

# FTDでSnort3のカスタムローカルSnortルールを設定する

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[方式 1.Snort 2からSnort 3へのインポート](#)

[ステップ 1: Snortバージョンの確認](#)

[ステップ 2: Snort 2でのカスタムローカルSnortルールの作成または編集](#)

[ステップ 3: Snort 2からSnort 3へのカスタムローカルSnortルールのインポート](#)

[ステップ 4: ルールの変更アクション](#)

[ステップ 5: インポートされたカスタムローカルSnortルールの確認](#)

[手順 6: 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](#)

[手順 7: 変更の展開](#)

[方式 2.ローカルファイルのアップロード](#)

[ステップ 1: Snortバージョンの確認](#)

[ステップ 2: カスタムローカルSnortルールの作成](#)

[ステップ 3: カスタムローカルSnortルールのアップロード](#)

[ステップ 4: ルールの変更アクション](#)

[ステップ 5: アップロードされたカスタムローカルSnortルールの確認](#)

[手順 6: 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](#)

[手順 7: 変更の展開](#)

[確認](#)

[ステップ 1: HTTPサーバでのファイルの内容の設定](#)

[ステップ 2: 初期HTTP要求](#)

[ステップ 3: 侵入イベントの確認](#)

[よく寄せられる質問 \(FAQ\)](#)

[トラブルシューティング](#)

[参考](#)

---

## 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Snort3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。

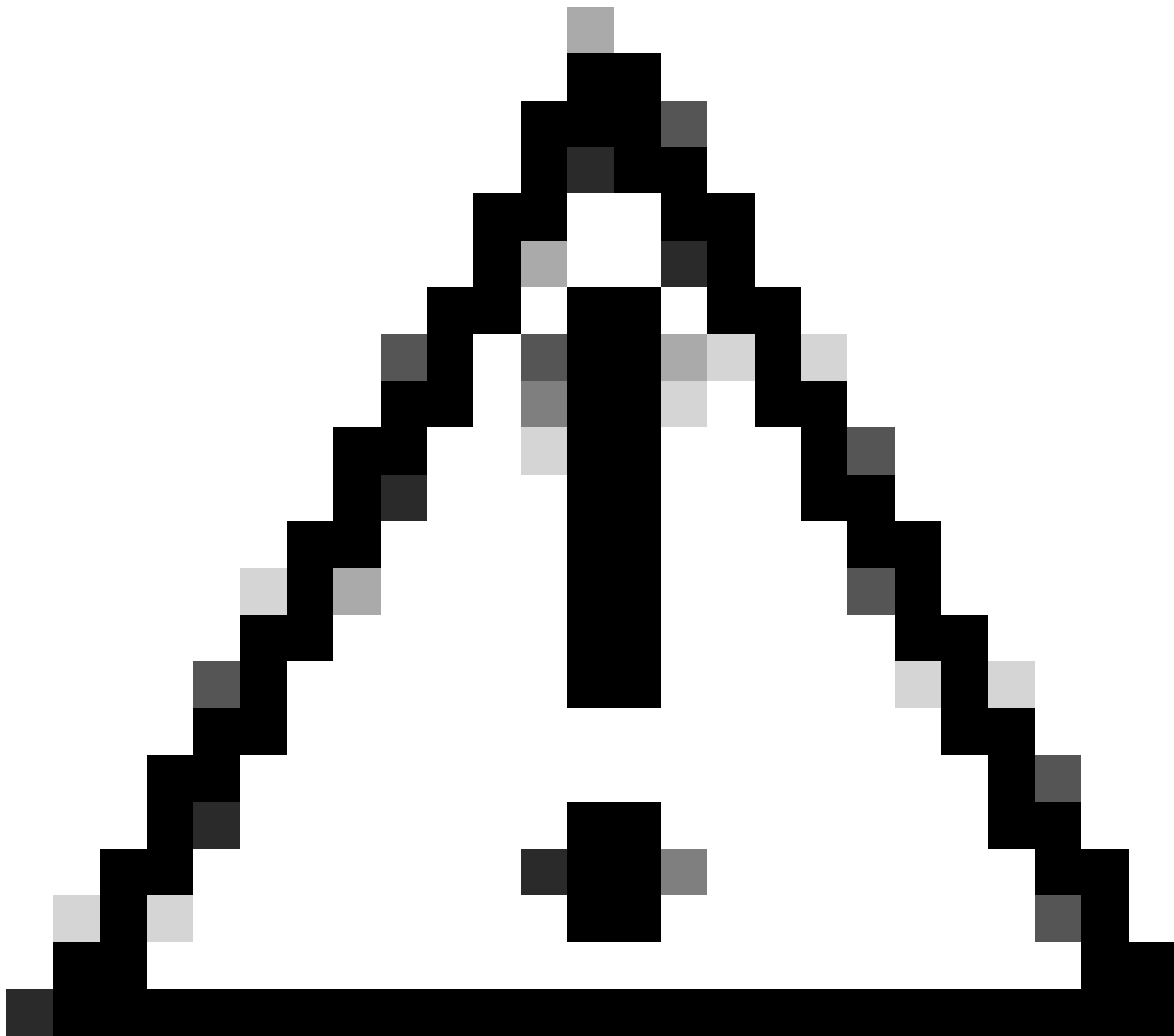
- VMWare 7.4.1向けCisco Firepower Management Center
- Cisco Firepower 2120 7.4.1

