Cisco
Customer Experience

Ask the Experts

機能概要（基礎編）：
侵入防御システム（IPS）の概要
（Feature Overview: Intrusion Prevention System Overview）

Disclaimer

This document is Cisco Confidential information provided for your internal business use in connection with the Cisco Services purchased by you or your authorized reseller on your behalf。 This document contains guidance based on Cisco's recommended practices。

You remain responsible for determining whether to employ this guidance、 whether it fits your network design、 business needs、 and whether the guidance complies with laws、 including any regulatory、 security、 or privacy requirements applicable to your business。

免責

この文書は、お客様またはお客様の代理人である認定リセラーが購入したシスコサービスに関連して、お客様が社内業務において使用することを目的としてシスコが提供するシスコの機密情報です。この文書にはシスコが推奨するプラクティスに基づく手引きが記載されています。

お客様は、この手引きを使用するか否かやお客様のネットワーク設計および業務上のニーズにこの手引きが適合しているか否か、さらにはこの手引きが法律（お客様の業務に適用される規制上の要件、セキュリティ上の要件およびプライバシーに関する要件を含みます）に準拠しているか否かを判断する責任を引き続き負います。

本日の学習内容

- 侵入防御システム（IPS）機能の概要
- Snort 3 の概要
- IPS のベストプラクティスとメリット
- IPS ポリシーの設定方法

本日のトピック

01 侵入防御システム（IPS）の概要

02 デコーダとプリプロセッサ

03 IPS としての Snort

04 IPS ポリシーのコンポーネント

05 デモ：IPS の設定

侵入防御システム（IPS）の概要

侵入防御システム（IPS）とは

主な機能

- パケットの条件に基づいて悪意のあるトラフィック、およびその可能性のあるトラフィックを識別
  - 通信は許可するがアラートを生成
  - 悪意のあるトラフィックをドロップする

