

警告ルールアクションの構成

内容

[はじめに](#)

[概要](#)

[アクセス期間](#)

[アクティビティレポートの概要](#)

[宛先リストの制限](#)

[HTTPSインスペクションの有効化](#)

[カスタム警告ページの作成](#)

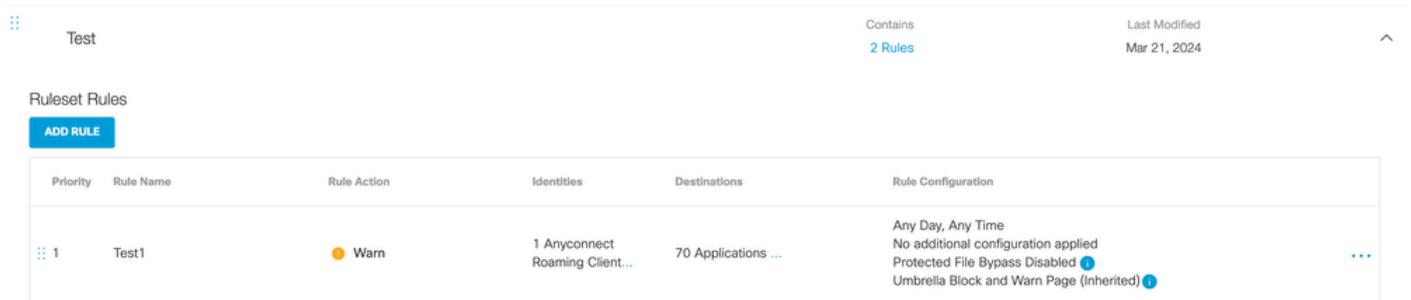
[結論](#)

