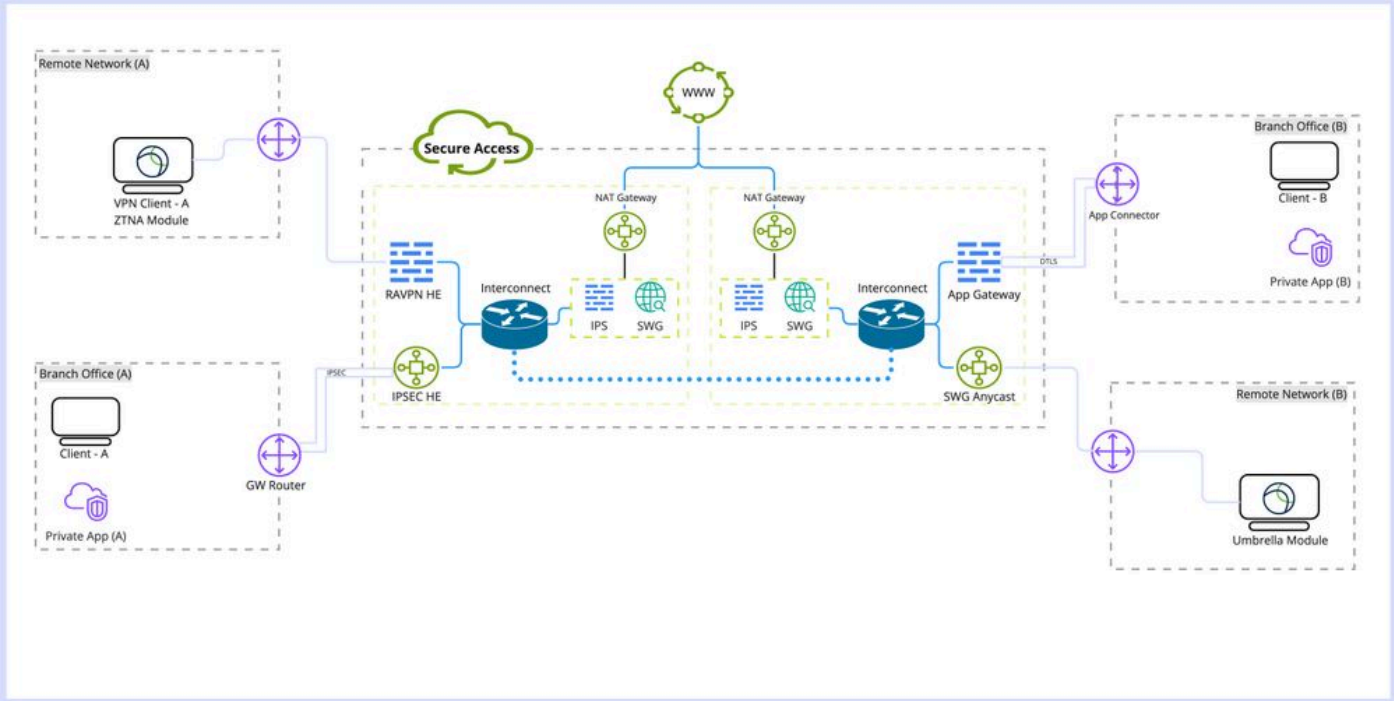
内容

はじめに

このドキュメントでは、セキュアアクセス復号化およびIPSワークフローについて説明し、重要な設定プロパティについて重点的に説明します。

セキュアアクセスアーキテクチャ

このセキュアアクセスアーキテクチャでは、セキュアアクセスによって提供されるさまざまなサービスと、ネットワークを保護するために確立できるさまざまな接続方法について説明します。



セキュアアクセスアーキテクチャ

アーキテクチャ詳細：

よく知っている用語：

RAVPN HE:リモートアクセス仮想プライベートネットワーク(VPN)ヘッドエンド

IPSEC HE:リモートトンネルInternet Protocol Security(IPSEC)ヘッドエンド

ZTNAモジュール：ゼロトラストネットワークアクセスモジュール

SWG:セキュアWebゲートウェイ

IPS:侵入防御システム

NATゲートウェイ：ネットワークアドレス変換(NAT)ゲートウェイ

SWG AnyCast:セキュアWebゲートウェイのエニーキャスト入力ポイント

導入タイプ：

1. リモートアクセスVPN

2. リモートアクセストンネル

3. Umbrellaローミングモジュール

4. アプリケーションコネクタ/アプリケーションゲートウェイ

5. ゼロトラストモジュール(ZTNA)

