

Umbrellaセキュアインターネットゲートウェイでのルールベースポリシーの使用

内容

[はじめに](#)

[ルールベースのポリシー移行の概要](#)

[よく寄せられる質問 \(FAQ\)](#)

[Webポリシーとは](#)

[ルールセットとは](#)

[ルールセットを使用する理由](#)

[ルールセットで構成できる設定](#)

[ルールとは](#)

[ルールを使用する理由](#)

[どのようなIDがサポートされていますか。](#)

[どの宛先がサポートされていますか。](#)

[どのようなアクションがサポートされていますか。](#)

[ルールに設定できる設定](#)

[ルールセットの評価方法](#)

[ルールの評価方法](#)

[ルールセットに一致した同じIDにルールが適用されるか](#)

[トランザクションで使用されたルールを確認する方法](#)

[ルールセットに関するオンライン・ドキュメントはどこで入手できますか？](#)

はじめに

このドキュメントでは、Umbrella Secure Internet Gateway(SIG)のルールベースポリシー(PBR)機能について説明し、一般的な質問に回答します。

ルールベースのポリシー移行の概要

2021年3月31日に、ルールベースのポリシーがUmbrella SIGのカスタマーに対してGAになりました。Umbrella SIGの顧客は、数週間かけてレガシーWebポリシーからルールベースポリシーに徐々に移行しています。お客様は、Umbrellaダッシュボードを通じて移行日と期間の通知を受け取ります。この変更は、Umbrella DNSカスタマーまたはDNSポリシー設定には影響しません。



注：このFAQは、レガシーWebポリシーからルールセットへの移行に関する、新規および経験豊富なUmbrellaユーザからの簡単な質問に対応することを目的としています。 詳細なドキュメントについては、更新された『[Umbrella Admin Guide](#)』を参照してください。

よく寄せられる質問 (FAQ)

Webポリシーとは

Webポリシーは、Umbrella組織内のすべてのルールセットのコレクションです。

ルールセットとは

ルールセットは、ルールセット内のルールに適用される一連のルールと設定の論理コンテナです。

ルールセットを使用する理由

ルールセットは、特定の地域、オフィスのグループ、または組織の他の部分とは異なる管理を必要とするユーザーを表すことができます。

ルールセットで構成できる設定

ルールセットで指定された設定を構成します。これらの設定は、そのルールセット内のルールにのみ適用されます。

- ルールセット名
- ルールセットID
- ブロックページ
- テナント制御
- ファイル分析
- ファイルタイプコントロール
- HTTPSインスペクション
- PAC ファイル
- ルールセットのログ
- SAML
- セキュリティ設定

詳細は、「ルールセットの構成」を参照してください。

ルールとは

ルールは、IDと宛先の両方が一致する場合に実行するアクションを定義するステートメントです。

ルールを使用する理由

ルールにより、きめ細かいアクセス制御や幅広いアクセス制御が可能になります。たとえば、優先順位の低いルールはすべてのユーザーに対して幅広いWebサイトをブロックし、優先順位の高いルールはすべての同じルールセット内で、ターゲットのグループに対して特定のサイトへのアクセスを許可できます。

どのようなIdがサポートされていますか。

ルールセットとルールはどちらも次のIDをサポートします。

- ADユーザ
- ADグループ
- ローミングコンピュータ (AnyConnectエンドポイント)
- 内部ネットワーク
- Tunnel (トンネル)
- Network