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

Management Centerを使用した脅威対策におけるSnort 3のサポートは、バージョン7.0以降で開始されます。バージョン7.0以降の新規および再イメージ化デバイスでは、Snort 3がデフォルトのインスペクションエンジンです。

このドキュメントでは、Snort 3用にSnortルールをカスタマイズする方法の例と、実際の検証例を紹介します。具体的には、特定の文字列（ユーザ名）を含むHTTPパケットをドロップするようにカスタマイズされたSnortルールを使用して侵入ポリシーを設定および確認する方法を紹介します。

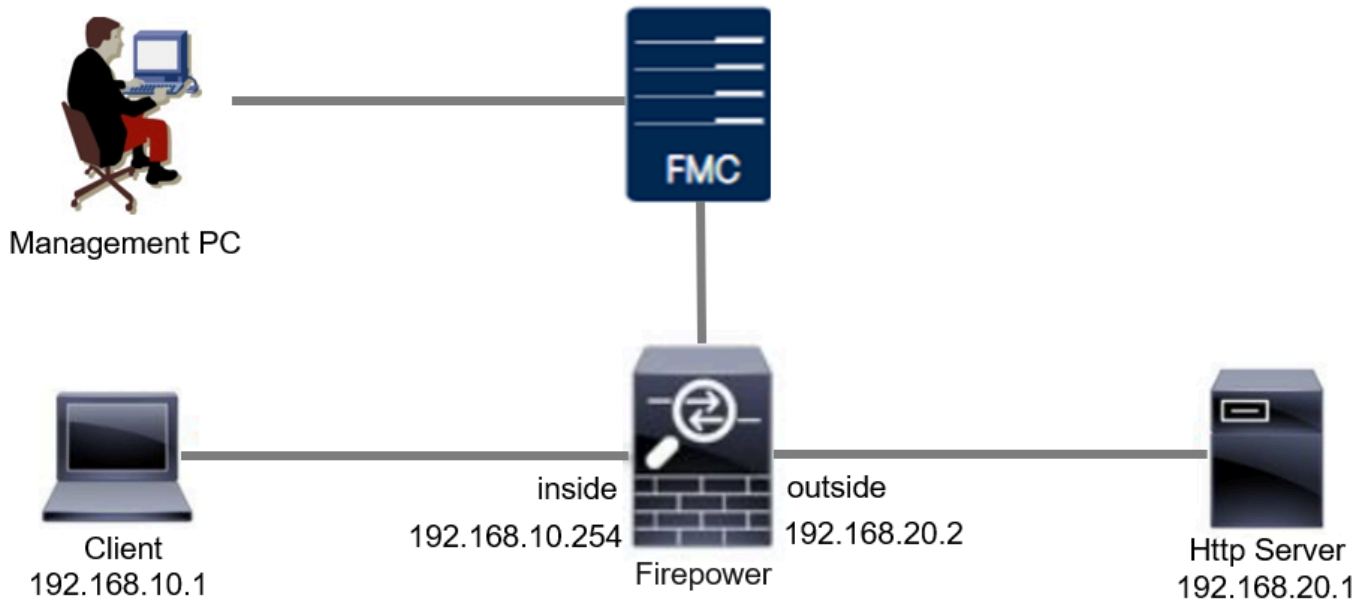


注意：カスタムのローカルSnortルールを作成してサポートを提供することは、TACのサポート対象外です。したがって、このドキュメントは参考資料としてのみ使用でき、これらのカスタムルールは独自の裁量と責任で作成および管理してください。

---

## ネットワーク図

このドキュメントでは、次の図に示すSnort3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。



ネットワーク図

## 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。



注：現時点では、FMC GUIのSnort 3 All RulesページからカスタムローカルSnortルールを追加することはできません。このドキュメントで紹介する方法を使用する必要があります。

