



シスコの Firewall は ASA だけじゃない! ~Cisco Firewall Threat Defense ご紹介~

2022年3月25日

シスコシステムズ合同会社

セキュリティ事業 テクニカルソリューションズアーキテクト

小林 達哉 (tatskoba@cisco.com)

アジェンダ

- Firewall Threat Defense の概要
- Firewall プラットホーム
- まとめと参考資料
- (Appendix) 技術者向け Firewall Threat Defense のアーキテクチャ

Firewall Threat Defense の概要

シスコの包括的なセキュリティポートフォリオ



ワールドクラスの
セキュリティコントロール



Secure Firewall Threat Defense



Secure Firewall ASA

TALOS Talos



一貫性のある
ポリシーと可視化



Secure Firewall Management Center



Secure Firewall Device Manager



Cisco Defense Orchestrator



SecureX threat response



Secure Network Analytics



統合された
セキュリティポートフォリオ



Secure Access by Duo



Secure Endpoint



TrustSec



Cisco Identity Services Engine



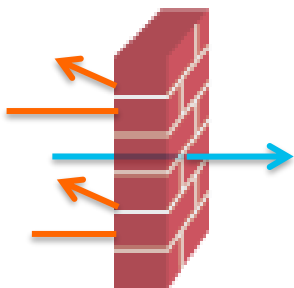
Rapid Threat Containment



Application Centric Infrastructure

現在の Firewall による脅威対策の課題

- 最新の脅威に追加の対策を行いたいが、何を選択すればよいのかわからない
- 次世代 Firewall は導入しているが、脅威対策としての性能には正直不安がある
- IPS やサンドボックスなどの専用機器の導入は、運用負荷が懸念



不正通信の防御

ファイアウォール



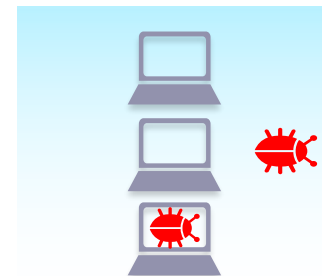
Web アプリケーション、ユーザ、
脅威の可視化

次世代ファイアウォール

```
01000111 0100 111001
0100 1110101001 1101 0011
011101 10001110100111
01 1110011 0110011 1010
00111 0100 1110101001
```

侵入検知と防御

IPS



不正プログラムの検知

サンドボックス

Firewall Threat Defense (FTD) が提供する脅威対策

次世代 Firewall



- ✓ アプリケーション制御
- ✓ ユーザ制御
- ✓ URL フィルタ
- ✓ Geo Location フィルタ

最も使われているIPS エンジン



- ✓ オープンソース IPS エンジン

運用の自動化 & イベント解析



- ✓ 自動チューニング、インパクト解析、インシデント相関分析
- ✓ 端末隔離機能 (ISE 連携)

ネットワークとホスト の可視化



- ✓ ネットワークとホスト学習

脅威情報フィルター



- ✓ Cisco 提供脅威情報活用
- ✓ 3rd パーティとの脅威情報連携

高度なマルウェア 防御



- ✓ シグネチャレスマルウェア検知
- ✓ マルウェアトラッキング
- ✓ クラウドリコール
- ✓ スレッドグリッドサンドボックス



ホストプロファイルの例

例)アラートが発生したホストの情報を確認したい

2020-07-30 15:38:32	medium	2	↓	192.168.10.101	192.168.20.102	8 (Echo Request) / tcp	0 (No Code) / icmp	Unknown (Unknown)	0	PROTOCOL-ICMP Und
2020-07-30 15:38:19	low	3	↓	146.112.41.2	NLD 192.168.20.102	443 (https) / tcp	49850 / tcp	Unknown (Unknown)	0	HI_SERVER_NO_CON
2020-07-30 15:37:51	high	2	↓	192.168.10.101	192.168.20.102	36735 / tcp	80 (http) / tcp	Unknown (Unknown)	0	SERVER-OTHER Novel

ホストプロフィール

IPアドレス 192.168.20.102
NetBIOS名
デバイス (Hop) FTDv66-1 (0)
MACアドレス(TTL) 00:0C:29:1D:47:5E (VMware, Inc.) (128)
ホストタイプ Host
最後の発見 2020-08-03 17:01:57
現在のユーザ

表示 [コンテキストエクスプローラ](#) | [接続イベント](#) | [侵入イベント](#) | [ファイアウォール](#) | [Malwareイベント](#)

アプリケーション (60)

アプリケーションプロトコル	クライアントアプリケーション
<input type="checkbox"/> DNS over HTTPS	<input type="checkbox"/> DNS over HTTPS
<input type="checkbox"/> SSL	<input type="checkbox"/> SSL client
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client
<input type="checkbox"/> SSL	<input type="checkbox"/> SSL client
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client

クライアントアプリケーション

侵入の痕跡 (1)

侵入の痕跡

カテゴリ	イベントタイプ	説明	最初の発見	最後の発見
Impact 2 Attack	Impact 2 Intrusion Event - attempted-user	The host was attacked and is potentially vulnerable	2020-07-30 15:37:51	2020-07-30 15:37:51

オペレーティングシステム

端末 OS

ベンダー	製品	バージョン	送信元
Microsoft	Windows	7, Server 2008, Phone 7.5, 8	Firepower

サーバ (15)

サーバアプリケーション

プロトコル	ポート	アプリケーションプロトコル	製造元およびバージョン
tcp	8000
tcp

User History

ユーザ履歴

Users	2020-08-03 09:05:39
Discovered Identities\setsuko.overton (LDAP)	...
armando zuniga (dcloud.cisco.com\azuniga, LDAP)	...

脆弱性 (1022)

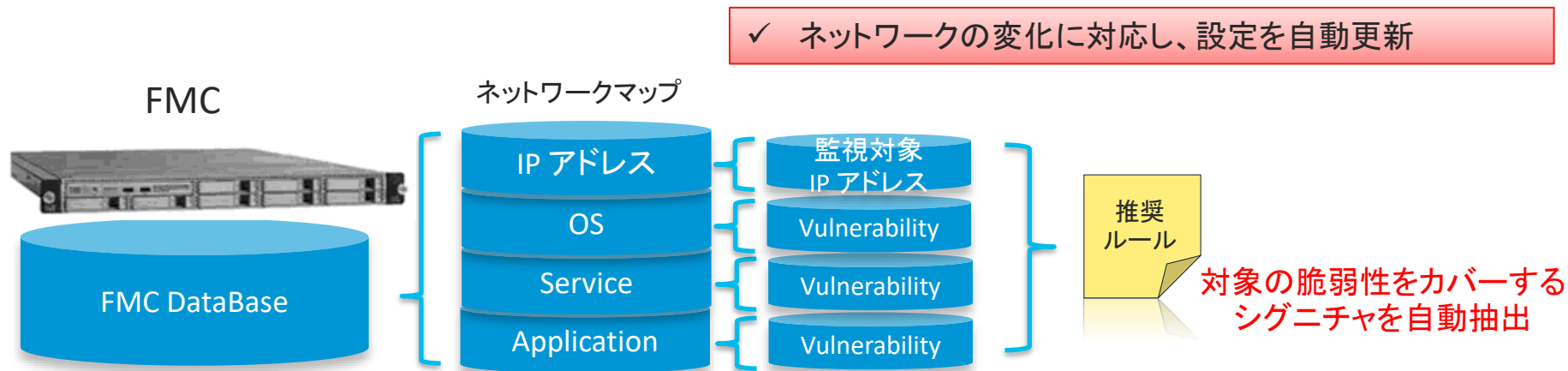
該当脆弱性リスト

名前	ポート
A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system, aka "Microsoft JET Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012	Windows 7, Server 2008, Phone 7.5, 8
A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system, aka "Microsoft JET Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012	Windows 7, Server 2008, Phone 7.5, 8
A DCOM object in Helppane.exe in Microsoft Windows 7 SP1; Windows Server 2008 R2; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows local users to gain privileges	Windows 7, Server 2008, Phone 7.5, 8

✓ 端末のセキュリティに関連する様々な情報を自動収集し、解析に活用

自動チューニング

- 対象ネットワークの保護に必要なシグネチャおよびアクション(イベント生成、ドロップ)を抽出
- 推奨設定の生成および適用は、オンデマンドまたはスケジューリングに対応



- ✓ 必要なシグネチャをのみを有効化することにより、誤検知を大幅削減

インパクトフラグ

- 全ての IPS イベントを、ターゲットホストの脆弱性情報と関連づけて解析
- 緊急度の高いイベントのみに、高インパクトのフラグを付けてアラート

- インパクトフラグ1 – 即時対応が必要

※ IDS (パケットドロップなし) の場合

- インパクトフラグ2 – 要調査

- インパクトフラグ3 – 対応の必要なし

		攻撃の危険度		インパクトフラグ		
2020-08-03 09:22:00	medium	3		3	10.1.120.17	62.51.0.36
2020-08-03 09:17:52	high	1	↓	2	10.1.108.15	144.76.133.38
2020-08-03 09:17:32	high	2	↓	3	10.1.114.34	10.100.9.4
2020-08-03 09:11:25	high	1	↓	1	10.1.104.115	188.120.225.17

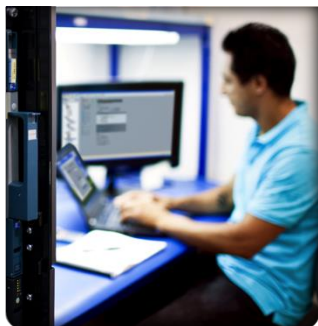
インパクトフラグ	FMC によりターゲットネットワークが監視されている	FMC によりターゲットホストが監視されている	攻撃がターゲットのポート、アプリケーションに該当	攻撃がターゲットの持つ脆弱性に該当
1	Yes	Yes	Yes	Yes
2	Yes	Yes	Yes	No
3	Yes	Yes	No	No
4	Yes	No	Unknown	Unknown
0	No	No	Unknown	Unknown

自動チューニング(推奨設定)とインパクト解析

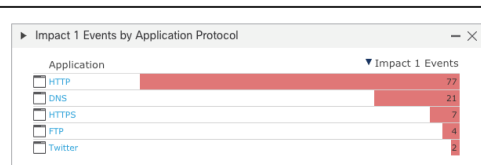
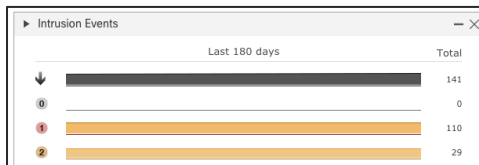
一般的な侵入検知機器 (IPS) の
運用者が抱える問題

環境に合わせて設定を調整
したいが、運用が大変...

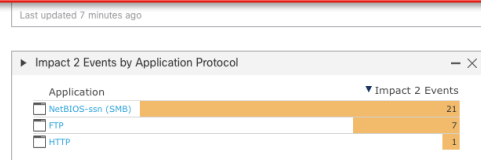
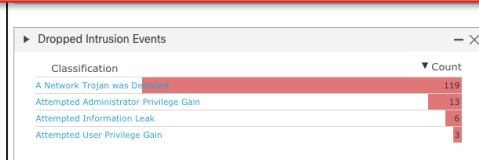
沢山のログが出るが、本当に
重要なものがわからない...



自動チューニング(推奨設定)
ネットワーク環境を学習し、
最適な推奨設定を自動生成

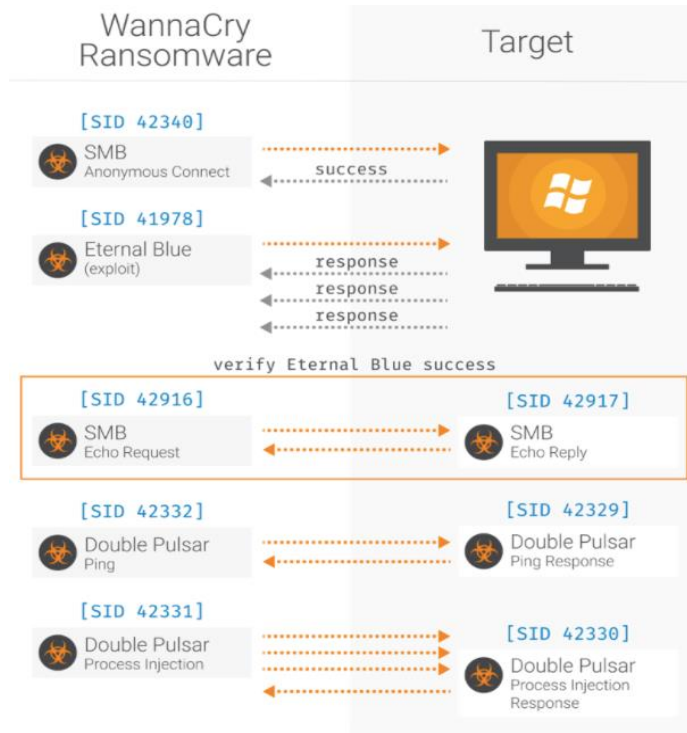


インパクト解析 攻撃と対象端末情報を解析し、本当に危険度の高いログを識別



Snort IPS ルール

- 単なる脆弱性を突く攻撃だけでなく一連の攻撃プロセスに沿った豊富な検知ルール
 - 外部だけでなく内部通信からも脅威検出
- Exploit-Kit / Malware-Backdoor / MS 脆弱性情報などカテゴリーごとに Snort IPS ルール分類
- Snort 言語と正規表現により内容確認可能
 - 全ルールの検知ロジック開示が可能
- 推奨ルール、自動チューニング
 - Cisco Talos 推奨ルール利用、もしくはホストプロファイルから学習した脆弱性情報に基づいてチューニング



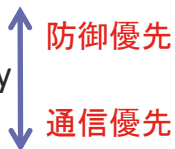
Snort 2 でのルール記述例

```
rule alert udp $HOME_NET any -> any 53 (msg:"APP-DETECT 12P DNS request attempt"; flow:to_server; byte_test:1,!&,0xF8,2; content:"[03|b32|03|i2p|00]"; fast_pattern:only; metadata:policy max-detect-ips drop, service dns; reference:url,geti2p.net; classtype:misc-activity; sid:37062; rev:2; gid:1; )
```

IPSポリシーの設定

・ ベースポリシー (ベンダー推奨ポリシー) の選択

- ・ Security Over Connectivity
- ・ Balanced Security and Connectivity
- ・ Connectivity Over Security



・ 自動チューニングの利用

- ・ FMC が推奨設定を生成
- ・ ベースポリシーを上書き

・ カスタムチューニング

- ・ ベースポリシーおよび推奨設定を上書き

侵入ポリシーの編集

名前*
INTRUSION-1

説明

インスペクションモード
 検知 防止

侵入ルールアクションが常に適用されます。切断ルールに一致しない接続はブロックされます。

ベースポリシー
Balanced Security and Connectivity

キャンセル 保存

Firepowerルールの推奨事項

セキュリティレベル (サイズを選択するには、タイルをクリックします)

ルールを無効にする推奨事項に同意する

Higher Efficiency - Keeps existing rules that match potential vulnerabilities on discovered hosts and disables rules for vulnerabilities not found on the network.

