



Firepower Management Center Snort 3 バージョン 7.0 設定ガイド

最終更新：2026 年 2 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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェアライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティングシステムの UCB パブリック ドメインバージョンの一部として開発されたプログラムを適応したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークボジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハードコピーおよびソフトコピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 カ所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices）をご覧ください。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



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

ネットワーク分析ポリシーと侵入ポリシーに関するガイドラインと制限事項 5

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

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 13

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 14

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 15

カスタム ネットワーク分析ポリシーの利点 16

カスタム侵入ポリシーの利点 17

カスタム ポリシーの制限 18

ネットワーク分析と侵入ポリシーの前提条件 21

第 2 章

Snort 2 から Snort 3 への移行 23

Snort 3 検査エンジン 23

Snort 2 と Snort 3 の比較 24

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 25

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	27
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	28
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	29
Snort 2 のルールと Snort 3 の同期	29
設定変更の展開	31

第 1 部 : **Snort 3 での侵入検知と防御** 35

第 3 章 **Snort 3 侵入ポリシーを開始するには** 37

侵入ポリシーの概要	37
ネットワーク分析と侵入ポリシーの前提条件	39
カスタム Snort 3 侵入ポリシーの作成	39
Snort 3 侵入ポリシーの編集	39
侵入ポリシーのベースポリシーの変更	40
侵入ポリシーの管理	40
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	41
アクセスコントロールルール設定と侵入ポリシー	42
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	42
設定変更の展開	43

第 4 章 **ルールを使用した侵入ポリシーの調整** 47

侵入ルールの調整の概要	47
侵入ルールのタイプ	48
ネットワーク分析と侵入ポリシーの前提条件	49
Snort 3 のカスタムルール	49
侵入ポリシーの Snort 3 侵入ルールの表示	50
侵入ルールアクション	51
侵入ルールアクションのオプション	51

	侵入ルールアクションの設定	52
	侵入ポリシーの侵入イベント通知フィルタ	53
	侵入イベントしきい値	53
	侵入イベントしきい値の設定	53
	Snort 3 での侵入ルールのしきい値の設定	55
	侵入イベントしきい値の表示と削除	56
	侵入ポリシー抑制の設定	57
	侵入ポリシー抑制タイプ	57
	Snort 3 での侵入ポリシーの抑制の設定	57
	抑制条件の表示と削除	58
	侵入ルールのコメントの追加	58
	Snort 2 カスタムルールの Snort 3 への変換	59
	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	60
	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	60
	ルールグループへのカスタムルールの追加	61
	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	63
	Snort 3 でのカスタムルールの管理	63
	カスタムルールの削除	64
	ルールグループの削除	65
<hr/>		
第 5 章	ネットワーク資産に応じた侵入防御の調整	67
	LSP 更新での Snort 3 ルールの変更	67
	Cisco Firepower 推奨ルールの概要	68
	ネットワーク分析と侵入ポリシーの前提条件	69
	Snort 2 で生成された Firepower 推奨事項の Snort 3 への移行	69
<hr/>		
第 11 部 :	Snort 3 での詳細なネットワーク分析	71
<hr/>		
第 6 章	ネットワーク分析ポリシーを開始するには	73
	ネットワーク分析ポリシーの概要	73
	ネットワーク分析ポリシーの管理	74

ネットワーク分析ポリシーの Snort 3 の定義と用語	75
ネットワーク分析と侵入ポリシーの前提条件	78
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	79
ネットワーク分析ポリシーのマッピング	82
ネットワーク分析ポリシーのマッピングの表示	83
ネットワーク分析ポリシーの作成	83
ネットワーク分析ポリシーの変更	84
[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	84
インスペクタ設定のコピー	85
ネットワーク分析ポリシーのカスタマイズ	85
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	89
インライン編集時の未保存の変更を元に戻す	90
インスペクタとオーバーライドのリストの表示	91
オーバーライドした設定のデフォルト設定の復元	91
カスタムネットワーク分析ポリシーの設定例	92
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	104



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 \(3 ページ\)](#)
- [ネットワーク分析ポリシーと侵入ポリシーに関するガイドラインと制限事項 \(5 ページ\)](#)
- [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 \(13 ページ\)](#)
- [ネットワーク分析と侵入ポリシーの前提条件 \(21 ページ\)](#)