---

## 方式 1.Snort 2からSnort 3へのインポート

### 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、Devicetabをクリックします。SnortのバージョンがSnort3であることを確認します。

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (1)						
FPR2120_FTD 1.10.0.29	Firepower 2120 with FTD	7.4.1	N/A	Essentials, IPS (1 more...)	acp-rule	

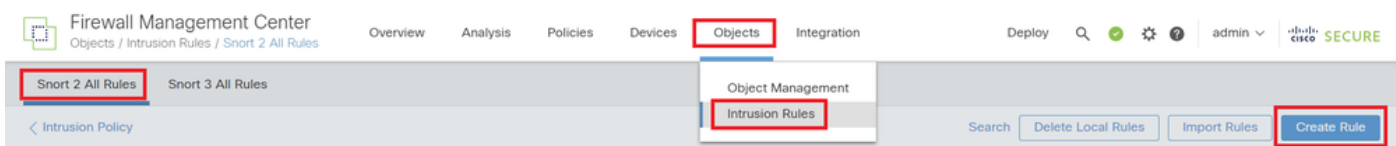
Snortバージョン

## ステップ 2 : Snort 2でのカスタムローカルSnortルールの作成または編集

FMCで、Objects > Intrusion Rules > Snort 2 All Rulesの順に移動します。Create RuleボタンをクリックしてカスタムローカルSnortルールを追加するか、FMCでObjects > Intrusion Rules > Snort 2 All Rules > Local Rulesの順に選択し、Editボタンをクリックして既存のカスタムローカルSnortルールを編集します。

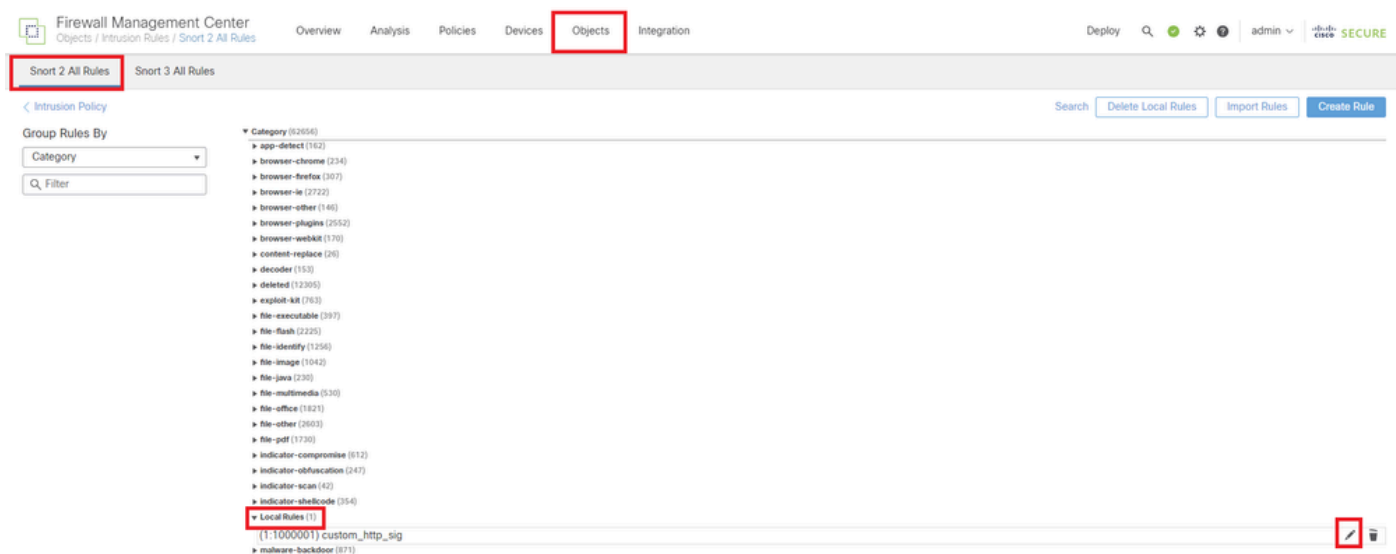
Snort 2でカスタムローカルSnortルールを作成する方法については、「[FTDでSnort2でカスタムローカルSnortルールを設定する](#)」を参照してください。

図に示すように、新しいカスタムローカルSnortルールを追加します。



新しいカスタムルールの追加

図に示すように、既存のカスタムローカルSnortルールを編集します。この例では、既存のカスタム規則を編集します。



既存のカスタム規則の編集

特定の文字列 ( ユーザ名 ) を含むHTTPパケットを検出するためのシグニチャ情報を入力します

- メッセージ: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 ( 未加工データ )

ルールに必要な情報の入力

### ステップ 3 : Snort 2からSnort 3へのカスタムローカルSnortルールのインポート

FMCでObjects > Intrusion Rules > Snort 3 All Rules > All Rulesの順に移動し、Convert Snort 2 rules and Import from Tasks プルダウンリストをクリックします。

警告メッセージをチェックして、OKをクリックします。

## Convert Snort 2 rules and import



The Snort 2 local rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. This action will convert all Snort 2 local rules to Snort 3 rules. All the enabled rules per the Snort 2 version of the policy will be added into different groups and enabled in the corresponding Snort 3 version of the policy.

