

# 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

SNORT

TALOS

IPS

### 目的

ネットワークトラフィックフローを調査し、エクスプロイトを検出して防止する

### 方法

悪意のあるトラフィックを定義する条件とのマッチング

# 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

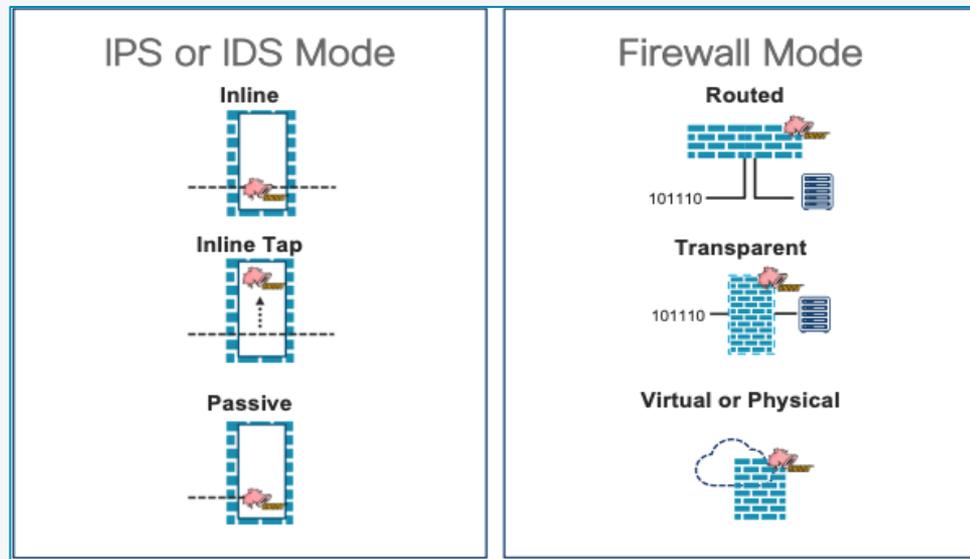
- Threat ライセンス



# 展開モード

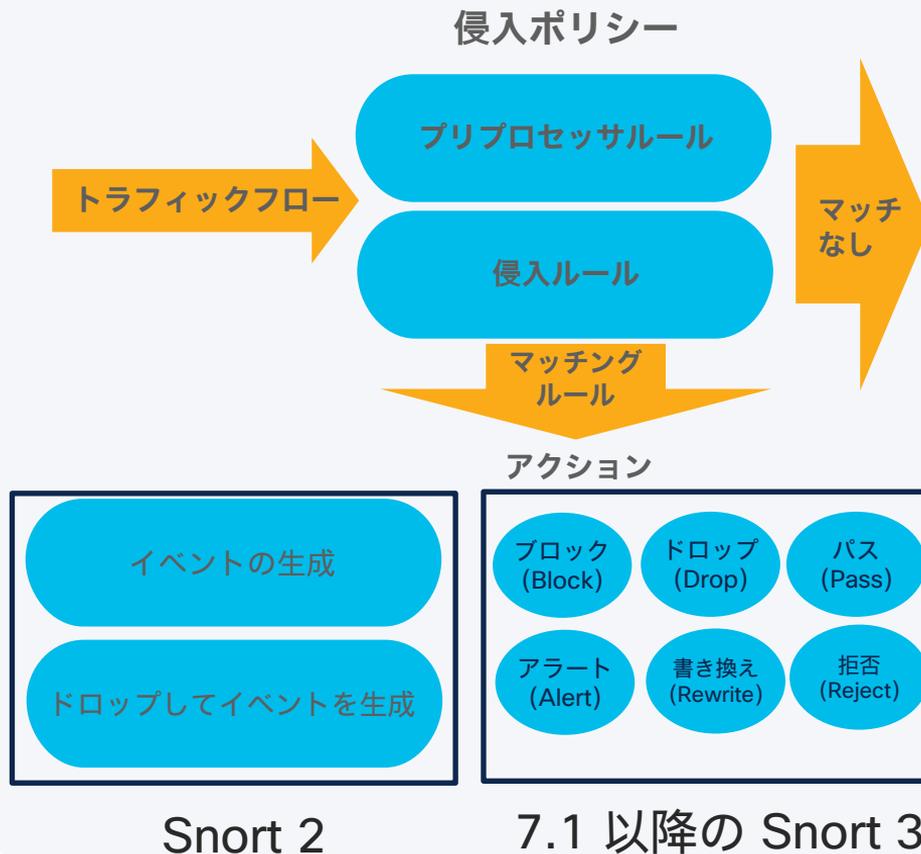
IPS 展開は次のいずれかのモードで可能

- 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パアレント 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



