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

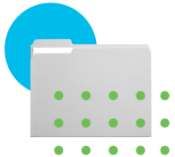
シスコの包括的なセキュリティポートフォリオ

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

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

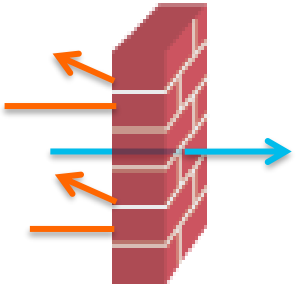


統合された
セキュリティポートフォリオ

- 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

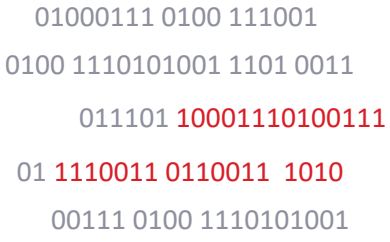


不正通信の防御

ファイアウォール

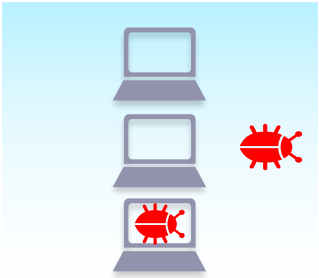
Web アプリケーション、ユーザ、脅威の可視化

次世代ファイアウォール



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) /	0 (No Code) / icmp	Unknown (Unknown)	0	PROTOCOL-ICMP Unu
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_CONT
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

ホストプロファイル　ホストのスキャン　ホワイトリストプロファ

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
Malwareイベント

アプリケーション (60)

クライアント アプリケーション

アプリケーションプロトコル	クライ	
DNS over HTTPS	DNS over HTTPS	
SSL	SSL client	Ad Nexus
HTTPS	SSL client	Ad Nexus
SSL	SSL client	Adobe Analytics
HTTPS	SSL client	Adobe Analytics

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)	

▼ 侵入の痕跡 (1)

侵入の痕跡

ール状態を編集する

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

▼ 脆弱性 (1022)　脆弱性を編集する

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

▼ オペレーティングシステム

端末 OS

オペレーティングシステムを編集する

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

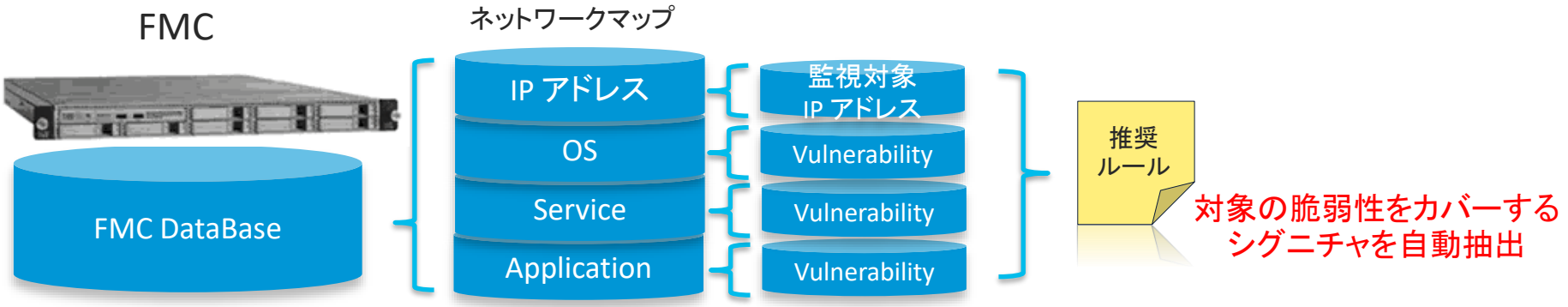
プロトコル	ポート	アプリケーションプロトコル	製造元およびバージョン
tcp	8080	SSL	
tcp	1		

✓ 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

✓ ネットワークの変化に対応し、設定を自動更新



✓ 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

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

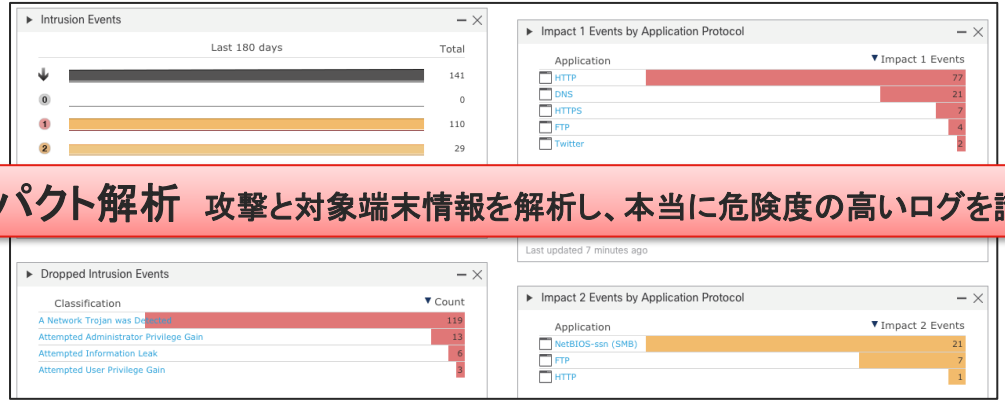
自動チューニング(推奨設定)とインパクト解析

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・・・

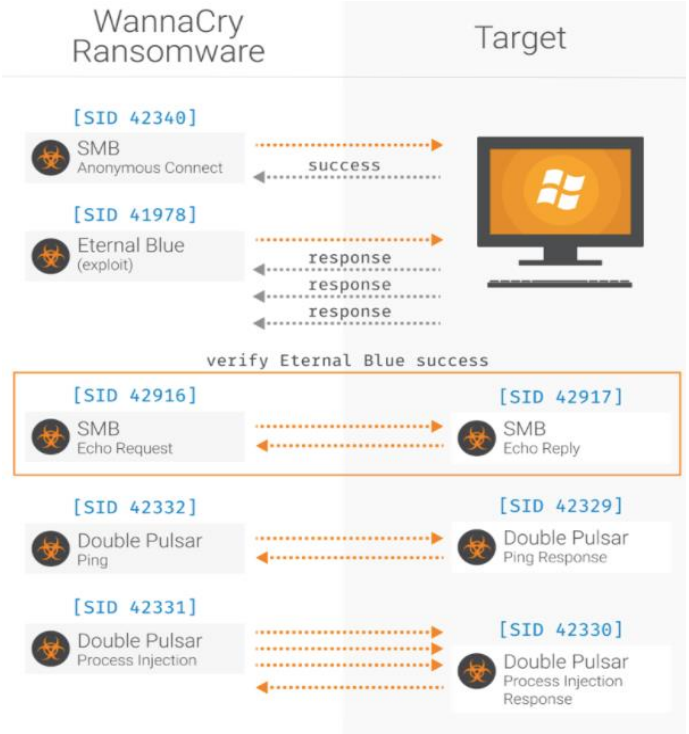
自動チューニング(推奨設定)
ネットワーク環境を学習し、
最適な推奨設定を自動生成



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

防御優先

通信優先

- 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

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

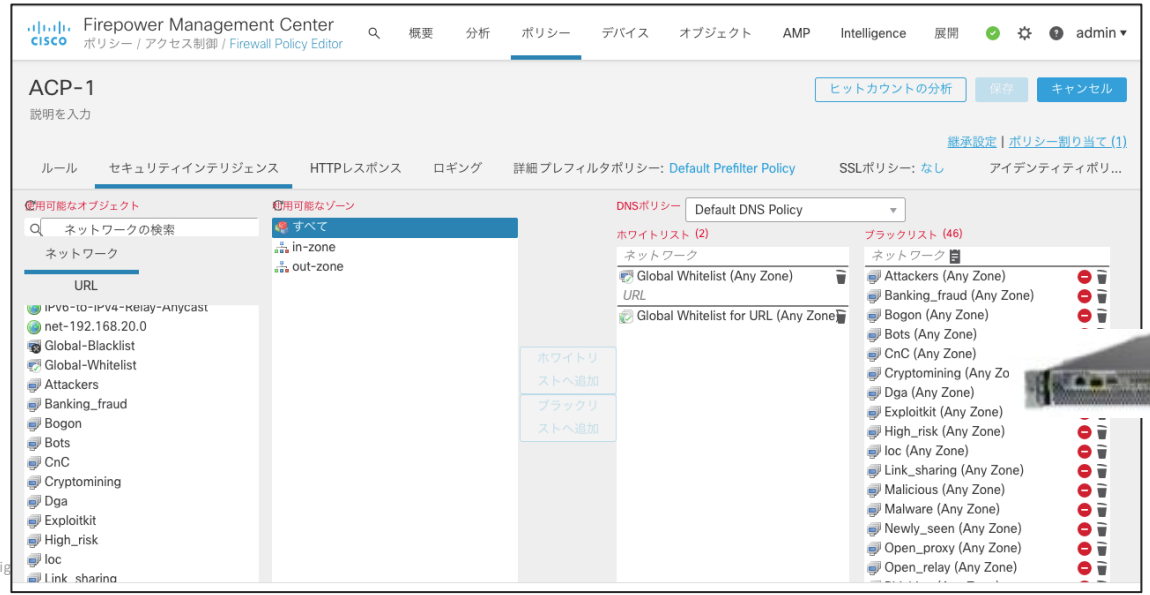
	Snort 2	Snort 3
マルチスレッド アーキテクチャ		✔
複数の Snort プロセス稼働	✔	✔
ポート番号から独立したプロトコルのインスペクション		✔
IPS でのアクセラレータ/ハイパースキャンをサポート		✔
モジュール性 – TALOS からの情報を容易に取り込み		✔
スケーラブルなメモリ割り当て		✔
次世代 TALOS ルール – 正規表現 / ルール最適化 / バッファ		✔
新しい HTTP インスペクタ – HTTP/2 をサポート		✔
TALOS からのアップデートを小型化		✔

補足) シンプルに処理が高速化されていることが大きなメリット

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 からのコネクションを　モニターもしくはブロック
- 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..

シスコ:

- TALOS
- Threat GRIDサンドボックス

レポート先:

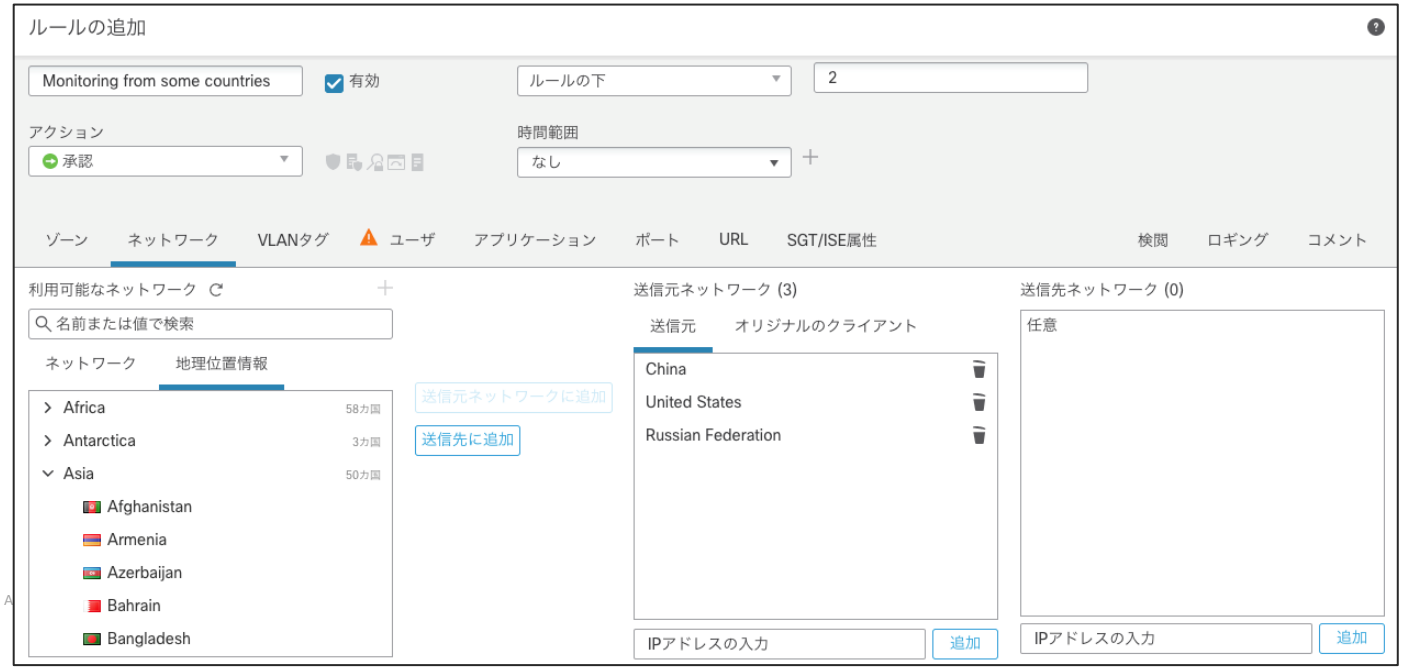
- SIEM
- インシデントマネージメントツール

FTD イベントログ

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

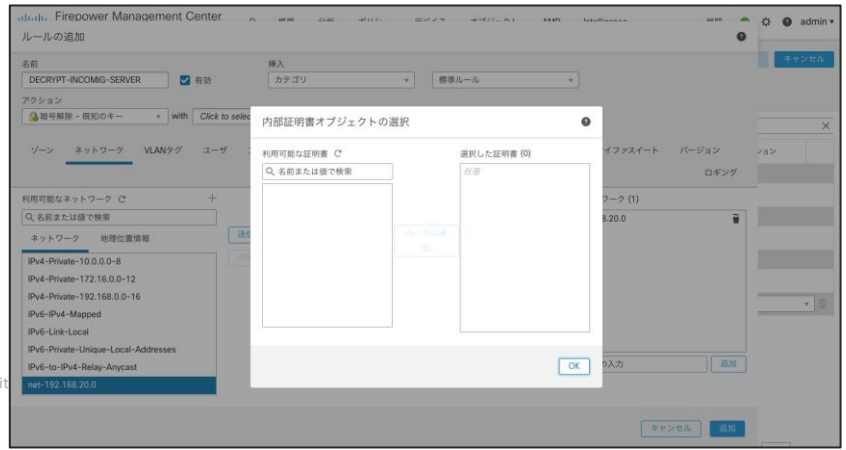
ジオロケーション

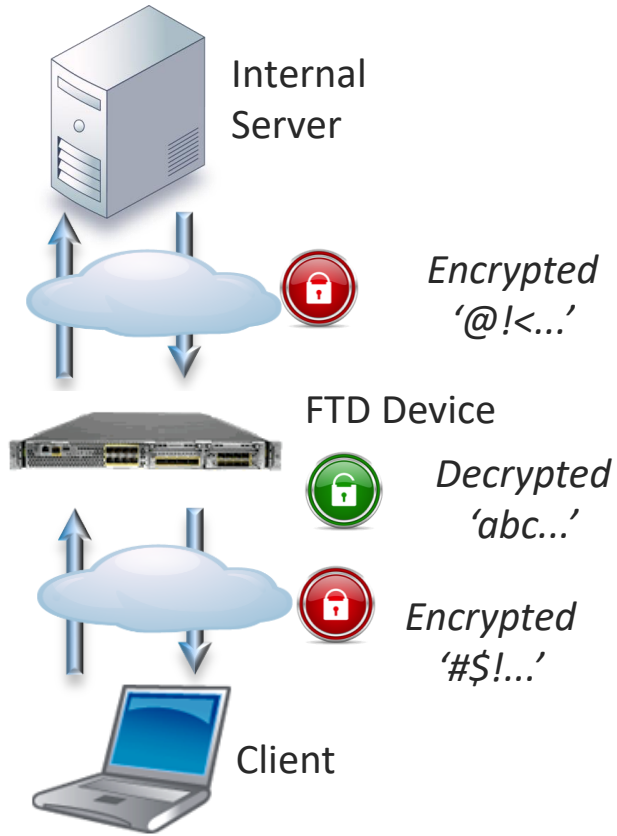
- IP アドレスと国や地域を紐づけたジオロケーションデータベース
- IPS、アプリケーション制御、ファイルポリシー等の任意の設定と組み合わせて利用可



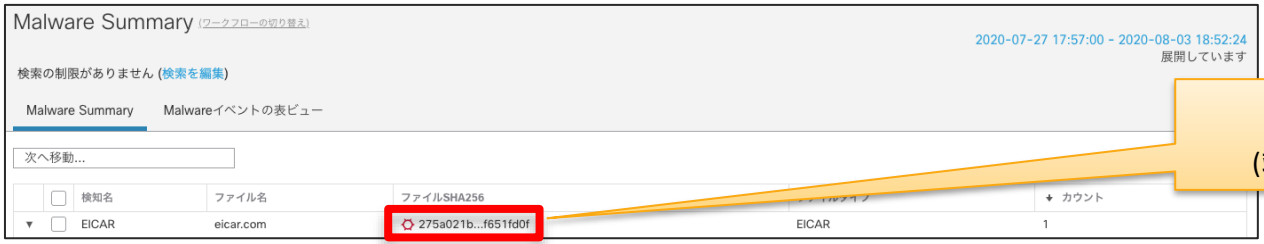
TLS 暗号化アクセラレーション

- 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

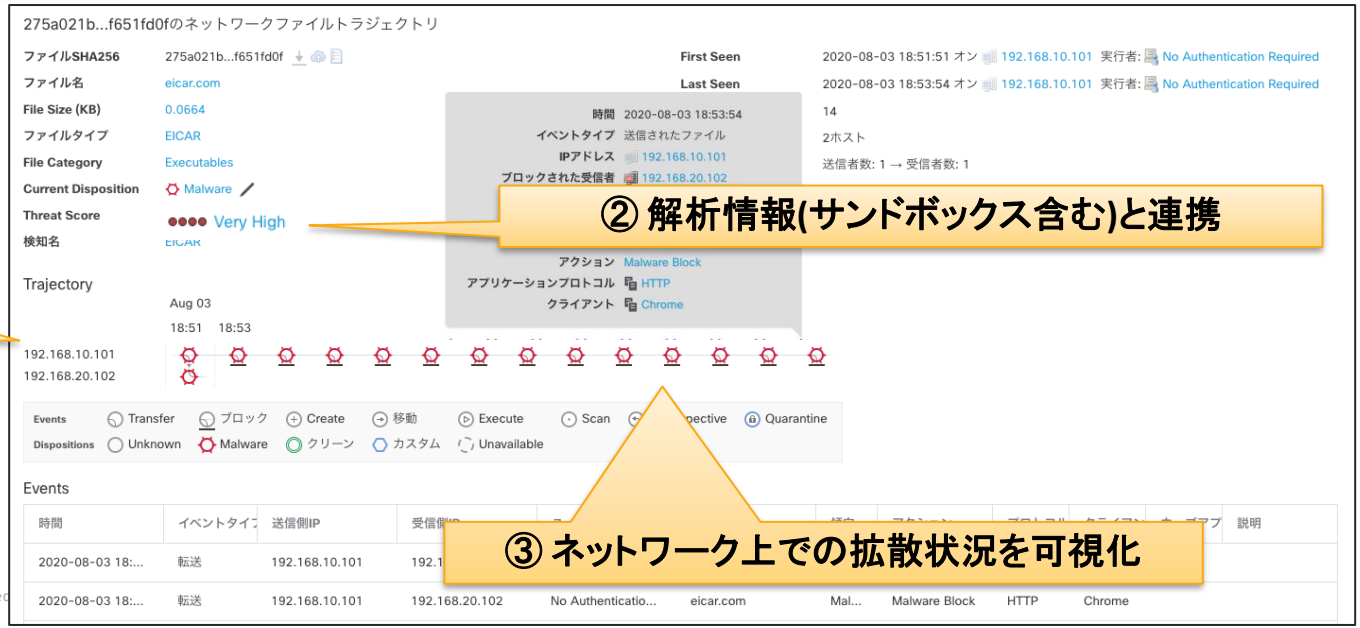




Malware Defense マルウェアの可視化と制御、トラッキング



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)