はじめに

このドキュメントでは、Warn rule action機能、その設定、およびCisco Umbrella内の関連する制限について包括的に説明します。

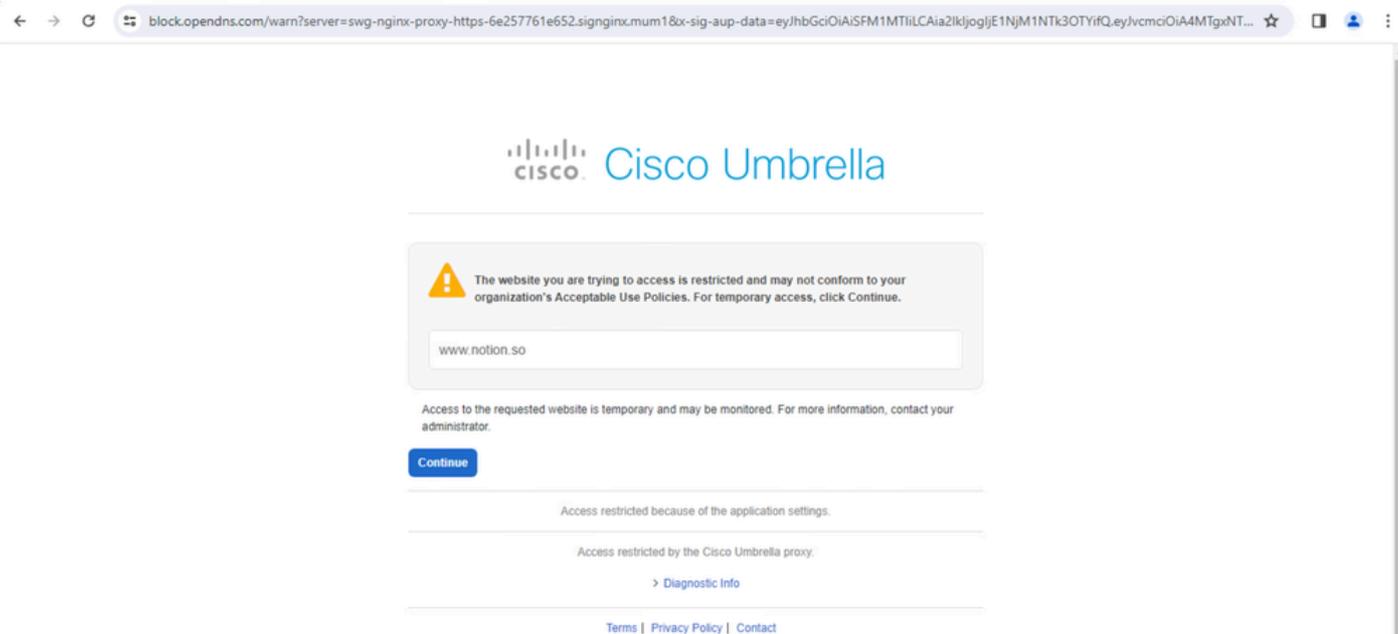
概要

ユーザがCisco UmbrellaのWarnカテゴリに分類されているWebサイトにアクセスしようとする、Warnページが表示されます。続行するには、[警告]ページをクリックする必要があります。



The screenshot shows the configuration for a rule named 'Test1'. The rule action is set to 'Warn'. The configuration includes 'Any Day, Any Time', 'No additional configuration applied', 'Protected File Bypass Disabled', and 'Umbrella Block and Warn Page (Inherited)'.

Priority	Rule Name	Rule Action	Identities	Destinations	Rule Configuration
1	Test1	Warn	1 Anyconnect Roaming Client...	70 Applications ...	Any Day, Any Time No additional configuration applied Protected File Bypass Disabled Umbrella Block and Warn Page (Inherited)



アクセス期間

[警告]ページをクリックすると、要求された宛先へのアクセスが1時間の制限期間で許可されます。この期間が経過すると、[警告]ページが再表示され、アクセスを続行するには再度クリックする必要があります。

アクティビティレポートの概要

警告ページのインタラクションはUmbrellaのアクティビティレポート内に記録され、管理者はユーザーインタラクションと警告ルールアクション機能によってトリガーされる警告に関する洞察を得ることができます。

4 Total Viewing activity from Mar 14, 2024 4:06 PM to Mar 15, 2024 4:06 PM Page: 1 Results per page: 50 1 - 4 of 4

Request	Identity	Policy or Ruleset Identity	Destination	Destination IP	Internal IP	External IP	Action	
DNS	DESKTOP-CSC	Lab - 123.63.117.88	www.notion.so		192.168.1.95	123.63.117.88	Allowed	...
DNS	DESKTOP-CSC	Lab - 123.63.117.88	www.notion.so		192.168.1.95	123.63.117.88	Allowed	...
WEB	DESKTOP-CSC	DESKTOP-CSC	https://www.notion.so/help/guides/category/ai		192.168.1.95	123.63.117.88	Allowed - Warn Page	...

Request	Identity	Policy or Ruleset Identity	Destination	Destination IP	Internal IP	Action
DNS	DESKTOP-CSC	Lab - 123.63.117.88	www.notion.so		192.168.1.95	Allowed - Warn Page Displayed
DNS	DESKTOP-CSC	Lab - 123.63.117.88	www.notion.so		192.168.1.95	
WEB	DESKTOP-CSC	DESKTOP-CSC	https://www.notion.so/help/guides/category/ai		192.168.1.95	
DNS	DESKTOP-CSC	Lab - 123.63.117.88	www.notion.so		192.168.1.95	

Time Mar 15, 2024 4:03 PM
Ruleset or Rule Test
Rule Name Test1
Identity DESKTOP-CSC Lab - 123.63.117.88
Policy or Ruleset Identity DESKTOP-CSC
Internal IP Address 192.168.1.95
External IP Address 123.63.117.88
Destination https://www.notion.so/help/guides/category/ai Hostname www.notion.so
Categories Application Warn, Online Document Sharing and Collaboration Dispute Categorization Public Application Notion AI Application Category Generative AI
Content Type text/html
File Action (Remote Browser Isolation) -
Total Size in Bytes 1083

宛先リストの制限

警告ページ機能を有効にすると、宛先リストへのアクセスが制限されます。「警告」に分類されたWebサイトに対して「宛先リスト」オプションを選択することはできません。

HTTPSインスペクションの有効化

警告ページ機能を効果的に適用するには、Cisco UmbrellaでHTTPSインスペクションを有効にする必要があります。HTTPSインスペクションは、HTTPSトラフィックを復号化して検査し、Umbrellaで暗号化された接続に対してWarnページを適用できるようにします。

