Snort3ネットワーク分析ポリシーを開始するには

この章では、ネットワーク分析ポリシーの基礎、前提条件、およびネットワーク分析ポリシーの管理方法について説明します。カスタムネットワーク分析ポリシーの作成とネットワーク分析ポリシーの設定に関する情報も提供します。

- ネットワーク分析ポリシーの概要 （1 ページ）
- ネットワーク分析ポリシーの管理 （2 ページ）
- ネットワーク分析ポリシーの Snort 3 の定義と用語 （3 ページ）
- ネットワーク分析と侵入ポリシーの前提条件 （6 ページ）
- Snort 3 の場合のカスタムネットワーク分析ポリシーの作成 （7 ページ）
- ネットワーク分析ポリシーの設定とキャッシュされた変更 （36 ページ）

ネットワーク分析ポリシーの概要

ネットワーク分析ポリシーは、多数のトラフィックの前処理オプションを制御し、アクセスコントロールポリシーの詳細設定で呼び出されます。ネットワーク分析に関連する前処理は、セキュリティ インテリジェンスによる照合や SSL 復号化の後、侵入またはファイル検査の開始前に実行されます。

デフォルトでは、システムは Balanced Security and Connectivity ネットワーク分析ポリシーを使用して、アクセス コントロール ポリシーによって処理されるすべてのトラフィックを前処理します。ただし、この前処理を実行するために別のデフォルトのネットワーク分析ポリシーを選択できます。便宜を図るため、システムによっていくつかの変更不可能なネットワーク分析ポリシーが提供されます。これらのポリシーは、Cisco Talos Intelligence Group（Talos）によってセキュリティおよび接続の一定のバランスがとれるように調整されています。カスタム前処理設定を使用して、カスタム ネットワーク分析ポリシーを作成することもできます。

ヒント システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。ネットワーク分析ポリシーと侵入ポリシーが連動してトラフィックを検査します。

複数のカスタムネットワーク分析ポリシーを作成し、それらに異なるトラフィックの前処理を割り当てることにより、特定のセキュリティ ゾーン、ネットワーク、VLAN 用に前処理オプションを調整できます。（ただし、ASA FirePOWER VLAN による前処理を制限することはできないことに注意してください）。

ネットワーク分析ポリシーの管理

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ツールバーのユーザ名の下に、利用可能なドメインのツリーが表示されます。ドメインを切り替えるには、アクセスするドメインを選択します。

ステップ 1 ネットワーク分析ポリシーにアクセスするには、次のいずれかのパスを選択します。

- **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]**、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。
- **[Policies]** > **[Access Control]** > **[Intrusion]**、次に **[Network Analysis Policies]**
- **[ポリシー（Policies）]** > **[侵入（Intrusion）]** > **[ネットワーク分析ポリシー（Network Analysis Policy）]**

（注） カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 ネットワーク分析ポリシーを管理します。

- 比較：[ポリシーの比較（Compare Policies）] をクリックします。*Cisco Secure Firewall Management Center* コンフィギュレーション ガイド [英語] の「*Comparing Policies*」を参照してください。

  （注） Snort 2 ポリシーのみを比較できます。

- 作成：新しいネットワーク分析ポリシーを作成する場合は、[ポリシーの作成（Create Policy）] をクリックします。

  ネットワーク分析ポリシーの 2 つのバージョン（[Snort 2 バージョン（Snort 2 Version）] と [Snort 3 バージョン（Snort 3 Version）]）が作成されます。

- Snort 2 バージョンの場合は、『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Custom Network Analysis Policy Creation for Snort 2*」を参照してください。
- Snort 3 バージョンについては、「Snort 3 の場合のカスタムネットワーク分析ポリシーの作成 （7 ページ）」を参照してください。

- 削除：ネットワーク分析ポリシーを削除する場合は、[削除（Delete）]アイコンをクリックして、ポリシーの削除を確認します。アクセス コントロール ポリシーが参照しているネットワーク分析ポリシーは削除できません。

  コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- 編集：既存のネットワーク分析ポリシーを編集する場合は、[編集（Edit）] アイコンをクリックします。

  代わりに [表示（View）]（） が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- レポート：[レポート（Report）]アイコンをクリックします。『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Generating Current Policy Reports*」を参照してください。

ネットワーク分析ポリシーの Snort 3 の定義と用語

次の表に、ネットワーク分析ポリシーで使用されるSnort 3の概念と用語を示します。

表 *1*：ネットワーク分析ポリシーの *Snort 3* の定義と用語

用語	説明
インスペクタ	インスペクタは、パケットを処理するプラグインです（Snort 2プ リプロセッサと同様）。
バインダインスペクタ	バインダインスペクタは、特定のインスペクタにアクセスして考慮する必要がある場合のフローを定義します。 トラフィックがバインダインスペクタで定義された条件に一致すると、そのインスペクタの値/設定のみが有効になります。 詳細については、Snort 3 の場合のカスタムネットワーク分析ポリシーの作成 （7 ページ）の「バインダインスペクタ」を参照してください。

用語	説明
シングルトンインスペクタ	シングルトンインスペクタには 1 つのインスタンスが含まれています。これらのインスペクタは、マルチトンインスペクタのようなインスタンスの追加をサポートしていません。シングルトンインスペクタ設定は、特定のトラフィックセグメントではなく、そのインスペクタに一致しているトラフィック全体に適用されます。 詳細については、Snort 3 の場合のカスタムネットワーク分析ポリシーの作成 （7 ページ）の「シングルトンインスペクタ」を参照してください。
マルチトンインスペクタ	マルチトンインスペクタには、必要に応じて設定できる複数のインスタンスが含まれています。これらのインスペクタは、ネットワーク、ポート、VLAN などの特定の条件に基づく設定をサポートしています。サポートされている一式の設定をインスタンスと呼びます。 詳細については、Snort 3 の場合のカスタムネットワーク分析ポリシーの作成 （7 ページ）の「マルチトンインスペクタ」を参照してください。
スキーマ	スキーマファイルは OpenAPI JSON 仕様に基づいており、アップロードまたはダウンロードしたコンテンツを検証します。スキーマファイルをダウンロードします。このファイルは、Swagger エディタなどのサードパーティ製 JSONエディタで開くことができます。スキーマファイルを使用すると、インスペクタに設定できるパラメータと、対応する許容値、範囲、および使用する際に受け入れられるパターンを識別できます。 詳細については、ネットワーク分析ポリシーのカスタマイズ （15 ページ）を参照してください。

用語	説明
ファイルのサンプル	これは、インスペクタ設定に役立つ設定例が含まれた既存のテンプレートです。 サンプルファイルに含まれている設定例を参照して、必要に応じて変更を加えることができます。 詳細については、ネットワーク分析ポリシーのカスタマイズ（15 ページ）を参照してください。
完全な設定	インスペクタ設定全体を 1 つのファイルにダウンロードできます。 インスペクタ設定に関するすべての情報がこのファイルで入手できます。 完全な設定は、デフォルト設定（Cisco Talos による LSP 更新の一部として展開）とカスタム NAP インスペクタ設定がマージされた設定です。 詳細については、ネットワーク分析ポリシーのカスタマイズ（15 ページ）を参照してください。

用語	説明
オーバーライドされた設定	ネットワーク分析ポリシーページの [Snort 3 バージョン（Snort 3 Version）] で、次の手順を実行します。 • オーバーライドされた設定を含んでいる JSON ファイルをアップロードするには、**[アクション（Actions）]** > **[アップロード（Upload）]** で [オーバーライドされた設定（Overridden Configuration）] をクリックします。 • オーバーライドされたインスペクタ設定をダウンロードするには、**[アクション（Actions）]** > **[ダウンロード（Download）]** で [オーバーライドされた設定（Overridden Configuration）] をクリックします。 インスペクタ設定をオーバーライドしていない場合、このオプションは無効になります。インスペクタ設定をオーバーライドすると、このオプションが自動的に有効になり、ダウンロードできるようになります。 詳細については、ネットワーク分析ポリシーのカスタマイズ（15 ページ）を参照してください。

