FTDでSnort2のカスタムローカルSnortルールを設定する

内容

はじめに

このドキュメントでは、ファイアウォール脅威対策(FTD)のSnort2でカスタムローカルSnortルールを設定する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Firepower Management Center（FMC）
- ファイアウォール脅威対策(FTD)

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。

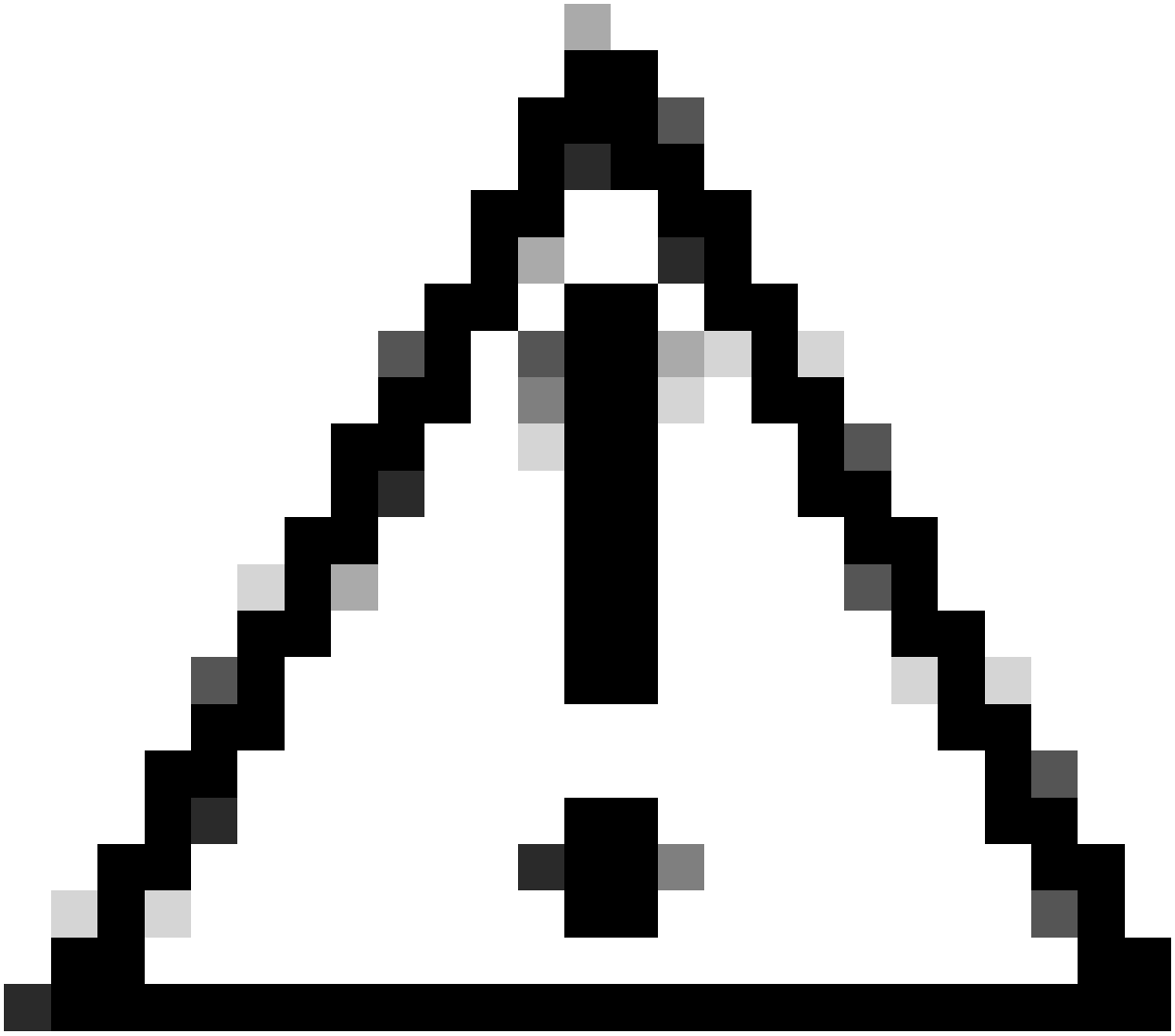
- VMWare 7.4.1向けCisco Firepower Management Center
- Cisco Firepower 2120 7.4.1

