# Cisco Secure AccessでのIPS復号化の確認

## 内容

## お問い合わせ内容

Secure Client経由でCisco Secure AccessとRAVPN(Remote Access VPN)を使用する場合、組織は、特定のWebサイトへのトラフィックに対してIPS（侵入防御システム）復号化および検査が正しく実行されているかどうかを確認する必要があります。主な課題は、アクティビティ検索などの標準管理UIログ以外の方法で、TLSの復号化および検査プロセスが正常に機能していることを確認することです。具体的な検証要件には、テスト検証をサポートし、管理インターフェイスを超えてIPSの動作の追加確認を提供できる、クライアント側の証明書チェックまたはデバッグ/レポートメカニズムの識別が含まれます。

## 環境

- RAVPN機能を備えたCisco Secure Access(CSA)
- リモートアクセスVPN接続用Cisco Secure Client
- IPSの復号化および検査機能を有効にする
- セキュリティ検査のために復号化が必要なTLS/SSLトラフィック
- RAVPNクライアントから外部WebサイトへのWebトラフィック

## 解決策

Cisco Secure Accessのリモートアクセスvpnトラフィックに対してIPS復号化と検査が正しく機能していることを確認するには、次の2つの方法があります。

### 方法1：管理UIアクティビティ検索（プライマリ方法）

Cisco Secure Access管理インターフェイスのアクティビティ検索機能は、IPSの復号化と検査の動作を確認する最も信頼性の高い方法です。このインターフェイスは、トラフィックがセキュリティサービスによって復号化および検査された時点を示す詳細なログと分析を表示します。

アクティビティ検索にアクセスする手順は、次のとおりです。

Cisco Secure Access管理ダッシュボードに移動し、アクティビティ検索機能を見つけて、特定のユーザセッションおよび宛先Webサイトのトラフィック検査ログと復号化ステータスを確認します。

復号化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

## 方法2：クライアント側の証明書の検証

追加の検証方法として、クライアント側の証明書チェックを実行して、トラフィックの復号化が行われていることを確認できます。

Cisco Secure AccessがTLSトラフィックの復号化と検査に成功すると、元のWebサイトの証明書ではなく、自身の証明書をクライアントに提示します。

証明書検査を通じて復号化を確認するには、次の手順を実行します。

1. Webサイト証明書の確認
ブラウザで証明書の詳細を開き、発行者と有効期間を確認します。

証明書がCisco Secure Access Root CAによって10日以内の有効期間で発行された場合、ファイアウォールレベルでの侵入防御システム(IPS)の復号化を示します。

証明書の有効期間が約5日の場合は、セキュアなWebゲートウェイベースの復号化を示します。

2. 証明書発行者の検証（DC名前付け）

このクライアント側の証明書検証方法は、プライマリアクティビティ検索方法と並ぶ補助的な確認手法として機能し、IPS復号化プロセスが期待どおりに機能していることを保証します。

Intrusion Prevention System（Ips；侵入防御システム）が復号化しない：

侵入防御システム(IPS)の復号化は、次の場合に行われます。

・ グローバル設定で有効になり、

・ 少なくとも1つのアクセスポリシールールで侵入防御システム(IPS)が有効になっている（ルールが無効になっていても、この条件は適用されると思う）

侵入防御システム(IPS)の復号化からドメインをバイパスしたい

提供されたシステムのdo not decryptリストを使用し、提供されたシステムのdo not decryptリストにドメインを追加します。

または

Cisco Secure accessのグローバル設定で送信元ベースの復号化を使用します。

注：これは、セキュアアクセスのネットワークトンネル設定にアウトバウンドNATが設定されていない場合に機能します。

# 原因

エンタープライズ環境でセキュリティポリシーの適用を検証するためには、複数の検証方法が必要です。管理UIログは包括的な可視性を提供しますが、クライアント側の検証方法は、管理インターフェイスへの直接アクセスが制限される可能性があるコンプライアンステスト、トラブルシューティング、検証のシナリオ、または完全なテスト手順のために複数の検証ポイントが必要な場合に役立つ追加の確認ポイントを提供します。

# 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。