Cisco Secure Firewall Management Center Snort 3 バージョン 7.4 コンフィギュレーションガイド

最終更新：2024 年 11 月 6 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章 **ネットワーク分析ポリシーと侵入ポリシーの概要 1**

ネットワーク分析ポリシーと侵入ポリシーについて 1

Snort 検査エンジン 2

Snort 3 3

Snort 2 と Snort 3 の比較 6

Management Center 管理対象の Threat Defense での Snort 3 の機能制限 6

ポリシーがトラフィックで侵入を検査する方法 7

復号、正規化、前処理：ネットワーク分析ポリシー 8

アクセス コントロール ルール：侵入ポリシーの選択 9

侵入インスペクション：侵入ポリシー、ルール、変数セット 10

侵入イベントの生成 12

Snort での非対称フロー検査 13

システム提供およびカスタムネットワーク分析ポリシーと侵入ポリシー 14

システム提供のネットワーク分析ポリシーと侵入ポリシー 15

カスタムネットワーク分析ポリシーと侵入ポリシーの利点 16

カスタム ネットワーク分析ポリシーの利点 17

カスタム侵入ポリシーの利点 18

カスタム ポリシーの制限 19

ネットワーク分析と侵入ポリシーの前提条件 22

第 2 章 **Snort 2 から Snort 3 への移行 23**

Snort 3 検査エンジン 23

ネットワーク分析と侵入ポリシーの前提条件 24

Snort 2 から Snort 3 への移行方法 24

Snort 2 から Snort 3 への移行の前提条件 24
個々のデバイス上での Snort 3 の有効化 25
複数のデバイス上での Snort 3 の有効化 26
Snort 2 のカスタム IPS ルールの Snort 3 への変換 26
すべての侵入ポリシーのすべての Snort 2 カスタムルールの Snort 3 への変換 27
単一の侵入ポリシーの Snort 2 カスタムルールの Snort 3 への変換 28
Snort 2 と Snort 3 のベースポリシーのマッピングの表示 28
Snort 2 のルールと Snort 3 の同期 29
設定変更の展開 30

第 I 部 : **Snort 3 での侵入検知と防御 33**

第 3 章 **Snort 3 侵入ポリシーを開始するには 35**
侵入ポリシーの概要 35
ネットワーク分析と侵入ポリシーの前提条件 37
カスタム Snort 3 侵入ポリシーの作成 37
Snort 3 侵入ポリシーの編集 37
ルールグループのレポート 42
ルールアクションのロギング 43
侵入ポリシーのベースポリシーの変更 44
侵入ポリシーの管理 44
侵入防御を実行するためのアクセスコントロールルール設定 45
アクセス コントロール ルール設定と侵入ポリシー 46
侵入防御を実行するアクセスコントロールルールの設定 46

第 4 章 **ルールを使用した侵入ポリシーの調整 49**
侵入ルールの調整の概要 49
侵入ルールのタイプ 50
ネットワーク分析と侵入ポリシーの前提条件 51
Snort 3 のカスタムルール 51
侵入ポリシーの Snort 3 侵入ルールの表示 54

侵入ルールアクション 55
侵入ルールアクションのオプション 55
侵入ルールアクションの設定 56
侵入ポリシーの侵入イベント通知フィルタ 56
侵入イベントしきい値 57
侵入イベントしきい値の設定 57
Snort 3 での侵入ルールのしきい値の設定 59
侵入イベントしきい値の表示と削除 60
侵入ポリシー抑制の設定 60
侵入ポリシー抑制タイプ 60
Snort 3 での侵入ポリシーの抑制の設定 61
抑制条件の表示と削除 61
侵入ルールのコメントの追加 62
Snort 2 カスタムルールの Snort 3 への変換 63
すべての侵入ポリシーのすべての Snort 2 カスタムルールの Snort 3 への変換 63
単一の侵入ポリシーの Snort 2 カスタムルールの Snort 3 への変換 64
ルールグループへのカスタムルールの追加 65
カスタムルールを含むルールグループの侵入ポリシーへの追加 66
Snort 3 でのカスタムルールの管理 67
カスタムルールの削除 68
ルールグループの削除 69

第 5 章 ネットワーク資産に応じた侵入防御の調整 71
LSP 更新での Snort 3 ルールの変更 71
Cisco Secure Firewall 推奨ルールの概要 72
ネットワーク分析と侵入ポリシーの前提条件 73
Snort 3 での新しい Cisco Secure Firewall 推奨事項の生成 73

第 II 部 : Snort 3 での詳細なネットワーク分析 77

第 6 章 Snort 3 ネットワーク分析ポリシーを開始するには 79

ネットワーク分析ポリシーの概要 79
ネットワーク分析ポリシーの管理 80
ネットワーク分析ポリシーの Snort 3 の定義と用語 81
ネットワーク分析と侵入ポリシーの前提条件 84
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 85
Common Industrial Protocol Safety 88
CIP パケットの Safety セグメントの検出とブロック 89
ネットワーク分析ポリシーのマッピング 90
ネットワーク分析ポリシーのマッピングの表示 90
ネットワーク分析ポリシーの作成 91
ネットワーク分析ポリシーの変更 91
[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 92
インスペクタ設定のコピー 93
ネットワーク分析ポリシーのカスタマイズ 94
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 98
インライン編集時の未保存の変更を元に戻す 99
インスペクタとオーバーライドのリストの表示 99
オーバーライドした設定のデフォルト設定の復元 100
Snort 3 ポリシーの検証 101
カスタムネットワーク分析ポリシーの設定例 103
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 115

第 III 部 : **Snort 3 向けの Encrypted Visibility Engine 117**

第 7 章 **暗号化された可視性エンジン 119**

Encrypted Visibility Engine の概要 119
EVE の仕組み 120
侵害の兆候イベント 121
EVE の QUIC フィンガープリント 122
EVE の設定 122
EVE イベントの表示 123

EVE ダッシュボードの表示 124

第 IV 部 : Snort 3 のエレファントフロー検出 127

第 8 章 エレファントフローの検出 129

エレファントフローの検出と修復について 129

インテリジェント アプリケーション バイパスからのエレファントフローのアップグレード 130

エレファントフローの設定 130

第 V 部 : Snort 3 の使用例 135

第 9 章 Cisco Secure Firewall Management Center での Snort 2 から Snort 3 への移行 137

Snort 2 から Snort 3 への移行 137

Snort 3 への移行の利点 137

ビジネスシナリオの例 138

Snort 2 から Snort 3 への移行のベストプラクティス 138

前提条件 138

エンドツーエンドの移行ワークフロー 139

Threat Defense で Snort 3 を有効にする 139

単一の侵入ポリシーの Snort 2 ルールの Snort 3 への変換 140

設定変更の展開 145

第 10 章 Cisco Secure Firewall Management Center での Snort 3 推奨事項の生成 149

Snort 3 ルールの推奨事項 149

利点 150

ビジネスシナリオの例 150

ベストプラクティス 150

前提条件 150

Snort 3 推奨事項の生成 151

設定変更の展開 154

第 11 章 EVE の脅威の確実性スコアに基づいてトラフィックをブロックする 157

Encrypted Visibility Engine について 157

利点 157

ビジネスシナリオの例 157

前提条件 158

ワークフローの概要 158

EVE でのブロックしきい値の設定 158

EVE イベントの表示 161

その他の参考資料 162

第 12 章 エレファントフロー検出結果の設定 163

エレファントフローについて 163

エレファントフローの検出と修復の利点 163

エレファントフローのワークフロー 164

ビジネスシナリオの例 164

前提条件 165

エレファント フロー パラメータの設定 165

エレファントフローのイベントの表示 168

エレファントフロー修復除外の設定 169

エレファントフロー修復除外のイベントの表示 172

その他の参考資料 172

第 13 章 Snort 3 侵入ポリシーでの MITRE フレームワークを使用した脅威の軽減 173

MITRE ATT&CK フレームワークについて 173

MITRE フレームワークの利点 174

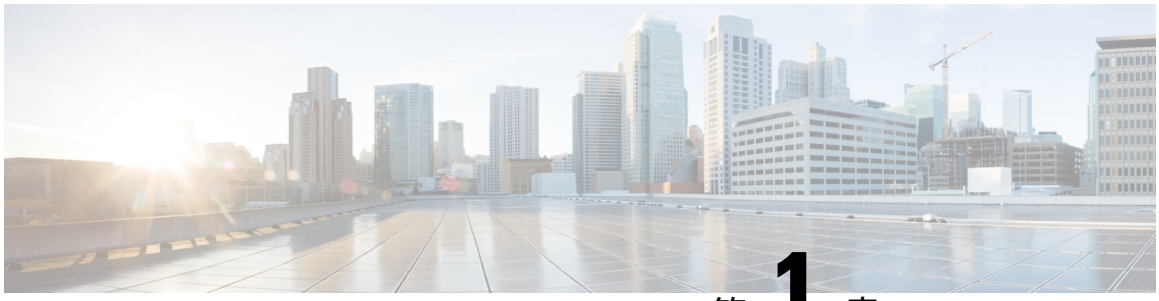
MITRE ネットワークのビジネスシナリオの例 174

MITRE フレームワークの前提条件 174

Snort 3 侵入ポリシーの表示と編集 175

侵入イベントの表示 179

その他の参考資料 182



第 1 章

ネットワーク分析ポリシーと侵入ポリシーの概要

Snort 検査エンジンは、Cisco Secure Firewall Threat Defense（旧 Firepower Threat Defense）デバイスに不可欠な部分です。この章では、Snort 3 とネットワーク分析ポリシーおよび侵入ポリシーの概要について説明します。システム提供およびカスタムのネットワーク分析ポリシーと侵入ポリシーについても説明します。

- ネットワーク分析ポリシーと侵入ポリシーについて （1 ページ）
- Snort 検査エンジン （2 ページ）
- Snort 3 （3 ページ）
- Snort 2 と Snort 3 の比較 （6 ページ）
- Management Center 管理対象の Threat Defense での Snort 3 の機能制限 （6 ページ）
- ポリシーがトラフィックで侵入を検査する方法 （7 ページ）
- システム提供およびカスタムネットワーク分析ポリシーと侵入ポリシー （14 ページ）
- ネットワーク分析と侵入ポリシーの前提条件 （22 ページ）

ネットワーク分析ポリシーと侵入ポリシーについて

ネットワーク分析ポリシーと侵入ポリシーは、侵入検知および防御の機能の一部として連携して動作します。

- 侵入検知という用語は、一般に、ネットワーク トラフィックへの侵入の可能性を受動的にモニタおよび分析し、セキュリティ分析用に攻撃データを保存するプロセスを指します。これは「IDS」とも呼ばれます。
- 侵入防御という用語には、侵入検知の概念が含まれますが、さらにネットワークを通過中の悪意のあるトラフィックをブロックしたり変更したりする機能も追加されます。これは「IPS」とも呼ばれます。

侵入防御の展開では、システムがパケットを検査するときに次のことが行われます。

- **ネットワーク分析ポリシー**は、トラフィックのデコードと前処理の方法を管理し、特に、侵入を試みている兆候がある異常なトラフィックについて、さらに評価できるようにします。
- **侵入ポリシー**では侵入およびプリプロセッサルール（総称的に「侵入ルール」とも呼ばれる）を使用し、パターンに基づき、デコードされたパケットを検査して攻撃の可能性を調べます。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映することができます。

ネットワーク分析ポリシーと侵入ポリシーは、どちらも親のアクセス コントロール ポリシーによって呼び出されますが、呼び出されるタイミングが異なります。システムでトラフィックが分析される際には、侵入防御（追加の前処理と侵入ルール）フェーズよりも前に、別途ネットワーク分析（デコードと前処理）フェーズが実行されます。ネットワーク分析ポリシーと侵入ポリシーを一緒に使用すると、広範囲で詳細なパケットインスペクションを行うことができます。このポリシーは、ホストとそのデータの可用性、整合性、機密性を脅かす可能性のあるネットワーク トラフィックの検知、通知および防御に役立ちます。

システムには、同様の名前（Balanced Security and Connectivity など）が付いたいくつかのネットワーク分析ポリシーおよび侵入ポリシーが付属しており、それらは互いに補完しあい、連携して動作します。システム付属のポリシーを使用することで、Cisco Talos Intelligence Group（Talos）の経験を活用できます。これらのポリシーでは、Talos は侵入ルールとインスペクタルールの状態を設定するとともに、インスペクタとその他の詳細設定の初期設定も提供します。

また、カスタムのネットワーク分析ポリシーや侵入ポリシーも作成できます。カスタム ポリシーの設定を調整することで、各自に最も役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

Webインターフェイスで同様のポリシーエディタを使用し、ネットワーク分析ポリシーや侵入ポリシーを作成、編集、保存、管理します。いずれかのタイプのポリシーを編集するときには、Web インターフェイスの左側にナビゲーション パネルが表示され、右側にさまざまな設定ページが表示されます。

追加のサポートと情報については、以下のビデオを参照してください。

- Snort 3 基本の概要
- Snort 3 拡張の概要

Snort 検査エンジン

Snort 検査エンジンは、Secure Firewall Threat Defense（旧 Firepower Threat Defense）デバイスに不可欠な部分です。検査エンジンは、トラフィックをリアルタイムで分析して、パケットを詳細に検査します。ネットワーク分析ポリシーと侵入ポリシーでは、Snort 検査エンジンの機能を利用して、侵入を検出して保護します。

Snort 3

Snort 3 は Snort 検査エンジンの最新バージョンで、以前のバージョンの Snort と比較して大幅に改善されています。Snort の古いバージョンは Snort 2 です。Snort 3 はより効率的で、パフォーマンスとスケーラビリティが向上します。

Snort 3 はアーキテクチャが再設計され、Snort 2 と比較すると同等のリソースでより多くのトラフィックを検査します。Snort 3 では、トラフィックパーサーを簡単かつ柔軟に挿入できます。Snort 3 には、ルールの記述を容易にし、同等の共有オブジェクトルールを表示できる新しいルールシンタックスも用意されています。

Snort 3 のその他の重要な変更点は次のとおりです。

- 複数の Snort インスタンスを使用する Snort 2 とは異なり、Snort 3 は複数のスレッドを単一の Snort インスタンスに関連付けます。これにより、使用するメモリが少なくなり、Snort のリロード時間が短縮され、より多くの侵入ルールとより大きなネットワークマップがサポートされます。Snort スレッドの数はプラットフォームによって異なり、各プラットフォームの Snort 2 インスタンスの数と同じです。使用方法はほぼ透過的です。
- 脅威に対する防御 ごとの Snort バージョン：Snort 検査エンジンは 脅威に対する防御 固有であり、Secure Firewall Management Center（旧 Firepower Management Center）固有ではありません。Management Center はそれぞれが Snort のいずれかのバージョン（Snort 2 および Snort 3）である複数の 脅威に対する防御 を管理できます。Management Center の侵入ポリシーは一意ですが、システムは、デバイスの選択した検査エンジンに応じて、侵入保護のために Snort 2 または Snort 3 バージョンの侵入ポリシーを適用します。デバイスの検査エンジンの詳細については、Snort 3 検査エンジン （23 ページ）を参照してください。
- デコーダルール：パケットデコーダルールは、デフォルトの侵入ポリシーでのみ起動します。他のポリシーで有効にしたデコーダルールは無視されます。
- 共有オブジェクトルール：Snort 3 は、すべてでなく一部の共有オブジェクト（SO）の侵入ルール（ジェネレータ ID（GID）が 3 のルール）をサポートします。サポートされていない有効な共有オブジェクトルールはトリガーされません。
- セキュリティ インテリジェンスのマルチレイヤ検査：Snort 2 はマルチレイヤトラフィックの 2 つのレイヤを検査します。Snort 3 は、レイヤに関係なく最も内側の IP アドレスを検出します。
- プラットフォームのサポート：Snort 3 には Threat Defense 7.0 以降が必要です。ASA FirePOWER または NGIPSv ではサポートされていません。
- 管理対象デバイス：バージョン 7.0 の Management Center は、バージョン 6.4、6.5、6.6、6.7、および 7.0 の Snort 2 脅威に対する防御 とバージョン 7.0 の Snort 3 脅威に対する防御 を同時にサポートできます。
- Snort バージョンの切り替え時のトラフィックの中断：Snort のバージョンを切り替えると、トラフィックの検査が中断され、展開中にいくつかのパケットがドロップされる可能性があります。

- 統合ポリシー：管理対象の 脅威に対する防御 で有効になっている基盤の Snort エンジンのバージョンに関係なく、Management Center で設定されたアクセス コントロール ポリシー、侵入ポリシー、およびネットワーク分析ポリシーは、ポリシーの適用時にシームレスに機能します。Management Center バージョン 7.0 以降のすべての侵入ポリシーには、Snort 2 バージョンと Snort 3 バージョンの 2 つのバージョンがあります。侵入ポリシーは統合されます。つまり、共通の名前、ベースポリシー、および検査モードを持ちます。ただし、ポリシーには 2 つのバージョン（Snort 2 バージョンと Snort 3 バージョン）があります。侵入ポリシーの Snort 2 バージョンと Snort 3 バージョンでは、ルール設定の観点からは異なる場合があります。ただし、侵入ポリシーがデバイスに適用されると、システムはデバイスで有効になっている Snort バージョンを自動的に識別し、そのバージョンに設定されたルール設定を適用します。

- Lightweight Security Package（LSP）：Snort ルールの更新（SRU）を Snort 3 の次世代の侵入ルールと設定の更新に置き換えます。更新をダウンロードすると、Snort 3 LSP と Snort 2 SRU の両方がダウンロードされます。

  LSP の更新では、新規と更新後の侵入ルールとインスペクタルール、既存のルールの変更後の状態、および Management Center と 脅威に対する防御 バージョン 7.0 以降の変更後のデフォルトの侵入ポリシー設定が提供されます。Management Center をバージョン 6.7 以前から 7.0 にアップグレードすると、LSP と SRU の両方がサポートされます。LSP の更新では、システムにより提供されたルールが削除されたり、新しいルールカテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。LSP の更新については、『Firepower Management Center Configuration Guide』の最新バージョンの「Update Intrusion Rules」のトピックを参照してください。

- Snort 2 と Snort 3 のルールと事前設定のマッピング：Snort 2 と Snort 3 のルールがマッピングされ、マッピングはシステムによって提供されます。ただし、1 対 1 のマッピングではありません。システムによって提供される侵入ベースポリシーは、Snort 2 と Snort 3 の両方に対して事前に設定されており、ルールセットが異なる場合でも同じ侵入防御を提供します。システムによって提供される Snort 2 と Snort 3 のベースポリシーは、同じ侵入防御設定で相互にマッピングされます。詳細については、Snort 2 と Snort 3 のベースポリシーのマッピングの表示 （28 ページ）を参照してください。

- Snort 2 と Snort 3 ルールオーバーライドの同期：脅威に対する防御 が 7.0 にアップグレードされると、脅威に対する防御 の検査エンジンを Snort 3 バージョンにアップグレードできます。Management Center は Snort 2 バージョンの侵入ポリシーの既存のルールのすべてのオーバーライドを、Talos が提供するマッピングを使用して、対応する Snort 3 ルールにマッピングします。ただし、アップグレード後に実行した追加のオーバーライドがある場合や、新しい 脅威に対する防御 のバージョン 7.0 をインストール場合は、それらを手動で同期する必要があります。詳細については、Snort 2 のルールと Snort 3 の同期 （29 ページ）を参照してください。

- カスタム侵入ルール：Snort 3 でカスタム侵入ルールを作成できます。また、Snort 2 に存在するカスタム侵入ルールを Snort 3 にインポートすることもできます。詳細については、Snort 3 のカスタムルール （51 ページ）を参照してください。

- ルールグループ：Management Center では、すべての Snort 3 ルールがルールグループにグループ化されます。ルールグループはルールの論理グループであり、ルールのアクセシビ

リティ、ルールのナビゲーション、およびルールグループのセキュリティレベルの制御を強化するための簡単な管理インターフェイスを提供します。

Management Center 7.3.0 以降、複数のレベルのルールグループのルールナビゲーションがサポートされ、ルールのより柔軟で論理的なグループ化を提供します。MITRE フレームワークを使用してルールをナビゲートできる MITRE フレームワークが追加されます。MITRE は、ルールグループの別のカテゴリであり、Talos ルールグループの一部です。

（注） MITRE の詳細については、 https://attack.mitre.orgを参照してください。

ルールは、MITRE ATT&CK ルールグループ、ルール カテゴリ ルール グループ、複数の「アセットタイプ」ルールグループ、マルウェア攻撃など、複数のルールグループの一部にできます。使用可能なルールグループが侵入ポリシーエディタに一覧表示され、ポリシーを強化するために選択できます。

この複数レベルの階層構造により、「リーフルールグループ」である最後の要素までトラバースできます。これらのルールグループには、特定のタイプの脆弱性、類似のターゲットシステム、類似の脅威カテゴリなど、相互に関連するルールのセットが含まれています。ルールグループには、4 つのセキュリティレベルが関連付けられています。セキュリティレベルの変更、ルールグループの追加や削除ができ、ネットワーク上で検出されるトラフィックに一致するルールのルールアクションを変更できます。これは、セキュリティ、パフォーマンス、および誤検知耐性の間で満足のいくバランスをもたらすために行われます。

Snort 3 侵入ポリシーを編集するには、Snort 3 侵入ポリシーの編集 （37 ページ）を参照してください。

侵入イベントのルールグループレポートについては、ルールグループのレポート （42 ページ）を参照してください。

- Snort 2 エンジンと Snort 3 エンジンの切り替え：Snort 3 をサポートする 脅威に対する防御は Snort 2 もサポートできます。Snort 3 から Snort 2 への切り替えは、有効性の観点から推奨されません。ただし、切り替えが必要な場合は、Snort 3 検査エンジン （23 ページ）の手順に従ってください。

重要 Snort のバージョンは自由に切り替えることができますが、Snort の一方バージョンでの侵入ルールを変更しても、もう一方のバージョンでは自動的に更新されません。Snort の一方のバージョンでルールのルールアクションを変更する場合は、Snort のバージョンを切り替える前に、もう一方のバージョンの変更を必ず複製してください。システムにより提供される同期オプションは、侵入ポリシーの Snort 2 バージョンの変更のみを Snort 3 バージョンに同期します。その逆の同期は行いません。

Snort 2 と Snort 3 の比較

Snort 3 はアーキテクチャが再設計され、Snort 2 と比較すると同等のリソースでより多くのトラフィックを検査します。Snort 3 では、トラフィックパーサーを簡単かつ柔軟に挿入できます。Snort 3 には、ルールの記述を容易にし、同等の共有オブジェクトルールを表示できる新しいルールシンタックスも用意されています。

次の表に、検査エンジン機能に関する Snort 2 バージョンと Snort 3 バージョンの違いを示します。

機能	Snort 2	Snort 3
パケットスレッド	プロセスごとに 1 つ	プロセスごとに任意の数
コンフィギュレーション メモリの使用	プロセス数 X *x* GB	合計 *x* GB。より多くのメモリをパケットに使用可能
設定のリロード	低速	より高速。1つのスレッドを個別のコアにピン留め可能
ルールのシンタックス	一貫性がなく、改行が必要	任意の空白を含む均一なシステム
ルールのコメント	コメントのみ	#、#begin、および #end マーク。C 言語スタイル

追加リファレンス：Firepower の Snort 2 と Snort 3 の違い。

Management Center 管理対象の Threat Defense での Snort 3 の機能制限

次の表に、Snort 2 でサポートされているが、Management Center 管理対象の 脅威に対する防御デバイスの Snort 3 ではサポートされていない機能を示します。

表 *1 : Snort 3* の機能制限

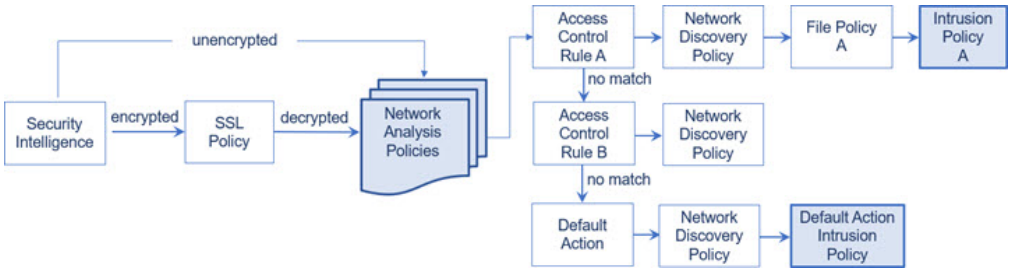
ポリシー/領域	サポートされない機能
アクセス コントロール ポリシー（Access Control Policy）	次のアプリケーション設定： • Safe Search • YouTube EDU

ポリシー/領域	サポートされない機能
侵入ポリシー（Intrusion Policy）	• グローバルルールのしきい値 • ロギングの設定： • SNMP • SRU ルールの更新（Snort 3 は LSP ルールの更新のみをサポートしているため）
その他の機能（Other features）	FQDN 名によるイベントのロギング

ポリシーがトラフィックで侵入を検査する方法

アクセス コントロールの展開の一部としてシステムがトラフィックを分析すると、ネットワーク分析（復号化と前処理）フェーズが侵入防御（侵入ルールおよび詳細設定）フェーズとは別にその前に実行されます。

次の図に、インラインでのトラフィック分析、侵入防御、およびネットワーク展開での AMP の順序を簡略化して示します。アクセス コントロール ポリシーが他のポリシーを呼び出してトラフィックを検査するしくみ、およびそれらのポリシーが呼び出される順序が示されています。ネットワーク分析ポリシーと侵入ポリシーの選択フェーズは強調表示されています。



インライン展開（つまり、ルーテッド、スイッチド、トランスペアレントインターフェイスまたはインラインインターフェイスのペアを使用して関連設定がデバイスに展開される展開）では、システムは上図のプロセスのほぼすべての段階において、追加のインスペクションなしでトラフィックをブロックすることができます。セキュリティインテリジェンス、SSLポリシー、ネットワーク分析ポリシー、ファイルポリシー、および侵入ポリシーのすべてで、トラフィックをドロップまたは変更できます。唯一の例外として、パッシブにパケットを検査するネットワーク検出ポリシーは、トラフィック フローに影響を与えることができません。

同様に、プロセスの各ステップで、パケットによってシステムがイベントを生成する場合があります。侵入およびプリプロセッサイベント（総称的に「侵入イベント」とも呼ばれる）は、パケットまたはそのコンテンツがセキュリティリスクを含んでいる可能性を示唆しています。

ヒント SSL インスペクションの設定で暗号化トラフィックの通過が許可されている場合や、SSL インスペクションが設定されていない場合について、この図は、そのような場合のアクセス コントロール ルールによる暗号化トラフィックの処理を反映していません。デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイル インスペクションは無効になっています。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

単一の接続の場合は、図に示すように、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定には影響**しません**。

復号、正規化、前処理：ネットワーク分析ポリシー

デコードと前処理を実行しないと、プロトコルの相違によりパターンマッチングを行えなくなるので、侵入についてトラフィックを適切に評価できません。これらのトラフィック処理タスクは、以下のタイミングでネットワーク分析ポリシーによる処理の対象となります。

- 暗号化トラフィックがセキュリティ インテリジェンスによってフィルタリングされた**後**
- 暗号化トラフィックがオプションの SSL ポリシーによって復号化された**後**
- ファイルまたは侵入ポリシーによってトラフィックを検査できるようになる**前**

ネットワーク分析ポリシーは、フェーズでのパケット処理を制御します。最初に、システムは最初の 3 つの TCP/IP 層を通ったパケットを復号し、次にプロトコル異常の正規化、前処理、および検出に進みます。

- パケットデコーダは、パケットヘッダーとペイロードを、インスペクタや後で侵入ルールで簡単に使用できる形式に変換します。TCP/IP スタックの各レイヤのデコードは、データリンク層から開始され、ネットワーク層、トランスポート層へと順番に行われます。パケット デコーダは、パケット ヘッダーのさまざまな異常動作も検出します。
- インライン展開では、インライン正規化プリプロセッサは、攻撃者が検出を免れる可能性を最小限にするために、トラフィックを再フォーマット（正規化）します。その他のインスペクタや侵入ルールによる検査用にパケットを準備し、システムで処理されるパケットがネットワーク上のホストで受信されるパケットと同じものになるようにします。
- ネットワーク層とトランスポート層のさまざまなインスペクタは、IP フラグメントを悪用する攻撃を検出したり、チェックサム検証を実行したり、TCP および UDP セッションの前処理を実行したりします。

  トランスポートおよびネットワークインスペクタの一部の詳細設定は、アクセス コントロール ポリシーのターゲットデバイスで処理されるすべてのトラフィックにグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

- 各種のアプリケーション層プロトコル デコーダは、特定タイプのパケット データを侵入ルール エンジンで分析可能な形式に正規化します。アプリケーション層プロトコルのエンコードを正規化することにより、システムはデータ表現が異なるパケットに同じコンテンツ関連の侵入ルールを効果的に適用し、大きな結果を得ることができます。
- Modbus、DNP3、CIP、および s7commplus SCADA インスペクタは、トラフィックの以上を検出し、侵入ルールにデータを提供します。Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャ プロセス、および設備プロセスからのデータをモニタ、制御、取得します。
- 一部のインスペクタでは、Back Orifice、ポートスキャン、SYN フラッドおよび他のレートベースの攻撃など、特定の脅威を検出できます。

  侵入ポリシーで、ASCII テキストのクレジットカード番号や社会保障番号などの機密データを検出する機密データインスペクタを設定することに注意してください。

新たに作成されたアクセス コントロール ポリシーでは、1 つのデフォルト ネットワーク分析ポリシーが、同じ親アクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシー向けのすべてのトラフィックの前処理を制御します。初期段階では、デフォルトで [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] ネットワーク分析ポリシーが使用されますが、別のシステム付属ポリシーやカスタム ネットワーク分析ポリシーに変更できます。より複雑な展開では、上級ユーザは、一致するトラフィックの前処理にさまざまなカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN に合わせてトラフィックの前処理オプションを調整できます。

（注） ルールアクションが [信頼（Trust）] であるアクセス コントロール ポリシーと、ロギングオプションが無効でアクションが [ファストパス（Fastpath）] であるプレフィルタルールの場合、フロー終了イベントが引き続きシステムで生成されることがわかります。このイベントは、Management Center のイベントページには表示されません。

アクセス コントロール ルール：侵入ポリシーの選択

最初の前処理の後、アクセスコントロールルール（ある場合）はトラフィックを評価します。ほとんどの場合、パケットが一致した最初のアクセス コントロール ルールがそのトラフィックを処理することになります。ユーザは一致したトラフィックをモニタ、信頼、ブロック、または許可することができます。

アクセス コントロール ルールでトラフィックを許可すると、ディスカバリ データ、マルウェア、禁止ファイル、侵入について、この順序でトラフィックを検査できます。アクセスコントロール ルールに一致しないトラフィックは、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。デフォルト アクションでは、ディスカバリ データと侵入についても検査できます。

（注） どのネットワーク分析ポリシーによって前処理されるかに**関わらず**、すべてのパケットは、設定されているアクセス コントロール ルールと上から順に照合されます（したがって、侵入ポリシーによる検査の対象となります）。

ポリシーがトラフィックで侵入を検査する方法 （7 ページ）の図に、インラインの侵入防御と AMP のネットワーク展開を次のように経由するトラフィックのフローを示します。

- アクセス コントロール ルール A により、一致したトラフィックの通過が許可されます。次にトラフィックは、ネットワーク検出ポリシーによるディスカバリ データの検査、ファイル ポリシー A による禁止ファイルおよびマルウェアの検査、侵入ポリシー A による侵入の検査を受けます。
- アクセス コントロール ルール B も一致したトラフィックを許可します。ただし、このシナリオでは、トラフィックは侵入（あるいはファイルまたはマルウェア）について検査されないので、ルールに関連付けられている侵入ポリシーやファイル ポリシーはありません。通過を許可されたトラフィックは、デフォルトでネットワーク検出ポリシーによって検査されます。したがって、この設定を行う必要はありません。
- このシナリオでは、アクセス コントロール ポリシーのデフォルト アクションで、一致したトラフィックを許可しています。次に、トラフィックはネットワーク検出ポリシー、さらにその後侵入ポリシーによって検査されます。アクセス コントロール ルールまたはデフォルト アクションに侵入ポリシーを関連付けるときに、必要に応じて、別の侵入ポリシーを使用できます。

ブロックされたトラフィックや信頼済みトラフィックは検査されないので、図の例には、ブロック ルールや信頼ルールは含まれていません。

侵入インスペクション：侵入ポリシー、ルール、変数セット

トラフィックが宛先に向かうことを許可する前に、システムの最終防御ラインとして侵入防御を使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーの主な機能は、どの侵入ルールおよびプリプロセッサ ルールを有効にしてどのように設定するかを管理することです。

侵入ルールとインスペクタ ルール

侵入ルールはキーワードと引数のセットとして指定され、ネットワーク上の脆弱性を悪用する試みを検出します。システムは侵入ルールを使用してネットワーク トラフィックを分析し、トラフィックがルールの条件に合致しているかどうかをチェックします。システムは各ルールで指定された条件をパケットに照らし合わせます。ルールで指定されたすべての条件にパケット データが一致する場合、ルールがトリガーされます。

システムには、Cisco Talos インテリジェンス グループ（Talos）によって作成された次のタイプのルールが含まれています。

- 共有オブジェクト侵入ルール：コンパイルされており、変更できません（ただし、送信元と宛先のポートや IP アドレスなどのルール ヘッダー情報を除く）。
- 標準テキスト侵入ルール：ルールの新しいカスタムインスタンスとして保存および変更できます。
- プリプロセッサルール：ネットワーク分析ポリシーのインスペクタとパケットデコーダの検出オプションが関連付けられたルールです。インスペクタルールはコピーしたり、編集したりできません。ほとんどのインスペクタルールはデフォルトで無効になっています。イベントを生成し、インライン展開で、違反パケットをドロップするためにインスペクタを使用するには、ルールを有効にする必要があります。

システムで侵入ポリシーに従ってパケットを処理する際には、最初にルール オプティマイザが、基準（トランスポート層、アプリケーションプロトコル、保護されたネットワークへの入出力方向など）に基づいて、サブセット内のすべてのアクティブなルールを分類します。次に、侵入ルールエンジンが、各パケットに適用する適切なルールのサブセットを選択します。最後に、マルチルール検索エンジンが3種類の検索を実行して、トラフィックがルールに一致するかどうかを検査します。

- プロトコル フィールド検索は、アプリケーション プロトコル内の特定のフィールドでの一致を検索します。
- 汎用コンテンツ検索は、パケット ペイロードの ASCII またはバイナリ バイトでの一致を検索します。
- パケット異常検索では、特定のコンテンツが含まれているかどうかではなく、確立されたプロトコルに違反しているパケット ヘッダーやペイロードが検索されます。

カスタム侵入ポリシーでは、ルールを有効化および無効化し、独自の標準テキストルールを記述および追加することで、検出を調整できます。Cisco 推奨機能を使用して、ネットワーク上で検出されたオペレーティングシステム、サーバー、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることもできます。

（注） ブロックルールと照合して特定のトラフィックを処理するのに十分なパケットがない場合、システムは残りのトラフィックを他のルールと照合して評価を続行します。残りのトラフィックのいずれかが、ブロックするように設定されているルールに一致すると、セッションはブロックされます。ただし、通過させる残りのトラフィックをシステムが分析すると、トラフィックステータスには、完全なパケットが不足しているルールで保留中と表示されます。

変数セット

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セット使用します。セット内の大部分の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスとポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

システムには、定義済みのデフォルト変数から構成される1つのデフォルト変数セットが含まれています。システム提供の共有オブジェクト ルールと標準テキスト ルールは、これらの定義済みのデフォルト変数を使用してネットワークおよびポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Webサーバに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。

ヒント システム提供の侵入ポリシーを使用する場合でも、シスコでは、デフォルトセットの主要なデフォルト変数を変更すること**強く**推奨します。ネットワーク環境を正確に反映する変数を使用すると、処理が最適化され、システムによって疑わしいアクティビティに関連するシステムをモニタできます。高度なユーザは、1つ以上のカスタム侵入ポリシーとペアリングするために、カスタム変数セットを作成して使用できます。

重要 カスタム変数セットを作成する場合は、カスタム変数セット名の最初の文字として数字を使用しないでください（たとえば、3Snort）。このようにして、Management Center の Threat Defense ファイアウォールに設定を展開すると、Snort 3 の検証が失敗します。

侵入イベントの生成

侵入されている可能性を特定すると、システムは侵入イベントまたはプリプロセッサイベント（まとめて侵入イベントと呼ばれることもあります）を生成します。管理対象デバイスはManagement Centerにイベントを送信します。ここで、集約データを確認し、ネットワーク アセットに対する攻撃を的確に把握できます。インライン展開では、管理対象デバイスは、有害であると判明しているパケットをドロップまたは置き換えることができます。

データベース内の各侵入イベントにはイベントヘッダーがあり、イベント名と分類、送信元と宛先の IP アドレス、ポート、イベントを生成したプロセス、およびイベントの日時に関する情報、さらに攻撃の送信元とそのターゲットに関するコンテキスト情報が含まれています。パケット ベースのイベントの場合、システムは復号化されたパケット ヘッダーとイベントをトリガーしたパケット（複数の場合あり）のペイロードのコピーもログに記録します。

パケット デコーダ、プリプロセッサ、および侵入ルール エンジンはすべて、システムによるイベントの生成を引き起こします。次に例を示します。

- （ネットワーク分析ポリシーで設定された）パケット デコーダが 20 バイト（オプションやペイロードのない IP データグラムのサイズ）未満の IP パケットを受け取った場合、デコーダはこれを異常なトラフィックと解釈します。パケットを検査する侵入ポリシー内の付随するデコーダルールが有効な場合、システムは後でインスペクタイベントを生成します。

- IP 最適化プリプロセッサが重複する一連の IP フラグメントを検出した場合、インスペクタはこれを潜在的な攻撃と解釈し、付随するインスペクタルールが有効な場合は、システムによってインスペクタイベントが生成されます。
- 侵入ルールエンジン内では、ほとんどの標準テキストルールおよび共有オブジェクトルールはパケットによってトリガーされた場合に侵入イベントを生成するように記述されます。

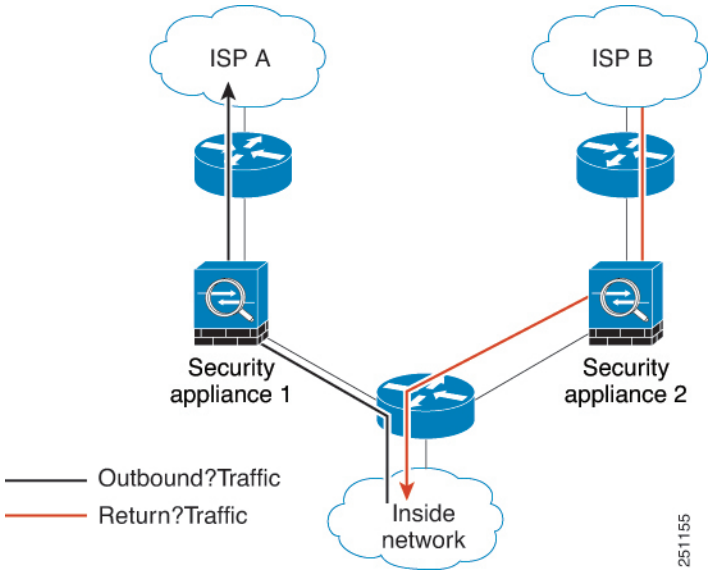
データベースに侵入イベントが蓄積されると、ユーザは攻撃の可能性について分析を開始できます。システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティ ポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールを提供します。