Cancel

OK

警告メッセージ

FMCでObjects > Intrusion Rules > Snort 3 All Rulesの順に移動し、All Snort 2 Converted Globalをクリックして、インポートされたカスタムローカルSnortルールを確認します。

Firewall Management Center  
Objects / Intrusion Rules / Snort 3 All Rules

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings Admin Secure

Snort 2 All Rules Snort 3 All Rules

Intrusion Policy

All Rules

- Local Rules (1 group)
  - All Snort 2 Converted Global
- MITRE (1 group)
- Rule Categories (9 groups)

Local Rules / All Snort 2 Converted Global

Description: Group created for custom rules enabled in snort 2 version

Rule Actions: Search by CVE, SID, Reference Info, or Rule Message

1 rule

The custom rules were successfully imported

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups	Alert Configuration
<input checked="" type="checkbox"/>	2000:1000000	custom_http_sig	Disable (Default)	All Snort 2 Converted Glo...	None

インポートされたカスタム規則の確認

### ステップ 4 : ルールの変更アクション

ターゲットカスタムルールのルールアクションに従って、Per Intrusion Policyをクリックします。



The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The main content area is titled 'Local Rules / All Snort 2 Converted Global'. A table lists rules, with one rule highlighted: '2000:1000000 custom\_http\_sig'. A dropdown menu is open for this rule, showing options: 'Disable (Default)', 'Block', 'Alert', 'Rewrite', 'Drop', 'Pass', 'Reject', 'Disable (Default)', 'Revert to default', and 'Per Intrusion Policy'. The 'Per Intrusion Policy' option is highlighted with a red box. A message above the table states: 'The custom rules were successfully imported X'.

ルールの変更アクション

Edit Rule Action画面で、PolicyとRule Actionに関する情報を入力します。

- ポリシー:snort\_test
- ルールアクション:BLOCK



注：ルールの処理は次のとおりです。

**Block**：イベントを生成し、現在的一致するパケットとこの接続の後続のすべてのパケットをブロックします。

**Alert**：一致するパケットのイベントのみを生成し、パケットや接続をドロップしません。

**Rewrite**：ルールのreplaceオプションに基づいて、イベントを生成し、パケットの内容を上書きします。

**通過**：イベントは生成されず、後続のSnortルールによる評価を受けずにパケットの通過が許可されます。

**ドロップ**：イベントを生成し、一致するパケットをドロップします。この接続ではこれ以上トラフィックをブロックしません。

**Reject**：イベントを生成し、一致するパケットをドロップします。この接続で今後のトラフィックをブロックし、それがTCPプロトコルである場合はTCP resetを送信元ホストと

---

宛先ホストに送信します。

Disable : このルールに対してトラフィックを照合しません。イベントは生成されません。

デフォルト – システムのデフォルトのアクションに戻します。

Edit Rule Action

2000:100... | custom\_http\_sig

All Policies  Per Intrusion Policy

Policy: snort\_test

Rule Action: BLOCK

Add Another

Comments (optional): Provide a reason to change if applicable

Cancel Save

ルールアクションの編集

ステップ 5 : インポートされたカスタムローカルSnortルールの確認

FMCでPolicies > Intrusion Policiesの順に移動し、行のターゲット侵入ポリシーに対応するSnort 3 Versionをクリックします。