機能の概要

Secure Accessは、Web暗号化解除と侵入防御システム(IPS)の両方を実行する機能を提供し、アプリケーションの検出と分類を強化して、トラフィックの詳細情報（URLパス、ファイル名、アプリケーションカテゴリなど）を提供し、ゼロデイ攻撃やマルウェアからの防御を支援します。

復号化：この記事では、復号化はSecure Web Gateway(SWG)モジュールを介したHyper Text Transfer Protocol(HTTPS)トラフィックの復号化と、IPS検査のためのトラフィックの復号化と呼ばれます。

IPS：ファイアウォールレベルのIntrusion Detection and Prevention System（侵入検知および防御システム）。すべての機能を実行するには、トラフィックの復号化が必要です。

復号化は、データ損失防止(DLP)やリモートブラウザ分離(RBI)、ファイルインスペクション、ファイル分析、ファイルタイプブロッキングなどの複数のセキュアアクセス機能に必要です。

セキュアアクセスにおける復号化およびIPS関連の設定

ここでは、セキュアアクセスで使用可能な復号化およびIPS関連の設定について簡単に説明します。

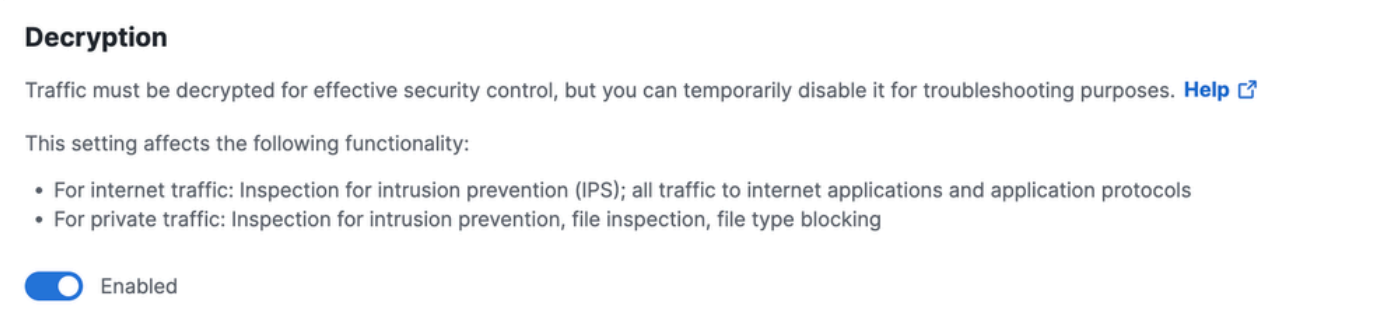
IPSの復号化

これは、すべてのポリシーのIPSエンジンを無効または有効にするために使用されるIPSのグローバル設定です。

プロパティ：

- このオプションは、セキュアWebゲートウェイ復号化（Web復号化）には影響しません
- ポリシーごとのIPSの無効化と有効化は、要求本文を検査せずにハンドシェイクの最初のフェーズのみを検査する機能が制限された状態で使用できます。

設定： Dashboard -> Secure -> Access Policy -> Rule Defaults and Global Settings -> Global Settings -> Decryption for IPSの順に選択します。



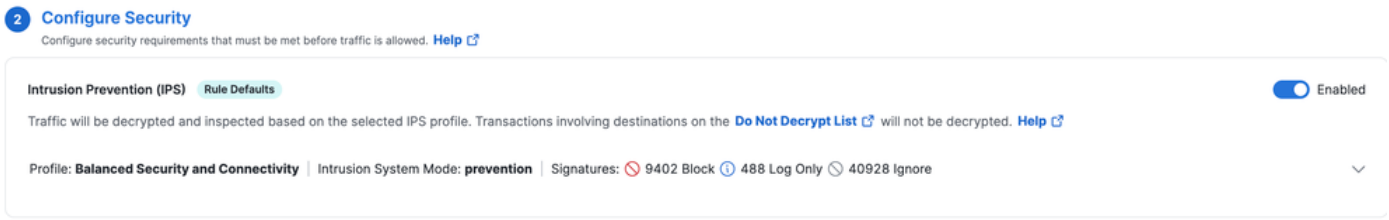
ポリシーごとのIPS設定

このオプションを使用すると、ポリシーベースごとにIPSを無効および有効にできます。

プロパティ：

- このオプションは、ポリシーごとにIPSを有効にするか無効にするかを制御します。
- このオプションはIPSの復号化の設定に依存します。グローバルなIPSの復号化オプションが無効になっている場合、動作は要求の本文を検査せずにハンドシェイクの初期フェーズのみを検査します。
- このオプションは、SWG(Web Decryption)には影響しません

設定：ダッシュボード – >セキュリティ – >アクセスポリシー – >ポリシーの編集 – >セキュリティの設定 – >侵入防御(IPS)