プラットフォームおよびライセンス要件

IPS プラットフォーム

- すべての Secure Firewall プラットフォーム

ライセンス

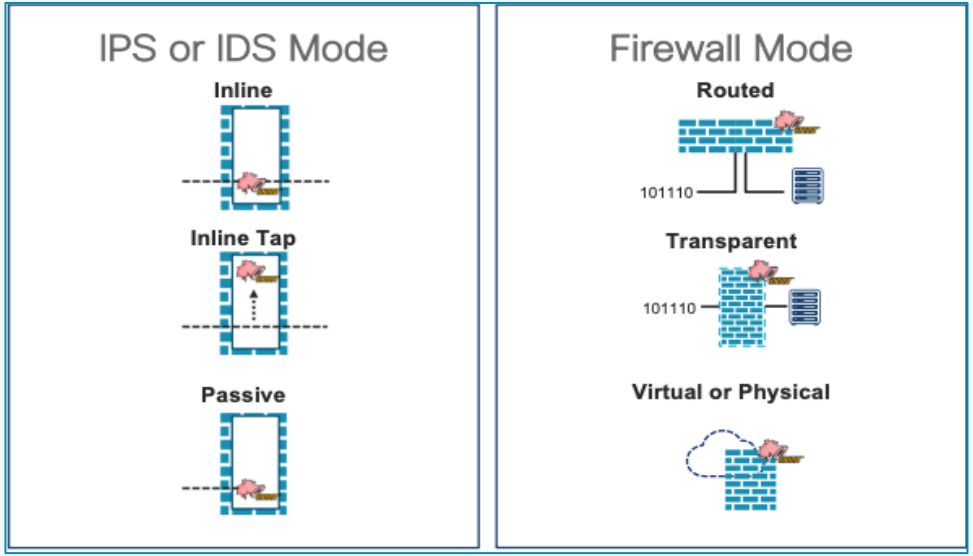
- Threat ライセンス

展開モード

IPS 展開は次のいずれかのモードで可能

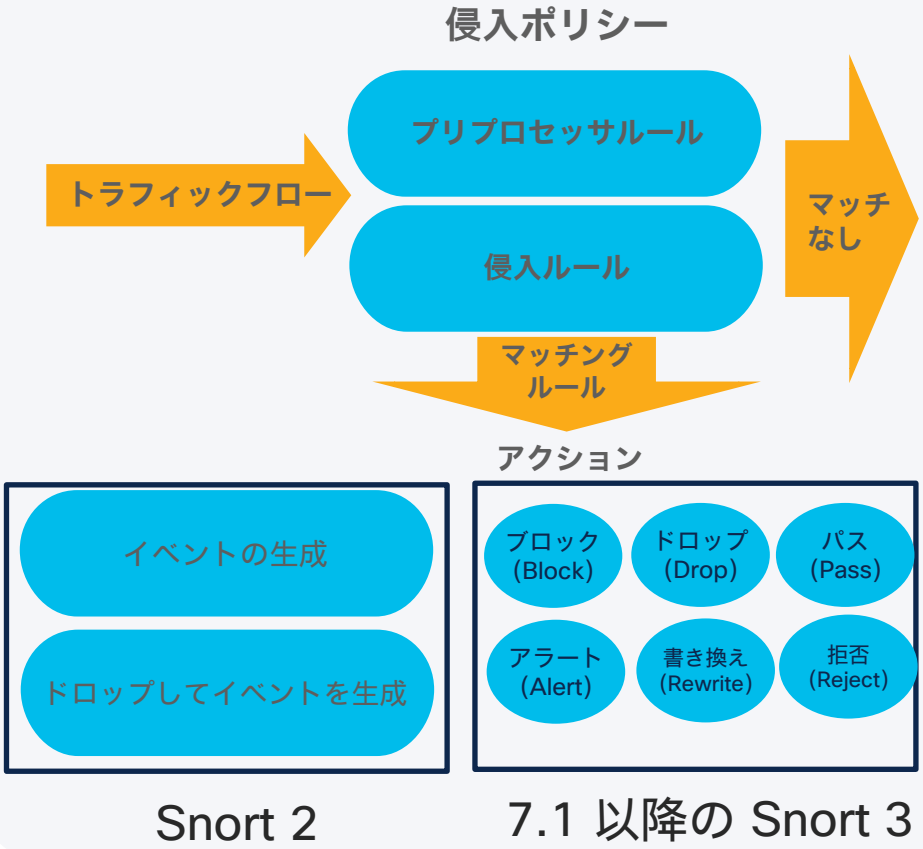
- ファイアウォールモード (Secure Firewall)
  - ルーテッドまたはトランスペアレント インターフェイス

- NGIPS（IPS 専用アプライアンス）
  - 侵入検知システム（IDS）展開
  - 侵入防御システム（IPS）展開



侵入ポリシーの概要

- IPS 侵入ポリシーの構成要素
  - プリプロセッサルール
  - 侵入ルール
  - ルールの状態/アクション
- Snort エンジンは IPS の中核