関連トピック

Snort 3 の場合のカスタムネットワーク分析ポリシーの作成 （7 ページ）
ネットワーク分析ポリシーのカスタマイズ （15 ページ）
ネットワーク分析ポリシーのマッピング （12 ページ）

ネットワーク分析と侵入ポリシーの前提条件

Snort検査エンジンが侵入およびマルウェア分析のトラフィックを処理できるようにするには、Threat Defense デバイスに対して IPS ライセンスを有効にする必要があります。

ネットワーク分析、侵入ポリシーを管理し、移行タスクを実行するには、管理者ユーザーである必要があります。

Snort 3 の場合のカスタムネットワーク分析ポリシーの作成

デフォルトのネットワーク分析ポリシーは、一般的なネットワーク要件を満たし、また、最適なパフォーマンスが得られるように調整されています。通常、ほとんどのネットワーク要件はデフォルトのネットワーク分析ポリシーで十分であり、ポリシーをカスタマイズする必要はありません。ただし、特定のネットワーク要件がある場合やパフォーマンスに問題がある場合は、デフォルトのネットワーク分析ポリシーをカスタマイズできます。ネットワーク分析ポリシーのカスタマイズは高度な設定であるため、上級ユーザーまたはシスコのサポート以外は行えないことに注意してください。

Snort 3 のネットワーク分析ポリシーの設定は、JSON と JSON スキーマに基づくデータ駆動型モデルです。スキーマは OpenAPI 仕様に基づいており、サポートされているインスペクタ、設定、設定タイプ、および有効な値を確認するのに役立ちます。Snort 3 インスペクタは、パケットを処理するプラグインです（Snort 2 プリプロセッサと同様）。ネットワーク分析ポリシーの設定は、JSON 形式でダウンロードできます。

Snort 3 では、インスペクタと設定のリストは Snort 2 のプリプロセッサと設定のリストと 1 対 1 でマッピングされていません。また、Management Center で使用可能なインスペクタと設定の数は、Snort 3 がサポートするインスペクタと設定の一部です。Snort 3 の詳細については、https://snort.org/snort3を参照してください。Management Center で使用可能なインスペクタの詳細については、https://www.cisco.com/go/snort3-inspectors を参照してください。

（注）

- Management Center を 7.0 リリースにアップグレードする際に、ネットワーク分析ポリシーの Snort 2 バージョンで行った変更については、アップグレード後も Snort 3 に移行されません。
- 侵入ポリシーとは異なり、Snort 2 のネットワーク分析ポリシーの設定を Snort 3 に同期するオプションはありません。

デフォルトのインスペクタ更新

Lightweight Security Package（LSP）の更新には、新しいインスペクタまたは既存のインスペクタ設定の整数範囲への変更が含まれている場合があります。LSP のインストール後、新しいインスペクタや更新された範囲は、ネットワーク分析ポリシーの Snort 3 バージョンのインスペクタで使用できます。

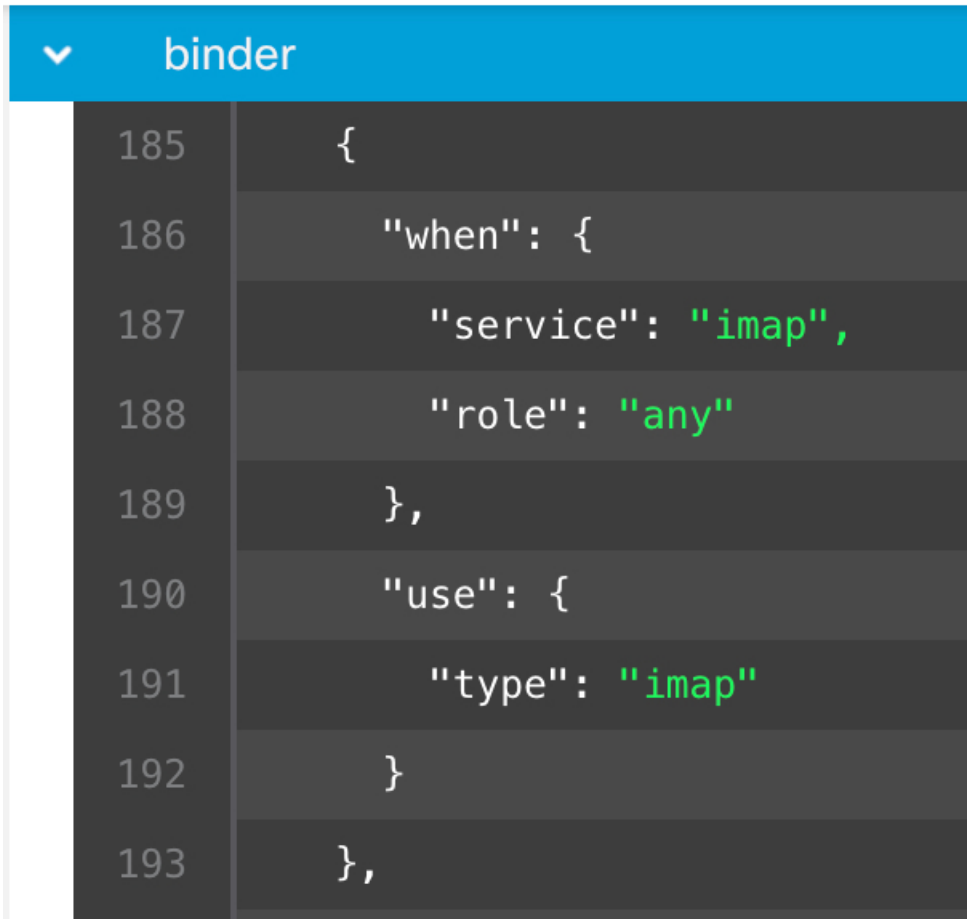
バインダインスペクタ

バインダインスペクタは、特定のインスペクタにアクセスして考慮する必要がある場合のフローを定義します。トラフィックがバインダインスペクタで定義された条件に一致すると、そのインスペクタの値/設定のみが有効になります。次に例を示します。

imap インスペクタの場合、バインダはアクセスする必要があるときに次の条件を定義します。つまり、次の場合です。

- サービスが imap と等しい。
- ロールが any と等しい。

これらの条件が満たされている場合は、imap タイプを使用します。



シングルトンインスペクタ

シングルトンインスペクタに含まれているインスタンスは 1 つです。これらのインスペクタは、マルチトンインスペクタのようなインスタンスの追加をサポートしていません。シングルトンインスペクタ設定は、特定のトラフィックセグメントではなく、トラフィック全体に適用されます。

次に例を示します。

```
{
   "normalizer":{
      "enabled":true,
      "type":"singleton",
      "data":{
```

```
        "ip4":{
           "df":true
        }
     }
  }
}
```

マルチトンインスペクタ

マルチトンインスペクタには、必要に応じて設定できる複数のインスタンスが含まれています。これらのインスペクタは、ネットワーク、ポート、VLANなどの特定の条件に基づく設定をサポートしています。サポートされている一式の設定をインスタンスと呼びます。デフォルトのインスタンスはありますが、特定の条件に基づいてインスタンスを追加することもできます。トラフィックがその条件に一致すると、そのインスタンスの設定が適用されます。それ以外の場合は、デフォルトインスタンスの設定が適用されます。また、デフォルトインスタンスの名前はインスペクタの名前と同じです。

マルチトンインスペクタの場合、オーバーライドされたインスペクタ設定をアップロードするときは、JSON ファイル内の各インスタンスの一致するバインダ条件（インスペクタにアクセスまたは使用する必要がある場合の条件）も含めるか、または定義する必要があります。そうしないと、アップロードはエラーになります。新しいインスタンスを作成することもできますが、エラーを回避するために、作成するすべての新しいインスタンスに必ずバインダ条件を含めてください。