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。

背景説明

カスタムローカルSnortルールとは、FTDに統合されているSnort侵入検知および防御システム内で作成および実装できるユーザ定義ルールを指します。Cisco FTDでカスタムローカルSnortルールを作成すると、基本的にSnortエンジンが監視できる新しいパターンまたは一連の条件を定義することになります。ネットワークトラフィックがカスタムルールで指定した条件に一致する場合、Snortはアラートの生成やパケットのドロップなど、ルールで定義されたアクションを実行できます。 管理者は、カスタムローカルSnortルールを使用して、一般的なルールセットの対象外である特定の脅威に対処します。

このドキュメントでは、特定の文字列（ユーザ名）を含むHTTP応答パケットを検出してドロップするように設計されたカスタムローカルSnortルールを設定し、確認する方法を紹介します。

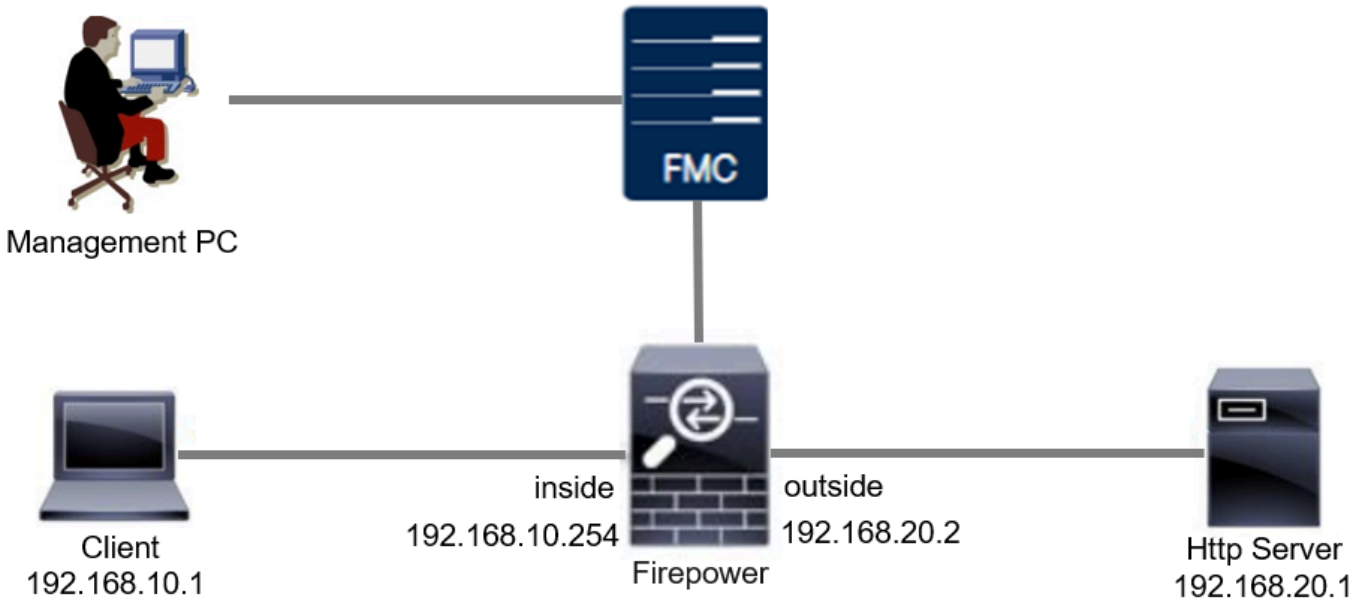


注意：カスタムのローカルSnortルールを作成してサポートすることは、TACのサポート対象外です。したがって、このドキュメントは参考資料としてのみ使用でき、これらのカスタムルールは独自の裁量と責任で作成および管理してください。