デコーダと
プリプロセッサ

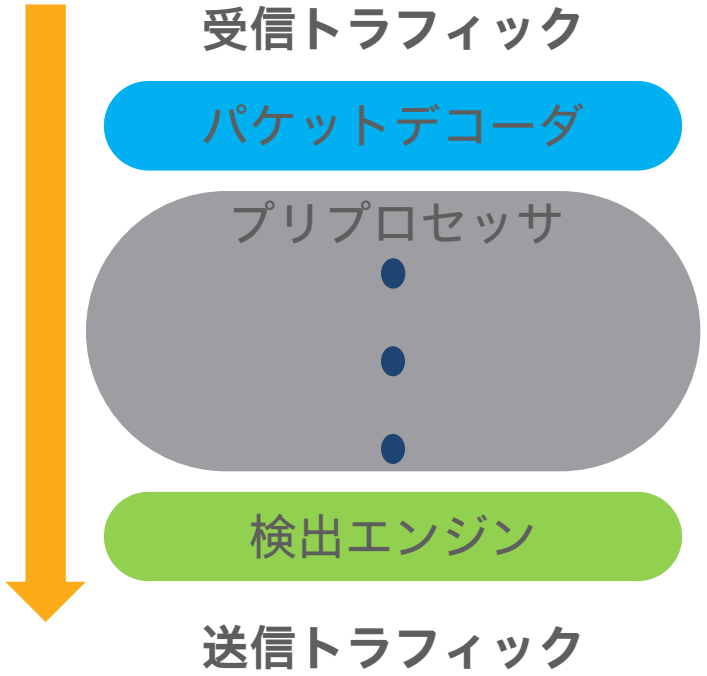
デコーダとプリプロセッサ

デコーダ

- データリンク、ネットワーク、トランスポートプロトコルをデコード

プリプロセッサ

- 以下のような異常を検出
  - 大きすぎる IP データグラム
  - IP フラグメントの重複
- トラフィックの正規化
- 再組み立て



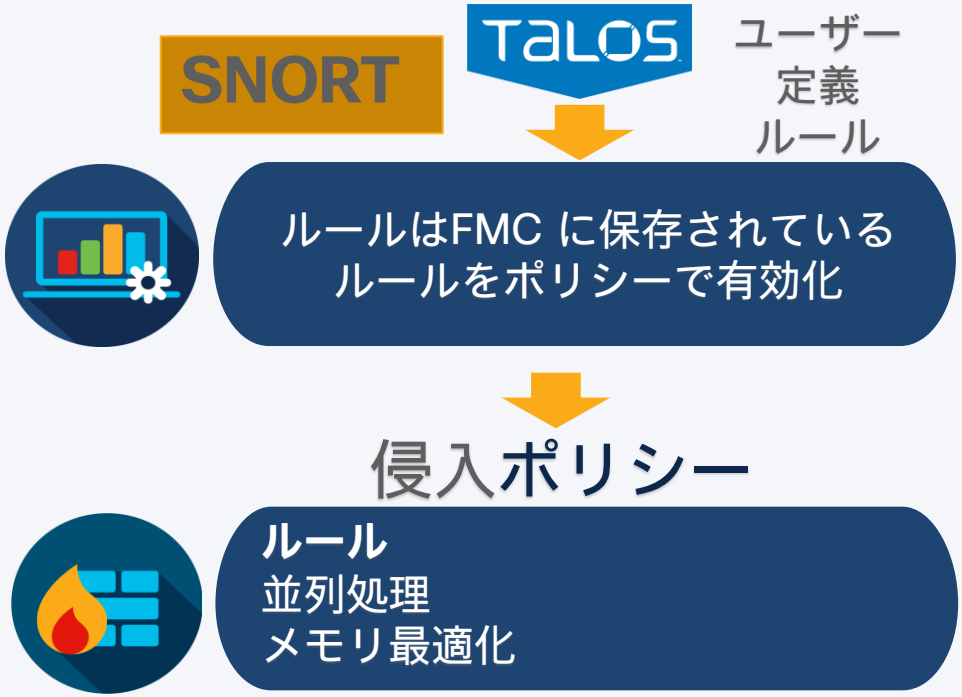
ネットワーク分析ポリシー（NAP）

- パケットデコーダとプリプロセッサは NAP で調整される
- ネットワーク分析ポリシー（NAP）は必須
- IPS と同様に、システム NAP にも 3 つのベースポリシーがある
- デフォルトポリシー：Balanced Security and Connectivity
- ベースポリシーまたはカスタムポリシー、いずれかの使用が可能

IPS としての Snort

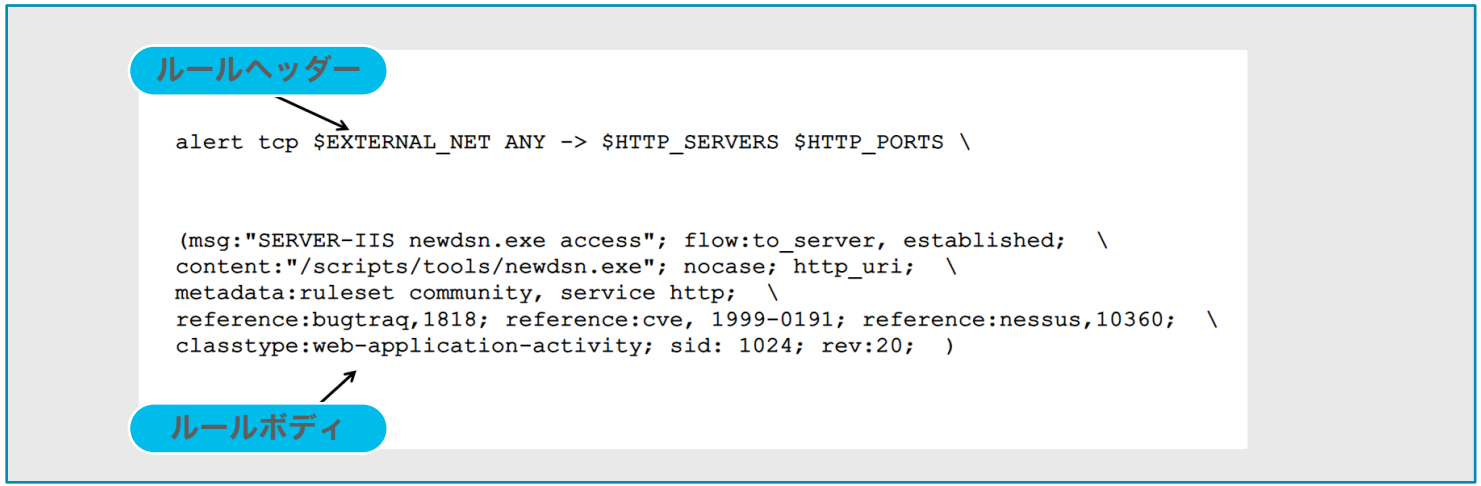
Snort エンジン

- 無料のオープンソースエンジン
- 侵入ポリシーでは、Snort エンジンと Snort ルールを活用
- ルールは Cisco Talos が提供
- 最新の脅威に基づいて定期的にルールを更新
- カスタムルールの作成も可能
- 2022年9月現在利用が推奨されている FTD バージョン 7.0.X は、Snort バージョン 3 がベース