Firewall Management Center

Policies / Access Control / Intrusion / Intrusion Policies

Overview Analysis Policies Devices Objects Integration Deploy

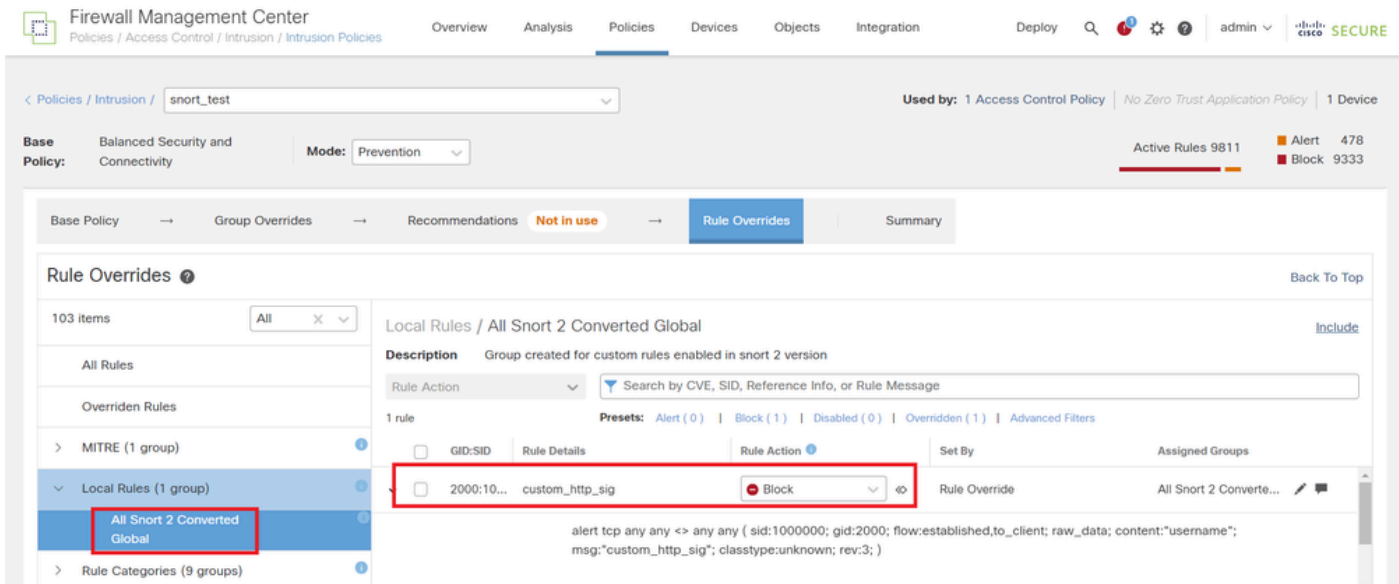
Intrusion Policies Network Analysis Policies

Hide Snort 3 Sync status Search by Intrusion Policy, Description, or Base Policy All IPS Rules IPS Mapping Compare Policies Create Policy

Intrusion Policy	Description	Base Policy	Usage Information
snort_test → Snort 3 is in sync with Snort 2. 2024-01-12		Balanced Security and Connectivity	1 Access Control Policy No Zero Trust Application Policy 1 Device Snort 2 Version Snort 3 Version

インポートされたカスタム規則の確認

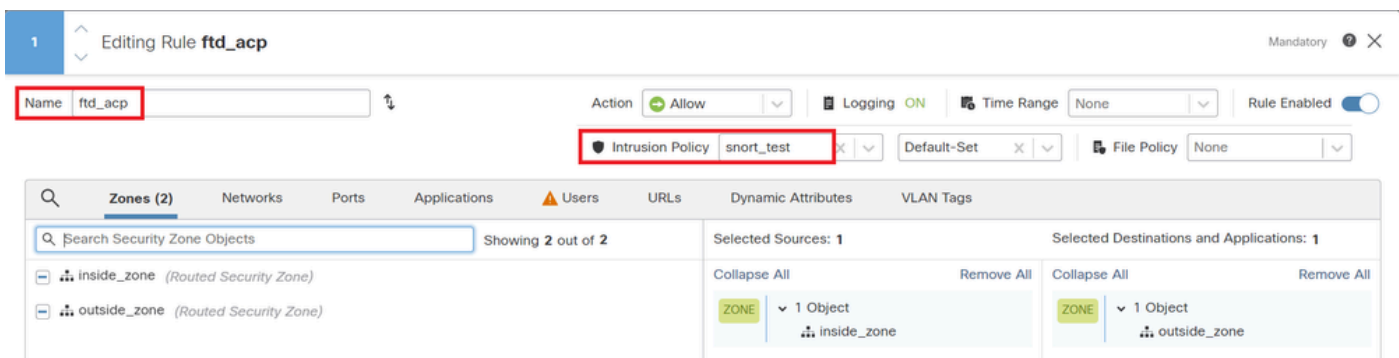
Local Rules > All Snort 2 Converted Globalの順にクリックして、カスタムローカルSnortルールの詳細を確認します。