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ー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、Firepower Threat Defense (FTD) 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。
- Firepower Threat Defense ごとの Snort バージョン：Snort 検査エンジンは Firepower Threat Defense 固有であり、Firepower Management Center (FMC) 固有ではありません。FMC 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 Firepower Threat Defense を管理できます。FMC 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せん。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 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 FTD 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 FMC は、バージョン 6.4、6.5、6.6、6.7、および 7.0 の Snort 2 Firepower Threat Defense とバージョン 7.0 の Snort 3 Firepower Threat Defense 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 Firepower Threat Defense 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、FMC 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。FMC 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ールール、既存のルールの変更後の状態、および FMC と Firepower Threat Defense 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。FMC 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 \(29 ページ\)](#) 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 :** Firepower Threat Defense が 7.0 にアップグレードされると、Firepower Threat Defense 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。FMC 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 Firepower Threat Defense 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 \(49 ページ\)](#) 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 Firepower Threat Defense は、Snort 2 もサポートします。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。



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。

ネットワーク分析ポリシーと侵入ポリシーに関するガイドラインと制限事項

- 小さなパケットが含まれるトラフィックの割合が高いと、Snort のパフォーマンスが低下します。この動作は、すべてのプリプロセッサが無効になっている場合でも見られます。
- メモリが不足している Threat Defense デバイスに構成の変更を展開しようとする、Snort の展開もトリガーされます。その結果、RSS メモリの消費量が高くなります。多数の Snort IPS ルール、ネットワークオブジェクト、およびアクセス制御リストを含む複数の IPS ポリシーなどの大規模な構成をデバイスに展開すると、Snort のメモリ使用量にも影響します。構成を最適化することで、このようなメモリの問題を軽減できます。構成を最適化するためのアクセス制御ルールの構成方法に関するベストプラクティスについては、「[アクセス制御ルールのベストプラクティス](#)」[英語]を参照してください。
- Threat Defense Virtual インスタンスのメモリを増やす場合、追加のメモリを使用するように Snort 3 の構成を再度展開する必要があります。



(注) Threat Defense Virtual インスタンスのメモリを増やしても、Snort 3 のメモリ割り当ては自動的に調整されません。構成を再度展開して、更新されたリソース制限を Snort 3 に適用する `memory_allocation.lua` などの関連する構成ファイルを再生成する必要があります。

FMC 管理対象の FTD 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、FMC 管理対象の Firepower Threat Defense 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。

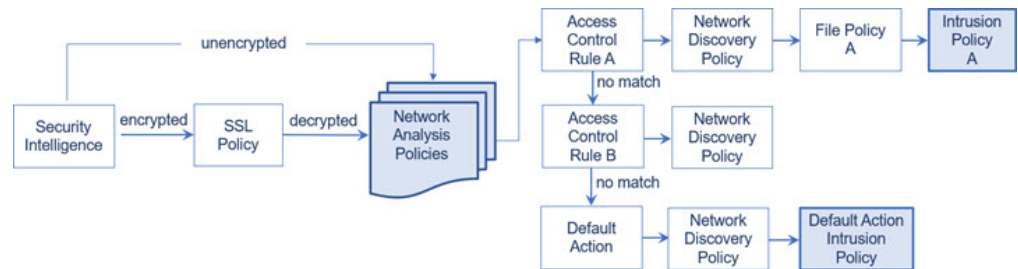
表 1: Snort 3 の機能制限

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 : <ul style="list-style-type: none"> • Safe Search • YouTube EDU
侵入ポリシー (Intrusion Policy)	<ul style="list-style-type: none"> • Firepower 推奨 • [ポリシー層 (Policy Layers)] • グローバルルールのしきい値 • ロギングの設定 : <ul style="list-style-type: none"> • 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)
アプリケーションの検出	Snort3 では、デフォルトですべてのネットワークに対してアプリケーション検出が有効になっています。Snort 2 とは異なり、ネットワーク検出ポリシーのネットワークフィルタを使用して、特定のネットワークのみに対するアプリケーション検出の有効化または無効化を制御することはできません。詳細については、『 <i>Firepower Management Center</i> コンフィギュレーションガイド』の最新バージョンの「Snort 2 および Snort 3 でのアプリケーション検出」のトピックを参照してください。
ネットワーク検出/RNA	<ul style="list-style-type: none"> • ホストポート/サービス ID (ネットワークマップに表示) • OSフィンガープリント (侵入ポリシーを自分のネットワークマップに合わせて調整することはできません)
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スイベント（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。