Snort ルール

- ヘッダーとボディ（本文）で構成されているルール
- ネットワークの脆弱性に対するエクスプロイトを検出するために、キーワードと引数のセットが指定されている
- ルールヘッダーの変数によって対象トラフィックが識別される



Snort 変数と変数セット

変数

- 送信元および宛先の IP アドレス/ポートを識別するために侵入ルールで使用される値
- 変更があった場合のルール管理をシンプルにする
- [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [変数セット（Variable Set）] で確認可能

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS

- デフォルトまたはカスタム変数の使用が可能

ネットワーク変数

ポート変数

Snort 変数と変数セット

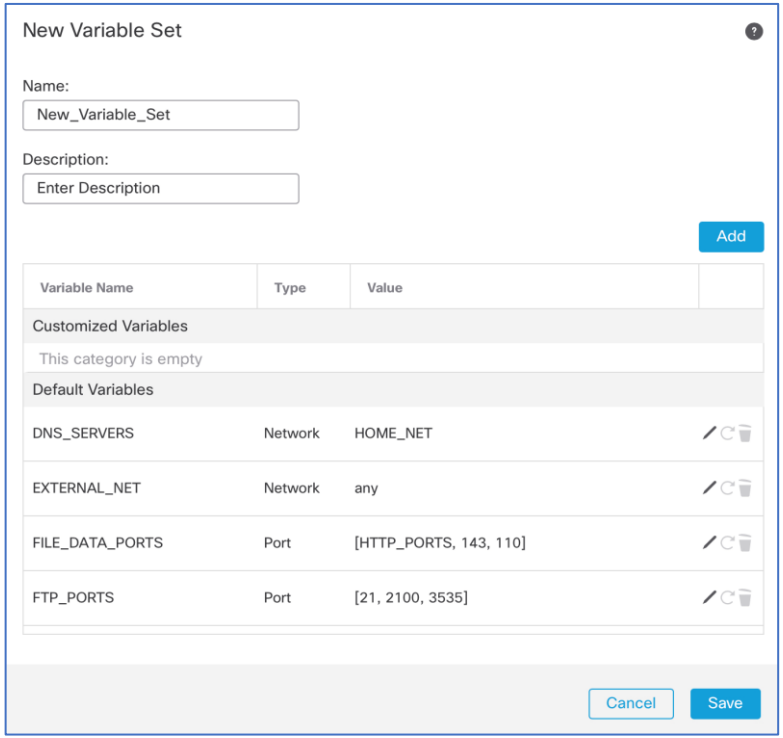
変数セット

- システム内でグループ化された変数
- 変数セットを利用することで複数の変数をグループ化が可能

[Default-Set] はデフォルトの変数セット

- Talos ルールで使用されるすべての変数が含まれている

シスコでは、監視対象の環境を反映するように **Default-Set** 変数（例：$HOME_NET）を変更することを推奨

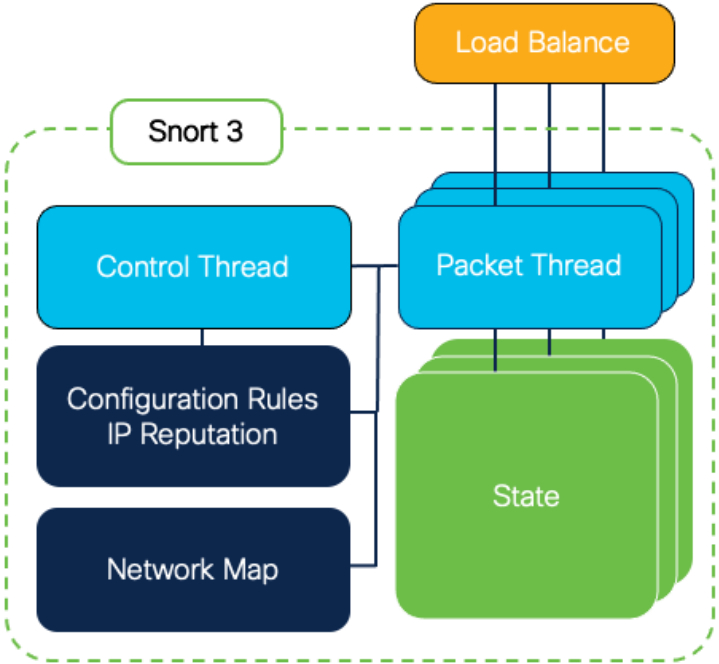


ルール状態

- ルール状態によってルールアクションが決まる
- アクションは侵入ポリシーで変更可能