Snort での非対称フロー検査

非対称ルーティングを使用したインライン展開では、Snort の単方向トラフィックの可視性が制限されるため、パケットの正規化が損なわれます。Snort は、未確認のフロー方向からの TCP ハンドシェイクパラメータ（ウィンドウスケーリングや最大セグメントサイズ（MSS）など）に対応することができず、結果としてホストが大量のパケットを受信する可能性があります。

次の図では、両方のデバイスが Snort エンジンを実行しています。ところが、どちらのエンジンも完全なトラフィックフローを監視していません。フローの TCP 3 ウェイハンドシェイクは完全にはキャプチャされないため、適用できる正規化のタイプが制限されます。ただし、他の効果的な正規化は、Snort エンジンに表示されるフローの側で実行されます。

図 *1* : 非対称ルーティング



非対称ルーティングの環境では、Snort は追加の設定を必要とせずに変化にシームレスに適応します。フローパターンに基づいて動作をダイナミックに調整します。非対称トラフィックは、ファイアウォールの有効性に影響を与える可能性があり、最適な選択ではない場合がある

ことに注意してください。とはいえ、Snort は、必要に応じてこのような展開をサポートするように設計されています。

システム提供およびカスタムネットワーク分析ポリシーと侵入ポリシー

新しいアクセス コントロール ポリシーを作成することは、システムを使用してトラフィックフローを管理するための最初のステップの 1 つです。デフォルトでは、新しく作成されたアクセス コントロール ポリシーは、システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーを呼び出してトラフィックを検査します。

次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理と侵入防御フェーズは強調表示されています。

以下の点に注意してください。

- デフォルトのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が制御されます。初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。
- アクセス コントロール ポリシーのデフォルト アクションは、システム付属の Balanced Security and Connectivity 侵入ポリシーによる検査に従って、悪意のないトラフィックをすべて許可します。デフォルトアクションはトラフィックの通過を許可するので、侵入ポリシーが悪意のあるトラフィックを検査して潜在的にブロックする前に、検出機能によって、ホスト、アプリケーション、ユーザ データについてトラフィックを検査できます。
- ポリシーは、デフォルトのセキュリティ インテリジェンス オプション（グローバルなブロックリストとブロックなしリストのみ）を使用し、SSL ポリシーによる暗号化トラフィックの復号や、アクセス コントロール ルールを使用したネットワークトラフィックの特別な処理や検査は実行しません。

侵入防御展開を調整するために実行できるシンプルなステップは、システム付属のネットワーク分析ポリシーと侵入ポリシーの別のセットをデフォルトとして使用することです。システムには、これらのポリシーの複数のペアが提供されています。

または、カスタム ポリシーを作成して使用することで、侵入防御展開を調整できます。それらのポリシーに設定されているインスペクタオプション、侵入ルール、およびその他の詳細設定が、ネットワークのセキュリティのニーズに適合しない場合があります。設定できるネットワーク分析ポリシーおよび侵入ポリシーを調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

システム提供のネットワーク分析ポリシーと侵入ポリシー

システムには、ネットワーク分析ポリシーと侵入ポリシーのペアがいくつか付属しています。システムによって提供されるネットワーク分析と侵入ポリシーを使用することで、Cisco Talos インテリジェンスグループ（Talos）の経験を活用できます。これらのポリシーでは、Talos が侵入ルールとインスペクタルールの状態とともに、インスペクタやその他の詳細設定の初期設定も提供します。

すべてのネットワーク プロファイル、最小トラフィック、または防御ポスチャに対応したシステム付属ポリシーはありません。これらの各ポリシーは一般的なケースとネットワークのセットアップに対応しているため、これらのポリシーに基づいて適切に調整された防御ポリシーを策定することができます。システム付属ポリシーは、変更せずにそのまま使用できますが、カスタム ポリシーのベースとして使用し、カスタム ポリシーを各自のネットワークに合わせて調整することが推奨されます。

ヒント システム付属のネットワーク分析ポリシーと侵入ポリシーを使用する場合でも、ネットワーク環境が正確に反映されるように、システムの侵入変数を設定する必要があります。少なくとも、デフォルトのセットにある主要なデフォルトの変数を変更します。

新たな脆弱性が判明すると、Talos は侵入ルールの更新（Lightweight Security Package（LSP）ともいう）をリリースします。これらのルールの更新により、システムによって提供されるネットワーク分析ポリシーや侵入ポリシーが変更され、侵入ルールやインスペクタルールの新規作成または更新、既存ルールの状態の変更、デフォルトのポリシー設定の変更が行われます。ルールアップデートでは、システム付属のポリシーからルールが削除されたり、新しいルールカテゴリが提供されたり、さらにデフォルトの変数セットが変更されることもあります。

ルール更新によって展開が影響を受けると、Web インターフェイスは影響を受けた侵入ポリシーやネットワーク分析ポリシー、およびそれらの親のアクセス コントロール ポリシーを失効したものとして扱います。変更を有効にするには、更新されたポリシーを再展開する必要があります。

必要に応じて、影響を受けた侵入ポリシーを（単独で、または影響を受けたアクセス コントロール ポリシーと組み合わせて）自動的に再展開するように、ルールの更新を設定できます。これにより、新たに検出されたエクスプロイトおよび侵入から保護するために展開環境を容易に自動的に最新に維持することができます。

前処理の設定を最新の状態に保つには、アクセス コントロール ポリシーを再展開する**必要があります**。これにより、現在実行されているものとは異なる、関連する SSL ポリシー、ネットワーク分析ポリシー、ファイル ポリシーが再展開され、前処理とパフォーマンスの詳細設定オプションのデフォルト値も更新できるようになります。

システムに付属しているネットワーク分析ポリシーと侵入ポリシーのペアは以下のとおりです。

[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、速度と検出の両方を目的として作成されています。一緒に使用すると、ほとんどの組織および展開タイプにとって最適な出発点となります。ほとんどの場合、システムは Balanced Security and Connectivity のポリシーおよび設定をデフォルトとして使用します。

Connectivity Over Security ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、接続（すべてのリソースに到達可能な）の方がネットワークインフラストラクチャのセキュリティより優先される組織向けに作られています。この侵入ポリシーは、[接続性よりもセキュリティを優先（Security over Connectivity）] ポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールだけが有効にされます。

[接続性よりもセキュリティを優先（Security over Connectivity）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、ネットワークインフラストラクチャのセキュリティがユーザの利便性より優先される組織向けに作られています。この侵入ポリシーは、正式なトラフィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。

[最大検出（Maximum Detection）] ネットワーク分析ポリシーおよび侵入ポリシー

このポリシーは、Security over Connectivity ポリシー以上にネットワーク インフラストラクチャのセキュリティを重視する組織のために作成されています。動作への影響がさらに高くなる可能性があります。たとえば、この侵入ポリシーでは、マルウェア、エクスプロイト キット、古い脆弱性や一般的な脆弱性、および既知の流行中のエクスプロイトを含め、多数の脅威カテゴリのルールを有効にします。

[アクティブなルールなし（No Rules Active）] 侵入ポリシー

[アクティブなルールなし（No Rules Active）] 侵入ポリシーでは、すべての侵入ルールと侵入ルールのしきい値を除くすべての詳細設定が無効にされます。このポリシーは、他のシステムによって提供されるポリシーのいずれかで有効になっているルールをベースにするのではなく、独自の侵入ポリシーを作成する場合の出発点を提供します。

（注） 選択されているシステムから提供されるベースポリシーによって、ポリシーの設定が異なります。ポリシー設定を表示するには、ポリシーの横にある [編集（Edit）] アイコンをクリックしてから、[ベースポリシー（Base Policy）] リンクをクリックします。

カスタムネットワーク分析ポリシーと侵入ポリシーの利点

システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーに設定されたインスペクタオプション、侵入ルール、およびその他の詳細設定は、組織のセキュリティのニーズに十分に対応しない場合があります。

カスタム侵入ポリシーを作成すると、環境内のシステムのパフォーマンスを向上させ、ネットワークで発生する悪意のあるトラフィックやポリシー違反を重点的に観察できるようになります。設定できるカスタムポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

すべてのカスタムポリシーには基本ポリシー（別名「基本レイヤ」）があり、それによって、ポリシー内のすべてのコンフィギュレーションのデフォルト設定が定義されます。レイヤは、複数のネットワーク分析ポリシーまたは侵入ポリシーを効率的に管理するために使用できる構成要素です。

ほとんどの場合、カスタムポリシーはシステム付属のポリシーに基づきますが、別のカスタムポリシーを使用することもできます。ただし、すべてのカスタム ポリシーには、ポリシーチェーンの根本的な基礎としてシステム付属ポリシーが含まれています。システム付属のポリシーはルールアップデートによって変更される可能性があるので、カスタムポリシーを基本として使用している場合でも、ルールアップデートをインポートするとポリシーに影響が及びます。ルール更新によって展開が影響を受けると、Web インターフェイスは影響を受けたポリシーを失効として扱います。

カスタム ネットワーク分析ポリシーの利点

デフォルトでは、1つのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべての暗号化されていないトラフィックが前処理されます。これは、侵入ポリシー（および侵入ルールセット）に関係なく、すべてのパケットが同じ設定に基づいてデコードされ、処理されることを意味します。

初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。

使用可能な調整オプションはインスペクタによって異なりますが、インスペクタやデコーダを調整できる方法には次のものがあります。

- モニタしているトラフィックに適用しないインスペクタは無効にできます。たとえば、HTTP Inspect インスペクタは HTTP トラフィックを正規化します。ネットワークに Microsoft インターネット インフォメーション サービス（IIS）を使用する Web サーバが含まれていないことが確実な場合は、IIS 特有のトラフィックを検出するインスペクタオプションを無効にすることで、システム処理のオーバーヘッドを軽減できます。

（注） カスタムネットワーク分析ポリシーでインスペクタが無効化されているときに、パケットを有効な侵入ルールまたはインスペクタルールと照合して評価するためにインスペクタを使用する必要がある場合、システムはインスペクタを自動的に有効にして使用します。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。

- 必要に応じて、特定のインスペクタのアクティビティを集中させるポートを指定します。たとえば、DNS サーバの応答や暗号化 SSL セッションをモニタするための追加ポートや、Telnet、HTTP、RPC トラフィックを復号するポートを特定できます。

複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。さらに、トラフィックのセキュリティ ゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます（ASA FirePOWER モジュールでは、VLAN による前処理を制限することはできません）。

（注） カスタム ネットワーク分析ポリシー（特に複数のネットワーク分析ポリシー）を使用して前処理を調整することは、高度なタスクです。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、単一の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が相互補完することを許可する場合は、注意する**必要があります**。

カスタム侵入ポリシーの利点

侵入防御を実行するように初期設定して、新規にアクセス コントロール ポリシーを作成した場合、そのポリシーでは、デフォルト アクションはすべてのトラフィックを許可しますが、最初にシステム付属の Balanced Security and Connectivity 侵入ポリシーでトラフィックをチェックします。アクセス コントロール ルールを追加するか、またはデフォルト アクションを変更しない限り、すべてのトラフィックがその侵入ポリシーによって検査されます。

侵入防御展開をカスタマイズするために、複数の侵入ポリシーを作成し、それぞれがトラフィックを異なる方法で検査するように調整できます。次に、どのポリシーがどのトラフィックを検査するかを指定するルールを、アクセス コントロール ポリシーに設定します。アクセス コントロール ルールは単純でも複雑でもかまいません。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、またはユーザなど、複数の基準を使用してトラフィックを照合および検査します。

侵入ポリシーの主な機能は、次のように、どの侵入ルールやインスペクタルールを有効にし、どのように設定するかを管理することです。

- 各侵入ポリシーで、環境に適用されるすべてのルールが有効になっていることを確認し、環境に適用されないルールを無効化することによって、パフォーマンスを向上させます。どのルールで悪質なパケットをドロップまたは変更するかを指定できます。
- Cisco 推奨機能を使用すると、ネットワーク上で検出されたオペレーティングシステム、サーバー、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。
- 必要に応じて、既存のルールの変更や、新しい標準テキストルールの作成により、新たなエクスプロイトの検出やセキュリティ ポリシーの適用が可能です。

侵入ポリシーに対して行えるその他のカスタマイズは次のとおりです。

- 機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。特定の脅威（Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃）を検出する他のインスペクタは、ネットワーク分析ポリシーで設定します。
- グローバルしきい値を設定すると、侵入ルールに一致するトラフィックが、指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成されます。これにより、大量のイベントによってシステムに過剰な負荷がかかることを回避できます。
- また、個々のルールまたは侵入ポリシー全体に対して、侵入イベント通知を抑制し、しきい値を設定することで、大量のイベントによってシステムに過剰な負荷がかかることを回避することもできます。
- Web インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、syslog ファシリティへのロギングを有効にしたり、イベント データを SNMP トラップ サーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。これらのポリシー単位のアラート設定に加えて、各ルールまたはルール グループの侵入イベントを通知する電子メール アラートをグローバルに有効化/無効化できます。どの侵入ポリシーがパケットを処理するかに関わらず、ユーザの電子メール アラート設定が使用されます。

カスタム ポリシーの制限

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、単一のパケットを処理および検査する、ネットワーク分析ポリシーと侵入ポリシーが相互補完することを設定で許可する場合は、注意する**必要があります**。

デフォルトでは、システムは、管理対象デバイスでアクセス コントロール ポリシーにより処理されるすべてのトラフィックを、1 つのネットワーク分析ポリシーを使用して前処理します。次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理と侵入防御フェーズは強調表示されています。

アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が、デフォルトのネットワーク分析ポリシーによってどのように制御されるのか注意してください。初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。

前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。ただし、カスタムネットワーク分析ポリシーでインスペクタを無効にしたときに、前処理されたパケットを有効な侵入ルールまたはインスペクタルールと照合して評価する必要がある場合、システムはインスペクタを自動的に有効にして使用します。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なままになります。

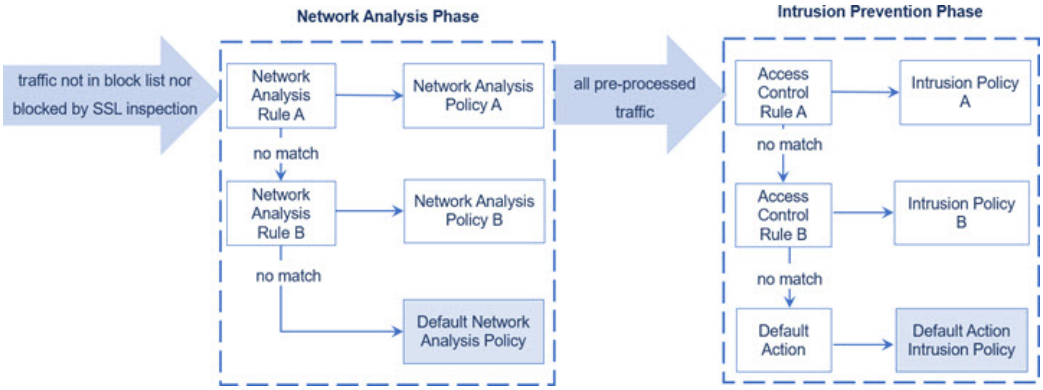
（注） インスペクタを無効にするパフォーマンス上の利点を得るには、侵入ポリシーでそのインスペクタを必要とするルールが有効になっていないことを確認する**必要があります**。

複数のカスタム ネットワーク分析ポリシーを使用する場合は、さらに課題があります。複雑な展開内の上級ユーザの場合は、一致したトラフィックの前処理にカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN に合わせて前処理を調整できます。（ASA FirePOWER では、VLAN による前処理を制限することはできません）。これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。各ルールにはネットワーク分析ポリシーが関連付けられており、ルールに一致するトラフィックの前処理を制御します。

ヒント アクセス コントロール ポリシーの詳細設定としてネットワーク分析ルールを設定します。他のタイプのルールとは異なり、ネットワーク分析ルールは、ネットワーク分析ポリシーに含まれているのではなく、ネットワーク分析ポリシーを呼び出します。

システムは、ルール番号の昇順で、設定済みネットワーク分析ルールとパケットを照合します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。これにより非常に柔軟にトラフィックを前処理できます。ただし、留意すべき点として、パケットがどのネットワーク分析ポリシーによって前処理されるかに**関係なく**、すべてのパケットは、それら独自のプロセスにおいて引き続きアクセス コントロール ルールと照合されます（つまり、侵入ポリシーにより検査される可能性があります）。つまり、特定のネットワーク分析ポリシーでパケットを前処理しても、そのパケットが確実に特定の侵入ポリシーで検査されるわけでは**ありません**。アクセス コントロール ポリシーを設定するときは、そのポリシーが正しいネットワーク分析ポリシーおよび侵入ポリシーを呼び出して特定のパケットを評価するように、慎重に行う**必要があります**。

次の図は、侵入防御（ルール）フェーズよりも前に、別にネットワーク分析ポリシー（前処理）の選択フェーズが発生するしくみを詳細に示しています。簡略化するために、図では検出フェーズとファイル/マルウェア インスペクション フェーズが省かれています。また、デフォルトのネットワーク分析ポリシーおよびデフォルト アクションの侵入ポリシーを強調表示しています。



このシナリオでは、アクセス コントロール ポリシーに、2 つのネットワーク分析ルールとデフォルトのネットワーク分析ポリシーが設定されています。

- Network Analysis Rule A は、一致するトラフィックを Network Analysis Policy A で前処理します。その後、このトラフィックを Intrusion Policy A で検査されるようにすることができます。
- Network Analysis Rule B は、一致するトラフィックを Network Analysis Policy B で前処理します。その後、このトラフィックを Intrusion Policy B で検査されるようにすることができます。
- 残りのトラフィックはすべて、デフォルトのネットワーク分析ポリシーにより前処理されます。その後、このトラフィックをアクセス コントロール ポリシーのデフォルト アクションに関連付けられた侵入ポリシーによって検査されるようにすることができます。

システムはトラフィックを前処理した後、侵入についてトラフィックを検査できます。図では、2 つのアクセス コントロール ルールとデフォルト アクションが含まれるアクセス コントロール ポリシーを示しています。

- アクセス コントロール ルール A は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy A によって検査されます。
- アクセス コントロール ルール B は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy B によって検査されます。
- アクセス コントロール ポリシーのデフォルト アクションは一致したトラフィックを許可します。トラフィックはその後、デフォルト アクションの侵入ポリシーによって検査されます。

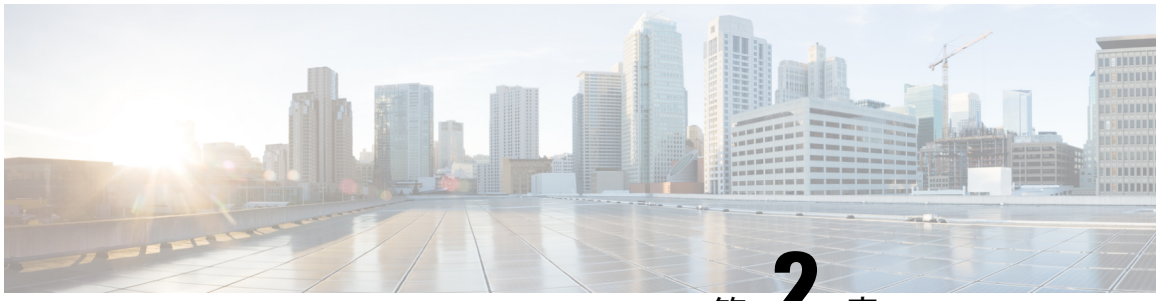
各パケットの処理は、ネットワーク分析ポリシーと侵入ポリシーのペアにより制御されますが、このペアはユーザに合わせて調整**されません**。アクセス コントロール ポリシーが誤って設定されているため、ネットワーク分析ルール A とアクセス コントロール ルール A が同じトラフィックを処理しない場合を想定してください。たとえば、特定のセキュリティ ゾーンのトラフィックの処理をポリシー ペアによって制御することを意図している場合に、誤まって、異なるゾーンを使用するように 2 つのルールの条件を設定したとします。この誤設定により、トラフィックが誤って前処理される可能性があります。したがって、ネットワーク分析ルールおよびカスタム ポリシーを使用した前処理の調整は、**高度な**タスクです。

単一の接続の場合は、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定には影響**しません**。

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。



第 2 章

Snort 2 から Snort 3 への移行

バージョン 7.0.0 以降では、Management Center を使用した Threat Defense 展開で、Snort 3 がデフォルトの検査エンジンです。まだ Snort 2 検査エンジンを使用している場合は、検出とパフォーマンスを向上させるために、今すぐ Snort 3 に切り替えてください。

Threat Defense をバージョン 7.2 ～ 7.6 にアップグレードすると、対象の Snort 2 デバイスも Snort 3 にアップグレードされます。カスタム侵入またはネットワーク分析ポリシーを使用しているために不適格なデバイスの場合、ここで説明する手順で手動で Snort 3 にアップグレードしてください。

個々のデバイスを元に戻すことはできますが、推奨されません。Snort 2 は将来のリリースで廃止され、最終的に Threat Defense のアップグレードを妨げるものになります。

- Snort 3 検査エンジン （23 ページ）
- ネットワーク分析と侵入ポリシーの前提条件 （24 ページ）
- Snort 2 から Snort 3 への移行方法 （24 ページ）
- Snort 2 と Snort 3 のベースポリシーのマッピングの表示 （28 ページ）
- Snort 2 のルールと Snort 3 の同期 （29 ページ）
- 設定変更の展開 （30 ページ）

Snort 3 検査エンジン

Snort 3 は、バージョン 7.0 以降の新規登録 脅威に対する防御 デバイスのデフォルト検査エンジンです。ただし、下位バージョンの 脅威に対する防御 デバイスでは、Snort 2 がデフォルトの検査エンジンです。管理対象の 脅威に対する防御 デバイスをバージョン 7.0 以降にアップグレードしても、検査エンジンは Snort 2 のままです。バージョン 7.0 以降のアップグレードされた 脅威に対する防御 で 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 3 をデバイスの検査エンジンとして有効にすると、（アクセス コントロール ポリシーを介して）デバイスに適用される侵入ポリシーの Snort 3 バージョンがアクティブ化され、デバイスを通過するすべてのトラフィックに適用されます。

必要に応じて Snort のバージョンを切り替えることができます。Snort 2 と Snort 3 の侵入ルールがマッピングされ、マッピングはシステムによって実行されます。ただし、Snort 2 と Snort 3 のすべての侵入ルールの 1 対 1 のマッピングが見つからない場合があります。Snort 2 で 1 つの

ルールのルールアクションを変更した場合、Snort 2 と Snort 3 を同期せずに Snort 3 に切り替えると、その変更は保持されません。同期の詳細については、Snort 2 のルールと Snort 3 の同期（29 ページ）を参照してください。

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 2 から Snort 3 への移行方法

Snort 2 から Snort 3 に移行するには、脅威に対する防御 デバイスの検査エンジンを Snort 2 から Snort 3 に切り替える必要があります。

要件に応じて、Snort 2 から Snort 3 へのデバイスの移行を完了するためのタスクを次の表に示します。

ステップ	タスク	手順へのリンク
1	Snort 3 の有効化	• 個々のデバイス上での Snort 3 の有効化 （25 ページ） • 複数のデバイス上での Snort 3 の有効化 （26 ページ）
2	Snort 2 のカスタムルールの Snort 3 への変換	• すべての侵入ポリシーのすべての Snort 2 カスタムルールの Snort 3 への変換 （27 ページ） • 単一の侵入ポリシーの Snort 2 カスタムルールの Snort 3 への変換 （28 ページ）
3	Snort 2 のルールと Snort 3 の同期	Snort 2 のルールと Snort 3 の同期 （29 ページ）

Snort 2 から Snort 3 への移行の前提条件

以下は、デバイスを Snort 2 から Snort 3 に移行する前に考慮する必要がある推奨される前提条件です。

- Snort の実用的な知識を持っている。Snort 3 アーキテクチャの詳細については、Snort 3 Adoption を参照してください。

- Management Center をバックアップする。「Backup the Management Center」を参照してください。
- 侵入ポリシーをバックアップする。「Exporting Configurations」を参照してください。
- 侵入ポリシーを複製する。複製する場合、既存のポリシーをベースポリシーとして使用して、侵入ポリシーのコピーを作成できます。[侵入ポリシー（Intrusion Policies）] ページで、[ポリシーの作成（Create Policy）] をクリックし、[ベースポリシー（Base Policy）] ドロップダウンリストから既存の侵入ポリシーを選択します。

個々のデバイス上での Snort 3 の有効化

重要 展開プロセス中に現在の検査エンジンをシャットダウンする必要があるため、一時的なトラフィック損失が発生します。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択します。

ステップ 2 デバイスをクリックして、デバイスのホームページに移動します。

（注） デバイスは Snort 2 または Snort 3 としてマークされ、デバイスの現在のバージョンが表示されます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [検査エンジン（Inspection Engine）] セクションで、[アップグレード（Upgrade）] をクリックします。

（注） Snort 3 を無効にする場合は、[検査エンジン（Inspection Engine）] セクションで [Snort 2 に戻す（Revert to Snort 2）] をクリックします。

ステップ 5 [はい（Yes）] をクリックします。

次のタスク

デバイスに変更を展開します。設定変更の展開 （30 ページ）を参照してください。.

選択した Snort バージョンとの互換性を得るため、システムは展開プロセス中にポリシー設定を変換します。

複数のデバイス上での Snort 3 の有効化

複数のデバイスで Snort 3 を有効にするには、必要なすべての 脅威に対する防御 デバイスがバージョン 7.0 以降であることを確認します。

重要 展開プロセス中に現在の検査エンジンをシャットダウンする必要があるため、一時的なトラフィック損失が発生します。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択します。

ステップ 2 Snort 3 を有効または無効にするすべてのデバイスを選択します。

（注） デバイスは Snort 2 または Snort 3 としてマークされ、デバイスの現在のバージョンが表示されます。

ステップ 3 [一括アクションの選択（Select Bulk Action）] ドロップダウンリストをクリックし、[Snort 3へのアップグレード（Upgrade to Snort 3）] を選択します。

ステップ 4 [はい（Yes）] をクリックします。

次のタスク

デバイスに変更を展開します。設定変更の展開 （30 ページ）を参照してください。.

選択した Snort バージョンとの互換性を得るため、システムは展開プロセス中にポリシー設定を変換します。

Snort 2 のカスタム IPS ルールの Snort 3 への変換

サードパーティベンダーのルールセットを使用している場合は、そのベンダーに連絡して、そのルールが Snort 3 に正常に変換されることを確認するか、または Snort 3 用にネイティブに作成された代わりのルールセットを取得します。独自に作成したカスタムルールがある場合は、変換前に Snort 3 ルールの作成に慣れておくと、変換後の Snort 3 検出を最適化するようにルールを更新できます。Snort 3 でのルールの作成の詳細については、次のリンクを参照してください。

- https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html
- https://blog.snort.org/2020/10/talos-transition-to-snort-3.html

Snort 3 ルールの詳細については、https://blog.snort.org/ にある他のブログを参照してください。

システム提供のツールを使用して Snort 2 ルールを Snort 3 ルールに変換するには、次の手順を参照してください。

- すべての侵入ポリシーのすべての Snort 2 カスタムルールの Snort 3 への変換 （27 ページ）
- 単一の侵入ポリシーの Snort 2 カスタムルールの Snort 3 への変換 （28 ページ）

重要 Snort 2 ネットワーク分析ポリシー（NAP）の設定を Snort 3 に自動的にコピーすることはできません。NAP 設定は、Snort 3 で手動で複製する必要があります。

すべての侵入ポリシーのすべての Snort 2 カスタムルールの Snort 3 への変換

手順

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 左側のペインで [すべてのルール（All Rules）] が選択されていることを確認します。

ステップ 4 [タスク（Tasks）] ドロップダウンリストから値を選択します。

- **[Snort 2ルールの変換とインポート（Convert Snort 2 rules and import）]**：すべての侵入ポリシーのすべての Snort 2 カスタムルールを Snort 3 に自動的に変換し、それらを Snort 3 カスタムルールとして Management Center にインポートします。
- **[Snort 2ルールの変換とダウンロード（Convert Snort 2 rules and download）]**：すべての侵入ポリシーのすべての Snort 2 カスタムルールを Snort 3 に自動的に変換し、それらをローカルシステムにダウンロードします。

ステップ 5 [OK] をクリックします。

（注）
- 前の手順で [変換してインポート（Convert and import）] を選択した場合は、変換されたすべてのルールが、[ローカルルール（Local Rules）] の下に新しく作成されたルールグループ [すべての Snort 2 をグローバルに変換（All Snort 2 Converted Global）] の下に保存されます。
- 前の手順で [変換してダウンロード（Convert and download）] を選択した場合は、ルールファイルをローカルに保存します。ダウンロードしたファイル内の変換済みのルールを確認します。後でルールグループへのカスタムルールの追加 （65 ページ）の手順に従ってアップロードできます。

追加のサポートと情報については、「Snort 2 ルールの Snort 3 への変換」ビデオを参照してください。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

単一の侵入ポリシーの Snort 2 カスタムルールの Snort 3 への変換

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 [侵入ポリシー（Intrusion Policies）] タブで、[Snort 3同期ステータスの表示（Show Snort 3 Sync status）] をクリックします。

ステップ 3 侵入ポリシーの [同期（Sync）] アイコン（ ）をクリックします。

（注） 侵入ポリシーの Snort 2 バージョンと Snort 3 バージョンが同期されている場合は、[同期（Sync）] アイコンが緑色の で表示されます。変換するカスタムルールがないことを示します。

ステップ 4 サマリーを読み、[カスタムルール（Custom Rules）] タブをクリックします。

ステップ 5 次のどちらかを選択します。

- [変換後のルールをこのポリシーにインポートする（Import converted rules to this policy）]：侵入ポリシーの Snort 2 カスタムルールを Snort 3 に変換し、Snort 3 カスタムルールとして Management Center にインポートします。
- [変換後のルールのダウンロード（Download converted rules）]：侵入ポリシーのSnort 2カスタムルールをSnort 3に変換し、ローカルシステムにダウンロードします。ダウンロードしたファイル内の変換後のルールを確認し、後でアップロードアイコンをクリックしてファイルをアップロードできます。

ステップ 6 [再同期（Re-Sync）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

Snort 2 と Snort 3 のベースポリシーのマッピングの表示

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 [侵入ポリシー（Intrusion Policies）] タブが選択されていることを確認します。

ステップ 3 [IPS マッピング（IPS Mapping）] をクリックします。

ステップ 4 [IPSポリシーマッピング（IPS Policy Mapping）] ダイアログボックスで、[マッピングの表示（View Mappings）] をクリックして、Snort 3 から Snort 2 への侵入ポリシーのマッピングを表示します。

ステップ 5 [OK] をクリックします。

Snort 2 のルールと Snort 3 の同期

Snort 2 のバージョン設定とカスタムルールが保持され、Snort 3 に引き継がれるための同期機能が Management Center によって提供されます。同期することで、過去数か月または数年にわたって変更または追加されている可能性がある、Snort 2 ルールのオーバーライド設定とカスタムルールを Snort 3 バージョンで複製できます。このユーティリティは、Snort 2 バージョンのポリシー設定を Snort 3 バージョンと同期して、同様の対象範囲で開始するのに役立ちます。

Management Center を 6.7 より前のバージョンから 7.0 以降のバージョンにアップグレードすると、設定が同期されます。Management Center が新しい 7.0 移行のバージョンの場合、より高いバージョンにアップグレードできますが、アップグレード中にコンテンツは同期されません。

デバイスを Snort 3 にアップグレードする前に、Snort 2 バージョンで変更が行われた場合は、このユーティリティを使用して Snort 2 バージョンから Snort 3 バージョンに最新の同期を行うことができ、同様の対象範囲で開始できます。

（注） Snort 3 への移行時に、Snort 3 バージョンのポリシーを別個に管理し、通常の運用としてこのユーティリティを使用しないことを推奨します。

重要

- Snort 2 ルールのオーバーライドとカスタムルールのみが Snort 3 にコピーされ、その逆は行われません。Snort 2 と Snort 3 のすべての侵入ルールの 1 対 1 のマッピングが見つからない場合があります。次の手順を実行すると、両方のバージョンに存在するルールのルールアクションに対する変更が同期されます。
- 同期では、カスタムまたはシステムによって提供されるルールのしきい値と抑制の設定は Snort 2 から Snort 3 に移行されません。

手順

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 [侵入ポリシー（Intrusion Policies）] タブが選択されていることを確認します。

ステップ 3 [Snort 3 の同期ステータスの表示（Show Snort 3 Sync status）] をクリックします。

ステップ 4 同期していない侵入ポリシーを特定します。

ステップ 5 [同期（Sync）] アイコン をクリックします。

（注） 侵入ポリシーの Snort 2 バージョンと Snort 3 バージョンが同期されている場合は、[同期（Sync）] アイコンが緑色の で表示されます。

ステップ 6 サマリーを読み、必要に応じてサマリーのコピーをダウンロードします。

ステップ 7 [再同期（Re-Sync）] をクリックします。

（注）
- 同期された設定は、Snort 3 侵入エンジンがデバイスに適用され、展開が成功した後にのみ適用されます。
- Snort 2 カスタムルールは、システム付属のツールを使用してSnort 3 に変換できます。Snort 2 カスタムルールがある場合は、[カスタムルール（Custom Rules）] タブをクリックし、画面の指示に従ってルールを変換します。詳細については、単一の侵入ポリシーの Snort 2 カスタムルールの Snort 3 への変換 （28 ページ）を参照してください。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

設定変更の展開

設定を変更した後に、影響を受けるデバイスに展開します。

（注） このトピックでは、設定変更を展開する基本的な手順について説明します。手順を進める前に、最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Deploy Configuration Changes*」トピックを参照し、変更を展開する上での前提条件と影響を理解しておくことを強く推奨します。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。

手順

ステップ 1 Secure Firewall Management Center メニューバーで、[展開（Deploy）] をクリックし、[展開（Deployment）] を選択します。

[GUI] ページには、期限切れの設定を持ち、ステータスが [保留中（Pending）] のデバイスのリストが表示されます。

- [変更者（Modified by）] 列には、ポリシーまたはオブジェクトを変更したユーザーの一覧が表示されます。デバイスリストを展開すると、ポリシーリストごとのポリシーを変更したユーザーが表示されます。

  （注） 削除されたポリシーおよびオブジェクトのユーザ名は表示されません。

- [インスペクションの中断（Inspect Interruption）] 列には、展開時にデバイスでトラフィック インスペクションの中断が発生する可能性があるかどうかが示されます。

  デバイスのこの列のエントリが空白の場合は、展開時にそのデバイス上でのトラフィック インスペクションが中断されないことを示します。

- [最終変更時刻（Last Modified Time）] 列は、最後に設定変更を行った時刻を示します。
- [プレビュー（Preview）] 列では、次の展開の変更をプレビューできます。
- [ステータス（Status）] 列には、各展開のステータスが表示されます。

ステップ 2 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**（[展開矢印（expand arrow）] アイコン [展開矢印（expand arrow）] アイコン） をクリックします。

  デバイスの横にあるチェックボックスをオンにすると、デバイスに加えられ、デバイスの下にリストされているすべての変更が展開のためにプッシュされます。ただし、**ポリシーの選択**（[ポリシーの選択（policy selection）] アイコン [ポリシーの選択（policy selection）] アイコン） を使用して展開する個々のポリシーや特定の設定を選択し、残りの変更は展開せずに保持することができます。

（注）
- [インスペクションの中断（Inspect Interruption）] 列のステータスに [あり（Yes）] と表示され、展開によって 脅威に対する防御 デバイスでインスペクションと、場合によってはトラフィックが中断されるときは、展開されたリストには中断の原因となった特定の設定が **インスペクションの中断**（[インスペクションの中断（inspect interruption）] アイコン [インスペクションの中断（inspect interruption）] アイコン） で示されます。
- インターフェイスグループ、セキュリティゾーン、またはオブジェクトに変更がある場合、影響を受けるデバイスは、Management Center で失効として表示されます。これらの変更が有効になるようにするには、これらのインターフェイスグループ、セキュリティゾーン、またはオブジェクトを含むポリシーも、これらの変更とともに展開する必要があります。影響を受けるポリシーは、Management Center の [プレビュー（Preview）] ページに失効として表示されます。

ステップ 3 [展開（Deploy）] をクリックします。

ステップ 4 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。

次の選択肢があります。

- [展開（Deploy）]：警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [閉じる（Close）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

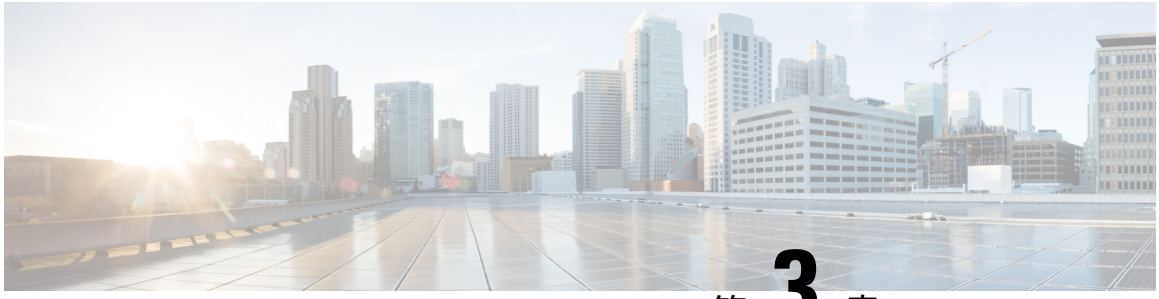
次のタスク

展開中に展開が失敗した場合、その障害がトラフィックに影響を与える可能性があります。ただし、特定の条件によって異なります。展開に特定の設定変更がある場合、展開の失敗によってトラフィックが中断されることがあります。詳細については、最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「Deploy Configuration Changes」のトピックを参照してください。

第 部

Snort 3 での侵入検知と防御

- Snort 3 侵入ポリシーを開始するには （35 ページ）
- ルールを使用した侵入ポリシーの調整 （49 ページ）
- ネットワーク資産に応じた侵入防御の調整 （71 ページ）



第 3 章

Snort 3 侵入ポリシーを開始するには

この章では、侵入検知と防御のための Snort 3 侵入ポリシーとアクセス制御ルール設定の管理について説明します。

- 侵入ポリシーの概要 （35 ページ）
- ネットワーク分析と侵入ポリシーの前提条件 （37 ページ）
- カスタム Snort 3 侵入ポリシーの作成 （37 ページ）
- Snort 3 侵入ポリシーの編集 （37 ページ）
- 侵入ポリシーのベースポリシーの変更 （44 ページ）
- 侵入ポリシーの管理 （44 ページ）
- 侵入防御を実行するためのアクセスコントロールルール設定 （45 ページ）

侵入ポリシーの概要

侵入ポリシーは定義済みの侵入検知のセットであり、セキュリティ違反についてトラフィックを検査し、インライン展開の場合は、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーは、アクセス コントロール ポリシーによって呼び出され、システムの最終防御ラインとして、トラフィックが宛先に到達することを許可するかどうかを判定します。

各侵入ポリシーの中核となるのは、侵入ルールです。ルールを有効にすると、ルールに一致するトラフィックに対して侵入イベントが生成されます（さらに、必要に応じてトラフィックがブロックされます）。ルールを無効にすると、ルールの処理が停止されます。

システムによって提供されるいくつかの基本侵入ポリシーにより、Cisco Talos Intelligence Group（Talos）の経験を活用できます。これらのポリシーでは、Talos が侵入ルールとインスペクタルールの状態（有効または無効）を設定し、他の詳細設定の初期設定も行います。

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。

カスタム侵入ポリシーを作成すると、以下を実行できます。

- ルールを有効化/無効化することに加え、独自のルールを作成して追加し、検出を調整する。
- ネットワーク上で検出されたオペレーティングシステム、サーバー、およびクライアントアプリケーションプロトコルをそれらの資産を保護するために明確に書き込まれたルールに関連付けるには、Secure Firewall の推奨事項を使用します。