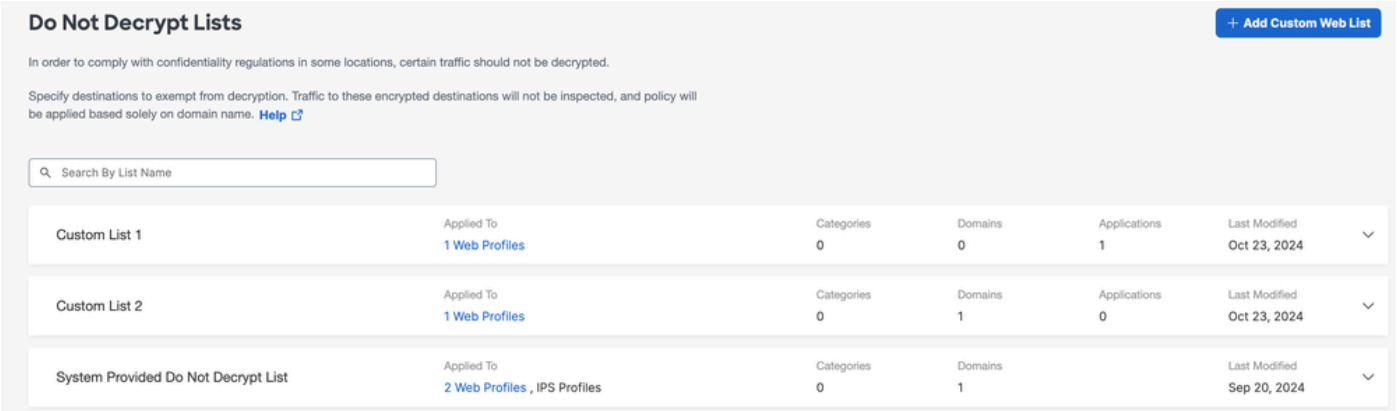
リストの暗号化を解除しない

ドメインまたはIPアドレスの復号化をバイパスするためにセキュリティプロファイルにリンクできる宛先リストのセット。

プロパティ：

- カスタムドメインのバイパスを許可するWeb復号化
- このリストは、「System Provided Do Not Decrypt List」を除き、IPSではなくWeb復号化のみに影響します
- IPSとWeb復号化の両方をバイパスする（System Provided Do Not Decryptリスト）を含む
- このオプションは、ポリシーに適用されるセキュリティプロファイルと組み合わせる必要があります
- このリストは、セキュリティプロファイルで復号化が有効になっている場合にのみ使用できます

設定：ダッシュボード – >セキュリティ – >リストを復号化しない



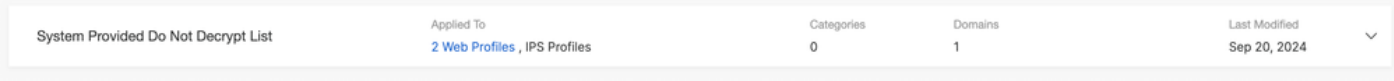
提供されたシステムは復号化しないリストを提供

Do Not Decryptリストの一部で、セキュアアクセスのDecryptionとIPSの両方に適用する追加機能を使用します。

プロパティ：

- これは、IPSとWeb復号化の両方に影響する唯一のカスタムDo Not Decryptリストです
- ポリシーごとにこのリストをカスタマイズするオプションはありません。

設定：ダッシュボード – >セキュリティ – >リストを復号化しない – >指定されたシステムはリストを復号化しない



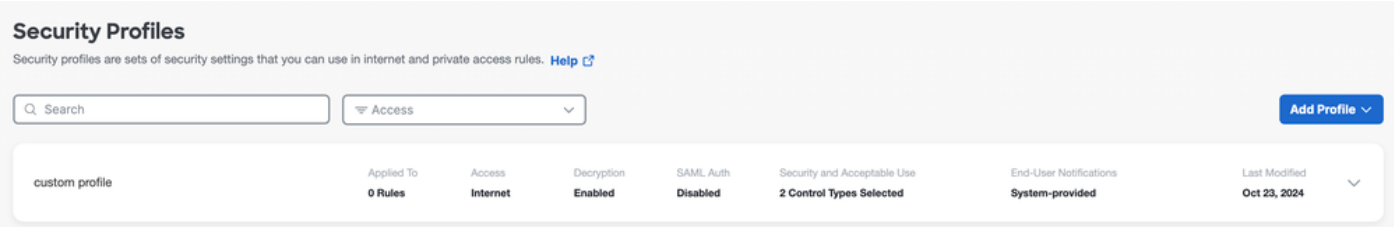
セキュリティプロファイルの設定

[セキュリティプロファイルの設定]で、後でインターネットポリシーに関連付けることができるWeb復号化の有効化または無効化を選択できます。復号化が有効になっている場合は、設定されているDo Not Decryptリストの1つを選択するオプションがあります。