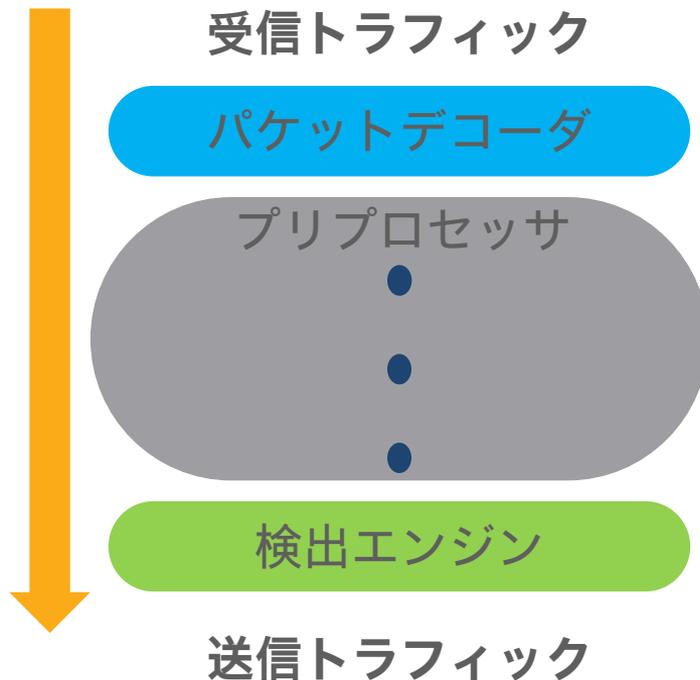
# デコーダとプリプロセッサ

## 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

## NAP ポリシー

デコーダ

プリプロセッサ

# 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

## ルールヘッダー

```
alert tcp $EXTERNAL_NET ANY -> $HTTP_SERVERS $HTTP_PORTS \
```

```
(msg:"SERVER-IIS newdsn.exe access"; flow:to_server, established; \  
content:"/scripts/tools/newdsn.exe"; nocase; http_uri; \  
metadata:ruleset community, service http; \  
reference:bugtraq,1818; reference:cve, 1999-0191; reference:nessus,10360; \  
classtype:web-application-activity; sid: 1024; rev:20; )
```

## ルールボディ

# 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



# 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

### New Variable Set

Name:

Description:

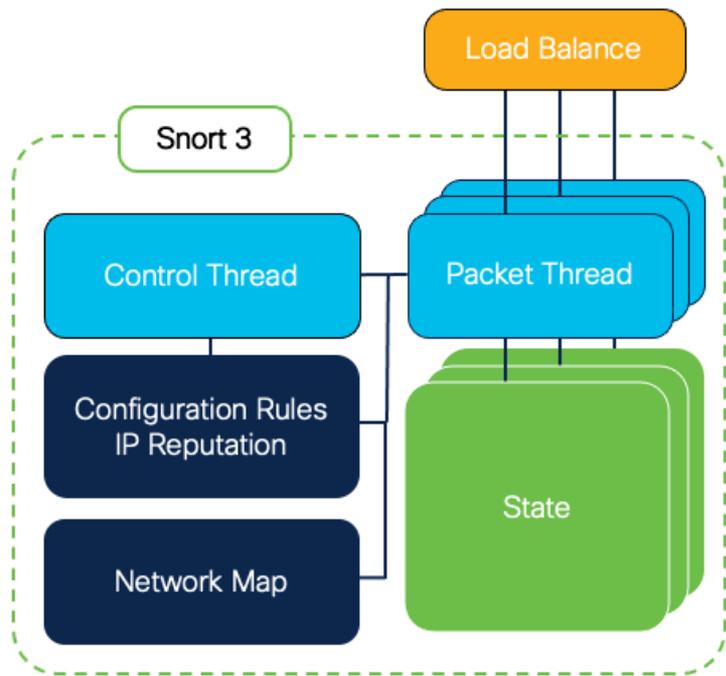
Variable Name	Type	Value	
Customized Variables			
This category is empty			
Default Variables			
DNS_SERVERS	Network	HOME_NET	<input type="button" value="edit"/> <input type="button" value="delete"/>
EXTERNAL_NET	Network	any	<input type="button" value="edit"/> <input type="button" value="delete"/>
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]	<input type="button" value="edit"/> <input type="button" value="delete"/>
FTP_PORTS	Port	[21, 2100, 3535]	<input type="button" value="edit"/> <input type="button" value="delete"/>