侵入ポリシーは一致するパケットをドロップして、侵入イベントを生成できます。侵入またはプリプロセッサのドロップルールを設定するには、その状態を [ブロック（Block）] に設定します。

留意事項として、侵入ポリシーを調整する場合（特にルールを有効化して追加する場合）、一部の侵入ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理する必要があります。侵入ポリシーによって検査される前に、パケットはネットワーク分析ポリシーの設定に従って前処理されます。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。

注意 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。

カスタム侵入ポリシーを設定した後、それを 1 つ以上のアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けることによって、カスタム侵入ポリシーをアクセスコントロール設定の一部として使用できます。これによって、システムは、最終宛先に渡す前に、特定の許可されたトラフィックを侵入ポリシーによって検査します。変数セットを侵入ポリシーと組み合わて使用することにより、ホーム ネットワークと外部ネットワークに加えて、必要に応じてネットワーク上のサーバを正確に反映させることができます。

デフォルトでは、暗号化ペイロードの侵入インスペクションは無効化されます。これにより、侵入インスペクションが設定されているアクセス コントロール ルールと暗号化された接続を照合する際の誤検出が減少し、パフォーマンスが向上します。

追加のサポートと情報については、「Snort 3 侵入ポリシーの概要」ビデオを参照してください。

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。

カスタム Snort 3 侵入ポリシーの作成

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

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）] に一意の名前を入力し、オプションで [説明（Description）] を入力します。

ステップ 4 [検査モード（Inspection Mode）] を選択します。

選択したアクションによって、侵入ルールでブロックしてアラートを発生させるか（**防御**モード）、またはアラートを発生させるのみにするか（**検出**モード）が決まります。

（注） 防御モードを選択する前に、多くの誤検出の原因となるルールを特定できるように、ブロックルールのみにアラートを発生させることができます。

ステップ 5 [ベースポリシー（Base Policy）] を選択します。

システム提供のポリシーまたは既存のポリシーをベースポリシーとして使用できます。

ステップ 6 [保存（Save）] をクリックします。

新しいポリシーにはベースポリシーと同じ設定項目が含まれています。

次のタスク

ポリシーをカスタマイズするには、Snort 3 侵入ポリシーの編集 （37 ページ）を参照してください。

Snort 3 侵入ポリシーの編集

Snort 3 ポリシーを編集している間、すべての変更は即座に保存されます。変更を保存するための追加のアクションは必要ありません。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 [侵入ポリシー（Intrusion Policies）] タブが選択されていることを確認します。

ステップ 3 設定する侵入ポリシーの横にある [Snort 3バージョン（Snort 3 Version）] をクリックします。

ステップ 4 ポリシーを編集します。

- モードの変更：検査モードを変更するには、[モード（Mode）] ドロップダウンをクリックします。

注意 検査モードは、Snort 3 バージョンのポリシーでのみ変更されます。既存の検査モードは Snort 2 バージョンでそのまま保持されます。つまり、Snort 2 バージョンと Snort 3 バージョンのポリシーの検査モードは異なることになります。そのため、このオプションは注意して使用することを推奨します。

- [防御（Prevention）]：トリガーされたブロックルールはイベント（アラート）を作成し、接続をドロップします。
- [検出（Detection）]：トリガーされたブロックルールはアラートを生成します。

  防御モードに入る前に、検出モードを選択できます。たとえば、防御モードを選択する前に、多くの誤検出の原因となるルールを特定できるように、ブロックルールでアラートのみを生成することができます。

ステップ 5 侵入ポリシーのデフォルト設定を定義する [ベースポリシー（Base Policy）] レイヤをクリックします。

- 検索ルール：検索フィールドを使用して表示をフィルタ処理します。GID、SID、ルールメッセージ、または参照情報を入力できます。たとえば、GID:1; SID:9621 は ルール 1:962 のみを表示し 、SID:9621,9622,9623 は異なる SID を持つ複数のルールを表示します。[検索（Search）] テキストボックス内をクリックして、次のオプションのいずれかを選択することもできます。
  - フィルタ [アクション＝アラート（Action＝Alert）] または [アクション：ブロック（Action: Block）] を適用する
  - [無効なルール（Disabled Rules）] フィルタを適用する
  - [カスタム/ユーザ定義ルール（Custom/User Defined Rules）] を表示する
  - GID、SID、または GID:SID でフィルタ処理する
  - CVE でフィルタ処理する
  - コメントでフィルタ処理する
- フィルタ処理されたルールの表示：[プリセット（Presets）]のいずれかをクリックすると、アラート、ブロック、無効などに設定されているルールが表示されます。

  オーバーライドされたルールは、ルールアクションがデフォルトアクションから別のアクションに変更されたルールを示します。変更すると、元のデフォルトアクションに戻す場合でも、ルールアクションのステータスは [オーバーライド済み（Overridden）] になります。ただし、[ルールアクション（Rule

Action）] ドロップダウンリストから [デフォルトに戻す（Revert to default）] を選択すると、[オーバーライド済み（Overridden）] ステータスが削除されます。

[高度なフィルタ（Advanced Filters）] は、Lightweight Security Package（LSP）のリリース、侵入の分類、および Microsoft の脆弱性に基づくフィルタオプションを提供します。

- ルールドキュメントの表示：ルールの Talos マニュアルを表示するには、ルール ID または [ルールマニュアル（Rule Documentation）] アイコンをクリックします。
- ルールの詳細の表示：ルールの詳細を表示するには、ルール行の **展開矢印**（[展開矢印（expand arrow）] アイコン [展開矢印（expand arrow）] アイコン） アイコンをクリックします。
- ルールコメントの追加：ルールに関するコメントを追加するには、[コメント（Comments）] 列の下にある **[コメント（Comment）]**（）をクリックします。

ステップ 6 グループのオーバーライド：ルールグループのすべてのルールカテゴリが一覧表示される [グループのオーバーライド（Group Overrides）] レイヤをクリックします。Description、Overrides、Enabled Groups などを含むトップレベルの親ルールグループが表示されます。親ルールグループは更新できず、読み取り専用です。リーフルールグループのみを更新できます。各ルールグループで、最後のリーフグループまでトラバースできます。各グループ全体で、ルールグループを上書き、包含、および除外できます。リーフルールグループでは、次のことができます。

- ルールグループの検索：検索フィールドを使用してキーワードを入力し、ルールグループを検索します。
- 左側のパネルで、ルールグループを検索するためのプリセットフィルタオプションのいずれかを選択できます。
  - [すべて（All）]：すべてのルールグループを表示します。
  - [除外（Excluded）]：除外されたグループを表示します。
  - [含む（Included）]：含まれているグループを表示します。
  - [オーバーライド（Overridden）]：設定がオーバーライドされたルールグループを表示します。
- ルールグループのセキュリティレベルの設定：左側のペインで必要なルールグループに移動し、クリックします。システム定義のルール設定に基づいてセキュリティレベルを引き上げるか、または引き下げるには、ルールグループの [セキュリティレベル（Security Level）] の横にある [編集（Edit）] をクリックします。

  [セキュリティレベルの編集（Edit Security Level）] ダイアログボックスには、[デフォルトに戻す（Revert to Default）] をクリックするオプションがあります。これにより、行った変更が元に戻ります。

  Management Center は、設定されたセキュリティレベルのルールグループのルールアクションを自動的に変更します。[ルールのオーバーライド（Rule Overrides）] レイヤで、セキュリティレベルを変更するたびに、[事前設定（Presets）] の [ブロックルール（Block Rules）] と [無効ルール（Disabled Rules）] の数に注意してください。
- セキュリティレベルを一括変更して、特定のルールカテゴリ内のすべてのルールグループのセキュリティレベルを変更できます。セキュリティレベルの一括変更は、複数のルールグループを含むルール

グループに適用されます。ルールグループの一括更新後も、その中の関連するルールグループのセキュリティレベルを更新できます。

ルールグループ内で[混在（mixed）]セキュリティレベルとすることができます。[混在（mixed）]は、子グループに親ルールグループ内のセキュリティレベルが混在していることを示します。

- ルールグループを含めるまたは除外する：表示されるルールグループは、システムによって提供される基本の侵入ポリシーに関連付けられているデフォルトのルールグループです。侵入ポリシーにルールグループを含めたり、除外したりできます。除外されたルールグループは侵入ポリシーから削除され、そのルールはトラフィックに適用されません。Management Center にカスタムルールをアップロードする方法については、ルールグループへのカスタムルールの追加 （65 ページ）を参照してください。

  ルールグループを除外するには、次の手順を実行します。

  1. [ルールグループ（Rule Groups）] ペインに移動し、除外するルールグループを選択します。
  2. 右側のペインで [除外（Exclude）] ハイパーリンクをクリックします。
  3. [除外（Exclude）] をクリックします。

  アップロードされたカスタムルールまたは以前に除外されたルールグループを使用して 1 つまたは複数の新しいルールグループを含めるには、次の手順を実行します。

  1. ルール グループ フィルタ ドロップダウン リストの横にある **Add** ( ) をクリックします。
  2. ルールグループの横にあるチェックボックスをオンにして、追加するグループをすべて選択します。
  3. [保存（Save）] をクリックします。

- リーフルールグループの場合、[オーバーライド（Override）]列ヘッダーの下にあるアイコンをクリックして、ルールアクションの証跡を表示します。これは、侵入ルールのベースポリシーおよびグループのオーバーライドのために割り当てることができる、オーバーライドされたルールアクションのシーケンスを示しています。ルールアクションは、ベースポリシー構成またはユーザーグループのオーバーライドから取得できます。ユーザーグループのオーバーライドは、この 2 つの間の優先順位を取得します。優先順位は、ルールグループに割り当てられた、オーバーライドされた最終的なアクションを参照します。

- [ルールカウント（Rule Count）]列ヘッダーの下にあるルールカウント（数）をクリックして、ルールグループの一部であるルールの概要を表示します。

ステップ 7 **推奨事項**：シスコが推奨するルールを生成して適用する場合は、[推奨事項（Recommendations）] レイヤをクリックします。推奨事項は、ホストのデータベースを使用して、既知の脆弱性に基づいてルールを有効または無効にします。

ステップ 8 **ルールのオーバーライド**：[ルールのオーバーライド（Rule Overrides）] レイヤをクリックして、アラート、ブロック、無効、オーバーライド済み、書き換え、パス、ドロップ、または拒否に設定されているルールを表示する、いずれかのプリセットを選択します。

- [設定者（Set By）] 列には、状態（ベースポリシー）ごとのデフォルトのセット、またはグループのオーバーライド、ルールのオーバーライド、または推奨事項ごとに変更されたルールの状態が表示されます。[すべてのルール（All Rules）]（左ペイン）の [設定者（Set By）] 列には、優先順位に基づいたルールアクションのオーバーライドアクションの証跡が表示されます。ルールアクションの優先順位は、[ルールのオーバーライド（Rule Override）]>[推奨事項（Recommendations）]>[グループのオーバーライド（Group Override）]>[ベースポリシー（Base Policy）] です。
- [ルールアクション（Rule Action）] の変更：ルールアクションを変更するには、次のいずれかを選択します。
  - 一括編集：1つまたは複数のルールを選択し、[ルールアクション（Rule Action）] ドロップダウンリストから必要なアクションを選択し、[保存（Save）] をクリックします。

    （注） ルールアクションの一括変更は、最初の 500 個のルールでのみサポートされます。

  - 単一ルールの編集：[ルールアクション（Rule Action）] 列のドロップダウンリストからルールアクションを選択します。

ルールアクションは次のとおりです。

- [ブロック（Block）]：イベントを生成し、現在の一致するパケットと、この接続内の後続のすべてのパケットをブロックします。
- [アラート（Alert）]：一致するパケットのイベントのみを生成し、パケットまたは接続をドロップしません。
- [無効（Disabled）]：このルールと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。
- [デフォルトに戻す（Revert to default）]：システムのデフォルトアクションに戻します。
- [成功（Pass）]：イベントは生成されず、後続の Snort ルールによる以降の評価なしでパケットが通過できます。

  （注） [成功（Pass）]アクションは、カスタムルールでのみ使用でき、システム提供のルールでは使用できません。

- [ドロップ（Drop）]：イベントを生成し、一致するパケットをドロップし、この接続でそれ以上のトラフィックをブロックしません。
- [拒否（Reject）]：イベントを生成し、一致するパケットをドロップし、この接続で後続のトラフィックをブロックして、TCP プロトコルの場合は TCP リセットを送信元および接続ホストに送信します。

  クライアントまたはサーバーに関連するさまざまなファイアウォールモードおよびIPアドレスまたは送信元または宛先での拒否の動作：Snort は、ルーティングされた、インライン、およびブリッジされたインターフェイスの場合、クライアントとサーバーの両方に RST パケットを送信します。Snort は 2 つの RST パケットを送信します。クライアント方向の RST パケットでは、送信元がサーバーの IP に設定され、宛先がクライアントの IP に設定されます。サーバー方向の RST パケットでは、送信元がクライアントの IP に設定され、宛先がサーバーの IP に設定されます。

- [書き換え（Rewrite）]：ルールの置き換え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。

IPS ルールアクションのロギングについては、「ルールアクションのロギング （43 ページ）」を参照してください。

[対応（React）] ルールがある場合は、アラートアクションに変換されます。

ステップ 9 ポリシーに対する現在の変更の全体像を表示するには、[概要（Summary）] レイヤをクリックします。[ポリシーの概要（policy summary）] ページには次の情報が表示されます。

- ポリシーのルール分布、つまり、アクティブなルール、無効なルールなど。
- ポリシーをエクスポートし、侵入ポリシーのレポートを生成するオプション。
- ベースポリシーの詳細。
- 推奨事項を生成するオプション。
- オーバーライドしたグループのリストを表示するグループオーバーライド。
- オーバーライドしたルールのリストを表示するルールオーバーライド。
- [概要（Summary）] レイヤで、[?] アイコンをクリックして、Snort レイヤリングの概念を説明する Snort ヘルパーガイドのポップアップウィンドウを開きます。

ベースポリシーを変更するには、侵入ポリシーのベースポリシーの変更 （44 ページ）を参照してください。

（注） **[オブジェクト（Objects）]** > **[侵入ルール（Intrusion Rules）]** に移動し、[Snort 3 すべてのルール（Snort 3 All Rules）] タブをクリックして、すべての侵入ルールグループをトラバースできます。親ルールグループには、関連する子グループとルール数がリストされます。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

ルールグループのレポート

ルールグループは、生成された侵入イベントに反映され、MITRE の戦術と手法も呼び出されます。MITRE の戦術と手法の列と、侵入イベントの非 MITRE ルールグループの列があります。侵入イベントにアクセスするには、Management Center で **[分析（Analysis）]** > **[侵入（Intrusion）]** > **[イベント（Events）]** に移動し、[イベントのテーブルビュー（Table View of Events）] タブをクリックします。[統合されたイベント（Unified Events）] ビューアに侵入イベントフィールドを表示することもできます。[分析（Analysis）] タブで、[統合されたイベント（Unified Events）] をクリックします。

[侵入イベント（Intrusion Events）] ページに、ルールグループのレポート用に次のフィールドが追加されます。以下の列を明示的に有効にする必要があることに注意してください。

- MITRE ATT&CK
- ルールグループ

これらのフィールドの詳細については、『Cisco Secure Firewall Management Center Administration Guide, 7.3』の「Intrusion Event Fields」セクションを参照してください。

ルールアクションのロギング

Management Center 7.2.0 以降、[侵入イベント（Intrusion Events）] ページの [インライン結果（Inline Result）] 列のイベントには、ルールに適用された IPS アクションと同じ名前が表示されるため、ルールに一致するトラフィックに適用されたアクションを確認できます。

IPS アクションについて、次の表に、[侵入イベント（Intrusion Events）] ページの [インライン結果（Inline Result）] 列と、[統合されたイベント（Unified Events）] ページの [侵入イベントタイプ（Intrusion Event Type）] の [アクション（Action）] 列に表示されるイベントを示します。

IPS アクション（Snort 3）	**インライン結果 - Management Center 7.1.0 以前**	**インライン結果 - Management Center 7.2.0 以降**
アラート（Alert）	成功（Pass）	アラート（Alert）
ブロック（Block）	Dropped/Would Have Dropped/Partially Dropped	Block/Would Block/Partial Block
削除（Drop）	Dropped/Would have dropped	Drop/Would drop
拒否（Reject）	Dropped/Would have dropped	Reject/Would reject
書き換え（Rewrite）	許可（Allow）	書き換え（Rewrite）

重要

- [置換（Replace）] オプションのないルールの場合、**書き換え**アクションは**「Would Rewrite」**と表示されます。
- また、[置換（Replace）] オプションが指定されているが、IPS ポリシーが検出モードであるか、デバイスがインライン TAP/パッシブモードである場合に、**書き換え**アクションは**「Would Rewrite」**と表示されます。

（注） 後方互換性の場合（Management Center 7.2.0 が Threat Defense 7.1.0 デバイスを管理している）、言及されているイベントは、[成功（Pass）] がイベントの [アラート（Alert）] として表示されるアラート IPS アクションにのみ適用されます。他のすべてのアクションについては、Management Center 7.1.0 のイベントが適用されます。

侵入ポリシーのベースポリシーの変更

別のシステム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

最大 5 つのカスタム ポリシーをチェーンすることができます。5 つのうちの 4 つのポリシーで事前に作成されたポリシーが基本ポリシーとして使用され、5つ目のポリシーでシステムによって提供されたポリシーをベースとして使用する必要があります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 設定する侵入ポリシーの横にある **[編集（Edit）]**（  ）をクリックします。

ステップ 3 [ベースポリシー（Base Policy）] ドロップダウンリストからポリシーを選択します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

侵入ポリシーの管理

[侵入ポリシー（Intrusion Policy）] ページ（**[ポリシー（Policies）]** > **[侵入（Intrusion）]**）では、現在のカスタム侵入ポリシーとともに次の情報を表示できます。

- トラフィックの検査に侵入ポリシーを使用しているアクセス コントロール ポリシーとデバイスの数
- マルチドメイン展開では、ポリシーが作成されたドメイン

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。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 侵入ポリシーを管理します。

- 作成：[ポリシーの作成（Create Policy）] をクリックします。カスタム Snort 3 侵入ポリシーの作成（37 ページ）を参照してください。

- 削除：削除するポリシーの横にある をクリックします。別のユーザが保存していないポリシーの変更がある場合は、システムによって確認と通知のプロンプトが表示されます。[OK] をクリックして確認します。

  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。

- 侵入ポリシーの詳細の編集：編集するポリシーの横にある [編集（Edit）]（✎） をクリックします。侵入ポリシーの [名前（Name）]、[検査モード（Inspection Mode）]、および [ベースポリシー（Base Policy）] を編集できます。

- 侵入ポリシー設定の編集：[Snort 3 バージョン（Snort 3 Version）] をクリックします。Snort 3 侵入ポリシーの編集 （37 ページ）を参照してください。

- エクスポート：侵入ポリシーをエクスポートして別の Management Center にインポートする場合は、[エクスポート（Export）] をクリックします。最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Exporting Configurations*」トピックを参照してください。

- 展開：**[展開（Deploy）]** > **[展開（Deployment）]**を選択します。設定変更の展開 （30 ページ）を参照してください。

- レポート：[レポート（Report）] をクリックします。最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Generating Current Policy Reports*」トピックを参照してください。ポリシーバージョンごとに 1 つずつ、2 つのレポートを生成します。

侵入防御を実行するためのアクセスコントロールルール設定

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールを侵入ポリシーに関連付けることができます。侵入インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なる侵入インスペクションプロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セット使用します。セット内の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

ヒント システム提供の侵入ポリシーを使用する場合であっても、正確にネットワーク環境を反映するためにシステムの侵入変数を設定することを**強く**推奨します。少なくとも、デフォルトセットにあるデフォルトの変数を変更します。

システムによって提供される侵入ポリシーとカスタム侵入ポリシーについて

システムには複数の侵入ポリシーが付属しています。システムによって提供される侵入ポリシーを使用することで、Cisco Talos インテリジェンスグループ（Talos）の経験を活用できます。これらのポリシーでは、Talos は侵入ルールとプリプロセッサルールの状態を設定し、詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタムポリシーのベースとして使用できます。カスタムポリシーを作成すれば、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。

接続イベントおよび侵入イベントのロギング

アクセス制御ルールによって呼び出された侵入ポリシーが侵入を検出すると、侵入イベントを生成し、そのイベントを Management Center に保存します。また、システムはアクセス制御ルールのロギング設定に関係なく、侵入が発生した接続の終了も Management Center データベースに自動的にロギングします。

アクセス コントロール ルール設定と侵入ポリシー

1 つのアクセス コントロール ポリシーで使用可能な一意の侵入ポリシーの数は、ターゲットデバイスのモデルによって異なります。より強力なデバイスは、より多数のポリシーを処理できます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。異なる侵入ポリシーと変数セットのペアをそれぞれの許可ルールおよびインタラクティブ ブロック ルール（およびデフォルト アクション）と関連付けることができますが、ターゲットデバイスが設定されたとおりに検査を実行するのに必要なリソースが不足している場合は、アクセス コントロール ポリシーを展開できません。

侵入防御を実行するアクセスコントロールルールの設定

このタスクを実行するには、管理者、アクセス管理者、またはネットワーク管理者である必要があります。

手順

ステップ 1 アクセス コントロール ポリシー エディタで新しいルールを作成するか、既存のルールを編集します。最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Access Control Rule Components*」を参照してください。

ステップ 2 ルール アクションが [許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定されていることを確認します。

ステップ 3 [検査（Inspection）] をクリックします。

ステップ 4 システムによって提供される侵入ポリシーまたはカスタムの侵入ポリシーを選択するか、あるいはアクセス コントロール ルールに一致するトラフィックに対する侵入検査を無効にするには [なし（None）] を選択します。

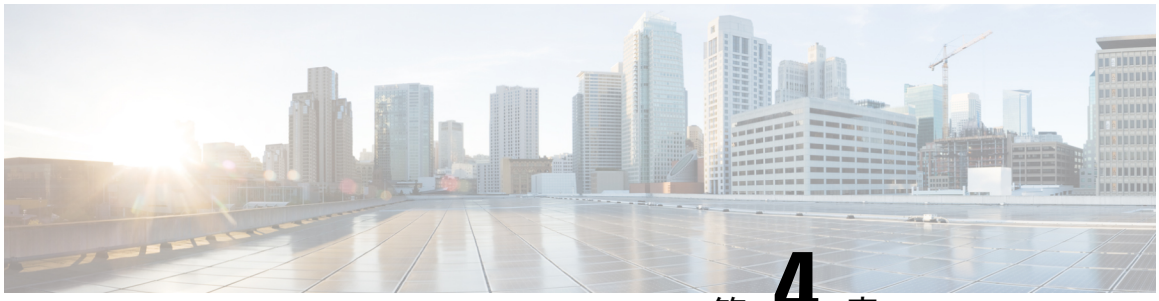
ステップ 5 侵入ポリシーに関連付けられた変数セットを変更するには、[変数セット（Variable Set）] ドロップダウンリストから値を選択します。

ステップ 6 [保存（Save）] をクリックしてルールを保存します。

ステップ 7 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。



第 4 章

ルールを使用した侵入ポリシーの調整

この章では Short 3 のカスタムルール、侵入ルールアクション、侵入ポリシー内の侵入イベント通知のフィルタ、Snort 2 カスタムルールの Snort 3 への変換、およびカスタムルールのあるルールグループの侵入ポリシーへの追加について説明します。

- 侵入ルールの調整の概要 （49 ページ）
- 侵入ルールのタイプ （50 ページ）
- ネットワーク分析と侵入ポリシーの前提条件 （51 ページ）
- Snort 3 のカスタムルール （51 ページ）
- 侵入ポリシーの Snort 3 侵入ルールの表示 （54 ページ）
- 侵入ルールアクション （55 ページ）
- 侵入ポリシーの侵入イベント通知フィルタ （56 ページ）
- 侵入ルールのコメントの追加 （62 ページ）
- Snort 2 カスタムルールの Snort 3 への変換 （63 ページ）
- ルールグループへのカスタムルールの追加 （65 ページ）
- カスタムルールを含むルールグループの侵入ポリシーへの追加 （66 ページ）
- Snort 3 でのカスタムルールの管理 （67 ページ）
- カスタムルールの削除 （68 ページ）
- ルールグループの削除 （69 ページ）

侵入ルールの調整の概要

共有オブジェクトルール、標準テキストルール、およびインスペクタルールにはルールの状態などを設定できます。

ルールを有効にするには、ルールの状態を [アラート（Alert）] または [ブロック（Block）] に設定します。ルールを有効にすると、システムがそのルールと一致するトラフィックに対するイベントを生成します。ルールを無効にすると、ルールの処理が停止されます。また、[ブロック（Block）]に設定したルールが一致するトラフィック上でイベントを生成したり、ドロップするように侵入ポリシーを設定することもできます。

ルールのサブセットを表示するようにルールをフィルタ処理することによって、ルール状態やルール設定を変更するルールのセットを正確に選択できます。

侵入ルールまたはルールの引数がインスペクタの無効化を必要とする場合、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が無効のままになりますが、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。

侵入ルールのタイプ

侵入ルールとは、ネットワーク内の脆弱性を不正利用する試みを検出するためにシステムが使用する、指定されたキーワードと引数のセットのことです。システムはネットワークトラフィックを分析する際に、パケットを各ルールに指定された条件に照らし合わせ、データパケットがルールに指定されたすべての条件を満たす場合、そのルールをトリガーします。

侵入ポリシーには以下の構成要素があります。

- 侵入ルール。共有オブジェクト ルールと標準テキスト ルールに分割されます。
- インスペクタルール。パケットデコーダの検出オプション、またはシステムに付属のインスペクタの 1 つに関連付けられます

次の表に、以上のルール タイプの属性を要約します。

表 *2:* 侵入ルールのタイプ

タイプ	ジェネレータ ID（GID）	Snort ID（SID）	ソース	コピーの可否	編集の可否
共有オブジェクトルール	3	1000000 未満	Cisco Talos Intelligence Group（Talos）	はい	制限付き
標準テキストルール	1（グローバル ドメインまたはレガシー GID）	1000000 未満	Talos	はい	制限付き
	1000～2000（子孫ドメイン）	1000000 以上	ユーザが作成またはインポート	はい	はい
プリプロセッサルール	デコーダまたはプリプロセッサに固有	1000000 未満	Talos	いいえ	いいえ
		1000000 以上	オプション設定時にシステムにより生成	いいえ	いいえ

Talos によって作成されたルールへの変更は保存できませんが、変更したルールのコピーをカスタムルールとして保存することはできます。ルールで使用される変数またはルールヘッダー情報（送信元と宛先のポートやIPアドレスなど）を変更できます。マルチドメイン展開では、

Talosによって作成されるルールはグローバルドメインに属します。子孫ドメインの管理者は、ルールのローカル コピーを保存してから、ルールを編集できます。

Talos によって作成されるルールには、各デフォルト侵入ポリシー内でデフォルトのルール状態が割り当てられます。ほとんどのプリプロセッサ ルールがデフォルトで無効になっているため、システムにプリプロセッサ ルールに対するイベントの生成とインライン展開での違反パケットの破棄を行わせる場合は、これらのルールを有効にする必要があります。

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 のカスタムルール

カスタム侵入ポリシーは、ローカルルールファイルをインポートすることによって作成できます。ルールファイルの拡張子は、`.txt` または `.rules` です。作成方法に関わらず、システムはカスタム ルールをローカル ルールに分類して保存します。カスタムルールはルールグループに属している必要があります。ただし、カスタムルールは複数のグループの一部になることもできます。

カスタム侵入ルールを作成すると、システムは一意のルール番号（番号の形式は`GID:SID:Rev`）を割り当てます。この番号には次の要素が含まれます。

- **GID**：ジェネレータ ID。カスタムルールの場合、GIDを指定する必要はありません。システムは、ルールのアップロード中にグローバルドメインまたはサブドメインのどちらにいるかに基づいて GID を自動的に生成します。標準テキスト ルールでは、グローバルドメインの値は 2000 です。
- **SID**：Snort ID。ルールがシステム ルールのローカル ルールであるかどうかを示します。新しいルールを作成する場合は、一意の SID をルールに割り当てます。

  ローカル ルールの SID 番号は 1000000 から始まり、新しいローカル ルールにつき番号が 1 ずつ増えます。
- **Rev**：リビジョン番号。新しいルールのリビジョン番号は 1 です。カスタムルールを変更するたびに、リビジョン番号は 1 ずつ増える必要があります。

カスタム標準テキスト ルールでは、ルール ヘッダー設定、ルール キーワード、およびルール引数を設定できます。特定のプロトコルを使用する、特定の IP アドレスまたはポートを行き来するトラフィックだけをルールで照合するよう、ルール ヘッダーを設定できます。

（注）

- Snort 3 カスタムルールは編集できません。カスタムルールのルールテキスト内に `classtype` の有効な分類メッセージが含まれていることを確認します。分類または誤分類なしでルールをインポートする場合は、ルールを削除してから再作成します。
- Snort 3 を使用してカスタム侵入ルールを作成できます。ただし、カスタム侵入ルールの調整と障害対応のサポートは現在利用できません。

Snort 3 の機密データの検出

社会保障番号、クレジットカード番号、E メールなどの機密データは、インターネットに意図的に、または誤って漏洩される可能性があります。機密データの検出は、機密データの漏洩の可能性を検出してイベントを生成するために使用されます。イベントは、大量の個人識別情報（PII）データが転送された場合にのみ生成されます。機密データの検出ではイベントの出力で PII をマスクできます。

sd_pattern オプション

PII を検出してフィルタリングするには、`sd_pattern` IPS オプションを使用します。この情報には、クレジットカード番号、米国社会保障番号、電話番号、電子メールアドレスが含まれます。独自の PII を定義するために、正規表現（regex）構文を使用できます。

sd_pattern オプションには、次の設定があります。

- [パターン（Pattern）]：PDU で検索する正規表現を指定する暗黙の必須設定。正規表現は、PCRE 構文で記述する必要があります。
- [しきい値（Threshold）]：イベントの生成に必要な PDU 内の一致数を指定する明示的なオプション設定。

  IPS ルールオプションとしての `sd_pattern` は、追加のインスペクタの要件なしで Snort で使用できます。ルールオプションの構文は次のとおりです。

  ```
  sd_pattern: "<pattern>"[, threshold <count>];
  ```

  次に例を示します。

  ```
  sd_pattern:"credit_card", threshold 2;
  ```

組み込みパターン

機密データには 5 つの組み込みパターンがあります。「パターン」設定で組み込みパターンを使用するには、照合する必要がある PII タイプの名前を指定する必要があり、必要な正規表現で置き換えられます。PII 名と正規表現のマッピングまたはパターンは次のとおりです。

- credit_card：

  ```
  \d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}
  ```

- us_ Social：

  ```
  [0-8]\d{2}-\d{2}-\d{4}
  ```

- us_social_nodashes：

```
[0-8]\d{8}
```

- Email：

```
[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+(?:\.[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+)*@(?:[a-zA-Z0-9]
(?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?
```

- us_phone：

```
(?:\+?1[-\.\s]?)?\(?([2-9][0-8]\d)\)?[-\.\s]([2-9]\d{2})[-\.\s](\d{4})
```

PII 名	パターン
credit_card	`\d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}`
us_social	`[0-8]\d{2}-\d{2}-\d{4}`
us_social_nodashes	`[0-8]\d{8}`
email	`[a-zA-Z0-9!#$%&'*+\/=?^_`{\|}~-]+(?:\.[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+)*@(?:[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?`
us_phone	`(?:\+?1[-\.\s]?)?\(?([2-9][0-8]\d)\)?[-\.\s]([2-9]\d{2})[-\.\s](\d{4})`

これらのパターンに一致するデータのマスキングは、クレジットカード、米国社会保障番号、電子メール、および米国の電話番号のシステム提供ルールまたは組み込みパターンでのみ機能します。マスキングは、カスタムルールまたはユーザー定義の PII パターンでは機能しません。ルールは、機密データ用の Lightweight Security Package（LSP）gid:13 で使用できます。デフォルトでは、システム提供のポリシーでは有効になっていません。

LSP の機密データルールは、すべての組み込みパターンを対象とし、次のしきい値があります。

- credit_card：2
- us_ social：2
- us_ social_nodashes：20
- email：20
- us_phone：20

sd_pattern オプションを使用すると、カスタムルールを作成したり、既存のルールを変更できます。これを行う場合は、Snort 3 侵入ポリシーインターフェイスを使用します。

カスタムパターンとしきい値を使用した sd_pattern を含むルールの例：

alert tcp (sid: 1000000001; sd_pattern:"[\w-\.]+@([\w-]+\.)+[\w-]{2,4}",threshold 4; msg: "email, threshold 4")

例

機密データ検出を使用したカスタムルールの例：

組み込みパターンを使用したルール：

```
alert tcp (
        msg:"SENSITIVE-DATA Email";
        flow:only_stream;
        pkt_data;
        sd_pattern:"email", threshold 5;
        service:http, smtp, ftp-data, imap, pop3;
        gid:2000;
        sid:1000001;
)
```

カスタムパターンを使用したルール：

```
alert tcp (
        msg:"SENSITIVE-DATA US phone numbers";
        flow:only_stream;
        file_data;
       sd_pattern:"+?3?8?(0[\s\.-]\d{2}[\s\.-]\d{3}[\s\.-]\d{2}[\s\.-]\d{2})", threshold
 2;
        service:http, smtp, ftp-data, imap, pop3;
        gid:2000;
        sid:1000002;
)
```

次に、組み込み機密データパターンを使用した完全な Snort IPS ルールの例をいくつか示します。

- alert tcp (sid:1; msg:"Credit Card"; sd_pattern:"credit_card", threshold 2;)
- alert tcp (sid:2; msg:"US Social Number"; sd_pattern:"us_social", threshold 2;)
- alert tcp (sid:3; msg:"US Social Number No Dashes"; sd_pattern:"us_social_nodashes", threshold 2;)
- alert tcp (sid:4; msg:"US Phone Number"; sd_pattern:"us_phone", threshold 2;)
- alert tcp (sid:5; msg:"Email"; sd_pattern:"email", threshold 2;)

データマスキングの無効化は、Cisco Secure Firewall Management Center および Cisco Secure Firewall Device Manager ではサポートされていません。

侵入ポリシーの Snort 3 侵入ルールの表示

侵入ポリシー内のルールの表示方法を調整できます。特定のルールの詳細を表示して、ルール設定、ルール ドキュメント、およびその他のルール仕様を確認することもできます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 ポリシーの横にある [Snort 3 バージョン（Snort 3 Version）] をクリックします。

ステップ 3 ルールを表示している間、以下を実行できます。

- ルールをフィルタ処理します。

- ルールグループを選択すると、そのグループに関連するルールが表示されます。
- 侵入ルールの詳細を表示します。
- ルールのコメントを表示します。
- ルールのドキュメンテーションを表示します。

これらのタスクの実行の詳細については、「Snort 3 侵入ポリシーの編集 （37 ページ）」を参照してください。

侵入ルールアクション

侵入ルールアクションでは、個々の侵入ポリシー内のルールを有効または無効にできるだけでなく、モニター対象の条件がルールをトリガーした場合にシステムが実行するアクションを指定できます。

Cisco Talos Intelligence Group（Talos）が各デフォルトポリシーの侵入およびインスペクタルールごとにデフォルトアクションを設定します。たとえば、ルールを Security over Connectivity デフォルト ポリシーでは有効にして、Connectivity over Security デフォルト ポリシーでは無効にすることができます。Talos がルール更新を使用してデフォルトポリシー内の 1 つ以上のルールのデフォルトアクションを変更する場合もあります。ルール更新でのベースポリシーの更新を許可すると、ポリシーの作成時に使用されたデフォルトポリシー（または基礎となるデフォルトポリシー）のデフォルトアクションが変更されたときの、そのポリシー内のルールのデフォルトアクションの変更も許可することになります。ただし、ルールアクションを変更している場合は、ルール更新でその変更がオーバーライドされないことに注意してください。

侵入ルールを作成すると、そのルールは、ポリシーの作成時に使用されたデフォルトポリシー内のルールのデフォルトアクションを継承します。

侵入ルールアクションのオプション

侵入ポリシーでは、ルールのアクションを次の値に設定できます。

アラート（Alert）

システムで特定の侵入試行を検出して、一致したトラフィックが見つかった時点で侵入イベントを生成する場合。悪意のあるパケットがネットワークを通過してルールをトリガーすると、そのパケットが宛先に送信され、システムが侵入イベントを生成します。悪意のあるパケットはその対象に到達しますが、イベントロギングによって通知されます。

ブロック（Block）

システムで特定の侵入試行を検出して、その攻撃を含むパケットをドロップし、一致したトラフィックが見つかった時点で侵入イベントを生成する場合。悪意のあるパケットはその対象に到達せず、イベントロギングによって通知されます。

無効（Disable）

システムで一致するトラフィックを評価しない場合。

（注） [アラート（Alert）] または [ブロック（Block）] オプションを選択すると、ルールが有効になります。[無効（Disable）] を選択すると、ルールが無効になります。

侵入ポリシー内のすべての侵入ルールを有効にしないことを強く推奨します。すべてのルールが有効になっている場合は、管理対象デバイスのパフォーマンスが低下する可能性があります。代わりに、できるだけネットワーク環境に合わせてルール セットを調整してください。

侵入ルールアクションの設定

侵入ルールアクションはポリシーに固有です。

手順

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 編集するポリシーの横にある [Snort 3 バージョン（Snort 3 Version）] をクリックします。

ヒント このページには、次の合計数が表示されます。

- 無効なルール
- [アラート（Alert）] に設定された有効なルール
- [ブロック（Block）] に設定された有効なルール
- オーバーライドされたルール

ステップ 3 ルールアクションを設定する 1 つ以上のルールを選択します。

ステップ 4 [ルールアクション（Rule Action）] ドロップダウンリストからルールアクションのいずれかを選択します。さまざまなルールアクションの詳細については、「Snort 3 侵入ポリシーの編集 （37 ページ）」を参照してください。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

侵入ポリシーの侵入イベント通知フィルタ

侵入イベントの重要度は、発生頻度、送信元 IP アドレス、または宛先 IP アドレスに基づいて設定できます。イベントが特定の回数発生するまで注意が必要ない場合もあります。たとえば、何者かがサーバにログインしようとしても、特定の回数失敗するまで、気にする必要はあ

りません。一方、ほんの少数の発生を見れば、広範な問題があることを理解できる場合もあります。たとえば、Web サーバに対して DoS 攻撃が行われた場合は、少数の侵入イベントの発生を確認しただけで、その状況に対処しなければならないことが分かります。同じイベントが何百回も確認されれば、システムの機能が麻痺します。

侵入イベントしきい値

指定した期間内にイベントを生成する回数に基づいて、システムが侵入イベントをログに記録して表示する回数を制限するには、個別のルールのしきい値を設定します。これにより、大量の同じイベントが原因で機能が麻痺するのを避けることができます。共有オブジェクトルール、標準テキストルール、またはインスペクタルールごとにしきい値を設定できます。

侵入イベントしきい値の設定

しきい値を設定するには、最初にしきい値のタイプを指定します。

表 *3:* しきい値設定オプション

オプション	説明
制限（Limit）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [制限（Limit）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。
しきい値（Threshold）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [しきい値（Threshold）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[秒（Seconds）] と [カウント（Count）] のカウンタを 0 にリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。

オプション	説明
両方（Both）	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [両方（Both）] に、[カウント（Count）] を 2 に、[秒（Seconds）] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値が満たされる）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。

次に、トラッキングを指定します。これにより、イベントしきい値が送信元 IP アドレス単位と宛先 IP アドレス単位のどちらで計算されるかが決まります。

表 *4: IP* しきい値設定オプション

オプション	説明
ソース（Source）	送信元 IP アドレス単位でイベント インスタンス カウントを計算します。
接続先（Destination）	宛先 IP アドレス単位でイベント インスタンス カウントを計算します。