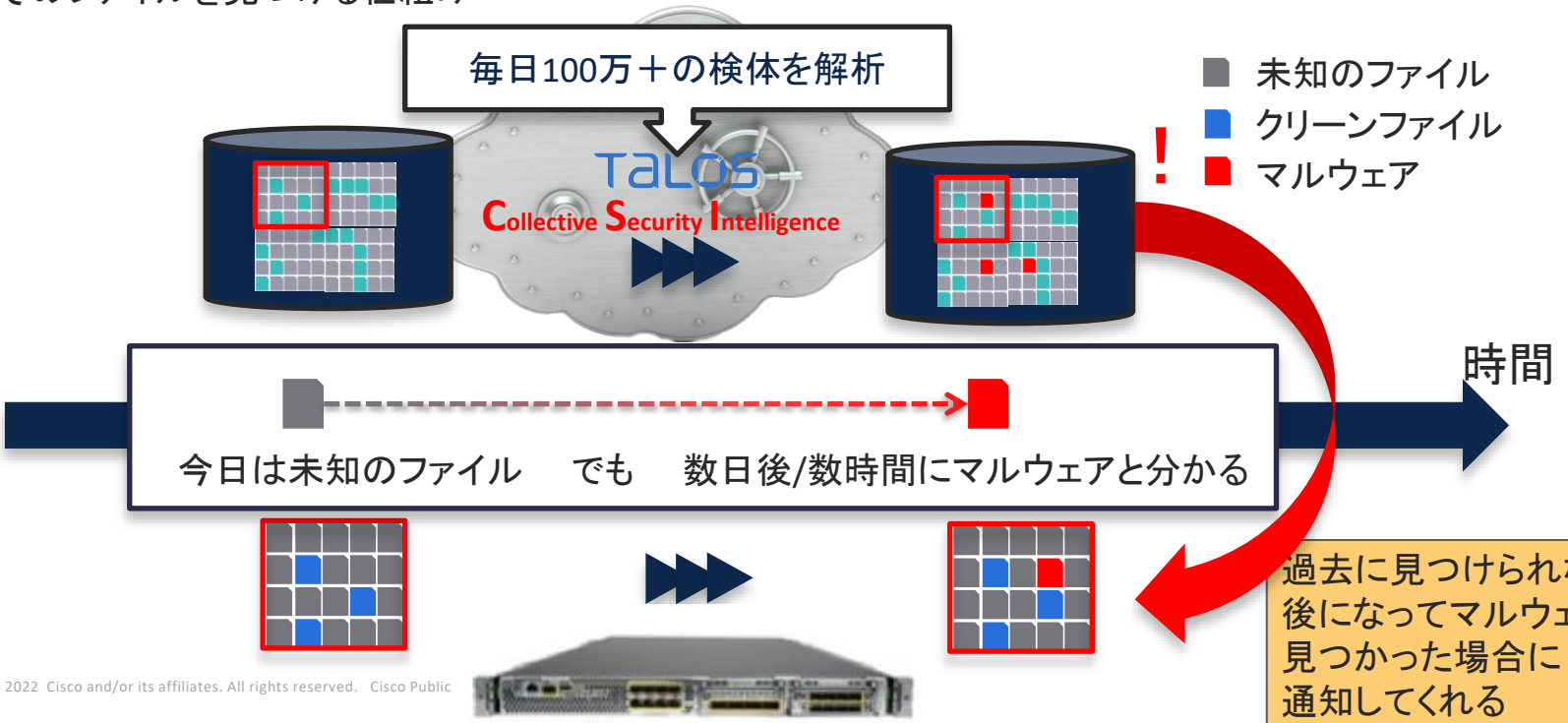
② 解析情報(サンドボックス含む)と連携

④ 端末の特定

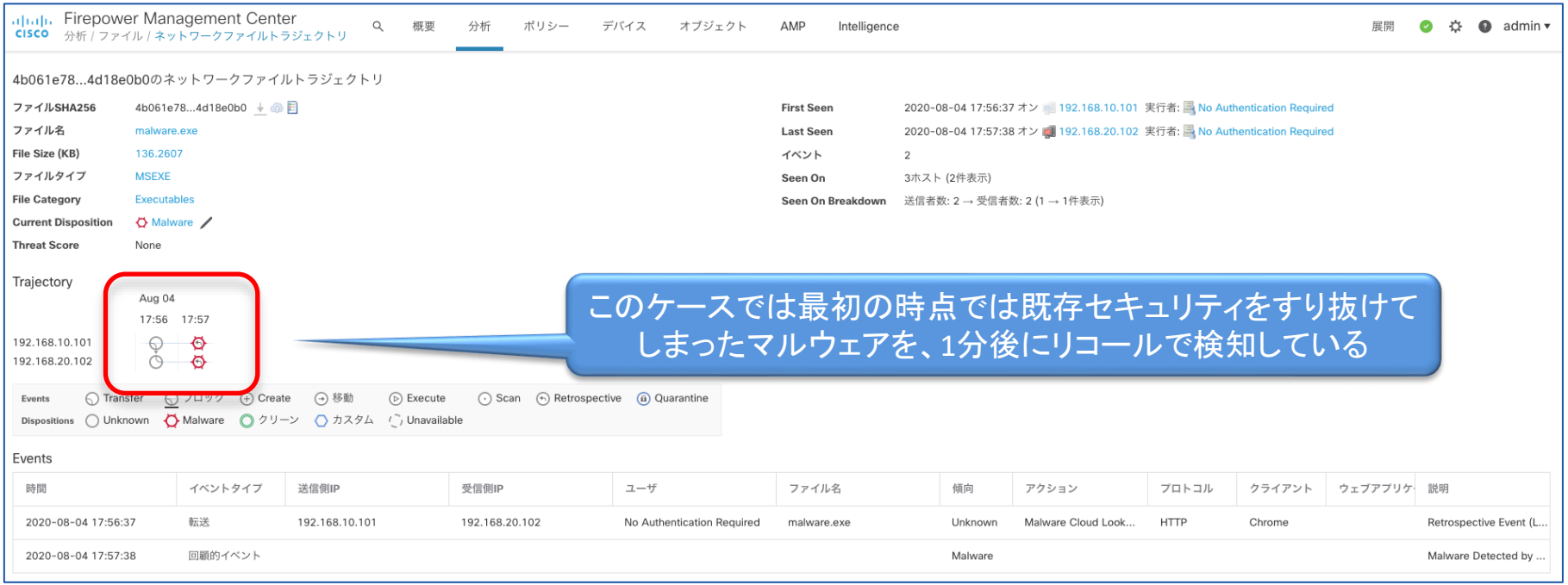
③ ネットワーク上での拡散状況を可視化

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

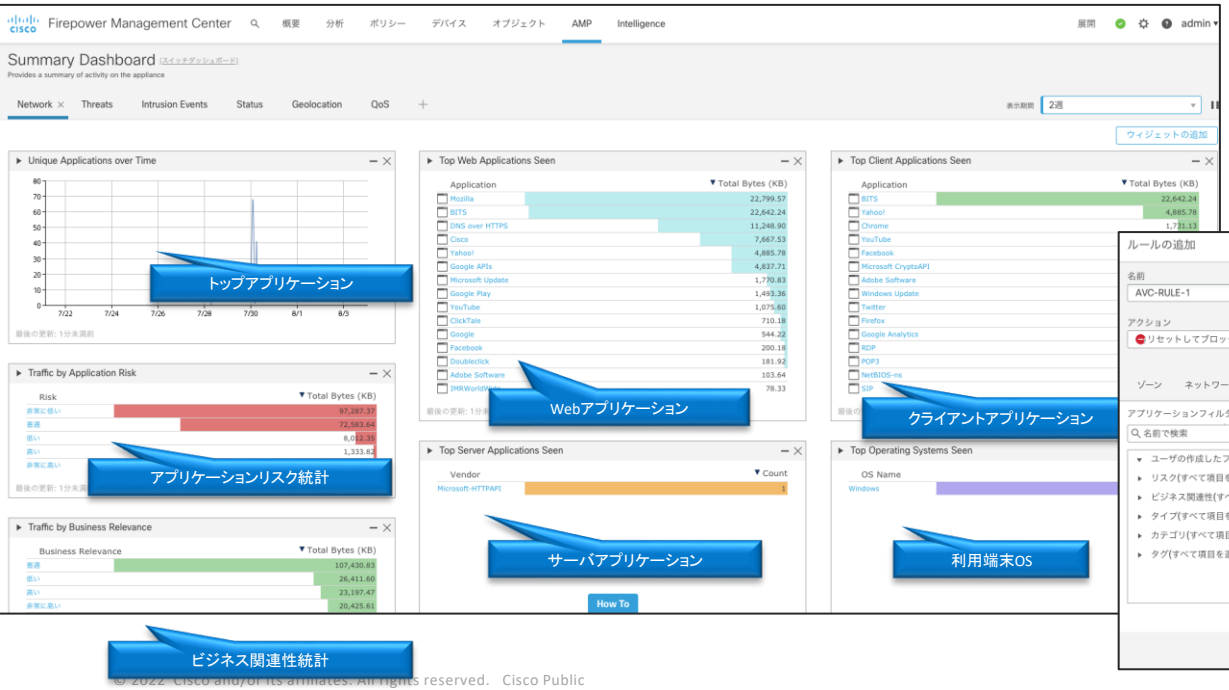


クラウドリコールによるゼロデイマルウェア検知例



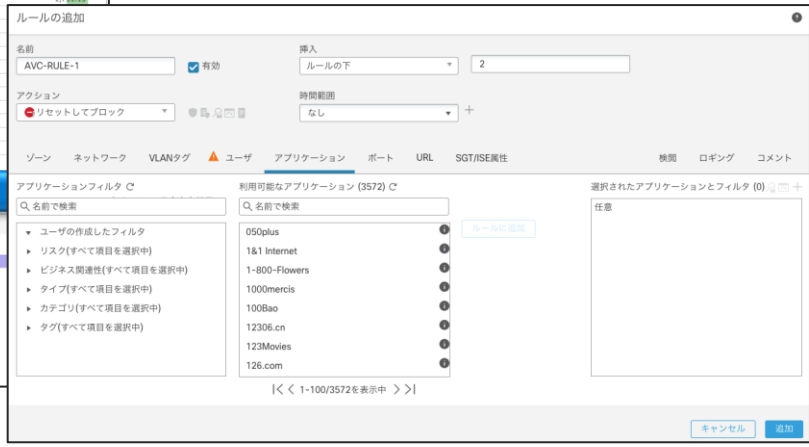
Application Visibility Control アプリケーションの可視化と制御

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



対応アプリケーションリスト https://appid.cisco.com/

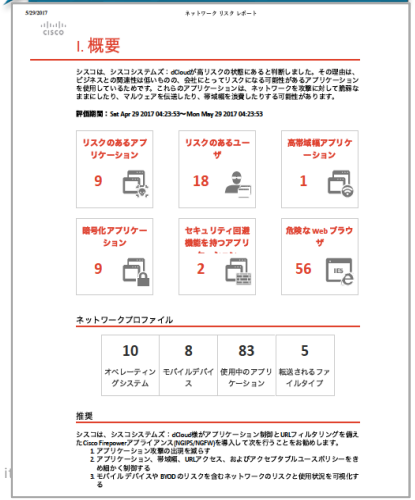
Custom Report レポート機能

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

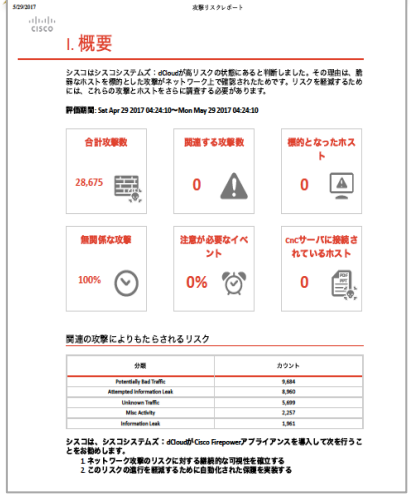
作成したレポートを任意のメールアドレスへ自動転送

PDF、HTML、CSV形式をサポート

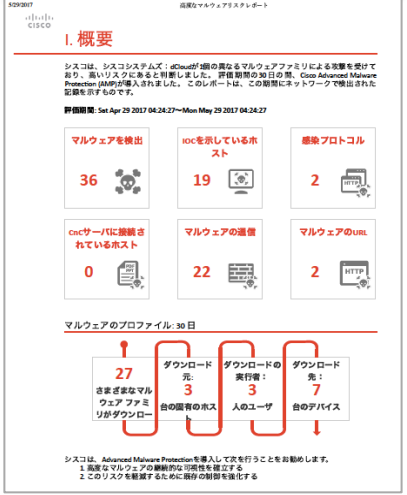
ネットワークレポート



アタックレポート



マルウェアレポート



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

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 *Chandrodaya 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。

導入事例

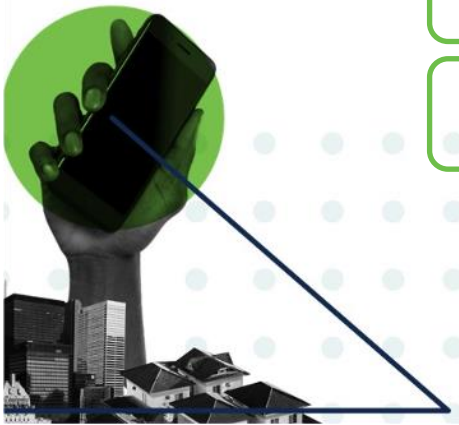
同志社大学様での Cisco Secure Firewall 導入事例

https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/2042-doshisha.html

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

FMC

SF Tunnel
互いの Management Interface 間にて
TCP/8305 で通信
設定、管理、イベント出力等が行われる

FP Sensor

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

Firewall Management Center プラットホーム一覧

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

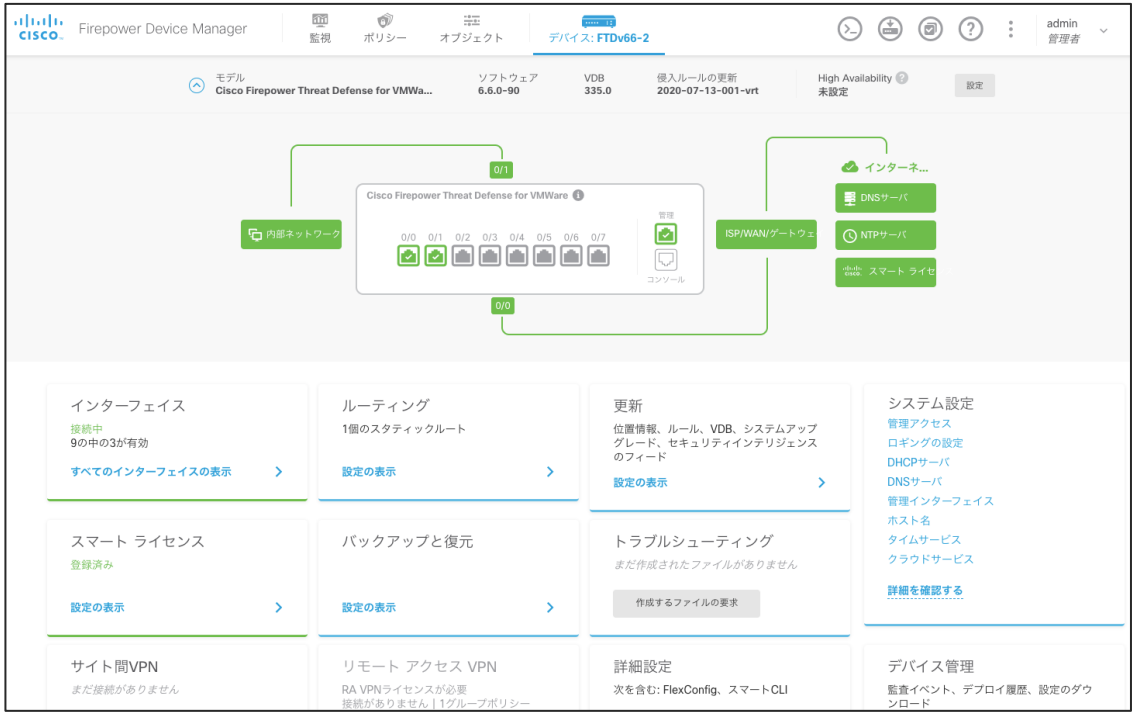
Virtual FMC
最大 25個のセンサー管理
最大イベント数 1,000万件
250GB のイベントストレージ
最大 5万ホスト、5万ユーザの
ネットワークマップ
300個のセンサー管理対応
モデルも有り (FMCv300)
HA対応 (VMware のみ)

FTD の機能を最大限に引き出す管理サーバ

Firewall Device Manager (FDM) 概要

フリーで提供される 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



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

共存不可

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

https で管理接続

Cisco Defense Orchestrator

*SDC

Internet

共存可能

https
ブラウザで管理・設定

CDOの画面

*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

注意) CDO から FMC の管理は可能、ただし、機能は大きく限られる

Firepower アプライアンスポートフォリオ

FPR 1010

650 Mbps AVC
650 Mbps AVC+IPS

SOHO/
SMB

FPR 1120/40/50

650 Mbps AVC
650 Mbps AVC+IPS

Branch
Office

FPR 2110/20/30/40

1.5-3 Gbps AVC
1.5-3 Gbps AVC+IPS

Mid-Size
Enterprise

FPR 4112/15/25/45

2-8.5 Gbps AVC
2-8.5 Gbps AVC+IPS

Large
Enterprise

FPR 9300 Series

SM-40
SM-48
SM-56

Stand-alone device:
12-53 Gbps AVC
10-47 Gbps AVC+IPS 6
Six node cluster:
Up to 254 Gbps AVC
Up to 226 Gbps AVC+IPS

Data
Center

One Module:
30-70 Gbps AVC
24-64 Gbps AVC+IPS
Six node (2 chassis) cluster:
Up to 336 Gbps AVC
Up to 307 Gbps AVC+IPS

Service
Provider

新モデル 近日リリース予定

Firewall バーチャルプラットホーム

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, ASAv は、既存の AWS, Azure に加えて、 Google Could 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

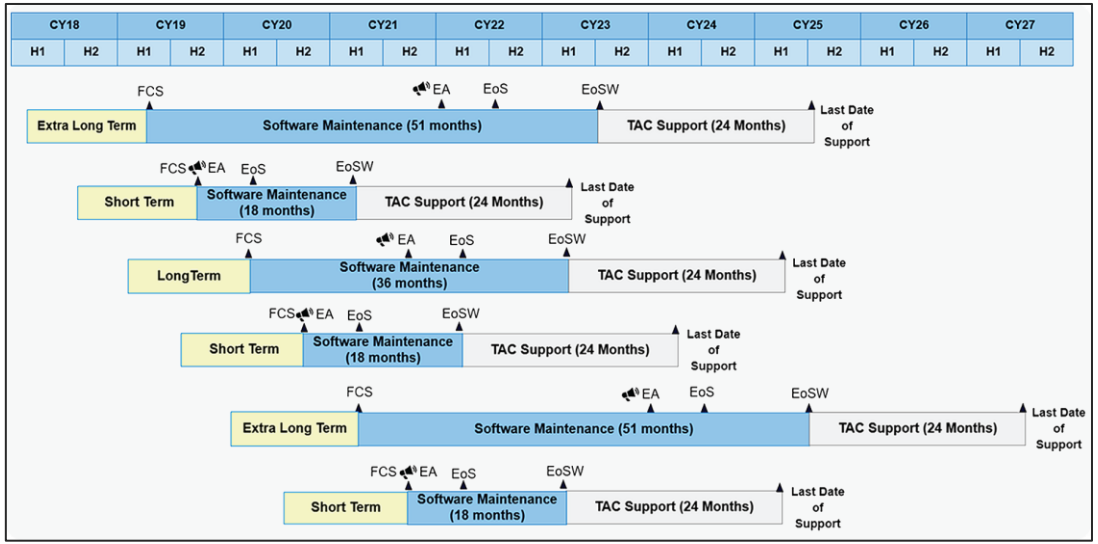
Cisco’s Next Generation Firewall Product Line Software Release and Sustaining Bulletin
https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html