どの宛先がサポートされていますか。

ルールでは、次の宛先がサポートされています。

- コンテンツカテゴリ
- [アプリケーション設定 (Application Settings)]
- 宛先リスト

どのようなアクションがサポートされていますか。

ルールは次のアクションをサポートします。

- プライベート ネットワーク間で
- Block
- 警告
- 分離

ルールに設定できる設定

ルールは次のように設定できます。

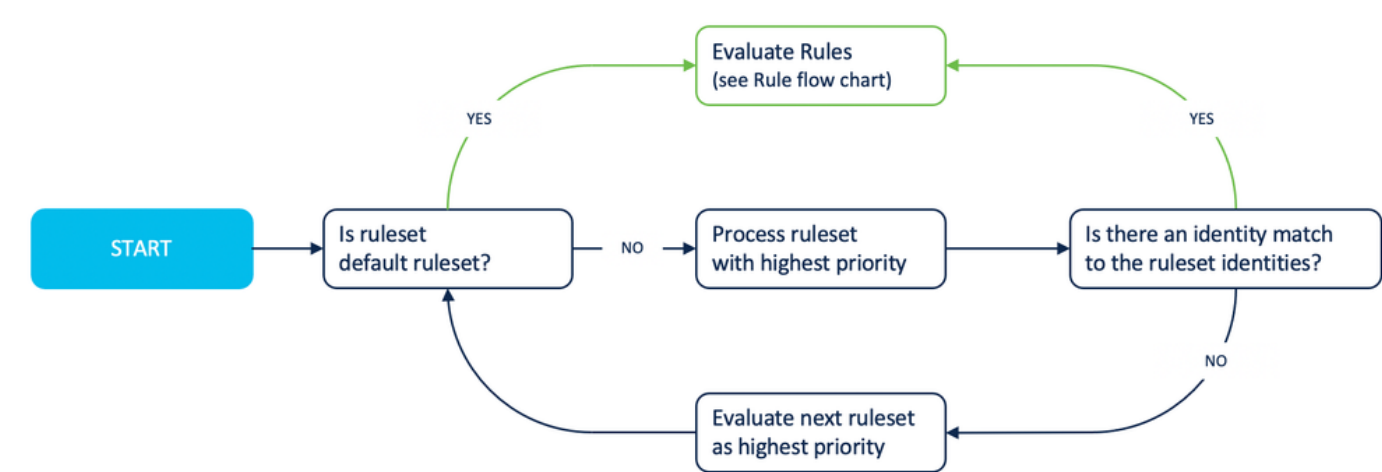
- ルール名
- アクション
- Identity
- 宛先
- 時間/日スケジュール

詳細については、「[ルールセットへのルールの追加](#)」を参照してください。

ルールセットの評価方法

ルールセットは、使用可能なIDに対してトップダウン階層で評価されます。最も高い優先度を持つルールセットが最初に評価されます。一致が見つからない場合は、次に優先度の高いルールセットが評価され、その次に優先度の高いルールセットが評価されます。どのルールセットにも一致が見つからない場合は、デフォルトのルールセットが適用されます。