保護ネットワーク 追加+

キャンセル 生成 生成と適用

推奨ルール

Firepowerでは、次の状態設定を9,183 ルールにすることを推奨しています。 2 ネットワーク 生成: 2022-03-04 19:07:36

ルールアクション Q CVE, SID, 参照情報, またはルールメッセージによる検索

9,183個の規則 プリセットフィルタ: 231アラートルール | 5,544ブロックルール | 3,408無効化されたルール | 0オーバーライドされたルール | 新しい推奨事項

Snort 2 vs. Snort 3

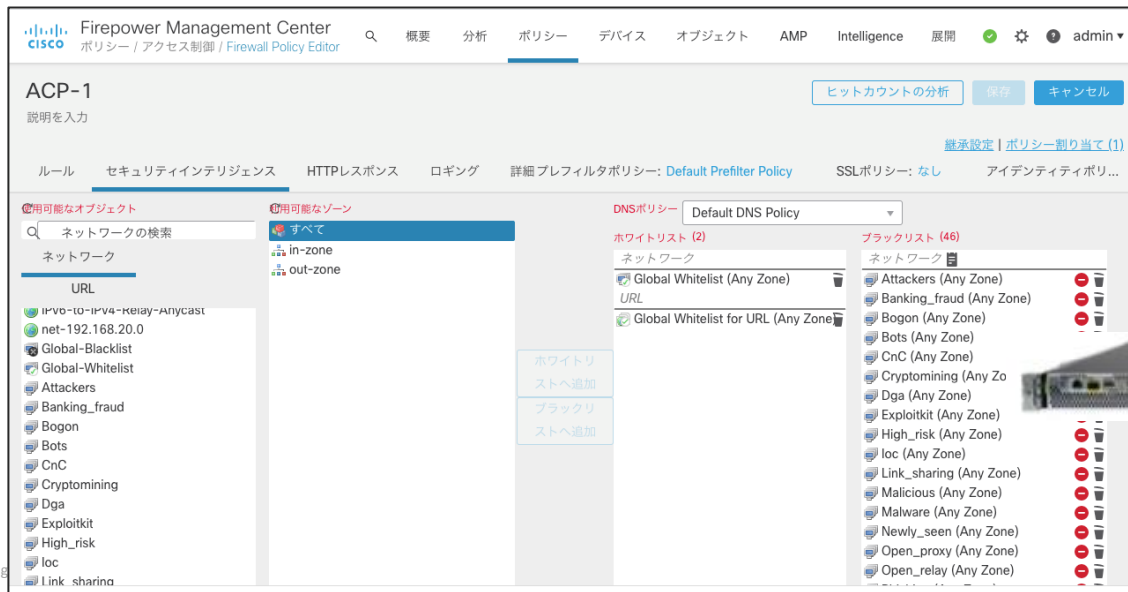
バージョン 7.0 より Snort 3 エンジンをサポート

	Snort 2	Snort 3
マルチスレッドアーキテクチャ		✓
複数の Snort プロセス稼働	✓	✓
ポート番号から独立したプロトコルのインスペクション		✓
IPS でのアクセラレータ/ハイパースキャンをサポート		✓
モジュール性 – TALOS からの情報を容易に取り込み		✓
スケーラブルなメモリ割り当て		✓
次世代 TALOS ルール – 正規表現 / ルール最適化 / バッファ		✓
新しい HTTP インスペクタ – HTTP/2 をサポート		✓
TALOS からのアップデートを小型化		✓

Security Intelligence 脅威情報フィルタ



- Cisco Collective Security Intelligence 提供のブロックリスト IP アドレス、URL、ドメインに基づく制御 (i.e. レピュテーション)
- 既知のブロックリスト宛て or からの接続を モニターもしくははブロック
- カテゴリー
 - CnC
 - Malware
 - Phishing
 - Bots
 - Attackers など



Threat Intelligence Director

サードパーティの脅威情報により、FTD 脅威情報機能を強化

サードパーティ:

- Crowdstrike
- Flashpoint
- Soltra Edge
- EclecticIQ
- Lookingglass etc..



レポート先:

- SIEM
- インシデントマネージメントツール



シスコ:

- TALOS
- Threat GRID サンドボックス

FTD イベントログ

Type	Name	Source	Incidents	Action	Publish	Last Updated	Status
IPv4	1.1.1.1 <i>Indicator Imported From a Flat File</i>	test	1	Monitor	Block Monitor	Jul 24, 2018 6:18 AM EDT	Completed

ジオロケーション

- IP アドレスと国や地域を紐づけたジオロケーションデータベース
- IPS、アプリケーション制御、ファイルポリシー等の任意の設定と組み合わせて利用可

The screenshot displays the 'Rule Addition' (ルールの追加) configuration page. The rule name is 'Monitoring from some countries', which is active (有効). The rule is applied to 'Rule 2' (ルールの下) with a priority of 2. The action is set to 'Allow' (承認) and the time range is 'None' (なし). The configuration is applied to the 'Network' (ネットワーク) zone.

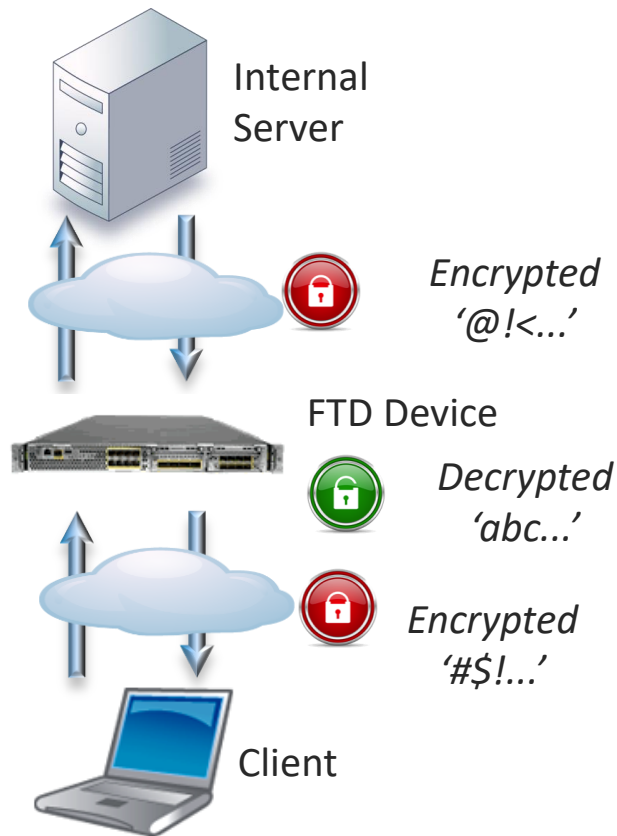
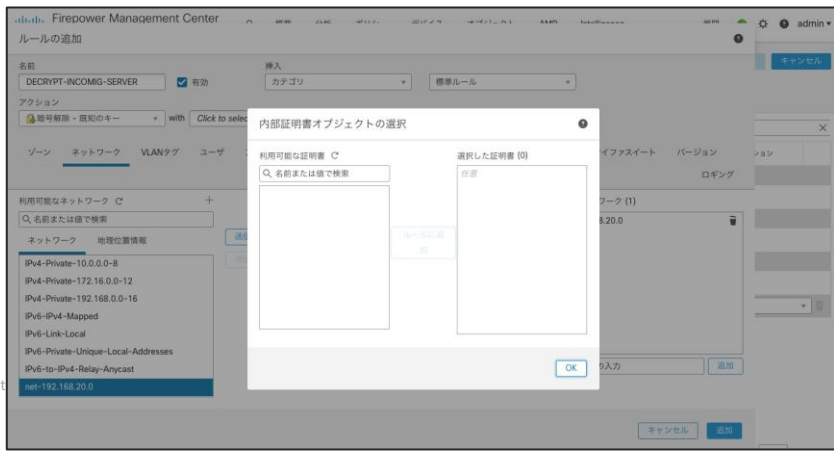
Under the 'Network' tab, the 'Available Networks' (利用可能なネットワーク) section shows a search bar and a tree view of geographical regions. The 'Asia' region is expanded, listing countries like Afghanistan, Armenia, Azerbaijan, Bahrain, and Bangladesh. There are buttons to add selected networks to the 'Source Networks' (送信元ネットワーク) or 'Destination Networks' (送信先ネットワーク) lists.

The 'Source Networks' (送信元ネットワーク) list currently contains three entries: China, United States, and Russian Federation. The 'Destination Networks' (送信先ネットワーク) list is currently empty.

At the bottom, there are input fields for 'IP Address Input' (IPアドレスの入力) with 'Add' (追加) buttons for both source and destination networks.

TLS 暗号化アクセラレーション

- TLS で暗号化された通信を復号してインスペクションを行う機能
- inbound inline
- outbound inline
- ハードウェア処理が可能なモデルと不可能なモデルがあるため、パフォーマンス見積もりに注意
- TLS 1.3 ネイティブには未対応(次期バージョンにて対抗予定あり)、TLS 1.2 にダウングレードしてのインスペクションは可能



Malware Defense マルウェアの可視化と制御、トラッキング

Malware Summary (ワークフローの切り替え) 2020-07-27 17:57:00 - 2020-08-03 18:52:24
展開しています

検索の制限がありません (検索を編集)

Malware Summary Malwareイベントの表ビュー

次へ移動...

<input type="checkbox"/>	検知名	ファイル名	ファイルSHA256	ファイルタイプ	カウント
▼	EICAR	eicar.com	275a021b...f651fd0f	EICAR	1

① ファイルをハッシュ値で特定
(端末で検知したマルウェアもブロック可能)

275a021b...f651fd0fのネットワークファイルトラジェクトリ

ファイルSHA256	275a021b...f651fd0f	First Seen	2020-08-03 18:51:51 オン	192.168.10.101	実行者: No Authentication Required
ファイル名	eicar.com	Last Seen	2020-08-03 18:53:54 オン	192.168.10.101	実行者: No Authentication Required
File Size (KB)	0.0664	時間	2020-08-03 18:53:54	14	
ファイルタイプ	EICAR	イベントタイプ	送信されたファイル	2ホスト	
File Category	Executables	IPアドレス	192.168.10.101	送信者数: 1 → 受信者数: 1	
Current Disposition	Malware	ブロックされた受信者	192.168.20.102		
Threat Score	Very High	アクション	Malware Block		
検知名	EICAR	アプリケーションプロトコル	HTTP		
Trajectory		クライアント	Chrome		
		Aug 03			
		18:51 18:53			
192.168.10.101					
192.168.20.102					

Events: Transfer, ブロック, Create, 移動, Execute, Scan, 検出, Quarantine

Dispositions: Unknown, Malware, クリーン, カスタム, Unavailable

時間	イベントタイプ	送信側IP	受信側IP	送信者	受信者	ファイル名	ファイルタイプ	ファイルSHA256	検知名	アクション
2020-08-03 18:...	転送	192.168.10.101	192.168.20.102	No Authentication Required	eicar.com	Malware	Malware Block	HTTP	Chrome	
2020-08-03 18:...	転送	192.168.10.101	192.168.20.102	No Authentication Required	eicar.com	Malware	Malware Block	HTTP	Chrome	

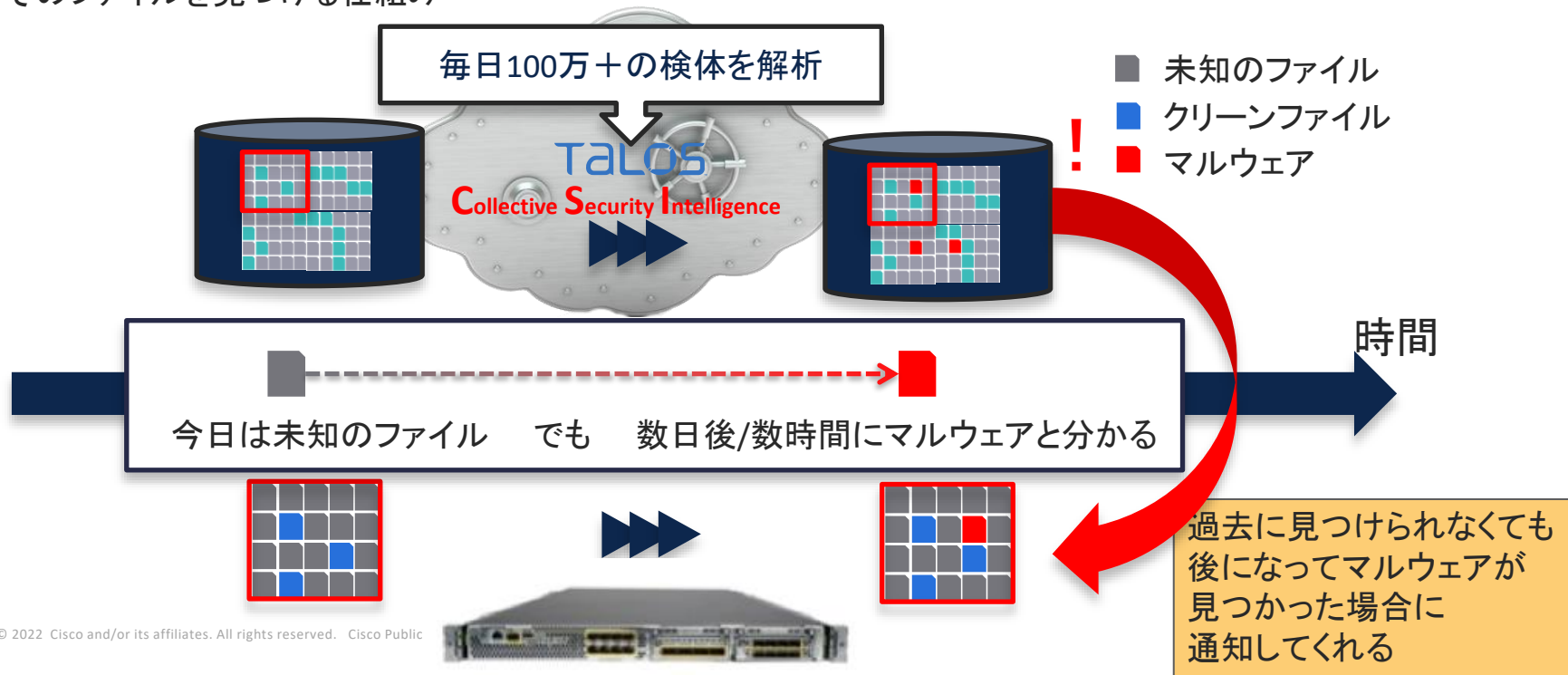
② 解析情報(サンドボックス含む)と連携

④ 端末の特定

③ ネットワーク上での拡散状況を可視化

Malware Defense クラウドリコール

一度調査したファイルを覚えておき、合致するマルウェアが見つかった場合に瞬時にそのファイルを見つける仕組み



クラウドリコールによるゼロデイマルウェア検知例

Firepower Management Center
分析 / ファイル / ネットワークファイルトラジェクトリ

4b061e78...4d18e0b0のネットワークファイルトラジェクトリ

ファイルSHA256 4b061e78...4d18e0b0
ファイル名 malware.exe
File Size (KB) 136.2607
ファイルタイプ MSEXE
File Category Executables
Current Disposition Malware
Threat Score None

First Seen 2020-08-04 17:56:37 オン 192.168.10.101 実行者: No Authentication Required
Last Seen 2020-08-04 17:57:38 オン 192.168.20.102 実行者: No Authentication Required
イベント 2
Seen On 3ホスト (2件表示)
Seen On Breakdown 送信者数: 2 → 受信者数: 2 (1 → 1件表示)

Trajectory

Aug 04
17:56 17:57

192.168.10.101
192.168.20.102

Events Transfer ログ Create 移動 Execute Scan Retrospective Quarantine
Dispositions Unknown Malware クリーン カスタム Unavailable

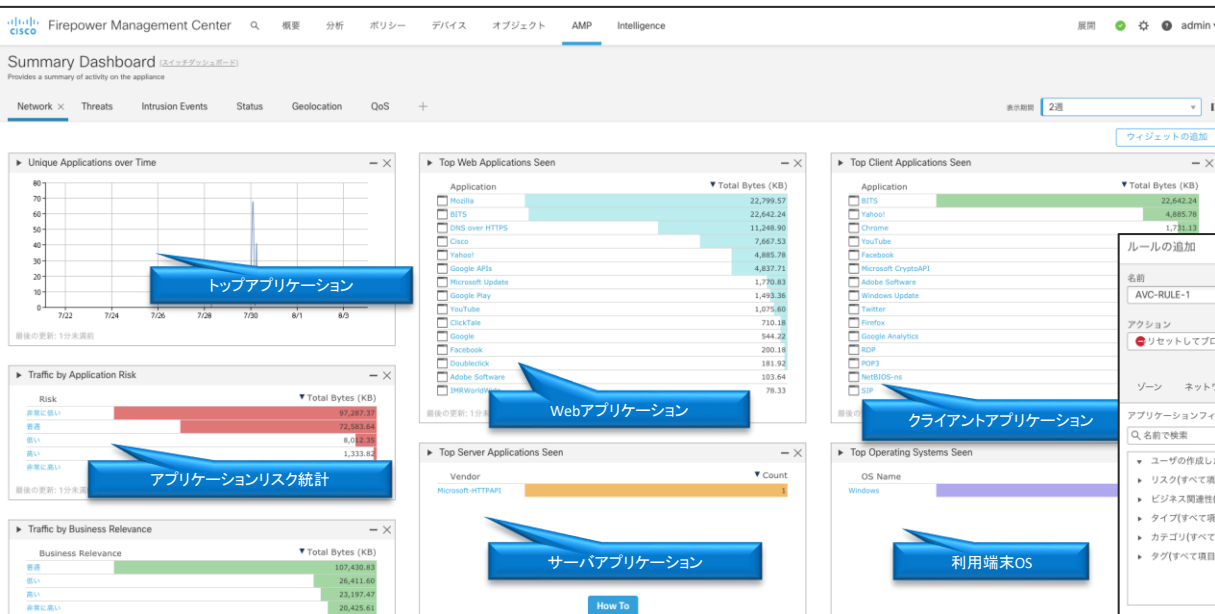
Events

時間	イベントタイプ	送信側IP	受信側IP	ユーザ	ファイル名	傾向	アクション	プロトコル	クライアント	ウェアアプリケ	説明
2020-08-04 17:56:37	転送	192.168.10.101	192.168.20.102	No Authentication Required	malware.exe	Unknown	Malware Cloud Look...	HTTP	Chrome		Retrospective Event (L...
2020-08-04 17:57:38	回顧的イベント					Malware					Malware Detected by ...