# 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

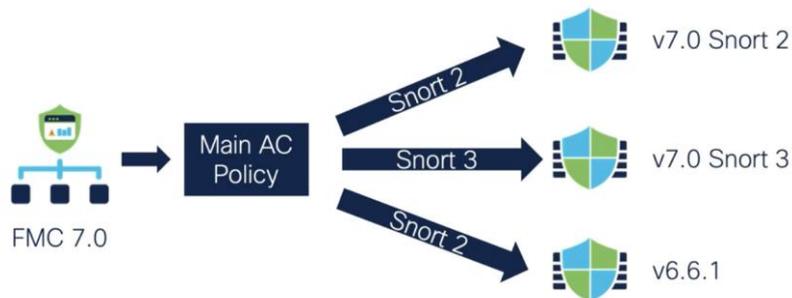
Firepower Management Center  
Policies / Access Control / Intrusion / Intrusion Policies

Overview Analysis Policies Devices Objects AMP Intelligence Deploy alext

Intrusion Policies Network Analysis Policies

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

Intrusion Policy	Description	Base Policy	Usage Information	Snort 2 Version	Snort 3 Version	
Balanced IPS Snort 3 is in sync with Snort 2		Balanced Security and Connectivity	No Access Control Policy No Device	Snort 2 Version	Snort 3 Version	
Secure IPS (migrated) Snort 3 is partially in sync with Snort 2. 2021-05-07 18:41:21		Security Over Connectivity	1 Access Control Policy 1 Device	Snort 2 Version	Snort 3 Version	



# Snort 3 に関する注意事項

- Syslog は ACP ポリシーに移動

The screenshot shows the 'Basic' configuration page for an intrusion policy. Under 'Default Syslog Settings', there are options to 'Send using specific syslog alert' and 'Use the syslog settings configured in the FTD Platform Settings policy'. A warning message states: 'At least one of the options in Default Syslog Settings must be selected if syslog is enabled and configured to use ACP policy logging settings on Access Rule, SSL, or Pre-Filter policy'. Below this, there are sections for 'IPS Settings' and 'File and Malware Settings', each with a checkbox to 'Send Syslog messages for...'.

- 新しいルールグループ

The screenshot shows the 'Rule Groups' configuration page for an intrusion policy. A blue box highlights the 'All Rules' section, which lists various rule groups such as 'Browser (9 groups)', 'Server (9 groups)', 'Policy (2 groups)', 'Indicator (4 groups)', 'Potentially Unwanted Applications (4 groups)', 'Malware (9 groups)', 'File (9 groups)', 'Operating Systems (9 groups)', and 'Protocol (14 groups)'. The 'All Rules' table on the right shows a list of rules with columns for 'Rule Action', 'Info', and 'Alert Configuration'.

- 抑制としきい値は [オブジェクト (Objects) ] に移動

The screenshot shows the 'All Rules' configuration page for an intrusion policy. The 'Rule Actions' column shows 'Disable (Default)' for several rules. The 'Alert Configuration' column shows 'None' for several rules. A tooltip is visible over the 'None' alert configuration, stating: 'Suppress intrusion event notification when a specific IP address or range of IP addresses triggers a specific rule or preprocessors.'



