Cisco Secure Accessへの移行後に一貫性のないブロッキングページが発生

内容

お問い合わせ内容

移行ツールを使用してUmbrellaからCisco Secure Access(SSE)に移行した後、ブロックされたWebトラフィックは、Cisco Secure Accessのブロックページではなく、一貫性のないレガシーUmbrellaのブロックページにリダイレクトされます。この問題は、異なるドメインがブロックルールをトリガーすると、異なるスプラッシュページとブロック理由の言い回しが発生するDNS防御で発生します。これにより、組織全体で一貫性のないエンドユーザブロッキング通知が作成されます。

確認された具体的な症状は次のとおりです。

- ブロックルールは、新しいCisco Secure Accessのブロックページではなく、古いUmbrellaのブロックページにユーザをリダイレクトする
- ブロックルールをトリガーするドメインが異なると、表示されるスプラッシュページも異なります
- 一貫性のないブロックの理由の表現がエンドユーザに提示される
- この動作は、移行後のDNS防御機能に影響します

環境

- テクノロジー：Cisco Secure Access(SSE)
- 移行：移行ツールを使用した包括からSSEへの移行
- サービスタイプ：DNS防御
- 導入：移行後の環境
- Webスキャン：Webスキャンが有効になっているFTDデバイス

解決策

FTDデバイスでWebスキャンを実行すると、Cisco Secure Accessのカスタムランディングページが適切に表示されなくなります。この問題を解決するには、FTDで次の3つのドメインのWebスキャンをバイパスします。

- opendns.com
- cisco-secure.com
- sse.cisco.com

この回避策により、従来のUmbrellaブロッキングページを表示する代わりに、カスタムCisco Secure Accessランディングページを正しくレンダリングできます。

確認手順

解決の有効性を検証するには、次の手順を実行します。

ステップ1：以前に一貫性のない動作を示したドメインに対してポリシーテストを実行します

ステップ2：回避策を実装した後で、ブロッキングページの動作を確認します

ブロックされたトラフィックが、従来のUmbrellaページではなく、Cisco Secure Accessのブロッキングページを常に表示するようになったことを確認します。

手順3：ブロックの一貫した理由の表現を検証する

すべてのブロックされたドメインに、Cisco Secure Access標準に沿った均一なブロック理由メッセージが表示されていることを確認します。

原因

この問題は、FTDデバイスのWebスキャン機能がCisco Secure Accessのカスタムランディングペ

ージの適切なレンダリングを妨げることで発生します。FTDでWebスキャンを有効にすると、新しいブロッキングページが正しく表示されなくなり、システムはレガシーのUmbrellaブロッキングページにフォールバックします。これにより、異なるドメインが異なるブロッキングページ形式をトリガーする可能性がある、一貫性のないユーザエクスペリエンスが生まれます。

エンジニアリングチームは、これをターロスの観点からの変更を必要とする設計レベルの問題として特定しました。現在のアーキテクチャでは、適切なカスタムランディングページ機能を確保するために、特定のシスコドメインに対してWebスキャンをバイパスする必要があります。

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。