Snort 2	Snort 3 バージョン 7.0	Snort 3 バージョン7.1以降
ルール状態を [イベントを生成（generate）] または、[ドロップしてイベントを生成（drop and generate）] に設定	[生成（generate）] は [アラート（alert）]、[ドロップして生成（drop and generate）] は [ブロック（block）]	以下を含む複数のルールアクションが利用可能 ブロック（Block） ドロップ（Drop） アラート（Alert） 書き換え（Rewrite） パス（Pass） 拒否（Reject）

Snort 3 の導入



有効性

- 最新のアーキテクチャ
- フローベースの検出エンジンによる、インテリジェントなトラフィックの正規化
- 改善されたルール言語

モジュール方式

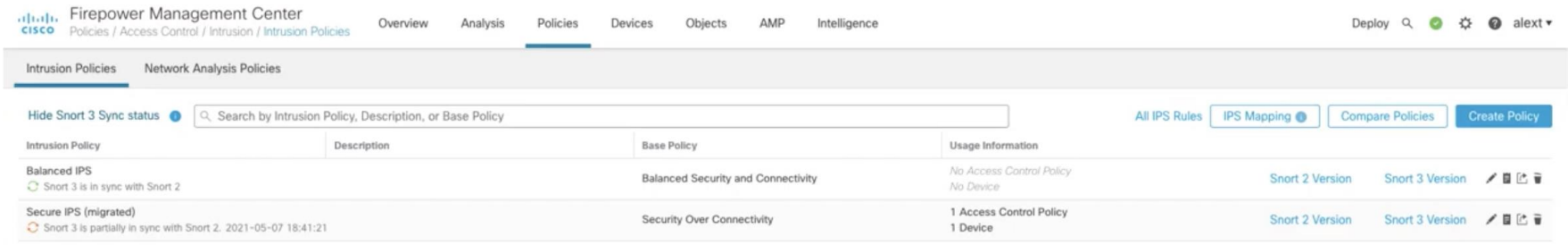
- 製品化までの時間の短縮
- クラウドサービスとしての展開が可能
- 管理とテレメトリの強化

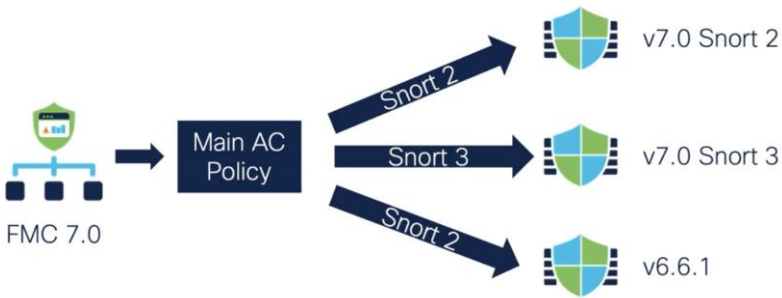
パフォーマンス

- 検査パフォーマンスの大きな向上
- マルチスレッドプロセスによるメモリ使用効率の向上

Snort 3 に関する注意事項

- バージョン 7.0.x にアップグレードしても使用していた Snort バージョンが維持され、自動で Snort 3 にはアップグレードされない
- 侵入ポリシーと NAP では、1 つのポリシーと 2 つのバージョン（Snort 2 と 3）を利用可能
- 異なるバージョンを実行する場合は、Snort ポリシーに同じルールが設定されていることを確認する