プロパティ：

- Web復号化リストやDo Not Decryptリストなど、複数のセキュリティ機能を制御
- 提供されたシステムをセキュリティプロファイルに添付しても復号化しないリストは、Web復号化とIPS復号化の両方に影響します

設定：ダッシュボード – >セキュア – >セキュリティプロファイル



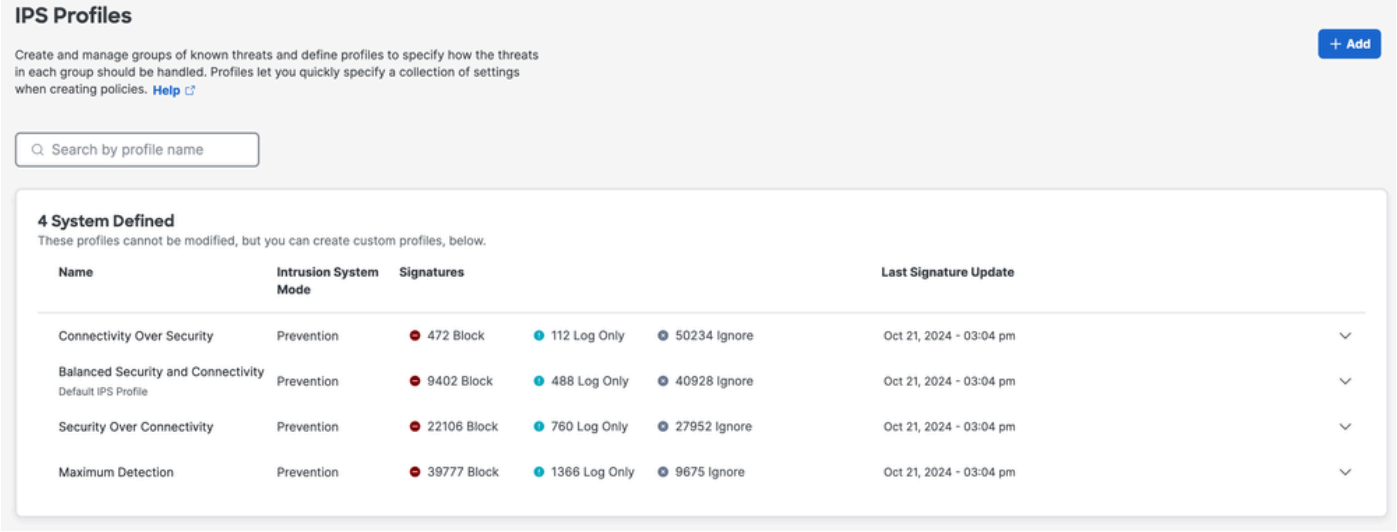
IPSプロファイル

IPSプロファイル設定には、IPSプロファイル用に事前定義された4つの主要なセキュリティ設定が含まれています。ポリシー設定ごとに選択できます。独自のカスタムIPSプロファイルを作成して、より厳密な設定や柔軟な設定を行うこともできます。