設定

ネットワーク図

このドキュメントでは、この図のSnort2のカスタムローカルSnortルールの設定および検証について説明します。

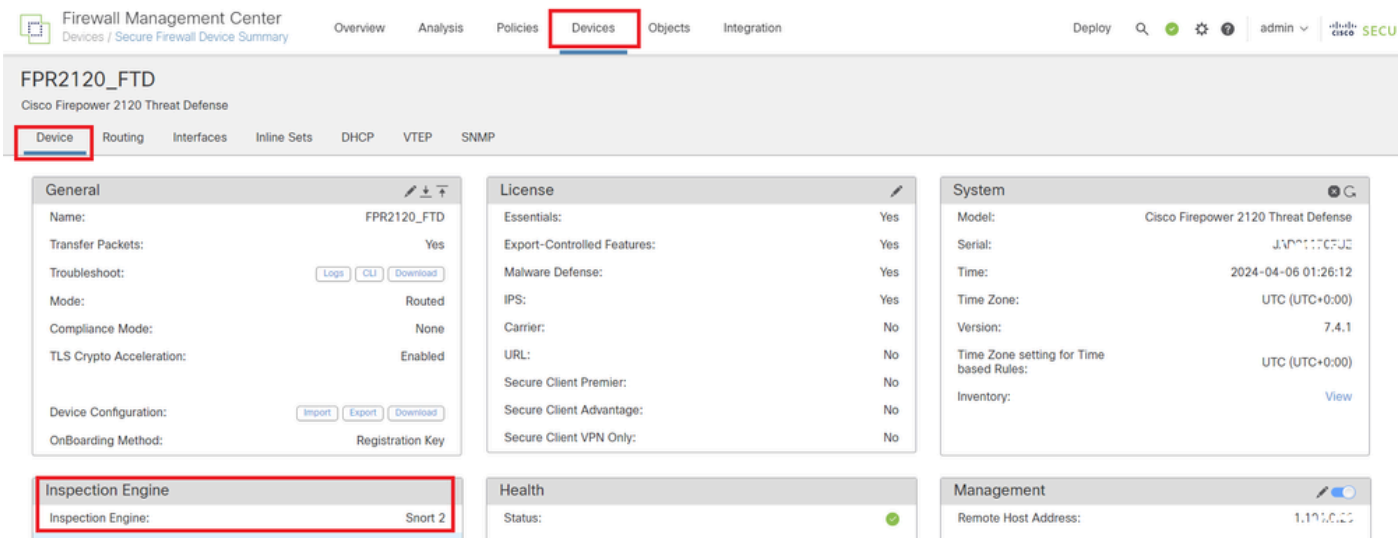


コンフィギュレーション

これは、特定の文字列（ユーザ名）を含むHTTP応答パケットを検出してドロップするカスタムローカルSnortルールの設定です。

ステップ 1：Snortバージョンの確認

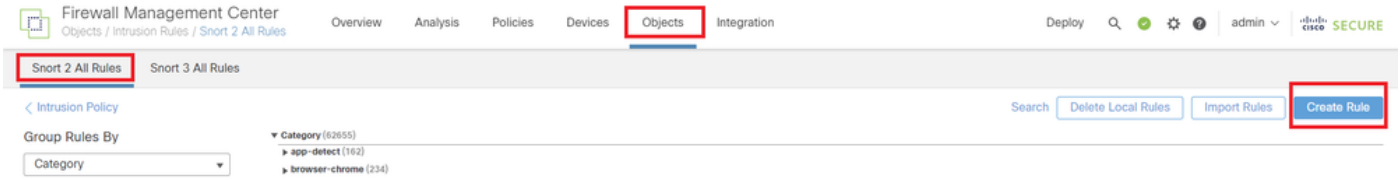
FMCでDevices > Device Managementの順に移動し、Deviceタブをクリックします。Snortのバージョンがsnort2であることを確認します。



Snortバージョン

ステップ 2：Snort 2でのカスタムローカルSnortルールの作成

FMCで、Objects > Intrusion Rules > Snort 2 All Rulesの順に移動し、Create Rule ボタンをクリックします。