- (注) TLS サーバーアイデンティティが無効になっている場合、Snort 3 は SNI 不一致検出を実行しません。Client Hello パケット内の SNI の評価のみを行い、Server Hello パケット内の証明書の共通名 (CN) の検証はバイパスします。

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ため、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ため、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ールール

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。インスペクター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ー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。Firepower 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を使用します。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、FMC の FTD 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FMC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せん。

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。

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ため、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ー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。
- Firepower 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されます。
- 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に注意してください。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ー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**。

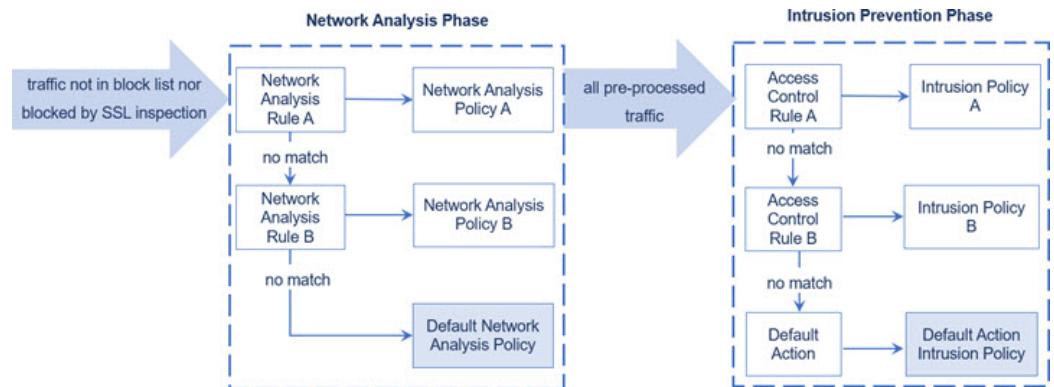
複数のカスタム ネットワーク分析ポリシーを使用する場合は、さらに課題があります。複雑な展開内の上級ユーザの場合は、一致したトラフィックの前処理にカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティゾーン、ネットワーク、VLAN に合わせて前処理を調整できます。(ASA FirePOWER では、VLAN による前処理を制限することはできません)。これを実現するには、アクセスコントロールポリシーにカスタム ネットワーク分析ルールを追加します。各ルールにはネットワーク分析ポリシーが関連付けられており、ルールに一致するトラフィックの前処理を制御します。



- 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спек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、FTD 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、FMC を使用した FTD 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。

- [Snort 3 検査エンジン](#) (23 ページ)
- [Snort 2 と Snort 3 の比較](#) (24 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](#) (29 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](#) (31 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 Firepower Threat Defense 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 Firepower Threat Defense 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 Firepower Threat Defense 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 Firepower Threat Defense 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스에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。

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](#)。

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、FTD 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、Firepower Threat Defense 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 (28 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)] を選択します。

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 \(31 ページ\)](#) 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 Firepower Threat Defense 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、一時的なパフォーマンス損失が発生します。

手順

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

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。

(注)

Snort 3 を無効にするには、[Snort 2 へのダウングレード (Downgrade to Snort 2)] をクリックします。

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 \(31 ページ\)](#) 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替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 \(28 ページ\)](#)
- [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)] を選択します。

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。

- : 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 FMC にインポートします。
- : 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 \(61 ページ\)](#) 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 \(31 ページ\)](#) 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)] > [アクセス制御 (Access Control)] 見出し > [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 [Snort が同期していない (Snort out-of-Sync)] () をクリックします。

(注)

侵入ポリシーの Snort 2 と Snort 3 バージョンが同期されている場合、[同期 (Sync)] アイコンが、緑[Snort が同期している (Snort in-Sync)] (➔) 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 FMC 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 \(31 ページ\)](#) 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)] > [アクセス制御 (Access Control)] 見出し > [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 FMC 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。

FMC 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。FMC 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)] > [アクセス制御 (Access Control)] 見出し > [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 [Snort が同期していない (Snort out-of-Sync)] () をクリックします。

(注)