プロパティ：

- IPS用の4つの定義済みセキュリティレベルプロファイルを含む
- カスタムIPSプロファイルを作成可能

設定：ダッシュボード – >セキュア – > IPSプロファイル

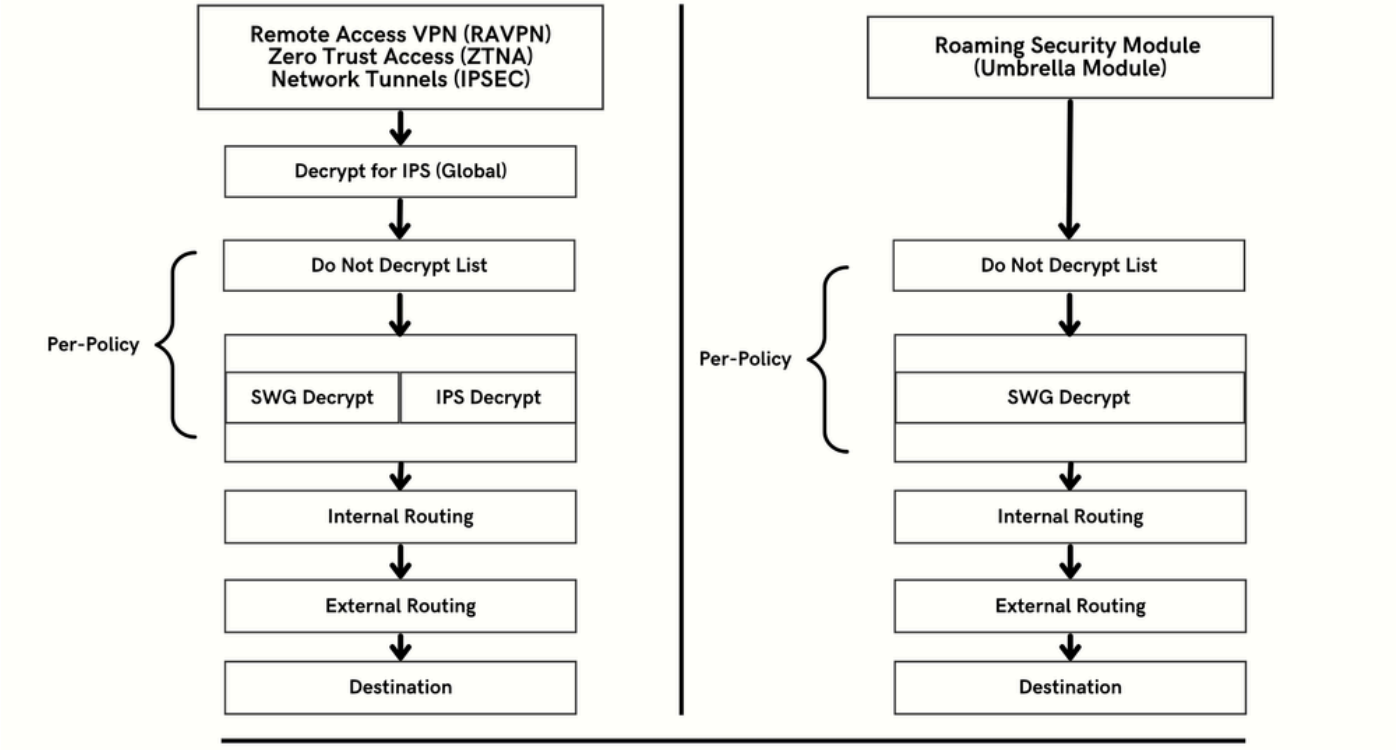


セキュアアクセスにおけるHTTPSトラフィックフロー