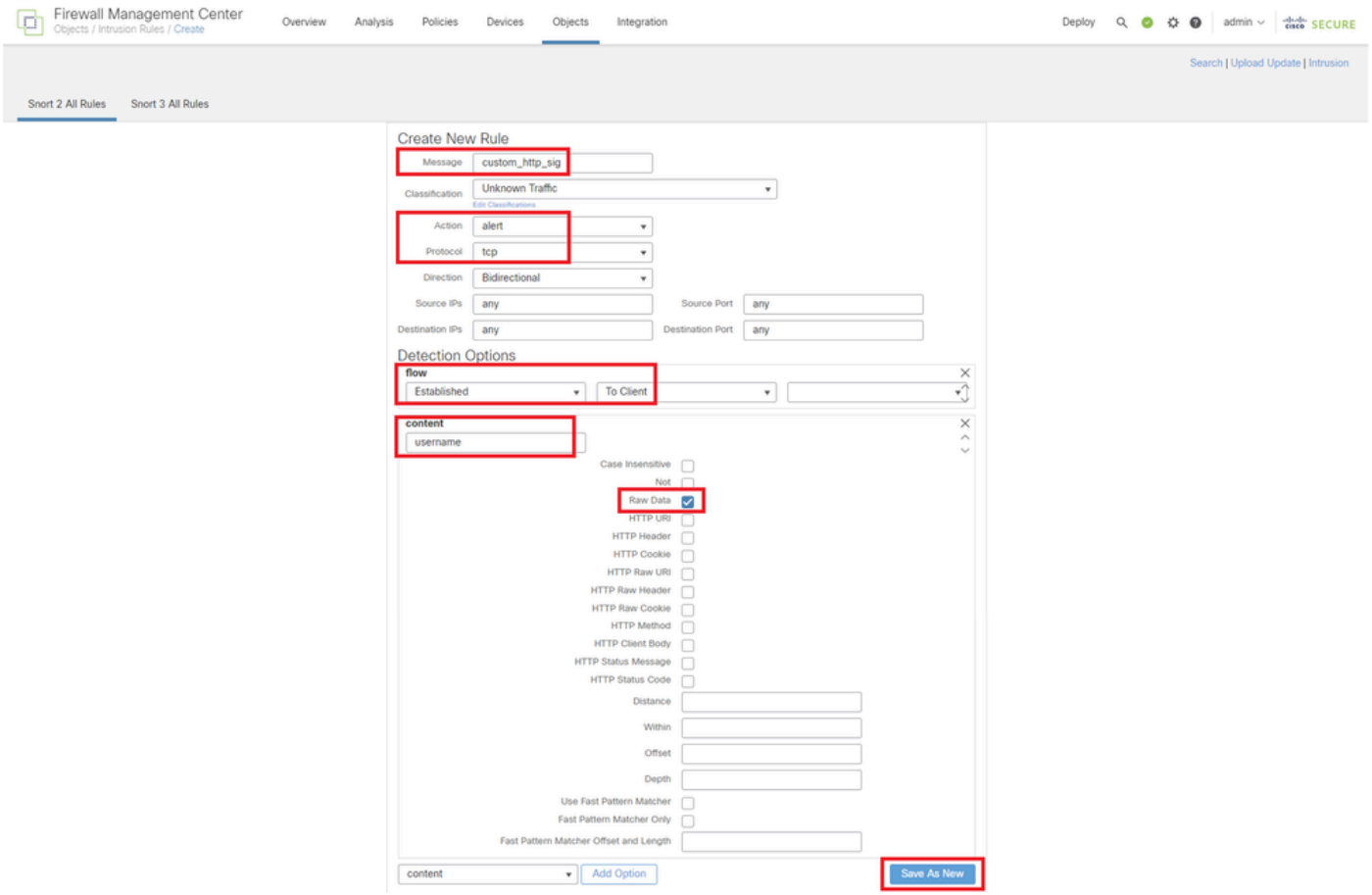


カスタムルールの作成

カスタムローカルSnortルールに必要な情報を入力します。

- 侵入:custom_http_sig
- アクション：アラート
- プロトコル:tcp
- フロー：確立、クライアントへ