- 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

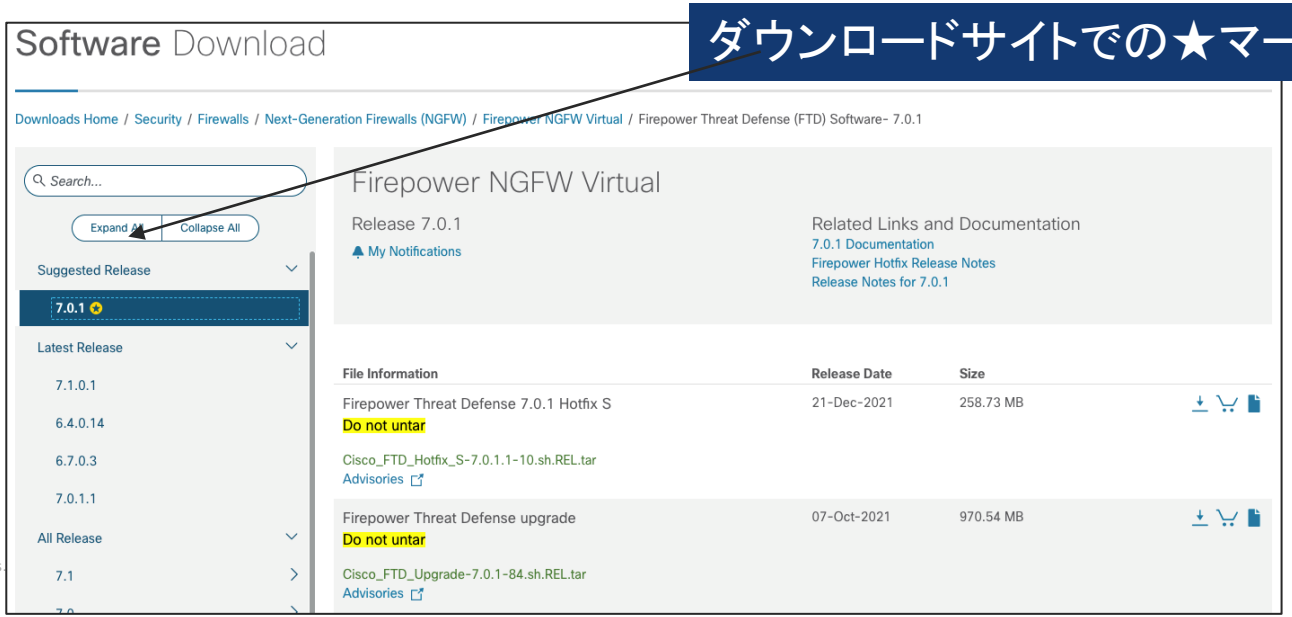
  FTD 6.6 → ロングタームサポート
- ロングタームサポートの中でも、奇数年にリリースされるものはエクストラロングタームサポートとなる

  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

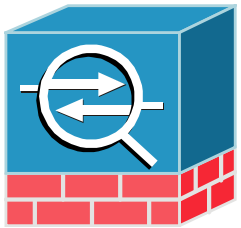
- 2022年3月時点で一般的な推奨バージョンは 7.0.1
- 稼働実績と重大な障害の数、および重大な不具合の数を総合的に見て推奨バージョンを選定している



[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)

どちらもまだまだシスコのセキュリティ製品の中核かつ主力

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

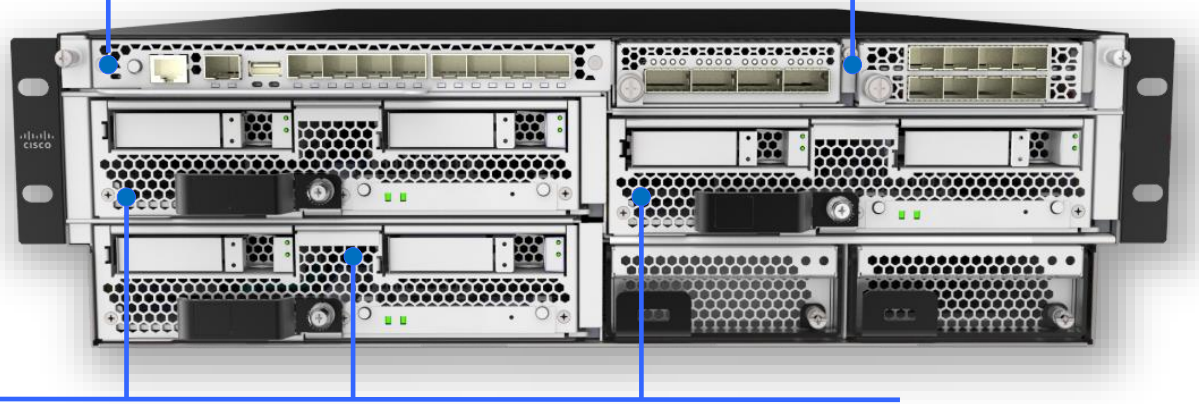
当セッションは以降 FTD にフォーカス

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

ソフトウェアは FTD と ASA の選択が可能

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 2nd Optional SSD for MSP 800GB		1 x 200GB Default 2nd 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

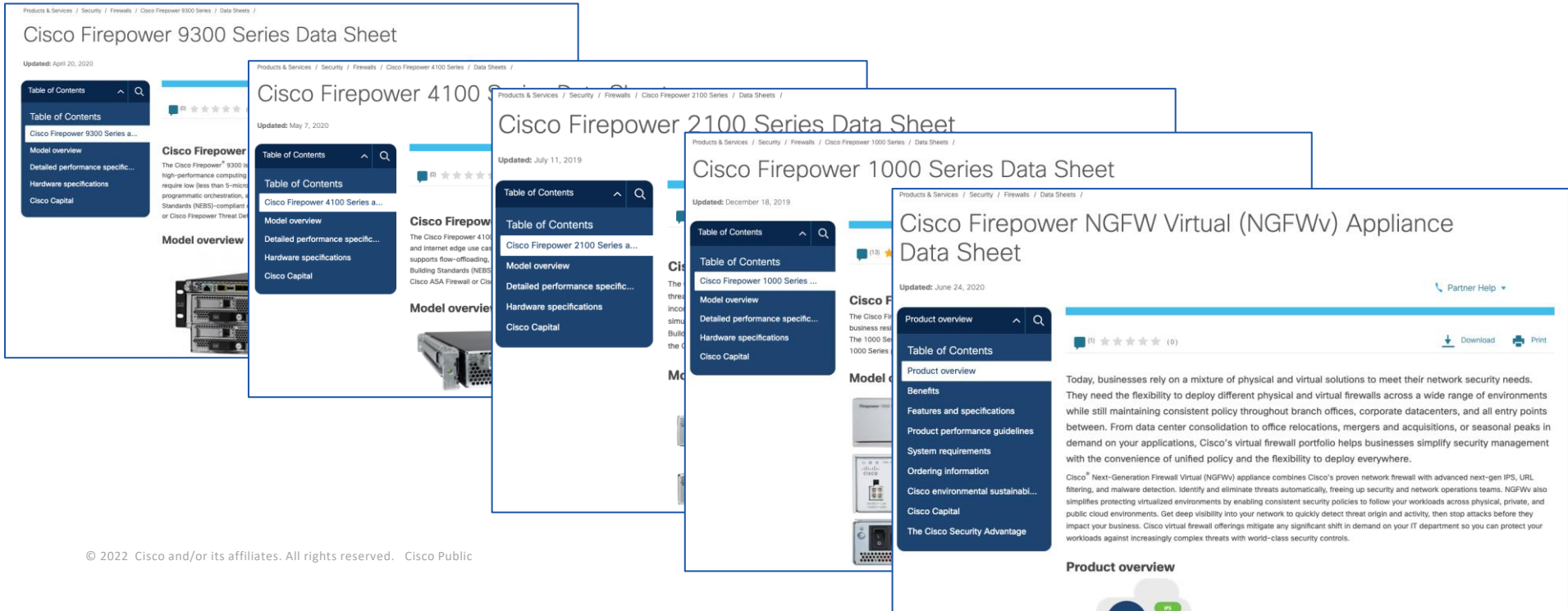
Firepower1120/1140/1150

- 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



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**

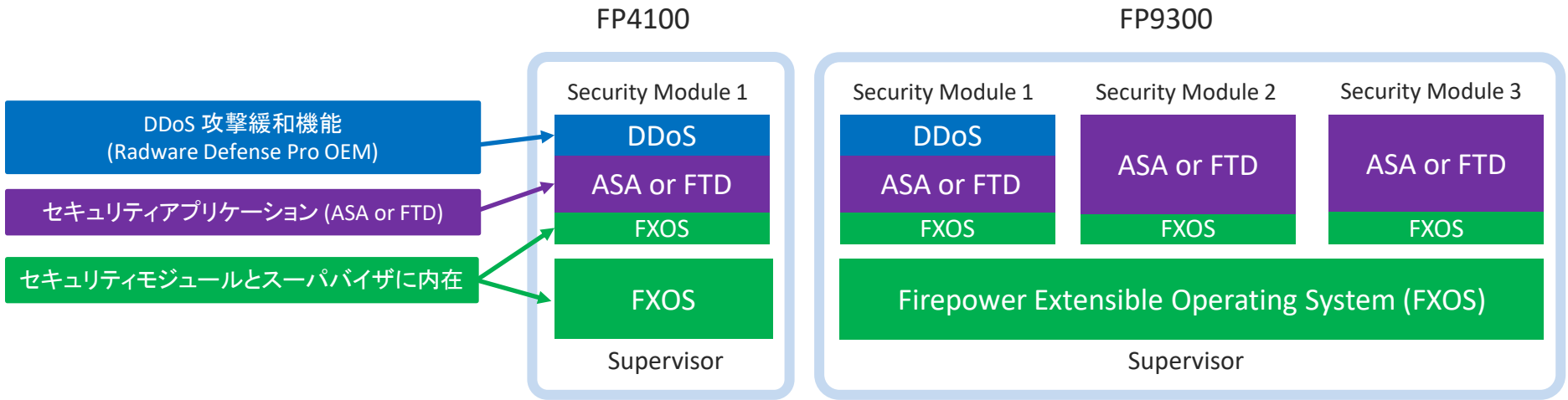
6 X 10 GE SR/LR ファイバ
Firepower **2100**、4100、9300

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

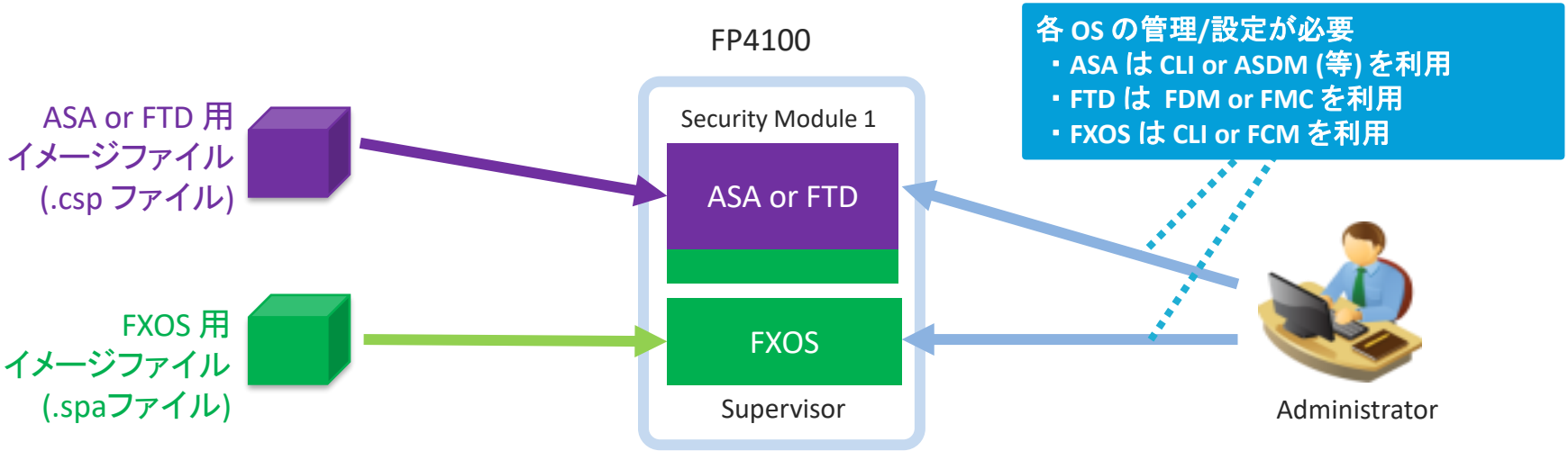
- FP4100/9300 内には Firepower eXtensible Operating System (FXOS) が動作
  - FXOS が、スーパーバイザや セキュリティモジュールを管理
  - FXOS が、シャーシや ネットワークモジュール、電源、FAN などハードウェアの管理
  - FXOS が、セキュリティモジュールに物理インターフェイス割当て



TIPS) FP4100 と FP9300 の主な違いは、セキュリティモジュール搭載数と対応ネットワークモジュール

FP4100/9300 と FXOS (続き)

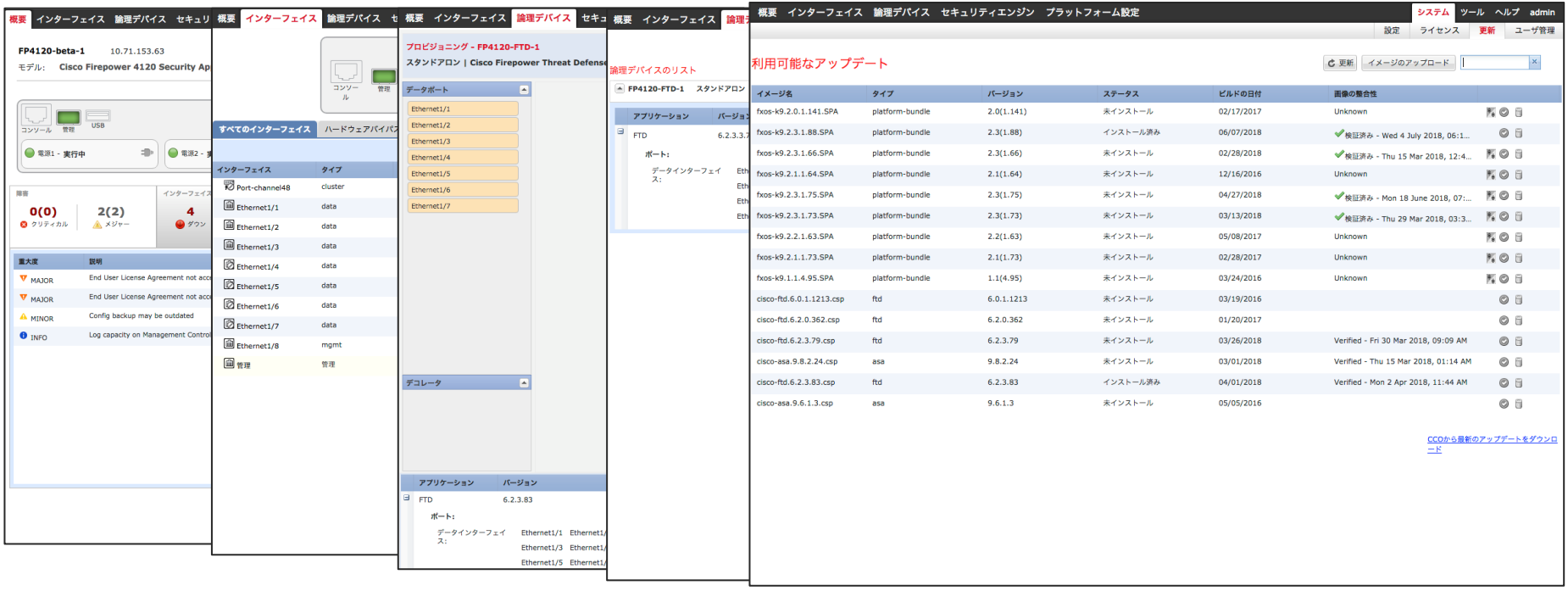
- FP4100/9300 は**プラットフォーム型**で、シャーシ内に複数 OS が動作可能
  - FXOS と ASA/FTD は、**各独立した OS** であり、イメージファイルや設定ファイルが異なる
  - FXOS と ASA/FTD の各アップグレードは、別々に実施が必要
  - FXOS と ASA/FTD は、各独立した管理インターフェイスと管理 IP アドレス, GUI, Syslog, SNMP Agent をもつ