セキュアアクセスでは、接続方法に基づいてトラフィックパスが異なります。

リモートアクセスVPN(RAVPN)とゼロトラストアクセス(ZTNA)は、同じコンポーネントを共有します。

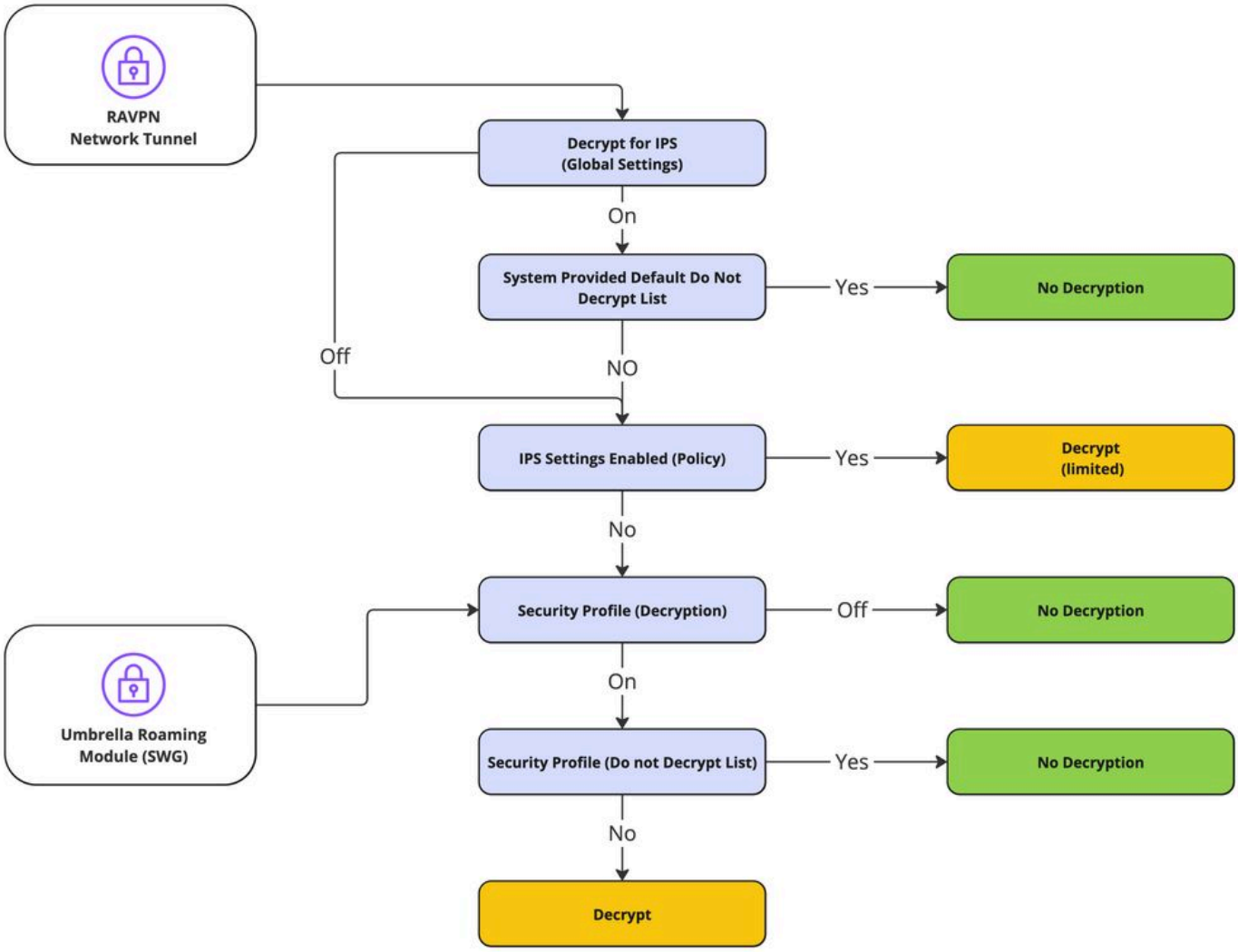
ローミングセキュリティモジュール（Umbrellaモジュール）のトラフィックパスが異なります。