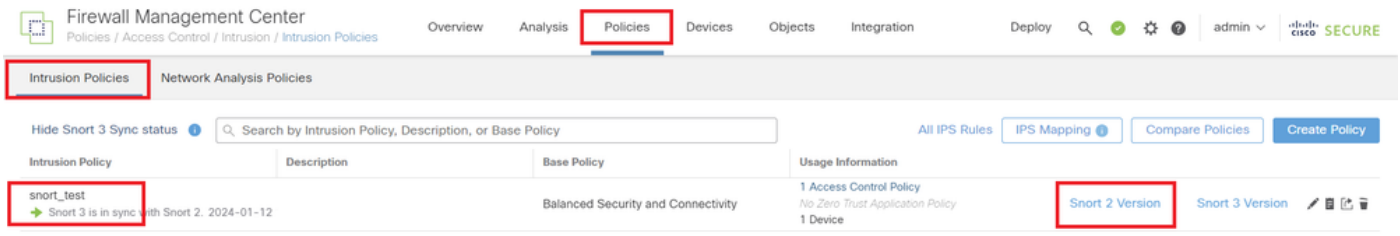
- コンテンツ：ユーザ名（未加エデータ）



ルールに必要な情報の入力

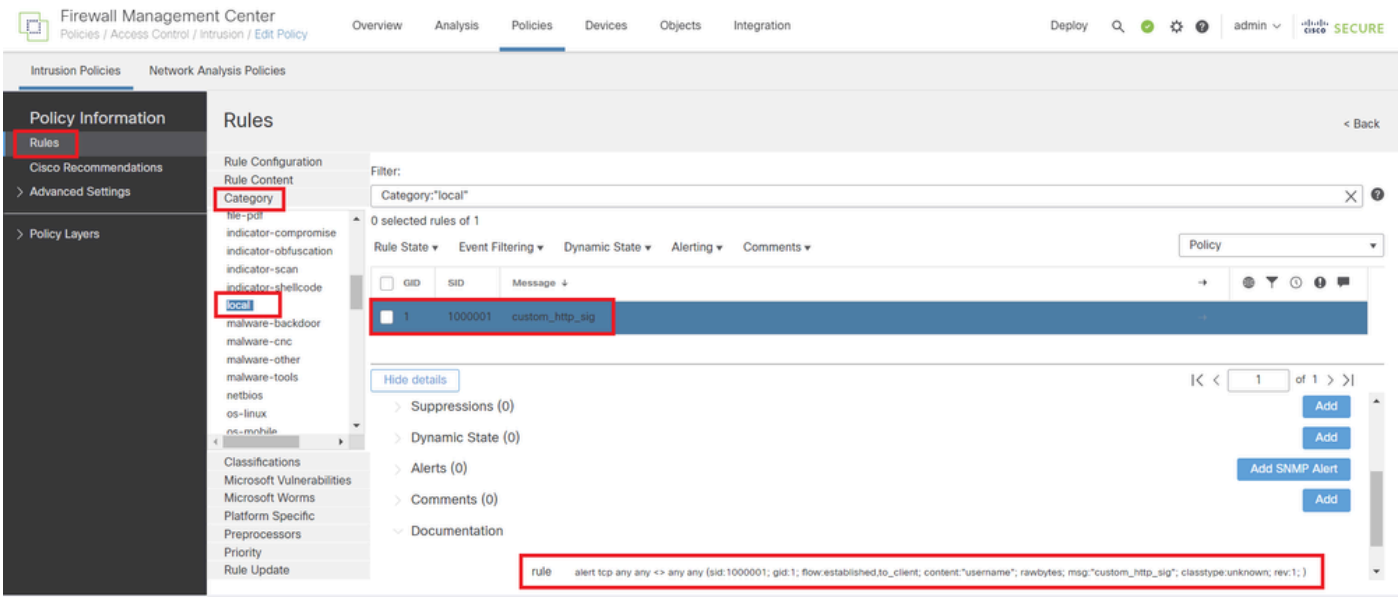
ステップ 3：カスタムローカルSnortルールの確認

FMCでPolicies >Intrusion