侵入ポリシーの Snort 2 と Snort 3 バージョンが同期されている場合、[同期 (Sync)] アイコンが、緑 [Snort が同期している (Snort in-Sync)] () 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せん。
- 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 \(31 ページ\)](#) 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『*Firepower 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 Firepower 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表示されます。
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 (▶)** 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 (Policy selection)] () 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 Firepower Threat Defense 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場合は、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 (Inspect Interruption)] () 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、FMC 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、FMC 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『*Firepower Management Center Configuration Guide*』の「Deploy Configuration Changes」のトピックを参照してください。



第 1 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 \(37 ページ\)](#)
- [ルールを使用した侵入ポリシーの調整 \(47 ページ\)](#)
- [ネットワーク資産に応じた侵入防御の調整 \(67 ページ\)](#)



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 \(37 ページ\)](#)
- [ネットワーク分析と侵入ポリシーの前提条件 \(39 ページ\)](#)
- [カスタム Snort 3 侵入ポリシーの作成 \(39 ページ\)](#)
- [Snort 3 侵入ポリシーの編集 \(39 ページ\)](#)
- [侵入ポリシーのベースポリシーの変更 \(40 ページ\)](#)
- [侵入ポリシーの管理 \(40 ページ\)](#)
- [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 \(41 ページ\)](#)
- [設定変更の展開 \(43 ページ\)](#)

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、**Firepower** 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せ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、FTD 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)] > [アクセス制御 (Access Control)] 見出し > [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で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 \(39 ページ\)](#) 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。

次のタスク

設定変更を展開します。[設定変更の展開 \(31 ページ\)](#) を参照してください。

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)] > [アクセス制御 (Access Control)] 見出し > [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 \(31 ページ\)](#) 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)] > [アクセス制御 (Access Control)] 見出し > [侵入 (Intrusion)]) では、次に示す情報とともに、現在のカスタム侵入ポリシーを表示できます。



- 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)] > [アクセス制御 (Access Control)] 見出し > [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 \(39 ページ\)](#) を参照してください。
- 削除：削除するポリシーの横にある [削除 (Delete)] () 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 \(39 ページ\)](#) 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 FMC 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『*Firepower 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 \(31 ページ\)](#) 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『*Firepower 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を使用します。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。

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『*Firepower 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 \(31 ページ\)](#) 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『*Firepower 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** Firepower 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表示されます。
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** (▶) 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 (Policy selection)] (☒) 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 Firepower Threat Defense 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場合は、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 (Inspect Interruption)] (🚫) 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、FMC 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、FMC 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『*Firepower Management Center Configuration Guide*』の「Deploy Configuration Changes」のトピック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 \(47 ページ\)](#)
- [侵入ルールのタイプ \(48 ページ\)](#)
- [ネットワーク分析と侵入ポリシーの前提条件 \(49 ページ\)](#)
- [Snort 3 のカスタムルール \(49 ページ\)](#)
- [侵入ポリシーの Snort 3 侵入ルールの表示 \(50 ページ\)](#)
- [侵入ルールアクション \(51 ページ\)](#)
- [侵入ポリシーの侵入イベント通知フィルタ \(53 ページ\)](#)
- [侵入ルールのコメントの追加 \(58 ページ\)](#)
- [Snort 2 カスタムルールの Snort 3 への変換 \(59 ページ\)](#)
- [ルールグループへのカスタムルールの追加 \(61 ページ\)](#)
- [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 \(63 ページ\)](#)
- [Snort 3 でのカスタムルールの管理 \(63 ページ\)](#)
- [カスタムルールの削除 \(64 ページ\)](#)
- [ルールグループの削除 \(65 ページ\)](#)

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。



(注) 共有オブジェクトルールは変更せず、Threat Defense デバイスに対してのみこれらのルールを有効または無効にすることをお勧めします。カスタム Snort ルールを作成するには、シスコサポートにお問い合わせください。

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спек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

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
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、FTD 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くかに基づいて 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。

SID が有効か無効かを確認するに

は、`./file-contents/ngfw/var/sf/detection_engines/<id>/ips/<id>` ディレクトリにある `snort.lua` ファイルのエントリを確認します。

- SID がデフォルトで無効になっている場合、ファイルにエントリは存在しません。
- SID を手動で有効にした場合、**enable:yes** というエントリが表示されます。
- SID を手動で有効にした後に無効になった場合、エントリはファイルに残り、**enable:no** と表示されます。