インポートされたカスタム規則の確認

## 手順 6 : 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 7 : 変更の展開

変更をFTDに展開します。



変更の展開

## 方式 2.ローカルファイルのアップロード

### ステップ 1 : Snortバージョンの確認

方法1のステップ1と同じです。

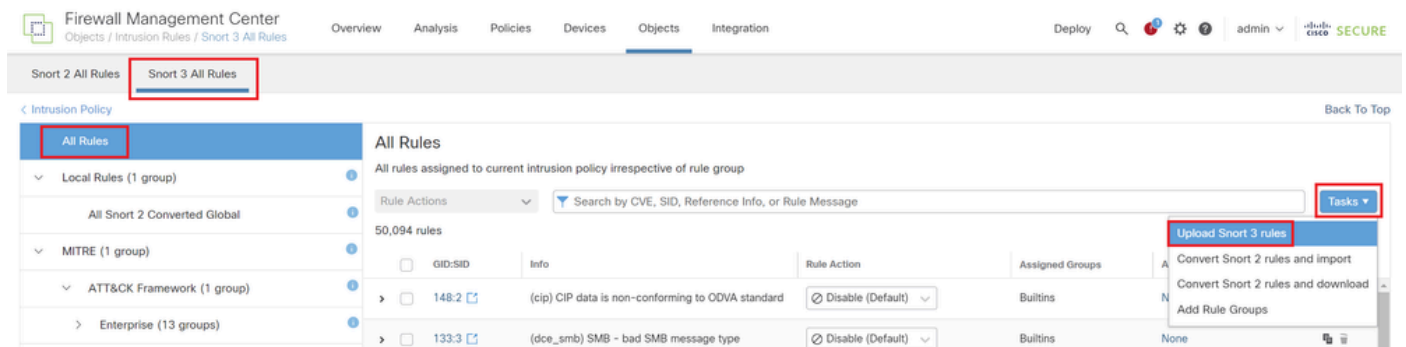
### ステップ 2 : カスタムローカルSnortルールの作成

カスタムローカルSnortルールを手動で作成し、custom-rules.txtという名前のローカルファイルに保存します。

```
alert tcp any any <> any any ( sid:1000000; flow:established,to_client; raw_data; content:"username"; m
```