最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 *5:* インスタンス/時間のしきい値設定オプション

オプション	説明
カウント（Count）	しきい値を満たすために必要な、追跡する IP アドレス単位で指定された期間単位のイベントインスタンスの数。
秒（Seconds）	カウントがリセットされるまでの秒数。しきい値タイプを [制限（limit）] に、トラッキングを [送信元IP（Source IP）] に、[カウント（count）] を [10] に、[秒（seconds）] を [10] に設定した場合は、システムが指定された送信元ポートから 10 秒間に発生した最初の 10 のイベントを記録して表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

侵入イベントのしきい値設定は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベント抑制のいずれかと組み合わせて使用することもできます。

ヒント 侵入イベントのパケット ビューでしきい値を追加することもできます。

Snort 3 での侵入ルールのしきい値の設定

[ルールの詳細（Rule Detail）] ページで、ルールの単一のしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

手順

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 侵入ルールの [アラート設定（Alert Configuration）] 列で、[なし（None）] リンクをクリックします。

ステップ 4 **[編集（Edit）]**（  ）をクリックします。

ステップ 5 [アラート設定（Alert Configuration）] ウィンドウで、[しきい値（Threshold）] タブをクリックします。

ステップ 6 [タイプ（Type）] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベント インスタンス数に通知を制限する場合は、[制限（Limit）] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[しきい値（Threshold）] を選択します。
- 指定されたイベント インスタンス数に達した後で、期間あたり 1 回ずつ通知を提供する場合は、[両方（Both）] を選択します。

ステップ 7 [追跡対象（Track By）] フィールドで [送信元（Source）] または [宛先（Destination）] を選択し、イベントインスタンスの追跡を送信元 IP アドレスで行うか、宛先の IP アドレスで行うかを指定します。

ステップ 8 [カウント（Count）] フィールドに、しきい値として使用するイベントインスタンスの数を入力します。

ステップ 9 [秒数（Seconds）] フィールドに、イベントインスタンスを追跡する期間（秒数）を指定する数値を入力します。

ステップ 10 [保存（Save）] をクリックします。

追加のサポートと情報については、「Snort 3 の抑制としきい値」ビデオを参照してください。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

侵入イベントしきい値の表示と削除

ルールのしきい値の既存の設定を表示または削除するには、[ルールの詳細（Rules Details）] ビューを使用して、しきい値の構成済み設定を表示し、それらがシステムに適切かどうかを確認します。そうでない場合は、新しいしきい値を追加して既存の値を上書きすることができます。

手順

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 [アラート設定（Alert Configuration）] 列に表示されるしきい値が設定されているルールを選択します（[アラート設定（Alert Configuration）] 列には、ルールのリンクとして [しきい値（Threshold）] が表示されます）。

ステップ 4 ルールのしきい値を削除するには、[アラート設定（Alert Configuration）] 列の [しきい値（Threshold）] リンクをクリックします。

ステップ 5 [編集（Edit）]（ ） をクリックします。

ステップ 6 [しきい値（Threshold）] タブをクリックします。

ステップ 7 [リセット（Reset）] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

侵入ポリシー抑制の設定

特定の IP アドレスまたは IP アドレスの範囲でインスペクタの特定のルールをトリガーしたときの侵入イベント通知を抑制できます。これは、誤検出を回避するのに役立ちます。たとえば、特定のエクスプロイトのように見えるパケットを伝送しているメールサーバが存在する場合は、そのメールサーバによってトリガーとして使用されたイベントに関するイベント通知を抑制できます。ルールはすべてのパケットに対してトリガーとして使用されますが、本物の攻撃に対するイベントだけが表示されます。

侵入ポリシー抑制タイプ

侵入イベント抑制は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベントしきい値構成のいずれかと組み合わせて使用することもできることに注意してください。

ヒント　侵入イベントのパケット ビュー内から抑制を追加できます。侵入ルールエディタページ（**[オブジェクト（Objects）]** > **[侵入ルール（Intrusion Rules）]** > **[Snort 3 のすべてのルール（Snort 3 All Rules）]**）の [アラート設定（Alert Configuration）] 列を使用して、抑制設定にアクセスすることもできます

Snort 3 での侵入ポリシーの抑制の設定

侵入ポリシーのルールに対して 1 つ以上の抑制を設定できます。

始める前に

送信元または宛先の抑制に追加する必要があるネットワークオブジェクトを作成していることを確認します。

手順

ステップ 1　**[オブジェクト（Objects）]** > **[侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2　[Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3　侵入ルールの [アラート設定（Alert Configuration）] 列の [なし（None）] リンクをクリックします。

ステップ 4　**[編集（Edit）]**（）をクリックします。

ステップ 5　[抑制（Suppressions）] タブで、次のオプションの横にある追加アイコン（+）をクリックします。

- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元ネットワーク（Source Networks）] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先ネットワーク（Destination Networks）] を選択します。

ステップ 6　[ネットワーク（Network）] ドロップダウンリストからプリセットネットワークを選択します。

ステップ 7　[保存（Save）] をクリックします。

ステップ 8　（任意）必要に応じて、最後の 3 つの手順を繰り返します。

ステップ 9　[アラート設定（Alert Configuration）] ウィンドウで [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

抑制条件の表示と削除

既存の抑制条件を表示または削除することもできます。たとえば、メールサーバがエクスプロイトのように見えるパケットを普段から送信しているという理由で、そのメール サーバの IP

アドレスから送信されたパケットに関するイベント通知を抑制できます。その後、そのメールサーバが使用停止になり、その IP アドレスが別のホストに再割り当てされたら、その送信元 IP アドレスの抑制条件を削除する必要があります。

手順

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。
ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。
ステップ 3 抑制を表示または削除するルールを選択します。
ステップ 4 [アラート設定（Alert Configuration）] 列の [抑制（Suppression）] をクリックします。
ステップ 5 [編集（Edit）]（） をクリックします。
ステップ 6 [抑制（Suppressions）] タブをクリックします。
ステップ 7 抑制の横にある [クリア（Clear）]（）をクリックして、抑制を削除します。
ステップ 8 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

侵入ルールのコメントの追加

侵入ポリシーのルールにコメントを追加できます。このようにして追加されたコメントはポリシー専用のコメントとなります。よって、ある侵入ポリシーのルールに追加したコメントは、他の侵入ポリシーでは表示されません。

手順

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。
ステップ 2 編集するポリシーの横にある [Snort 3 バージョン（Snort 3 Version）] をクリックします。
ステップ 3 すべてのルールがリストされているページの右側で、コメントを追加するルールを選択します。
ステップ 4 [コメント（Comments）]列の下にある **コメント**（[コメント（comment）]アイコン[コメント（comment）]アイコン） をクリックします。
ステップ 5 [コメント（Comments）] フィールドに、ルールコメントを入力します。
ステップ 6 [コメントを追加（Add a Comment）] をクリックします。
ステップ 7 [保存（Save）] をクリックします。

ヒント　[コメント（Comments）]列のルールの横に[コメント（Comment）]（）が表示されます。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

Snort 2 カスタムルールの Snort 3 への変換

カスタムルールを使用している場合は、Snort 2 から Snort 3 に変換する前に、Snort 3 のルールセットを管理する準備ができていることを確認してください。サードパーティベンダーのルールセットを使用している場合は、そのベンダーに連絡して、そのルールが Snort 3 に正常に変換されることを確認するか、または Snort 3 用にネイティブに作成された置換ルールセットを取得します。独自に作成したカスタムルールがある場合は、変換前に Snort 3 ルールの作成に慣れておくと、変換後の Snort 3 検出を最適化するようにルールを更新できます。Snort 3 でのルールの作成の詳細については、次のリンクを参照してください。

- https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html
- https://blog.snort.org/2020/10/talos-transition-to-snort-3.html

Snort 3 ルールの詳細については、https://blog.snort.org/ にある他のブログを参照してください。

システム付属のツールを使用して Snort 2 ルールを Snort 3 ルールに変換するには、Snort 2 カスタムルールの Snort 3 への変換 （63 ページ）を参照してください。

重要　Snort 2 ネットワーク分析ポリシー（NAP）の設定を Snort 3 に自動的にコピーすることはできません。NAP 設定は、Snort 3 で手動で複製する必要があります。

すべての侵入ポリシーのすべての Snort 2 カスタムルールの Snort 3 への変換

手順

ステップ 1　**[オブジェクト（Objects）]** > **[侵入ルール（Intrusion Rules）]** をクリックします。
ステップ 2　[Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。
ステップ 3　左側のペインで [すべてのルール（All Rules）] が選択されていることを確認します。
ステップ 4　[タスク（Tasks）] ドロップダウンリストから値を選択します。

- **[Snort 2ルールの変換とインポート（Convert Snort 2 rules and import）]**：すべての侵入ポリシーのすべての Snort 2 カスタムルールを Snort 3 に自動的に変換し、それらを Snort 3 カスタムルールとして Management Center にインポートします。
- **[Snort 2ルールの変換とダウンロード（Convert Snort 2 rules and download）]**：すべての侵入ポリシーのすべての Snort 2 カスタムルールを Snort 3 に自動的に変換し、それらをローカルシステムにダウンロードします。

ステップ 5 [OK] をクリックします。

（注）
- 前の手順で [変換してインポート（Convert and import）] を選択した場合は、変換されたすべてのルールが、[ローカルルール（Local Rules）] の下に新しく作成されたルールグループ [すべての Snort 2 をグローバルに変換（All Snort 2 Converted Global）] の下に保存されます。
- 前の手順で [変換してダウンロード（Convert and download）] を選択した場合は、ルールファイルをローカルに保存します。ダウンロードしたファイル内の変換済みのルールを確認します。後でルールグループへのカスタムルールの追加（65 ページ）の手順に従ってアップロードできます。

追加のサポートと情報については、「Snort 2 ルールの Snort 3 への変換」ビデオを参照してください。

次のタスク

設定変更を展開します。設定変更の展開（30 ページ）を参照してください。

単一の侵入ポリシーの Snort 2 カスタムルールの Snort 3 への変換

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 [侵入ポリシー（Intrusion Policies）] タブで、[Snort 3同期ステータスの表示（Show Snort 3 Sync status）] をクリックします。

ステップ 3 侵入ポリシーの [同期（Sync）] アイコン（ ）をクリックします。

（注） 侵入ポリシーの Snort 2 バージョンと Snort 3 バージョンが同期されている場合は、[同期（Sync）] アイコンが緑色の で表示されます。変換するカスタムルールがないことを示します。

ステップ 4 サマリーを読み、[カスタムルール（Custom Rules）] タブをクリックします。

ステップ 5 次のどちらかを選択します。

- [変換後のルールをこのポリシーにインポートする（Import converted rules to this policy）]：侵入ポリシーの Snort 2 カスタムルールを Snort 3 に変換し、Snort 3 カスタムルールとして Management Center にインポートします。
- [変換後のルールのダウンロード（Download converted rules）]：侵入ポリシーのSnort 2カスタムルールをSnort 3に変換し、ローカルシステムにダウンロードします。ダウンロードしたファイル内の変換後のルールを確認し、後でアップロードアイコンをクリックしてファイルをアップロードできます。

ステップ 6 [再同期（Re-Sync）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

ルールグループへのカスタムルールの追加

Management Center でカスタムルールをアップロードすると、ローカルで作成したカスタムルールがすべての Snort 3 ルールのリストに追加されます。

手順

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 [タスク（Tasks）] ドロップダウンリストをクリックします。

ステップ 4 [Snort 3ルールのアップロード（Upload Snort 3 Rules）] をクリックします。

ステップ 5 作成した Snort 3 カスタムルールを含む `.txt` または `.rules` ファイルをドラッグアンドドロップします。

ステップ 6 [OK] をクリックします。

（注） 選択したファイルにエラーがある場合、それ以上先に進むことはできません。エラーファイルをダウンロードし、エラーを修正した後に [ファイルの置換（Replace File）] リンクをクリックし、ファイルのバージョン 2 をアップロードできます。

ステップ 7 ルールをルールグループに関連付けて、そのグループに新しいルールを追加します。

新しいカスタムルールグループを作成し（[新しいカスタムルールグループの作成（Create New Custom Rule Group）] リンクをクリック）、新しいグループにルールを追加することもできます。

（注） 既存のローカルルールグループがない場合は、[新しいカスタムルールグループの作成（Create New Custom Rule Group）] をクリックして続行します。新しいルールグループの [名前（Name）] を入力して、[保存（Save）] をクリックします。

ステップ 8 次のいずれかを選択します。

- [ルールのマージ（Merge Rules）] は、追加する新しいルールをルールグループ内の既存のルールとマージします。
- [グループ内のすべてのルールをファイルの内容に置換（Replace all rules in the group with file contents）] は、既存のすべてのルールを追加する新しいルールに置換します。

（注） 前の手順で複数のルールグループを選択した場合は、使用できるオプションは[ルールのマージ（Merge Rules）] のみになります。

ステップ 9 [次へ（Next）] をクリックします。

サマリーを確認して、追加する新しいルール ID を確認し、必要に応じてダウンロードします。

ステップ 10 [終了（Finish）] をクリックします。

重要 アップロードされたすべてのルールのルールアクションは無効な状態になっています。ルールをアクティブにするために必要な状態に変更する必要があります。

次のタスク

- Management Center でカスタムルールをアップロードすると、作成したカスタムルールがすべての Snort 3 ルールのリストに追加されます。これらのカスタムルールをトラフィックに適用するには、必要な侵入ポリシーでこれらのルールを追加して有効にします。カスタムルールを含むルールグループを侵入ポリシーに追加する方法については、カスタムルールを含むルールグループの侵入ポリシーへの追加（66ページ）を参照してください。カスタムルールを有効にする方法については、Snort 3 でのカスタムルールの管理 （67ページ）を参照してください。
- 設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

カスタムルールを含むルールグループの侵入ポリシーへの追加

システムにアップロードされたカスタムルールを侵入ポリシーで有効にし、それらのルールをトラフィックに適用する必要があります。Management Center にカスタムルールをアップロードした後、侵入ポリシーに新しいカスタムルールを含むルールグループを追加します。

手順

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 [侵入ポリシー（Intrusion Policies）] タブで、侵入ポリシーの [Snort 3 バージョン（Snort 3 Version）] をクリックします。

ステップ 3 [ルールグループ（Rule Groups）] 検索バーの横にある [追加（Add）]（+）をクリックします。

ステップ 4 [ルールグループの追加（Add Rule Groups）] ウィンドウで、ルールグループの横にある [>] アイコンをクリックして、ローカルルールグループを展開します。

ステップ 5 アップロードしたカスタムルールグループの横にあるチェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

Snort 3 でのカスタムルールの管理

システムにアップロードしたカスタムルールを侵入ポリシーに追加し、それらのルールを有効にしてトラフィックに適用する必要があります。アップロードされたカスタムルールは、すべてのポリシーで有効にすることも、個々のポリシーで選択して有効にすることもできます。

次の手順に従って、1 つ以上の侵入ポリシーでカスタムルールを有効にします。

手順

ステップ 1 **[オブジェクト（Objects）]** > **[侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 [ローカルルール（Local Rules）] を展開します。

ステップ 4 必要なルールグループを選択します。

ステップ 5 ルールの横にあるチェックボックスをオンにしてルールを選択します。

ステップ 6 [ルールアクション（Rule Actions）] ドロップダウンリストから [侵入ポリシーごと（Per Intrusion Policy）] を選択します。

ステップ 7 次のどちらかを選択します。

- [すべてのポリシー（All Policies）]：追加するすべてのルールに対して同じルールアクションを設定します。
- [侵入ポリシーごと（Per Intrusion Policy）]：侵入ポリシーごとに異なるルールアクションを設定します。

ステップ 8 ルールアクションを次のように設定します。

- 前の手順で [すべてのポリシー（All Policies）] を選択した場合は、[オーバーライド状態の選択（Select Override state）] ドロップダウンリストから必要なルールアクションを選択します。

- 前の手順で [侵入ポリシーごと（Per Intrusion Policy）] を選択した場合は、ポリシー名に [ルールアクション（Rule Action）] を選択します。さらにポリシーを追加するには、[別のポリシーの追加（Add Another）] をクリックします。

ステップ 9 必要に応じて、[コメント（Comments）] テキストボックスにコメントを追加します。

ステップ 10 [保存（Save）] をクリックします。

次のタスク

デバイスに変更を展開します。設定変更の展開 （30 ページ）を参照してください。.

カスタムルールの削除

手順

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 左側のペインの [ローカルルール（Local Rules）] を展開します。

ステップ 4 削除するルールのチェックボックスをオンにします。

ステップ 5 選択したすべてのルールのルールアクションが [無効（Disable）] であることを確認します。

必要に応じて次の手順に従い、選択した複数のルールのルールアクションを無効にします。

a) [ルールアクション（Rule Actions）] ドロップダウンボックスから、[侵入ポリシーごと（Per Intrusion Policy）] を選択します。
b) [すべてのポリシー（All Policies）] オプションボタンを選択します。
c) [オーバーライド状態の選択（Select Override state）] ドロップダウンリストから [無効（Disable）] を選択します。
d) [保存（Save）] をクリックします。
e) 削除するルールのチェックボックスをオンにします。

ステップ 6 [ルールアクション（Rule Actions）] ドロップダウンリストから、[削除（Delete）] を選択します。

ステップ 7 [ルールの削除（Delete Rules）] ポップアップウィンドウで [削除（Delete）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

ルールグループの削除

始める前に

含めたすべての侵入ポリシーから削除するルールグループを除外します。侵入ポリシーからルールグループを除外する手順については、Snort 3 侵入ポリシーの編集 （37 ページ）を参照してください。

手順

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 左側のペインの [ローカルルール（Local Rules）] を展開します。

ステップ 4 削除するルールグループを選択します。

ステップ 5 続行する前に、グループ内のすべてのルールのルールアクションが [無効（Disable）] に設定されていることを確認します。

いずれかのルールのルールアクションが [無効（Disable）] 以外の場合、ルールグループは削除できません。必要に応じて、次の手順に従ってすべてのルールのルールアクションを無効にします。

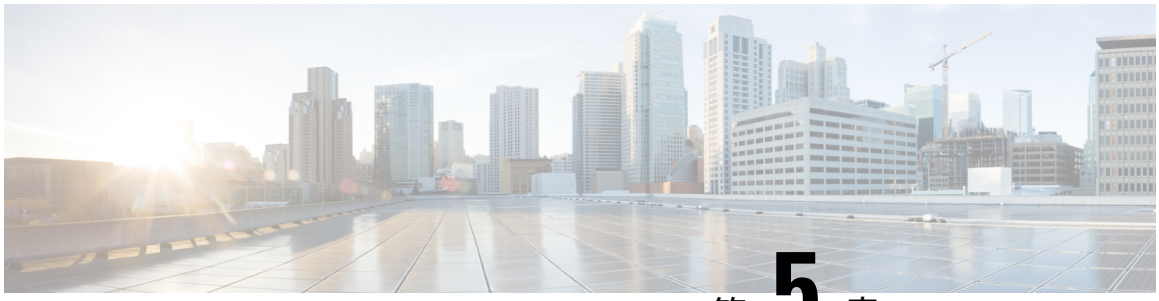
a) [ルールアクション（Rule Actions）] ドロップダウンリストの下にあるチェックボックスをオンにして、グループ内のすべてのルールを選択します。
b) [ルールアクション（Rule Actions）] ドロップダウンボックスから、[侵入ポリシーごと（Per Intrusion Policy）] を選択します。
c) [すべてのポリシー（All Policies）] オプションボタンを選択します。
d) [オーバーライド状態の選択（Select Override state）] ドロップダウンリストから [無効（Disable）] を選択します。
e) [保存（Save）] をクリックします。

ステップ 6 ルールグループの横にある **[削除（Delete）]**（  ）をクリックします。

ステップ 7 [ルールグループの削除（Delete Rule Group）] ポップアップウィンドウで [OK] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。



第 5 章

ネットワーク資産に応じた侵入防御の調整

この章では、Cisco Secure Firewall の推奨ルールと、Cisco Secure Firewall 推奨ルールの生成と適用について説明します。

- LSP 更新での Snort 3 ルールの変更 （71 ページ）
- Cisco Secure Firewall 推奨ルールの概要 （72 ページ）
- ネットワーク分析と侵入ポリシーの前提条件 （73 ページ）
- Snort 3 での新しい Cisco Secure Firewall 推奨事項の生成 （73 ページ）

LSP 更新での Snort 3 ルールの変更

通常の Snort 3 Lightweight Security Package（LSP）の更新中に、既存のシステム定義の侵入ルールが新しい侵入ルールに置き換えられることがあります。1 つのルールが複数のルールに置き換えられたり、または複数のルールが 1 つのルールに置き換えられたりする可能性があります。これは、結合または拡張されたルールに対してより適切な検出が可能な場合に発生します。管理を向上させるために、既存のシステム定義ルールの一部を LSP アップデートの一部として削除することもできます。

LSP 更新中にオーバーライドされたシステム定義ルールの変更に関する通知を受け取るには、[削除された Snort 3 ルールのユーザオーバーライドの保持（Retain user overrides for deleted Snort 3 rules）] チェックボックスがオンになっていることを確認します。

[削除された Snort 3 ルールのユーザオーバーライドの保持（Retain user overrides for deleted Snort 3 rules）] チェックボックスに移動するには、[**歯車**（Cog）]（⚙）をクリックして、**[設定（Configuration）] > [侵入ポリシー設定（Intrusion Policy Preferences）]** を選択します。

デフォルトでは、チェックボックスがオンになっています。このチェックボックスをオンにすると、LSP 更新の一部として追加される新しい置換ルールのルールオーバーライドが保持されます。通知は、[歯車（Cog）]（⚙）の横にある [通知（Notification）] アイコンの下にある [タスク（Task）] タブに表示されます。

Cisco Secure Firewall 推奨ルールの概要

侵入ルールの推奨事項を使用して、ネットワークで検出されたホストアセットに関連付けられている脆弱性を対象にすることができます。たとえば、オペレーティングシステム、サーバ、クライアント アプリケーション プロトコルなどです。これにより、モニタ対象のネットワークの特定ニーズに合わせて侵入ポリシーを調整できます。

システムは、侵入ポリシーごとに個別の推奨事項のセットを作成します。これにより、通常、標準テキストルールと共有オブジェクトルールのルール状態の変更が推奨されます。ただし、インスペクタやデコーダのルールの変更も推奨されています。

ルール状態の推奨事項を生成する場合は、デフォルト設定を使用するか、詳細設定を指定できます。詳細設定では次の操作が可能です。

- システムが脆弱性をモニタするネットワーク上のホストを再定義する。
- ルール オーバーヘッドに基づき、システムが推奨するルールに影響を与える。
- ルールを無効にする推奨事項を生成するかどうかを指定する。

推奨事項をすぐに使用するか、推奨事項（および影響を受けるルール）を確認してから受け入れることができます。

推奨ルール状態を使用することを選択すると、読み取り専用の Secure Firewall 推奨レイヤが侵入ポリシーに追加されますが、後で、推奨ルール状態を使用しないことを選択すると、そのレイヤが削除されます。

侵入ポリシーに最近保存された構成設定に基づいて自動的に推奨を生成するためのタスクをスケジュールできます。

システムは、次のような手動で設定されたルール状態を変更しません。

- 推奨を生成する前に指定したルールの状態を手動で設定すると、その後、システムはそのルールの状態を変更できなくなる。
- 推奨の生成後に指定したルールの状態を手動で設定すると、そのルールの推奨状態が上書きされる。

ヒント 侵入ポリシー レポートには、推奨状態と異なるルール状態を持つルールのリストを含めることができます。

推奨が絞り込まれた [ルール（Rules）] ページを表示している最中に、あるいは、ナビゲーション パネルまたは [ポリシー情報（Policy Information）] ページから [ルール（Rules）] ページに直接アクセスした後に、手動で、ルール状態を設定したり、ルールをソートしたり、[ルール（Rules）] ページで可能なその他の操作（ルールの抑制やルールしきい値の設定など）を実行することができます。

（注） Cisco Talos Intelligence Group（Talos）は、システムによって提供されるポリシーでの各ルールの適切な状態を決定します。システムによって提供されるポリシーをベースポリシーとして使用し、システムがルールを Cisco Secure Firewall の推奨ルール状態に設定できるようにすると、侵入ポリシーのルールは、ネットワークアセットに推奨された設定と一致します。

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 での新しい Cisco Secure Firewall 推奨事項の生成

侵入ポリシーの Cisco Secure Firewall 推奨事項を生成し、ここに記載されている手順に従って、推奨された新しいルール設定を Snort 3 に作成します。ルールのオーバーヘッドは、Snort 3 で選択したしきい値ポリシーに基づいて**セキュリティレベル**として解釈されます。推奨されるアクションが、選択したセキュリティレベルに基づいていて、それがベースポリシーよりも高い場合、推奨されるのはイベントの生成だけではありません。

Secure Firewall 推奨事項を設定する前に、以下にリストされている 3 つのポイントのうちどれが目標に最も近いかを尋ねる必要があります。

- 保護の強化：ホストデータベースで見つかった脆弱性に基づいて追加のルールを有効にし、ルールを自動的に無効にしません。これにより、ルールセットが大きくなる可能性があります。
- 保護の集中：ホストデータベースで見つかった脆弱性に基づいて追加のルールを有効にし、既存のルールを無効にします。これにより、検出された脆弱性に応じてルールの数を増減できます。
- より高い効率：現在有効になっているルールセットを使用し、ホストデータベースで見つからない脆弱性のルールを無効にします。これにより、有効なルールセットが小さくなる可能性があります。

応答に基づく、推奨アクションは次のとおりです。

- 推奨事項を次に高いセキュリティレベルに設定し、無効化ルールのチェックを外します。
- 推奨事項を次に高いセキュリティレベルに設定し、無効化ルールを確認します。
- 推奨事項を現在のセキュリティレベルに設定し、無効化ルールを確認します。

始める前に

Secure Firewall 推奨事項には、次の要件があります。

- 推奨を生成するホストがシステムに存在することを確認します。
- 推奨事項に設定された保護されたネットワークは、システムに存在するホストにマッピングする必要があります。

手順

ステップ 1 **[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

ステップ 2 侵入ポリシーの [Snort 3バージョン（Snort 3 Version）] ボタンをクリックします。

ステップ 3 [推奨事項（未使用）（Recommendations (Not in Use)）] レイヤをクリックして、ルールの推奨事項を設定します。[開始（Start）] をクリックします。

[Secure Firewallルールの推奨事項（Firepower Rule Recommendations）] ウィンドウでは、次の項目を設定できます。

- [セキュリティレベル（Security Level）]：クリックして、セキュリティレベルを選択します。必要に応じて、[ルールを無効にする推奨を受け入れる（Accept Recommendations to Disable Rules）] チェックボックスをオンにして、入力セキュリティレベルおよび保護されたネットワークで有効になっていないルールを無効にできます。アラートの数が多いためにルールセットをトリミングする必要がある場合、またはインスペクションのパフォーマンスを向上させる必要がある場合にのみ、このオプションを有効にします。セキュリティレベルは次のとおりです。
  - セキュリティレベル 1：セキュリティよりも接続性を優先（Connectivity Over Security）

    [影響なし（No Impact）]：新しいルールは有効にならず、既存のルールも無効になりません。保護を強化するには、より高いセキュリティレベルを選択してください。

    [セキュリティの低減（Lower Security）]（チェックボックスがオン）：検出されたホストの潜在的な脆弱性に一致する Connectivity Over Security ルールセットのルールを除き、すべてのルールが無効になります。代わりにベースポリシーを調整することを推奨します。
  - セキュリティレベル 2：バランスのとれた接続性よりもセキュリティを優先（Balanced Security Over Connectivity）

    [影響なし（No Impact）]：新しいルールは有効にならず、既存のルールも無効になりません。保護を強化するには、より高いセキュリティレベルを選択してください。

    [より高い効率（Higher Efficiency）]（チェックボックスがオン）：検出されたホストの潜在的な脆弱性に一致する既存のルールを保持し、ネットワークで検出されなかった脆弱性に関するルールを無効にします。
  - セキュリティレベル 3：接続性よりもセキュリティを優先（Security Over Connectivity）

    [セキュリティの向上（Increased Security）]：Maximum Detection ルールセットに基づいて、検出されたホストの潜在的な脆弱性に一致する追加のルールを有効にします。

[集中型セキュリティ（Focused Security）]（チェックボックスがオン）：Security Over Connectivity ルールセットに基づいて、検出されたホストの脆弱性に一致する追加のルールを有効にし、検出されたホストの潜在的な脆弱性に一致しない既存のルールを無効にします。

- セキュリティレベル 4：最大検出（Maximum Detection）

  [セキュリティの向上（Increased Security）]：Security Over Connectivity ルールセットに基づいて、検出されたホストの潜在的な脆弱性に一致する追加のルールを有効にします。

  [集中型セキュリティ（Focused Security）]（チェックボックスがオン）：Maximum Detection ルールセットに基づいて、検出されたホストの脆弱性に一致する追加のルールを有効にし、検出されたホストの潜在的な脆弱性に一致しない既存のルールを無効にします。

  （注） Maximum Detection ルールは非常に多くのルールを有効にするため、パフォーマンスに影響する可能性があります。実稼働環境に導入する前に、この設定を確認してテストすることをお勧めします。

- [保護されたネットワーク（Protected Networks）]：モニタ対象のネットワークまたは個々のホストを指定して、推奨事項を調べます。ドロップダウンリストから、1 つ以上のシステムまたはカスタム定義のネットワークオブジェクトを選択できます。デフォルトでは、IPv4 ネットワークまたは IPv6 ネットワークが選択されます（選択されていない場合）。

  重要 Secure Firewall ルールの推奨事項は、ネットワーク検出に依存します。保護されたネットワークは、ネットワーク検出ポリシーで構成された範囲内で検出されたすべてのホストに適用されます。詳細については、『*Cisco Secure Firewall Management Center Device Configuration guide*』の「Network Discovery Policies」の章を参照してください。

[追加+（Add+）]ボタンをクリックして、タイプが[ホスト（Host）]または[ネットワーク（Network）]の新しいネットワークオブジェクトを作成し、[保存（Save）] をクリックします。

ステップ 4 推奨事項を生成および適用します。

- [生成（Generate）]：侵入ポリシーの推奨事項を生成します。このアクションは、[推奨ルール（未使用）（Recommended Rules (Not in use)）] の下にルールのリストを表示します。
- [生成して適用（Generate and Apply）]：侵入ポリシーの推奨事項を生成して適用します。このアクションは、[推奨ルール（使用中）（Recommended Rules (in use)）] の下にルールのリストを表示します。

推奨事項が正常に生成されました。すべての推奨ルールと対応する推奨アクションが新しい推奨タブに表示されます。ルールアクションの事前設定フィルタは、新しい推奨事項に加えて、このタブでも使用できます。

ステップ 5 推奨事項を確認し、それに応じて適用することを選択できます。

- [受け入れる（Accept）]：生成済みの侵入ポリシーの推奨事項を適用します。
- [更新（Refresh）]：侵入ポリシーのルール推奨事項を再生成および更新します。
- [編集（Edit）]：[推奨事項（Recommendations）] ダイアログボックスが開くので、推奨入力値を入力して推奨事項を生成します。

- [すべて削除（Remove All）]：適用された推奨ルールを元に戻すか、ポリシーから削除し、推奨タブも削除します。

[すべてのルール（All Rules）] の下に、推奨ルールを表示する [推奨ルールRecommended Rules] セクションがあります。

（注） 侵入ルールの最終アクションは、ルールアクションの優先順位に基づいて適用されます。次に、ルールアクションの優先順位を示します。

[ルールのオーバーライド（Rule Override）]>[生成された推奨事項（Generated Recommendations）]>[グループのオーバーライド（Group Override）]>[ベースポリシーのデフォルトアクション（Base Policy Default Action）]

推奨事項が有効になっている場合、Management Center では現在の状態（グループのオーバーライド、ベースポリシー、および推奨の設定）が考慮されます。アクションの優先順位は次のとおりです。

[パス（Pass）]>[ブロック（Block）]>[拒否（Reject）]>[ドロップ（Drop）]>[書き換え（Rewrite）]>[アラート（Alert）]

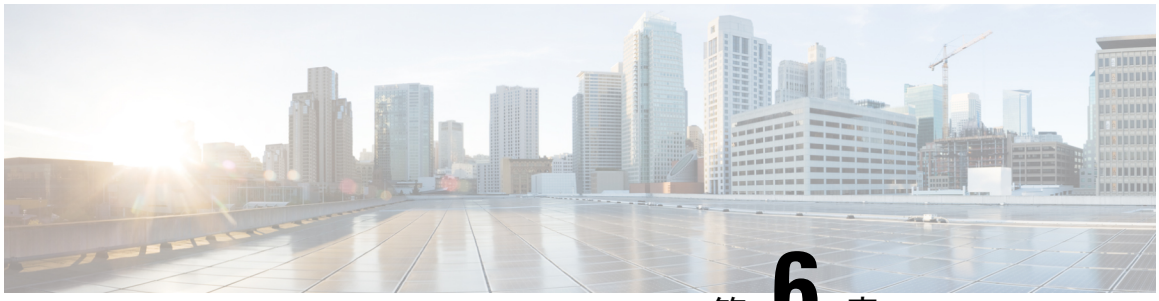
次のタスク

設定変更を展開します。設定変更の展開 （30 ページ）を参照してください。

第 II 部

Snort 3 での詳細なネットワーク分析

• Snort 3 ネットワーク分析ポリシーを開始するには （79 ページ）



第 6 章

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 （79 ページ）
- ネットワーク分析ポリシーの管理 （80 ページ）
- ネットワーク分析ポリシーの Snort 3 の定義と用語 （81 ページ）
- ネットワーク分析と侵入ポリシーの前提条件 （84 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 （85 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 （115 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

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。

手順

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（85 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 *6*：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（85 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（85 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（85 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（94 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（94 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（94 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（94 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 （85 ページ）
ネットワーク分析ポリシーのカスタマイズ （94 ページ）
ネットワーク分析ポリシーのマッピング （90 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。

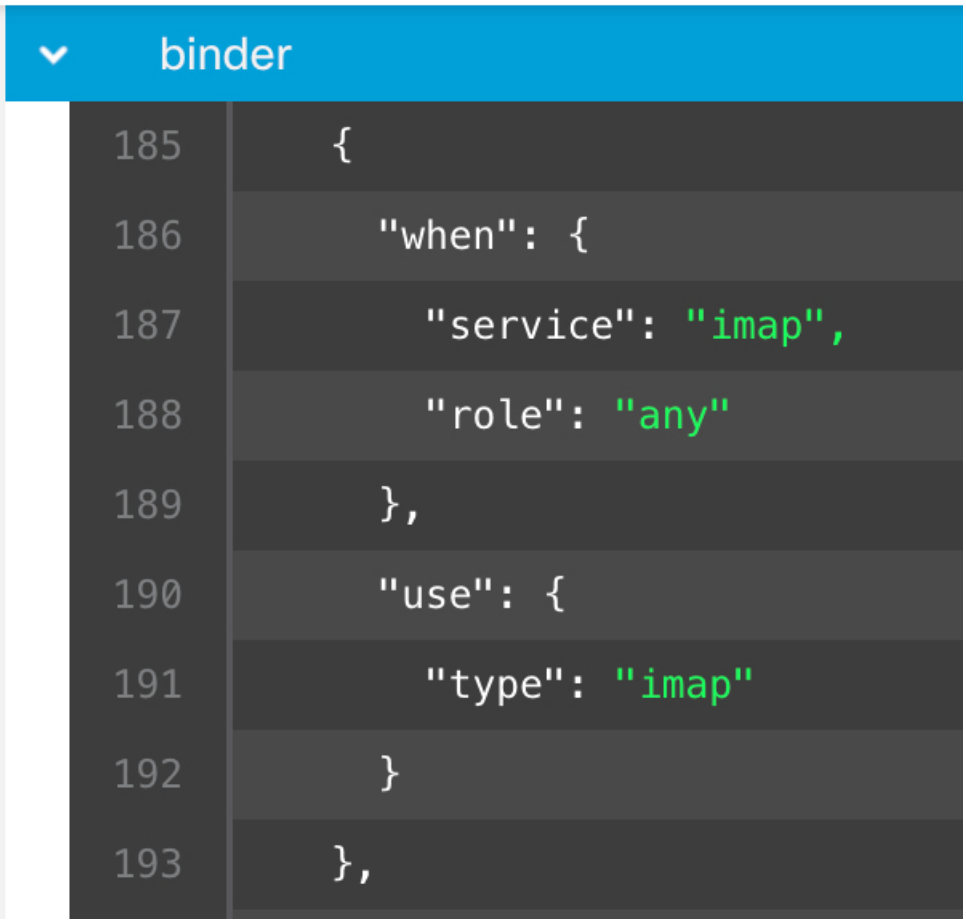
バインダインスペクタ

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 （89 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。

手順

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 [編集（Edit）]（✎） 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

手順

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。

手順

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。

手順

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「ドロップされる」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。

手順

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 （103 ページ）
インスペクタとオーバーライドのリストの表示 （99 ページ）
ネットワーク分析ポリシーの Snort 3 の定義と用語 （81 ページ）
ネットワーク分析ポリシーのカスタマイズ （94 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 （98 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。

手順

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 （94 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。

手順

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。

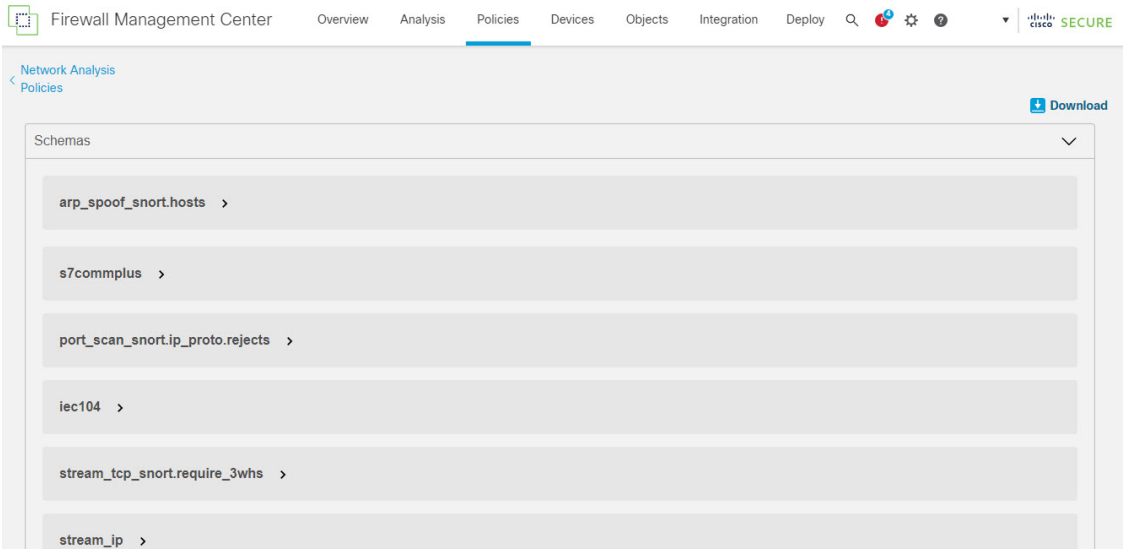
ステップ 2 ネットワーク分析ポリシーの [Snort 3 バージョン（Snort 3 Version）] に移動します。