- (注)
- Snort3 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。
 - Snort3 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 ルールの `classtype` は、イベントに関連する攻撃のタイプを示す分類をルールに割り当てます。各 `classtype` には 1 ~ 4 の優先順位レベルも関連付けられます。ただし、Threat Defense デバイス上の特定の `classtypes` の優先順位レベルは、Snort の [ドキュメント](#) に記載されているオープンソース Snort の `classtypes` の優先順位レベルと一致しません。たとえば、オープンソース Snort では `tcp-connection` の優先順位は 4 ですが、Threat Defense デバイスでは優先順位 3 が割り当てられています。

ルールグループにカスタムルールを追加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 \(61 ページ\)](#)」を参照してください。

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)] > [アクセス制御 (Access Control)] 見出し > [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 \(39 ページ\)](#)」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ー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があります。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)] > [アクセス制御 (Access Control)] 見出し > [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 \(39 ページ\)](#)」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 \(31 ページ\)](#) 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ー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。

侵入イベントしきい値の設定

オプション	説明
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タに達し、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。
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。 <ul style="list-style-type: none"> • 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	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。

オプション	説明
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 packets view 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。侵入ルールに設定したしきい値が、各パケットスレッドに適用されます。ただし、構成が完全に適用されるのは、一意のフローのコンテキスト内のみです。異なるネットワークフローでより多くのアラートが存在する場合がありますが、構成されている数よりもアラートが少なくなることはありません。

手順

- ステップ 1 [オブジェクト (Objects)] > [侵入ルール (Intrusion Rules)] を選択します。
- 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。

侵入イベントしきい値の表示と削除

- 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)]を選択します。
- 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 \(31 ページ\)](#)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 익스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)] をクリック) 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)**] を選択します。
- 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 [追加 (Add)] () 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 \(31 ページ\)](#) 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)] を選択します。
- 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 \(31 ページ\)](#) 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)] > [アクセス制御 (Access Control)] 見出し > [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** (🗨️) 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

システムは [コメント (Comments)] カラムのルールの横に **コメント** (🗨️) を表示します。

次のタスク

設定変更を展開します。[設定変更の展開 \(31 ページ\)](#) 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。



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)] を選択します。

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。

- : 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 FMC にインポートします。
- : 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 \(61 ページ\)](#) 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 \(31 ページ\)](#) 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)] > [アクセス制御 (Access Control)] 見出し > [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 [Snortが同期していない (Snort out-of-Sync)] () をクリックします。

(注)

侵入ポリシーの Snort 2 と Snort 3 バージョンが同期されている場合、[同期 (Sync)] アイコンが、緑[Snortが同期している (Snort in-Sync)] () 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 FMC 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 \(31 ページ\)](#) 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

FMC 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)] を選択します。

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 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 5 [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 6 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 7 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 8 [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 9 [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

- FMC 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 \(63 ページ\)](#) 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 \(63 ページ\)](#) 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 \(31 ページ\)](#) 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。FMC 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)] > [アクセス制御 (Access Control)] 見出し > [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 展開矢印 (>) 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 \(31 ページ\)](#) 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)] を選択します。
- 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 \(31 ページ\)](#) 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)] を選択します。
- 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。
- [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。
 - [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 \(31 ページ\)](#) 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 \(39 ページ\)](#) 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)] を選択します。

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 \(31 ページ\)](#) 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 Firepower の推奨ルールと、Cisco Firepower 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](#) (67 ページ)
- [Cisco Firepower 推奨ルールの概要](#) (68 ページ)
- [ネットワーク分析と侵入ポリシーの前提条件](#) (69 ページ)
- [Snort 2 で生成された Firepower 推奨事項の Snort 3 への移行](#) (69 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 ルールのユーザーオーバーライドを保持 (Retain user overrides for deleted Snort 3 rules)] チェックボックスに移動するには、[[システム (System)] (⚙️) > [設定 (Configuration)] > [侵入ポリシーの優先設定 (Intrusion Policy Preferences)] をクリックします。

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、[通知 (Notifications)] [[システム (System)] (⚙️) の横にある [通知 (Notifications)] アイコンの [タスク (Task)] タブに表示されます。

Cisco Firepower 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 Firepower 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 Firepower 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、FTD 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 で生成された Firepower 推奨事項の Snort 3 への移行

Firepower の推奨事項の使用を開始または停止する場合、ネットワークのサイズと侵入ルールセットに応じて、数分かかる場合があります。

Firepower の推奨事項は、Snort 3 バージョンでは直接生成できません。侵入ポリシーの Snort 2 バージョンの Firepower 推奨事項を生成し、ここに記載されている手順に従って、推奨されたルール設定を Snort 3 に移行します。