TIPS) FP4100/9300 は拡張性重視のため、FXOS と ASA/FTD の独立性が高い

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)



FP2100/1000 と FXOS

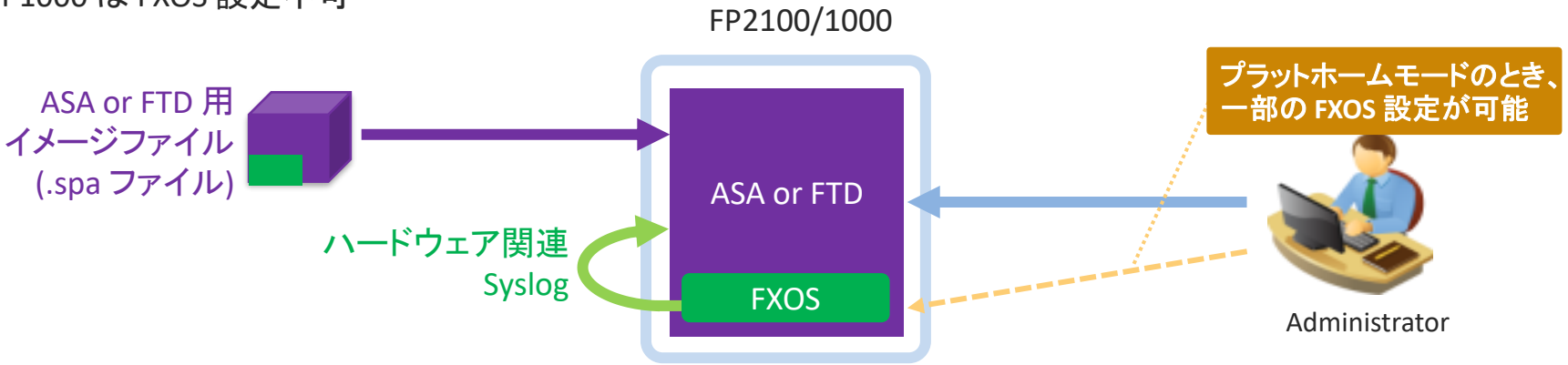
- FP2100/1000 は**アプライアンス型**で、FXOS と ASA/FTD の統合が進んだモデル

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

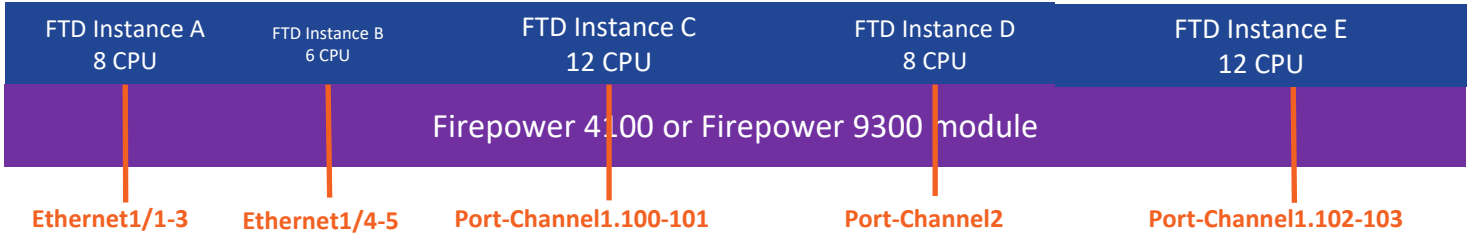
FP2100 での ASA の場合、FXOS 設定不可のモード (アプライアンスモード) と FXOS の設定を必要最小限 (管理 IP アドレスや物理インターフェイス割当て、NTP 設定など) 行えるモード (プラットホームモード) がある。アプライアンスモードが推奨。FTD の場合、FXOS 設定不可

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

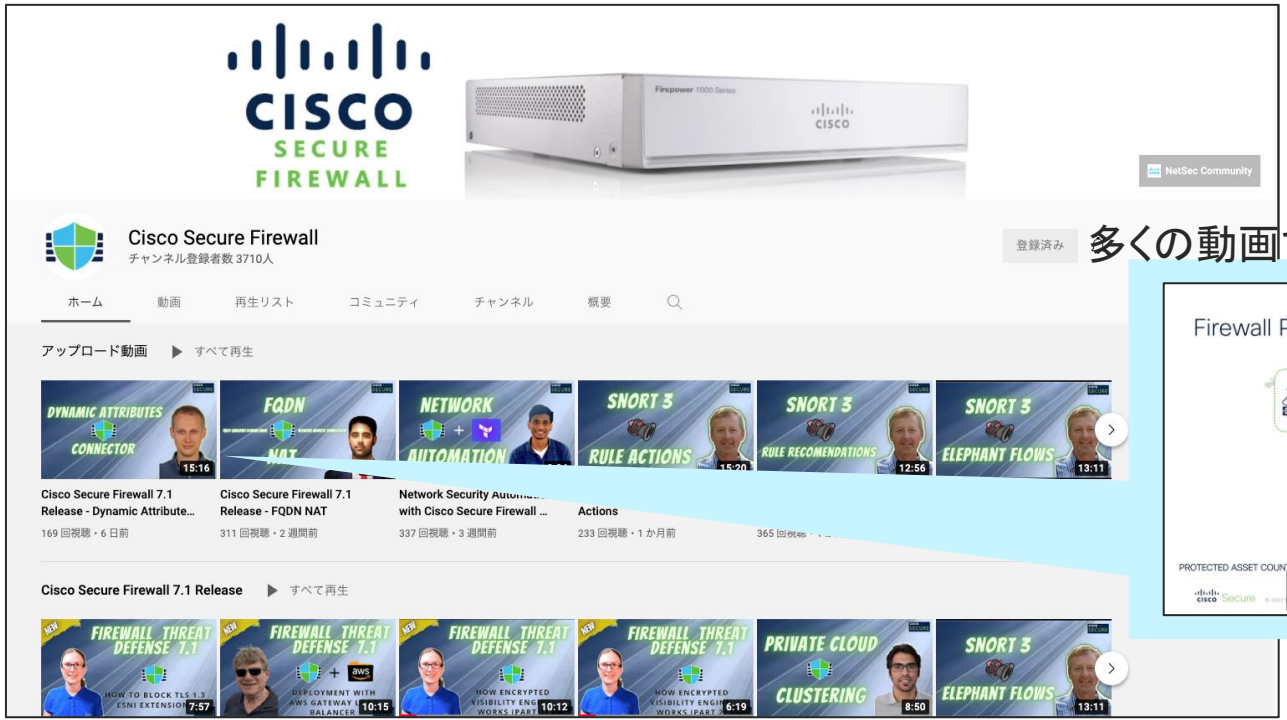
- Firewall Threat Defense (FTD) が上位レイヤの脅威対策を行う NGFW & IPS 製品として位置づけられ、市場で認知されている
- L4 までの Basic Firewall である ASA と L7 Security の FTD を適材適所で使い分ける
- “本当に使える” 脅威対策として FTD は優れた機能や管理性を持つ
- FTD は ASA の機能を包含した新たな NGFW + IPS + Malware Defense 製品として利用可能
- FTD も ASA も同一ハードウェアで動作し、豊富なラインナップがある
- FTD と ASA の明確な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

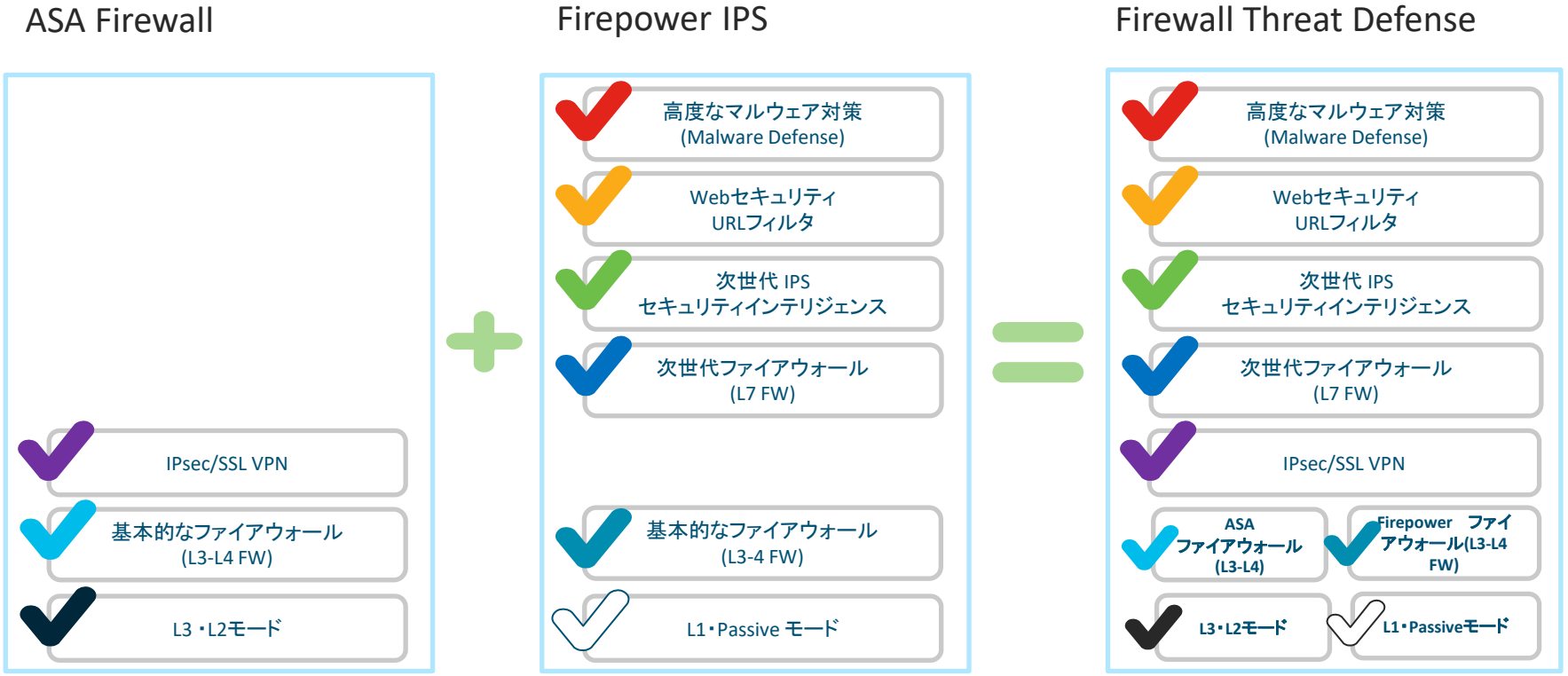


多くの動画で日本語への自動翻訳が有効


CISCO

(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

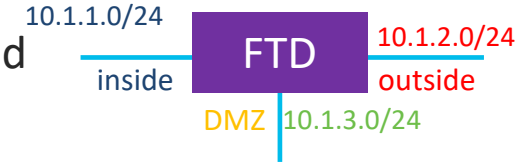


FTD インターフェースモード

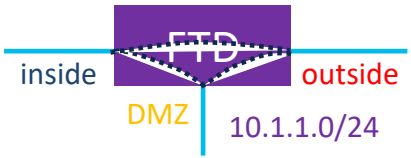
NGFW

ASAから継承

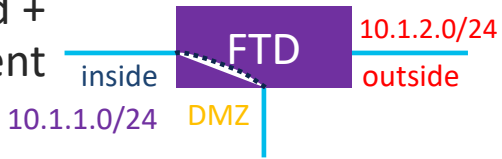
Routed



Transparent



Routed +
Transparent



Firepowerから継承

NGIPS

Inline

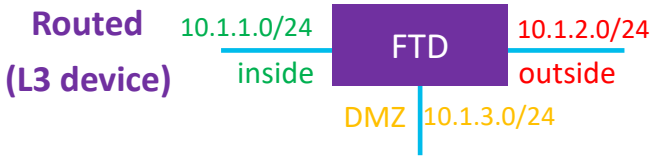
Inline Tap

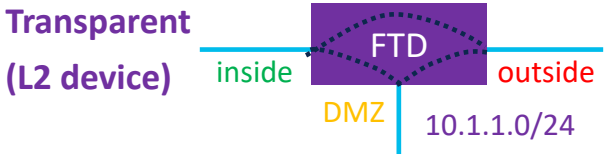
Passive

※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

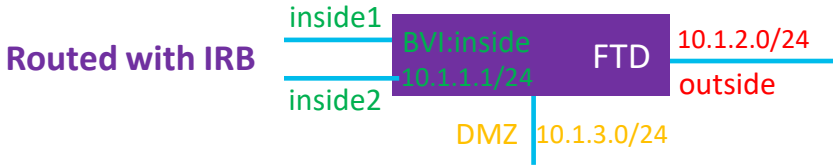
- FTD 新規デプロイ時にその FTD の Firewall としてのモードについて、Routed Firewall か Transparent Firewall の選択が必須