次に例を示します。

- デフォルトインスタンスが変更されたマルチトンインスペクタ。

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   }
}
```

- デフォルトのインスタンスとデフォルトのバインダが変更されたマルチトンインスペクタ。

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
```

```
    },
    "binder":{
       "type":"binder",
       "enabled":true,
       "rules":[
          {
             "use":{
                "type":"http_inspect"
             },
             "when":{
                "role":"any",
                "ports":"8080",
                "proto":"tcp",
                "service":"http"
             }
          }
       ]
    }
}
```

- カスタムインスタンスとカスタムバインダが追加されたマルチトンインスペクタ。

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect1",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
      "enabled":true,
      "rules":[
         {
            "use":{
               "type":"http_inspect",
               "name":"http_inspect1"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
         }
      ]
   }
}
```

Common Industrial Protocol Safety

Common Industrial Protocol（CIP）Safety は、デバイスの安全な動作を可能にする CIP の一連の拡張機能です。また、CIP ネットワーク上の異なるノード間のフェールセーフ通信も提供します。

CIP Safety プロトコルは、次の 2 つの主要コンポーネントで構成されています。

- CIP Safety セグメント：Forward Open メッセージで、後続の Safety セッションの安全性パラメータを交換するために使用されます。
- CIP Safety メッセージ：実際の安全性情報を交換するために使用されます。

CIP インスペクタは、以下を検出して識別します。

- CIP（サービスおよびクライアント）
- ペイロード（CIP Read、CIP Admin、CIP Infrastructure、CIP Write など）

  CIP インスペクタは、CIP セグメントを解析し、Forward Open 要求で CIP Safety セグメントを検出できます。

CIP Safety 機能をテストするには、CIP インスペクタを有効にする必要があります。CIP パケットの Safety セグメントの検出とブロック （11 ページ） を参照してください。

CIP パケットの Safety セグメントの検出とブロック

使用例：他の CIP パケットを許可しながら、CIP Safety セグメントを検出してブロックするには、次の手順を実行します。

- **cip_safety** という名前のカスタムネットワーク分析ポリシーを作成します。
- アクセス コントロール ポリシーでアクセス制御ルールを作成して、CIP Safety をブロックし、他のすべてのパケットを許可します。

CIP Safety 機能をテストするには、Management Center で CIP インスペクタを有効にし、アクセス コントロール ポリシーに割り当てます。

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）] > [ネットワーク分析ポリシー（Network Analysis Policies）]** に移動します。

ステップ 2 作成したネットワーク分析ポリシー **cip_safety** の [Snort 3バージョン（Snort 3 Version）] をクリックします。

ステップ 3 [インスペクタ（Inspectors）] で、[cip] をクリックして展開します。

デフォルト設定は左側の列に表示され、オーバーライドされた設定はインスペクタの下の右側の列に表示されます。

ステップ 4 右側の列の [オーバーライドされた設定（Overridden Configuration）] で、[インスペクタの 編集（Edit Inspector）] アイコンをクリックし、**cip** の [有効（enabled）] フィールドを false（デフォルト）から true に変更します。

ステップ 5 [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 アクセス コントロール ポリシーに **cip** インスペクタを割り当てるには、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[編集（Edit）]** の順に選択し、[詳細設定（Advanced Settings）] オプションを選択します。

ステップ 8 [ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある をクリックします。

ステップ 9 [ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ウィンドウで、[デフォルトのネットワーク分析ポリシー（Default Network Analysis Policy）] ドロップダウンリストから作成したアクセス コントロール ポリシー **cip_safety** を選択します。

これで、Management Center で CIP インスペクタが有効になり、CIP Safety をブロックし、他のすべての CIP パケットを許可するカスタムアクセス制御ルールを作成できます。

ステップ 10 CIP Safety パケットフローを含むライブトラフィックを送信した後、[接続イベント（Connection Events）] に移動して、ペイロードが、この手順で説明されている検出およびブロックの使用例の CIP Safety パケットログを含む、予期されたペイロードであることを確認します。**CIP** はアプリケーションプロトコルおよびクライアントとして検出され（[アプリケーションプロトコル（Application Protocol）] フィールドと [クライアント（Client）] フィールドを参照）、[Webアプリケーション（Web Application）] フィールドに **CIP Safety** が表示されます。

ネットワーク分析ポリシーのマッピング

ネットワーク分析ポリシーの場合、Cisco Talos は Snort 3 バージョンのポリシーに対応する Snort 2 バージョンを見つけるために使用するマッピング情報を提供します。

このマッピングにより、Snort 3 バージョンのポリシーが Snort 2 バージョンと同等になります。

ネットワーク分析ポリシーのマッピングの表示

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** > **[ネットワーク分析ポリシー（Network Analysis Policies）]** に移動します。

ステップ 2 [NAP マッピング（NAP Mapping）] をクリックします。

ステップ 3 [マッピングの表示（View Mappings）] の矢印を展開します。

Snort 2 同等ポリシーに自動的にマッピングされる Snort 3 ネットワーク分析ポリシーが表示されます。

ステップ 4 [OK] をクリックします。

ネットワーク分析ポリシーの作成

既存のすべてのネットワーク分析ポリシーは、対応する Snort 2 バージョンでも Snort 3 バージョンでも Management Center で使用できます。新しいネットワーク分析ポリシーを作成すると、Snort 2 バージョンと Snort 3 バージョンの両方で作成されます。

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** > **[ネットワーク分析ポリシー（Network Analysis Policies）]** に移動します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 3 [名前（Name）] と [説明（Description）] に入力します。

ステップ 4 [ベースポリシー（Base Policy）] を選択し、[保存（Save）] をクリックします。

新しいネットワーク分析ポリシーが、対応する Snort 2 バージョンと Snort 3 バージョンで作成されます。

ネットワーク分析ポリシーの変更

ネットワーク分析ポリシーを変更して、名前、説明、またはベースポリシーを変更できます。

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** > **[ネットワーク分析ポリシー（Network Analysis Policies）]** に移動します。

ステップ 2 名前、説明、検査モード、またはベースポリシーを変更するには、[編集（Edit）] をクリックします。

注目 **検出モードの廃止**：Management Center 7.4.0 以降では、ネットワーク分析ポリシー（NAP）の場合、[検出（Detection）] インスペクションモードは廃止され、今後のリリースで削除されます。

[検出（Detection）] モードは、トラフィックをドロップするように設定する前に、インスペクションを有効にして、ネットワークでのインスペクションの動作を確認できるように、テストモードとして使用する（つまり、ドロップされるトラフィックを表示する）ことを目的としていました。

この動作が改善され、すべてのインスペクタのドロップがルール状態によって制御され、イベントを生成するように各インスペクタを設定できるようになりました。これは、トラフィックをドロップするようにルール状態を設定する前に、テストするために行われます。Snort 3 ではトラフィックドロップをきめ細かく制御できるようになったため、[検出（Detection）] モードは製品の複雑さを増すだけで、必要ではないため、検出モードは廃止されました。