このケースでは最初の時点では既存セキュリティをすり抜けてしまったマルウェアを、1分後にリコールで検知している

Application Visibility Control アプリケーションの可視化と制御

利用されている Web アプリケーション、クライアントアプリケーション、サーバアプリケーション、利用量、リスク統計から、問題点を的確に捉え、アプリケーション制限を実施し、リスクを軽減することが可能



3,500 以上のアプリケーションから、利用状況をチェック

問題のあるアプリケーション、利用している端末を割り出し、利用の制限を実施し内在するリスクを軽減

The screenshot shows the "ルール追加" (Add Rule) configuration page. The rule name is "AVC-RULE-1" and it is active. The action is "リセットしてブロック" (Reset and Block). The rule is applied to the "アプリケーション" (Application) zone. The configuration includes a list of applications to be blocked, such as "050plus", "1&1 Internet", "1-800-Flowers", "1000mercis", "100Bao", "12306.cn", "123Movies", and "126.com".

Custom Report レポート機能

柔軟なレポート機能: レポートデザイナー機能でフルカスタマイズ可能

作成したレポートを任意のメールアドレスへ自動転送

PDF、HTML、CSV形式をサポート

ネットワークレポート

SD-WAN Cisco ネットワーク リポート

I. 概要

シスコは、シスコシステムズ: aCloudが検出したリスクの状態にあると判断しました。その理由は、シスコは、最新の脅威情報から、最近の脆弱性やリスクのあるソフトウェアアップデートを適用しているためです。これらのアップデートは、ネットワークを攻撃に対して脆弱なままにしたり、マルウェアを伝播したり、脅威を減らす可能性があります。

詳細期間: Sat Apr 29 2017 04:25:53 ~ Mon May 29 2017 04:25:53

リスクのあるアップデート 9	リスクのあるユーザ 18	高権限アプリケーション 1
暗号化アプリケーション 9	セキュリティ関連機能を持つアプリ 2	危険な Web ブラウザ 56

ネットワークプロファイル

オペレーティングシステム 10	モバイルデバイス 8	使用中的アプリケーション 83	転送されるファイルタイプ 5
--------------------	---------------	--------------------	-------------------

推奨

シスコは、シスコシステムズ: aCloudがアプリケーション脆弱性と脆弱なプラグインをシスコ Firepower アプライアンスに検出していることを通知します。アプリケーション更新の適用を促すアップデート、パッチ、更新、脆弱性、および脆弱なソフトウェアのインストールを必要とするモバイルデバイスや WDC のリスクを自己ネットワークのリスクと統合して視覚化する。

アタックレポート

SD-WAN Cisco 攻撃 リポート

I. 概要

シスコはシスコシステムズ: aCloudが検出したリスクの状態にあると判断しました。その理由は、悪質なホストを識別した危険なネットワーク上で検出されたからです。リスクを軽減するために、これらの攻撃とリスクを自己ネットワークに転送する必要があります。

詳細期間: Sat Apr 29 2017 04:24:27 ~ Mon May 29 2017 04:24:27

合計攻撃数 28,675	軽減する攻撃数 0	脆弱となったホスト 0
無関係な攻撃 100%	注意が必要なイベント 0%	CnCサーバに接続されているホスト 0

関連の攻撃によりもたらされるリスク

攻撃	カウント
Prevalent bot traffic	6,888
Advanced Information Leak	8,900
Unknown Traffic	5,899
Site scripts	2,257
Information Leak	1,961

シスコは、シスコシステムズ: aCloudが Cisco Firepower アプライアンスを導入して実行することを勧めます。
1. ネットワーク全体のリスクに対する脆弱性の可能性を減らす。
2. このリスクを軽減するために自動化された保護を適用する。

マルウェアレポート

SD-WAN Cisco 高度なマルウェア リポート

I. 概要

シスコは、シスコシステムズ: aCloudが検出されたマルウェアファミリーによる攻撃を検出しており、高いリスクであると判断しました。脅威情報から、Cisco Advanced Malware Protection (AMP) が導入されました。このレポートは、この期間にネットワークで検出された攻撃を示すものです。

詳細期間: Sat Apr 29 2017 04:24:27 ~ Mon May 29 2017 04:24:27

マルウェアを検出 36	IOC を示しているホスト 19	連絡プロトコル 2
CnCサーバに接続されているホスト 0	マルウェアの通信 22	マルウェアの URL 2

マルウェアのプロファイル: 30 日

さまざまなマルウェアファミリーがダウンロード 27	ダウンロード元: 3	ダウンロードの実行数: 3	ダウンロード先: 7
	自の固有のホスト	人のユーザ	自のデバイス

シスコは、Advanced Malware Protectionを導入して実行することを勧めます。
1. 高度なマルウェアの継続的な可能性を減らす。
2. このリスクを軽減するために適切な制御を強化する。

FTD の市場評価

2020年の Forrester Wave で、エンタープライズ ファイアウォール分野のリーダーにシスコが選出

詳しくは以下の記事を参照

<https://gblogs.cisco.com/jp/2020/08/cisco-named-a-leader-in-the-2020-forrester-wave-for-enterprise-firewalls/>



Cisco Japan Blog > セキュリティ



セキュリティ

エンタープライズ ファイアウォール分野の Forrester Wave 2020 年版でシスコがリーダーに選出



小林 達哉
2020年8月25日

この記事は、*Network, Cloud and Workload Security* の Senior Director Product Management 担当である Chandrodya Prasad によるブログ「*Cisco Named a Leader in the 2020 Forrester Wave for Enterprise Firewalls*」(2020/8/11) の抄訳です。



『The Forrester Wave™: Enterprise Firewalls, Q3 2020』をダウンロードしてご覧ください

組織のセキュリティ体制の根幹は、長らくファイアウォールが支えてきました。しかし、単一のネットワーク制御ポイントで対応するという旧来の考え方は、もはや通用しなくなっています。アプリケーションとデータがクラウドに移行し、ユーザがあらゆる場所で業務をするようになったためです。組織は、各種の物理アプライアンスと仮想アプライアンスを追加することで、従来型ファイアウォールの強化を進めています。これらはネットワークに組み込まれる場合もあれば、サービスとして提供される場合もあります。ホストベースの場合もあれば、パブリッククラウドの環境に制御機能として直接実装される場合すらあります。

Firewall プラットホーム

Cisco Secure Firewall ブランドネーム変更

Firepower Management
Center (FMC)



Cisco Secure Firewall Management
Center (FMC)

Firepower Threat Defense
(FTD)



Cisco Secure Firewall
Threat Defense (FTD)

Adaptive Security
Appliance (ASA)



Cisco Secure Firewall
ASA

Firepower Threat Defense
Virtual / NGFWv



Cisco Secure Firewall
Threat Defense Virtual (FTDv)



Firewall Management Center (FMC) 概要

- FTD デバイスをまとめて管理
- Access Control Policy 等、各 Policy を共有可能



FTD Virtual 版と FP2110 を 1台の FMC で管理している例

The screenshot shows the Firepower Management Center interface. The top navigation bar includes "概要", "分析", "ポリシー", "デバイス", and "オブジェクト". Below the navigation bar, there are status indicators for "すべて (2)", "エラー (0)", "警告 (0)", "オフライン (0)", "正常 (2)", and "導入保留中 (0)". A table lists the managed devices:

名前	モデル	バージョン	シャーシ	ライセンス
FP2110-b1 10.71.153.56 - Routed	FTD on Firepower 2110	6.4...	N/A	ベース、脅威 (2 more...)
FTDv66-1 10.71.132.199 - Routed	FTD for VMWare	6.6.0	N/A	ベース、脅威 (2 more...)

✓ FP2110-b1 10.71.153.56 - Routed	FTD on Firepower 2110	6.4....
✓ FTDv66-1 10.71.132.199 - Routed	FTD for VMWare	6.6.0

Firewall Management Center プラットフォーム一覧



FMC1600

最大 50個のセンサー管理
最大イベント数 3,000万件
900GB のイベントストレージ
最大 5万ホスト、5万ユーザの
ネットワークマップ
HA対応



FMC2600

最大 300個のセンサー管理
最大イベント数 6,000万件
1.8TB のイベントストレージ
最大 15万ホスト、15万ユーザの
ネットワークマップ
HA対応



FMC4600

最大 750個のセンサー管理
最大イベント数 3億件
3.2TB のイベントストレージ
最大 60万ホスト、60万ユーザの
ネットワークマップ
HA対応



Virtual FMC

最大 25個のセンサー管理
最大イベント数 1,000万件
250GB のイベントストレージ
最大 5万ホスト、5万ユーザの
ネットワークマップ
300個のセンサー管理対応
モデルも有り (FMCv300)
HA対応 (VMware のみ)

FTD の機能を最大限に引き出す管理サーバ

Firewall Device Manager (FDM) 概要

無料で提供される OnBox の **FTD** ローカル管理ツール

- Web ブラウザで FTD デバイスに直接アクセスして FTD の設定・管理を行うことが可能

The screenshot displays the Cisco Firepower Device Manager (FDM) web interface. At the top, the navigation menu includes '監視', 'ポリシー', 'オブジェクト', and 'デバイス: FTDv66-2'. The main content area shows a network diagram with a central 'Cisco Firepower Threat Defense for VMWare' device connected to '内部ネットワーク' and 'ISP/WAN/ゲートウェイ'. Below the diagram, there are several management tiles:

- インターフェイス**: 接続中, 9の中の3が有効, すべてのインターフェイスの表示 >
- ルーティング**: 1個のスタティックルート, 設定の表示 >
- 更新**: 位置情報、ルール、VDB、システムアップグレード、セキュリティインテリジェンスのフィード, 設定の表示 >
- システム設定**: 管理アクセス, ログインの設定, DHCPサーバ, DNSサーバ, 管理インターフェイス, ホスト名, タイムサービス, クラウドサービス, 詳細を確認する
- スマート ライセンス**: 登録済み, 設定の表示 >
- バックアップと復元**: 設定の表示 >
- トラブルシューティング**: まだ作成されたファイルがありません, 作成するファイルの要求
- サイト間VPN**: まだ接続がありません
- リモート アクセス VPN**: RA VPNライセンスが必要, 接続がありません | 1グループポリシー
- 詳細設定**: 次を含む: FlexConfig, スマートCLI
- デバイス管理**: 監査イベント、デプロイ履歴、設定のダウンロード

FMC を導入して FTD の全機能を使うよりも、**FMC を導入せずにシンプルに FTD を管理したい**、というユースケースに対応

<FMC にあって FDM 未対応の主な機能>

- ネットワークマップ
- IPS ルール自動チューニング
- IPS インパクトフラグ
- Malware Defense Threat Grid を使った動的解析
- トランスペアレントファイアウォール
- クラスタリング

FTD の管理・設定アーキテクチャ

FTD デバイスの設定・管理には以下のどれかが必要。コンソール CLI は初期設定時およびトラブルシューティング時にしか使わない

FMC 管理

複数の FTD に対し、高度なセキュリティ監視・管理と設定を実施

FTD 本体



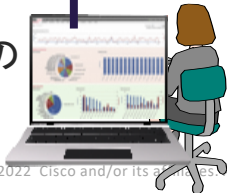
SF Tunnel
互いの Management Interface 間にて TCP/8305 で通信
設定、管理、Event 出力等

FMC



https
ブラウザで管理・設定

FMCの
画面



FDM 管理

基本的なセキュリティポリシーを、シンプルに1つの FTD に対して実施

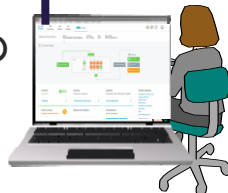
FTD 本体



https
ブラウザで管理・設定

FDM
= Firewall Device Manager

FDMの
画面



CDO 管理

FTD だけでなく ASA や Meraki MX も含めて複数デバイスを同時にクラウドから管理

Cisco Defense
Orchestrator

Internet

https
ブラウザで
管理・設定

CDOの
画面

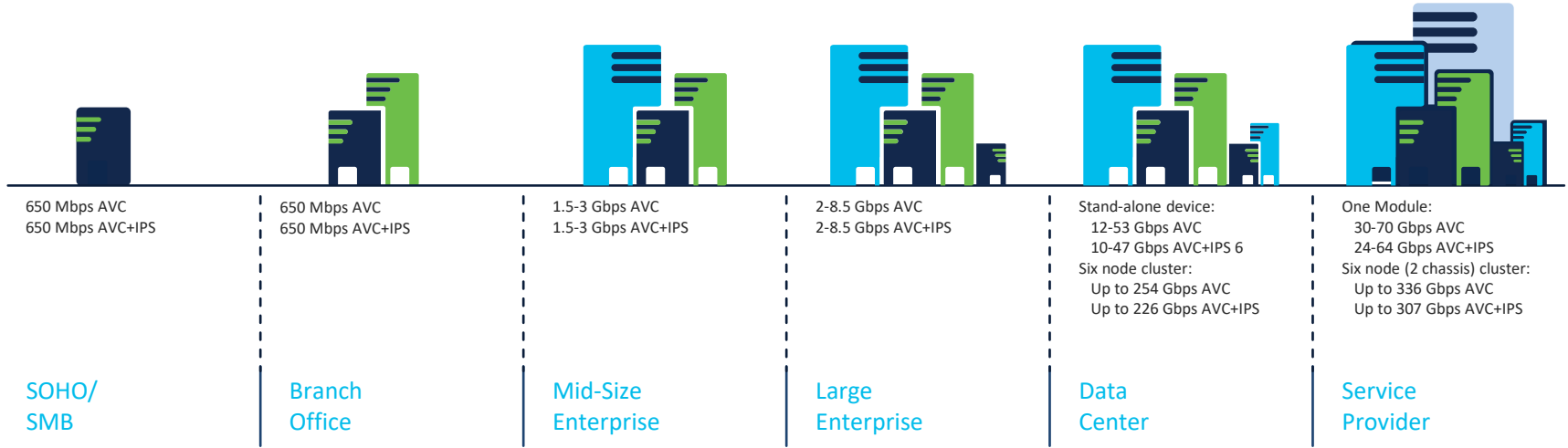
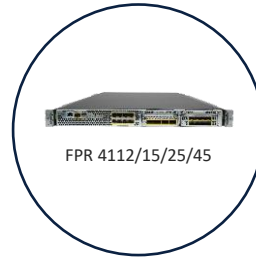
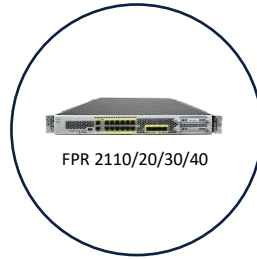
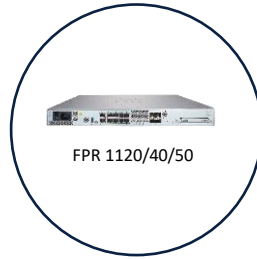
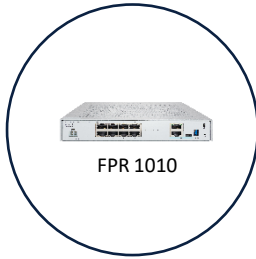


共存
不可

共存
可能

*SDC = Secure Device Connector, 無償提供の VM, FTD 管理アドレスがプライベートの場合に必要

Firepower アプライアンスポートフォリオ



Firewall バーチャルプラットフォーム

Private Cloud

- FMCv と FTDv
 - ESXi 7.0 サポート済み
 - Cisco HyperFlex, Nutanix Enterprise Cloud, OpenStack は FTD / FMC 7.0 でサポート
- ASAc Docker containers