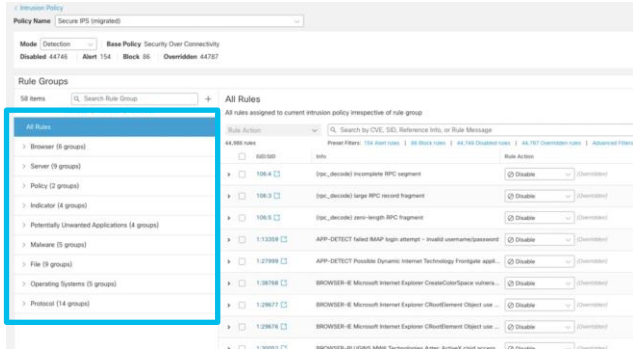




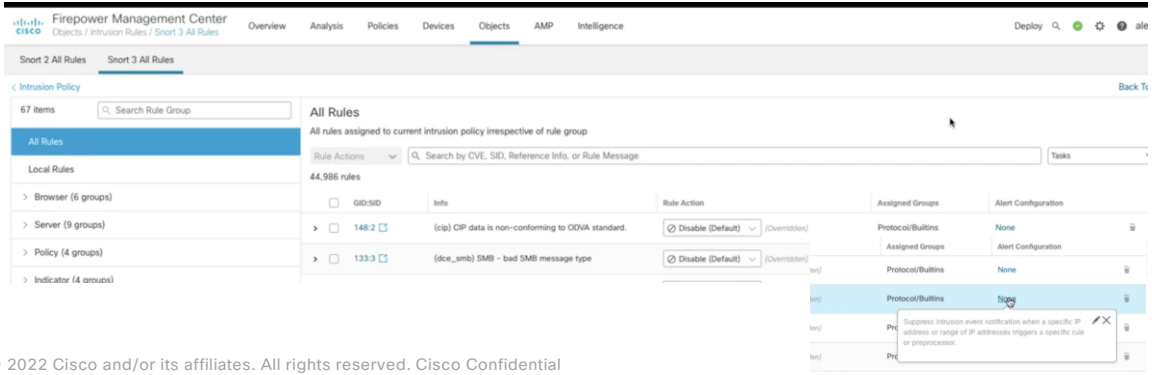
Snort 3 に関する注意事項

- Syslog は ACP ポリシーに移動

- 新しいルールグループ



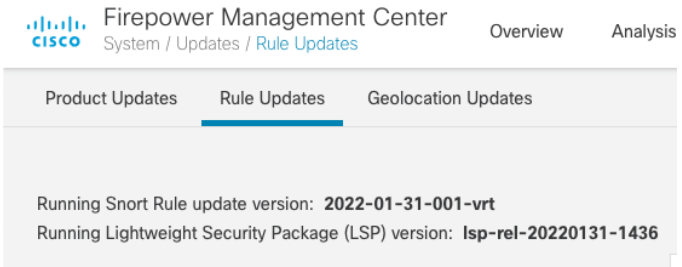
- 抑制としきい値は [オブジェクト（Objects）] に移動



Snort 3 に関する注意事項

- **詳細設定**
  - グローバルルールのしきい値が固定値に（変更不可）
  - SNMP アラート（廃止）
  - Syslog アラート（ACPのログ設定に移動）
- **ポリシーレイヤ**
  - ユーザーが作成したレイヤは Snort 3 ポリシーでは利用不可
- **ポリシーの仕組み**
  - [保存（Save）] または [コミット（Commit）] ボタンがないため、ポリシーを編集する際にユーザーインターフェイスで変更するとすぐにコミットされる
- **ルールの更新方法が変更（LSP）**

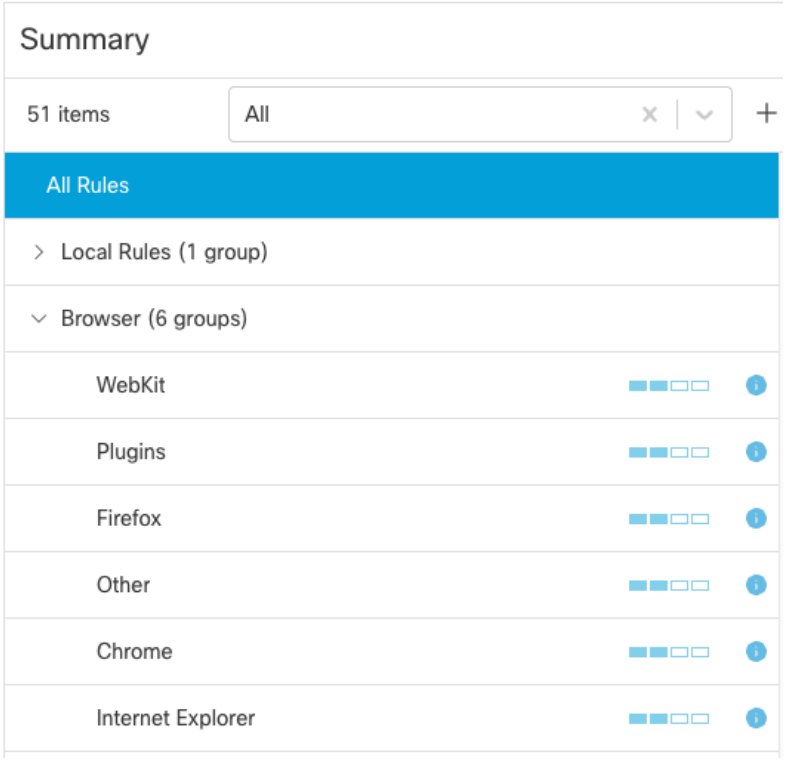
Snort 2のSRUに比べ、Snort 3 のLSPでは柔軟性が向上しサイズが小さく