# 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）

## • ルールの更新方法が変更（LSP）

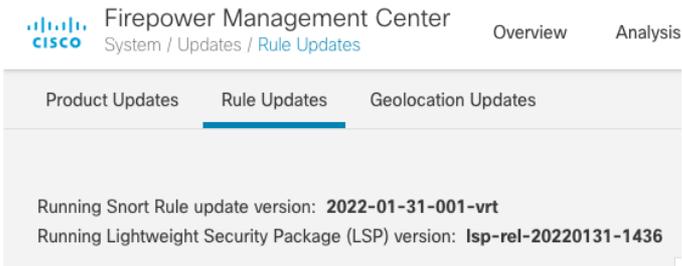
Snort 2のSRUに比べ、Snort 3のLSPでは柔軟性が向上しサイズが小さく

## • 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



The screenshot shows the Firepower Management Center interface. At the top, it says "Firepower Management Center" with the Cisco logo. Below that, it says "System / Updates / Rule Updates". There are two tabs: "Overview" and "Analysis". Under "Analysis", there are three sub-tabs: "Product Updates", "Rule Updates" (which is selected), and "Geolocation Updates". Below the sub-tabs, there is a box containing the following text: "Running Snort Rule update version: 2022-01-31-001-vrt" and "Running Lightweight Security Package (LSP) version: lsp-rel-20220131-1436".



# Snort 3 侵入ポリシー固有の機能

- ・ルールグループのオーバーライド

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

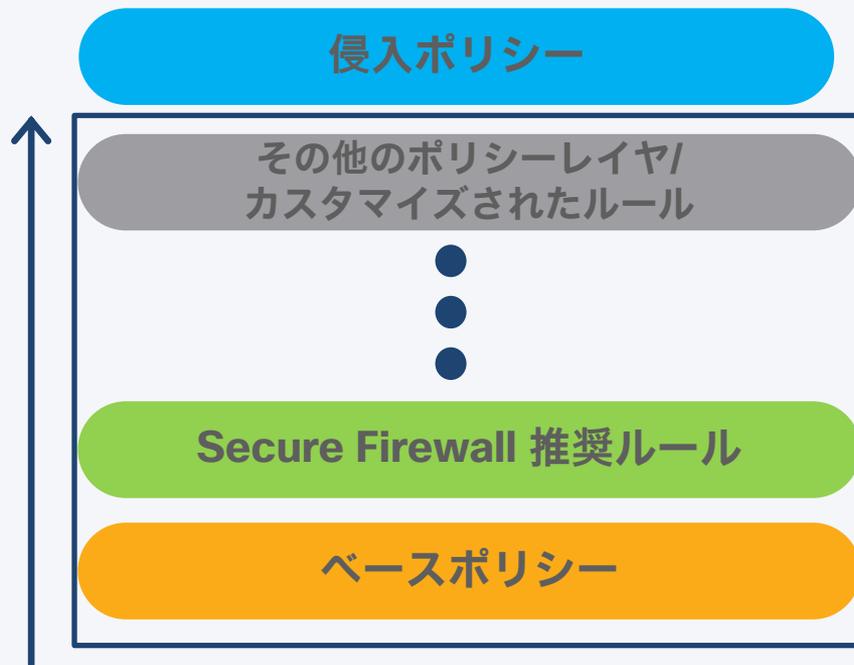
Summary	
51 items	All <span>×</span> <span>▼</span> <span>+</span>
All Rules	
> Local Rules (1 group)	
▼ Browser (6 groups)	
WebKit	<span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>1</span>
Plugins	<span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>1</span>
Firefox	<span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>1</span>
Other	<span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>1</span>
Chrome	<span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>1</span>
Internet Explorer	<span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>■</span> <span>1</span>