始める前に

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。

手順

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

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

ステップ 3 侵入ポリシーの Snort 2 バージョンで推奨事項を生成して適用します。

最新バージョンの『*Firepower Management Center Configuration Guide*』の「*Generate and Applying Firepower Recommendations*」のトピックを参照し、そのトピックに記載されている手順を実行します。

ステップ 4 Snort 2 のルール変更を Snort 3 と同期します。

手順については、[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。

(注)

7.0 より前から 7.0 バージョンへのアップグレード中に、既存の Snort 2 の推奨事項が Snort 3 に同期されます。ただし、7.0 へのアップグレード後に Snort 2 の推奨事項を生成（新規ではない）した場合は、これらすべての推奨事項を Snort 3 バージョンに同期できません。

次のタスク

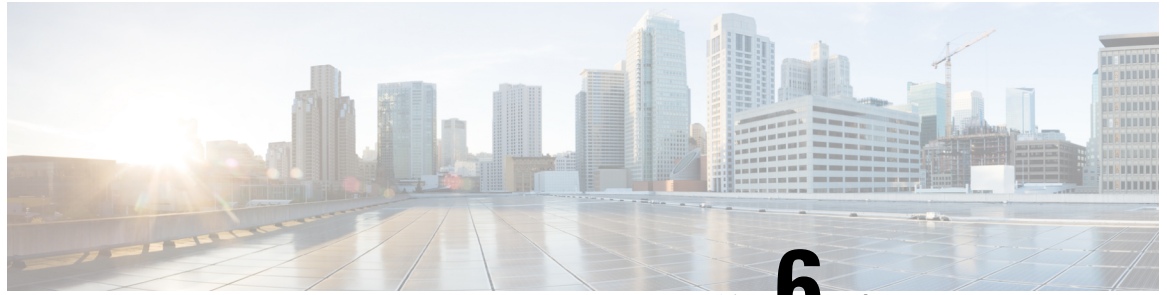
設定変更を展開します。[設定変更の展開 \(31 ページ\)](#) を参照してください。



第 II 部

Snort 3 での詳細なネットワーク分析

- [ネットワーク分析ポリシーを開始するには \(73 ページ\)](#)



第 6 章

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 \(73 ページ\)](#)
- [ネットワーク分析ポリシーの管理 \(74 ページ\)](#)
- [ネットワーク分析ポリシーの Snort 3 の定義と用語 \(75 ページ\)](#)
- [ネットワーク分析と侵入ポリシーの前提条件 \(78 ページ\)](#)
- [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 \(79 ページ\)](#)
- [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 \(104 ページ\)](#)

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

(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。

- 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、『*Firepower 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 \(79 ページ\)](#)」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。『*Firepower 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 (79 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tonsインスペクタ	<p>シングルtons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tons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tons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。</p> <p>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 (79ページ) の「シングルtonsインスペクタ」を参照してください。</p>
マルチtonsインスペクタ	<p>マルチtons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。</p> <p>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 (79ページ) の「マルチtonsインスペクタ」を参照してください。</p>
スキーマ	<p>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。</p> <p>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 (85ページ) を参照してください。</p>

用語	説明
ファイルのサンプル	<p>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。</p> <p>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。</p> <p>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 (85 ページ) を参照してください。</p>
完全な設定	<p>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。</p> <p>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。</p> <p>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。</p> <p>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 (85 ページ) を参照してください。</p>

用語	説明
オーバーライドされた設定	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <p>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 (85 ページ) を参照してください。</p>

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 \(79 ページ\)](#)

[ネットワーク分析ポリシーのカスタマイズ \(85 ページ\)](#)

[ネットワーク分析ポリシーのマッピング \(82 ページ\)](#)

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、FTD 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に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、FMC 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。FMC 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)
- FMC 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спек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。

```

▼ binder
185     {
186         "when": {
187             "service": "imap",
188             "role": "any"
189         },
190         "use": {
191             "type": "imap"
192         }
193     },