Policiesの順に移動し、Snort 2 Versionボタンをクリックします。



カスタムルールの確認

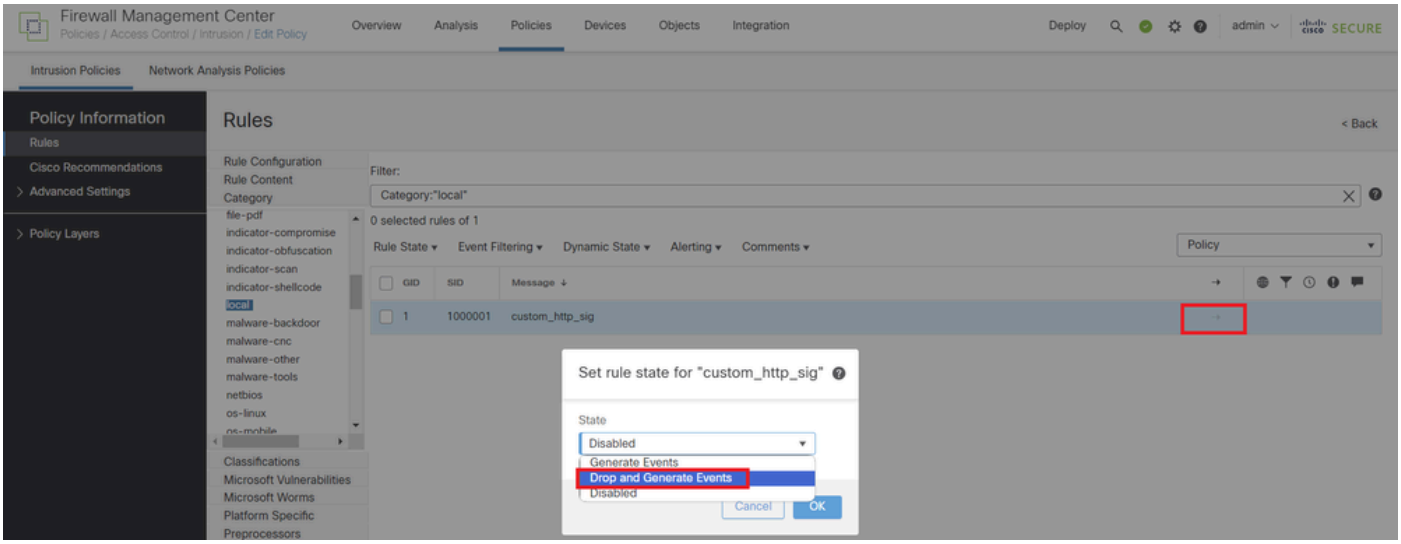
FMCでRules > Category > localの順に移動し、Custom Local Snort Ruleの詳細を確認します。