[検出（Detection）] モードの NAP を [防御（Prevention）] に変更すると、侵入イベントのトラフィックを処理し、その結果が「ドロップするべき」となった NAP は実際に「ドロップ」になり、対応するトラフィックはこれらのイベントからのトラフィックをドロップします。これは、GID が 1 または 3 ではないルールに適用されます。GID 1 と 3 はテキスト/コンパイルされたルール（通常は Talos によって提供されるか、カスタム/インポートされたルールから提供されます）であり、他のすべての GID は異常のインスペクションです。これらは、ネットワークでトリガーするための、まれなルールです。[防御（Prevention）] モードに変更しても、トラフィックに影響を与える可能性はほとんどありません。ドロップされるトラフィックに適用可能な侵入ルールを無効にし、単に生成または無効にするように設定する必要があります。

インスペクションモードとして [防御（Prevention）] を選択することをお勧めしますが、[防御（Prevention）] を選択した場合は、[検出（Detection）] モードに戻すことはできません。

（注） ネットワーク分析ポリシーの名前、説明、ベースポリシー、および検査モードを編集すると、編集内容は Snort 2 と Snort 3 の両方のバージョンに適用されます。特定のバージョンの検査モードを変更する場合は、それぞれのバージョンのネットワーク分析ポリシーページから変更できます。

ステップ 3 [保存（Save）] をクリックします。

[ネットワーク分析ポリシー（Network Analysis Policy）] ページでのインスペクタの検索

[ネットワーク分析ポリシー（Network Analysis Policy）] ページの Snort 3 バージョンで、検索バーに関連するテキストを入力してインスペクタを検索する必要がある場合があります。

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）] > [ネットワーク分析ポリシー（Network Analysis Policies）]** に移動します。

ステップ 2 ネットワーク分析ポリシーの [Snort 3 バージョン（Snort 3 Version）] に移動します。

ステップ 3 [検索（Search）] バーに、検索するインスペクタの名前または関連するテキストを入力します。

検索するテキストに一致するすべてのインスペクタが表示されます。

たとえば、**pop** と入力すると、一致する結果としてポップインスペクタとバインダインスペクタが画面に表示されます。

関連トピック

カスタムネットワーク分析ポリシーの設定例 （25 ページ）
インスペクタとオーバーライドのリストの表示 （21 ページ）
ネットワーク分析ポリシーの Snort 3 の定義と用語 （3 ページ）
ネットワーク分析ポリシーのカスタマイズ （15 ページ）
設定をオーバーライドするインスペクタのインライン編集 （19 ページ）

インスペクタ設定のコピー

要件に応じて、ネットワーク分析ポリシーの Snort 3 バージョンのインスペクタ設定をコピーできます。

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）] > [ネットワーク分析ポリシー（Network Analysis Policies）]** に移動します。

ステップ 2 ネットワーク分析ポリシーの [Snort 3 バージョン（Snort 3 Version）] に移動します。

ステップ 3 [インスペクタ（Inspectors）] で、設定をコピーする必要があるインスペクタを展開します。

デフォルト設定は左側の列に表示され、オーバーライドされた設定はインスペクタの下の右側の列に表示されます。

ステップ 4 [クリップボードにコピー（Copy to clipboard）] アイコンをクリックして、次のいずれかまたは両方のインスペクタ設定をクリップボードにコピーします。

- 左側の列の [デフォルト設定（Default Configuration）]
- 右側の列の [オーバーライドされた設定（Overridden Configuration）]

ステップ 5 コピーしたインスペクタ設定を JSON エディタに貼り付けて、必要に応じて編集します。

関連トピック

ネットワーク分析ポリシーのカスタマイズ （15 ページ）

ネットワーク分析ポリシーのカスタマイズ

Snort 3 バージョンのネットワーク分析ポリシーは、要件に応じてカスタマイズできます。

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）] > [ネットワーク分析ポリシー（Network Analysis Policies）]** に移動します。

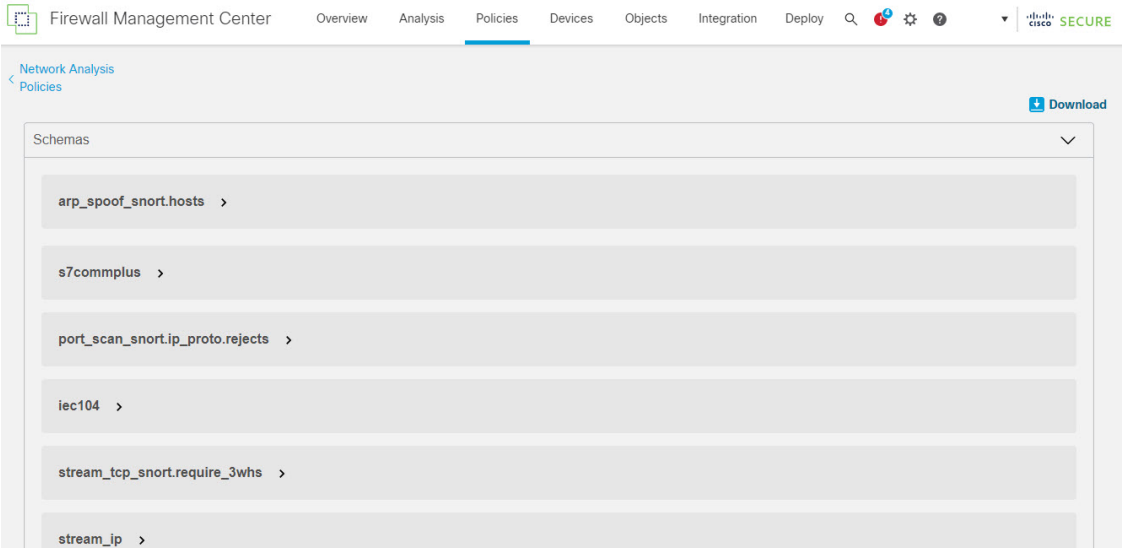
ステップ 2 ネットワーク分析ポリシーの [Snort 3 バージョン（Snort 3 Version）] に移動します。

ステップ 3 [アクション（Actions）] ドロップダウンメニューをクリックします。

次のオプションが表示されます。

- スキーマの表示（View Schema）
- スキーマのダウンロード（Download Schema）、サンプルファイル/テンプレートのダウンロード（Download Sample File/Template）
- 完全な設定のダウンロード（Download Full Configuration）
- オーバーライドされた設定のダウンロード（Download Overridden Configuration）
- オーバーライドされた設定のアップロード（Upload Overridden Configuration）

ステップ 4 [スキーマの表示（View Schema）] をクリックして、スキーマファイルをブラウザで直接開きます。



ステップ 5 必要に応じてスキーマファイル、サンプルファイル/テンプレート、完全な設定、またはオーバーライドされた設定をダウンロードできます。

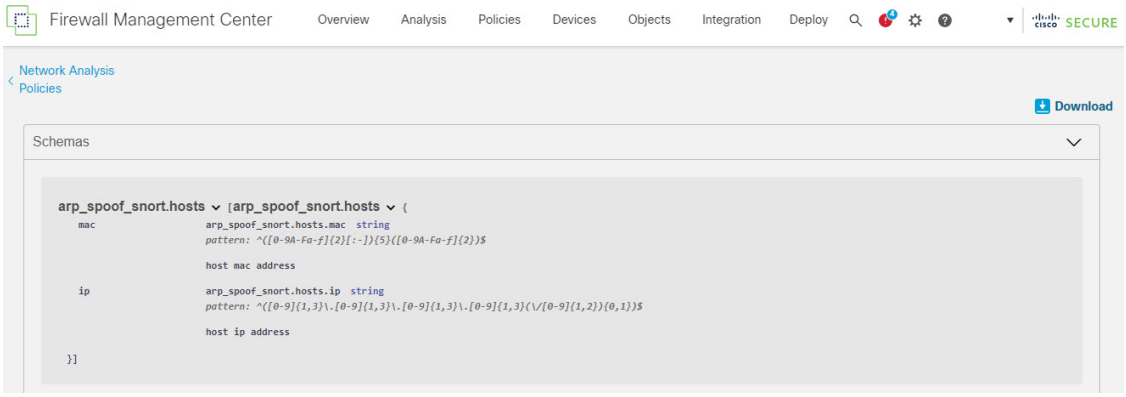
これらのオプションでは、許容値、範囲、パターン、既存およびデフォルトのインスペクタ設定、ならびにオーバーライドされたインスペクタ設定に関する情報が得られます。

a) **[スキーマのダウンロード（Download Schema）]** をクリックしてスキーマファイルをダウンロードします。

スキーマファイルはアップロードまたはダウンロードしたコンテンツを検証します。スキーマファイルをダウンロードし、サードパーティ製JSONエディタを使用して開くことができます。スキーマファイルを使用すると、インスペクタに設定できるパラメータと、対応する許容値、範囲、および使用する際に受け入れられるパターンを識別できます。

たとえば、arp_spoof_snort インスペクタの場合は、ホストを設定できます。ホストには、MAC アドレスと IP アドレスの値が含まれます。スキーマファイルは、これらの値に対して受け入れられる次のパターンを示します。

- **mac**：`pattern: ^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$`
- **ip**：`pattern: ^([0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}(/[0-9]{1,2}){0,1})$`



インスペクタ設定を正常にオーバーライドできるようにするには、スキーマファイルで受け入れられる値、範囲、パターンに従って値、範囲、パターンを指定する必要があります。指定しないと、エラーメッセージが表示されます。

b) インスペクタ設定に役立つ設定例を含んだ既存のテンプレートを使用するには、**[サンプルファイル/テンプレートのダウンロード（Download Sample File/Template）]** をクリックします。

サンプルファイルに含まれている設定例を参照して、必要に応じて変更を加えることができます。

c) **[完全な設定のダウンロード（Download Full Configuration）]** をクリックして、インスペクタ設定全体を 1 つの JSON ファイルにダウンロードします。

インスペクタを個別に展開する代わりに、完全な設定をダウンロードして必要な情報を探すことができます。インスペクタ設定に関するすべての情報がこのファイルで入手できます。

d) **[オーバーライドされた設定のダウンロード（Download Overridden Configuration）]** をクリックして、オーバーライドされたインスペクタ設定をダウンロードします。

ステップ 6 既存の設定をオーバーライドするには、次の手順を実行します。

次の方法を使用して、インスペクタ設定をオーバーライドすることができます。

- Management Center でインスペクタのインライン編集を直接行います。『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』の「**Getting Started with Network Analysis Policies**」の章にある「**Make Inline Edit for an Inspector to Override Configuration**」トピックを参照してください。
- [アクション（Actions）] ドロップダウンメニューを使用してオーバーライドされたコンフィギュレーション ファイルをアップロードする現在の手順を続行します。

Management Center でインライン編集を直接行った場合は、これ以上現在の手順に従う必要はありません。それ以外の場合は、この手順を完全に実行する必要があります。

a) [インスペクタ（Inspectors）] で、デフォルト設定をオーバーライドする必要があるインスペクタを展開します。

デフォルト設定は左側の列に表示され、オーバーライドされた設定はインスペクタの下の右側の列に表示されます。

検索バーに関連するテキストを入力して、インスペクタを検索する必要がある場合があります。

b) [クリップボードにコピー（Copy to clipboard）] アイコンをクリックして、デフォルトのインスペクタ設定をクリップボードにコピーします。
c) JSON ファイルを作成し、デフォルト設定を貼り付けます。
d) オーバーライドするインスペクタ設定を保持し、他のすべての設定とインスタンスを JSON ファイルから削除します。

[サンプルファイル/テンプレート（Sample File/Template）] を使用すると、デフォルト設定をオーバーライドする方法を理解することもできます。これは、Snort 3 のネットワーク分析ポリシーをカスタマイズする方法について説明する JSON スニペットを含むサンプルファイルです。

e) 必要に応じて、インスペクタ設定に変更を加えます。

変更を検証し、スキーマファイルに準拠していることを確認します。マルチトンインスペクタの場合は、すべてのインスタンスのバインダ条件が JSON ファイルに含まれていることを確認します。詳細については、『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』の「**Custom Network Analysis Policy Creation for Snort 3**」トピックの「Multiton Inspectors」を参照してください。