トラフィックの復号化が予想される状況

このセクションでは、アクションのチェーンと、復号化または非復号化の主な結果について詳し

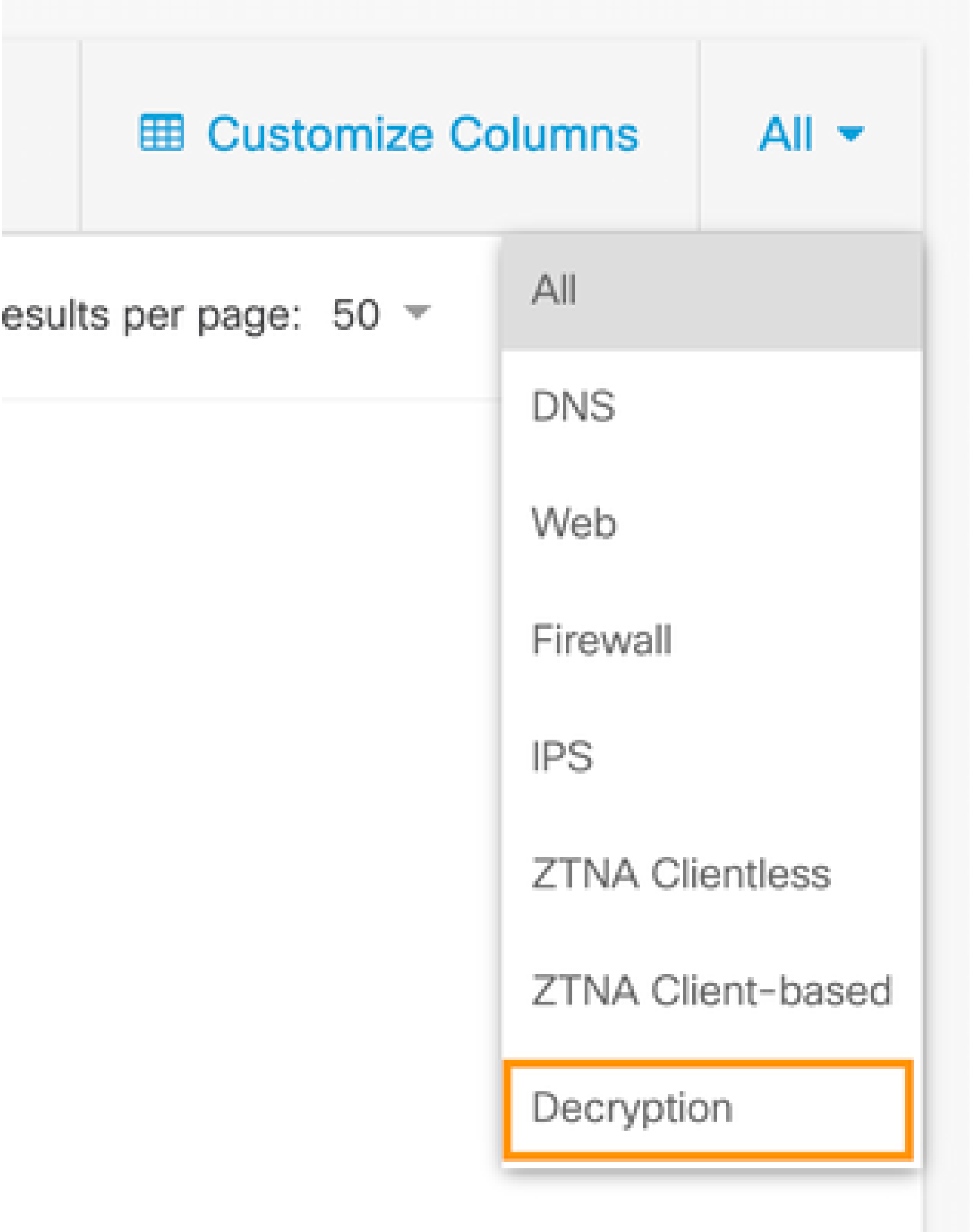
く説明します。

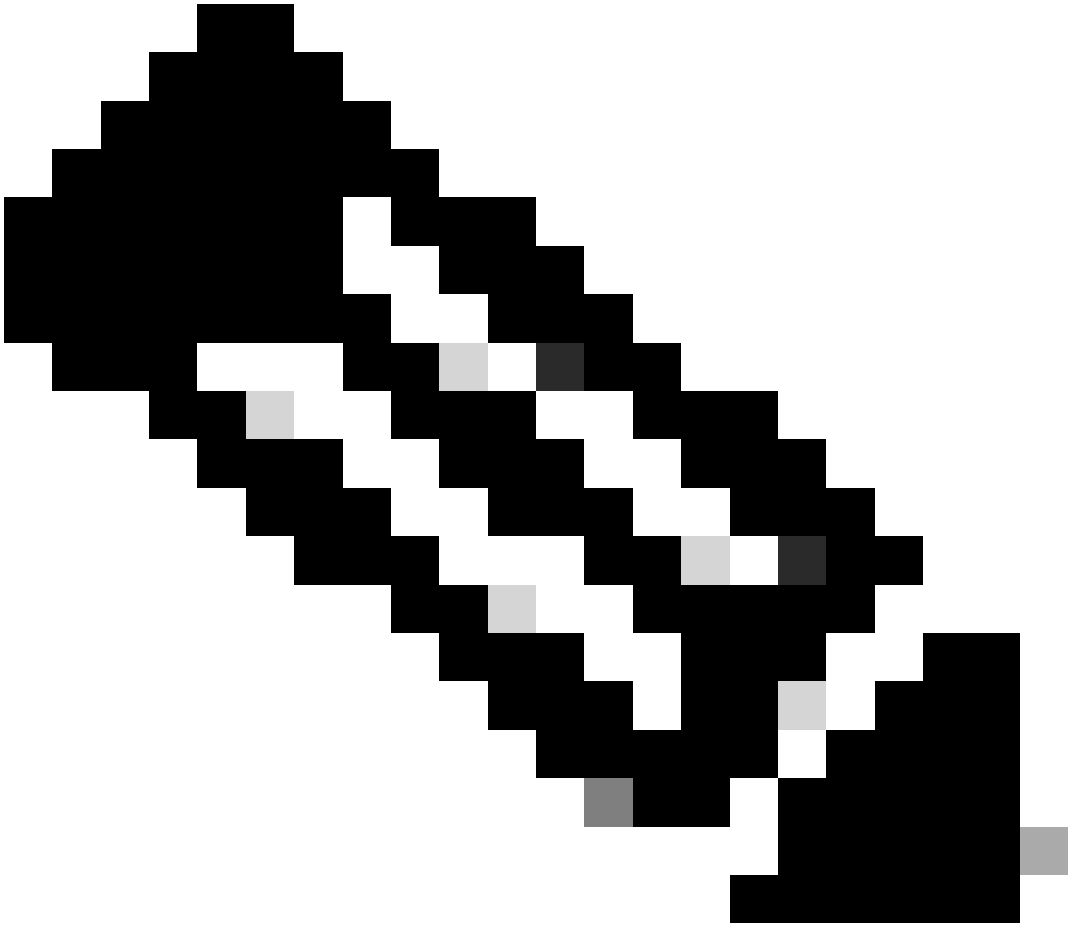


復号化フロー

復号化とIPS関連のロギングおよびレポート

セキュアアクセスには、新しいレポートセクション（復号化）が含まれています。このセクションには、ダッシュボード – >モニタ – >アクティビティ検索 – >復号化への切り替えを介してアクセスできます。