  - Transparent Mode での BVI には IP アドレス設定が必須

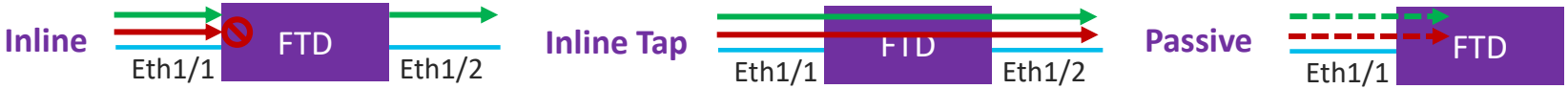
- Routed インターフェイスと IRB (Integrated Routing and Bridging) の併用が可能



- 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

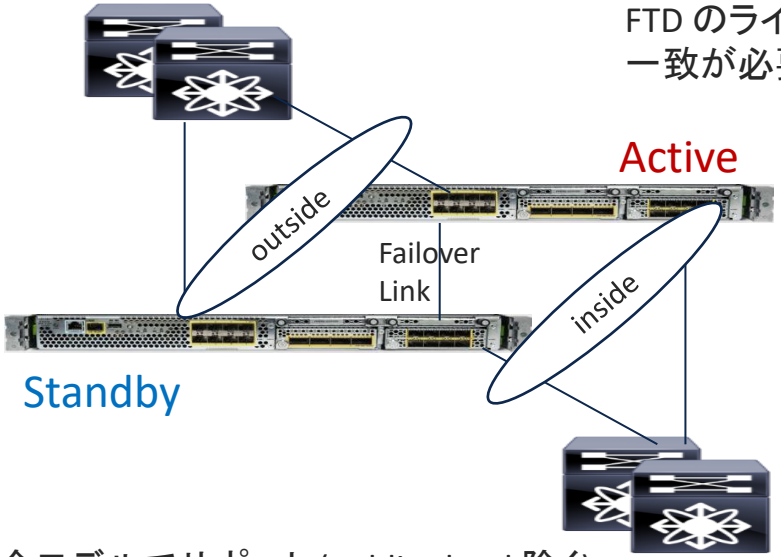


- Inline は Intelligence なケーブルとして動作 (L1 mode とも言う)
- 物理 / EtherChannel での Inline Pair が利用可能: Inline Sets は非対称通信をサポート
- VLAN と LACP はパススルー可能。Q-in-Q のパススルーは不可。
- 全ての Security Policy は有効。Inline モードではブロック可、Inline TAP と Passive モードはブロック不可
- データプレーンは HA / Clustering 時にコネクションをトラック (データプレーンでの Block は無い)
- NAT、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