カスタム規則の詳細

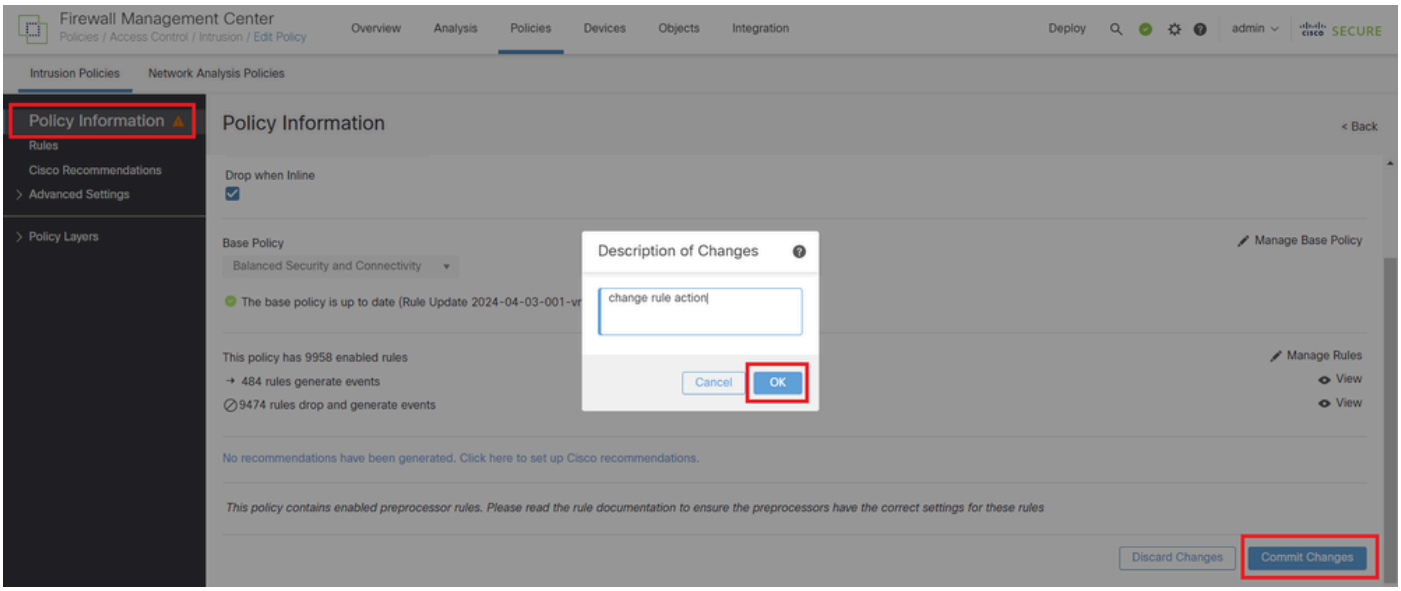
ステップ 4：ルールの変更アクション

Stateボタンをクリックし、StateをDrop and Generate Eventsに設定して、OKボタンをクリックします。



ルールアクションの変更

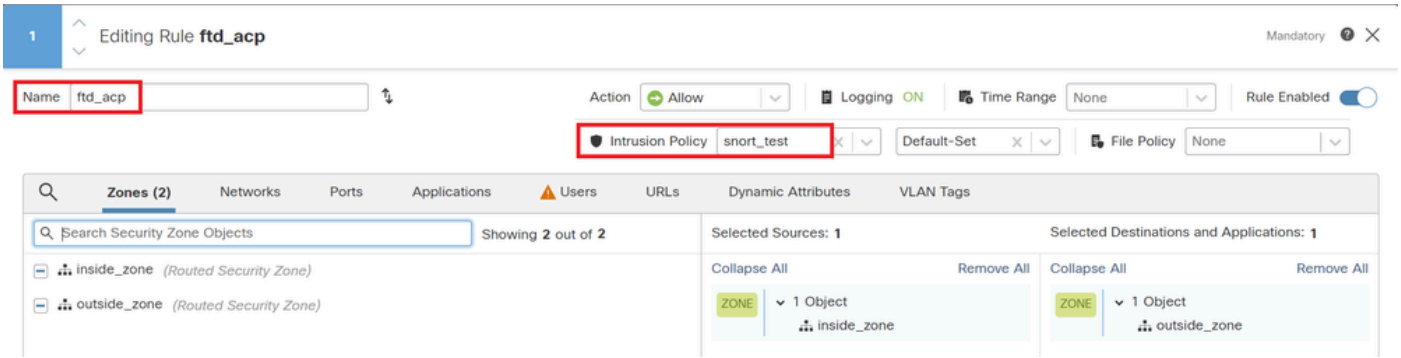
Policy Informationボタンをクリックし、Commit Changesボタンをクリックして変更を保存します。



変更の確定

ステップ 5：侵入ポリシーとアクセスコントロールポリシー(ACP)ルールの関連付け

FMCでPolicies >Access Controlの順に移動し、侵入ポリシーをACPに関連付けます。



ACPルールとの関連付け

手順 6：変更の展開

変更をFTDに展開します。

変更の展開

確認

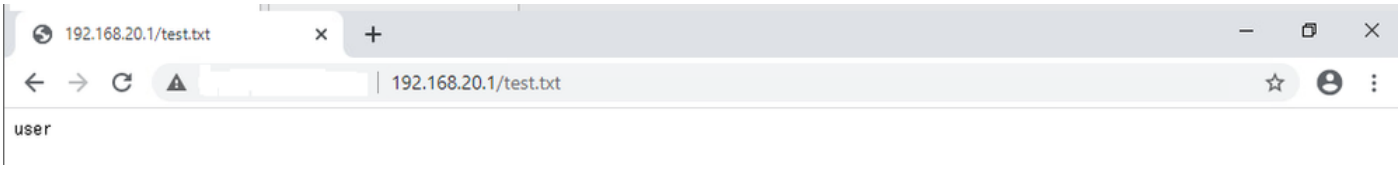
カスタムローカルSnortルールがトリガーされない

ステップ 1：HTTPサーバでのファイル内容の設定

HTTPサーバ側のtest.txtファイルの内容をuserに設定します。

ステップ 2：初期HTTP要求

クライアント(192.168.10.1)のブラウザからHTTPサーバ(192.168.20.1/test.txt)にアクセスし、HTTP通信が許可されていることを確認します。