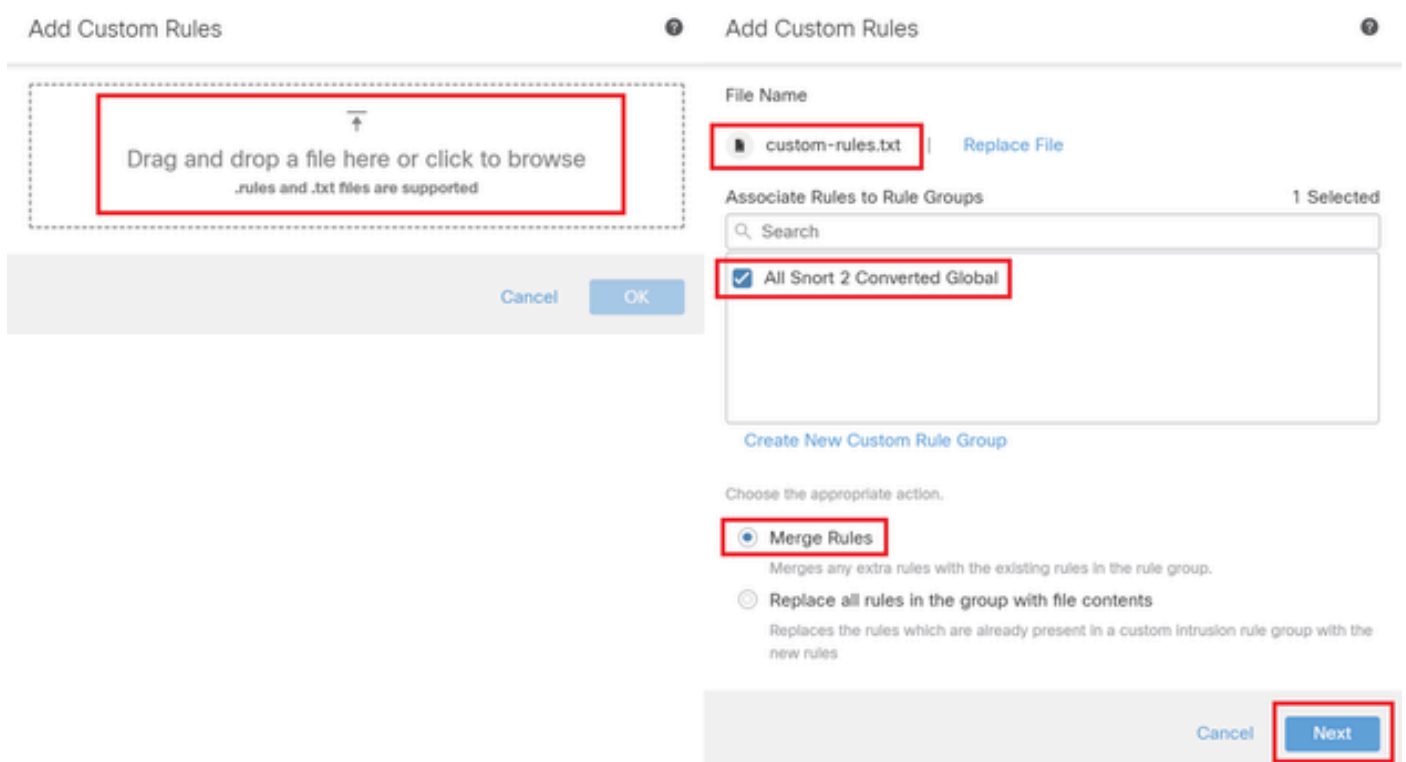
### ステップ 3 : カスタムローカルSnortルールのアップロード

FMCでObjects > Intrusion Rules > Snort 3 All Rules > All Rulesの順に移動し、TasksプルダウンリストからUpload Snort 3 rules をクリックします。



カスタムルールのアップロード

Add Custom Rules画面で、ローカルのcustom-rules.txtファイルをドラッグアンドドロップし、Rule Groups (この例ではMerge Rules) と適切なアクション (この例ではMerge Rules) を選択して、Nextボタンをクリックします。



カスタムルールの追加

ローカルルールファイルが正常にアップロードされたことを確認します。

## Add Custom Rules



### Summary

✓ 1 new rule

2000:1000000

Download the summary file.

Back

Finish

アップロード結果の確認

FMCでObjects > Intrusion Rules > Snort 3 All Rulesの順に移動し、All Snort 2 Converted Globalをクリックして、アップロードされたカスタムローカルSnortルールを確認します。

The screenshot shows the Fire Management Center interface. The breadcrumb path is Objects / Intrusion Rules / Snort 3 All Rules. The 'Snort 3 All Rules' tab is selected. Under 'Local Rules / All Snort 2 Converted Global', a rule with ID '2000:1000000' and name 'custom\_http\_sig' is highlighted. The rule details show it is disabled and has the following configuration:

```
alert tcp any any <-> any any ( sid:1000000, gid:2000, flow:established,to_client, raw_data, content:"username"; msg:"custom_http_sig"; classtype:unknown; rev:3; )
```