Public Cloud

- FTD のメトリック監視に Azure Application Insights 利用可能
- FMCv/FTDv, ASA v は、既存の AWS, Azure に加えて、Google Cloud Platform & Oracle Cloud Infrastructure でもサポート開始



FTDv での新ライセンス (FTD 7.0 より)

- FTD 7.0 より FTDv の処理速度に応じたライセンスに変更
- FTD 7.0 以前の永久ベースライセンスはサブスクリプションモデルに移行

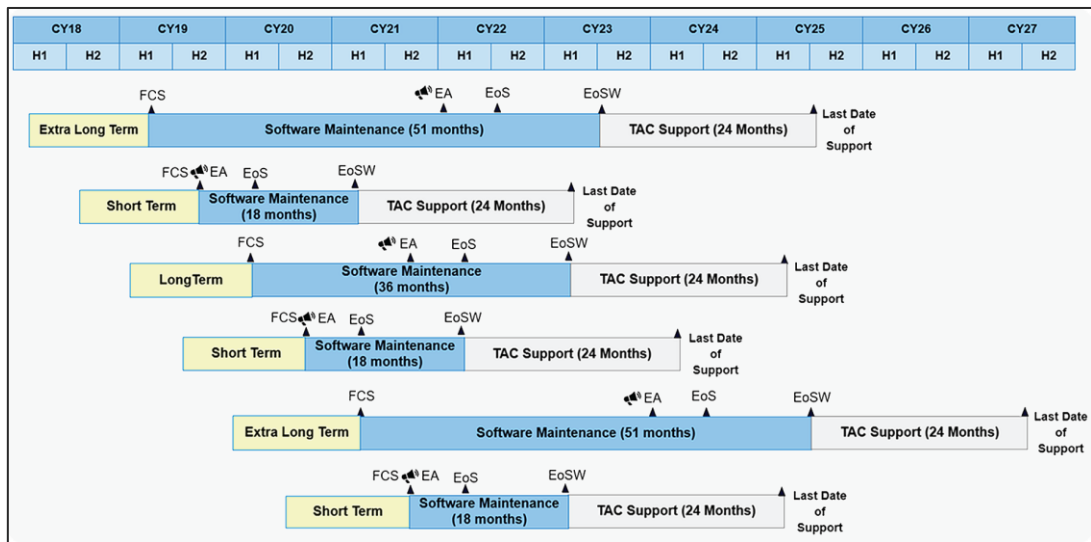
Performance Tier	Device Specifications	Rate Limit	RA VPN Session Limit
FTDv5	4 cores/8 GB	100Mbps	50
FTDv10	4 cores/8 GB	1Gbps	250
FTDv20	4 cores/8 GB	3Gbps	250
FTDv30	8 cores/16 GB	5Gbps	250
FTDv50	12 cores/24 GB	10Gbps	750
FTDv100	16 cores/32 GB	16Gbps	10,000

ソフトウェアライフサイクルポリシー

Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin

<https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html>

- 年の前半と後半にそれぞれ新しいソフトウェアをリリースする
- FTD (ASA も) のバージョンの数字の小数点1桁目が偶数ならロングタームサポート、奇数ならショートタームサポートとなる
 - FTD 6.5 → ショートタームサポート
 - FTD 6.6 → ロングタームサポート
- ロングタームサポートの中でも、奇数年にリリースされるものはエクストラロングタームサポートとなる
 - FTD 7.0 → 2021年前半リリースなのでエクストラロングタームサポート



FTD / FMC 推奨ソフトウェアバージョン

- 2022年3月時点で一般的な推奨バージョンは 7.0.1
- 稼働実績と重大な障害の数、および重大な不具合の数を総合的に見て推奨バージョンを選定している

Software Download

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Firepower NGFW Virtual / Firepower Threat Defense (FTD) Software- 7.0.1

Search...

Expand Collapse All

Suggested Release

7.0.1

Latest Release

7.1.0.1

6.4.0.14

6.7.0.3

7.0.1.1

All Release

7.1

Firepower NGFW Virtual

Release 7.0.1

My Notifications

Related Links and Documentation

7.0.1 Documentation

Firepower Hotfix Release Notes

Release Notes for 7.0.1

File Information	Release Date	Size	
Firepower Threat Defense 7.0.1 Hotfix S Do not untar	21-Dec-2021	258.73 MB	↓ 🛒 📄
Cisco_FTD_Hotfix_S-7.0.1.1-10.sh.REL.tar Advisories			
Firepower Threat Defense upgrade Do not untar	07-Oct-2021	970.54 MB	↓ 🛒 📄
Cisco_FTD_Upgrade-7.0.1-84.sh.REL.tar Advisories			

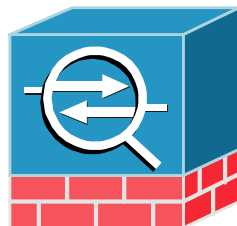
ダウンロードサイトでの★マークに注目

[参考] ASA と AnyConnect



• ASA の特長

- CLI で操作できる Basic Firewall
- リモートアクセス VPN 終端装置として豊富な機能
- 多量の ACL でも安価に実現
- 18年目のロングセラー
(PIX まで遡ると28年)



• AnyConnect の特長

- どこからでも安全なアクセスを提供
- IPsec でも SSLでも利用可能なフルトンネル VPN
- PC だけでなくスマートフォンでも利用可能
- VPN 以外の機能も豊富 (NAM, NVM, AMP enabler, Umbrella)
- 16年目のロングセラー
(Cisco VPN Client まで遡ると22年)

Firewall は ASA か FTD か？

- Firepower アプライアンスは ASA ソフトウェアか FTD ソフトウェアを選択して動作させることができる。また、ASA も FTD もそれぞれ仮想版ソフトウェアが存在する

	ASA	FTD
Basic (L4まで) Firewall, Routing / Switching, NAT	◎	○
RA VPN 終端	◎	○
Site-to-Site VPN	○	○
IPS / IDS	X	◎
AVC, URL Filter	X	◎
Malware 対策	X	◎
SSL / TLS 復号	X	◎

L4 までの Basic FW, RA VPN 終端だけであれば ASA を選択

L7 セキュリティ (IPS, AVC, Malware, SSL 復号) が 必要であれば FTD を選択

当セッションは以降 FTD にフォーカス

Firepower9300



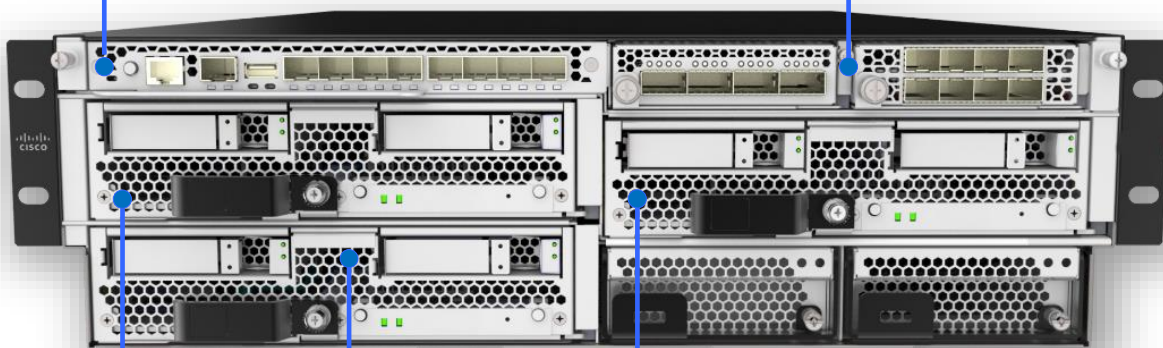
Supervisor

- アプリケーションの導入とオーケストレーション
- ネットワーク接続とトラフィック分散
- ASA/FTDのためのクラスタリングベースレイヤ

Network Modules

- 1GE,10GE,40GE,100GE
- NGIPSインライン時のハードウェアバイパス

3RU



Security Modules

- SM-40,48,56 の3つのモデル有り
- 組み込み暗号化ハードウェアとSmart NIC
- Cisco (ASA, FTD) とサードパーティ(Radware DDoS) アプリケーションが動作
- スタンドアローンとシャーシ内/シャーシ間クラスタリング構成

Firepower4100シリーズ



Supervisor と Security Module (ビルトイン)

- FP9300と同じハードウェアとソフトウェアアーキテクチャ
- 4つのモデルの固定構成 (4112, 4115, 4125, 4145)

Solid State Drives (SSD)

- 独立した管理 (no RAID)
- Slot 1: Malware ストレージで利用
- Slot 2: 追加の400GB Malware ストレージ対応

1RU



Network Modules

- 10GE/40GE (FP9300と互換性あり)
- NGIPS インライン時のハードウェアバイパス (Fail-to-Wire オプション)

ソフトウェアは FTD と ASA の選択が可能

Firepower2100シリーズ

ソフトウェアは FTD と ASA の選択が可能



	FP 2110	FP 2120	FP 2130	FP 2140
Chassis & I/O	1RU 12 Fixed RJ-45 (1G) 4 x SFP (1G)	1RU 12 Fixed RJ-45 (1G) 4 x SFP (1G)	1RU 12 Fixed RJ-45 (1G) 4 x SFP+ (10G) 1 x NM Slot	1RU, 12 Fixed RJ-45 (1G) 4 x SFP+ (10G) 1 x NM Slot
CPU x86	4-Core	6-Core	8-Core	16-Core
CPU DDR4 DRAM	16GB	16GB	32GB	64GB
NPU Octeon	6-Core	8-Core	12-Core	16-Core
NPU DDR4 DRAM	8 GB	8 GB	16 GB	16 GB
SSD	1 x 100GB Default 2 nd Optional SSD for MSP 800GB		1 x 200GB Default 2 nd Optional SSD for MSP 800GB	
PSU – Default/Options	1x 250W Fixed AC PSU	1x 250W Fixed AC PSU	1x 400W AC default 2x AC, 1x or 2x DC options	2x 400W AC default 2x 350W DC options

Firepower1000 シリーズ

ソフトウェアは FTD と ASA の選択が可能

小規模環境 & スモールビジネスに最適なアプライアンス



Firepower1010

- ハイパフォーマンスなデスクトップ型NGFW
- PoE, 8 x 10/100/1000 Base-T RJ45 switching ports
- [FTD] ステートフル Firewall, AVC, NGIPS, Malware, URL Filtering 全てに対応
- [FTD] 650Mbps の NGFW スループット



Firepower1120/1140/1150

- ハイパフォーマンスなラックマウント型NGFW
- 8 x 10/100/1000 Base-T RJ45 switching ports, . 4 x 1000Base-X SFP switching ports (FP1150 はうち 2ポートが 10GbE 対応)
- [FTD] ステートフル Firewall, AVC, NGIPS, Malware, URL Filtering 全てに対応
- [FTD] それぞれ 1.5 / 2.2 / 3.0 Gbps の NGFW スループット

Firepowerシリーズのデータシート

- ・モデル別に存在、英語/日本語ともに公開 (英語版の方が最新)

[FP9300](#), [FP4100](#), [FP2100](#), [FP1000](#), [Virtual Appliance](#)

Cisco Firepower 9300 Series Data Sheet

Updated: April 20, 2020

- Table of Contents
- Cisco Firepower 9300 Series a...
- Model overview
- Detailed performance specific...
- Hardware specifications
- Cisco Capital

Cisco Firepower
The Cisco Firepower® 9300 is high-performance computing require low (less than 5-micro programmatic orchestration, Standards (NIST)-compliant or Cisco Firepower Threat De

Model overview



Cisco Firepower 4100 Series Data Sheet

Updated: May 7, 2020

- Table of Contents
- Cisco Firepower 4100 Series a...
- Model overview
- Detailed performance specific...
- Hardware specifications
- Cisco Capital

Cisco Firepower
The Cisco Firepower 4100 and Internet edge use case supports flow-offloading, Building Standards (NIST) Cisco ASA Firewall or C

Model overview



Cisco Firepower 2100 Series Data Sheet

Updated: July 11, 2019

- Table of Contents
- Cisco Firepower 2100 Series a...
- Model overview
- Detailed performance specific...
- Hardware specifications
- Cisco Capital

Cis

The

inc

simu

Bu

the

C

M

Mo

de

de

de

de

de

de

de

Cisco Firepower 1000 Series Data Sheet

Updated: December 18, 2019

- Table of Contents
- Cisco Firepower 1000 Series ...
- Model overview
- Detailed performance specific...
- Hardware specifications
- Cisco Capital

Cisco F

The Cisco F

business res

The 1000 Se

1000 Series

Model o

Model o

Model o

Model o

Model o

Model o

Model o

Model o

Model o

Model o

Cisco Firepower NGFW Virtual (NGFWv) Appliance Data Sheet

Updated: June 24, 2020

- Product overview
- Table of Contents
- Product overview
- Benefits
- Features and specifications
- Product performance guidelines
- System requirements
- Ordering information
- Cisco environmental sustainabl...
- Cisco Capital
- The Cisco Security Advantage

Today, businesses rely on a mixture of physical and virtual solutions to meet their network security needs. They need the flexibility to deploy different physical and virtual firewalls across a wide range of environments while still maintaining consistent policy throughout branch offices, corporate datacenters, and all entry points between. From data center consolidation to office relocations, mergers and acquisitions, or seasonal peaks in demand on your applications, Cisco's virtual firewall portfolio helps businesses simplify security management with the convenience of unified policy and the flexibility to deploy everywhere.

Cisco® Next-Generation Firewall Virtual (NGFWv) appliance combines Cisco's proven network firewall with advanced next-gen IPS, URL filtering, and malware detection. Identify and eliminate threats automatically, freeing up security and network operations teams. NGFWv also simplifies protecting virtualized environments by enabling consistent security policies to follow your workloads across physical, private, and public cloud environments. Get deep visibility into your network to quickly detect threat origin and activity, then stop attacks before they impact your business. Cisco virtual firewall offerings mitigate any significant shift in demand on your IT department so you can protect your workloads against increasingly complex threats with world-class security controls.