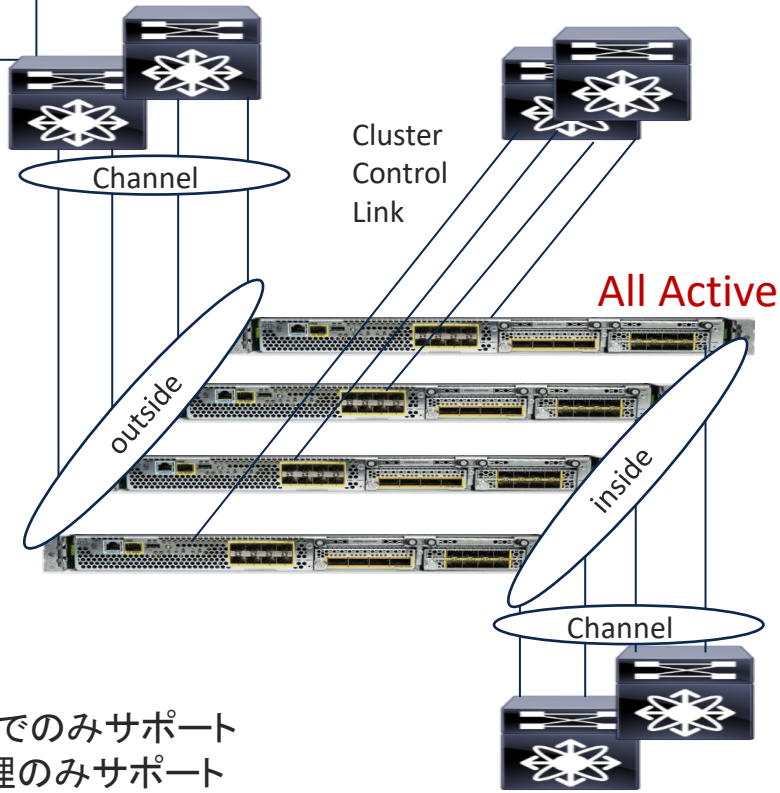
Active - Standby



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

注2) どちらの構成でも
FTD のライセンスは
一致が必要

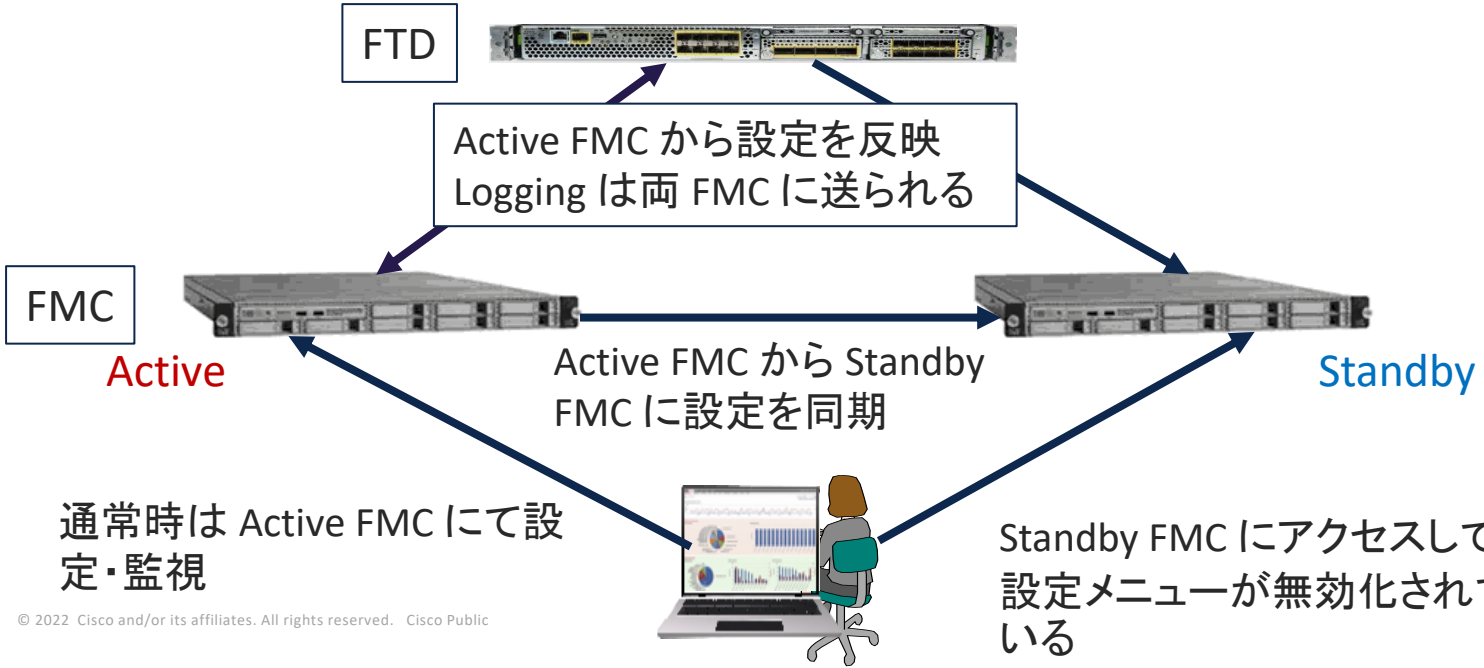
Cluster



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

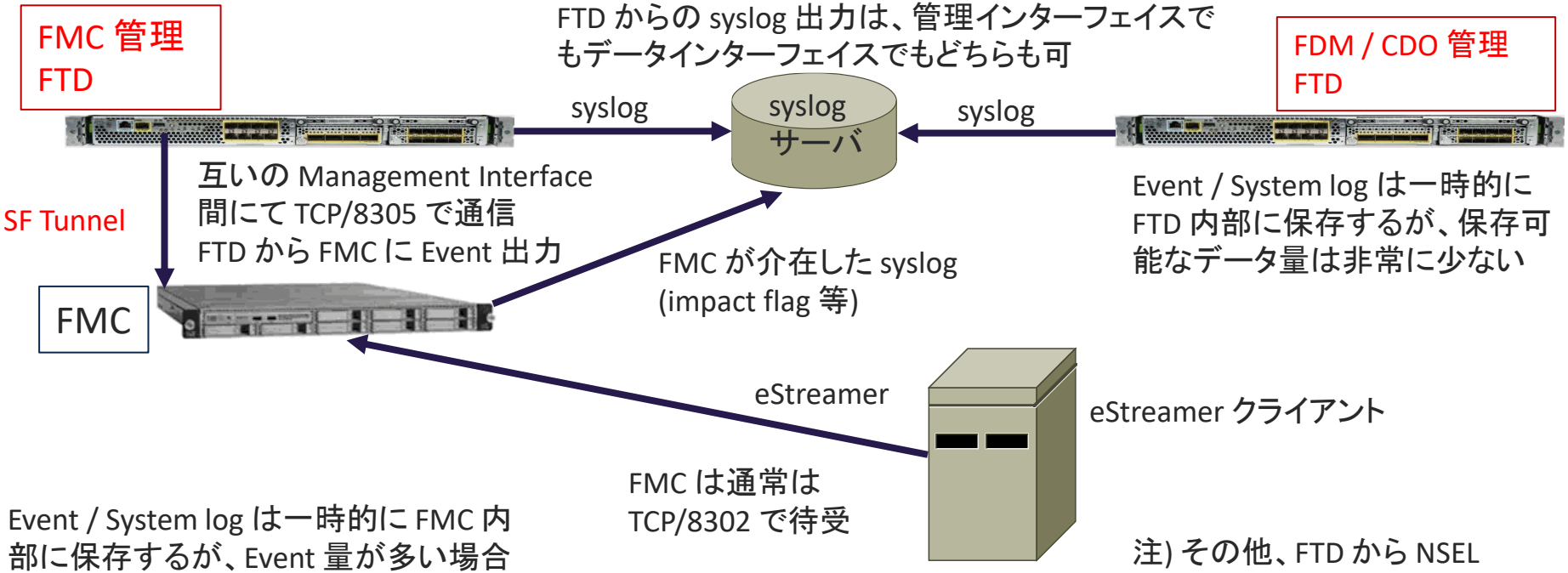
FMC の高可用性

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



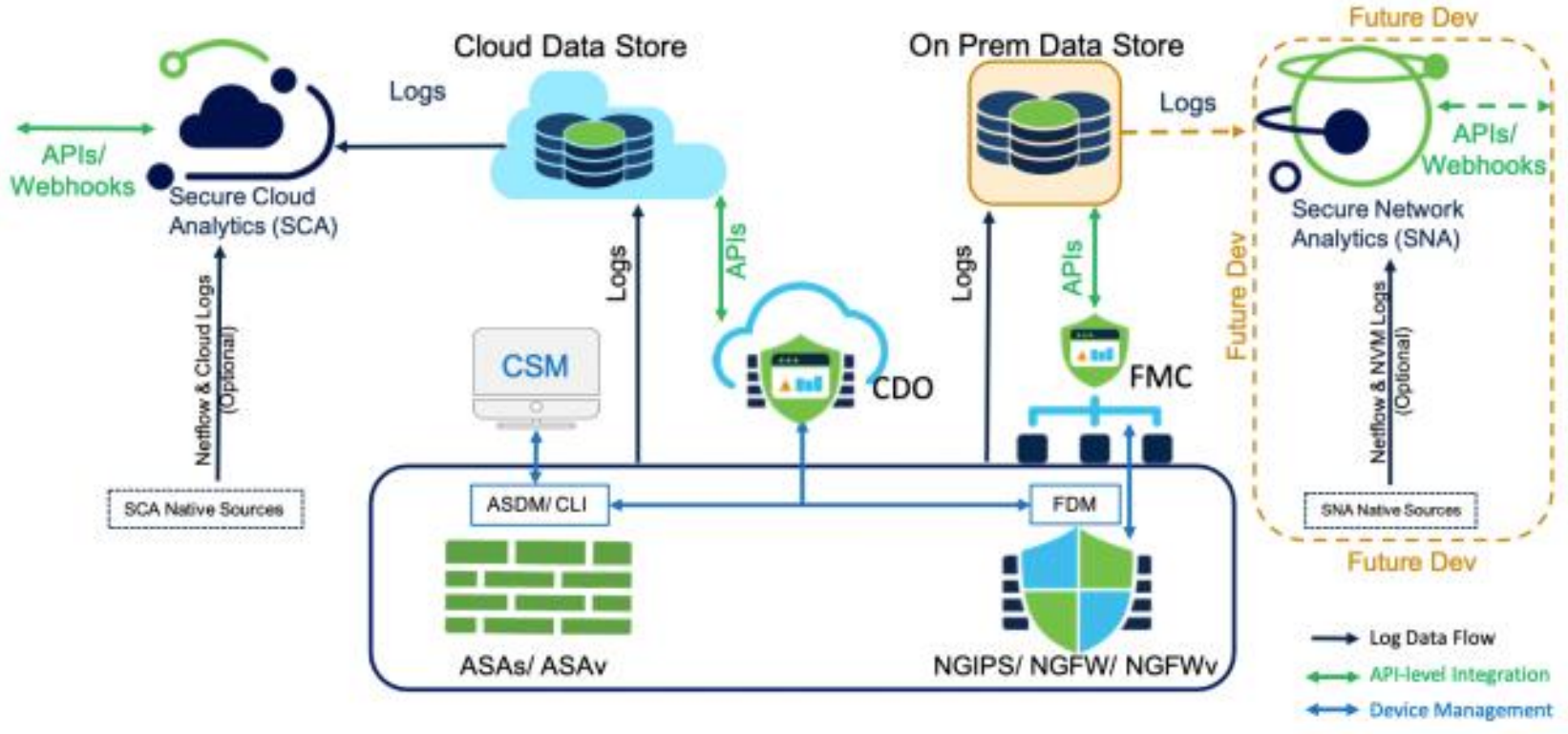
Logging

FTD から直接出力される syslog と FMC からサーブされる eStreamer がある



SAL (Security Analytics Logging) アーキテクチャ

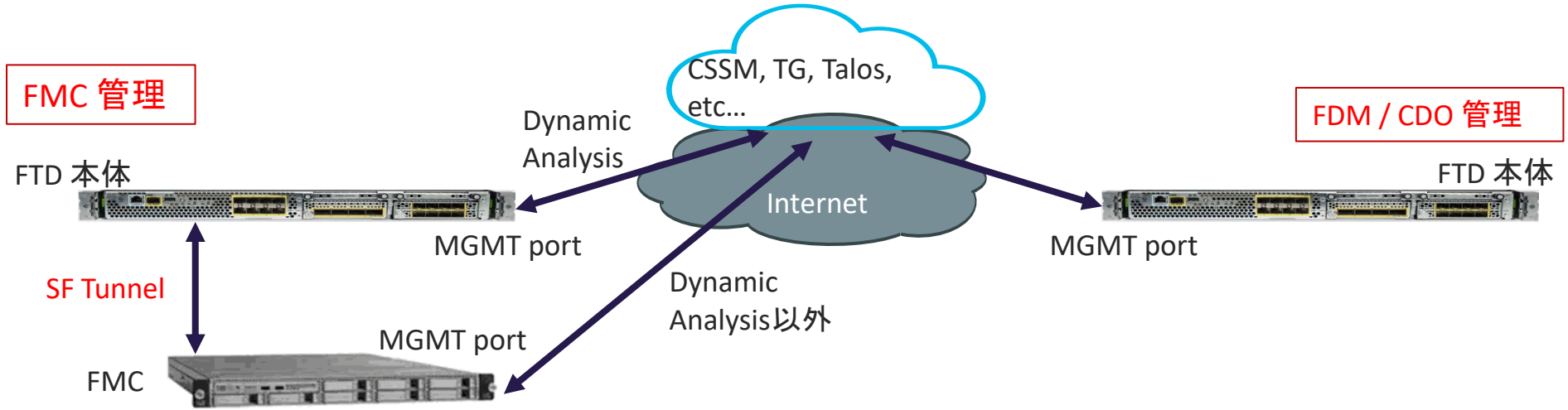
Firewall の logging をクラウド or オンプレミスに実施し、そのデータを有効活用



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

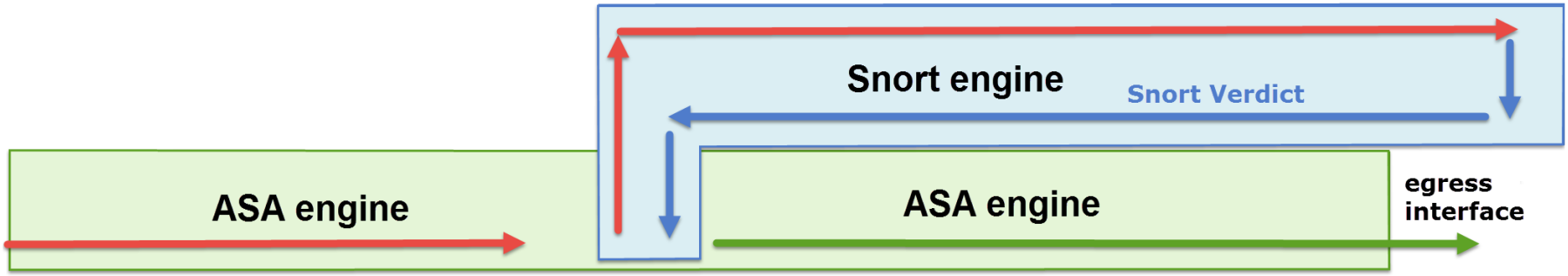


FMC 管理の場合、CSSM へのアクセスも含め、ほとんどのインターネットアクセスは FMC が実施する
ただし、Cloud の Threat Grid にファイルを submit する (Dynamic Analysis) のは FTD から行われる
Proxy 経由、NAT 越えはサポート
CSSM へのアクセスが不可な場合 (Air Gap 環境)、License Reservation を利用

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

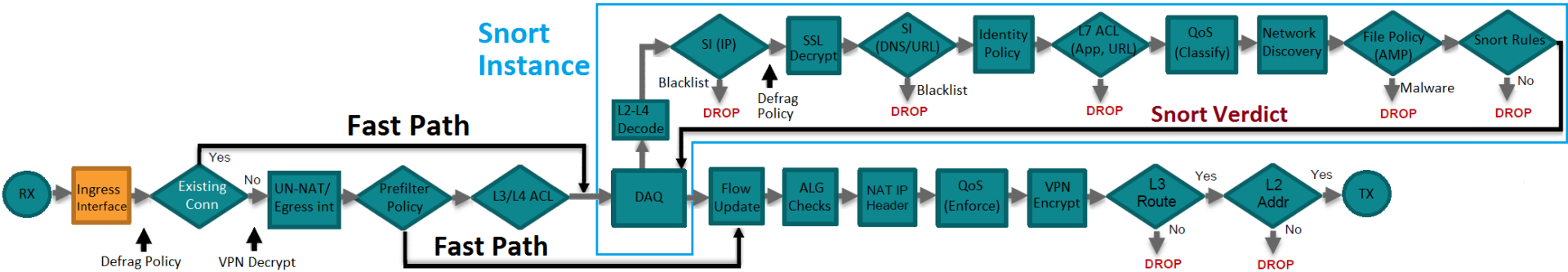
FTD パケット処理の大まかなプロセス



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

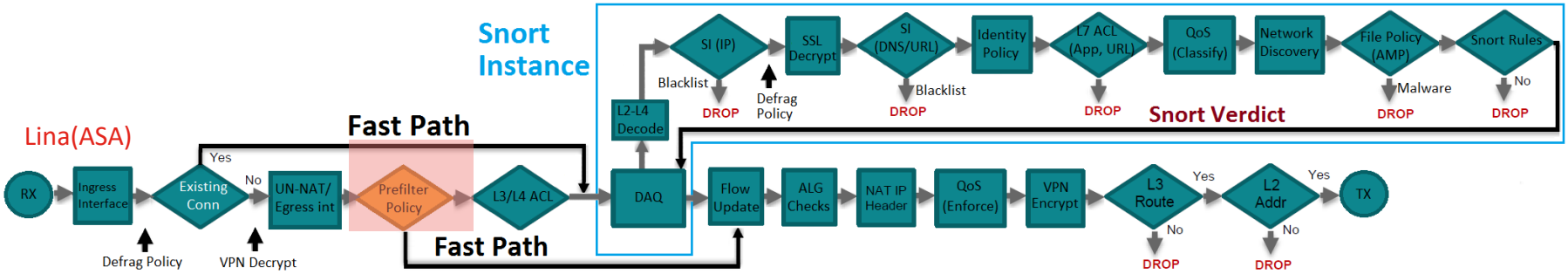
- Snort エンジンは 6.x のコードで動作
- ASA エンジンは 9.x のコードで動作

FTD パケット処理 詳細



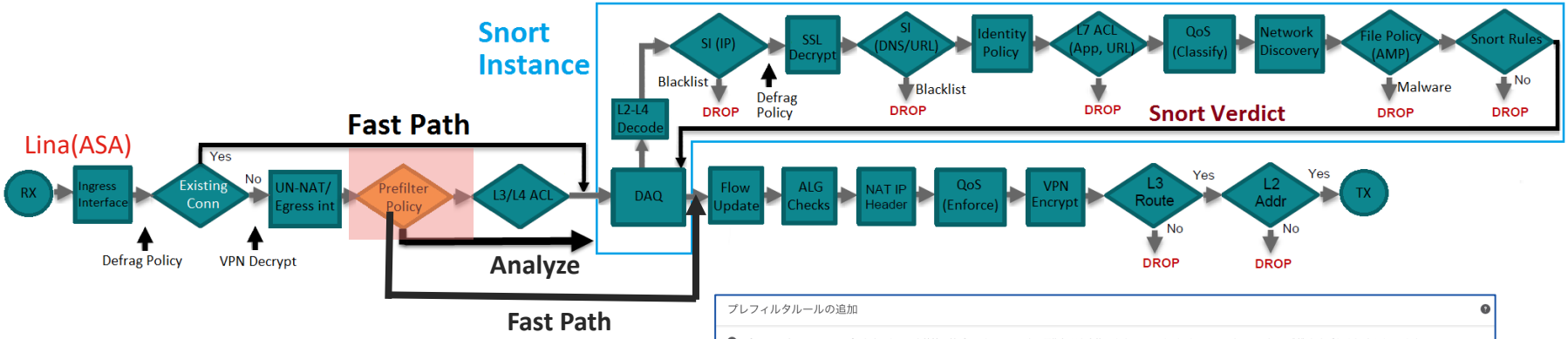
Routed / Switched(Transparent) mode: ASA + Snort フル機能
その他: ASA 一部機能 (L3-4ACL)

Prefilter ポリシーの役割



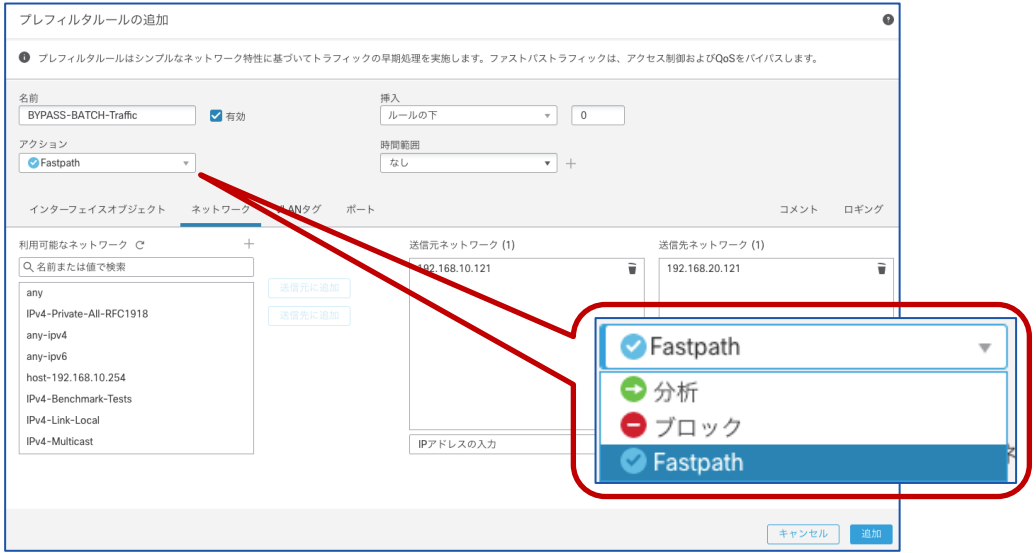
- Prefilter ポリシーは主に2つの役割を提供
  1. トンネル内のパケットに対するインスペクション処理
     - GRE、IP-in-IP、IPv6-in-IP、Teredo Port 3544
  2. Snort 処理前のアクセスコントロール
     - 監視系 / バックアップなど L7 レベルでの検査が不要な信頼された通信をバイパスする、等

Prefilter ポリシーの役割 (続き)

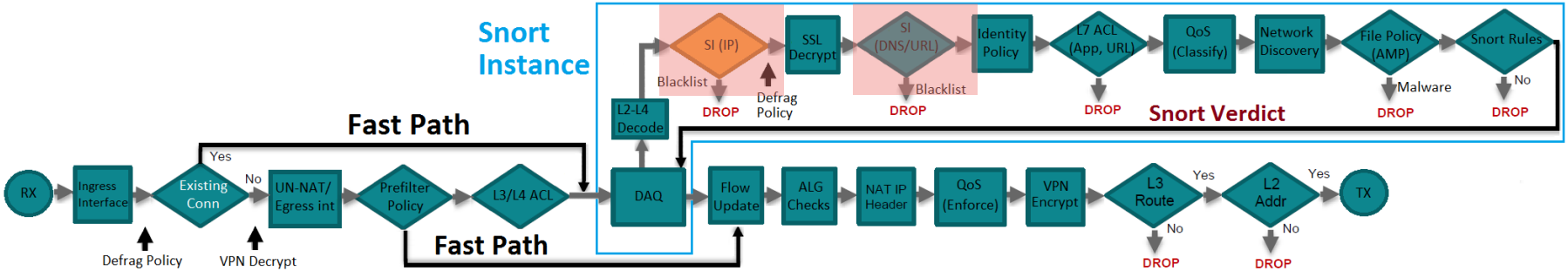


- Snort 処理前のアクセスコントロール、3つのアクション

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)