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。

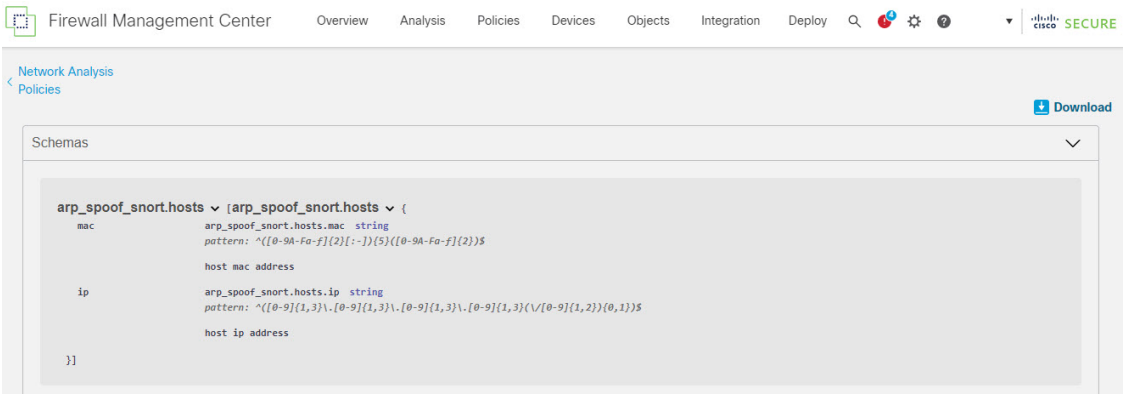
これらのオプションでは、許容値、範囲、パターン、既存およびデフォルトのインスペクタ設定、ならびにオーバーライドされたインスペクタ設定に関する情報が得られます。

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 （100 ページ）
インスペクタとオーバーライドのリストの表示 （99 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 （92 ページ）
インスペクタ設定のコピー （93 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 （94 ページ）を参照してください。

手順

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 （94 ページ）

インライン編集時の未保存の変更を元に戻す （99 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 （100 ページ）
カスタムネットワーク分析ポリシーの設定例 （103 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。

手順

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 （100 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 （98 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。

手順

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（92 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（98 ページ）
ネットワーク分析ポリシーのカスタマイズ（94 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。

手順

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（99 ページ）
ネットワーク分析ポリシーのカスタマイズ（94 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 （98 ページ）
カスタムネットワーク分析ポリシーの設定例 （103 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。

手順

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 （98 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 （94 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 （81 ページ）
ネットワーク分析ポリシーのマッピング （90 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 （85 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 （92 ページ）
インスペクタ設定のコピー （93 ページ）
ネットワーク分析ポリシーのカスタマイズ （94 ページ）
インスペクタとオーバーライドのリストの表示 （99 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。

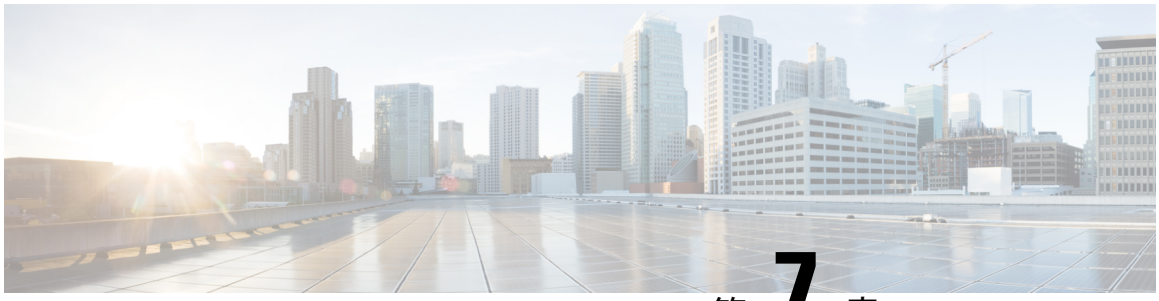
（注） 前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。

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。

第 III 部

Snort 3 向けの Encrypted Visibility Engine

• 暗号化された可視性エンジン （119 ページ）



第 7 章

暗号化された可視性エンジン

Encrypted Visibility Engine（EVE）は、TLS 暗号化を使用するクライアント アプリケーションとプロセスを識別するために使用されます。可視性を実現し、管理者が環境内でアクションを実行してポリシーを適用できるようにします。EVEテクノロジーは、マルウェアの特定と阻止にも使用できます。

- Encrypted Visibility Engine の概要 （119 ページ）
- EVE の仕組み （120 ページ）
- 侵害の兆候イベント （121 ページ）
- EVE の QUIC フィンガープリント （122 ページ）
- EVE の設定 （122 ページ）

Encrypted Visibility Engine の概要

暗号化された可視性エンジン（EVE）は、復号を必要とせずに暗号化セッションの可視性を高めるために使用されます。暗号化されたセッションに関する洞察は、シスコの脆弱性データベース（VDB）にパッケージ化されているシスコのオープンソースライブラリによって取得されます。ライブラリは、着信暗号化セッションをフィンガープリントして分析し、一連の既知のフィンガープリントと照合します。この既知のフィンガープリントのデータベースも、Cisco VDB で利用できます。

（注） 暗号化された可視性エンジンの機能は、Snort 3 を実行している Management Center の管理対象デバイスでのみサポートされます。この機能は、Snort 2 デバイス、Device Manager の管理対象管理デバイス、または CDO ではサポートされていません。

EVE の重要な機能の一部を次に示します。

- EVEから取得した情報を使用して、トラフィックに対してアクセス コントロール ポリシー アクションを実行できます。

- Cisco Secure Firewall に含まれる VDB には、EVE によって高い信頼値で検出された一部のプロセスにアプリケーションを割り当てる機能があります。または、次の目的でカスタムアプリケーション ディテクタを作成できます。
  - EVE で検出されたプロセスを新しいユーザー定義アプリケーションにマッピングする。
  - EVE で検出されたプロセスにアプリケーションを割り当てるために使用されるプロセス確実性の組み込み値を上書きする。

  『Cisco Secure Firewall Management Center Device Configuration Guide』の「**Application Detection**」の章にある項「**Configuring Custom Application Detectors**」と「**Specifying EVE Process Assignments**」を参照してください。
- EVE は、暗号化されたトラフィックで Client Hello パケットを作成したクライアントのオペレーティングシステムのタイプとバージョンを検出できます。
- EVE は、Quick UDP Internet Connections（QUIC）トラフィックのフィンガープリントと分析もサポートします。Client Hello パケットからのサーバー名は、[接続イベント（Connection Events）] ページの [URL] フィールドに表示されます。

注目 Management Center で EVE を使用するには、デバイスに有効な IPS ライセンスが必要です。IPS ライセンスがない場合、ポリシーによって警告が表示され、展開は許可されません。

（注） EVE は SSL セッションのオペレーティングシステムのタイプとバージョンを検出できます。アプリケーションやパッケージ管理ソフトウェアの実行など、オペレーティングシステムの通常の使用により、OS 検出がトリガーされる可能性があります。クライアント OS 検出を表示するには、EVE トグルボタンを有効にすることに加えて、**[ポリシー（Policies）]**>**[ネットワークの検出（Network Discovery）]**で [ホスト（Hosts）] を有効にする必要があります。ホスト IP アドレスで使用可能なオペレーティングシステムのリストを表示するには、**[分析（Analysis）]**>**[ホスト（Hosts）]** > **[ネットワークマップ（Network Map）]**をクリックし、該当するホストを選択します。

関連リンク

EVE の設定 （122 ページ）

EVE の仕組み

Encrypted Visibility Engine（EVE）は、TLS ハンドシェイクの Client Hello 部分を検査して、クライアントプロセスを識別します。Client Hello は、サーバーに送信される最初のデータパケットです。これにより、ホスト上のクライアントプロセスがよくわかります。このフィンガープリントと、宛先 IP アドレスなどの他のデータが組み合わされて、EVE のアプリケーション識

別の基礎となります。TLS セッションの確立で特定のアプリケーション フィンガープリントを識別することで、システムはクライアントプロセスを識別し、適切なアクション（許可/ブロック）を実行することができます。

EVEは、5,000を超えるクライアントプロセスを識別できます。システムは、アクセス制御ルールの基準として使用するために、多数のこれらのプロセスをクライアントアプリケーションにマッピングします。これにより、システムは TLS 復号を有効にすることなく、これらのアプリケーションを識別して制御することができます。既知の悪意のあるプロセスのフィンガープリントを使用することで、EVEテクノロジーを使用して、アウトバウンド復号を使用せずに暗号化された悪意のあるトラフィックを識別してブロックすることもできます。

機械学習（ML）テクノロジーにより、シスコは 10 億を超える TLS フィンガープリントと 10,000 を超えるマルウェアサンプルを毎日処理し、EVE フィンガープリントを作成および更新しています。これらの更新は、その後、シスコの脆弱性データベース（VDB）パッケージを使用してお客様に配信されます。

EVEは、フィンガープリントを認識できない場合、クライアントアプリケーションを識別し、IPアドレス、ポート、サーバー名などの接続先の詳細情報を使用して最初のフローの脅威スコアを推定します。この時点で、フィンガープリントのステータスはランダム化され、デバッグログで確認できます。同じフィンガープリントを持つ後続のフローの場合、EVEは再分析をスキップし、フィンガープリントのステータスをラベルなしとしてマークします。EVEの低い、または非常に低いスコアしきい値に基づいてトラフィックをブロックする場合、最初のフローはブロックされます。ただし、アプリケーションのフィンガープリントがキャッシュされると、その後のフローは許可されます。

侵害の兆候イベント

ホストの暗号化された可視性エンジン検出の侵害の兆候（IoC）イベントにより、非常に高いマルウェアの確実性レベルで、EVE によって報告された接続イベントをチェックできます。IoC イベントは、悪意のあるクライアントを使用してホストから生成された暗号化セッションに対してトリガーされます。悪意のあるホストの IP アドレス、MAC アドレス、OS 情報などの情報と、不審なアクティビティのタイムスタンプを表示できます。

接続イベントで示される、暗号化された可視性脅威の確実性スコアが「非常に高い」となっているセッションは、IoC イベントを生成します。**[ポリシー（Policies）]** > **[ネットワーク検出（Network Discovery）]** から [ホスト（Hosts）] を有効にする必要があります。 Management Center では、次の場所から IoC イベントの存在を表示できます。

- **[分析（Analysis）]** > **[侵害の兆候（Indications of Compromise）]**
- **[分析（Analysis）]** > **[ネットワークマップ（Network Map）]** > **[侵害の兆候（Indications of Compromise）]** > チェックする必要があるホストを選択します。

  IoC を生成したセッションのプロセス情報は、以下から表示できます。

  [分析（Analysis）] > **[接続イベント（Connection Events）]** > **[接続イベントのテーブルビュー（Table View of Connection Events）]** > **[IoC]**。暗号化された可視性フィールドと IoC フィールドを手動で選択する必要があることに注意してください。

EVE の QUIC フィンガープリント

Snort は、EVE に基づいて Quick UDP Internet Connections（QUIC セッション）内のクライアントアプリケーションを識別できます。QUIC フィンガープリントでは次を実行できます。

- 復号を有効にせずに QUIC でアプリケーションを検出する。
- 復号を有効にせずにマルウェアを特定する。
- サービスアプリケーションを検出する。QUIC プロトコルで検出されたサービスに基づいて、アクセスコントロールルールを割り当てることができます。

EVE の設定

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択します。

ステップ 2 編集するアクセス コントロール ポリシーの横にある [編集（Edit）]（✎）をクリックします。

ステップ 3 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 [詳細設定（Advanced Settings）] を選択します。

ステップ 4 [Encrypted Visibility Engine] の横にある [編集（Edit）]（✎）をクリックします。

ステップ 5 [Encrypted Visibility Engine] ページで、[Encrypted Visibility Engine (EVE)] トグルボタンを有効にします。

ステップ 6 [アプリケーション検出にEVEを使用（Use EVE for Application Detection）]：このトグルボタンはデフォルトで有効になっています。つまり、EVE はクライアントアプリケーションをプロセスに割り当てることができます。

接続イベントまたは統合イベントの [暗号化された可視性フィンガープリント（Encrypted Visibility Fingerprint）] 列ヘッダーに EVE のフィンガープリント情報が追加されます。収集された EVE データをさらに分析する場合は、フィンガープリント情報を右クリックしてドロップダウンメニューを開くことができます。メニューで、[暗号化された可視性エンジンプロセス分析の表示（View Encrypted Visibility Engine Process Analysis）] をクリックして appid.cisco.com に移動し、フィンガープリント、VDB バージョンなどの詳細を表示します。同じフィンガープリント文字列を持つ異なる行と、それらに関連付けられている潜在的なプロセス名およびその拡散度が表示されます。拡散度は、データ収集システム内の特定のフィンガープリントに関連付けられたプロセスの頻度を示します。プロセス名を選択し、[リクエストの送信（Submit Request）] をクリックすると、EVE のプロセス検出の不一致に関するフィードバックを送信することができます。たとえば、検出されたプロセス名が送信されているトラフィックと一致しない場合や、特定のフィンガープリントについてプロセス名がまったく検出されない場合に、リクエストを送信できます。

[アプリケーション検出にEVEを使用（Use EVE for Application Detection）] トグルボタンを無効にした場合：

- AppID で識別されたクライアントがプロセスに割り当てられ、EVE プロセスとスコアは表示されますが、EVE で検出されたプロセスからアプリケーションへのマッピングはなく、アクションも実行されません。イベントの詳細は、[接続イベント（Connection Events）] または [統合イベント（Unified Events）] で確認できます。接続イベントの違い（アプリケーションの割り当ての有無）を確認するには、[クライアントアプリケーション（Client Application）] 列ヘッダーを確認します。
- 接続イベントまたは統合イベントの [暗号化された可視性フィンガープリント（Encrypted Visibility Fingerprint）] フィールドは空です。

ステップ 7 [EVEスコアに基づくトラフィックのブロック（Block Traffic Based on EVE Score）] トグルボタンを有効にして、EVE の脅威の確実性スコアに基づいてトラフィックをブロックします。潜在的な脅威である着信トラフィックは、デフォルトでブロックされます。

デフォルトのブロックしきい値は 99% で、次のことを意味します。

- EVE がトラフィックを 99% 以上の確実性でマルウェアであると検出した場合、トラフィックはブロックされます。
- EVE がトラフィックを 99% 未満の確実性でマルウェアであると検出した場合、EVE は何も実行しません。

（注） EVE がトラフィックをブロックした場合、[接続イベント（Connection Events）] ページの [理由（Reason）] 列ヘッダーに [暗号化された可視性ブロック（Encrypted Visibility Block）] が表示されます。

ステップ 8 スライダを使用して、EVE の脅威の確実性に基づいたブロックのしきい値を調整します（[非常に低い（Very Low）] ～ [非常に高い（Very High）] の範囲）。

ステップ 9 さらに細かく制御するには、[詳細モード（Advanced Mode）] トグルボタンを有効にします。これで、トラフィックをブロックするための特定の EVE 脅威確実性スコアを割り当てることができるようになりました。デフォルトのブロックしきい値は 99% です。

注意 最適なパフォーマンスを確保するために、しきい値を 50% 未満に設定しないことを推奨します。

ステップ 10 [OK] をクリックします。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。

EVE イベントの表示

[Encrypted Visibility Engine] を有効にして、アクセス コントロール ポリシーを展開すると、システムを介してライブトラフィックの送信を開始できます。ログに記録された接続イベント

は、[接続イベント（Connection Events）] ページで表示できます。接続イベントにアクセスするには、Management Center で次の手順を実行します。

手順

ステップ 1 **[分析（Analysis）] > [接続（Connection）] > [イベント（Events）]** の順にクリックします。

ステップ 2 [接続イベントのテーブルビュー（Table View of Connection Events）] タブをクリックします。

[分析（Analysis）] メニューにある [統合イベント（Unified Events）] ビューアに接続イベントフィールドを表示することもできます。

暗号化された可視性エンジンでは、接続を開始したクライアントプロセス、クライアントのOS、そのプロセスにマルウェアが含まれているかどうかを特定できます。

ステップ 3 [接続イベント（Connection Events）] ページで、Encrypted Visibility Engine 用に追加された次の列を表示します。以下の列を明示的に有効にする必要があることに注意してください。

- [暗号化された可視性プロセス名（Encrypted Visibility Process Name）]
- [暗号化された可視性プロセスの信頼スコア（Encrypted Visibility Process Confidence Score）]
- [暗号化された可視性脅威の信頼度（Encrypted Visibility Threat Confidence）]
- [暗号化された可視性脅威の信頼スコア（Encrypted Visibility Threat Confidence Score）]
- [検出タイプ（Detection Type）]

これらのフィールドの詳細については、『Cisco Secure Firewall Management Center Administration Guide』の「**Connection and Security-Related Connection Events**」の章の「**Connection and Security Intelligence Event Fields**」の項を参照してください。

（注） プロセスにアプリケーションが割り当てられている場合、[接続イベント（Connection Events）] ページの [検出タイプ（Detection Type）] 列には、クライアントアプリケーションが EVE によって識別されたことを示す [暗号化された可視性エンジン（Encrypted Visibility Engine）] が表示されます。プロセス名へのアプリケーションの割り当てがない場合、[検出タイプ（Detection Type）] 列には、クライアントアプリケーションを識別したエンジンが AppID であることを示す [AppID] が表示されます。

EVE ダッシュボードの表示

EVE分析情報は2つのダッシュボードに表示できます。ダッシュボードにアクセスするには、次の手順を実行します。

手順

ステップ 1 [Overview] > [Dashboards] に移動し、[Dashboard] をクリックします。

ステップ 2 [概要ダッシュボード（Summary Dashboard）] ウィンドウで、スイッチダッシュボードのリンクをクリックし、ドロップダウンボックスから [アプリケーション統計（Application Statistics）] を選択します。

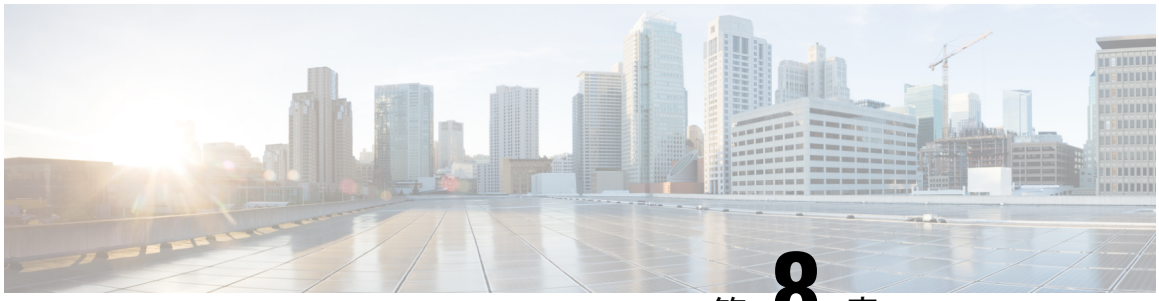
ステップ 3 **[Encrypted Visibility Engine]** タブを選択し、次の 2 つのダッシュボードを表示します。

- **[上位の暗号化された可視性エンジンで検出されたプロセス（Top Encrypted Visibility Engine Discovered Processes）]**：ネットワークで使用されている上位の TLS プロセス名と接続数が表示されます。テーブルのプロセス名をクリックすると、[接続イベント（Connection Events）] ページのフィルタリングされたビューが表示されます。このビューはプロセス名でフィルタリングされています。
- **[暗号化可視性エンジンの脅威の信頼度別の接続（Connections by Encrypted Visibility Engine Threat Confidence）]**：マルウェアの確実性レベル（非常に高い、非常に低いなど）別に接続が表示されます。テーブル内の脅威の信頼レベルをクリックすると、[接続イベント（Connection Events）] ページのフィルタリングされたビューが表示されます。このビューは、信頼レベルによってフィルタリングされています。

第 IV 部

Snort 3 のエレファントフロー検出

- エレファントフローの検出 （129 ページ）



第 8 章

エレファントフローの検出

エレファントフローは（合計バイト数が）非常に大きい連続フローであり、ネットワークリンク上で測定される TCP（または他のプロトコル）フローによって設定されます。デフォルトでは、エレファントフローとは 1 GB/10 秒を超えるフローです。これらのフローは、Snort コアでのパフォーマンス拘束の原因となります。エレファントフローはそれほど多くありませんが、一定期間にわたって総帯域幅の不均衡な割合を占める可能性があります。これらのフローは、CPU 使用率の上昇やパケットドロップなどの問題につながる可能性があります。

Management Center 7.2.0 以降（Snort 3 デバイスのみ）では、エレファントフロー機能を使用して、エレファントフローを検出および修復できます。こうしたアクションはシステムストレスを軽減し、前述の問題を解決するために役立ちます。

- エレファントフローの検出と修復について （129 ページ）
- インテリジェント アプリケーション バイパスからのエレファントフローのアップグレード （130 ページ）
- エレファントフローの設定 （130 ページ）

エレファントフローの検出と修復について

エレファントフロー検出機能を使用して、エレファントフローを検出して修復できます。次の修復アクションを適用できます。

- **エレファントフローをバイパスする**：Snort インスペクションをバイパスするようにエレファントフローを設定できます。このアクションが設定されている場合、Snort はエレファントフローからパケットを受信しません。
- **エレファントフローをスロットルする**：フローにレート制限を適用して、フローの検査を続行できます。フローレートは動的に計算され、フローレートの 10% が削減されます。Snort は、判定結果（フローレートが 10% 少ない QoS フロー）をファイアウォールエンジンに送信します。識別されていないアプリケーションを含むすべてのアプリケーションをバイパスすることを選択した場合、いずれのフローに対してもスロットルアクション（レート制限）を設定できません。

（注） エレファントフロー検出を機能させるには、Snort 3 を検出エンジンにする必要があります。

インテリジェントアプリケーションバイパスからのエレファントフローのアップグレード

バージョン 7.2.0 以降の Snort 3 デバイスでは、インテリジェント アプリケーション バイパス（IAB）は廃止されました。

7.2.0 以降を実行しているデバイスの場合、AC ポリシー（[詳細設定（Advanced Settings）] タブ）の [エレファントフロー設定（Elephant Flow Settings）] セクションでエレファントフロー設定を構成する必要があります。

7.2.0（または以降）へのアップグレード後、Snort 3 デバイスを使用している場合、エレファントフロー構成設定は、[インテリジェントアプリケーションバイパス設定（Intelligent Application Bypass Settings ）] セクションからではなく、[エレファントフロー設定（Elephant Flow Settings ）] セクションから選択されて展開されるため、エレファントフロー構成設定に移行していない場合、次の展開時にデバイスのエレファントフロー構成は失われます。

次の表は、Snort 3 または Snort 2 エンジンを実行しているバージョン 7.2.0 以降およびバージョン 7.1.0 以前に適用できる IAB またはエレファントフロー構成を示しています。

Management Center	Threat Defense	エレファントフローまたは IAB 構成
Management Center 7.0 または 7.1	Snort 2 デバイス	IAB の構成が適用されます。
	Snort 3 デバイス	IAB の構成が適用されます。
Management Center 7.2.0	Snort 2 デバイス	IAB の構成が適用されます。
	Snort 3 デバイス（7.1.0 以前）	IAB の構成が適用されます。
	Snort 3 デバイス（7.2.0 以降）	エレファントフローの構成が適用されます。

エレファントフローの設定

エレファントフローでアクションを実行するようにエレファントフローを設定できるため、システムの危機、高い CPU 使用率、パケットドロップなどの問題の解決に役立ちます。

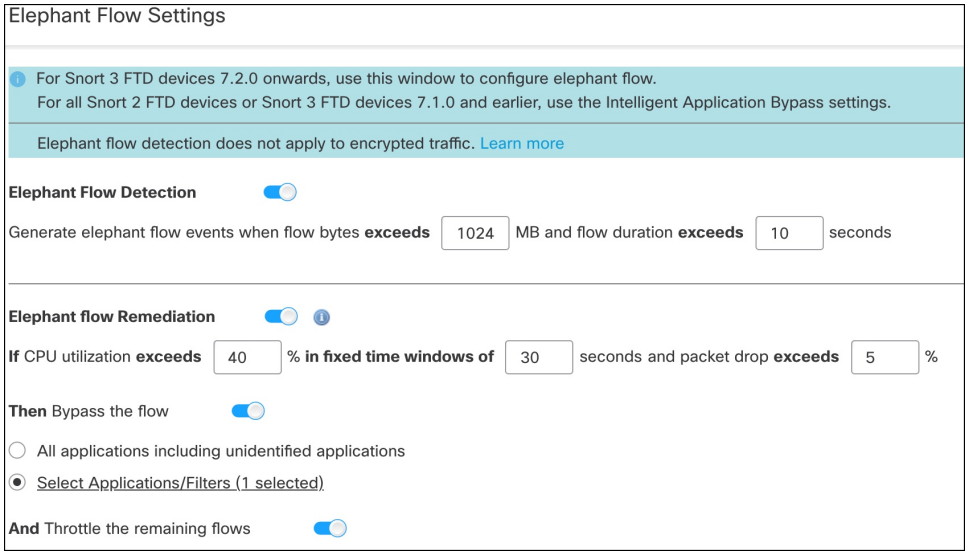
注目 エレファントフロー検出は、Snort を介して処理されない、事前フィルタリングされたフロー、信頼されたフロー、または高速転送フローには適用できません。エレファントフローは Snort によって検出されるため、エレファントフロー検出は暗号化されたトラフィックには適用されません。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、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 [詳細設定（Advanced Settings）] をクリックします。次に、[エレファントフロー設定（Elephant Flow Settings ）] の横にある **[編集（Edit）]**（✎）をクリックします。

代わりに [表示（View）]（👁）が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

図 *2*: エレファントフロー検出の設定



ステップ 2 [エレファントフロー検出（Elephant Flow Detection）] トグルボタンはデフォルトで有効になっています。フローバイトとフロー期間の値を設定できます。設定した値を超えると、エレファントフローイベントが生成されます。

ステップ 3 エレファントフローを修復するには、[エレファントフローの修復（Elephant Flow Remediation）] トグルボタンを有効にします。

ステップ 4 エレファントフローの修復基準を設定するには、CPU 使用率 %、固定時間ウィンドウの継続時間、およびパケットドロップ % の値を設定します。

ステップ 5 設定された基準を満たしている場合、エレファントフローの修復に対して次のアクションを実行できます。

1. [フローをバイパスする（Bypass the flow）]：選択したアプリケーションまたはフィルタの Snort インスペクションをバイパスするには、このボタンを有効にします。次から選択します。

   - [識別されていないアプリケーションを含むすべてのアプリケーション（All applications including unidentified applications）]：すべてのアプリケーション トラフィックをバイパスするには、このオプションを選択します。このオプションを設定すると、すべてのフローにスロットルアクション（レート制限）を設定できなくなります。
   - [アプリケーション/フィルタの選択（Select Applications/Filters）]：トラフィックをバイパスするアプリケーションまたはフィルタを選択するには、このオプションを選択します。『Cisco Secure Firewall Management Center Device Configuration Guide』の「**Access Control Rules**」の章にある「**Configuring Application Conditions and Filters**」トピックを参照してください。

2. [フローをスロットルする（Throttle the flow）]：フローにレート制限を適用し、フローの検査を続行するには、このボタンを有効にします。Snortインスペクションをバイパスし、残りのフローをスロットルするアプリケーションまたはフィルタを選択できます。

（注） スロットルされたエレファントフローからスロットルが自動的に削除されるのは、システムが危機を脱した場合、つまり、Snort パケットドロップのパーセンテージが設定されたしきい値よりも低い場合です。その結果、レート制限も削除されます。

次の Threat Defense コマンドを使用して、スロットルされたエレファントフローからスロットルを手動で削除することもできます。

- **clear efd-throttle <5-tuple/all> bypass**：このコマンドは、スロットルされたエレファントフローからスロットルを削除し、Snort インスペクションをバイパスします。
- **clear efd-throttle <5-tuple/all>**：このコマンドは、スロットルされたエレファントフローからスロットルを削除し、Snortインスペクションを続行します。このコマンドを使用すると、エレファントフローの修復はスキップされます。

これらのコマンドの詳細については、『Cisco Secure Firewall Threat Defense コマンドリファレンス』を参照してください。

（注） エレファントフローに対するアクション（フローのバイパスとスロットル）の実行は、Cisco Firepower 2100 シリーズ デバイスではサポートされていません。

ステップ 6 [修復除外ルール（Remediation Exemption Rule）] セクションで、[ルールの追加（Add Rule）] をクリックして、修復から除外する必要があるフローの L4 アクセス制御リスト（ACL）ルールを設定します。

ステップ 7 [ルールの追加（Add Rule）] ウィンドウで、[ネットワーク（Networks）] タブを使用してネットワークの詳細、つまり送信元ネットワークと宛先ネットワークを追加します。[ポート（Ports）] タブを使用して、送信元ポートと宛先ポートを追加します。

エレファントフローが検出され、定義されているルールに一致する場合、[接続イベント（Connection Events）] の [理由（Reason）] 列ヘッダーに理由として [エレファントフローの除外（Elephant Flow Exempted）] が表示されてイベントが生成されます。

ステップ 8 [修復除外ルール（Remediation Exemption Rule）] セクションで、修復アクションから除外されているフローを確認できます。

ステップ 9 [OK] をクリックして、エレファントフロー設定を保存します。

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。

次のタスク

設定変更を展開します設定変更の展開を参照してください。

エレファントフロー設定を構成した後、接続イベントをモニターして、フローが検出、バイパス、またはスロットリングされているかどうかを確認します。これは、接続イベントの [理由（Reason）] フィールドで確認できます。エレファントフロー接続の 3 つの理由は次のとおりです。

- エレファントフロー（Elephant Flow）
- エレファントフローがスロットリングされている（Elephant Flow Throttled）
- エレファントフローが信頼されている（Elephant Flow Trusted）

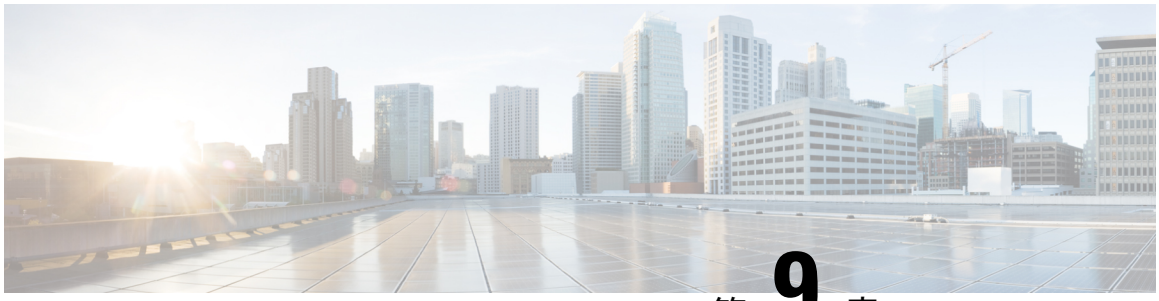
注目 エレファントフロー検出を有効にしただけでは、エレファントフローの接続イベントは生成されません。接続イベントが別の理由ですでにログに記録されており、フローもエレファントフローである場合、[理由（Reason）] フィールドにはこの情報が含まれます。ただし、すべてのエレファントフローを確実にロギングするには、該当するアクセス制御ルールで接続ロギングを有効にする必要があります。

詳細については、『Cisco Secure Firewall Elephant Flow Detection』を参照してください。

第 V 部

Snort 3 の使用例

- Cisco Secure Firewall Management Center での Snort 2 から Snort 3 への移行 （137 ページ）
- Cisco Secure Firewall Management Center での Snort 3 推奨事項の生成 （149 ページ）
- EVE の脅威の確実性スコアに基づいてトラフィックをブロックする （157 ページ）
- エレファントフロー検出結果の設定 （163 ページ）
- Snort 3 侵入ポリシーでの MITRE フレームワークを使用した脅威の軽減 （173 ページ）



第 9 章

Cisco Secure Firewall Management Center での Snort 2 から Snort 3 への移行

- Snort 2 から Snort 3 への移行 （137 ページ）
- Snort 3 への移行の利点 （137 ページ）
- ビジネスシナリオの例 （138 ページ）
- Snort 2 から Snort 3 への移行のベストプラクティス （138 ページ）
- 前提条件 （138 ページ）
- エンドツーエンドの移行ワークフロー （139 ページ）
- Threat Defense で Snort 3 を有効にする （139 ページ）
- 単一の侵入ポリシーの Snort 2 ルールの Snort 3 への変換 （140 ページ）
- 設定変更の展開 （145 ページ）

Snort 2 から Snort 3 への移行

Snort は、バージョン 2 からバージョン 3 に大幅な変更が加えられた侵入検知および防御システムです。Snort 3 の拡張機能を活用するには、Snort 2 から既存のルールセットを移行することが重要になります。この移行プロセスでは、Snort 2 ルールを変換して Snort 3 ルール構文への適応を行い、検出とパフォーマンスを向上させるためにルールを最適化します。

組織によっては、脅威防御デバイスを Cisco Secure Firewall Management Center で管理することができます。組織では、Snort 2 から Snort 3 への移行時にハイブリッド展開アプローチを選択できます。このアプローチにより、段階的な移行が可能になり、中断の可能性が最小限に抑えられます。

Snort 3 への移行の利点

- **プロトコルサポートの強化**：Snort 3 ではプロトコルサポートが改善されており、暗号化されたトラフィックを含む幅広い最新のプロトコルで脅威をモニターおよび検出できます。
- **ルール管理の合理化**：Snort 3 は、より使いやすいルール言語とルール管理システムを提供し、ルールの作成、変更、および効果的な管理を容易にします。

- **パフォーマンスの向上**：Snort 3 は、大量のトラフィックをより効率的に処理するように最適化されているため、パフォーマンスのボトルネックのリスクが軽減され、タイムリーな脅威検出が可能になります。

ビジネスシナリオの例

Alice は、ネットワーク インフラストラクチャのモニターと保護を Snort インスペクションエンジンに大きく依存している大規模な組織でセキュリティアナリストとして働いています。この組織は数年間 Snort バージョン 2 を使用していますが、いくつかの制限と課題に直面しています。

ネットワーク管理者の Bob は、これらの問題を克服し、組織のネットワークセキュリティ機能を強化するために、Snort 2 から Snort 3 に移行しようとしています。

この移行により、ネットワークセキュリティのモニタリングが改善され、パフォーマンスが向上し、ルール管理が合理化されます。

Snort 2 から Snort 3 への移行のベストプラクティス

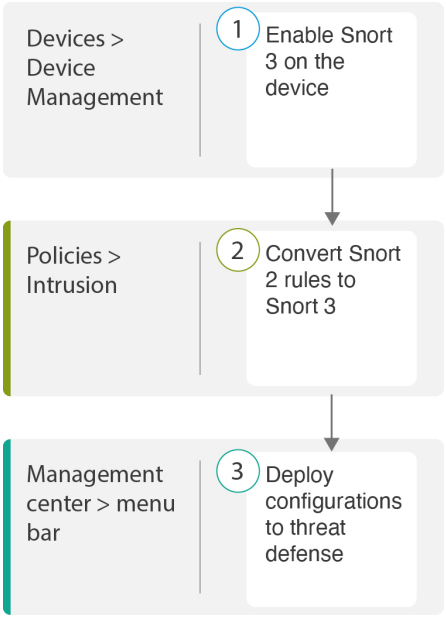
- 移行を実行する前に、侵入ポリシーをバックアップします。『Cisco Secure Firewall Management Center Administration Guide』の「Export Configurations」タスクを参照してください。
- デバイスを Snort 3 にアップグレードする前に、Snort 2 で変更が行われた場合は、同期ユーティリティを使用して Snort 2 から Snort 3 に最新の同期を追加すると、同様の対象範囲で開始できます。Snort 2 のルールと Snort 3 の同期 （29 ページ） を参照してください。
- Snort 2 カスタムルールは Snort 3 に自動的に変換されないため、手動で移行する必要があります。Snort 2 のカスタム IPS ルールの Snort 3 への変換 （26 ページ） を参照してください。
- 同期では、しきい値または抑制を含む Snort 2 ルールは移行されません。これらのルールは、Snort 3 で再度作成する必要があります。

前提条件

- Snort の実用的な知識を持っている。Snort 3 アーキテクチャの詳細については、Snort 3 Adoption を参照してください。
- Management Center をバックアップする。「Backup the Management Center」を参照してください。
- 侵入ポリシーをバックアップする。「Exporting Configurations」を参照してください。

エンドツーエンドの移行ワークフロー

次のフローチャートは、Cisco Secure Firewall Management Center で Snort 2 を Snort 3 に移行するためのワークフローを示しています。



ステップ	説明
1	デバイスで Snort 3 を有効にします。Threat Defense で Snort 3 を有効にする（139 ページ） を参照してください。
2	Snort 2 ルールを Snort 3 に変換します。単一の侵入ポリシーの Snort 2 ルールの Snort 3 への変換 （140 ページ） を参照してください。
3	設定を展開します。設定変更の展開 （30 ページ） を参照してください。

Threat Defense で Snort 3 を有効にする

注目 展開プロセス中に現在の検査エンジンをシャットダウンする必要があるため、一時的なトラフィック損失が発生します。

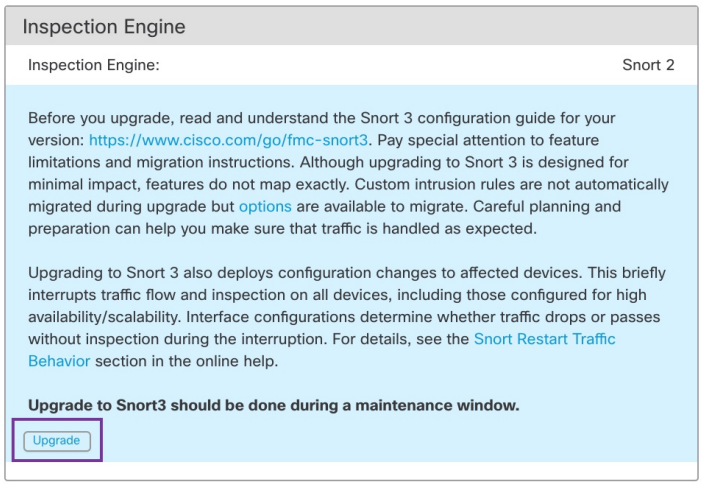
手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択します。

ステップ 2 対応するデバイスをクリックして、デバイスのホームページに移動します。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [検査エンジン（Inspection Engine）] セクションで、[アップグレード（Upgrade）] をクリックします。



ステップ 5 [はい（Yes）] をクリックします。

次のタスク

デバイスに変更を展開します。設定変更の展開 （30 ページ） を参照してください。

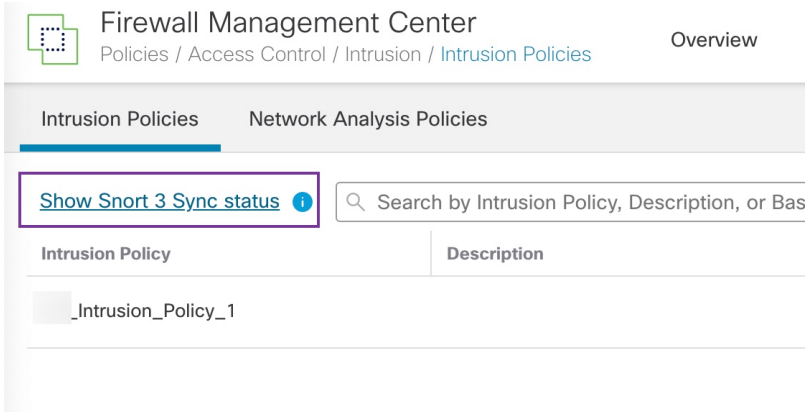
選択した Snort バージョンとの互換性を得るため、システムは展開プロセス中にポリシー設定を変換します。