Product overview

FTD ライセンス一覧 (1)

FTD はスマートライセンス必須

Airgap 環境では License Reservation を申請するか Cisco Smart Software Manager On-Prem を構築

★ は FTD のモデル毎に1,3,5年のライセンスを購入

FMC 利用時は FMC でまとめてライセンスを管理

FDM 利用時は FTD 毎にデバイス内でライセンスを管理

どちらの場合も初期インストール後、90日間の評価ライセンスが利用可能 (Smart Software Manager への接続不要)

- Base (無償)

AVC, Basic Firewall, Routing & Switching

- Threat ★

IPS / IDS, Security Intelligence

FTD ライセンス一覧 (2)

- URL Filtering ★

カテゴリ、reputation

- Malware ★

Malware Defense, Threat Grid (Dynamic File Analysis), ファイル保存

- Threat Grid

Threat Grid ポータル利用時に必要、組織毎に1,3,5年で選択

- AnyConnect

サイト単位で APEX or Plus ライセンスを適用 or デバイス単位で VPN-Only ライセンスを利用
評価ライセンス利用のためには別途申請が必要 (初期の 90日間評価ライセンスには含まれない)

- FMC Virtual

管理デバイス数 (2,10,25) 毎に永続ライセンスの購入が必要 (初期の 90日間評価ライセンス有り)
300デバイス管理が可能な大型モデルもあり (FMCv300)

インターフェイス拡張モジュール

標準モジュール



8 X 10 GE SFP
Firepower 2100、4100、9300



4 X 40 GE SFP
Firepower 4100、9300



2 X 100 GE QSFP 28
Firepower 9300

FP2100 は 2130/40 のみ
インターフェイス拡張に対応

FTW(Fail-To-Wire) モジュール



6 X 1 GE SX ファイバ
Firepower **2100**、4100



8 X 1 GE TX (銅線)
Firepower **2100**、4100



6 X 10 GE SR/LR ファイバ
Firepower **2100**、4100、9300

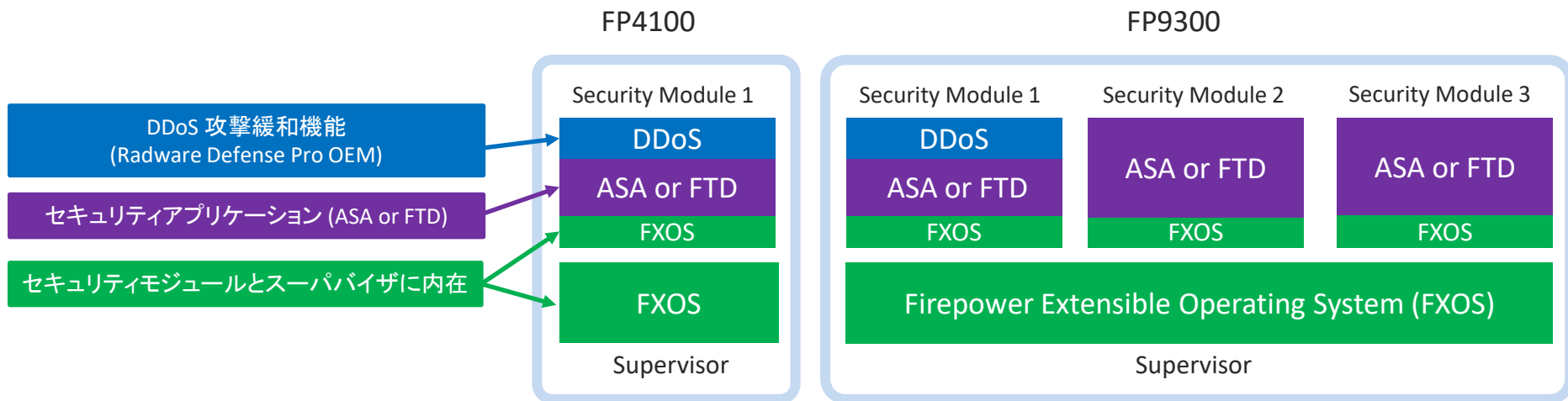


2 X 40 GE SR4 ファイバ
Firepower 4100、9300

FTW によるハードウェアバイパスは NGIPS
(Inline mode)でのみ提供

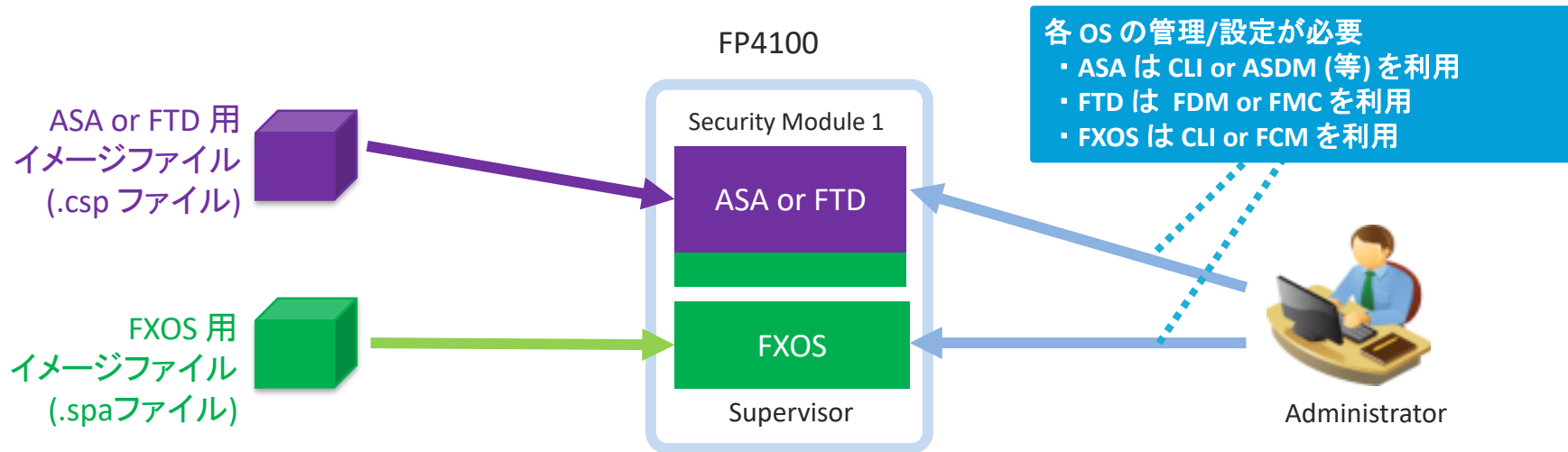
FP4100/9300 と FXOS

- FP4100/9300 内には Firepower eXtensible Operating System (FXOS) が動作
 - FXOS が、スーパーバイザや セキュリティモジュールを管理
 - FXOS が、シャーシや ネットワークモジュール、電源、FAN などハードウェアの管理
 - FXOS が、セキュリティモジュールに物理インターフェイス割当て



FP4100/9300 と FXOS (続き)

- FP4100/9300 はプラットフォーム型で、シャーシ内に複数 OS が動作可能
 - FXOS と ASA/FTD は、各独立した OS であり、イメージファイルや設定ファイルが異なる
 - FXOS と ASA/FTD の各アップグレードは、別々に実施が必要
 - FXOS と ASA/FTD は、各独立した管理インターフェイスと管理 IP アドレス, GUI, Syslog, SNMP Agent をもつ



Firepower Chassis Manager (FCM)

FXOS の設定を簡単に GUI で提供

Web ブラウザで FXOS の管理 IP アドレスにアクセスすることで利用可能

日本語対応 (Web ブラウザの言語設定に依存)

The screenshot displays the Firepower Chassis Manager (FCM) web interface. The top navigation bar includes tabs for '概要' (Overview), 'インターフェイス' (Interfaces), '論理デバイス' (Logical Devices), 'セキュリティ' (Security), 'システム' (System), 'ツール' (Tools), 'ヘルプ' (Help), and 'admin'. The main content area is divided into several panels:

- Overview Panel:** Shows device information for 'FP4120-beta-1' (Cisco Firepower 4120 Security Appliance) with IP 10.71.153.63. It includes status indicators for console, USB, and power, and a summary of alerts (0 Critical, 2 Major, 4 Minor, 0 Info).
- Interfaces Panel:** Lists all interfaces (Ethernet1/1 to Ethernet1/8) and their types (cluster, data, mgmt).
- Configuration Panel:** Shows configuration for 'FP4120-FTD-1' (Cisco Firepower Threat Defense) with a list of ports (Ethernet1/1 to Ethernet1/7) and their associated applications (FTD).
- Updates Panel:** Displays a table of available updates for the device.

イメージ名	タイプ	バージョン	ステータス	ビルドの日付	画像の整合性
fxos-k9.2.0.1.141.SPA	platform-bundle	2.0(1.141)	未インストール	02/17/2017	Unknown
fxos-k9.2.3.1.88.SPA	platform-bundle	2.3(1.88)	インストール済み	06/07/2018	✓ 検証済み - Wed 4 July 2018, 06:1...
fxos-k9.2.3.1.66.SPA	platform-bundle	2.3(1.66)	未インストール	02/28/2018	✓ 検証済み - Thu 15 Mar 2018, 12:4...
fxos-k9.2.1.1.64.SPA	platform-bundle	2.1(1.64)	未インストール	12/16/2016	Unknown
fxos-k9.2.3.1.75.SPA	platform-bundle	2.3(1.75)	未インストール	04/27/2018	✓ 検証済み - Mon 18 June 2018, 07:...
fxos-k9.2.3.1.73.SPA	platform-bundle	2.3(1.73)	未インストール	03/13/2018	✓ 検証済み - Thu 29 Mar 2018, 03:3...
fxos-k9.2.2.1.63.SPA	platform-bundle	2.2(1.63)	未インストール	05/08/2017	Unknown
fxos-k9.2.1.1.73.SPA	platform-bundle	2.1(1.73)	未インストール	02/28/2017	Unknown
fxos-k9.1.1.4.95.SPA	platform-bundle	1.1(4.95)	未インストール	03/24/2016	Unknown
cisco-fts.6.0.1.1213.csp	fts	6.0.1.1213	未インストール	03/19/2016	
cisco-fts.6.2.0.362.csp	fts	6.2.0.362	未インストール	01/20/2017	
cisco-fts.6.2.3.79.csp	fts	6.2.3.79	未インストール	03/26/2018	Verified - Fri 30 Mar 2018, 09:09 AM
cisco-asa.9.8.2.24.csp	asa	9.8.2.24	未インストール	03/01/2018	Verified - Thu 15 Mar 2018, 01:14 AM
cisco-fts.6.2.3.83.csp	fts	6.2.3.83	インストール済み	04/01/2018	Verified - Mon 2 Apr 2018, 11:44 AM
cisco-asa.9.6.1.3.csp	asa	9.6.1.3	未インストール	05/05/2016	

[CCOから最新のアップデートをダウンロード](#)

FP2100/1000 と FXOS

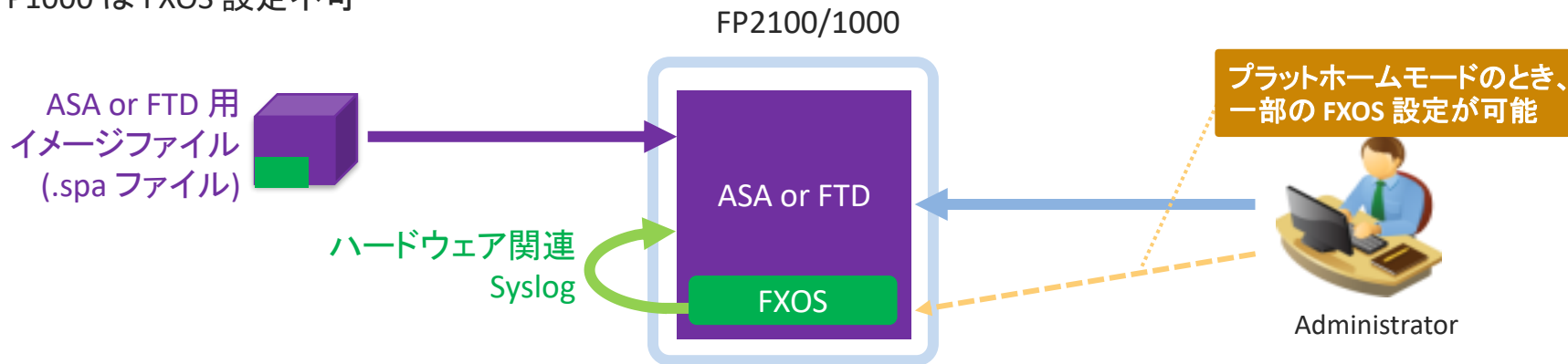
- FP2100/1000 は**アプライアンス型**で、FXOS と ASA/FTD の統合が進んだモデル

FXOS 関連のソフトウェアが、ASA/FTD のパッケージ内に同梱 (=シングルイメージ)

FXOS と ASA/FTD で、共通の管理インターフェイスを利用、ハードウェア関連 Syslog は ASA/FTD 側に出力

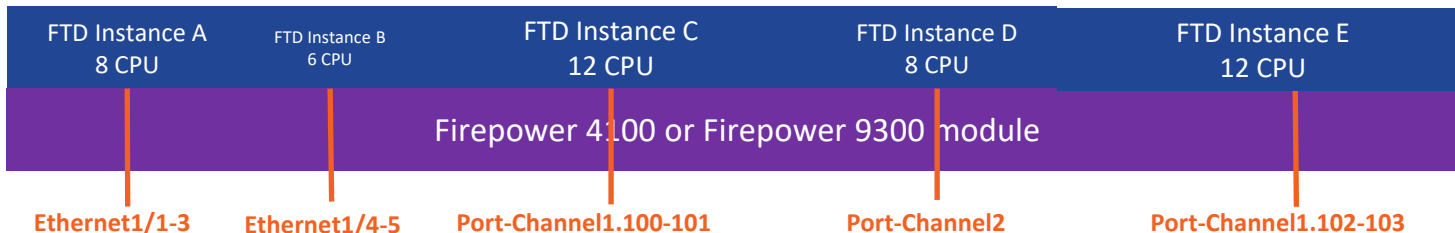
FP2100 での ASA の場合、FXOS 設定不可のモード (アプライアンスモード) と FXOS の設定を必要最小限 (管理 IP アドレスや物理インターフェイス割当て、NTP 設定など) 行えるモード (プラットフォームモード) がある。アプライアンスモードが推奨。FTD の場合、FXOS 設定不可

FP1000 は FXOS 設定不可



マルチインスタンスの概要

- FTD 6.3 より、Firepower 4100 と 9300 **のみでサポート**
- 1つのモジュール or アプライアンスで複数の論理デバイスが稼働
 - まずは FTD のみでサポート、FTD と ASA の混在は**未サポート**
 - Docker インフラとコンテナのパッケージングを活用
- トラフィックも管理も完全に分離
- 物理/論理インターフェイスと VLAN は Supervisor で実施



マルチインスタンスの管理とライセンス

- どのインスタンスも完全に独立したデバイスとして動作する
 - ソフトウェアのアップグレード、再起動、ポリシー管理など、全てが独立して動作する
 - どのインスタンスもそれぞれ独自の管理 IP アドレスが必要
- マルチインスタンスのための追加のライセンスは不要
- ブレードに対して適用したすべてのサブスクリプションライセンスは全インスタンスで共有される
 - それぞれのインスタンスが異なる FMC で管理される場合には個別にサブスクリプションライセンスが必要

まとめと参考資料

まとめ

- Firewall Threat Defense (FTD) が上位レイヤの脅威対策を行う NGFW & IPS 製品として位置づけられ、市場で認知されている
- L4 までの Basic Firewall である ASA と L7 Security の FTD を適材適所で使い分ける
- “本当に使える” 脅威対策として FTD は優れた機能や管理性を持つ
- FTD は ASA の機能を包含した新たな NGFW + IPS + Malware Defense 製品として利用可能
- FTD も ASA も同一ハードウェアで動作し、豊富なラインナップがある
- FTD と ASA の明確なソフトウェアリリース & サポートポリシーがある

参考サイト

- Cisco Secure Firewall への cisco.comでのショートカット
<http://cisco.com/go/ngfw>
- シスコ セキュリティ パートナー ガイド
https://www.cisco.com/c/m/ja_jp/partners/documents/security-guide.html
- パートナー向け技術資料 (Firewall 基本説明動画、FTD 初期設定ガイド、FDM 初期設定ガイド等、いろいろ公開中)
https://www.cisco.com/c/m/ja_jp/partners/documents.html
- Japan Partner Community : セキュリティ
<https://salesconnect.cisco.com/#/program/PAGE-17530>
- [必見!] シスコサポートコミュニティ セキュリティ
<https://community.cisco.com/t5/-/ct-p/5041-security>
- シスコジャパン ブログ セキュリティ
<https://gblogs.cisco.com/jp/category/security/>