f) さらにデフォルトのインスペクタ設定をコピーする場合は、オーバーライドされた設定を含んでいる既存のファイルにそのインスペクタ設定を追加します。

（注） コピーしたインスペクタ設定は、JSON 標準に準拠する必要があります。

g) オーバーライドされたコンフィギュレーション ファイルをシステムに保存します。

ステップ 7 オーバーライドされた設定を含んでいる JSON ファイルをアップロードするには、[アクション（Actions）] ドロップダウンメニューから [オーバーライドされた設定のアップロード（Upload Overridden Configuration）] を選択します。

注意 必要な変更のみをアップロードします。オーバーライドが本質的にスティッキになるため、設定全体をアップロードしないでください。その場合、LSP 更新の一部としてのデフォルトの設定に対する後続の変更は適用されません。

ファイルをドラッグアンドドロップするか、またはクリックして、オーバーライドされたインスペクタ設定を含むシステムに保存された JSON ファイルを参照します。

- [インスペクタオーバーライドのマージ（Merge inspector overrides）]：共通のインスペクタがない場合は、アップロードされたファイルの内容が既存の設定にマージされます。共通のインスペクタがある場合は、アップロードされたファイル（共通のインスペクタ用）のコンテンツが以前のコンテンツより優先され、それらのインスペクタの以前の設定が置き換えられます。
- [インスペクタオーバーライドの置換（Replace inspector overrides）]：以前のすべてのオーバーライドを削除し、アップロードされたファイル内の新しいコンテンツに置き換えます。

注目 このオプションを選択すると、以前のオーバーライドがすべて削除されます。このオプションを使用して設定をオーバーライドする前に、十分な情報を得た上で決定してください。

オーバーライドされたインスペクタのアップロード中にエラーが発生した場合は、[オーバーライドされた設定ファイルのアップロード（Upload Overridden Configuration File）] ポップアップウィンドウにエラーが表示されます。また、エラーのあるファイルをダウンロードしてからエラーを修正してファイルを再アップロードすることもできます。

ステップ 8 [オーバーライドされた設定ファイルのアップロード（Upload Overridden Configuration File）] ポップアップウィンドウで、[インポート（Import）] をクリックして、オーバーライドされたインスペクタ設定をアップロードします。

オーバーライドされたインスペクタ設定をアップロードすると、インスペクタの横にオレンジ色のアイコンが表示され、オーバーライドされたインスペクタであることを示します。

また、インスペクタの下の [オーバーライドされた設定（Overridden Configuration）] 列には、オーバーライドされた値が表示されます。

また、検索バーの横にある [オーバーライドのみを表示（Show Overrides Only）] チェックボックスを使用して、オーバーライドされたすべてのインスペクタを表示することもできます。

（注） 常にオーバーライドされた設定をダウンロードし、JSON ファイルを開いて、このファイルにインスペクタ設定に対する新しい変更/オーバーライドを追加します。このアクションは、オーバーライドされた古い設定を失わないようにするために必要です。

ステップ 9 （任意）新しいインスペクタ設定に変更を加える前に、システム上のオーバーライドされたコンフィギュレーション ファイルのバックアップを作成します。

ヒント インスペクタ設定をオーバーライドするときは、バックアップを適宜作成することを推奨します。

関連トピック

オーバーライドした設定のデフォルト設定の復元 （21 ページ）
インスペクタとオーバーライドのリストの表示 （21 ページ）
[ネットワーク分析ポリシー（Network Analysis Policy）] ページでのインスペクタの検索 （14 ページ）
インスペクタ設定のコピー （14 ページ）

設定をオーバーライドするインスペクタのインライン編集

ネットワーク分析ポリシーの Snort 3 バージョンでは、インスペクタ設定のインライン編集を行い、要件に応じて設定をオーバーライドできます。

または、[アクション（Actions）] ドロップダウンメニューを使用して、オーバーライドされたコンフィギュレーション ファイルをアップロードすることもできます。詳細については、ネットワーク分析ポリシーのカスタマイズ （15 ページ）を参照してください。

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）] > [ネットワーク分析ポリシー（Network Analysis Policies）]** に移動します。

ステップ 2 ネットワーク分析ポリシーの [Snort 3 バージョン（Snort 3 Version）] に移動します。

ステップ 3 [インスペクタ（Inspectors）] で、デフォルト設定をオーバーライドする必要があるインスペクタを展開します。

デフォルト設定は左側の列に表示され、オーバーライドされた設定はインスペクタの下の右側の列に表示されます。

ステップ 4 右側の列の [オーバーライドされた設定（Overridden Configuration）] で、[インスペクタの編集（Edit Inspector）]（鉛筆）アイコンをクリックして、インスペクタ設定を変更します。

[設定のオーバーライド（Override Configuration）] ポップアップが表示され、必要な編集を行うことができます。

（注）
- オーバーライドする設定のみを保持するようにしてください。設定を同じ値のままにすると、そのフィールドはスティッキになります。つまり、その設定が将来 Talos によって変更されたときに、現在の値が保持されることを意味します。
- カスタムインスタンスを追加または削除する場合は、そのインスタンスのバインダルールもバインダインスペクタに追加するか、または削除します。

ステップ 5 [OK] をクリックします。

JSON 標準に従ってエラーが発生した場合は、エラーメッセージが表示されます。

ステップ 6 [保存（Save）] をクリックして、変更内容を保存します。

変更が OpenAPI スキーマ仕様に準拠している場合は、Management Center で設定を保存できます。それ以外の場合は、[オーバーライドされた設定の保存中にエラーが発生しました（Error Saving Overridden Configuration）] ポップアップが表示され、エラーが示されます。エラーのあるファイルをダウンロードすることもできます。

関連トピック

ネットワーク分析ポリシーのカスタマイズ （15 ページ）
インライン編集時の未保存の変更を元に戻す （20 ページ）
オーバーライドした設定のデフォルト設定の復元 （21 ページ）
カスタムネットワーク分析ポリシーの設定例 （25 ページ）

インライン編集時の未保存の変更を元に戻す

インスペクタ設定をオーバーライドするインライン編集を行っている間、未保存の変更を元に戻すことができます。このアクションでは、未保存のすべての変更が最後に保存された値に戻りますが、インスペクタのデフォルト設定には戻りません。

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）] > [ネットワーク分析ポリシー（Network Analysis Policies）]** に移動します。

ステップ 2 ネットワーク分析ポリシーの [Snort 3 バージョン（Snort 3 Version）] に移動します。

ステップ 3 [インスペクタ（Inspectors）] で、未保存の変更を元に戻す必要があるインスペクタを展開します。

デフォルト設定は左側の列に表示され、オーバーライドされた設定はインスペクタの下の右側の列に表示されます。

ステップ 4 右側の列の [オーバーライドされた設定（Overridden Configuration）] で、[十字（Cross）]（X）アイコンをクリックして、インスペクタの未保存の変更を元に戻します。

または、[キャンセル（Cancel）] をクリックして変更をキャンセルします。

インスペクタ設定に未保存の変更がない場合、このオプションは表示されません。

関連トピック

オーバーライドした設定のデフォルト設定の復元 （21 ページ）
設定をオーバーライドするインスペクタのインライン編集 （19 ページ）

インスペクタとオーバーライドのリストの表示

オーバーライドされたすべてのインスペクタのリストを表示できます。

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** > **[ネットワーク分析ポリシー（Network Analysis Policies）]** に移動します。

ステップ 2 ネットワーク分析ポリシーの [Snort 3 バージョン（Snort 3 Version）] に移動します。

ステップ 3 検索バーの横にある [オーバーライドのみ表示（Show Overrides Only）] チェックボックスをオンにして、オーバーライドされたインスペクタのリストを表示します。

オーバーライドされたすべてのインスペクタは、識別しやすいように名前の横にオレンジ色のアイコンが表示されます。

関連トピック

[ネットワーク分析ポリシー（Network Analysis Policy）] ページでのインスペクタの検索 （14 ページ）
設定をオーバーライドするインスペクタのインライン編集 （19 ページ）
ネットワーク分析ポリシーのカスタマイズ （15 ページ）

オーバーライドした設定のデフォルト設定の復元

インスペクタのデフォルト設定をオーバーライドするために行った変更を元に戻すことができます。このアクションは、オーバーライドされた設定をインスペクタのデフォルト設定に戻します。

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** > **[ネットワーク分析ポリシー（Network Analysis Policies）]** に移動します。

ステップ 2 ネットワーク分析ポリシーの [Snort 3 バージョン（Snort 3 Version）] に移動します。

ステップ 3 [インスペクタ（Inspectors）] で、オーバーライドされた設定を元に戻す必要があるインスペクタを展開します。

オーバーライドされたインスペクタは、名前の横にオレンジ色のアイコンが表示されます。

デフォルト設定は左側の列に表示され、オーバーライドされた設定はインスペクタの下の右側の列に表示されます。右側の列の [オーバーライドされた設定（Overridden Configuration）] で、[デフォルト設定に戻す（Revert to default configuration）]（戻る矢印）アイコンをクリックして、インスペクタのオーバーライドされた設定をデフォルト設定に戻します。