単一の侵入ポリシーの Snort 2 ルールの Snort 3 への変換

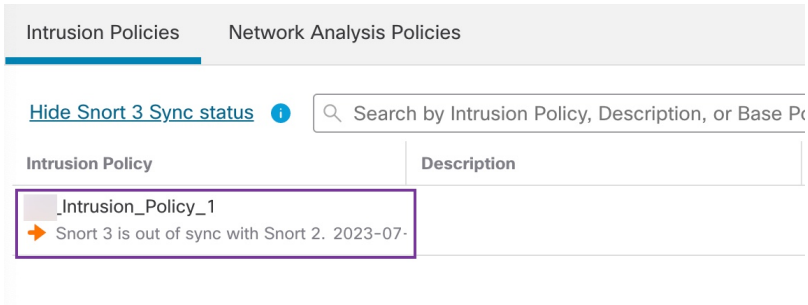
手順

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 [侵入ポリシー（Intrusion Policies）] タブで、[Snort 3同期ステータスの表示（Show Snort 3 Sync status）] をクリックします。

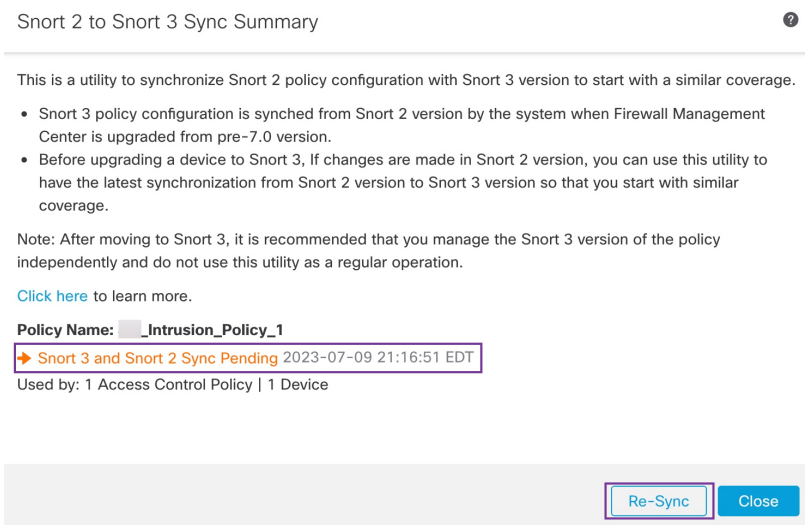


ポリシーにオレンジ色の矢印が表示されている場合は、侵入ポリシーの Snort 2 バージョンと Snort 3 バージョンが同期されていないことを示しています。



ステップ 3 オレンジ色の矢印をクリックします。

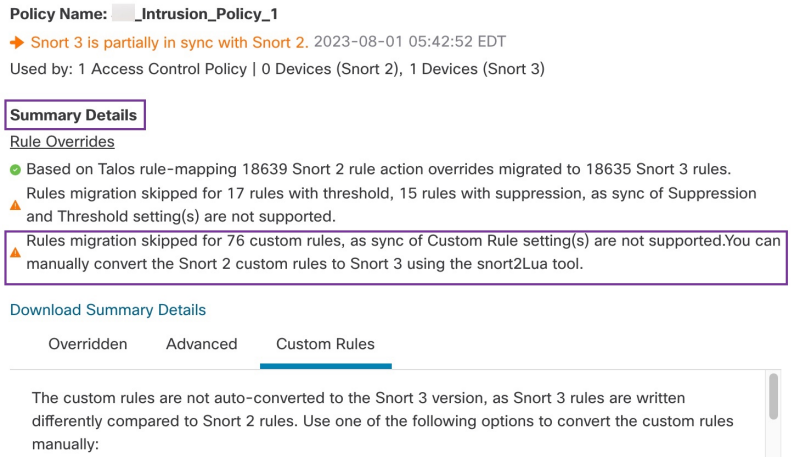
[Snort 2からSnort 3への同期の概要（Snort 2 to Snort 3 Sync Summary）] ページに、Snort 2 から Snort 3 への同期が保留中であることが表示されます。



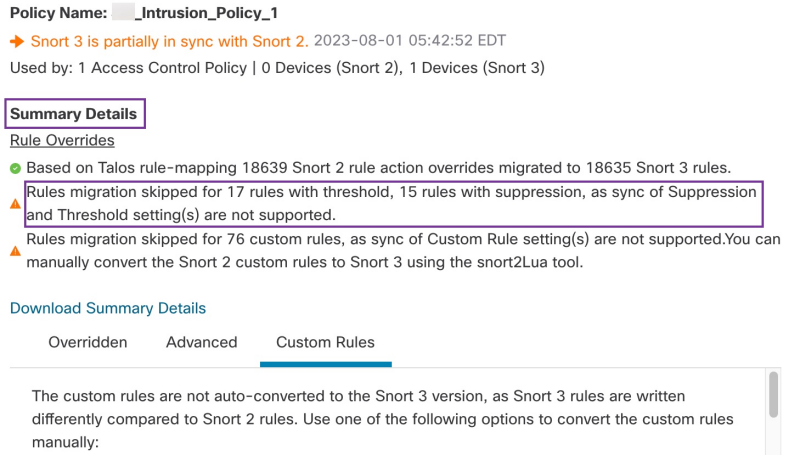
ステップ 4 [再同期（Re-Sync）] をクリックして同期を開始します。

（注） [再同期（Re-Sync）] をクリックすると、snort2Lua ツールはルールを Snort 2 から Snort 3 に変換します。

[概要の詳細（Summary Details）] セクションには、移行またはスキップされたルールが一覧表示されます。この使用例では、76 個のカスタム Snort 2 ルール、しきい値がある 17 個のルール、および同期プロセス中にスキップされた抑制付きの 15 個のルールがあります。カスタムルールを移行するには、次のステップに進みます。



しきい値と抑制を含むルールを移行するには、ステップ 6 に進みます。



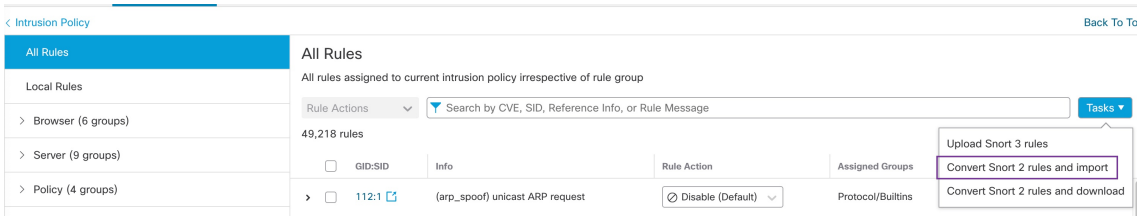
ステップ 5 76 個のカスタムルールを移行するには、次のいずれかの手順を実行します。

- [カスタムルール（Custom Rules）] タブで、[インポート（Import）] アイコンをクリックして、ローカルルールをポリシーの Snort 3 バージョンに変換して自動インポートします。

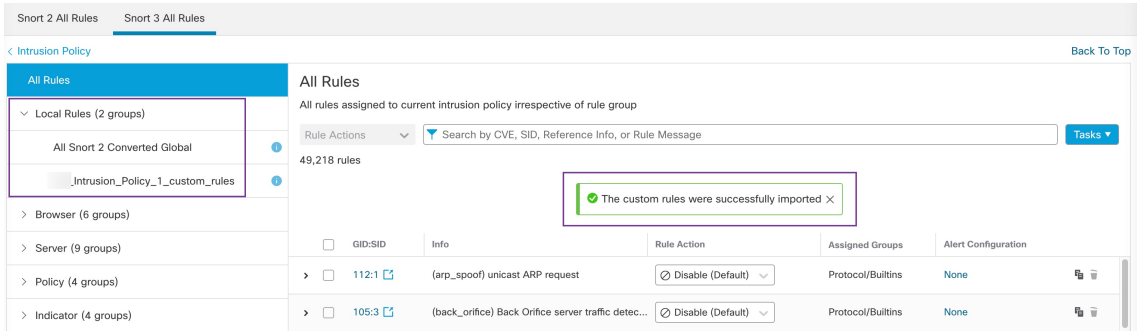
ルールが正常にインポートされると、確認メッセージが表示されます。

- [オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）] を選択し、[Snort 3のすべてのルール（Snort 3 All Rules）] をクリックします。

1. 左側のパネルで[ローカルルール（Local Rules）]をクリックして、ルールが移行されているかどうかを確認します。Snort 2 のカスタムルールは移行されていないことに注意してください。
2. [タスク（Tasks）] ドロップダウンリストから、[Snort 2ルールの変換とインポート（Convert Snort 2 rules and import）] を選択します。

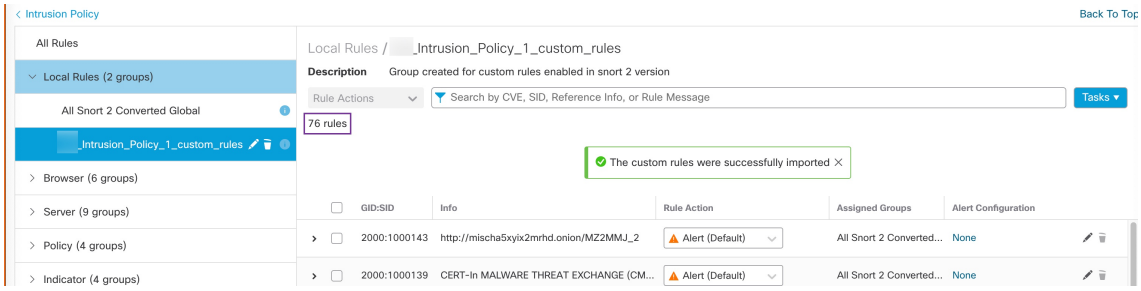


3. [OK] をクリック



新しく作成されたルールグループ（[すべてのSnort 2変換済みグローバル（All Snort 2 Converted Global）]）が、左側のパネルの [ローカルルール（Local Rules）] の下に作成されます。

次の図に示すように、76 個のカスタムルールがすべて移行されています。



または、前の手順で [Snort 2ルールの変換とダウンロード（Convert Snort 2 rules and download）] を選択して、ルールファイルをローカルに保存します。ダウンロードしたファイル内の変換後のルールを確認し、後で [Snort 3ルールのアップロード（Upload Snort 3 rules）] オプションを使用してファイルをアップロードできます。

ステップ 6 [サマリーの詳細のダウンロード（Download Summary Details）] リンクをクリックして、.txt 形式でルールをダウンロードします。

次に、表示されるサマリーの例を示します。


```
  "id": "00505691-15DC-0ed3-0000-004294988561",
  "name": "_Intrusion_Policy_1",
  "type": "IntrusionPolicy",
  "syncStatus": {
    "source": {
      "id": "bdce2d6a-1ebe-11ee-8e88-220032eb1fb5",
      "type": "IntrusionPolicy"
    },
    "status": "WARN",
   "description": "Migration is partially successful. Some of the rules are not copied to Snort3.",

    "timestamp": 1690883954814,
    "lastUser": {
      "name": "admin"
    },
    "details": [
      {
        "type": "Summary",
        "status": "INFO",
        "description": "Based on Talos rule-mapping 18639 Snort 2 rule action overrides migrated
 to 18635 Snort 3 rules."
      },
      {
        "id":
"1:1000156=alert,1:1000114=alert,1:1000160=alert,1:1000135=alert,1:1000115=alert,1:1000118=alert,

1:1000092=alert,1:1000139=alert,1:1000123=alert,1:1000159=alert,1:1000149=disabled,1:1000167=alert,

1:1000133=alert,1:1000095=alert,1:1000143=alert,1:1000106=alert,1:1000153=alert,1:1000097=alert,1:1000141=alert,

1:1000148=alert,1:1000090=alert,1:1000119=alert,1:1000112=alert,1:1000138=alert,1:1000128=alert,1:1000132=alert,

1:1000134=alert,1:1000145=disabled,1:1000110=disabled,1:1000107=alert,1:1000163=alert,1:1000124=alert,1:1000125=alert,

1:1000094=alert,1:1000113=disabled,1:1000147=alert,1:1000161=alert,1:1000105=disabled,1:1000140=alert,1:1000111=alert,

1:1000102=alert,1:1000129=disabled,1:1000108=alert,1:1000144=disabled,1:1000088=alert,1:1000091=alert,1:1000131=alert,

1:1000157=alert,1:1000120=alert,1:1000126=alert,1:1000165=alert,1:1000146=alert,1:1000162=alert,1:1000116=alert,1:1000142=alert,

1:1000170=disabled,1:1000169=alert,1:1000104=alert,1:1000099=disabled,1:1000171=alert,1:1000093=alert,1:1000087=alert,1:1000100=alert,

1:1000137=alert,1:1000158=alert,1:1000103=alert,1:1000098=alert,1:1000127=disabled,1:1000130=alert,1:1000164=alert,1:1000089=alert,

         1:1000109=alert,1:1000136=alert,1:1000117=alert,1:1000166=alert,1:1000168=alert",
        "type": "PolicyInfo",
        "description": "Corresponding Snort 2 policy overridden custom (local) rules."
      },
      {
        "type": "AssignedDevices",
```

```
  "status": "INFO",
  "description": "Snort3:0 , Snort2:0"
},
{
  "id": "122:6",
  "type": "Threshold",
  "status": "ERROR",
  "description": "PSNG_TCP_FILTERED_DECOY_PORTSCAN"
},
{
  "id": "122:15",
  "type": "Threshold",
  "status": "ERROR",
  "description": "PSNG_IP_PORTSWEEP_FILTERED"
 },
{
  "id": "122:1",
  "type": "Threshold",
  "status": "ERROR",
  "description": "PSNG_TCP_PORTSCAN"
},
```


ステップ 7 [閉じる（Close）] をクリックして、[同期の概要（Sync Summary）] ダイアログボックスを閉じます。

ステップ 8 ステータスが ERROR のルールを確認するには、[ポリシー（Policies）] > [侵入（Intrusion）] を選択し、侵入ポリシーの [Snort 2] バージョンをクリックします。

ステップ 9 [ポリシー情報（Policy Information）] で、[ルール（Rules）] をクリックし、ルールをフィルタ処理します。たとえば、[フィルタ（Filter）] フィールドに **PSNG_TCP_PORTSCAN** と入力してルールを検索します。

ステップ 10 ルールの詳細バージョンを表示するには、[詳細の表示（Show Details）] をクリックします。

ステップ 11 Snort 3 ルールガイドラインを使用して Snort 3 でルールを再度作成し、ファイルを .txt または .rules ファイルとして保存します。詳細については、www.snort3.org を参照してください。

ステップ 12 ローカルで作成したカスタムルールがすべての Snort 3 ルールのリストにアップロードされます。「Add Custom Rules to Rule Groups」を参照してください。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ） を参照してください。

設定変更の展開

設定を変更した後に、影響を受けるデバイスに展開します。

（注） このトピックでは、設定変更を展開する基本的な手順について説明します。手順を進める前に、最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Deploy Configuration Changes*」トピックを参照し、変更を展開する上での前提条件と影響を理解しておくことを強く推奨します。

⚠

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。

手順

ステップ 1 Secure Firewall Management Center メニューバーで、[展開（Deploy）] をクリックし、[展開（Deployment）] を選択します。

[GUI] ページには、期限切れの設定を持ち、ステータスが [保留中（Pending）] のデバイスのリストが表示されます。

- [変更者（Modified by）] 列には、ポリシーまたはオブジェクトを変更したユーザーの一覧が表示されます。デバイスリストを展開すると、ポリシーリストごとのポリシーを変更したユーザーが表示されます。

  （注） 削除されたポリシーおよびオブジェクトのユーザ名は表示されません。

- [インスペクションの中断（Inspect Interruption）] 列には、展開時にデバイスでトラフィック インスペクションの中断が発生する可能性があるかどうかが示されます。

  デバイスのこの列のエントリが空白の場合は、展開時にそのデバイス上でのトラフィック インスペクションが中断されないことを示します。

- [最終変更時刻（Last Modified Time）] 列は、最後に設定変更を行った時刻を示します。
- [プレビュー（Preview）] 列では、次の展開の変更をプレビューできます。
- [ステータス（Status）] 列には、各展開のステータスが表示されます。

ステップ 2 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**（[展開矢印（expand arrow）] アイコン [展開矢印（expand arrow）] アイコン） をクリックします。

  デバイスの横にあるチェックボックスをオンにすると、デバイスに加えられ、デバイスの下にリストされているすべての変更が展開のためにプッシュされます。ただし、**ポリシーの選択**（[ポリシーの選択（policy selection）] アイコン [ポリシーの選択（policy selection）] アイコン） を使用して展開する個々のポリシーや特定の設定を選択し、残りの変更は展開せずに保持することができます。

（注）
- [インスペクションの中断（Inspect Interruption）] 列のステータスに [あり（Yes）] と表示され、展開によって 脅威に対する防御 デバイスでインスペクションと、場合によってはトラフィックが中断されるときは、展開されたリストには中断の原因となった特定の設定が **インスペクションの中断**（[インスペクションの中断（inspect interruption）] アイコン [インスペクションの中断（inspect interruption）] アイコン） で示されます。
- インターフェイスグループ、セキュリティゾーン、またはオブジェクトに変更がある場合、影響を受けるデバイスは、Management Center で失効として表示されます。これらの変更が有効になるようにするには、これらのインターフェイスグループ、セキュリティゾーン、またはオブジェクトを含むポリシーも、これらの変更とともに展開する必要があります。影響を受けるポリシーは、Management Center の [プレビュー（Preview）] ページに失効として表示されます。

ステップ 3 [展開（Deploy）] をクリックします。

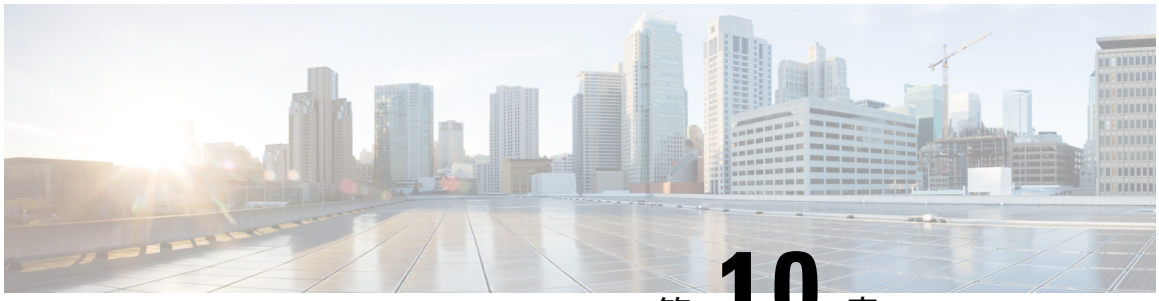
ステップ 4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証メッセージ（Validation Messages）] ウィンドウにその内容が表示されます。完全な詳細を表示するには、警告またはエラーの前にある矢印アイコンをクリックします。

次の選択肢があります。

- [展開（Deploy）]：警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [閉じる（Close）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

次のタスク

展開中に展開が失敗した場合、その障害がトラフィックに影響を与える可能性があります。ただし、特定の条件によって異なります。展開に特定の設定変更がある場合、展開の失敗によってトラフィックが中断されることがあります。詳細については、最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「Deploy Configuration Changes」のトピックを参照してください。



第 10 章

Cisco Secure Firewall Management Center での Snort 3 推奨事項の生成

- Snort 3 ルールの推奨事項 （149 ページ）
- 利点 （150 ページ）
- ビジネスシナリオの例 （150 ページ）
- ベストプラクティス （150 ページ）
- 前提条件 （150 ページ）
- Snort 3 推奨事項の生成 （151 ページ）
- 設定変更の展開 （154 ページ）

Snort 3 ルールの推奨事項

ルールの推奨事項は、ホスト環境に固有のルールを使用して侵入ポリシーを自動的に調整します。ネットワークに存在しない脆弱性のルールを無効にすることで、追加のルールを有効にしたり、現在のルールセットを調整できます。詳細については、Cisco Secure Firewall 推奨ルールの概要 （72 ページ）を参照してください。

動作の仕組み

Management Center は、パッシブ検出を通じて、IP アドレス、ホスト名、オペレーティングシステム、サービス、ユーザー、クライアントアプリケーションなどの詳細を含む、ネットワーク上のホストのデータベースを構築します。この情報に基づいて、システムは検出された各ホストに脆弱性をマッピングします。推奨機能は、このホストデータベースを使用して、環境に適用するルールを決定します。

Snort 3 には 4 つのセキュリティレベルがあり、それぞれが特定の Talos ポリシーに対応しています。その内容は次のとおりです。

- レベル 1：セキュリティよりも接続性を優先（Connectivity Over Security）
- レベル 2：セキュリティと接続性のバランスをとる（Balanced Security and Connectivity）
- レベル 3：接続性よりもセキュリティを優先（Security Over Connectivity）
- レベル 4：最大検出（Maximum Detection）

ネットワーク内のホストで検出されない脆弱性のルールを無効にするには、[ルールを無効にするための推奨事項を受け入れる（Accept Recommendations to Disable Rules）] チェックボックスをオンにします。アラートの数が多いためにルールセットをトリミングする必要がある場合、またはインスペクションのパフォーマンスを向上させる必要がある場合にのみ、このオプションをオンにします。

利点

- 推奨事項を設定することで、侵入ポリシーを調整して、ホスト環境に固有のルールを使用して特定のタイプの脅威をより効果的に検出できます。
- 推奨事項は、誤検出と検出漏れを減らすことで、より効率的で効果的なインシデント対応プロセスに役立ちます。

ビジネスシナリオの例

大規模な企業ネットワークで、主要な侵入検知および防御システムとして Snort 3 を使用しているとします。セキュリティへの脅威が急速に進化する状況では、堅牢なネットワークセキュリティ対策を採用する必要があります。セキュリティチームは、インシデント対応機能を強化したいと考えています。これを行う方法の 1 つは、ホストネットワークで検出された脆弱性に基づいて推奨事項またはルールセットを生成することです。これは、侵入ポリシーを最適化し、ネットワークをより効果的に保護するのに役立ちます。

ベストプラクティス

- 高品質で正確なホストデータが必要です。

  ネットワーク検出はパッシブな性質であるため、脅威防御デバイスは保護されたホストのできるだけ近くに配置する必要があります。これにより、脅威防御デバイスはこれらのホストで送受信されるネットワークトラフィックを監視し、ネットワークに存在するアプリケーション、サービス、および脆弱性に関する正確なデータを提供できます。
- デバイスは、正確なホストプロファイルを作成するために、水平方向（East-West）および垂直方向（North-South）のトラフィックフローを可視化する必要があります。
- スケジュールされたタスクを作成して、推奨事項を自動的に更新できます。

前提条件

- 推奨を生成するホストがシステムに存在することを確認します。

- 推奨事項に設定された保護されたネットワークは、システムに存在するホストにマッピングする必要があります。

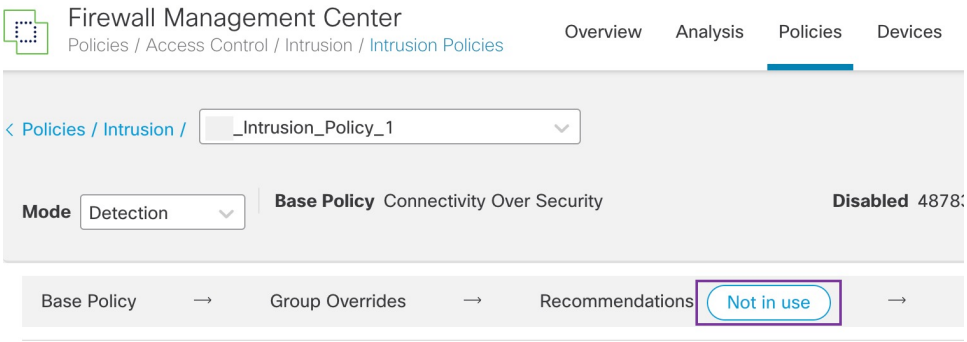
Snort 3 推奨事項の生成

手順

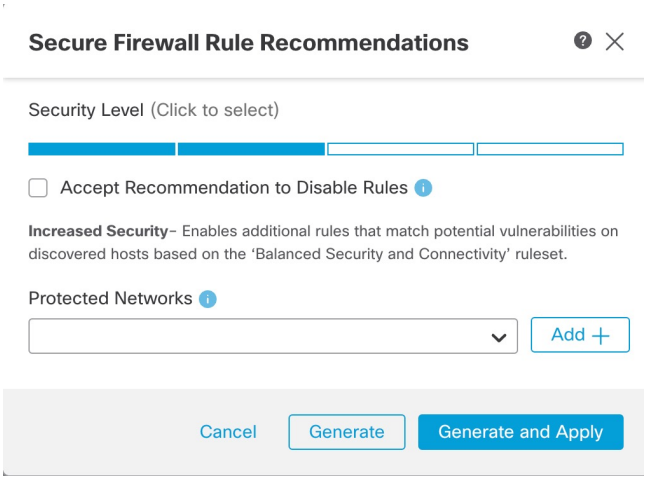
ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

ステップ 2 対応する侵入ポリシーの [Snort 3バージョン（Snort 3 Version）] ボタンをクリックします。

ステップ 3 [推奨事項（未使用）（Recommendations (Not in Use)）] レイヤをクリックして、ルールの推奨事項を設定します。



[シスコ推奨ルール（Cisco Recommended Rules）] ウィンドウで、セキュリティレベルを設定できます。



ステップ 4 クリックして、セキュリティレベルを設定します。

ステップ 5 （オプション）ネットワーク内のホストで検出されない脆弱性用に記述されたルールを無効にするには、[ルールを無効にするための推奨事項を受け入れる（Accept Recommendations to Disable Rules）] チェックボックスをオンにします。

アラートの数が多いためにルールセットをトリミングする必要がある場合、またはインスペクションのパフォーマンスを向上させる必要がある場合にのみ、このオプションを使用します。

ステップ 6 [保護されたネットワーク（Protected Networks）] ドロップダウンリストから、推奨事項によって調べる必要があるネットワークオブジェクトを選択します。デフォルトでは、選択されていない場合、IPv4 または IPv6 ネットワークが選択されます。

[追加+（Add +）] をクリックして、タイプが [ホスト（Host）] または [ネットワーク（Network）] の新しいネットワークオブジェクトを作成し、[保存（Save）] をクリックします。

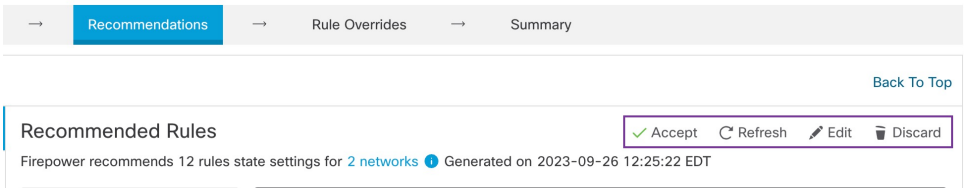
ステップ 7 推奨事項を生成および適用します。

- [生成（Generate）]：侵入ポリシーの推奨事項を生成します。このアクションは、[推奨ルール（未使用）（Recommended Rules (Not in use)）] の下にルールのリストを表示します。
- [生成して適用（Generate and Apply）]：侵入ポリシーの推奨事項を生成して適用します。このアクションは、[推奨ルール（未使用）（Recommended Rules (Not in use)）] の下にルールのリストを表示します。

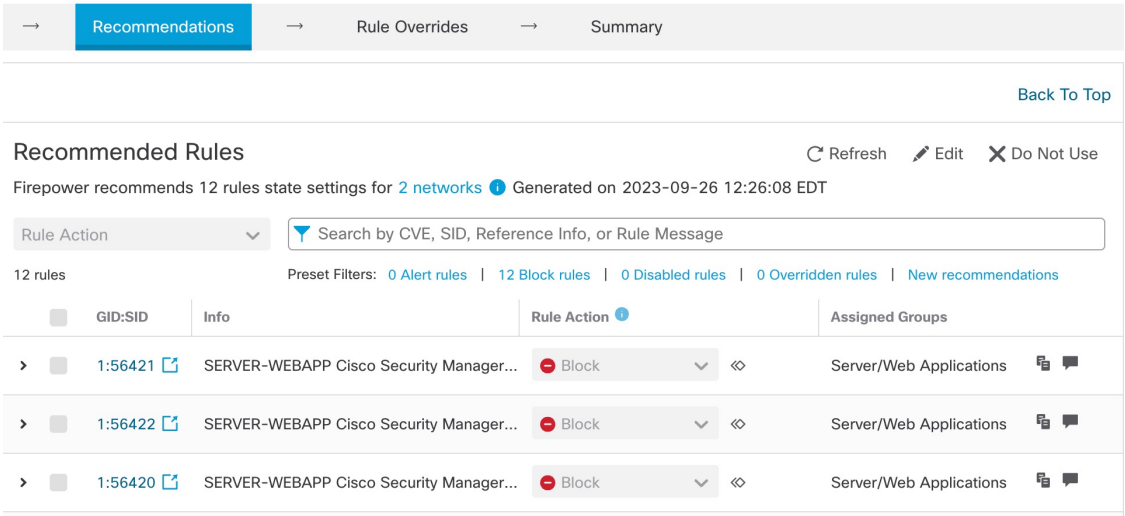
推奨事項が正常に生成されました。すべての推奨ルールと対応する推奨アクションが新しい推奨タブに表示されます。ルールアクションの事前設定フィルタは、新しい推奨事項に加えて、このタブでも使用できます。

ステップ 8 推奨事項を確認し、次のように適用します。

- [受け入れる（Accept）]：生成済みの侵入ポリシーの推奨事項を適用します。
- [更新（Refresh）]：侵入ポリシーのルール推奨事項を再生成および更新します。
- [編集（Edit）]：[推奨事項（Recommendations）] ダイアログボックスが開くので、推奨入力値を入力して推奨事項を生成します。
- [破棄（Discard）]：適用された推奨ルールを元に戻すか、ポリシーから削除し、[推奨事項（Recommendations）] タブも削除します。

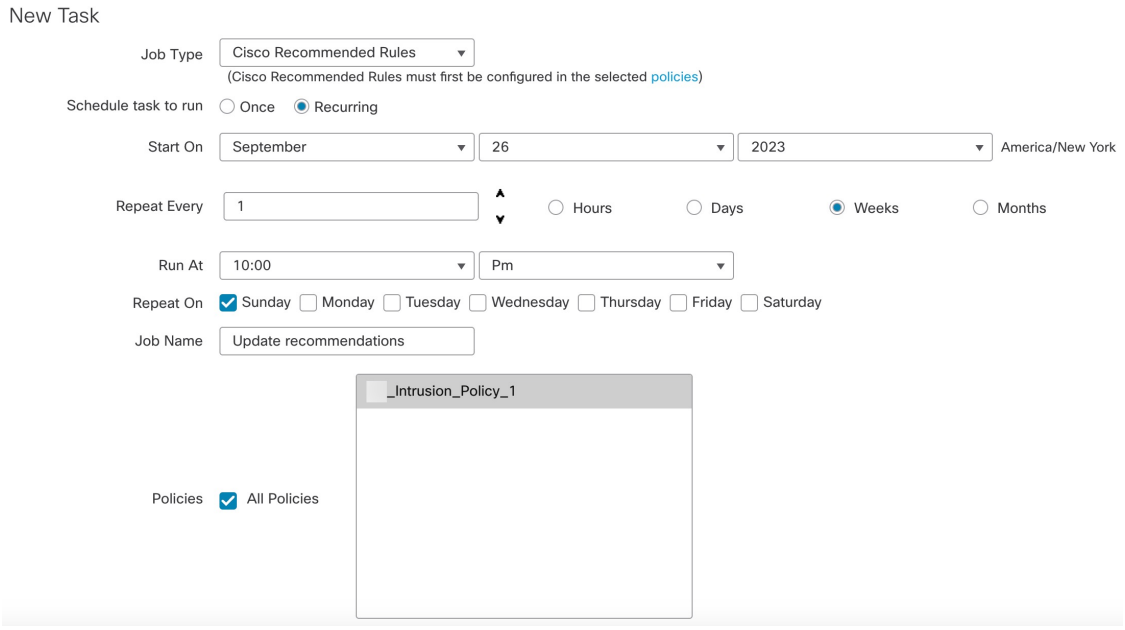


[すべてのルール（All Rules）] の [推奨ルール（Recommended Rules）] セクションに推奨ルールが表示されます。



ステップ 9 推奨事項を効果的に使用するには、定期的に更新する必要があります。次の手順に従ってください。

1. [システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）] の順に選択します。
2. [タスクの追加（Add Task）] をクリックします。
3. [ジョブタイプ（Job Type）] ドロップダウンリストから [シスコ推奨ルール（Cisco Recommended Rules）] を選択します。
4. 必要に応じて、フィールドを更新してください。



5. [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ） を参照してください。

設定変更の展開

設定を変更した後に、影響を受けるデバイスに展開します。

（注） このトピックでは、設定変更を展開する基本的な手順について説明します。手順を進める前に、最新バージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「*Deploy Configuration Changes*」トピックを参照し、変更を展開する上での前提条件と影響を理解しておくことを強く推奨します。

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。

手順

ステップ 1 Secure Firewall Management Center メニューバーで、[展開（Deploy）] をクリックし、[展開（Deployment）] を選択します。

[GUI] ページには、期限切れの設定を持ち、ステータスが [保留中（Pending）] のデバイスのリストが表示されます。

- [変更者（Modified by）] 列には、ポリシーまたはオブジェクトを変更したユーザーの一覧が表示されます。デバイスリストを展開すると、ポリシーリストごとのポリシーを変更したユーザーが表示されます。

  （注） 削除されたポリシーおよびオブジェクトのユーザ名は表示されません。

- [インスペクションの中断（Inspect Interruption）] 列には、展開時にデバイスでトラフィック インスペクションの中断が発生する可能性があるかどうかが示されます。

  デバイスのこの列のエントリが空白の場合は、展開時にそのデバイス上でのトラフィック インスペクションが中断されないことを示します。

- [最終変更時刻（Last Modified Time）] 列は、最後に設定変更を行った時刻を示します。
- [プレビュー（Preview）] 列では、次の展開の変更をプレビューできます。

- [ステータス（Status）] 列には、各展開のステータスが表示されます。

ステップ 2 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**（[展開矢印（expand arrow）] アイコン [展開矢印（expand arrow）] アイコン） をクリックします。

  デバイスの横にあるチェックボックスをオンにすると、デバイスに加えられ、デバイスの下にリストされているすべての変更が展開のためにプッシュされます。ただし、**ポリシーの選択**（[ポリシーの選択（policy selection）] アイコン [ポリシーの選択（policy selection）] アイコン） を使用して展開する個々のポリシーや特定の設定を選択し、残りの変更は展開せずに保持することができます。

  （注）
  - [インスペクションの中断（Inspect Interruption）] 列のステータスに [あり（Yes）] と表示され、展開によって 脅威に対する防御 デバイスでインスペクションと、場合によってはトラフィックが中断されるときは、展開されたリストには中断の原因となった特定の設定が **インスペクションの中断**（[インスペクションの中断（inspect interruption）] アイコン [インスペクションの中断（inspect interruption）] アイコン） で示されます。
  - インターフェイスグループ、セキュリティゾーン、またはオブジェクトに変更がある場合、影響を受けるデバイスは、Management Center で失効として表示されます。これらの変更が有効になるようにするには、これらのインターフェイスグループ、セキュリティゾーン、またはオブジェクトを含むポリシーも、これらの変更とともに展開する必要があります。影響を受けるポリシーは、Management Center の [プレビュー（Preview）] ページに失効として表示されます。

ステップ 3 [展開（Deploy）] をクリックします。

ステップ 4 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。

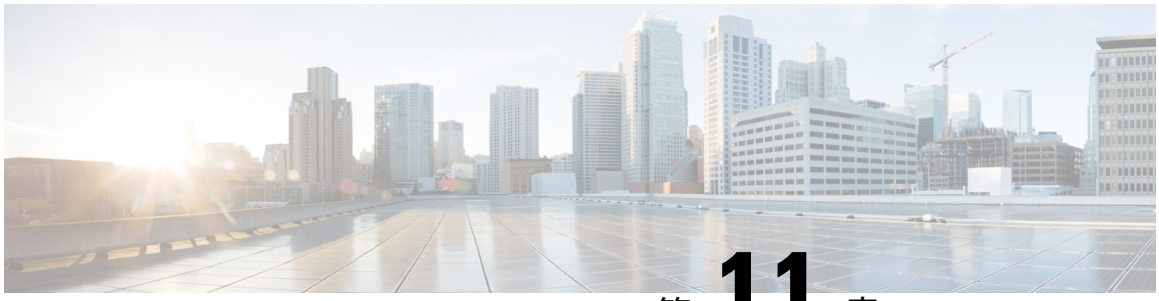
次の選択肢があります。

- [展開（Deploy）]：警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [閉じる（Close）]：展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

次のタスク

展開中に展開が失敗した場合、その障害がトラフィックに影響を与える可能性があります。ただし、特定の条件によって異なります。展開に特定の設定変更がある場合、展開の失敗によってトラフィックが中断されることがあります。詳細については、最新バージョンの『*Cisco*

Secure Firewall Management Center Configuration Guide』の「Deploy Configuration Changes」のトピックを参照してください。



第 11 章

EVEの脅威の確実性スコアに基づいてトラフィックをブロックする

- Encrypted Visibility Engine について （157 ページ）
- 利点 （157 ページ）
- ビジネスシナリオの例 （157 ページ）
- 前提条件 （158 ページ）
- ワークフローの概要 （158 ページ）
- EVE でのブロックしきい値の設定 （158 ページ）
- その他の参考資料 （162 ページ）

Encrypted Visibility Engine について

Encrypted Visibility Engine（EVE）を使用すると Transport Layer Security（TLS）暗号化を使用するクライアント アプリケーションとプロセスを識別できます。EVE は、復号せずに暗号化されたセッションの可視性を高めます。EVE の結果に基づいて、管理者は環境内のトラフィックにポリシーアクションを適用できます。また、EVE を使用してマルウェアを特定して阻止することもできます。

利点

管理者は EVE の脅威スコアを活用し、調整して、悪意のある暗号化トラフィックをブロックできます。着信トラフィックが悪意のある可能性がある場合は、脅威スコアに基づいて、接続をブロックするように EVE を設定できます。

ビジネスシナリオの例

大規模な企業ネットワークで、主要な侵入検知および防御システムとして Snort 3 を使用しているとします。セキュリティへの脅威が急速に進化する状況では、堅牢なネットワークセキュリティ対策の採用が必要かつ重要です。セキュリティチームは EVE を使用して、完全な中間

者（MITM）復号を実装することなく、暗号化されたトラフィックの検査を強化します。EVE テクノロジーは、既知の悪意のあるプロセスのフィンガープリントを使用して、マルウェアを特定して阻止します。ネットワーク管理者は、設定されたブロックしきい値に基づいて、悪意のある可能性がある接続をブロックするために、EVE のブロックトラフィックしきい値を柔軟に設定できる必要があります。

前提条件

- Management Center 7.4.0 以降を実行している必要があり、管理対象 Threat Defense も 7.4.0 以降である必要があります。
- 有効な侵入防御システム（IPS）ライセンスがあり、Snort 3 が検出エンジンであることを確認します。

ワークフローの概要

1. EVE は着信トラフィックを分析し、着信トラフィックがマルウェアであるかどうかを判定します。
2. EVE が着信トラフィックを特定の信頼度でマルウェアであると検出した場合、そのトラフィックをブロックするように EVE を設定できます。
3. パケットのマルウェア確率または脅威スコアが最初にチェックされ、脅威スコアが設定済みのブロックしきい値と比較されます。
4. 脅威スコアが設定済みのしきい値よりも高い場合、EVE はトラフィックをブロックします。
5. 脅威スコアが設定済みのしきい値よりも小さい場合、EVE はアクションを実行しません。