Snort 3 侵入ポリシー固有の機能

Level 1 - **Connectivity** Over Security
Level 2 - **Balanced** Security and Connectivity
Level 3 - **Security** Over Connectivity
Level 4 - Maximum Detection <試験用>

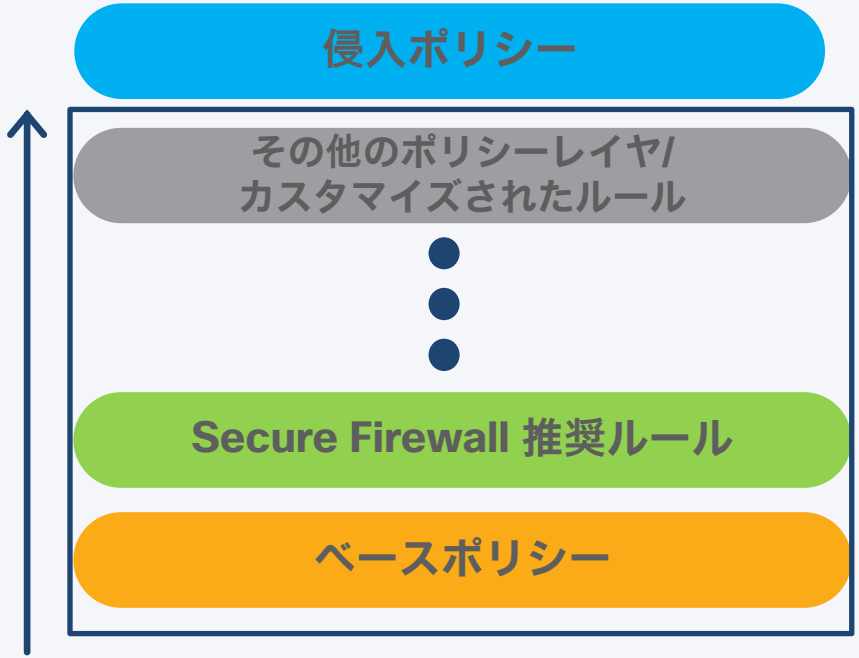
- ルールグループのオーバーライド



IPS ポリシーのコンポーネント

侵入ポリシーの構造

- ポリシーレイヤで構成されている
- Snort ルールをカスタマイズまたは追加できる
- ユーザーレイヤを設定すると、選択したベースポリシーの設定がオーバーライドされる
- オプションで Secure Firewall の推奨ルールを追加可能