# 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**

## ベースポリシー

Connectivity over Security

Balanced Security and Connectivity

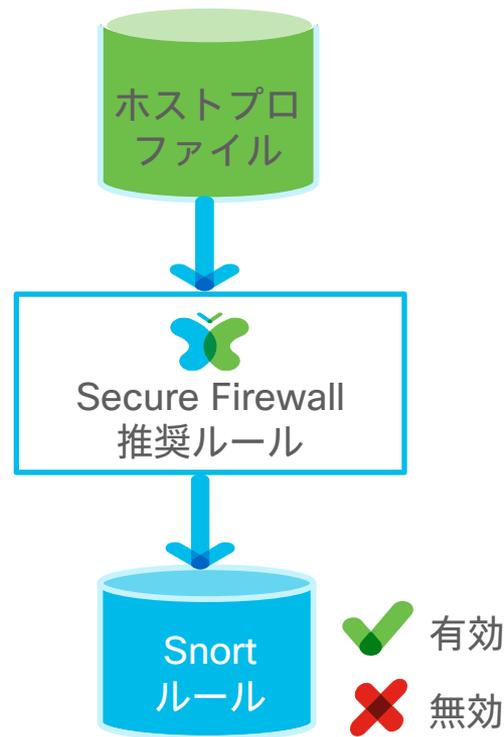
Security over Connectivity

有効なルールが少ない

保護レベルが高い

# 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

The screenshot displays the Cisco Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Intelligence'. The 'Analysis' tab is active, showing 'Events By Priority and Classification'. A search filter 'Predefined Searches' is highlighted. The main content area shows a table of events with columns for Time, Priority, Impact, Source IP, Destination IP, and Message. The table lists several events, including those related to malware (ZeusPanda) and data exfiltration.

	<input type="checkbox"/>	Time ×	Priority ×	Impact ×	Inline Result ×	Source IP ×	Source Country ×	Destination IP ×	Destination Country ×	Source Port / ICMP × Type	Destination Port / ICMP × Code	Message ×
▼	<input type="checkbox"/>	2021-06-18 11:56:56	low	3		10.1.112.31		104.20.16.113	USA	51723 / tcp	80 (http) / tcp	HI_CLIENT_IIS_UNICODE (119:7:1)
▼	<input type="checkbox"/>	2021-06-18 11:41:27	high	1	↓	10.1.119.9		185.43.223.6	NLD	49202 / tcp	80 (http) / tcp	MALWARE-CNC Win.Trojan.ZeusPanda outbound cnc connection (1:48499:1)
▼	<input type="checkbox"/>	2021-06-18 11:41:27	high	1	↓	10.1.119.9		185.43.223.6	NLD	49200 / tcp	80 (http) / tcp	MALWARE-CNC Win.Trojan.ZeusPanda outbound cnc connection (1:48504:1)
▼	<input type="checkbox"/>	2021-06-18 11:41:27	high	1	↓	10.1.119.9		185.43.223.6	NLD	49200 / tcp	80 (http) / tcp	MALWARE-CNC Win.Trojan.Zeus encrypted POST Data exfiltration (1:27919:5)
▼	<input type="checkbox"/>	2021-06-18 11:25:04	high	3	↓	192.99.198.158	CAN	10.1.22.9		80 (http) / tcp	50473 / tcp	EXPLOIT-KIT Angler exploit kit Internet Explorer encoded shellcode detected (1:319:1)
▼	<input type="checkbox"/>	2021-06-18 11:13:19	medium	3		10.1.45.16		64.12.249.201	USA	54245 / tcp	80 (http) / tcp	HI_CLIENT_OVERSIZE_DIR (119:15:2)
▼	<input type="checkbox"/>	2021-06-18 10:50:05	medium	3		10.1.104.64		95.172.94.20	GBR	57874 / tcp	80 (http) / tcp	HI_CLIENT_OVERSIZE_DIR (119:15:2)
▼	<input type="checkbox"/>	2021-06-18 10:48:01	medium	3		10.1.104.36		152.163.66.132	USA	60040 / tcp	80 (http) / tcp	HI_CLIENT_OVERSIZE_DIR (119:15:2)
▼	<input type="checkbox"/>	2021-06-18 10:42:33	low	3		10.1.88.14		50.17.197.129	USA	54231 / tcp	80 (http) / tcp	HI_CLIENT_IIS_UNICODE (119:7:1)
▼	<input type="checkbox"/>	2021-06-18 10:41:28	medium	3		10.1.78.4		95.172.94.56	GBR	54287 / tcp	80 (http) / tcp	HI_CLIENT_OVERSIZE_DIR (119:15:2)
▼	<input type="checkbox"/>	2021-06-18 10:32:27	high	1	↓	10.1.10.6		204.152.254.221	USA	49203 / tcp	80 (http) / tcp	MALWARE-CNC Win.Trojan.CryptoWall variant outbound connection (1:34318:5)

# 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。