Cisco Secure Firewall 新機能解説動画

- Cisco Secure Firewall チャンネルに多くのデモ動画あり

<https://www.youtube.com/c/CiscoNetSec>

CISCO
SECURE
FIREWALL

Firepower 1000 Series
CISCO

NetSec Community

Cisco Secure Firewall
チャンネル登録者数 3710人

登録済み

ホーム 動画 再生リスト コミュニティ チャンネル 概要

アップロード動画 ▶ すべて再生

DYNAMIC ATTRIBUTES CONNECTOR 15:16

FQDN NAT 15:20

NETWORK AUTOMATION 15:20

SNORT 3 RULE ACTIONS 15:20

SNORT 3 RULE RECOMMENDATIONS 12:56

SNORT 3 ELEPHANT FLOWS 13:11

Cisco Secure Firewall 7.1 Release - Dynamic Attribute... 169 回視聴・6 日前

Cisco Secure Firewall 7.1 Release - FQDN NAT 311 回視聴・2 週間前

Network Security Autom... with Cisco Secure Firewall ... 337 回視聴・3 週間前

Actions 233 回視聴・1 か月前

365 回視聴・1 か月前

Cisco Secure Firewall 7.1 Release ▶ すべて再生

NEW FIREWALL THREAT DEFENSE 7.1 HOW TO BLOCK TLS 1.3 CSN EXTENSION 7:57

NEW FIREWALL THREAT DEFENSE 7.1 DEPLOYMENT WITH AWS GATEWAY BALANCER 10:15

NEW FIREWALL THREAT DEFENSE 7.1 HOW ENCRYPTED VISIBILITY ENGINE WORKS (PART 1) 10:12

NEW FIREWALL THREAT DEFENSE 7.1 HOW ENCRYPTED VISIBILITY ENGINE WORKS (PART 2) 6:19

PRIVATE CLOUD CLUSTERING 8:50

SNORT 3 ELEPHANT FLOWS 13:11

多くの動画で日本語への自動翻訳が有効

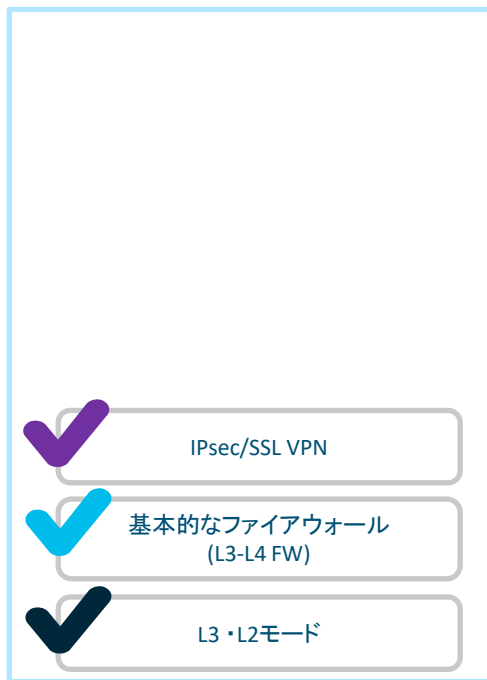




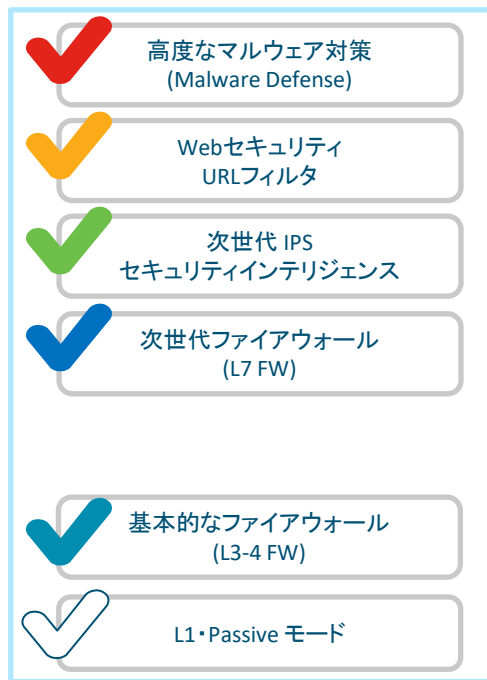
(Appendix)
技術者向け Firewall Threat
Defense のアーキテクチャ

ASA FW, Firepower IPS, FTD の関係性

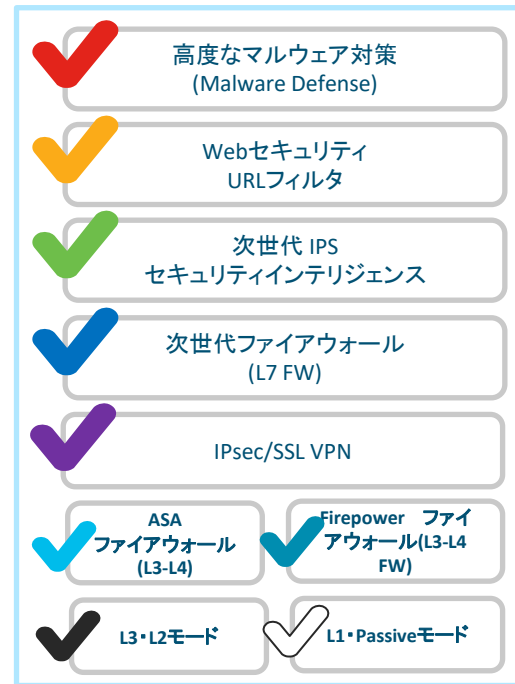
ASA Firewall



Firepower IPS



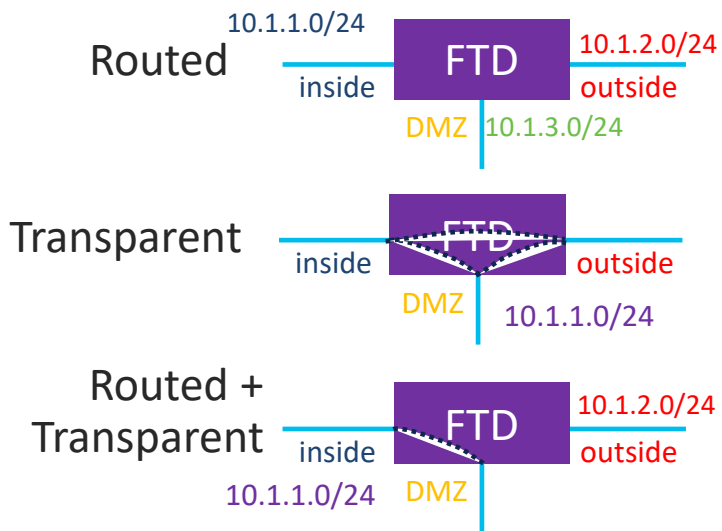
Firewall Threat Defense



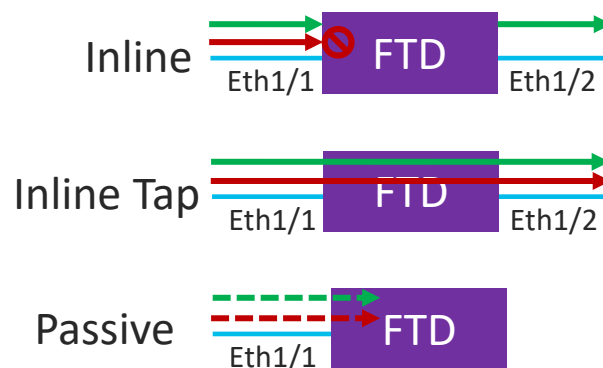
FTD インターフェースモード



ASAから継承



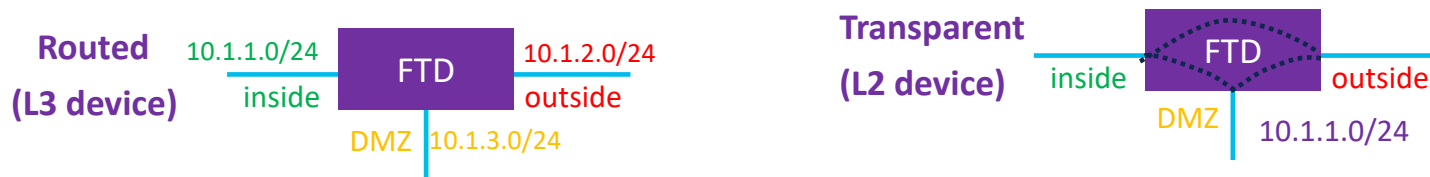
Firepowerから継承



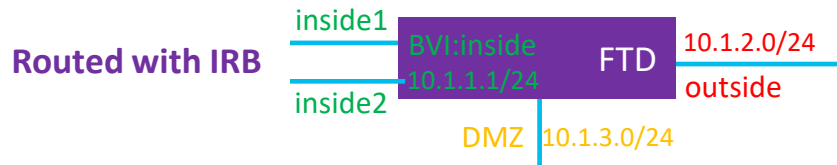
※Inline / Inline Tapのみ、ハードウェアバイパスモジュールにて、Fail-to-Wire 機能利用可能

FTD Firewall モードとそれぞれのインターフェイス

- FTD 新規デプロイ時にその FTD の Firewall としてのモードについて、Routed Firewall か Transparent Firewall の選択が**必須**



- Transparent Mode での BVI には IP アドレス設定が**必須**
- Routed インターフェイスと IRB (Integrated Routing and Bridging) の併用が可能

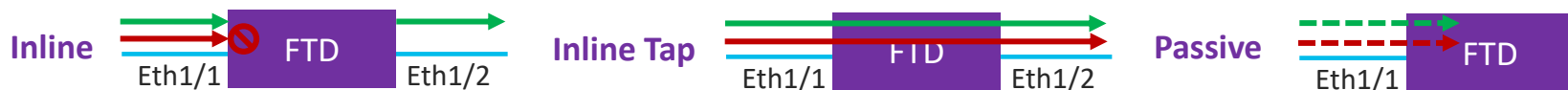


- FTD の全機能の利用が可能 (i.e. Firewall 機能と IPS 機能の両方が利用可能)

- VLAN or VxLAN ID は FTD を越える際に変更が**必須**

FTD の NGIPS インターフェイスモード

- Routed / Transparent Firewall にて未使用のインターフェイスは NGIPS モードのインターフェイスとして利用可能

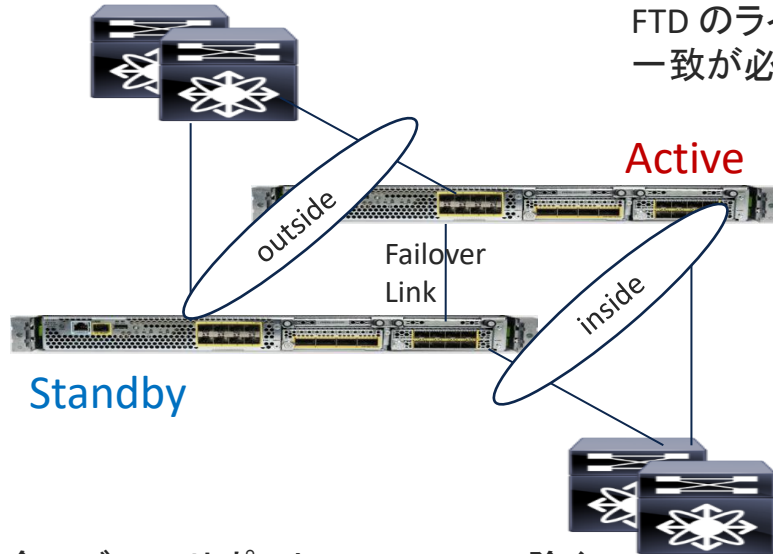


- Inline は Intelligence なケーブルとして動作 (L1 mode とも言う)
- 物理 / EtherChannel での Inline Pair が利用可能: Inline Sets は非対称通信をサポート
- VLAN と LACP はパススルー可能。Q-in-Q のパススルーは不可。
- 全ての Security Policy は有効。Inline モードではブロック可、Inline TAP と Passive モードはブロック不可
- データプレーンは HA / Clustering 時に接続をトラック (データプレーンでの Block は無い)
- NAT、アプリケーションインスペクション等の ASA の機能は無効
- Flow Offload も使われない

注1) FTD 7.0 より ASA と同じ仕組みの VPN Load Balancing もサポート開始

FTD の高可用性

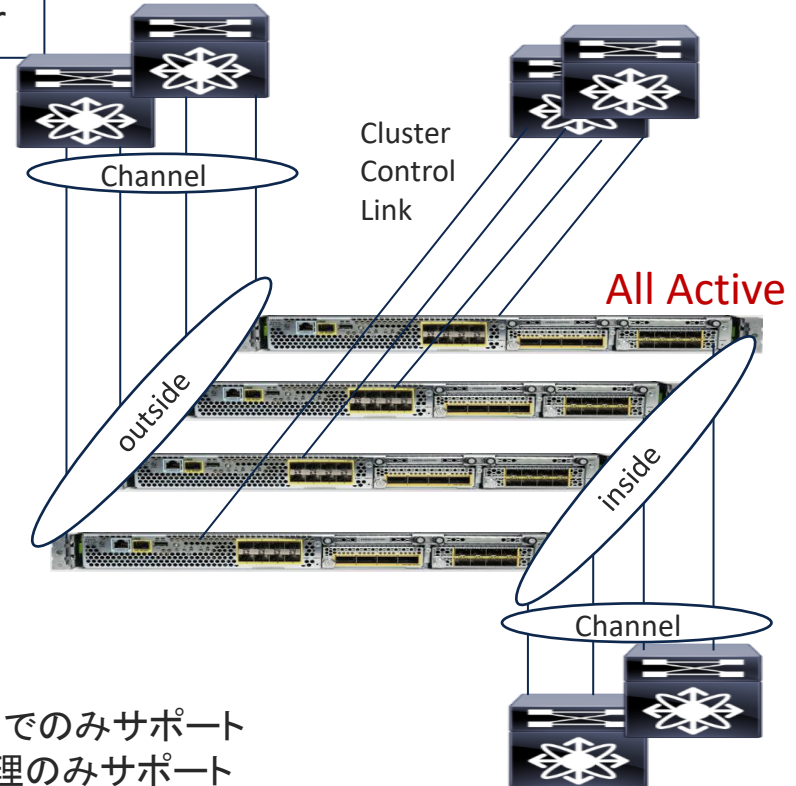
Active - Standby



注2) どちらの構成でも
FTD のライセンスは
一致が必要

全モデルでサポート (public cloud 除く)
FMC 管理 / FDM 管理どちらも可
同一モデル同士でペアを組む
ASA での Active - Standby と全く同じ仕組み
Routed / Transparent / Inline IPS で動作可

Cluster



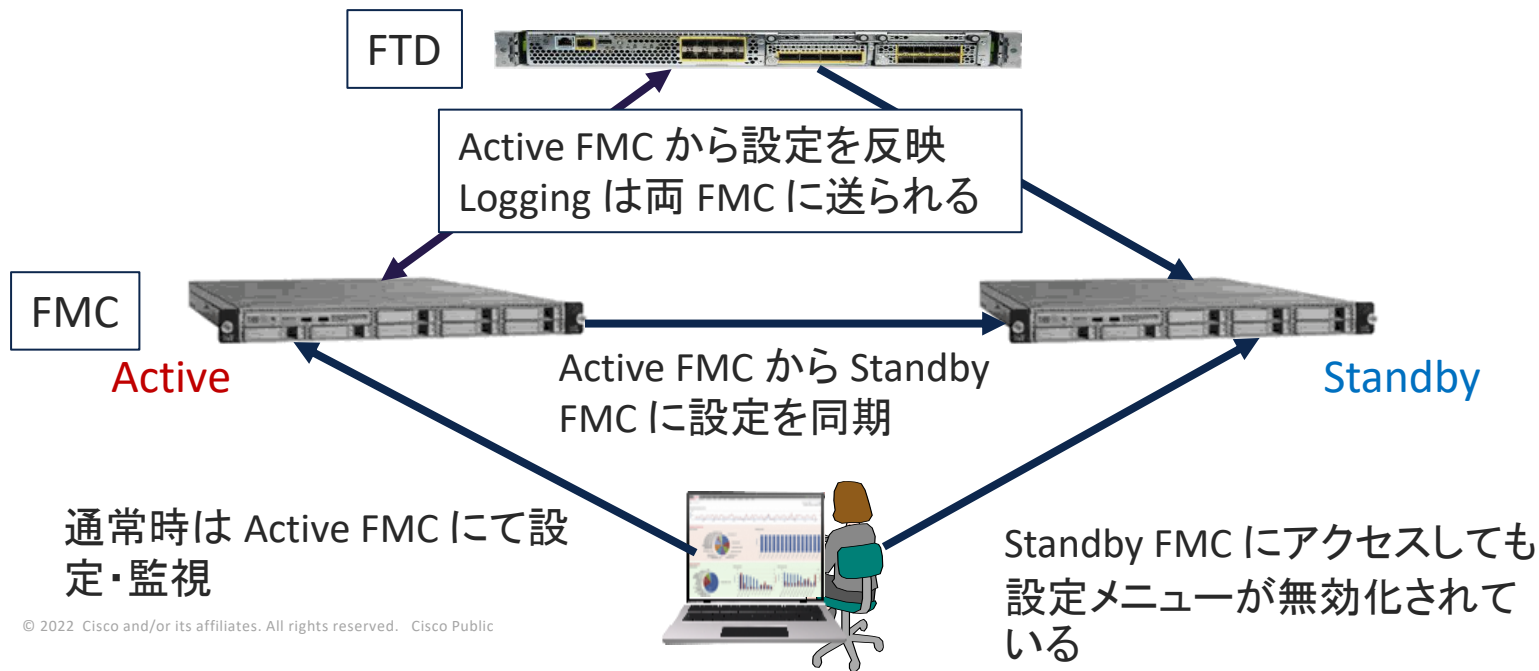
FP4k/9k でのみサポート
FMC 管理のみサポート
同一モデル or 同一インスタンスサイズでメンバーを組む
ASA での Shared Interface 利用時の Cluster と同じ仕組み
Routed / Transparent / Inline IPS で動作可