HTTPS Inspection

Enabled

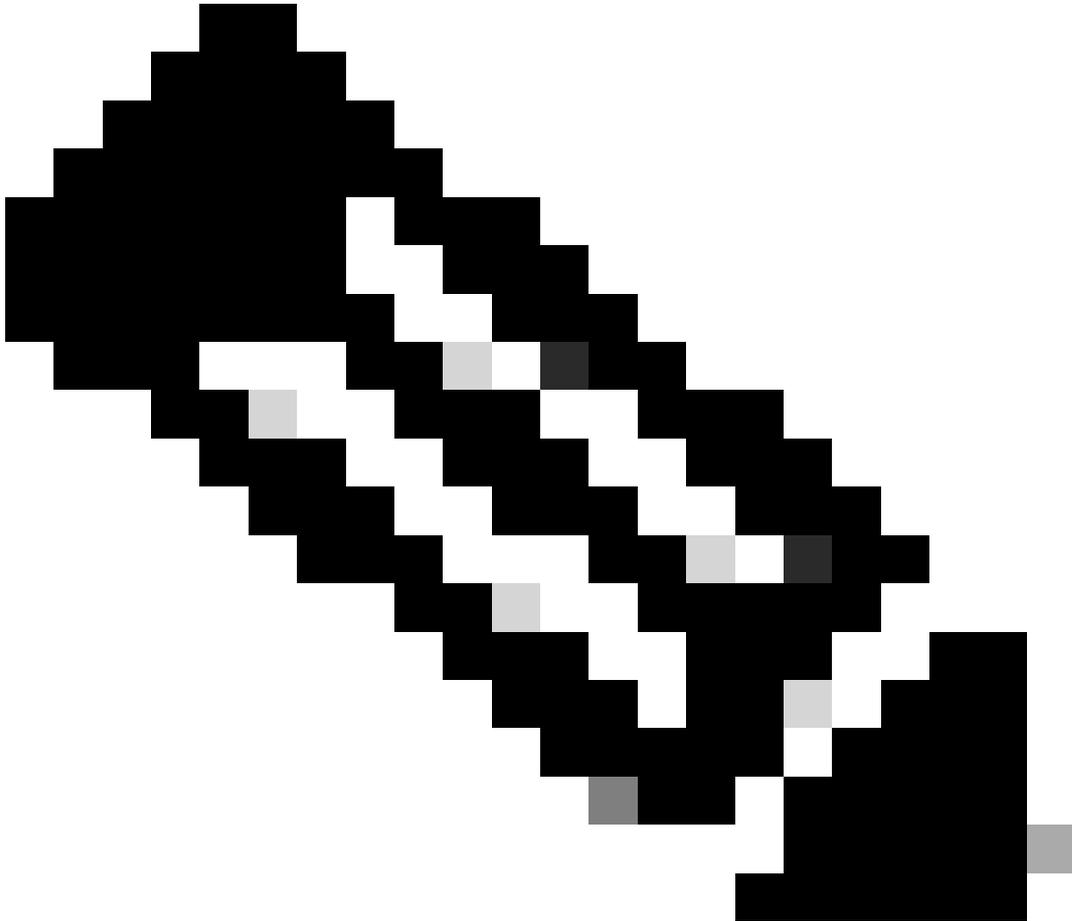
Edit

カスタム警告ページの作成

管理者は、パーソナライズされたメッセージを含むカスタムの警告ページを作成できます。この

カスタム警告ページは、ルールセットにルールを追加するときに選択でき、ユーザーに合わせてカスタマイズされた警告を提供します。

カスタム警告ページの作成手順、および警告ルールアクションの設定の詳細については、公式文書「[カスタム警告ページの作成](#)」を参照してください。



注：選択的な復号化リストの例外は、プロキシが特定のポリシーと機能を適用する機能に影響します。警告ページもその1つです。

結論

Warnルールアクションの設定と関連する制限を理解することは、Cisco Umbrella内に効果的なセキュリティポリシーを実装するために不可欠です。WarnページとHTTPSインスペクションを活用することで、組織はセキュリティポスチャを強化し、ユーザに安全なブラウジングエクスペリエンスを提供できます。

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。