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

方法1のステップ4と同じです。

ステップ 5 : アップロードされたカスタムローカルSnortルールの確認

方法1のステップ5と同じです。

手順 6 : 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

方法1のステップ6と同じです。

## 手順 7：変更の展開

方法1のステップ7と同じです。

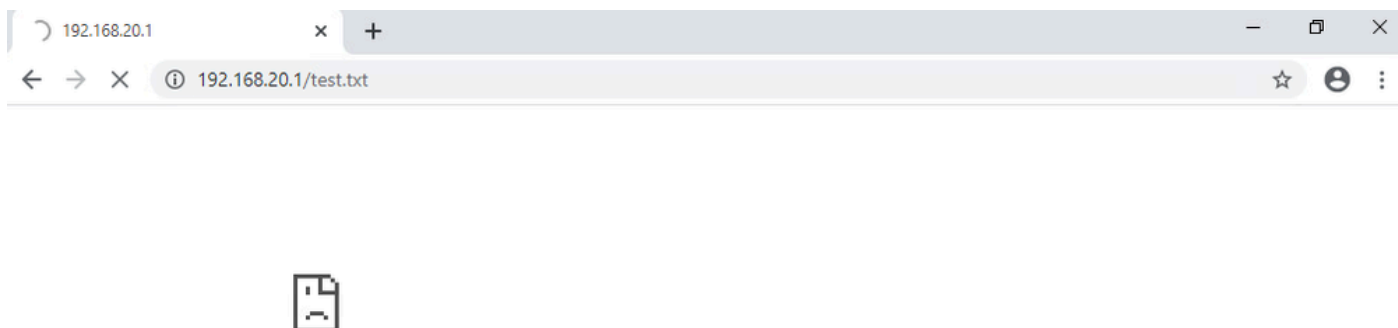
## 確認

### ステップ 1：HTTPサーバでのファイルの内容の設定

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

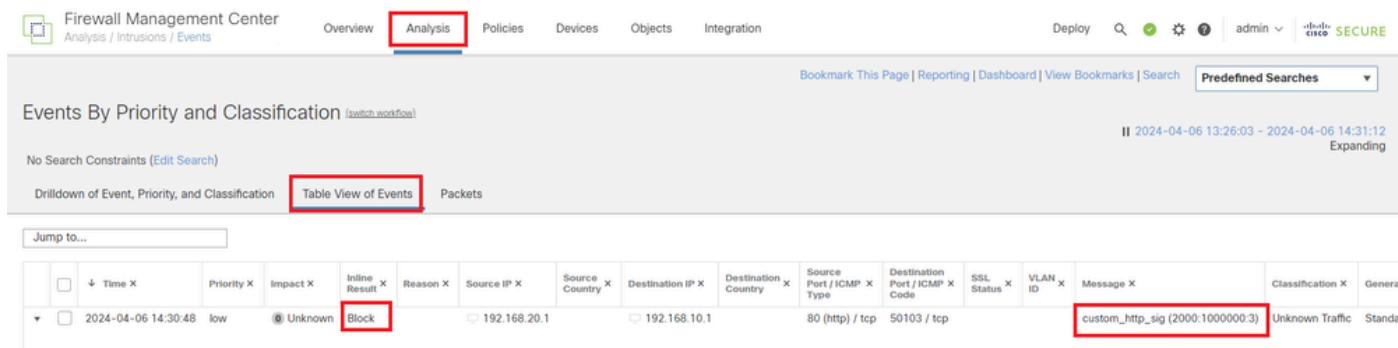
クライアント(192.168.10.1)のブラウザからHTTPサーバ(192.168.20.1/test.txt)にアクセスし、HTTP通信がブロックされていることを確認します。



### 初期HTTP要求

### ステップ 3：侵入イベントの確認

Analysis>Intrusions>Eventson FMC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ることを確認します。

A screenshot of the Cisco Firepower Management Center (FMC) interface. The 'Analysis' tab is selected. The main area shows 'Events By Priority and Classification' for the period 2024-04-06 13:26:03 to 2024-04-06 14:31:12. A table of events is displayed, with one event highlighted. The event details are as follows:

Time	Priority	Impact	Inline Result	Reason	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	VLAN ID	Message	Classification	General
2024-04-06 14:30:48	low	Unknown	Block		192.168.20.1		192.168.10.1		80 (http) / tcp	50103 / tcp			custom_http_sig (2000:1000000:3)	Unknown Traffic	Standar

### 侵入イベント

Packetstabをクリックし、侵入イベントの詳細を確認します。

The screenshot shows the FMC Analysis page with the following details:

- Navigation: Overview, Analysis (selected), Policies, Devices, Objects, Integration
- Page Title: Events By Priority and Classification
- Search: No Search Constraints (Edit Search)
- View: Packets (selected)
- Event Information:
  - Message: custom\_http\_sig (2000:1000000:3)
  - Time: 2024-04-06 14:31:26
  - Classification: Unknown Traffic
  - Priority: low
  - Ingress Security Zone: outside\_zone
  - Egress Security Zone: inside\_zone
  - Device: FPR2120\_FTD
  - Ingress Interface: outside
  - Egress Interface: inside
  - Source IP: 192.168.20.1
  - Source Port / ICMP Type: 80 (http) / tcp
  - Destination IP: 192.168.10.1
  - Destination Port / ICMP Code: 50105 / tcp
  - HTTP Hostname: 192.168.20.1
  - HTTP URI: /nest.txt
  - Intrusion Policy: snort\_test
  - Access Control Policy: acp\_rule
  - Access Control Rule: ftd\_acp
- Rule: alert tcp any any < any any ( sid:1000000; gid:2000; flow:established,to\_client; rax\_data: content:'username'; msg:'custom\_http\_sig'; classtype:unknown; rev:3; )

侵入イベントの詳細

## よく寄せられる質問 ( FAQ )

Q:Snort 2とSnort 3のどちらが推奨されますか。

A:Snort 2と比較して、Snort 3は処理速度の向上と新機能を備えているため、より推奨されるオプションです。

Q:7.0より前のバージョンのFTDから7.0以降のバージョンにアップグレードした後、Snortのバージョンは自動的にSnort 3に更新されますか。

A: いいえ。インスペクションエンジンはSnort 2上に残ります。アップグレード後にSnort 3を使用するには、明示的に有効にする必要があります。Snort 2は今後のリリースで廃止される予定であり、今すぐ使用しないことを強く推奨します。

Q:Snort 3では、既存のカスタムルールを編集できますか。

A: いいえ、編集できません。特定のカスタム規則を編集するには、関連する規則を削除して再作成する必要があります。

## トラブルシューティング

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(2000:1000000:3)によってブロックされます。

```
<#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:

```
192.168.10.1 50104 -> 192.168.20.1 80 6 AS=0 ID=4 GR=1-1 Firewall: allow rule, '
```

```
ftd_acp
```

```
', allow
```

```
192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1
```

```
Event
```

```
:
```

```
2000:1000000:3
```

```
, Action
```

```
block
```

```
192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist
```

```
192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict Reason:
```

```
ips, block
```

参考

[Cisco Secure Firewall Management Center Snort 3コンフィギュレーションガイド](#)

## 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。