インスペクタのデフォルト設定を変更しなかった場合、このオプションは無効になります。

ステップ 4 [元に戻す（Revert）] をクリックして、決定を確定します。

ステップ 5 [保存（Save）] をクリックして、変更内容を保存します。

変更内容を保存しない場合は、[キャンセル（Cancel）] または [十字（Cross）]（X）アイコンをクリックします。

関連トピック

インライン編集時の未保存の変更を元に戻す （20 ページ）
ネットワーク分析ポリシーのカスタマイズ （15 ページ）
設定をオーバーライドするインスペクタのインライン編集 （19 ページ）
カスタムネットワーク分析ポリシーの設定例 （25 ページ）

Snort 3 ポリシーの検証

Snort 3 ポリシーを検証するために、ユーザーがメモできる基本情報のリストを次に示します。

- 現在のバージョンの Management Center は複数の 脅威に対する防御 バージョンを管理できます。
- Management Center の現在のバージョンは、以前のバージョンの 脅威に対する防御 デバイスには適用できない NAP 構成をサポートしています。
- 現在の NAP ポリシーと検証は、現在のバージョンのサポートに基づいて機能します。
- 変更には、以前のバージョンの 脅威に対する防御 では無効なコンテンツが含まれる場合があります。
- ポリシー構成の変更は、現在のバージョンで有効な構成であり、現在の Snort 3 バイナリと NAP スキーマを使用して実行されている場合に受け入れられます。
- 以前のバージョンの 脅威に対する防御 の場合、検証は展開中にその特定のバージョンの NAP スキーマと Snort 3 バイナリを使用して実行されます。特定のバージョンに適用できない構成がある場合、ユーザーには、特定のバージョンでサポートされていない構成はデプロイされず、残りの構成がデプロイされるという情報または警告が表示されます。

この手順では、NAP ポリシーをアクセス コントロール ポリシーに関連付けてデバイスに展開するときに、たとえば、レートフィルタ設定のようなインスペクタを適用して Snort 3 ポリシーを検証します。

ステップ 1 **NAP ポリシー設定を上書きする手順**：ネットワーク分析ポリシーの [Snort 3 バージョン（Snort 3 Version）] の [インスペクタ（Inspectors）] で、デフォルト設定をオーバーライドする必要なインスペクタを展開します。

デフォルト設定は左側の列に表示され、オーバーライドされた設定はインスペクタの下の右側の列に表示されます。

ステップ 2 右側の列の [オーバーライドされた設定（Overridden Configuration）] で、[インスペクタの編集（Edit Inspector）]（鉛筆）アイコンをクリックして、rate_filter のようなインスペクタを変更します。

rate_filter インスペクタに必要な編集を加えることができる [オーバーライドされた設定（Override Configuration）] ポップアップが表示されます。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存（Save）] をクリックして、変更内容を保存します。

または、[アクション（Actions）] ドロップダウンメニューを使用して、オーバーライドされたコンフィギュレーション ファイルをアップロードすることもできます。

ステップ 5 ネットワーク分析ポリシーの [Snort 3 バージョン（Snort 3 Version）] の [アクション（Actions）] ドロップダウンメニューをクリックします。

ステップ 6 [アップロード（Upload）] で、[オーバーライドされた設定（Overridden Configuration）] をクリックして、オーバーライドされた設定を含む JSON ファイルをアップロードできます。

注意 必要な変更のみをアップロードします。オーバーライドが本質的にスティッキになるため、設定全体をアップロードしないでください。その場合、LSP 更新の一部としてのデフォルトの設定に対する後続の変更は適用されません。

ファイルをドラッグアンドドロップするか、またはクリックして、オーバーライドされたインスペクタ設定を含むシステムに保存された JSON ファイルを参照します。

- [インスペクタオーバーライドのマージ（Merge inspector overrides）]：共通のインスペクタがない場合は、アップロードされたファイルの内容が既存の設定にマージされます。共通のインスペクタがある場合は、アップロードされたファイル（共通のインスペクタ用）のコンテンツが以前のコンテンツより優先され、それらのインスペクタの以前の設定が置き換えられます。
- [インスペクタオーバーライドの置換（Replace inspector overrides）]：以前のすべてのオーバーライドを削除し、アップロードされたファイル内の新しいコンテンツに置き換えます。

  注目 このオプションを選択すると、以前のすべてのオーバーライドが削除されます。そのため、このオプションを使用して設定をオーバーライドする前に、十分な情報を得た上で決定してください。

オーバーライドされたインスペクタのアップロード中にエラーが発生した場合は、[オーバーライドされた設定ファイルのアップロード（Upload Overridden Configuration File）] ポップアップウィンドウにエラーが表示されます。また、エラーのあるファイルをダウンロードしてからエラーを修正してファイルを再アップロードすることもできます。

ステップ 7 **アクセス コントロール ポリシーに NAP ポリシーを関連付ける手順**：アクセス コントロール ポリシー エディタで、[詳細設定（Advanced）] をクリックし、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] セクションの横にある [編集（Edit）] をクリックします。

ステップ 8 [デフォルトのネットワーク分析ポリシー（Default Network Analysis Policy）] ドロップダウンリストから、デフォルトのネットワーク分析ポリシーを選択します。

ユーザが作成したポリシーを選択した場合は、[編集（Edit）] をクリックして、新しいウィンドウでポリシーを編集できます。システムによって提供されたポリシーは編集できません。

ステップ 9 [OK] をクリックします。

ステップ 10 [保存（Save）] をクリックしてポリシーを保存します。

ステップ 11 または、アクセス コントロール ポリシー エディタで、[詳細設定（Advanced）] をクリックし、[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] セクションの横にある [編集（Edit）] をクリックします。

ステップ 12 [ルールの追加（Add Rule）] をクリックします。

ステップ 13 追加する条件をクリックして、ルールの条件を設定します。

ステップ 14 [ネットワーク分析（Network Analysis）] タブをクリックし、このルールに一致するトラフィックの前処理に使用する [ネットワーク分析ポリシー（Network Analysis Policy）] を選択します。

ステップ 15 [追加（Add）] をクリックします。

ステップ 16 **展開**：Management Center メニューバーで、[展開（Deploy）] をクリックして、[展開（Deployment）] を選択します。

ステップ 17 設定変更を展開するデバイスを特定して選択します。

- [検索（Search）]：[検索（Search）] ボックスのデバイス名、タイプ、ドメイン、グループ、またはステータスを検索します。
- [展開（Expand）]：展開するデバイス固有の設定変更を表示するには、[展開矢印（Expand Arrow）] をクリックします。

  デバイスのチェックボックスを選択すると、デバイスの下に表示されているデバイスのすべての変更がプッシュされ、展開されます。ただし、[ポリシーの選択（Policy Selection）] を使用すると、展開する個々のポリシーまたは設定を選択できるとともに、残りの変更は展開せずに保留できます。

  必要に応じて、[ポリシーの表示または非表示（Show or Hide Policy）] を使用して、関連付けられている未変更のポリシーを選択して表示したり、非表示にしたりできます。

ステップ 18 [展開（Deploy）] をクリックします。

ステップ 19 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証メッセージ（Validation Messages）] ウィンドウにその内容が表示されます。完全な詳細を表示するには、警告またはエラーの前にある矢印アイコンをクリックします。

（注） Snort 3 ネットワーク分析ポリシーに、この脅威に対する防御バージョンでは無効なインスペクタまたは属性が含まれていることを示す警告が表示されます。この場合、無効な設定は展開時にスキップされます。無効なインスペクタは、バージョン 7.1 より前のデバイスの場合にのみ [“rate_filter”] です。

カスタムネットワーク分析ポリシーの設定例

これは、Snort 3 のネットワーク分析ポリシーをカスタマイズする方法について説明する JSON スニペットを含むサンプルファイルです。次の方法を使用して、インスペクタ設定をオーバーライドできます。

- Management Center でインスペクタのインライン編集を直接行います。設定をオーバーライドするインスペクタのインライン編集 （19 ページ）を参照してください。
- [アクション（Actions）] ドロップダウンメニューを使用して、オーバーライドされたコンフィギュレーションファイルをアップロードします。ネットワーク分析ポリシーのカスタマイズ （15 ページ）を参照してください。

これらのオプションのいずれかを選択する前に、ネットワーク分析ポリシーのオーバーライドを正常に定義するのに役立つ次の詳細情報と例をすべて確認してください。リスクとエラーを回避するために、ここで説明するさまざまなシナリオの例を読んで理解する必要があります。

[アクション（Actions）] ドロップダウンメニューからインスペクタ設定をオーバーライドする場合は、ネットワーク分析ポリシーのオーバーライド用の JSON ファイルを作成し、そのファイルをアップロードする必要があります。

ネットワーク分析ポリシーでインスペクタ設定をオーバーライドするには、必要な変更のみをアップロードする必要があります。オーバーライドが本質的にスティッキになるため、設定全体をアップロードしないでください。その場合、LSP 更新の一部としてのデフォルト値や設定に対する後続の変更は適用されません。

さまざまなシナリオの例を次に示します。

ベースポリシーのデフォルトの状態が無効な場合のシングルトンインスペクタの有効化