```

シングルトンインспекタ

シングルトンインспек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спекタは、マルチトンインспек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спек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нда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нда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нда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"
        }
      }
    ]
  }
}

```

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)] > [アクセス制御 (Access Control)] 見出し > [侵入 (Intrusion)] > [ネットワーク分析ポリシー (Network Analysis Policies)] に進みます。

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 FMC 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)] > [アクセス制御 (Access Control)] 見出し > [侵入 (Intrusion)] > [ネットワーク分析ポリシー (Network Analysis Policies)] に進みます。

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 使用可能な選択肢から [検査モード (Inspection Mode)] を選択します。

- [検出 (Detection)]
- [防御 (Prevention)]

ステップ 5 [ベースポリシー (Base Policy)] を選択し、[保存 (Save)] をクリックします。

(注)

Snort 3 および SSL 復号または TLS サーバーアイデンティティを使用している場合は、**防止**モードでネットワーク分析ポリシー (NAP) を構成します。

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)] > [アクセス制御 (Access Control)] 見出し > [侵入 (Intrusion)] > [ネットワーク分析ポリシー (Network Analysis Policies)] に進みます。

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)

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)] > [アクセス制御 (Access Control)] 見出し > [侵入 (Intrusion)] > [ネットワーク分析ポリシー (Network Analysis Policies)] に進みます。

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ディング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 \(92 ページ\)](#)

[インスペクタとオーバーライドのリストの表示 \(91 ページ\)](#)

[ネットワーク分析ポリシーの Snort 3 の定義と用語 \(75 ページ\)](#)

[ネットワーク分析ポリシーのカスタマイズ \(85 ページ\)](#)

[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](#) (89 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)] > [アクセス制御 (Access Control)] 見出し > [侵入 (Intrusion)] > [ネットワーク分析ポリシー (Network Analysis Policies)] に進みます。
- 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

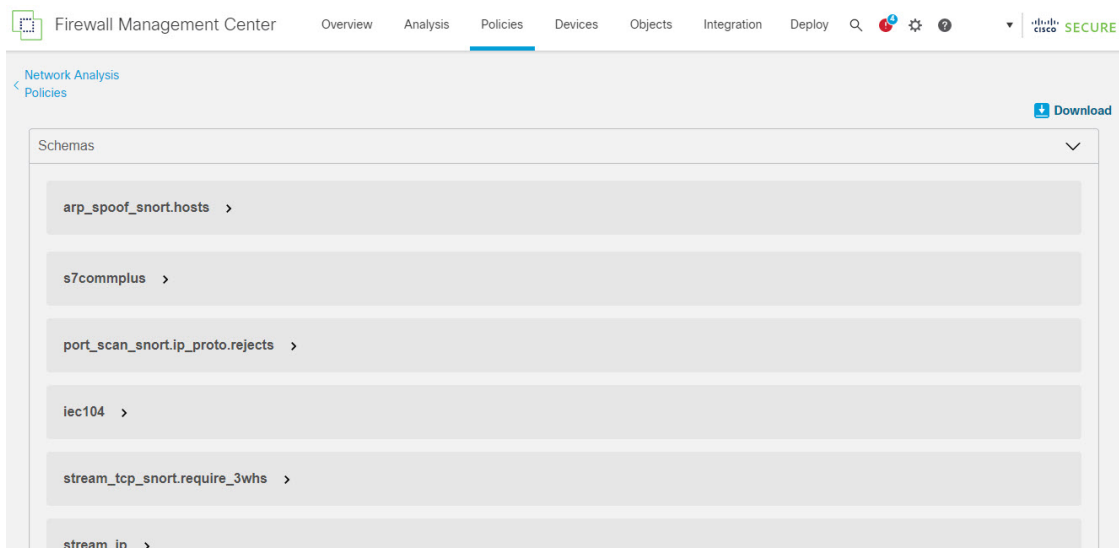
[ネットワーク分析ポリシーのカスタマイズ](#) (85 ページ)

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)] > [アクセス制御 (Access Control)] 見出し > [侵入 (Intrusion)] > [ネットワーク分析ポリシー (Network Analysis Policies)] に進みます。
- 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。

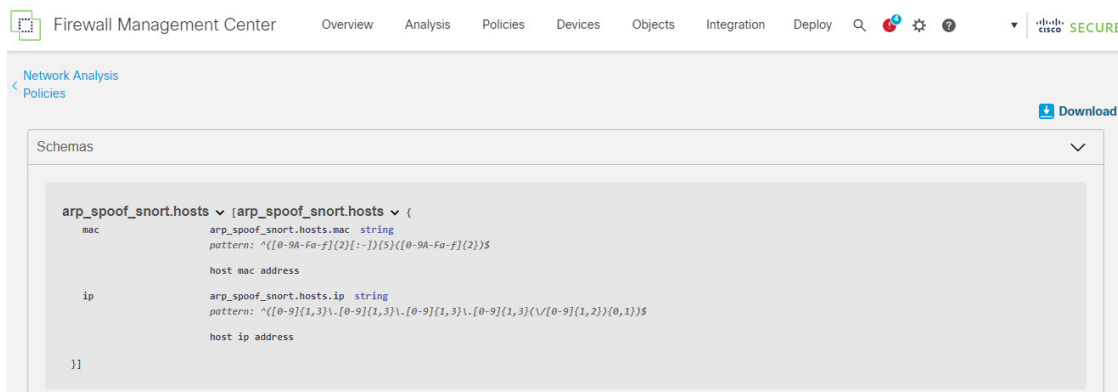
これらのオプションでは、許容値、範囲、パターン、既存およびデフォルトのインスペクタ設定、ならびにオーバーライドされたインスペクタ設定に関する情報が得られます。

a) 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。

- 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、 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。
- 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ることができます。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。
- 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。

- FMC 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。

FMC 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。

- [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。
- [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。
- 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、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ーになるため、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](#) (91 ページ)

[インスペクタとオーバーライドのリストの表示](#) (91 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](#) (84 ページ)

[インスペクタ設定のコピー](#) (85 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](#) (85 ページ) を参照してください。

手順

ステップ 1 [ポリシー (Policies)] > [アクセス制御 (Access Control)] 見出し > [侵入 (Intrusion)] > [ネットワーク分析ポリシー (Network Analysis Policies)] に進みます。