EVE でのブロックしきい値の設定

この手順では、90% 以上の EVE の脅威の確実性スコアに基づいて、悪意のある可能性があるトラフィックをブロックする方法を示します。

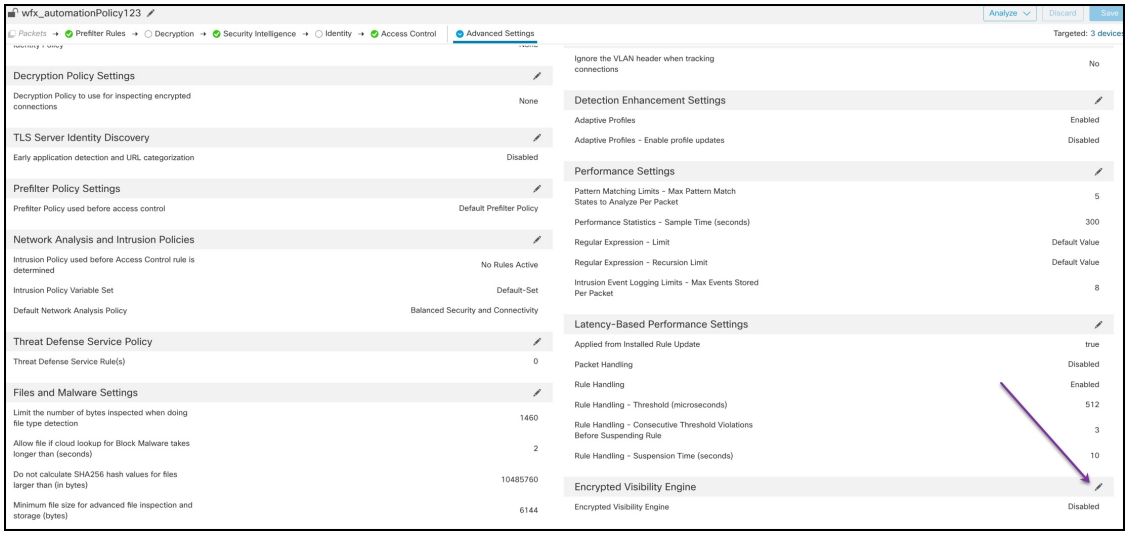
手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択します。

ステップ 2 編集するアクセス コントロール ポリシーの横にある [編集（Edit）]（✎）をクリックします。

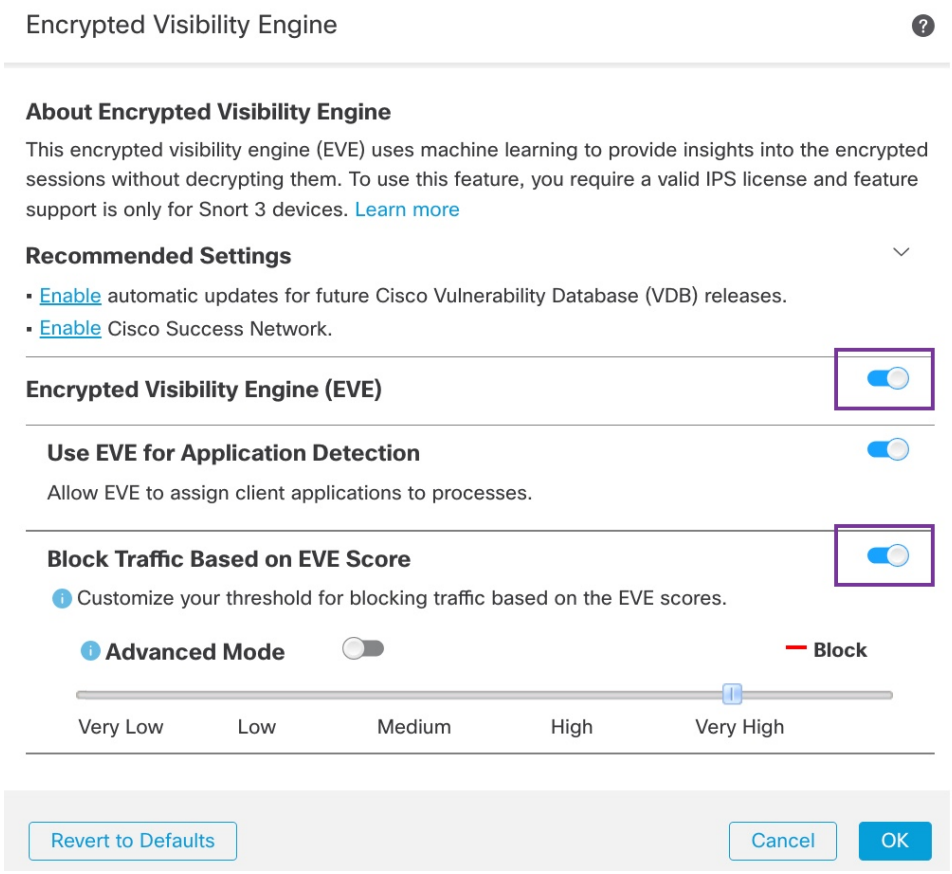
ステップ 3 パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 4 [Encrypted Visibility Engine] の横にある [編集（Edit）]（✎）をクリックします。



ステップ 5 [Encrypted Visibility Engine] ページで、[Encrypted Visibility Engine (EVE)] トグルボタンを有効にします。

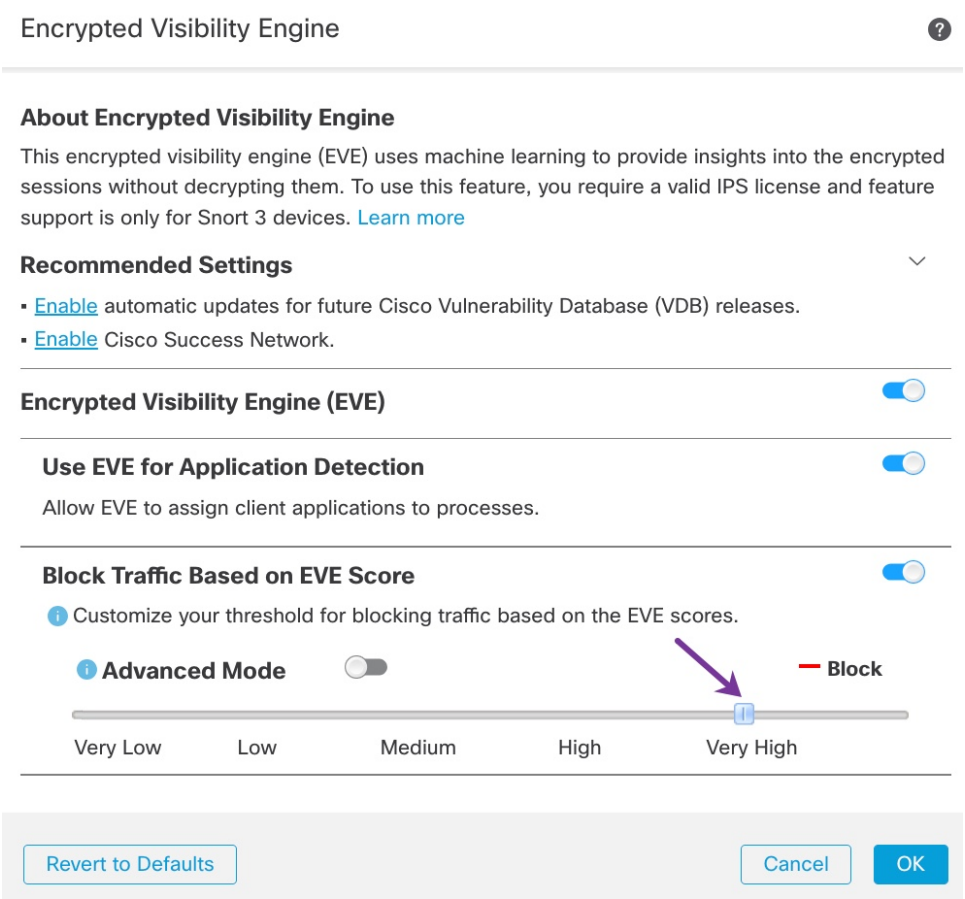
ステップ 6 [EVEスコアに基づいてトラフィックをブロック（Block Traffic Based on EVE Score）] トグルボタンを有効にします。潜在的な脅威である着信トラフィックは、デフォルトでブロックされます。



（注） デフォルトでは、マルウェアがブロックされるしきい値は99%です。これは、次のことを意味します。

- EVE がトラフィックを 99% 以上の確実性でマルウェアであると検出した場合、EVE はトラフィックをブロックします。
- EVE がトラフィックを 99% 未満の確実性でマルウェアであると検出した場合、EVE は何も実行しません。

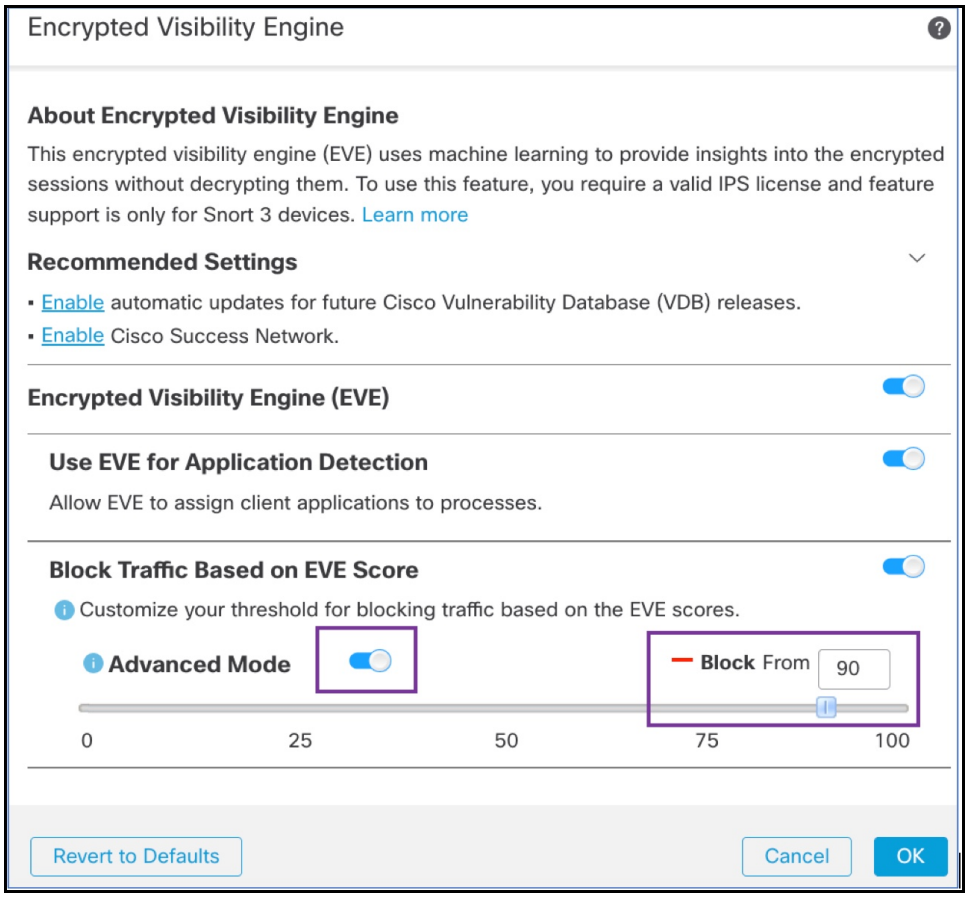
ステップ 7 スライダを使用して、EVE の脅威の確実性に基づいたブロックのしきい値を調整します。この範囲は、[非常に低い（Very Low）] から [非常に高い（Very High）] です。この例では、スライダは [非常に高い（Very High）] に設定されています。



ステップ 8 さらに細かく制御するには、[詳細モード（Advanced Mode）] トグルボタンを有効にします。これで、トラフィックをブロックするための特定の EVE 脅威確実性スコアを割り当てることができるようになりました。デフォルトのしきい値は、99 % です。

ステップ 9 この例では、ブロックしきい値を **90**% に変更します。

注目 ベストプラクティスとして、最適なパフォーマンスを確保するために、ブロックしきい値を 50% 未満に設定しないことを推奨します。



ステップ 10 [OK] をクリックします。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

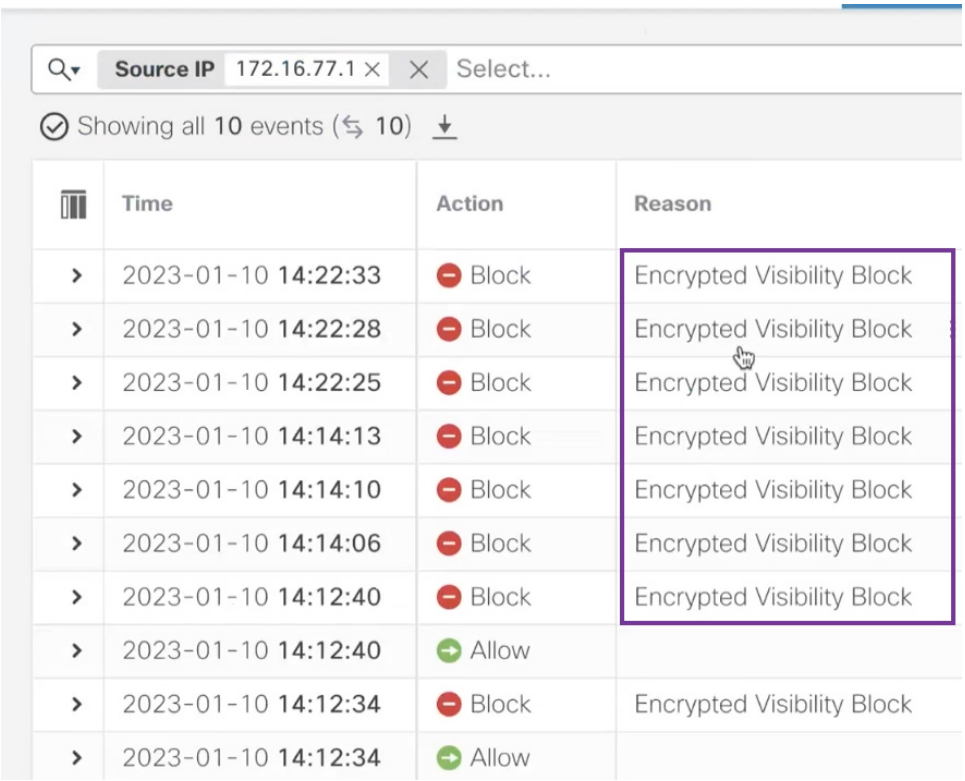
設定変更を展開します。設定変更の展開 （30 ページ） を参照してください。

EVE イベントの表示

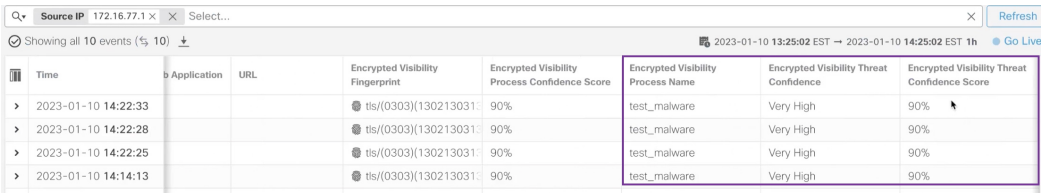
手順

ステップ 1 ブロックアクションを確認するには、**[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]** の順に選択します。[統合されたイベント（Unified Events）] ビューアからイベントを表示することもできます。

ステップ 2 トラフィックをブロックするように EVE を設定した場合、[理由（Reason）] フィールドには [Encrypted Visibilityブロック（Encrypted Visibility Block）] と表示されます。



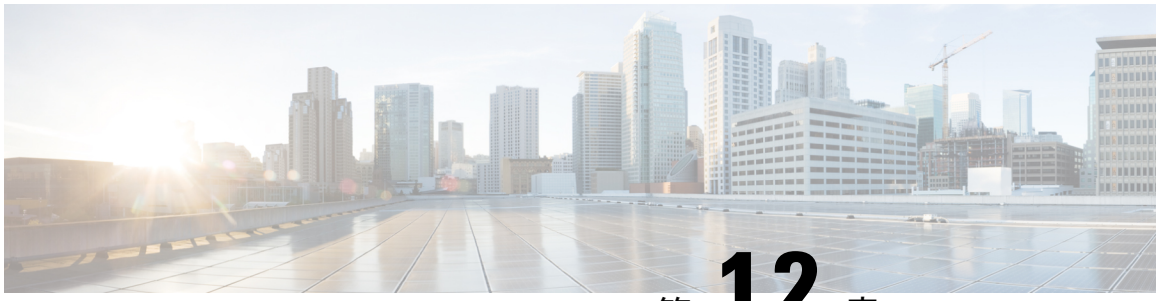
ステップ 3 次に、[Encrypted Visibilityプロセス名（Encrypted Visibility Process Name）] が **test_malware**、[Encrypted Visibility脅威の確実性（Encrypted Visibility Threat Confidence）] が [非常に高い（Very High）]、[Encrypted Visibility脅威の確実性スコア（Encrypted Visibility Threat Confidence Score）] が **90%** の例を示します。



その他の参考資料

概念の詳細については、このガイドの「Snort 3 向けの Encrypted Visibility Engine」の章または次のリンクの内容を参照してください。

暗号化された可視性エンジン



第 12 章

エレファントフロー検出結果の設定

- エレファントフローについて （163 ページ）
- エレファントフローの検出と修復の利点 （163 ページ）
- エレファントフローのワークフロー （164 ページ）
- ビジネスシナリオの例 （164 ページ）
- 前提条件 （165 ページ）
- エレファント フロー パラメータの設定 （165 ページ）
- エレファントフロー修復除外の設定 （169 ページ）
- その他の参考資料 （172 ページ）

エレファントフローについて

エレファントフローは（合計バイト数が）非常に大きく、ネットワークリンク上で測定される、TCP（または他のプロトコル）フローによって設定される比較的長期間実行されるネットワーク接続です。デフォルトでは、エレファントフローとは 1 GB/10 秒を超えるフローまたは接続です。これらのフローは、Snort コアでのパフォーマンス拘束または問題の原因となります。エレファントフローは、過剰な量の CPU リソースを消費し、検出リソースの他の競合フローに影響を与え、遅延やパケットドロップの増加などの問題を引き起こす可能性があるため、重要です。

エレファントフローの検出と修復の利点

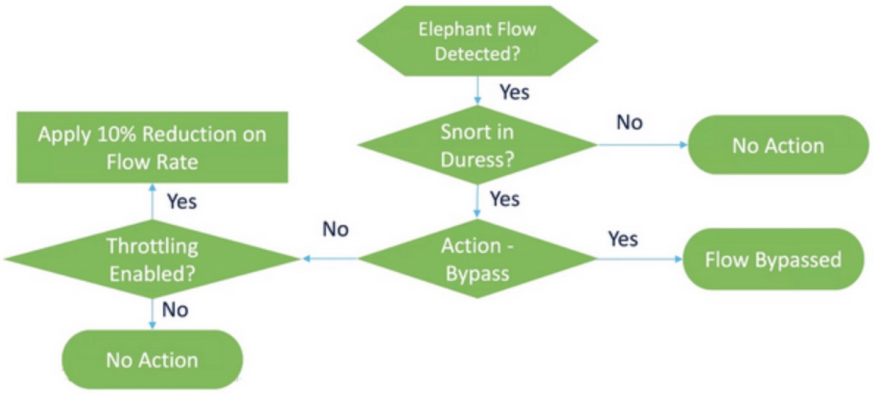
- エレファントフロー設定により、カスタマイズと、エレファントフローをバイパスまたはスロットルするオプションが可能になります。
- 信頼できるトラフィックをバイパスしながら、疑わしいトラフィックの Snort インスペクションを提供するために、選択したアプリケーションに基づいてフローをバイパスまたはスロットルすることを選択できます。
- エレファントフロー修復は、特定の要件に応じて、内部アプリケーション用に優先順位を付けて、より多くの帯域幅を解放するのに役立ちます。

エレファントフローのワークフロー

設定されたパラメータに基づいてエレファントフローが検出された場合、フローをバイパスするかスロットルするかを選択できます。フローがバイパスされると、トラフィックは Snort インスペクションなしで通過できます。スロットリングは、フローのスループットが減少することを意味します。フローレートの削減は、CPU 使用率が設定済みしきい値を下回るまで 10% ずつ減少します。バイパスまたはスロットリングは、エレファントフローが特定され、追加の CPU および時間枠パラメータが満たされた後に行われます。許可ルールで設定済みの場合、エレファントフローを識別する前に、侵入ポリシーはフローを処理します。これは、ほとんどの攻撃が接続の非常に早い段階で検出されるため、エレファントフローが完全に未検査の状態でシステムを通過できないことを意味します。

フローの処理方法を理解するには、次のフロー図を参照してください。

図 *3:* エレファントフローのワークフロー



システムが Snort の抑制状態（パフォーマンスの問題）を検出しない限り、アクションは実行されません。システムは、フローが大きいという理由だけでフローをスロットルまたはバイパスしません。また、スロットルとバイパスのアクションは相互に排他的です。つまり、フローをバイパスまたはスロットルすることはできますが、両方を行うことはできません。

抑制の原因となるすべてのエレファントフローをバイパスしたくない場合は、バイパスオプションを特定のアプリケーションのみに制限できます。パフォーマンスをスロットリングすることなく、信頼するアプリケーションの接続を優先することができます。バイパスする必要があるアプリケーションを設定できますが、残りのフロー（抑制の原因となる）はスロットリングされます。これにより、他の信頼できないアプリケーションフローは、帯域幅が削減されても、引き続き完全な Snort インスペクションを受信します。

ビジネスシナリオの例

データセンターでは、クラスタ間のデータのレプリケーション、仮想マシンの統合、データベースのバックアップなど、いくつかのアクティビティが発生しています。組織内のユーザーは、OTT でビデオを視聴したり、ダウンロードしたりしている可能性があります。このような

アクティビティによる帯域幅の利用は、エレファントフローを引き起こし、ネットワークの速度を低下させ、重要なタスクのパフォーマンスに影響を与える可能性があります。ネットワーク管理者（特定の要件によっては異なります）として、帯域幅の問題を引き起こしている大規模なフローを可視化し、それらを修復する必要があります。

たとえば、エレファント フロー パラメータを設定して、Webex トラフィック（組織がリアルタイムのビデオ会議に使用）の Snort インスペクションをバイパスし、その他のアプリケーションまたは接続（ビデオ、映画など）をスロットリングする方法を見てみましょう。

前提条件

- Management Center 7.2.0 以降を実行していること、および管理対象の Threat Defense も 7.2.0 以降であることを確認します。
- エレファントフロー検出を有効にするだけでは、追加の接続イベントは生成されません。エレファントフロー検出は、すでに Management Center のログに記録されている一致する接続にエレファントフロー表記を追加します。**これらのイベントをログに記録するには、アクセス コントロール ポリシーで接続ロギングを有効にする必要があります。**特定のルールに対してこれを行うか、エレファントフローを含むすべての接続をログに記録するモニタールールを追加できます。

エレファント フロー パラメータの設定

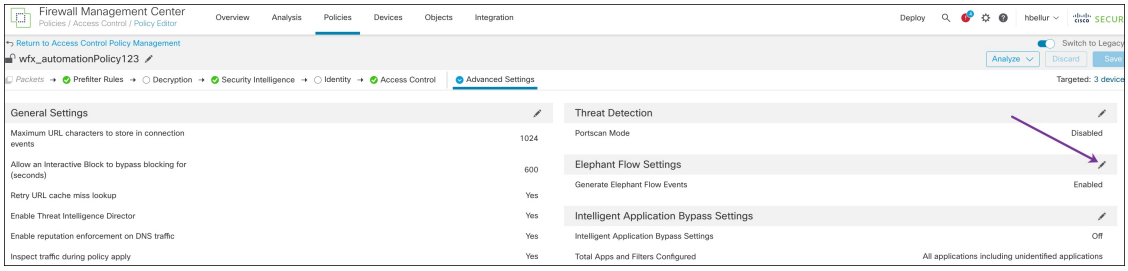
手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）]** を選択します。

ステップ 2 編集するアクセス コントロール ポリシーの横にある [編集（Edit）]（✎）をクリックします。

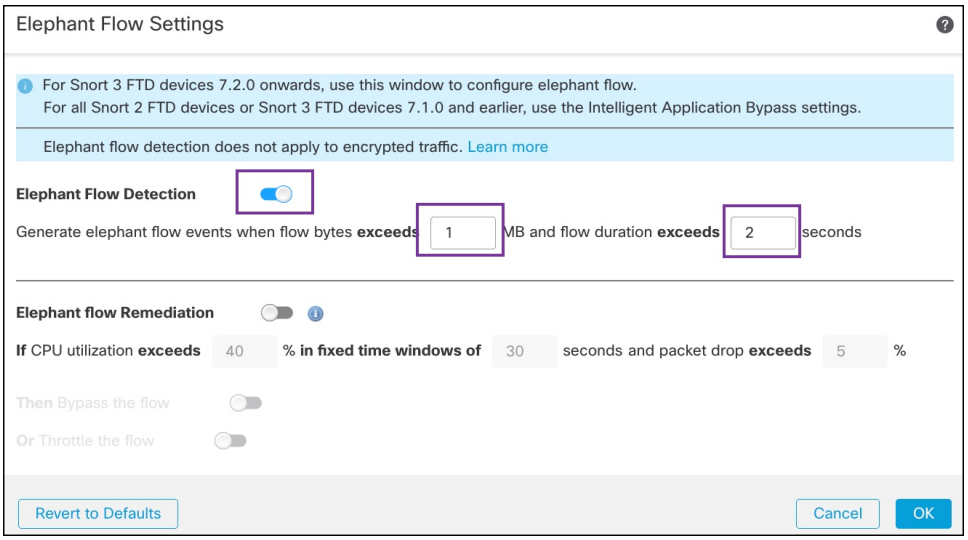
ステップ 3 パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] を選択します。

ステップ 4 [エレファントフロー設定（Elephant Flow Settings）] の横にある [編集（Edit）]（✎）をクリックします。



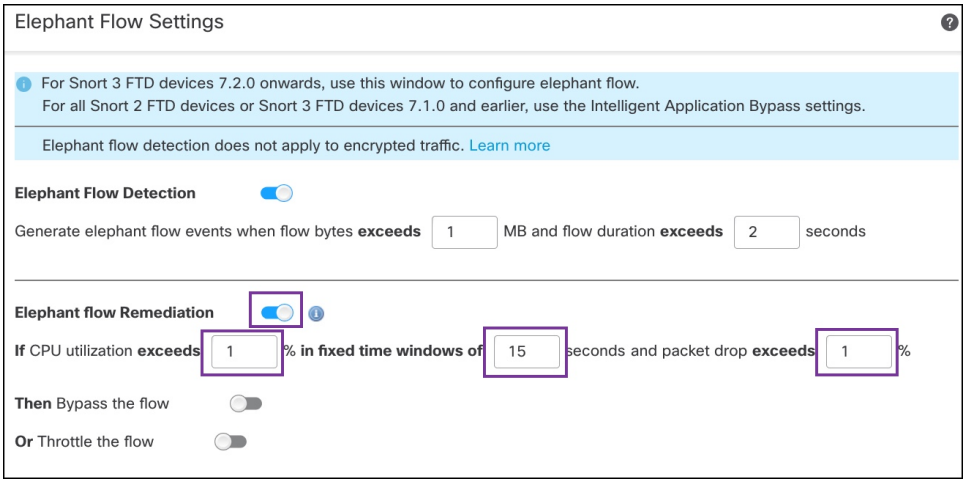
ステップ 5 [エレファントフロー検出（Elephant Flow Detection）] トグルボタンはデフォルトで有効になっています。デフォルト設定では、検出のみが有効になり、デフォルトアクションは設定されません。検出設定では、システム内のエレファントフローを識別できるように、フローのバイト数と期間を調整できます。

テスト設定として、次の図に示すように、フローのバイト数と期間のパラメータを設定します。

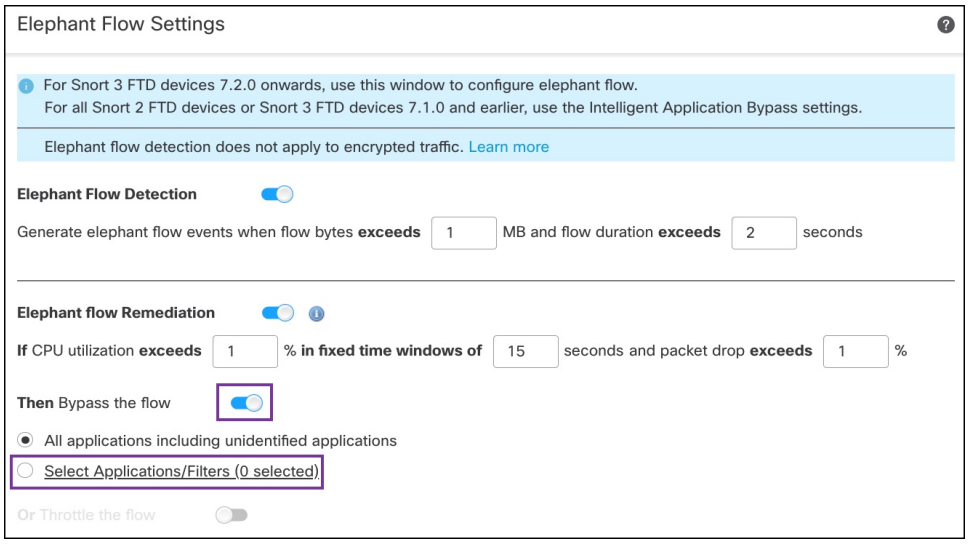


ステップ 6 [エレファントフローの修復（Elephant Flow Remediation）] トグルボタンを有効にします。エレファントフローが検出された場合、フローをバイパスするかスロットルするかを選択できます。フローのバイパスとは、トラフィックが Snort インスペクションなしで通過できることを意味します。スロットリングは、フローのスループットが減少することを意味します。このレートは、CPU 使用率が設定済みしきい値を下回るまで 10% ずつ減少します。

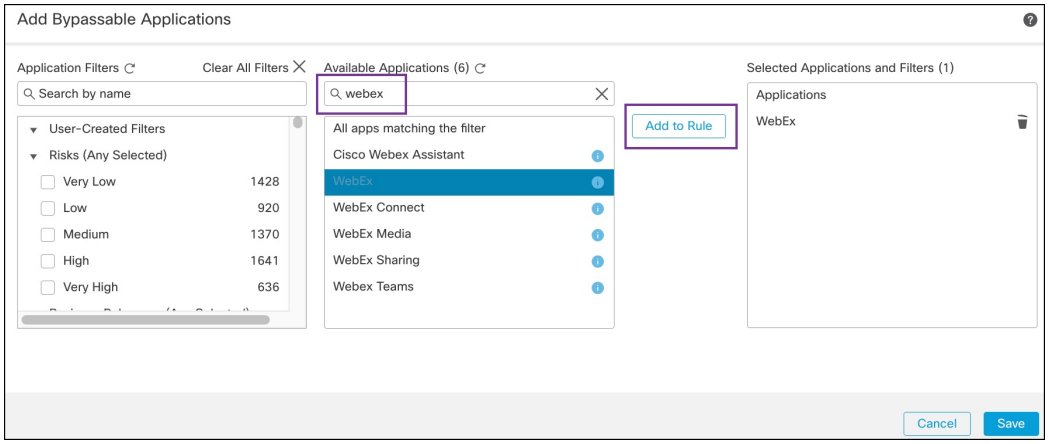
テスト設定として、次の図に示すようにエレファントフロー修復パラメータを設定します。



ステップ 7 [フローのバイパス（Bypass the flow）] トグルボタンを有効にし、[アプリケーション/フィルタの選択（Select Applications/Filters）] ラジオボタンをクリックします。



ステップ 8 [アプリケーションフィルタ（Application Filters）] で、**Webex** アプリケーションを検索して選択し、ルールに追加して [保存（Save）] をクリックします。つまり、設定されたパラメータに基づいて、これらの Webex 接続がエレファントフローとして検出された場合、Webex 接続は信頼され、優先されるため、Snort インスペクションがスキップされます。



ステップ 9 [スロットル（Throttle）] トグルボタンを有効にして、残りのフローをスロットルします（抑制の原因となります）。これにより、Snort の抑制条件が満たされるまで、他のすべてのフローの速度が 10% ずつ低下します。

ステップ 10 [OK] をクリックします。

ステップ 11 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開 （30 ページ） を参照してください。

エレファントフローのイベントの表示

エレファントフロー設定を構成した後、接続イベントをモニターして、フローが検出、バイパス、またはスロットリングされているかどうかを確認します。この情報は、接続イベントの [理由（Reason）] フィールドで確認できます。エレファントフロー接続の 3 つのタイプは次のとおりです。

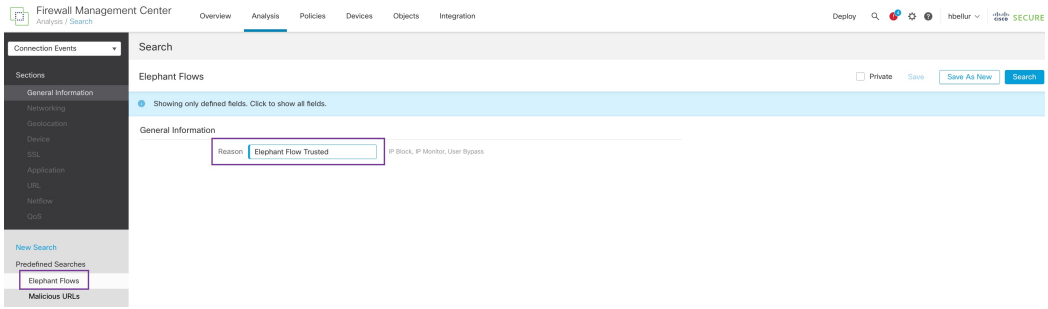
- エレファントフロー（Elephant Flow）
- エレファントフローがスロットリングされている（Elephant Flow Throttled）
- エレファントフローが信頼されている（Elephant Flow Trusted）

手順

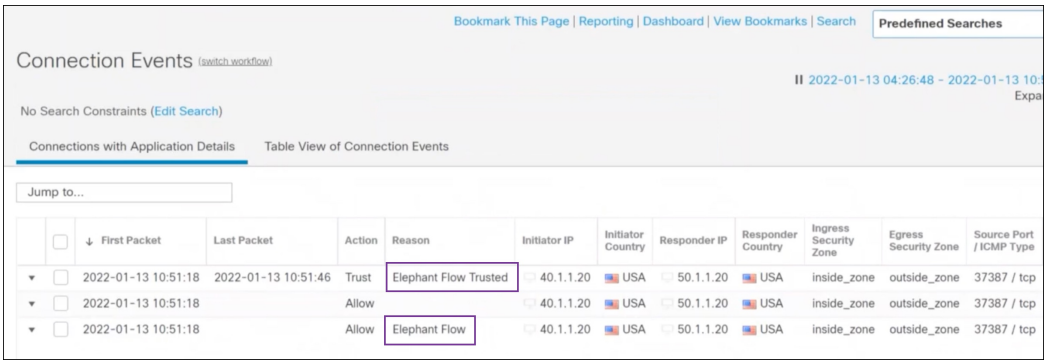
ステップ 1 **[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]**を選択します。[統合されたイベント（Unified Events）] ビューアからイベントを表示することもできます。

ステップ 2 [接続イベント（Connection Events）] ページで、[定義済み検索（Predefined Search）] ドロップダウンリストから [エレファントフロー（Elephant Flows）] を選択してエレファントフローイベントを表示します。

ヒント　**Elephant Flow Trusted** または **Elephant Flow Throttled** のイベントタイプを表示するには、ページの左上隅にある [検索の編集（Edit Search）] リンクをクリックし、[理由（Reason）] フィールドで、左側のパネルの [エレファントフロー（Elephant Flows）] を選択します。検索する内容に応じて、**Elephant Flow Trusted** または **Elephant Flow Throttled** と入力します。



ステップ 3 フローの途中で検出されたエレファントフローを表示すると、[理由（Reason）] フィールドに [エレファントフロー（Elephant Flow）] と表示されます。フローの最後にバイパスされると、[理由（Reason）] フィールドに [エレファントフローが信頼されている（Elephant Flow Trusted）] と表示されます。



エレファントフロー修復除外の設定

修復から除外する必要があるフローのL4アクセス制御リスト（ACL）ルールを設定できます。フローがエレファントフローとして検出され、それが、定義されたルールに一致する場合、そのフローは修復アクションから除外されます。

始める前に

Management Center 7.4.0 以降を実行している必要があり、管理対象 Threat Defense も 7.4.0 以降である必要があります。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）]** を選択します。

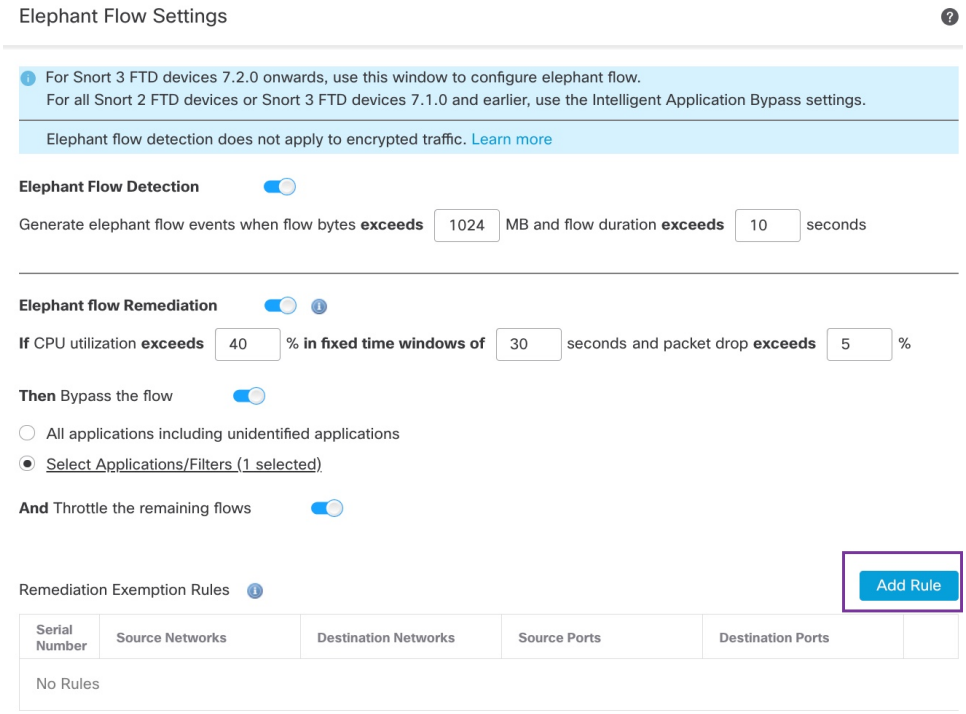
ステップ 2 編集するアクセス コントロール ポリシーの横にある [編集（Edit）]（✎）をクリックします。

ステップ 3 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 [詳細設定（Advanced Settings）] を選択します。