```
{
  "rate_filter": {
    "enabled": true,
    "type": "singleton",
    "data": []
  }
}
```

ベースポリシーのデフォルトの状態が有効な場合のシングルトンインスペクタの無効化

```
{
  "rate_filter": {
    "enabled": false,
    "type": "singleton",
    "data": []
  }
}
```

ベースポリシーのデフォルトの状態が無効な場合のマルチトンインスペクタの有効化

```
{
  "ssh": {
    "enabled": true,
    "type": "multiton",
    "instances": []
```

```
  }
}
```

ベースポリシーのデフォルトの状態が有効な場合のマルチトンインスペクタの無効化

```
{
  "ssh": {
    "enabled": false,
    "type": "multiton",
    "instances": []
  },
  "iec104": {
    "type": "multiton",
    "enabled": false,
    "instances": []
  }
}
```

シングルトンインスペクタの特定の設定のデフォルト値のオーバーライド

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  }
}
```

マルチトンインスペクタでのデフォルトインスタンス（インスタンス名がインスペクタタイプと一致する）の特定の設定のオーバーライド

```
{
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false
        },
        "name": "http_inspect"
      }
    ]
  }
}
```

必要な変更を含むデフォルトインスタンスのバインダルールの追加

（注） デフォルトのバインダルールは編集できません。常に最後に追加されます。

```
{
  "binder": {
    "enabled": true,
```

```
    "type": "binder",
    "rules": [
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

新しいカスタムインスタンスの追加

（注） 対応するバインダルールエントリは、バインダインスペクタで定義する必要があります。

```
{
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      }
    ]
  }
}
```

シングルトンインスタンス、マルチトン デフォルト インスタンスのオーバーライド、および単一の JSON オーバーライドでの新しいマルチトンインスタンスの作成

単一の JSON オーバーライドで次を表示する例：

- シングルトンインスタンスのオーバーライド（**normalizer** インスペクタ）

- マルチトン デフォルト インスタンスのオーバーライド（**http_inspect** インスペクタ）
- 新しいマルチトンインスタンスの作成（**telnet** インスペクタ）

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  },
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false,
          "xff_headers": "x-forwarded-for true-client-ip x-another-forwarding-header"
        },
        "name": "http_inspect"
      }
    ]
  },
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      },
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
```

```
      }
    ]
  }
}
```