初期HTTP要求

カスタムローカルSnortルールがトリガーされる

ステップ 1：HTTPサーバでのファイル内容の設定

HTTPサーバ側のtest.txtファイルの内容をusernameに設定します。

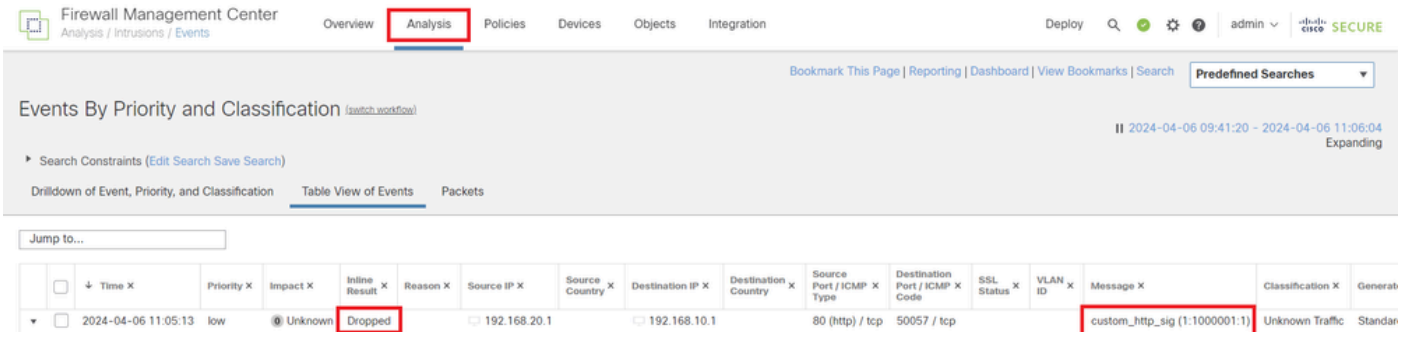
ステップ 2：初期HTTP要求

クライアント(192.168.10.1)のブラウザからHTTPサーバ(192.168.20.1/test.txt)にアクセスし、HTTP通信がブロックされていることを確認します。

初期HTTP要求

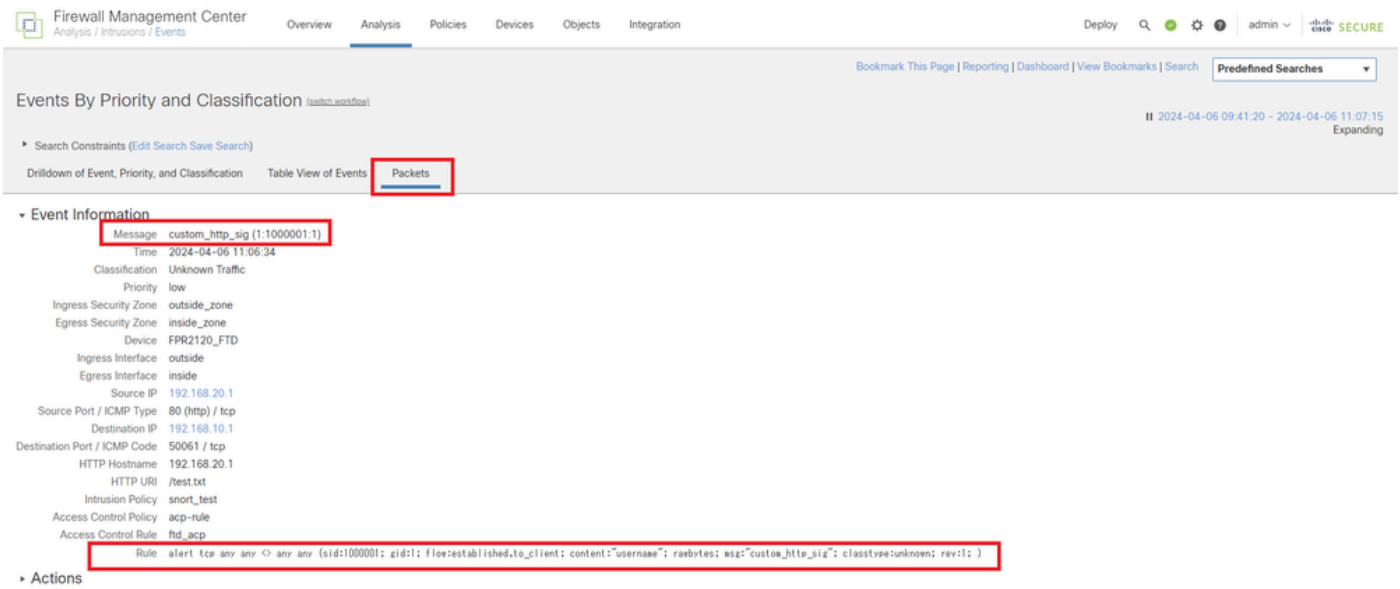
ステップ 3：侵入イベントの確認

FMCでAnalysis > Intrusions > Eventsの順に移動し、侵入イベントがカスタムローカルSnortルールによって生成されていることを確認します。



侵入イベント

Packetsタブをクリックし、侵入イベントの詳細を確認します。



侵入イベントの詳細

トラブルシュート

system support traceコマンドを実行して、FTDの動作を確認します。この例では、HTTPトラフィックはIPSルール(gid 1、sid 1000001)によってブロックされています。

<#root>

>

system support trace

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.1
Please specify a client port:
Please specify a server IP address: 192.168.20.1
Please specify a server port:

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Firewall: allow rule, '
```

ftd_acp

', allow
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0

IPS Event

:

gid 1

,

sid 1000001

, drop

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Snort id 3, NAP id 2, IPS id 1, Verdict BLOCKFLOW
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 ===>

Blocked by IPS

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。