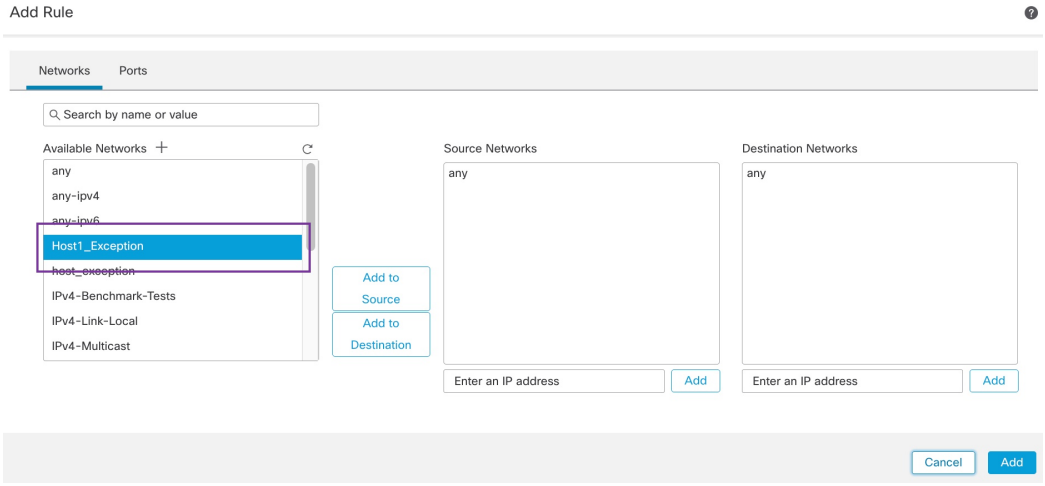
ステップ 4 [エレファントフロー設定（Elephant Flow Settings）] の横にある [編集（Edit）]（✎）をクリックします。

ステップ 5 エレファントフロー検出および修復パラメータが設定されていることを確認します。エレファントフローパラメータの設定 （165 ページ） を参照してください。

ステップ 6 [修復除外ルール（Remediation Exemption Rules）] の横にある [ルールの追加（Add Rule）] ボタンをクリックします。



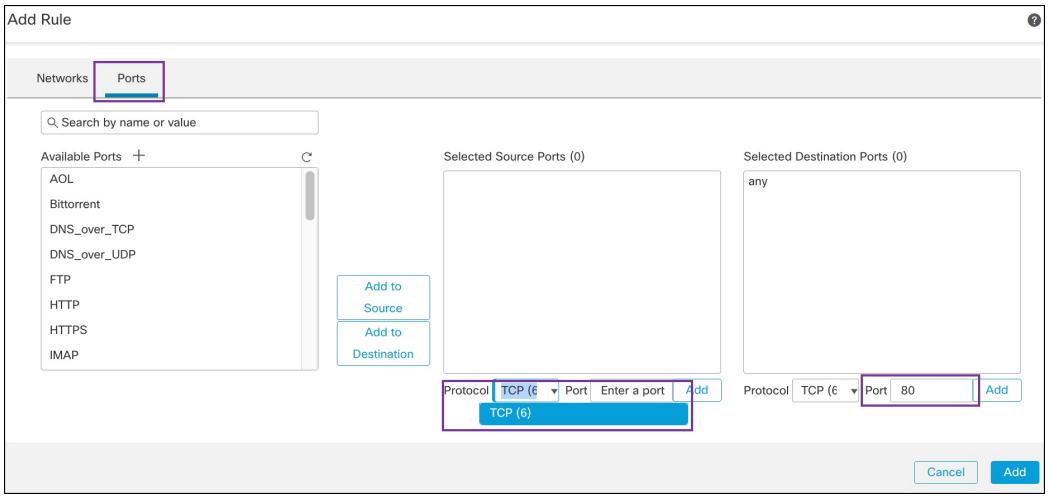
ステップ 7 [使用可能なネットワーク（Available Networks）] のリストから、エレファントフロー修復から除外する設定済みホストを選択します。この例では、「Host1_Exception」というホストを作成しました。



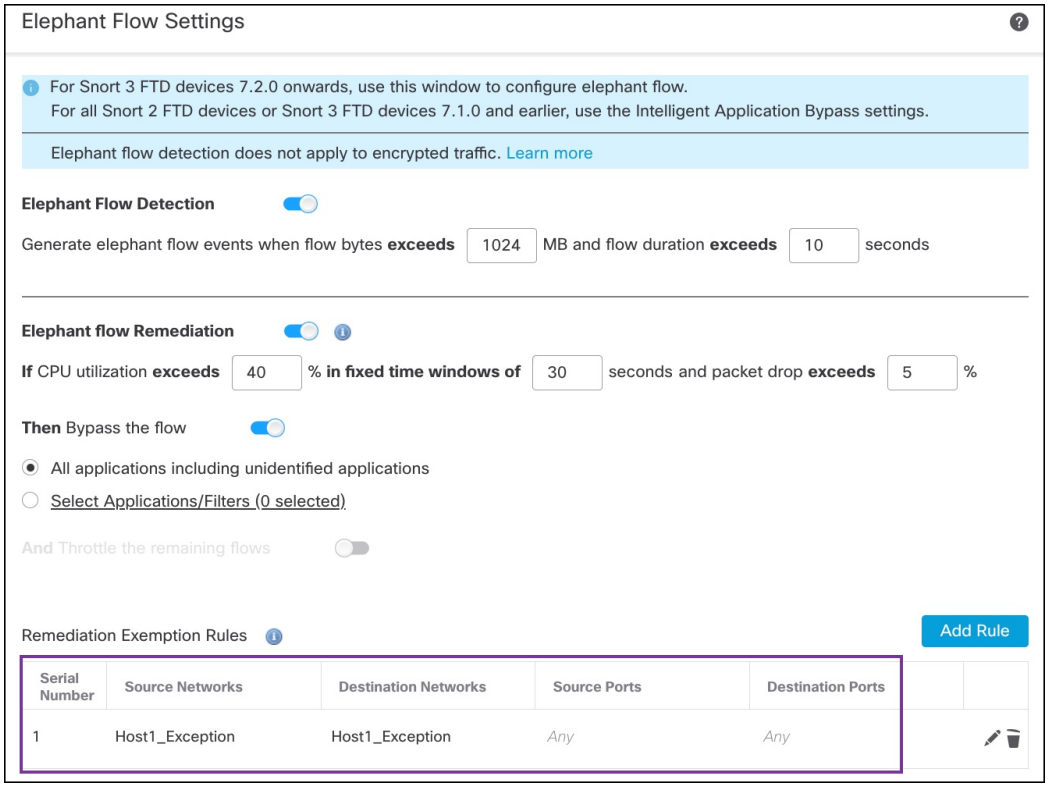
ステップ 8 必要に応じて、[送信元に追加（Add to Source）] または [宛先に追加（Add to Destination）] をクリックして、このホストを送信元または宛先に追加します。

ステップ 9 [ポート（Ports）] タブをクリックします。

ステップ 10 送信元ポートとして、[プロトコル：TCP（Protocol as TCP）] を選択し、宛先ポートとして **80** を入力し、[追加（Add）] をクリックします。



ステップ 11 [OK] をクリックします。



ステップ 12 [保存（Save）] をクリックします。

次のタスク

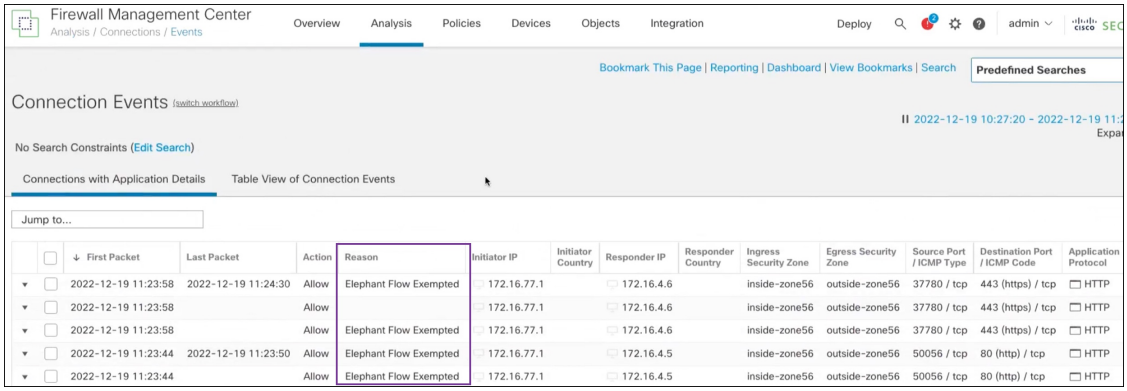
設定変更を展開します。設定変更の展開 （30 ページ） を参照してください。

エレファントフロー修復除外のイベントの表示

手順

ステップ 1 **[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]**を選択します。[統合されたイベント（Unified Events）] ビューアからイベントを表示することもできます。

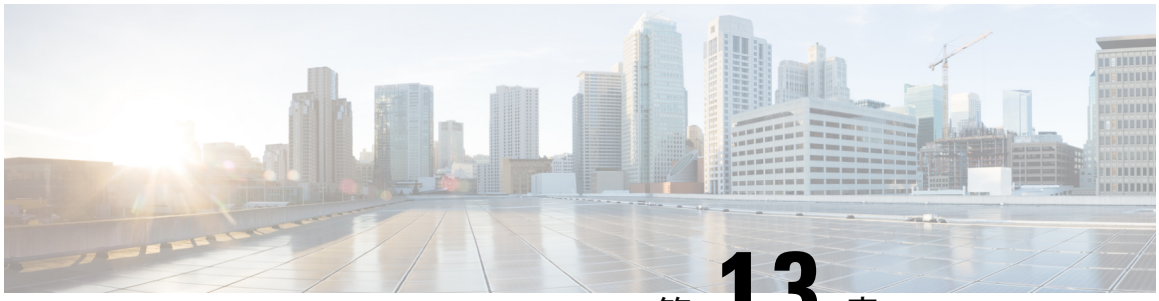
ステップ 2 修復から除外されたエレファントフローを表示します。[理由（Reason）] フィールドに [エレファントフロー除外（Elephant Flow Exempted）] と表示されます。



その他の参考資料

概念の詳細については、このガイドの「Snort 3 のエレファントフロー検出」の章または次のリンクの内容を参照してください。

- エレファントフローの検出



第 13 章

Snort 3 侵入ポリシーでの MITRE フレームワークを使用した脅威の軽減

- MITRE ATT&CK フレームワークについて （173 ページ）
- MITRE フレームワークの利点 （174 ページ）
- MITRE ネットワークのビジネスシナリオの例 （174 ページ）
- MITRE フレームワークの前提条件 （174 ページ）
- Snort 3 侵入ポリシーの表示と編集 （175 ページ）
- 侵入イベントの表示 （179 ページ）
- その他の参考資料 （182 ページ）

MITRE ATT&CK フレームワークについて

MITRE ATT&CK フレームワークは、攻撃者がシステムを侵害するために使用する戦術、手法、および手順（TTP）の概要を示す包括的なナレッジベースです。これらの TTP をさまざまなオペレーティングシステムとプラットフォームのマトリックスに編成し、各攻撃段階（戦術）を特定の方法（手法）にマッピングします。各手法には、実行、手順、防御、検出、および実際の例に関する情報が含まれています。

（注） MITRE ATT&CK に関するその他の情報については、https://attack.mitre.org [英語] を参照してください。

Management Center では、MITRE ATT&CK フレームワークを使用して脅威検出と対応が強化されており、次の機能が組み込まれています。

- 侵入イベントには TTP が含まれます。これにより、管理者は、脆弱性タイプ、ターゲットシステム、または脅威カテゴリに従ってルールをグループ化して、より緻密にトラフィックを管理できるようになります。
- TTP を使用するマルウェアイベントを選択して、脅威を検出して対応する機能を強化できます。

MITRE フレームワークの利点

- MITREの戦術、手法、および手順（TTP）が侵入イベントに追加されることで、管理者はMITRE ATT&CK フレームワークに基づいてトラフィックに対処できるようになります。これにより、管理者はトラフィックをより細かく表示および処理でき、脆弱性タイプ、ターゲットシステム、または脅威カテゴリ別にルールをグループ化することができます。
- MITRE ATT&CK フレームワークに従って侵入ルールを編成できます。これにより、特定の攻撃者の戦術と手法に応じてポリシーをカスタマイズできます。

MITRE ネットワークのビジネスシナリオの例

大規模な企業ネットワークで、主要な侵入検知および防御システムとして Snort 3 を使用しているとします。セキュリティへの脅威が急速に進化する状況では、堅牢なネットワークセキュリティ対策の採用が必要かつ重要です。ネットワーク管理者は、設定されたポリシーで対象のトラフィックが検出されているかどうかと、既知の攻撃グループがトラッキングされているかどうかを知る必要があります。たとえば、攻撃者がシステムまたはアプリケーションの弱点を利用して、予期しない動作を引き起こそうとしているかどうかを知る必要がある場合があります。考えられるシステムの弱点には、バグ、グリッチ、または設計上の脆弱性があります。考えられるアプリケーションには、Web サイト、データベース、サーバーメッセージブロック（SMB）やセキュアシェル（SSH）などの標準サービス、ネットワークデバイスの管理プロトコル、または Web サーバーや関連サービスなどのアプリケーションがあります。

MITRE フレームワークによって提供されるインサイトにより、管理者は特定の資産の保護を指定し、特定の脅威グループからネットワークを保護するための、より適切な機会を得ることができます。

MITRE フレームワークの前提条件

- Cisco Secure Firewall Management Center および Cisco Secure Firewall Threat Defense バージョン 7.3.0 以降を Snort 3 とともに実行している必要があります。
- 少なくとも 1 つの侵入ポリシーが必要です。カスタム Snort 3 侵入ポリシーの作成 （37 ページ） を参照してください。

Snort 3 侵入ポリシーの表示と編集

手順

ステップ 1 **[ポリシー（Policies）] > [侵入（Intrusion）]** を選択します。

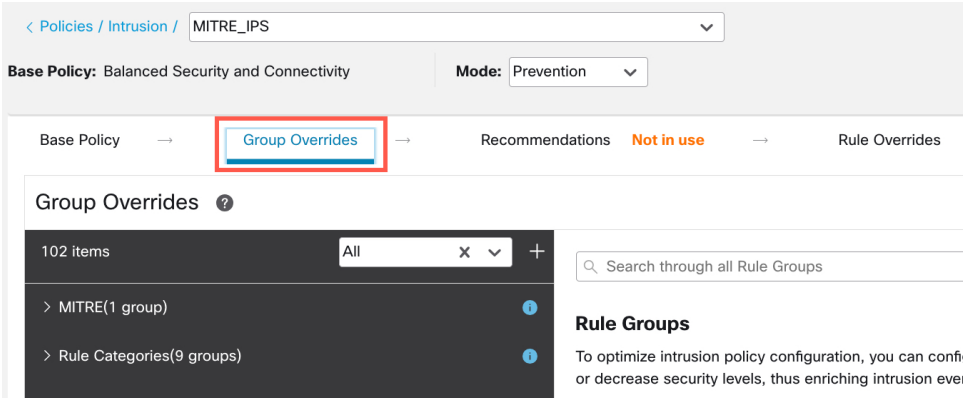
ステップ 2 [侵入ポリシー（Intrusion Policies）] タブが選択されていることを確認します。

ステップ 3 表示または編集する侵入ポリシーの横にある [Snort 3バージョン（Snort 3 Version）] をクリックします。

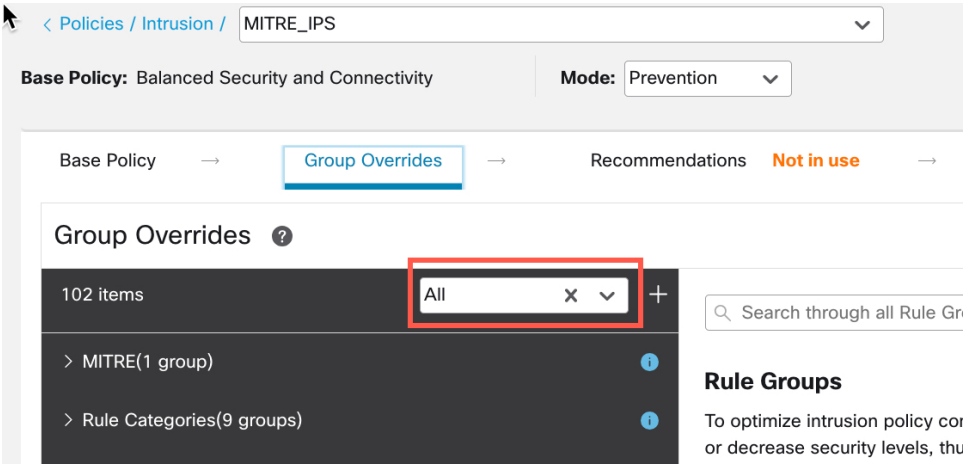
ステップ 4 表示された Snort ヘルパーガイドを閉じます。

ステップ 5 [グループのオーバーライド（Group Overrides）] レイヤをクリックします。

このレイヤには、ルールグループのすべてのカテゴリが階層構造で一覧表示されます。各ルールグループで、最後のリーフルールグループまでドリルダウンできます。

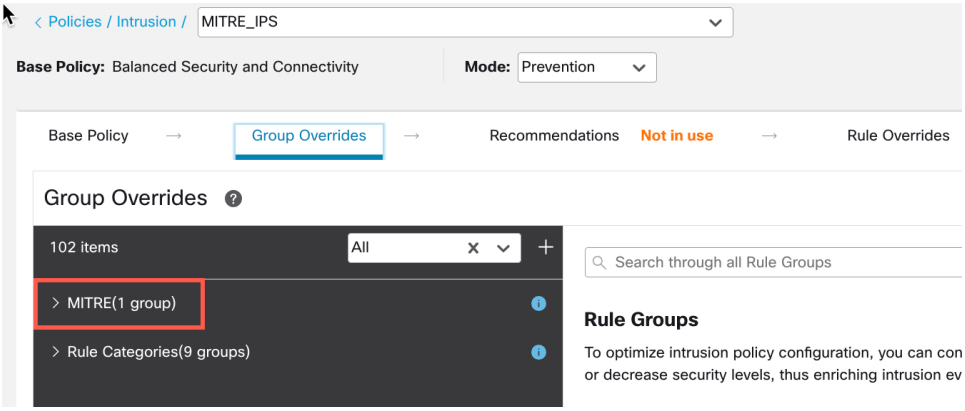


ステップ 6 [グループのオーバーライド（Group Overrides）] で、ドロップダウンリストで [すべて（All）] が選択されていることを確認します。これにより、対応する侵入ポリシーのすべてのルールグループが左側のペインに表示されます。

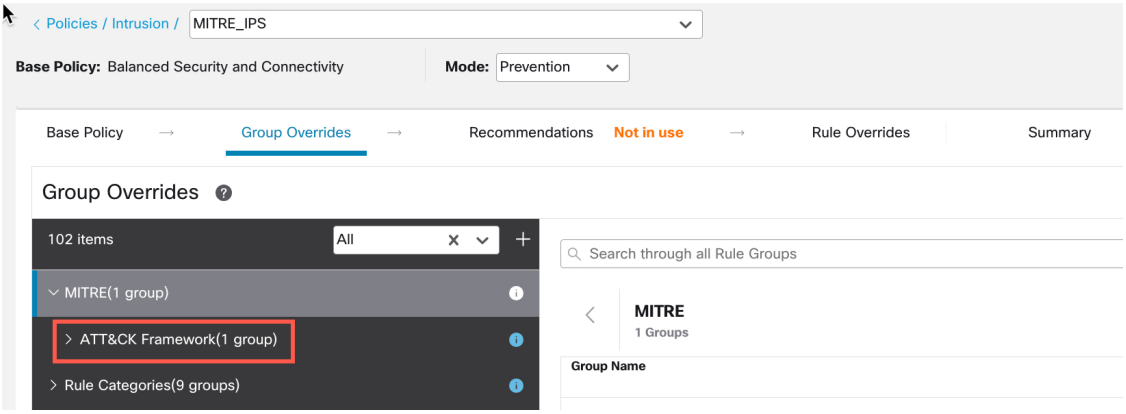


ステップ 7 左側のペインで、[MITRE] をクリックします。

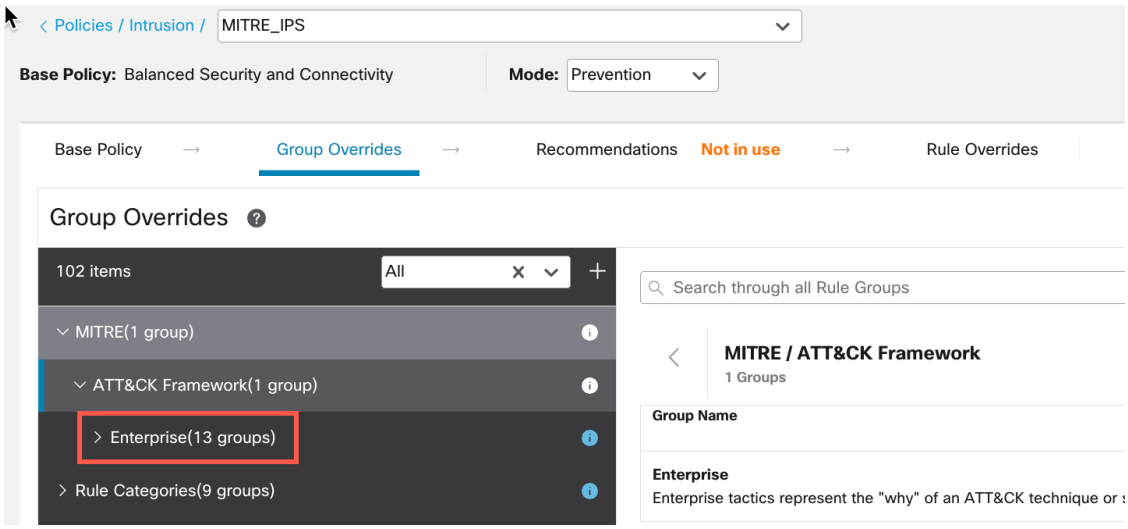
（注） 特定の要件に応じて、[ルールカテゴリ（Rule Categories）] ルールグループまたはその他のルールグループと、その下のサブルールグループを選択できます。すべてのルールグループで MITRE フレームワークが使用されます。



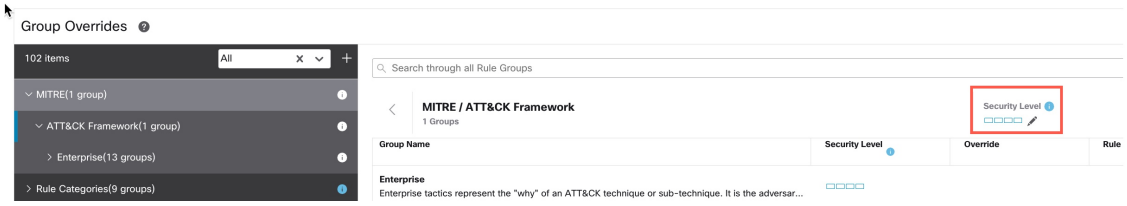
ステップ 8 [MITRE] で、[ATT&CKフレームワーク（ATT&CK Framework）] をクリックしてドリルダウンします。



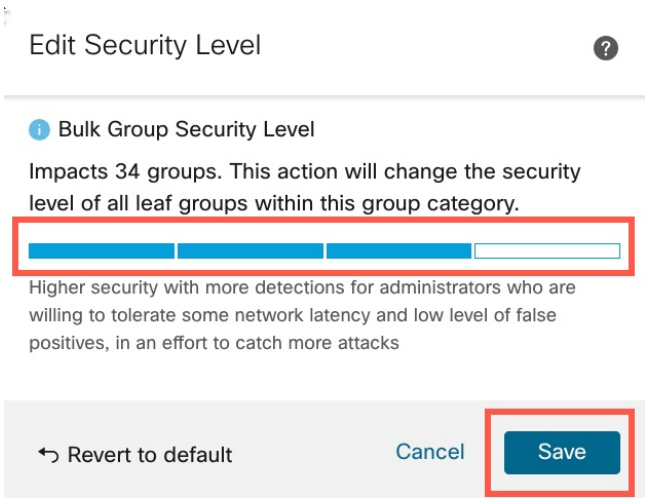
ステップ 9 [ATT&CKフレームワーク（ATT&CK Framework）] の下で、[エンタープライズ（Enterprise）] をクリックして展開します。



ステップ 10 ルールグループの [セキュリティレベル（Security Level）] の横にある [編集（Edit）]（✎）をクリックして、[エンタープライズ（Enterprise）] ルールグループカテゴリにあるすべての関連ルールグループのセキュリティレベルを一括変更します。

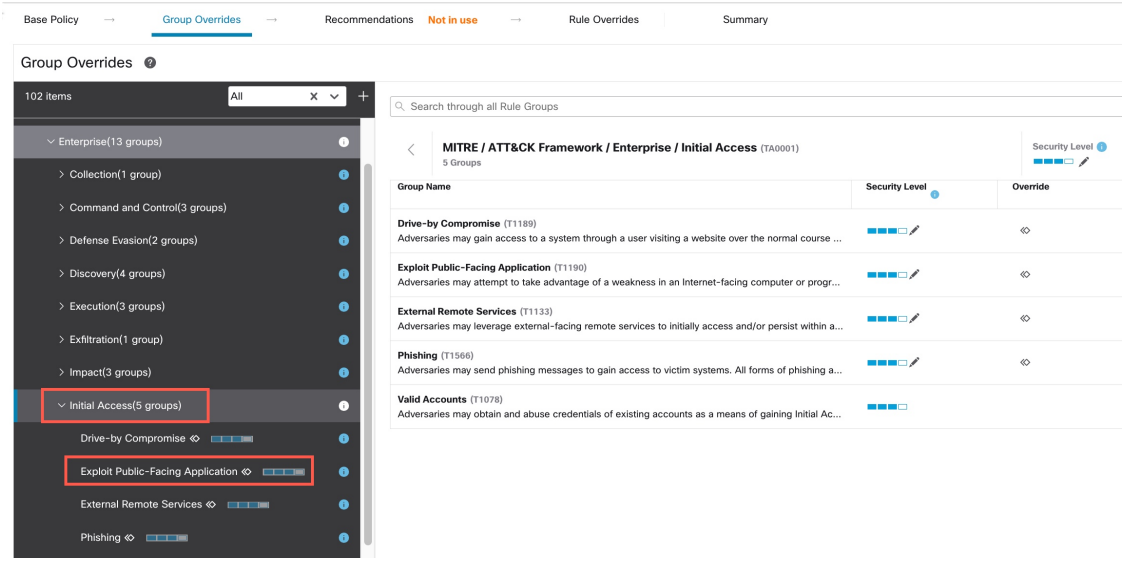


ステップ 11 [セキュリティレベルの編集（Edit Security Level）] ウィンドウで**セキュリティレベル**（この例では **3**）を選択し、[保存（Save）] をクリックします。

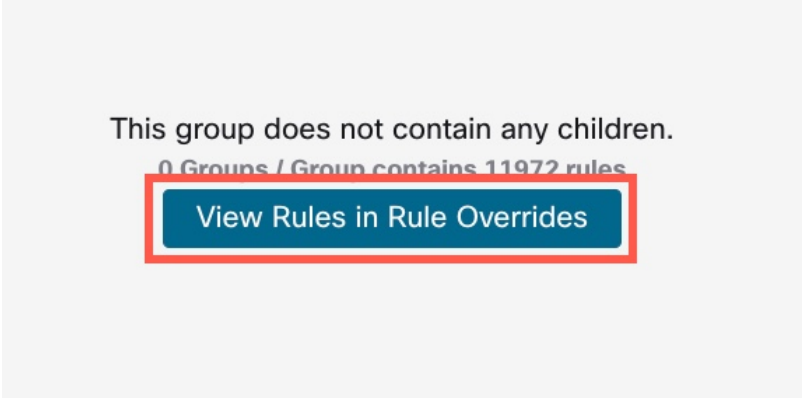


ステップ 12 [エンタープライズ（Enterprise）] の下で、[初期アクセス（Initial Access）] をクリックして展開します。

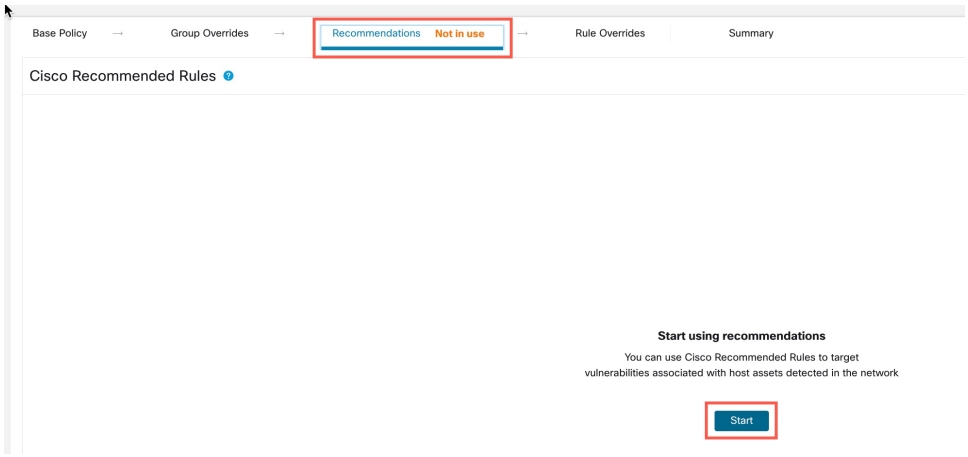
ステップ 13 [初期アクセス（Initial Access）] で、最後のリーフグループである [外部公開されたアプリケーションへの攻撃（Exploit Public-Facing Application）] をクリックします。



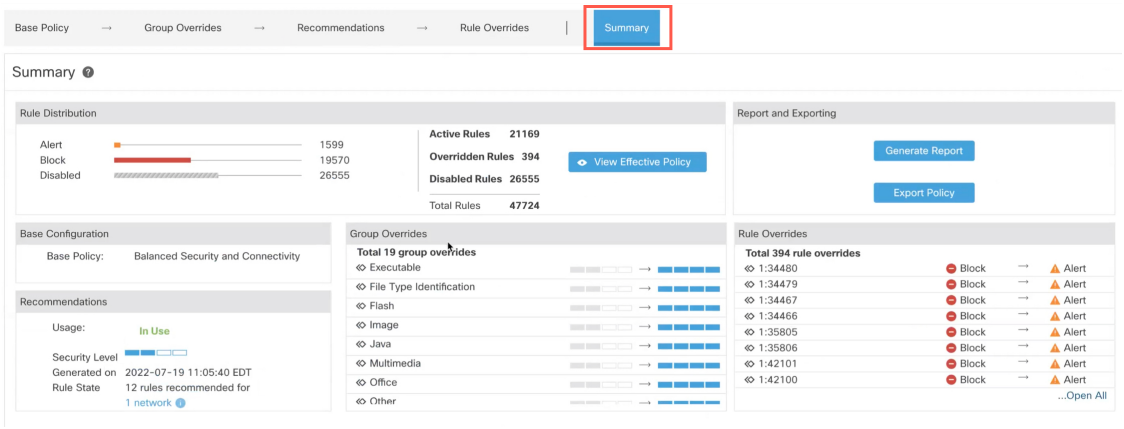
ステップ 14 [ルールのオーバーライドでルールを表示する（View Rules in Rule Overrides）] をクリックして、さまざまなルール、およびさまざまなルールのルール詳細やルールアクションなどを表示します。[ルールのオーバーライド（Rule Overrides）] レイヤで、1 つまたは複数のルールのルールアクションを変更できます。



ステップ 15 [推奨事項（Recommendations）] レイヤをクリックしてから [開始（Start）] をクリックして、シスコが推奨するルールの使用を開始します。侵入ルールの推奨事項を使用して、ネットワークで検出されたホストアセットに関連付けられている脆弱性を対象にすることができます。詳細については、「Snort 3 での新しい Cisco Secure Firewall 推奨事項の生成 （73 ページ）」を参照してください。



ステップ 16 ポリシーに対する現在の変更の全体像を表示するには、[概要（Summary）] レイヤをクリックします。ルールのオーバーライド、セキュリティレベルの変更、およびシスコが推奨するルールの生成に基づいて、ポリシーのルール配分、グループのオーバーライド、ルールのオーバーライド、ルールの推奨事項などを表示して、変更を確認することができます。



次のタスク

侵入ポリシーを展開し、Snort ルールによってトリガーされたイベントを検出してログに記録します。設定変更の展開 （30 ページ） を参照してください。

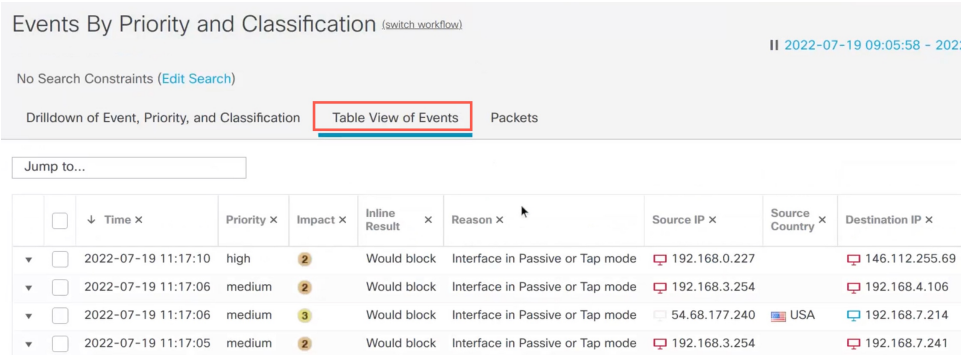
侵入イベントの表示

[クラシックイベントビューア（Classic Event Viewer）]ページと [統合イベントビューア（Unified Event Viewer）] ページで、侵入イベントの MITRE ATT&CK の手法とルールグループを表示できます。Talos により、Snort ルール（GID:SID）から MITRE ATT&CK の手法とルールグループへのマッピングが提供されます。これらのマッピングは、Lightweight Security Package（LSP）の一部としてインストールされます。

手順

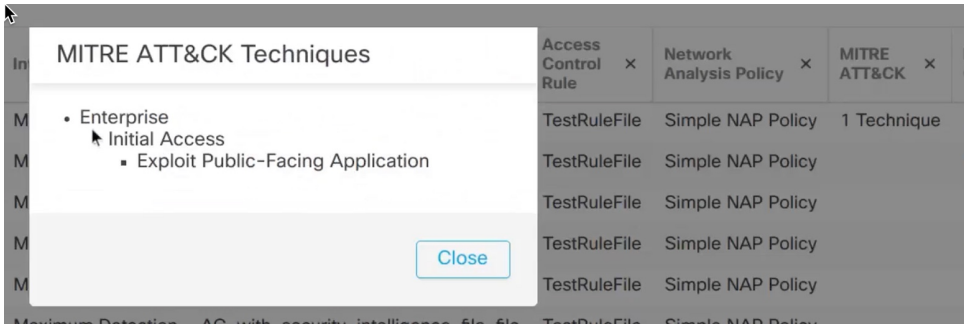
ステップ 1 [分析（Analysis）] をクリックし、[侵入（Intrusions）] で [イベント（Events）] を選択します。

ステップ 2 [イベントのテーブルビュー（Table View of Events）] タブをクリックします。



ステップ 3 [MITRE ATT&CK] で、侵入イベント用の手法を確認できます。[1件の手法（1 Technique）] をクリックして、MITRE ATT&CK の手法を表示します。

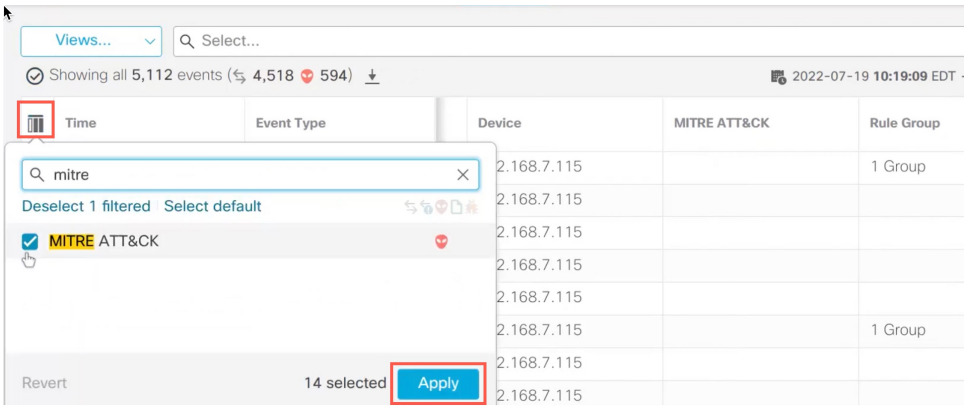
この例では、手法は [外部公開されたアプリケーションへの攻撃（Exploit Public-Facing Application）] です。



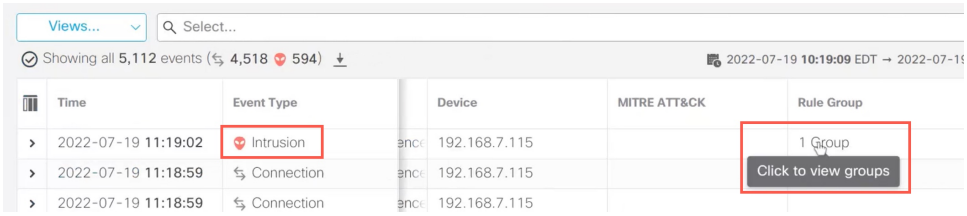
ステップ 4 [閉じる（Close）] をクリックします。

ステップ 5 [分析（Analysis）] をクリックして [統合イベント（Unified Events）] を選択します。

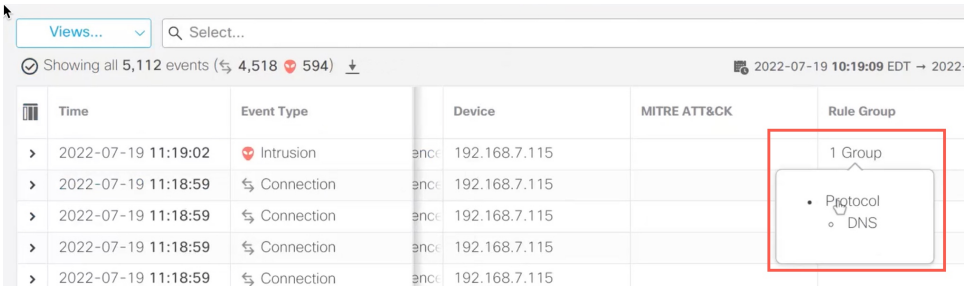
ステップ 6 [MITRE ATT&CK] 列と [ルールグループ（Rule Group）] 列が有効になっていない場合は、列セレクタアイコンをクリックして有効にします。



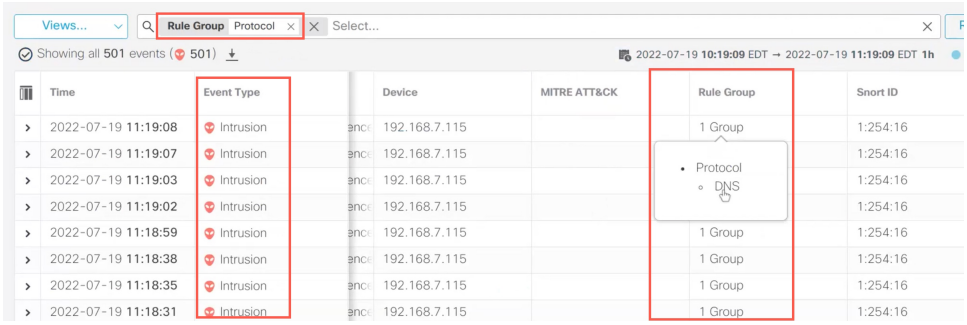
ステップ 7 この例では、侵入イベントは、1 つのルールグループにマッピングされたイベントによってトリガーされます。[ルールグループ（Rule Group）] 列の下にある [1つのグループ（1 Group）] をクリックします。



ステップ 8 親ルールグループである [プロトコル（Protocol）] と、その下の [DNS] ルールグループを表示できます。**[プロトコル（Protocol）] > [DNS]** を選択して、少なくとも 1 つのルールグループを持つすべての侵入イベントを検索します。



検索結果が表示されます。



その他の参考資料

- Intrusion Policy in Snort 3
- Snort 3 侵入ポリシーの編集 （37 ページ）
- MITRE Information in Malware Events

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。