Secure Access Application Protocolのブロッキングによるインターネット接続の妨害

内容

- お問い合わせ内容
- 環境
- 解決策
  - ステップ1：ブロッキングルールの特定
  - 手順2：アプリケーション設定の変更
  - ステップ3：変更の適用と確認
- 原因
- 関連コンテンツ

お問い合わせ内容

Cisco Secure Accessに移行した後、ユーザがWebサービスにアクセスしようとすると、インターネット接続がブロックされる問題が発生しました。特定の症状として、セキュリティポリシーによってHTTPトラフィックがブロックされ、正当なWebサイトやアプリケーションへのアクセスが妨げられたことが挙げられます。

ブロッキングイベントの詳細には、次の特性が示されています。

- アクション：ブロック
- イベントブロックの理由： AC_RULE_MATCH_BLOCK
- 宛先：http://www.bing.com/api/shopping/v1/user/shoppingsettings

- 宛先ポート：443
- カテゴリ：未分類
- アプリケーションカテゴリ：検索
- アプリケーションプロトコル：ハイパーテキスト転送プロトコル
- プロトコル：TCP

環境

- シスコセキュアアクセスの導入
- アプリケーションプロトコルの制限を伴うアクティブなセキュリティポリシー

解決策

この解決策では、真の非信頼アプリケーションのセキュリティポスチャを維持しながら、HTTPアプリケーションプロトコルトラフィックを許可するようにセキュリティルール設定を変更します。

ステップ1：ブロッキングルールの特定

Secure Access管理インターフェイスで、ブロックの原因となっている特定のルールを見つけます。

- ルール名: Test
- 現在の構成：アプリケーション設定ブロックを宛先として使用しています。

手順2：アプリケーション設定の変更

ルール設定にアクセスし、宛先のアプリケーション設定の名前を確認します。

- Resources > Internet and SaaS resources > Application Listsの順に移動します。次に、アプリケーションをクリックします。
- アプリケーションプロトコルの設定を確認します。
- ブロックされたアプリケーションプロトコルリストのHTTPのチェックマークを外すか、削除します。
- 実際の信頼できないアプリケーションに対して、他のセキュリティ制御が適用されていることを確認します。

ステップ3：変更の適用と確認

ルールの変更を保存し、接続をテストします。

1. – 設定変更をアクティブなポリシーに適用します。

2. – 以前にブロックされた宛先へのインターネット接続をテストします。

3. – セキュリティログを監視して、正規のHTTPトラフィックが許可されていることを確認します。

4. – 他のセキュリティ保護が有効なままであることを確認します。

原因

根本的な原因は、Cisco Secure Accessのセキュリティルール設定が過度に制限されていることでした。このルールは、すべてのHTTPアプリケーションプロトコルトラフィックをブロックするように設定されており、これにより正当なWebブラウジングとアプリケーションアクセスが防止されました。HTTPプロトコルをブロックする広範なアプリケーションは、HTTP/HTTPSプロトコルを使用する正規のWebサービスおよびアプリケーションにアクセスするユーザの通常のインターネット接続に影響を与えました。

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。