ベース侵入ポリシー

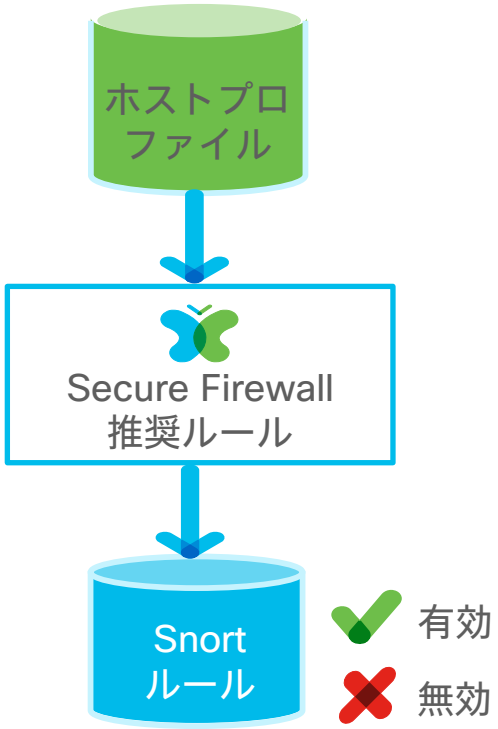
システム提供のポリシー

- Talos インテリジェンスベース
- 常に更新される（Talosチームより）
- そのまま利用、またはカスタム ポリシーのベースとして利用

シスコ推奨：**Balanced Security and Connectivity**

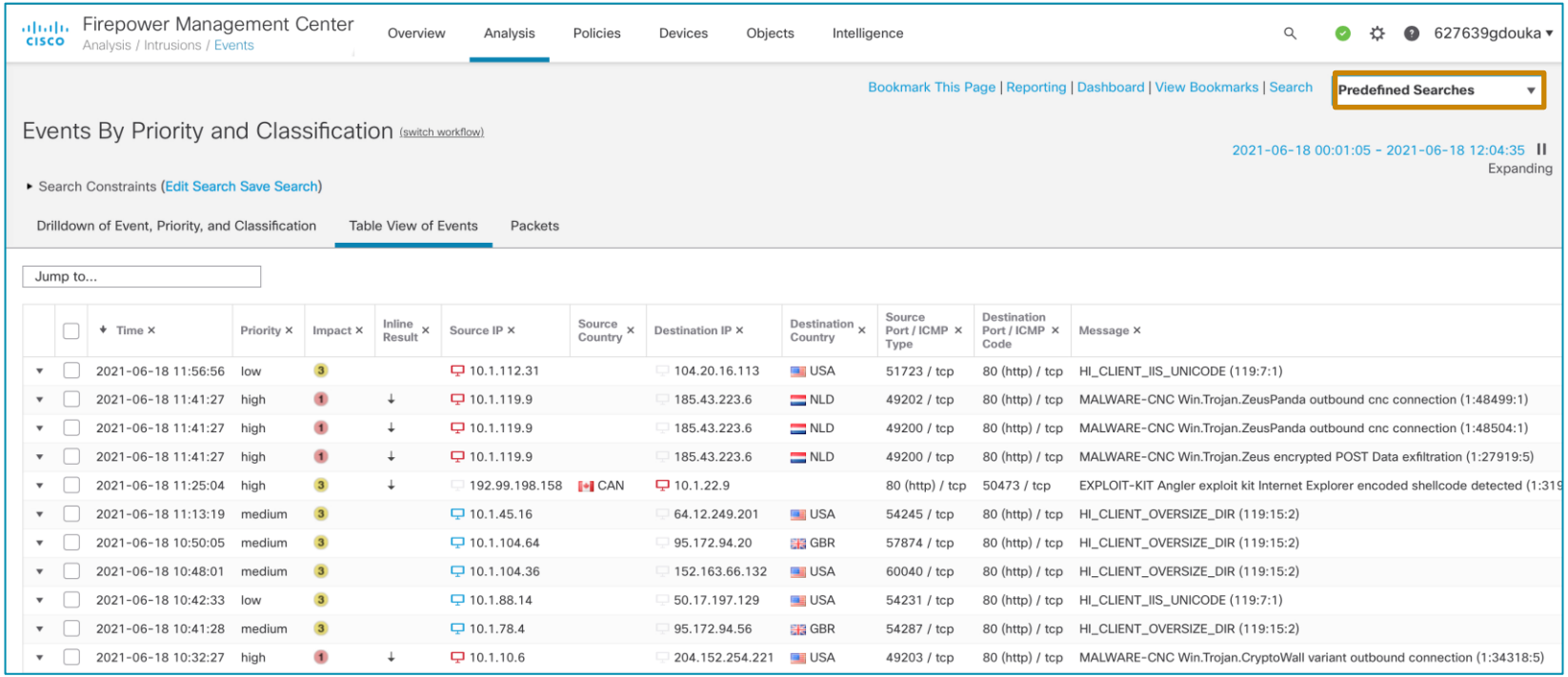
Secure Firewall 推奨ルール

- 監視対象のネットワーク固有のニーズに応じて侵入ポリシーを調節する
- 監視対象のインフラストラクチャを反映するようにNetwork Discovery が調整されている場合にのみ使用する
- ベースポリシールールは、ネットワーク/アセットに関連する脆弱性に対してチェックされる
- ベースポリシールールの有効化/無効化に関する推奨ルールが作成される
- 推奨ルールは定期的に更新する必要がある（スケジューリング機能を活用可能）また、VDBも常に最新版の適用を
  - 推奨ルールは、Snort 3 利用時はFMC7.1 以降で利用可能



侵入イベント

- 侵入イベントは、システムが攻撃の可能性を特定したときに生成される
- 詳細は [分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）] で確認できる



キーポイント

IPS にはセキュリティに関する多数のメリットがある

ベースポリシーは（迷ったら）Balanced Security and Connectivity の設定を

ルールを定期的に更新する

環境に合わせてルールを調整する

環境に基づいて変数の値を設定する

Network Discovery が適切に設定され情報収集されている場合にのみ Secure Firewall の推奨ルール機能を実行する

Snort 3 で新たに導入された多数の変更を必ずチェックする

Resources

- Secure Firewall（NGFW）ATXsリソースリンク集
- https://community.cisco.com/t5/-/-/ta-p/4437061
- ※本日のATXs以外のリソースリンクも確認できます。


Cisco
Customer Experience