包括DNSポリシーテスターの制限事項の理解

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

概要

技術詳細

- セキュアWebゲートウェイ
- セキュアインターネットゲートウェイ
- 包括（DNS追加レイヤ）

はじめに

このドキュメントでは、Umbrella DNSポリシーテスターの制限事項について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- セキュアWebゲートウェイ
- セキュアインターネットゲートウェイ
- 包括（DNS追加レイヤ）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

Umbrella Policy Testerを使用すると、特定のIDがアクセスしたときに、特定の宛先をシスコでブロックまたは許可できるかどうかを判断できます。ただし、ポリシーテスターが特定の宛先に関する正確な（または任意の）情報を返すことができない状況がいくつかあります。この記事では、これらの制限の概要を説明します。

技術詳細

Policy Testerの全般的な概要については、Umbrella Policy Testerに関するUmbrellaのドキュメントを参照してください。

次のポリシーテスターの結果が正しくない可能性があります。

セキュアWebゲートウェイ

- サポートされていない

セキュアインターネットゲートウェイ

- サポートされていない

包括（DNS追加レイヤ）

- インテリジェントプロキシによってブロックされた宛先は、ポリシーテスターによって誤って「Allowed」と報告される可能性があります。これには次の項目も含まれます。
  - カスタムURLブロックリスト
  - プロキシブロックリストまたはグレイリストドメイン
  - ファイルインスペクションブロック
- ブロックされた宛先タイプ「Application」（名前はDropbox、Box、Facebookなど）は、ポリシーテスターによって「Allowed」と誤って報告される可能性があります。
- ネットワークがWebポリシーにも適用されている場合、Webポリシーが正しく表示されないことがあります。ポリシーテスターは、Webポリシーの一部でもあるネットワークでは現在サポートされていません。
- 関連するID情報をすべて提供しないテストでは、誤った結果が表示される可能性があります。たとえば、保護されたネットワーク上でActive Directory (AD)統合が有効になっているローミングコンピューターでは、ADユーザーのみが指定され、ローミングコンピューターがポリシーの決定を勝ち取ると、テストが失敗することがあります。
- コンテンツカテゴリによってブロックされた通知先は、大文字と小文字を使用して入力するか、大文字で入力すると、許可されている通知先として表示されます。たとえば、「ヌード」カテゴリをブロックしている場合、ドメインplayboy.comはブロックと表示され、Playboy.comは許可と表示されます。
- 「ダイナミックDNS」の宛先は、そのセキュリティカテゴリが選択されている場合はブロックできますが、ポリシーテスターによって誤って「Allowed」と報告される可能性があります。
- アプリケーション制御によって許可された宛先が、ポリシーテスターで誤ってブロックとして表示される可能性があります。
- カスタム統合用のUmbrella Enforcement APIによってブロックされた宛先は、ポリシーテスターによって「Allowed」と誤って報告される可能性があります。
- Umbrella AMP Threat Grid統合によってブロックされた宛先は、ポリシーテスターによって誤って「Allowed」と報告される可能性があります。
- CNAMEが原因でブロックされた宛先は、ポリシーテスターによって誤って「Allowed」と報告される可能性があります。
- IPアドレスである宛先は、現時点ではポリシーテスターではサポートされていません。

- URLである宛先は、現時点ではポリシーテスターではサポートされていません。
- 悪意のあるIPへの解決のためにブロックされた宛先は、ポリシーテスターによって「Allowed」と誤って報告される可能性があります。
- 「潜在的に有害な」宛先は、そのセキュリティカテゴリが選択されている場合はブロックできますが、ポリシーテスターによって「許可」として誤ってレポートされる可能性があります。
- 自動DDOS保護によって一時的にDNSが影響を受けるドメインに応答できない宛先は、ポリシーテスターには表示されません。
- コンテンツカテゴリ「German Youth Protection（ドイツの若者の保護）」でブロックされた宛先は、ポリシーテスターによって「Allowed（許可）」と誤って報告される可能性があります。このカテゴリは、ポリシーテスターの結果には記載できません。
- 「暗号通貨」セキュリティ分類のためにブロックされた宛先は、セキュリティ設定によってブロックされた場合でも、誤って「許可」と表示される可能性がある。
- DNSトンネリングVPNカテゴリによるブロックは、ポリシーテスターで結果を正しく表示できません。許可されているとおりに正しく表示されません。
- 仮想アプライアンスの背後にあるChromebookデバイスは、誤ったポリシーを表示する可能性があります。Chromebook(UCC)アイデンティティブロックは仮想アプライアンスで適用されたポリシーを上書きできますが、仮想アプライアンスブロックはUCCを上書きできます。
- グループがUmbrellaに同期されていないADグループのメンバー（親または子ドメインの一部のグループや、Umbrellaに選択的に同期されていないグループのメンバーであるグループを含む）は、ポリシーテスターに表示されたポリシーに一致するものとして表示できます。ユーザーポリシーはクラウドに適用できません。ポリシーに1人のユーザを追加して確認し、5分以内に正しく適用されることを確認します。
- 内部ドメインリストにある宛先。ポリシーテスターは、テスト結果のレポート時に内部ドメインリストを取得しません。
- OpenDNSコミュニティドメインのタギングサイトに表示されないカテゴリは、ポリシーテスターで正しいカテゴリを表示することが保証されていません。分類のソースは1つしか表示されません。
- ポリシーテスターでは、IDの検索時に20件の結果を表示するように制限されています。
- ADユーザはネストされたADグループのメンバーですが、DNSポリシーの作成時にIDで選択されるのは親ADグループだけです。ポリシーテスターのルックアップで、正しいポリシーの照合に失敗する可能性があります。
- 保護された許可リスト内の宛先が、ポリシーテスターによって誤って「ブロック済み」と報告される可能性があります。

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。