Ruleset flow

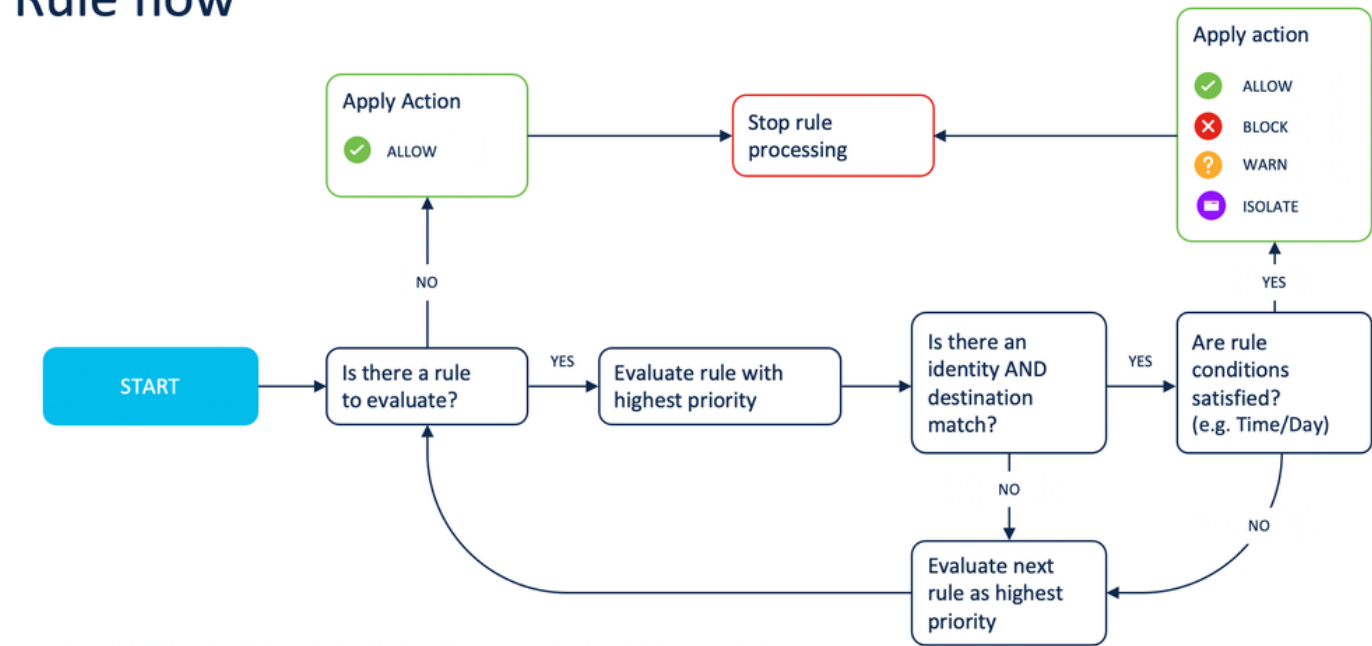


スクリーンショット_2021-04-07_at_2.37.22_PM.png

ルールの評価方法

選択したルールセット内のルールは、使用可能なIDおよび宛先に対してトップダウンで評価されます。ルールは、IDと宛先の両方が一致する場合にのみ適用されます。その後、ルールに対して設定されたアクション（許可、ブロック、警告、または分離）が適用されます。

Rule flow



スクリーンショット_2021-05-10_at_10.33.03_AM.png

ルールセットに一致した同じIDにルールが適用されるか

ルールはルールセットと同じIDに一致できますが、常にそうであるとは限りません。UmbrellaはWeb要求を受信すると、存在するすべてのIDを収集します。選択したルールセット内のルールは、IDの同じプールに対して評価され、宛先とも一致する必要があります。ルールで使用される実際のIDは、ルールセットに一致したIDとは異なる場合があります。

例：

- JDoeはネットワークBから動作します。
- 組織には次のルールセットがあります。
 - ルールセット1：ネットワークA
 - ルールセット2：ネットワークB
 - ルールセット3：ネットワークC

JDoeにはルールセット2のみが適用されます。ルールセット2内：

- ルール1：アイデンティティASmith、宛先ドメインB、アクション許可
- ルール2：アイデンティティマーケティング、通知先SomeSocialApp、アクション許可
- ルール3：アイデンティティネットワークB、宛先コンテンツカテゴリ（ドメインB、SomeSocialApp）、アクションブロック

成果：

- JDoeはドメインBからブロックされます（ルール3）。
- JDoeは、マーケティングのメンバーとして、SomeSocialAppへのアクセスを許可されています（ルール2）。

ルール評価順序によって結果が決まります。より具体的なアイデンティティ（ユーザ、グループ）は、より具体的でないアイデンティティ（ネットワーク）の前に配置されます。最初の一致が勝ち。

トランザクションで使用されたルールを確認する方法

アクティビティ検索レポートには、トランザクションで使用されるルールセットとルールの両方が取り込まれます。この情報は、「URL要求の全詳細」の下にあります。現在、このフィールドには「Policy/Rule」というラベルが付いていますが、顧客が従来のWebポリシーからルールセットに移行すると、「Ruleset/Rule」に変更されます。

ルールセットに関するオンライン・ドキュメントはどこで入手できますか？

Umbrella管理ガイド「[Webポリシーの管理](#)」を参照してください。

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。