FMC の高可用性

FMC は Active / Standby での冗長化が可能

FMCv も version 6.7 より VMware 版のみで可能になった (FMCv2 除く)

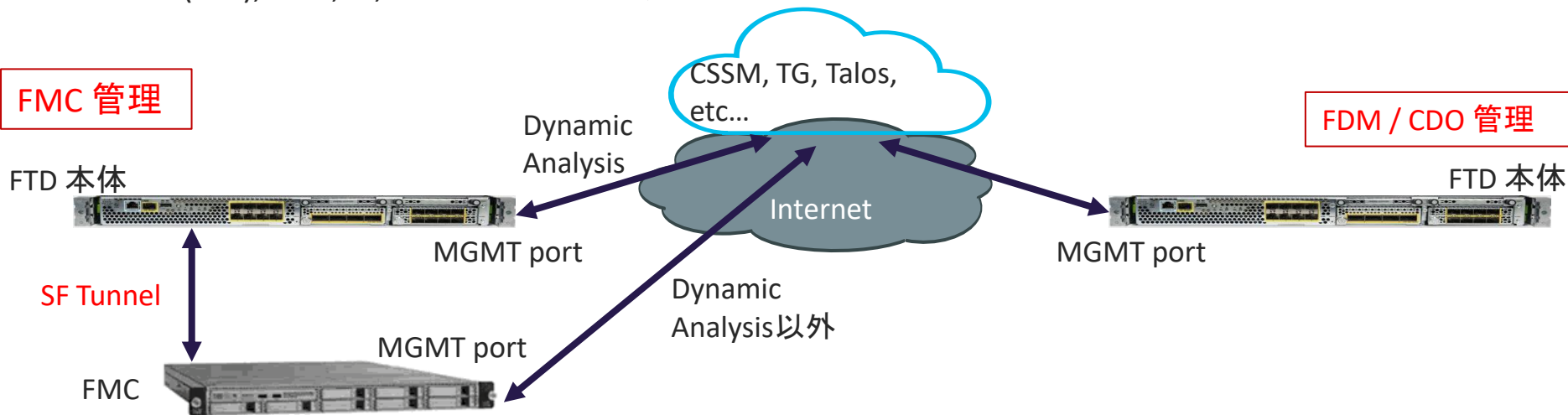
FMC には Active / Standby 自動切り替わり機能は無く、手動で切り替える必要がある



インターネットアクセスの必要性

FMC, FTD デバイス自身からインターネットへのアクセスが必要

- ライセンス管理のための Cisco Smart Software Manager (CSSM) へのアクセス
- Malware 機能における Cloud Lookup と Dynamic Analysis
- SRU (LSP), VDB, SI, GeoDB 等の定期更新



FMC 管理の場合、CSSM へのアクセスも含め、ほとんどのインターネットアクセスは FMC が実施する
ただし、Cloud の Threat Grid にファイルを submit する (Dynamic Analysis) のは FTD から行われる

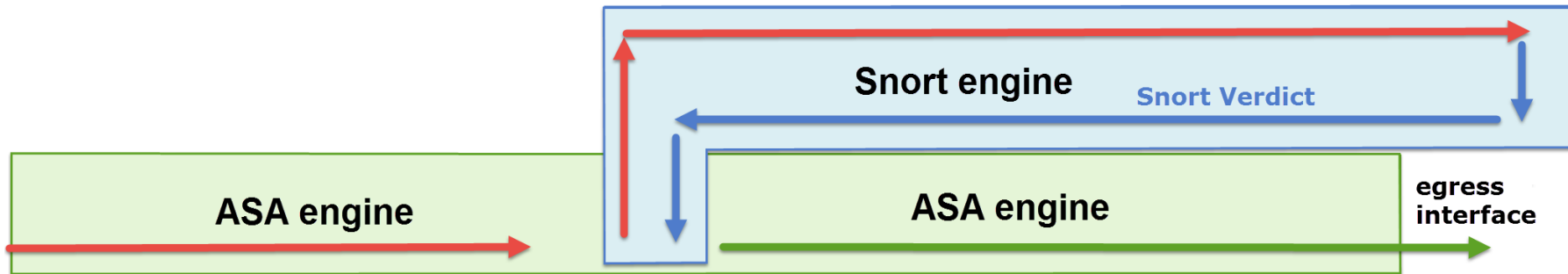
Proxy 経由、NAT 越えはサポート

CSSM へのアクセスが不可な場合 (Air Gap 環境)、License Reservation を利用

本当に Air Gap 環境か？

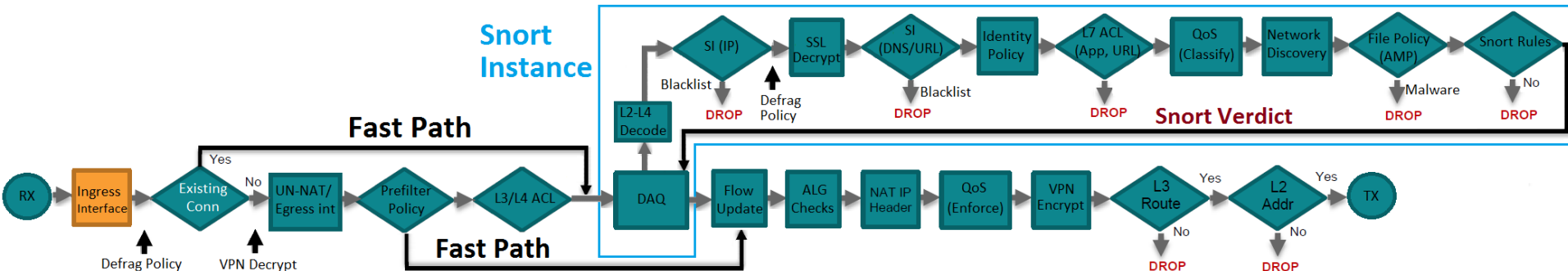
- そもそも本当に Air Gap 環境で使うのか？再度検討する必要がある
- Air Gap 環境だと、Malware Cloud Lookup / Dynamic Analysis や URL Filter, Security Intelligence 等が使えず、SRU (LSP) や Geo DB, VDB 更新も完全にマニュアルで実行する必要がある。本当にそのような環境で FTD を使うのか？
- License Reservation にしても、初期セットアップ時にオフラインでスマートアカウントに登録し、エンジニアがオフライン環境で CSSM から必要な情報を入手しなくてはならない
- License Reservation のメリットは、FMC や FDM の管理インターフェイスから、定期的に CSSM にアクセスしなくても良いこと、のみ
- 「なんとなく License Reservation を申請」しないこと

FTD パケット処理の大まかなプロセス



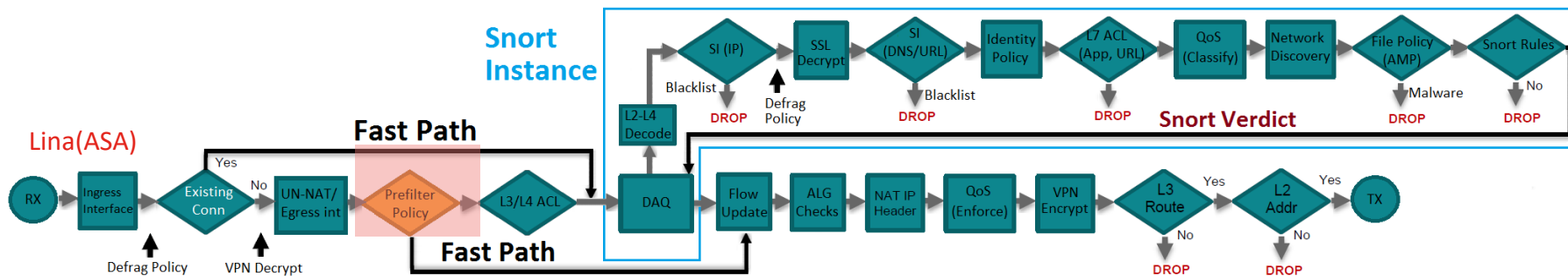
1. Ingress Interface に入ってきたパケットはまずは ASA エンジン (通称 LINA) にて処理される
 2. ポリシーに適合すれば、パケットは Snort エンジンにてインスペクションされる
 3. Snort エンジンがパケット転送の許可/破棄を決定
 4. ASA エンジンは Snort の判断に従ってパケットを転送するか破棄する
- Snort エンジンは 6.x のコードで動作
 - ASA エンジンは 9.x のコードで動作

FTD パケット処理 詳細



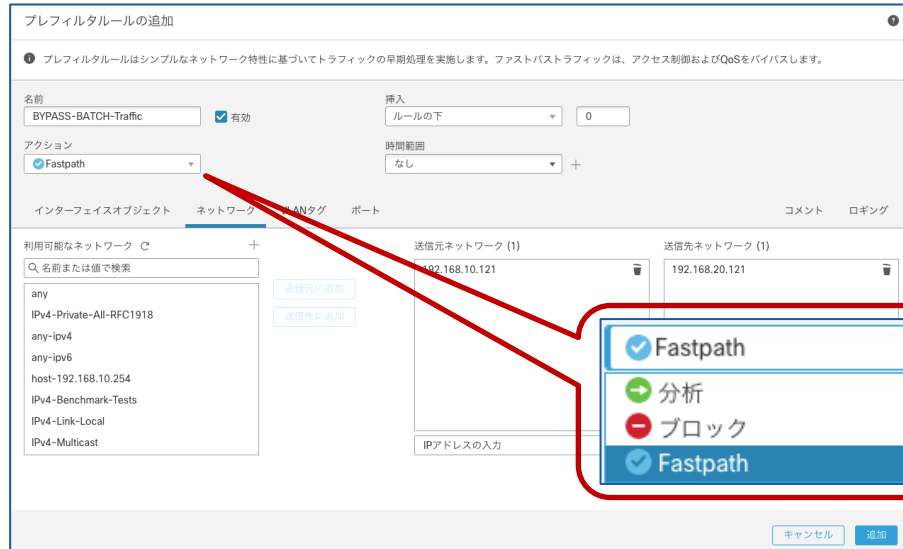
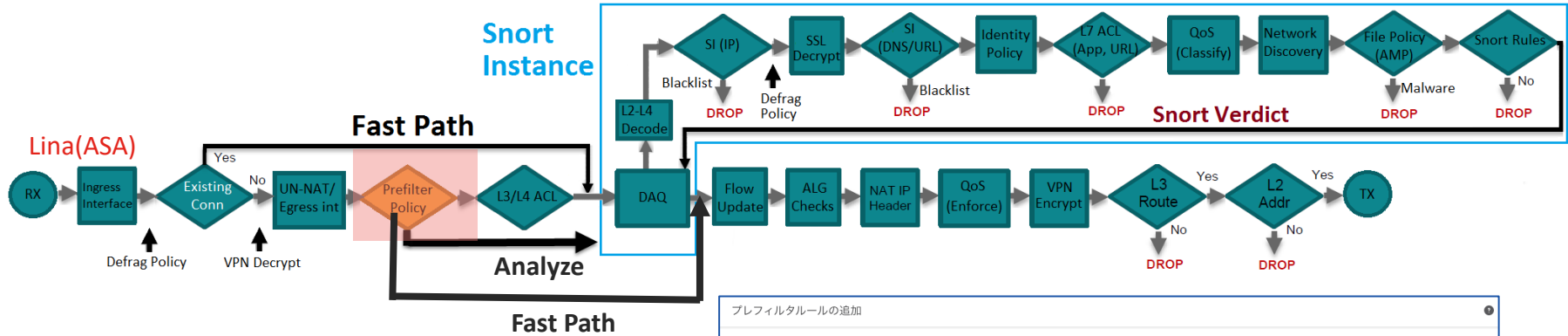
Routed / Switched(Transparent) mode: ASA + Snort フル機能
その他: ASA 一部機能 (L3-4ACL)

Prefilter ポリシーの役割



- Prefilter ポリシーは主に2つの役割を提供
 1. トンネル内のパケットに対するインスペクション処理
 - GRE、IP-in-IP、IPv6-in-IP、Teredo Port 3544
 2. Snort 処理前のアクセスコントロール
 - 監視系 / バックアップなど L7 レベルでの検査が不要な信頼された通信をバイパスする、等

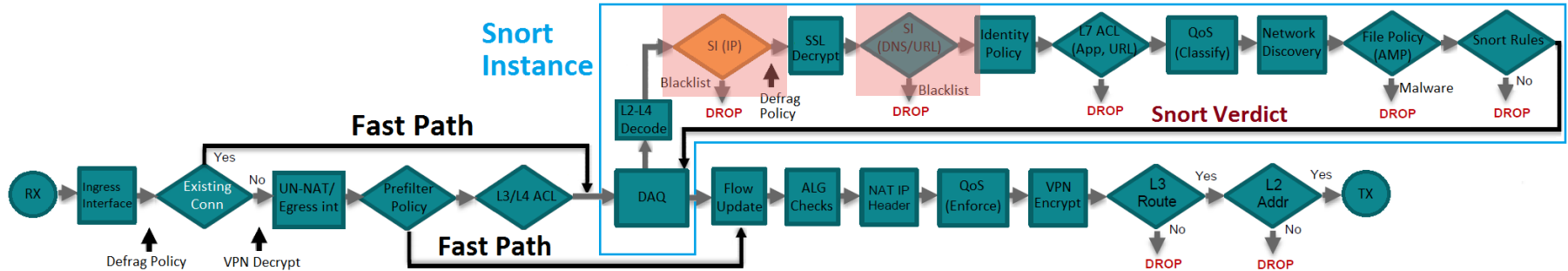
Prefilter ポリシーの役割 (続き)



• Snort 処理前のアクセスコントロール、3つのアクション

1. ブロック (Block): パケットをドロップ処理 (L4レベルで判定できる Deny アクセスリストなど)
2. Fastpath: Snort 側へパケットを渡さずバイパス処理 (監視通信、夜間のバッチ処理など)
3. 分析 (Analyze): Snort 側へパケットを通過処理 (デフォルト設定)

Security Intelligence (IP/URL/DNS)



Security Intelligence (IP Address / URL):

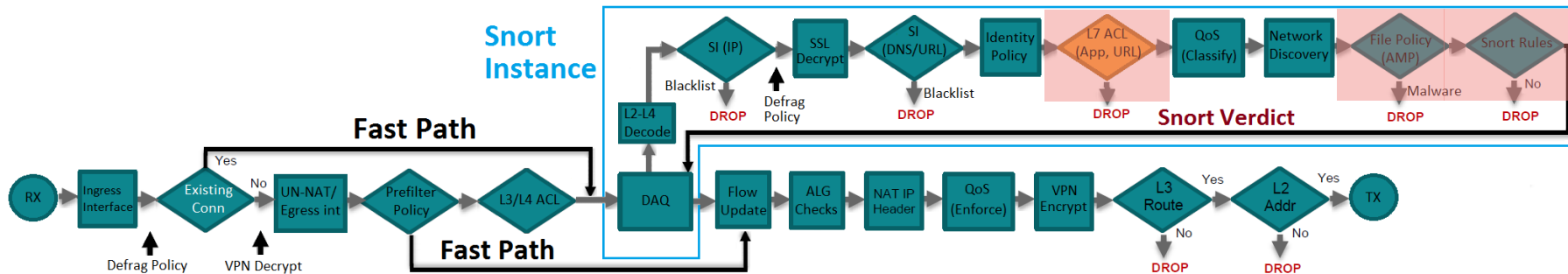
- Security Intelligence に指定された IP アドレス & URL 群への / からの通信を Blocklist or Allowlist に従って処理
- Blocklist は 手動設定 or 自動設定 (Intelligence Feed by Talos or custom)

Security Intelligence (DNS):

- Security Intelligence に指定された DNS 群を以下の処理を実施可能
 1. Whitelist
 2. Monitor
 3. Domain Not Found (NXDOMAIN)
 4. Drop (DNSクエリー)
 5. Sinkhole (IP リダイレクト)
- Blocklist は 手動設定 or 自動設定 (Intelligence Feed by Talos or custom)



L7 ACL (Access Control Policy)



Access Control Policy:

アプリケーションコントロール、URL フィルタリング、IPS、Malware Defense を設定するポリシー

IPS / File Policy など個別に作成したポリシーが紐づく根本となるポリシー

Firepower Management Center

ポリシー / アクセス制御 / Firewall Policy Editor

ACP-1

説明を入力

ルール セキュリティインテリジェンス HTTPレスポンス ログギング 詳細

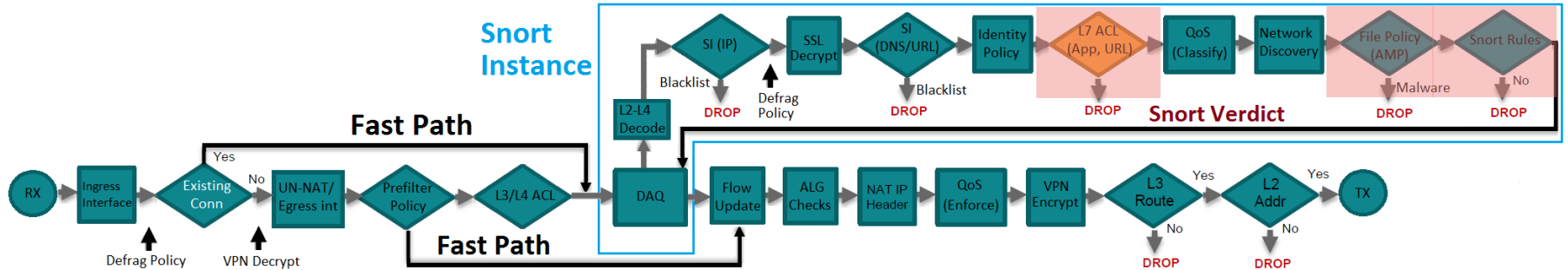
プレフィルタポリシー: Default Prefilter Policy SSLポリシー: なし アイデンティティポリシー: なし

#	名前	送信元ゾーン	送信先ゾーン	送信元ネットワ-	送信先ネットワ-	VLANタグ	ユーザ	アプリケーション	送信元ポート	宛先ポート	URL	送信元SGT (Source SGT)	Dest SGT	アクション
▼ Mandatory - ACP-1 (1-2)														
1	BLOCK-GAMBLE-SPO	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	Gambling (Any R Sports and Recre	すべて	すべて	リセットして
2	BLOCK-FACEBOOK	すべて	すべて	すべて	すべて	すべて	すべて	Facebook	すべて	すべて		すべて	すべて	ブロック
▼ Default - ACP-1 (3-3)														
3	CATCH-ALL	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	承認

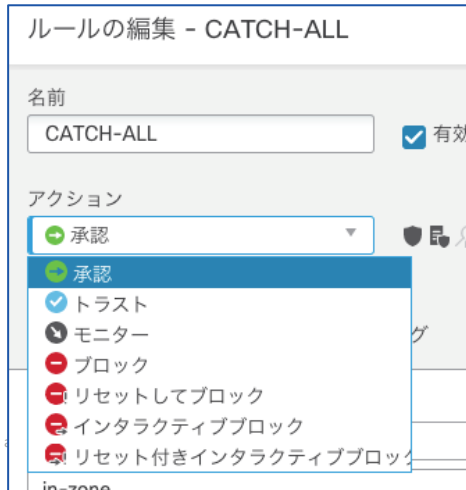
デフォルトアクション

アクセス制御: すべてのトラフィックをブロックする ▼

L7 ACL (Access Control Policy) (続き)

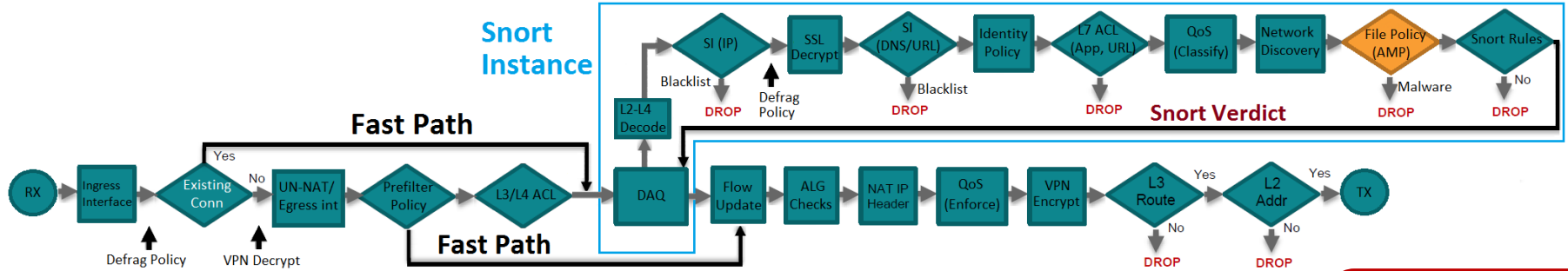


Access Control ルール、7つのアクション



1. 承認 (Allow): パケットを許可、IPS / File 検査可能
2. トラスト (Trust): パケットを信頼、IPS / File 検査スキップ
3. モニター (Monitor): パケットのログ取得、次のルールへ処理を回す
4. ブロック (Block): パケットを破棄
5. リセットしてブロック (Block with reset): パケットを破棄、送信元へリセットパケット送信
6. インタラクティブブロック (Interactive Block): 警告画面表示
7. リセット付きインタラクティブブロック (Interactive Block with reset): 警告画面表、送信元へリセットパケット送信

Malware & File Policy



- Malware & File Policy: 通過するファイルを検査するためのポリシー
- クラウド上のデータベースからマルウェアを発見することや、ファイル拡張子に応じてキャプチャやブロックなど設定可能

ルール名: Malwareのブロック

アプリケーションプロトコル: すべて

転送方向: すべて

アクション:

- Malwareのブロック
- MSEXE向けSPERO分析
- ダイナミック分析
- 容量処理
- ローカルMalware分析
- 接続をリセットする

ファイルの保存:

- Malware
- 不明
- クリーン
- カスタム

ファイルタイプカテゴリ:

- Office Documents 18
- Archive 19
- Multimedia 4
- Executables 10
- PDF files 1
- Encoded 0
- Graphics 1

ファイルタイプ:

7Z (7-Zip compressed file)

ACCOB (Microsoft Access 20...)

ALZ (Archive file for Microsof...)

ARJ (Compressed archive file)

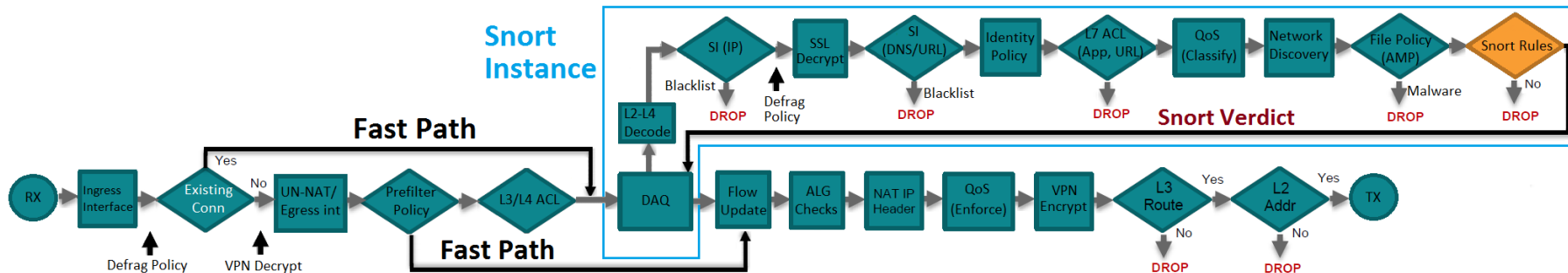
BINARY_DATA (Universal Bin...)

BINHEX (Macintosh BinHex 4 ...)

選択されたファイルカテゴリとタイプ:

- カテゴリ: Local Malware Anal...
- カテゴリ: Dynamic Analysis C...
- カテゴリ: System files
- カテゴリ: Graphics
- カテゴリ: Encoded
- カテゴリ: PDF files
- カテゴリ: Executables

Intrusion Policy



- Intrusion Policy: Snort IPS を用いたパケット検査ポリシー
- 推奨ルール、カスタムルール、独自に作成したルールなど設定が可能

Firepower Management Center

ポリシー / アクセス制御 / ポリシーの編集

概要 分析 ポリシー デバイス オブジェクト AMP Intelligence

ポリシー情報

ルール

Firepower推奨

> 詳細設定

> ポリシーレイヤー

ルール

Rule Configuration

Rule Content

Category

app-detect

browser-chrome

browser-firefox

browser-ie

browser-other

browser-plugins

browser-webkit

content-replace

decoder

exploit-kit

file-executable

file-flash

file-identify

file-image

file-java

フィルタ:

echo reply

5ルール中 1 個を選択しました

ルールの状態 イベントのフィルタリング 動的状态 警告 コメント

<input type="checkbox"/>	GID	SID	メッセージ*
<input type="checkbox"/>	1	6128	MALWARE-BACKDOOR dkangel runtime detection - icmp echo reply client-to-server
<input type="checkbox"/>	1	409	PROTOCOL-ICMP Echo Reply undefined code
<input checked="" type="checkbox"/>	1	408	PROTOCOL-ICMP Echo Reply
<input type="checkbox"/>	1	18473	PROTOCOL-ICMP ICMPv6 Echo Reply
<input type="checkbox"/>	1	31767	SERVER-OTHER MRLQG fastping echo reply memory corruption attempt

Flow Offload(フローオフロード)

- FP9k/4k のみでサポートされた、Smart NIC による信頼されたフロー処理 (セキュリティ可視化の制限あり)
 - 最大約 40Gbps : シングルUDP (1500byteパケット) フロー
 - 2.9usの遅延 : 64-byte UDPパケット
- 最大128K ステートフルコネクションのオフロードをサポート
 - IPv4 TCP/UDP (Untag:32K/Tag:32K), GRE (Untag:32K/Tag:32K)
- ASAの IP/SGACL (MPF) や FTD での Prefilter による Fastpath を静的にオフロード
- FTD の ACP の Trust や IAB (Intelligent Application Bypass)、File & Intrusion Policy の Detection はダイナミックオフロードが可能

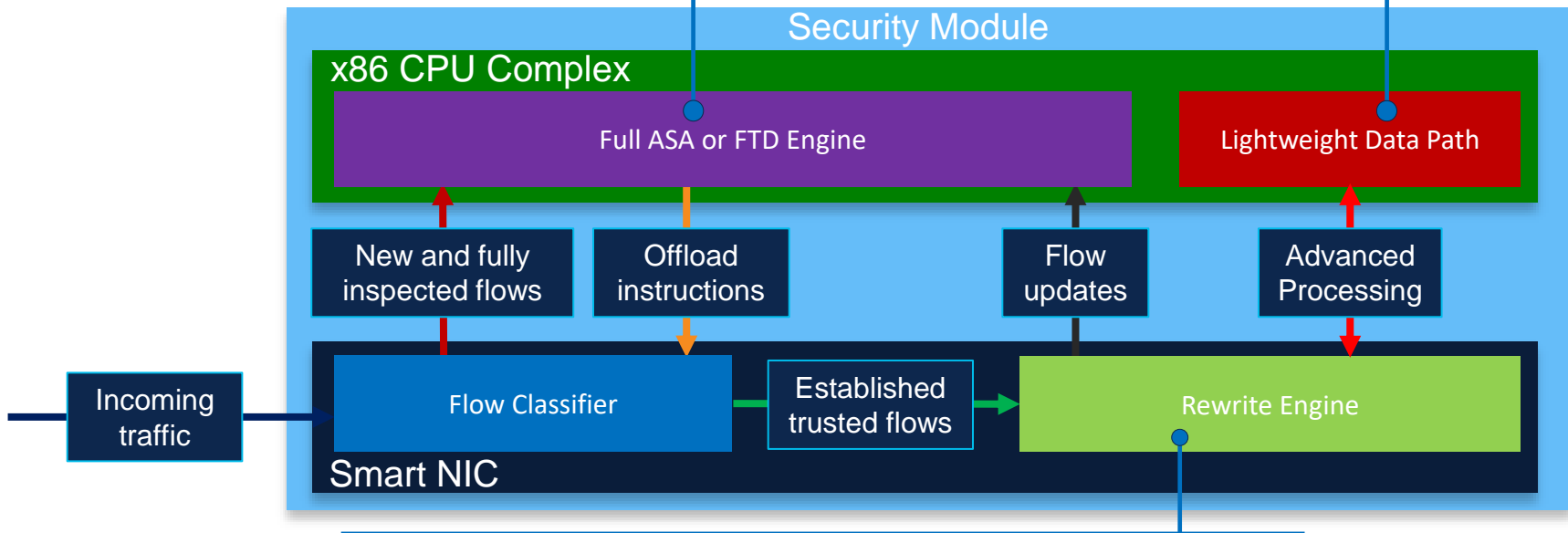
Flow Offload の動き

Full Inspection

- フロー確立後、動的にオフロードエンジンにプログラム
- 瞬時にフルインスペクションとオフロードを切り替え可能

Extended Offload Path

- 高度な処理に対する専用の x86 core
- パケットキャプチャと拡張された統計情報



Flow Offload

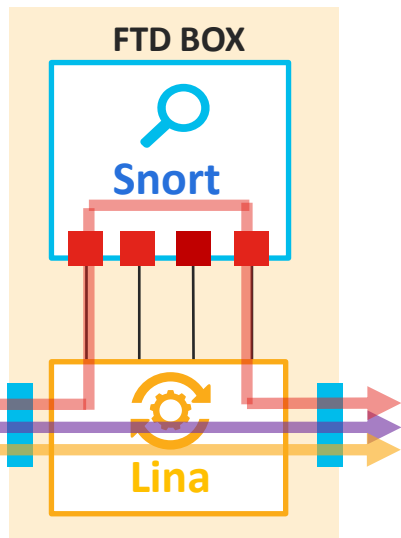
- 制限されたステートトラッキング, NAT/PAT, TCPシーケンスのランダム化
- シングルUDPフローで約40Gbps、2.9us以下の遅延、32K tracked flows

Snort プロセスがリスタートするケース

- Version 6.3 以降であれば、Snort リスタートが起きるシナリオは以下を実施した際の FTD デバイスへのデプロイ時のみ
 - Talos が関係しない VDB 更新やカスタムアプリケーションディテクタの変更
 - File Policy のオプション変更 (Snort のインスタンス数が変わる際のみ)
 - TLS or Captive Portal Policy の有効化/無効化
 - HA ペアの作成/破棄時 (これはデプロイ時ではなく作成、破棄のタイミングで発生)
 - Network Discovery での Traffic-Based Detection で HTTP, FTP, or MDNS の有効化/無効化
 - 全データインターフェイスでの最大 MTU の変更

NGIPS Snort リスタートの影響・Fail-Open

NGIPS



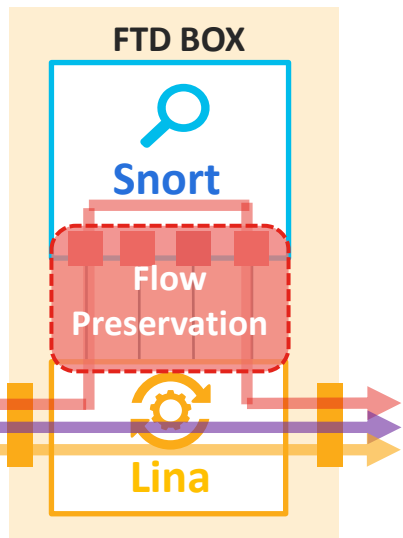
- デフォルト
- Fail-Open
- Prefilter Policy Fastpath

- NGIPS (Inline モードインターフェース) 利用時の Snort リスタートによる影響をバイパスさせる機能
- 従来から存在している機能
- Snort リスタート中、全コネクションにて Snort エンジンバイパス
- Snort リスタート後、セッションをピックアップして処理を再開
- Prefilter Policy で fastpath されたコネクションは、影響を受けない

NGFW Snort リスタートの影響・Flow Preservation

NGFW

- NGFW モード (Routed/Transparent モードインターフェース) 利用時の Snort リスタートによる影響を緩和する機能
- Snort リスタート中、既存接続のみ LINA (ASA) 側で許可 Flow Preserve されたセッションは、セッション終了もしくはタイムアウトまで、LINA(ASA) 側に留まる
Snort リスタート後、新規セッションから Snort 側で処理
- Prefilter Policy で fastpath された接続は、影響を受けない
- FTD version 6.2.0 ラインの 6.2.0.2 以降、または v6.2.3 からサポート (※ v6.2.1/6.2.2 は未サポート) かつデフォルト有効



- デフォルト
- Flow Preservation
- Prefilter Policy Fastpath