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ーになります。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ー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、FMC 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](#) (85 ページ)

[インライン編集時の未保存の変更を元に戻す](#) (90 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](#) (91 ページ)

[カスタムネットワーク分析ポリシーの設定例](#) (92 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)] > [アクセス制御 (Access Control)] 見出し > [侵入 (Intrusion)] > [ネットワーク分析ポリシー (Network Analysis Policies)] に進みます。

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 右の列の [オーバーライドされた構成 (Overridden Configuration)] で、[十字 (Cross)] **✕** 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 \(91 ページ\)](#)

[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 \(89 ページ\)](#)

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)] > [アクセス制御 (Access Control)] 見出し > [侵入 (Intrusion)] > [ネットワーク分析ポリシー (Network Analysis Policies)] に進みます。

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 \(84 ページ\)](#)

[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 \(89 ページ\)](#)

[ネットワーク分析ポリシーのカスタマイズ \(85 ページ\)](#)

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)] > [アクセス制御 (Access Control)] 見出し > [侵入 (Intrusion)] > [ネットワーク分析ポリシー (Network Analysis Policies)] に進みます。

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)] (✕) 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](#) (90 ページ)

[ネットワーク分析ポリシーのカスタマイズ](#) (85 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](#) (89 ページ)

[カスタムネットワーク分析ポリシーの設定例](#) (92 ページ)

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。

- FMC 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](#) (89 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](#) (85 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ーになるため、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": []
  },
  "iecl104": {
    "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ールールの追加



(注) デフォルトのバインダー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) 対応するバインダールールエントリは、バインダインスpek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спек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спекタ)
- 新しいマルチトンインスタンスの作成 (**telnet** インспек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) バインダー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спек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ールールの設定

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、バインダールールを作成する方法を示します。バインダー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ールールは、全体として真の情報源です。

Firepower Threat Defense 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ー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ールールも定義しました。親ポリシーからのバインダールールをここにコピーする必要があります。その後、子ポリシーのバインダー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спекタで **alt_max_command_line_len** 属性のトリム値を取得します。**smtp** インспек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ます。

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "decompress_zip": false,
          "normalize_cmds": "ATRN AUTH BDAT CHUNCKING 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 QUEUE 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` という名前でも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](#) (75 ページ)

[ネットワーク分析ポリシーのマッピング](#) (82 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](#) (79 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](#) (84 ページ)

[インスペクタ設定のコピー](#) (85 ページ)

[ネットワーク分析ポリシーのカスタマイズ](#) (85 ページ)

[インスペクタとオーバーライドのリストの表示](#) (91 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時に、任意のメニューまたは別のページへの他のパスを選択した場合、変更内容はそのページを離れてもシステム キャッシュにとどまります。

翻訳について

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

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。