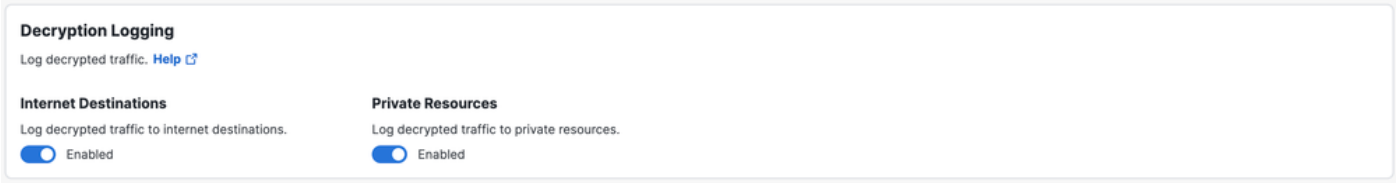

Customize Columns
All
esults per page: 50
All
DNS
Web
Firewall
IPS
ZTNA Clientless
ZTNA Client-based
Decryption



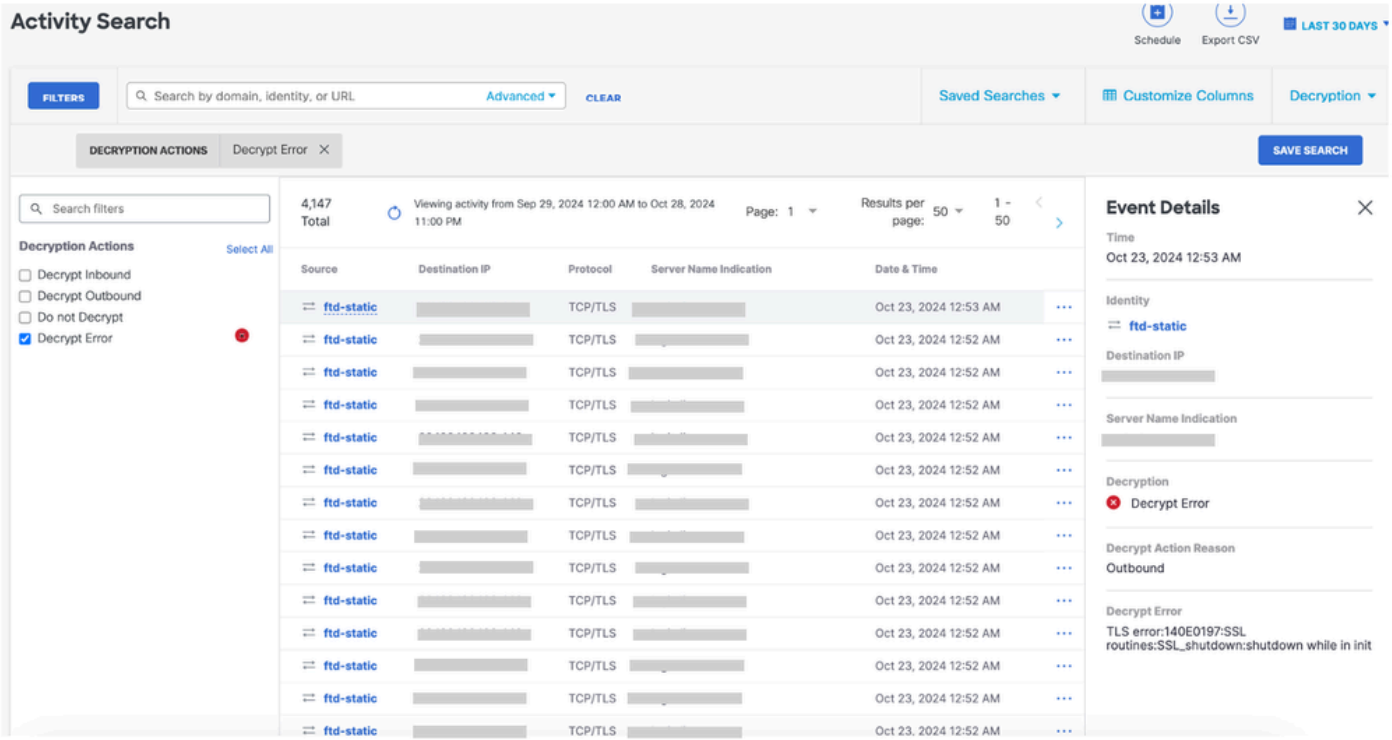
注：復号ログを有効にするには、グローバル設定で次の設定を有効にします。

ダッシュボード – >セキュリティ – >アクセスポリシー – >ルールのデフォルトとグローバル設定 – >グローバル設定 – >復号化ログ

復号化ログ設定：



復号化エラーの例：



関連情報

- セキュアアクセスユーザガイド
- テクニカルサポートとダウンロード - Cisco Systems

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。