認証後の銀行サイトのSecure Access 502エラー

内容

問題

FCBankingへの認証に成功した後、502 Bad Gateway HTTPエラーコードを受信したとユーザから報告されました。認証プロセスは正常に完了し、ユーザはログインクレデンシャルを入力できますが、ブラウザには認証直後に502 bad gatewayエラーが表示されます。

FCBankingのドメインとその関連カテゴリはSSLとIPSの復号化から除外されており、この設定変更では502 HTTPエラーは解決されませんでした。この問題は断続的に発生し、FCBankingドメイン全体に対してセキュアアクセスをバイパスした後にのみ解決されました。HARファイル分析では、「my.fcbanking.com」の宛先で502個のエラーが見つかりました。また、アクティビティ検索ログには、HARファイルでキャプチャされた502個のエラーは表示されず、これらのエラーが中間デバイスレベルで発生していることが示されました。

環境

- Cisco Secure Access – インターネットアクセス (ローミングモジュール、VA、DNS、SWG、PAC、IPS、証明書)
- ネットワークトポロジ：ユーザPC >スイッチ> Catalyst SD-WANルータ>ローカルインターネットまたはCSAトンネル
- Network Tunnel Group(NTG)をバイパスし、Direct Internet Access(DIA)を介してポート80および443上のすべてのトラフィックを送信するように設定されたCatalyst SD-WANエッジ(CatOS)
- Cisco Secure Clientは、バイパスリストを使用してセキュアアクセスへのトラフィックルーティングを決定する
- バンキングドメイン：fcbanking.comおよび関連するサブドメイン(my.fcbanking.com、treasury.fcbanking.com)

解決方法

主な解決策は、バンキングドメインを追加してセキュアアクセスを完全にバイパスし、トラフィックがインターネットに直接流れるようにしながら、DNS層のセキュリティを維持することです。

ステップ1：バイパスリストへのプライマリドメインの追加

- セキュアアクセス設定のバイパスプロキシのみのリストに、fcbanking.comを追加します。これにより、Webトラフィックがセキュアアクセスプロキシをバイパスする一方で、DNSレイヤのセキュリティは適用されアクティビティ検索に記録されたままになります。

手順2：ドメインエイリアスを特定して追加する

- 銀行サイトでは、バイパスリストにも追加する必要がある複数のエイリアスを使用することがよくあります。Cache Checkを使用して、バンキングドメインのすべてのエイリアスを識別します。
- fcbanking.comでは、次のエイリアスが識別され、バイパスリストに追加されています。
    - treasury.fcbanking.com（エイリアス：treasuryvanity.jackhenry.com）
    - my.fcbanking.com（エイリアス：banno-online.jackhenry.bank）
    - treasuryvanity.jackhenry.com
    - banno-online.jackhenry.bank（オンラインバンノ。ジャッキヘンリー。バンク）

ステップ3:IPアドレスを使用した代替解決

- ドメインベースのバイパスの代わりに、バンキングサイトの解決済みIPアドレスをバイパスリストに追加できます。Cisco Secure Clientは、バイパスリストで見つかったFQDNをIPアドレスに変換し、Webトラフィックをインターネットに直接ルーティングします。

手順4：トラブルシューティング用のデバッグロギングの有効化

- 詳細なログを取得してさらに分析するには、最大デバッグロギングを有効にします。
- 次のコンテンツを使用して、「SWGConfigOverride.json」という名前のファイルを作成します。

```
{"logLevel": "1"}
```

SWGフォルダにSWGConfigOverride.jsonファイルを配置します。

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
```

SWGまたはUmbrellaサービスを再起動するか、システムを再起動してデバッグロギング設定を適用します。

注：デバッグロギングはシステムパフォーマンスに影響しませんが、ログファイルのサイズを増やす可能性があります。DARTバンドルの取得後にSWGConfigOverride.jsonファイルを削除し、通常のログレベルに戻します。

ステップ5：検証

- バイパス設定の実装後、ユーザはバンキングサイトにアクセスする際に502件のエラーが発生していないと報告しています。DNSトラフィックはアクティビティ検索に記録され続けますが、Webトラフィックはインターネットに直接送信されます。

原因

銀行サイトは一般に、プロキシサーバまたは共有IPアドレス範囲から発信されるトラフィックを検出してブロックするセキュリティ対策を実装します。Cisco Secure Accessは、プロキシトラフィックに共有IP範囲（151.186.144.0/20および151.186.176.0/20）を使用します。銀行サイトは、このトラフィックを検出し、サイレントにドロップするか、HTTP 502エラーで応答できます。

ドメインがDo Not Decryptリストに含まれる場合、送信元IPは引き続きSecure Accessの共有IPの範囲から発信されているように見え、バンキングサイトのセキュリティメカニズムがトリガーされます。さらに、バンキングトラフィックに対するIPS検査と、適切に除外されないドメインエイリアスは、接続障害の原因となる可能性があります。この問題の断続的な性質と、HARファイルには表示されるがアクティビティ検索ログには表示されない502エラーは、エラーが宛先バンキングサーバではなく、中間プロキシ処理によって生成されたことを示します。

関連コンテンツ

- SWG Webサイトアクセス問題のトラブルシューティング
- QUICプロトコルを無効にしてWebトラフィック検査を適切に行う
- Cisco Secure Access IP範囲に関するドキュメント
- 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。