（注） バインダルールでデフォルトインスタンスの **name** 属性を指定する必要はありません。

arp_spoof の設定

arp_spoof の設定例：

arp_spoof インスペクタには、属性のデフォルト設定はありません。次に、オーバーライドを指定できる場合を示します。

```
{
  "arp_spoof": {
    "type": "singleton",
    "data": {
      "hosts": [
        {
          "ip": "1.1.1.1",
          "mac": "ff:0f:f1:0f:0f:ff"
        },
        {
          "ip": "2.2.2.2",
          "mac": "ff:0f:f2:0f:0f:ff"
        }
      ]
    },
    "enabled": true
  }
}
```

rate_filter の設定

```
{
  "rate_filter": {
    "data": [
      {
        "apply_to": "[10.1.2.100, 10.1.2.101]",
        "count": 5,
        "gid": 135,
        "new_action": "alert",
        "seconds": 1,
        "sid": 1,
        "timeout": 5,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

マルチ階層ネットワーク分析ポリシーを使用する場合のバインダルールの設定

この例では、子ポリシーに新しいカスタムインスタンスを追加し、バインダルールを作成する方法を示します。バインドルールはリストとして定義されます。そのため、ルールは自動的にマージされないため、親ポリシーで定義されたルールを選択し、その上に新しいルールを作成することが重要です。子ポリシーで使用可能なバインダルールは、全体として真の情報源です。

脅威に対する防御 では、デフォルトの Cisco Talos ポリシールールがこれらのユーザー定義のオーバーライドに追加されます。

親ポリシー：

telnet_parent_instance という名前と対応するバインダルールでカスタムインスタンスを定義しました。

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

子ポリシー：

このネットワーク分析ポリシーには、ベースポリシーとして前述のポリシーがあります。**telnet_child_instance** という名前でカスタムインスタンスを定義し、このインスタンスのバインダルールも定義しました。親ポリシーからのバインダルールをここにコピーする必要があります。その後に、子ポリシーのバインダルールはルールの性質に基づいて最上部の先頭または末尾に追加できるようになります。

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
```

```
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_child_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet",
          "nets": "10.2.2.0/24"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_child_instance"
        }
      },
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

一般的なリストインスペクタ属性の設定

タイプリストの属性のオーバーライドを変更する場合、部分的なオーバーライドではなく、内容全体を渡すことが重要です。つまり、ベースポリシー属性が次のように定義されている場合です。

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

value1 を **value1-new** に変更する場合、オーバーライドのペイロードは次のようになります。

正しい方法：

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

不正な方法：

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    }
  ]
}
```

この設定を理解するには、**smtp** インスペクタで **alt_max_command_line_len** 属性のトリム値を取得します。**smtp** インスペクタのデフォルト（基本）ポリシー設定が次のようになっているとします。

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "decompress_zip": false,
          "normalize_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
           EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
           NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
           TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
           ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
           XSTA XTRN XUSR",
          "ignore_data": false,
          "max_command_line_len": 512,
          "max_header_line_len": 1000,
          "log_rcptto": false,
          "decompress_swf": false,
          "max_response_line_len": 512,
          "b64_decode_depth": -1,
          "max_auth_command_line_len": 1000,
          "log_email_hdrs": false,
          "xlink2state": "alert",
          "binary_data_cmds": "BDAT XEXCH50",
          "auth_cmds": "AUTH XAUTH X-EXPS",
          "log_filename": false,
          "uu_decode_depth": -1,
          "ignore_tls_data": false,
          "data_cmds": "DATA",
          "bitenc_decode_depth": -1,
```

```
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            }
          ],
          "log_mailfrom": false,
          "decompress_pdf": false,
          "normalize": "none",
          "email_hdrs_log_depth": 1464,
          "valid_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
           EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
           NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
           TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
           ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
           XSTA XTRN XUSR",
          "qp_decode_depth": -1
        }
      }
    ],
    "enabled": true
  }
}
```

ここで、次のように **alt_max_command_line_len** リストにさらに 2 つのオブジェクトを追加します。

```
{
    "length": 246,
    "command": "XEXCH50"
},
{
    "length": 246,
    "command": "X-EXPS"
}
```

カスタムネットワーク分析ポリシーのオーバーライド JSON は次のようになります。

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
```

```
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            },
            {
              "length": 246,
              "command": "XEXCH50"
            },
            {
              "length": 246,
              "command": "X-EXPS"
            }
          ]
        }
      }
    ],
    "enabled": true
  }
}
```

マルチトンインスペクタで多階層ネットワーク分析ポリシーが使用されている場合のオーバーライドの設定

この例では、子ポリシーの属性のオーバーライドと、マージされた設定がどのようにインスタンスの子ポリシーで使用されるかを示します。子ポリシーで定義されたオーバーライドは、親ポリシーとマージされます。したがって、attribute1 と attribute2 が親ポリシーでオーバーライドされ、attribute2 と attribute3 が子ポリシーでオーバーライドされると、マージされた設定は子ポリシー用になります。つまり、attribute1（親ポリシーで定義）、attribute2（子ポリシーで定義）、および attribute3（子ポリシーで定義）がデバイスに設定されます。

親ポリシー：

これまでに、**telnet_parent_instance** という名前でカスタムインスタンスを定義し、カスタムインスタンスの **normalize** と **encrypted_traffic** の 2 つの属性をオーバーライドしました。

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
```

```
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

子ポリシー：

このネットワーク分析ポリシーには、ベースポリシーとして前述のポリシーがあります。親ポリシーから属性**encrypted_traffic**をオーバーライドし、新しい属性**ayt_attack_thresh**もオーバーライドしました。

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  }
}
```

上記のポリシーJSONでは、ネットワーク分析ポリシーを展開すると、次のマージされたJSONがデバイスに設定されます。

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
```

```
            "type": "telnet",
            "name": "telnet_parent_instance"
          }
        }
      ]
    }
}
```

次に、カスタムネットワーク分析ポリシーの詳細の例を示します。同じ動作がデフォルトインスタンスでも発生します。また、シングルトンインスペクタでも同様のマージが行われます。

ネットワーク分析ポリシーのすべてのインスペクタオーバーライドの削除：

特定のネットワーク分析ポリシーのすべてのオーバーライドを削除する場合は、空の JSON をアップロードできます。オーバーライドをアップロードする際に、[インスペクタのオーバーライドの置換（Replace inspector overrides）] オプションを選択します。

```
{
}
```

関連トピック

ネットワーク分析ポリシーの Snort 3 の定義と用語 （3 ページ）
ネットワーク分析ポリシーのマッピング （12 ページ）
Snort 3 の場合のカスタムネットワーク分析ポリシーの作成 （7 ページ）
[ネットワーク分析ポリシー（Network Analysis Policy）] ページでのインスペクタの検索 （14 ページ）
インスペクタ設定のコピー （14 ページ）
ネットワーク分析ポリシーのカスタマイズ （15 ページ）
インスペクタとオーバーライドのリストの表示 （21 ページ）

ネットワーク分析ポリシーの設定とキャッシュされた変更

新しいネットワーク分析ポリシーを作成すると、そのポリシーには基本ポリシーと同じ設定が付与されます。

ネットワーク分析ポリシーの調整時に、特にインスペクタを無効にするときは、インスペクタと侵入ルールによっては、トラフィックを特定の方法で最初にデコードまたは前処理する必要があることに留意してください。必要なインスペクタを無効にすると、システムは自動的に現在の設定でインスペクタを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではインスペクタは無効のままになります。

（注） 前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。

システムは、ユーザごとに1つのネットワーク分析ポリシーをキャッシュします。ネットワーク分析ポリシーの編集中に、任意のメニューまたは別のページへの他のパスを選択した場合、変更内容はそのページを離れてもシステム キャッシュにとどまります。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。