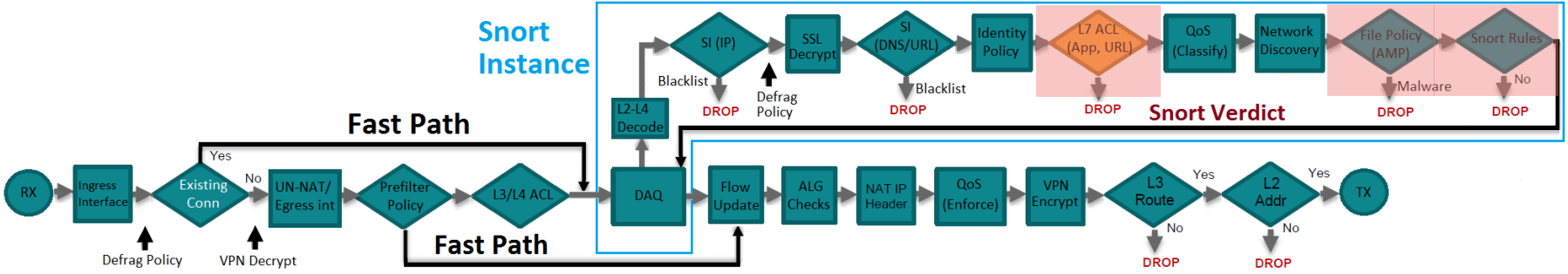
Security Intelligence (IP Address / URL):

- 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):

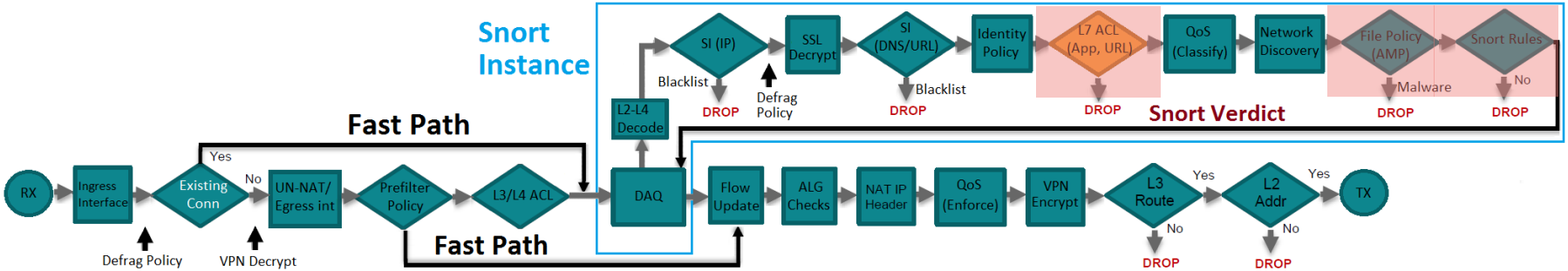
- Security Intelligence に指定された DNS 群を以下の処理を実施可能
  1. Whitelist
  2. Monitor
  3. Domain Not Found (NXDOMAIN)
  4. Drop (DNSクエリー)
  5. Sinkhole (IP リダイレクト)
- Blocklist は 手動設定 or 自動設定 (Intelligence Feed by Talos or custom)

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

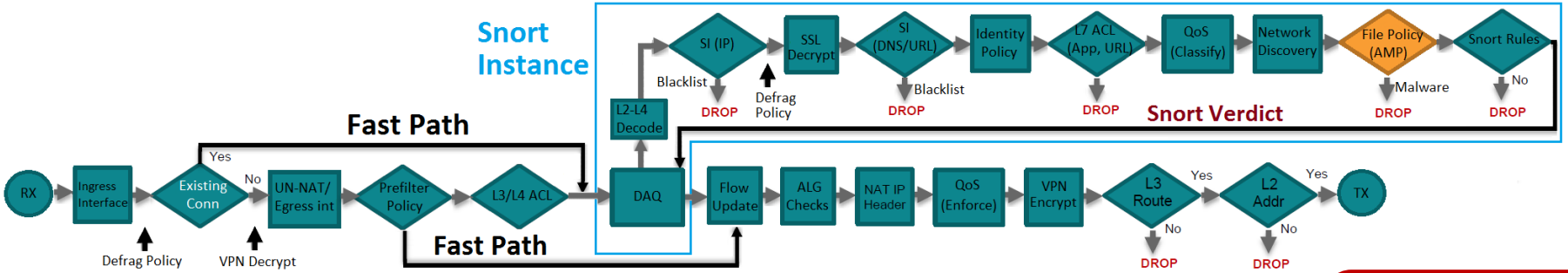
L7 ACL (Access Control Policy) (続き)



- 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

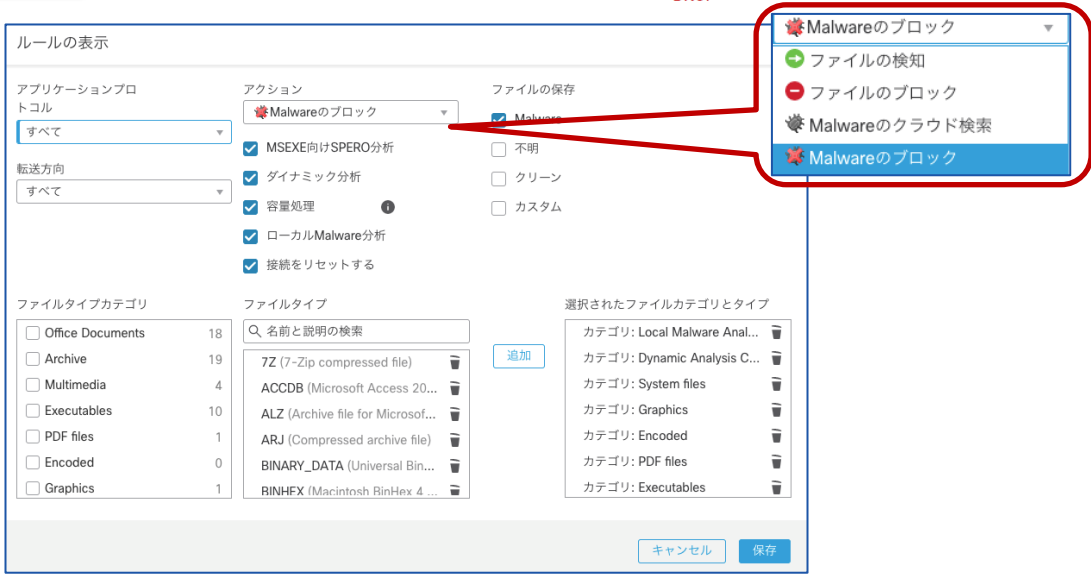
Malware & File Policy



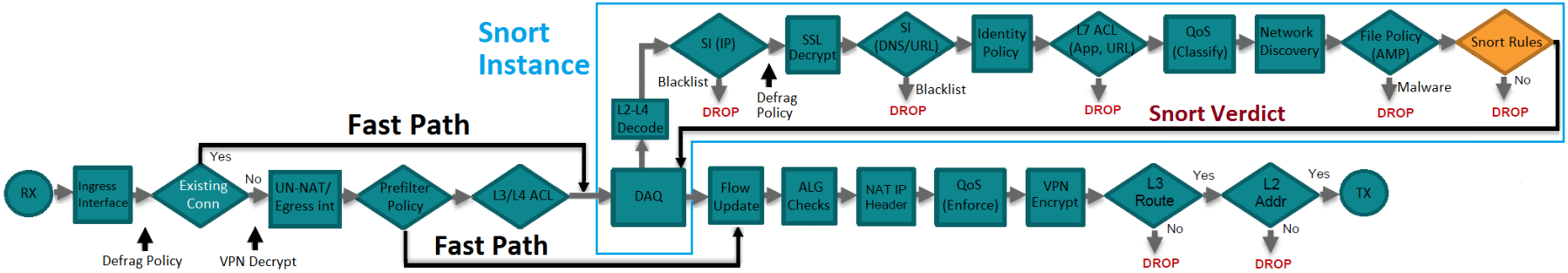
- Malware & File Policy：

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



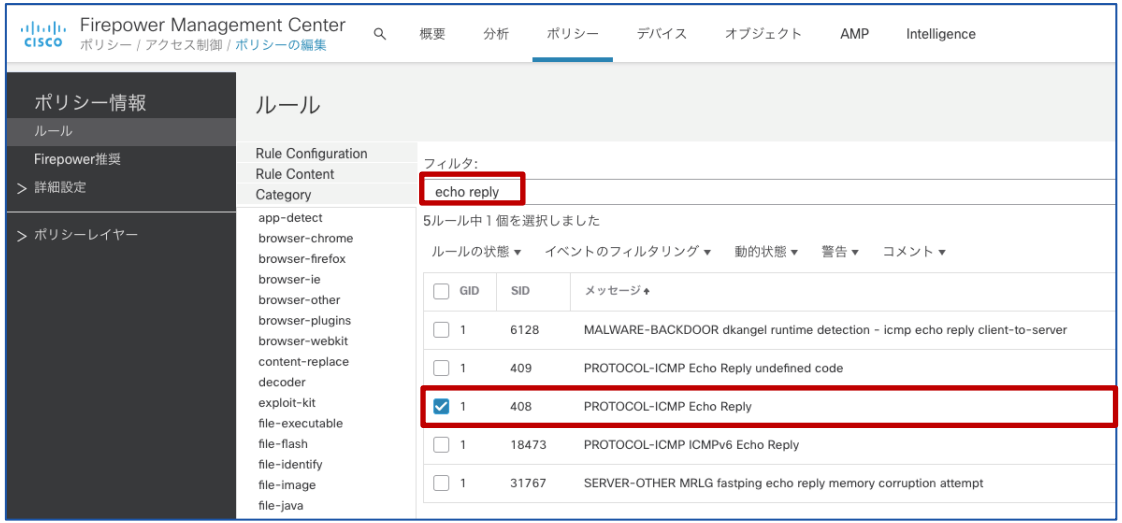
Intrusion Policy



- 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



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

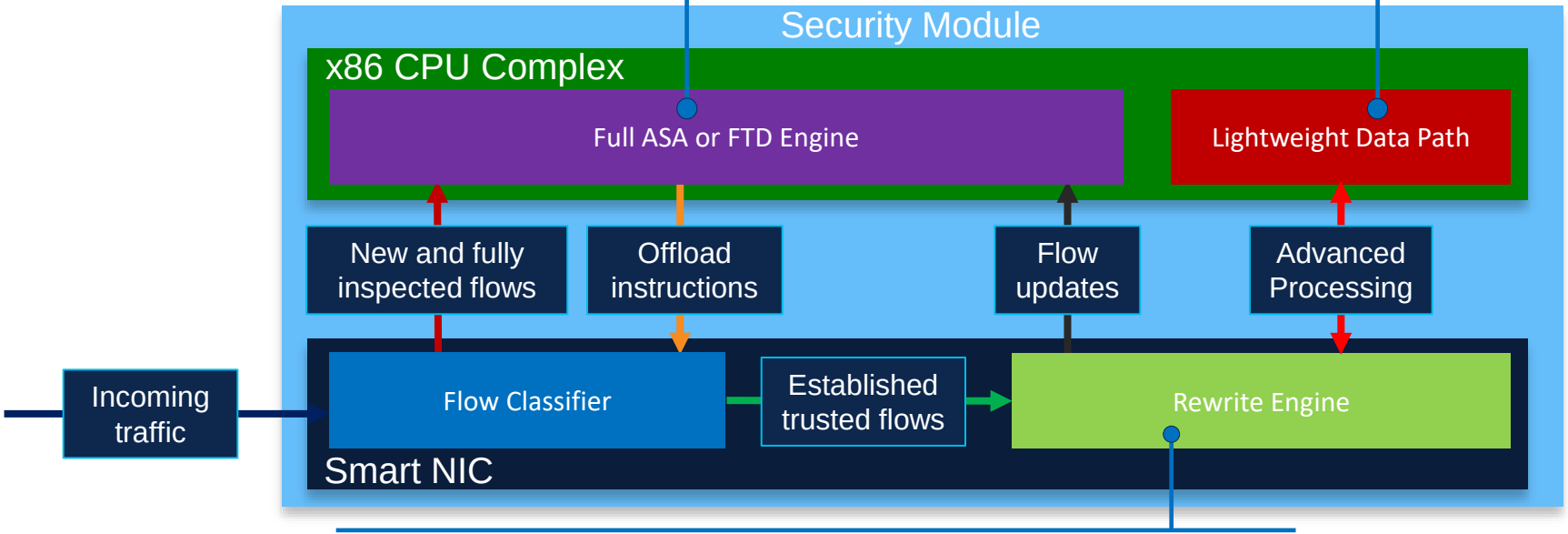
Flow Offload の動き

Full Inspection

- フロー確立後、ダイナミック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

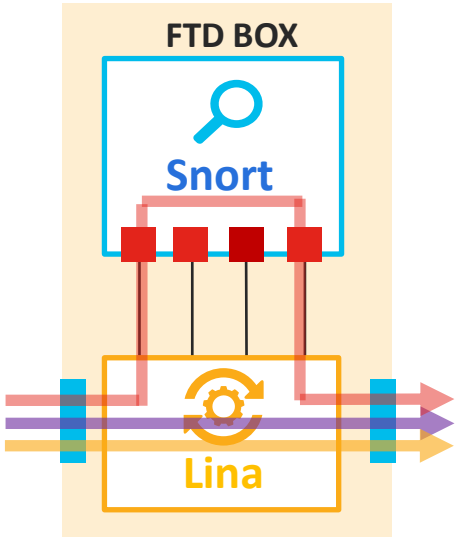
- 制限されたステートトラッキング, NAT/PAT, TCP シーケンスのランダム化
- シングルUDPフローで約40Gbps、2.9us以下の遅延、32K tracked flows

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



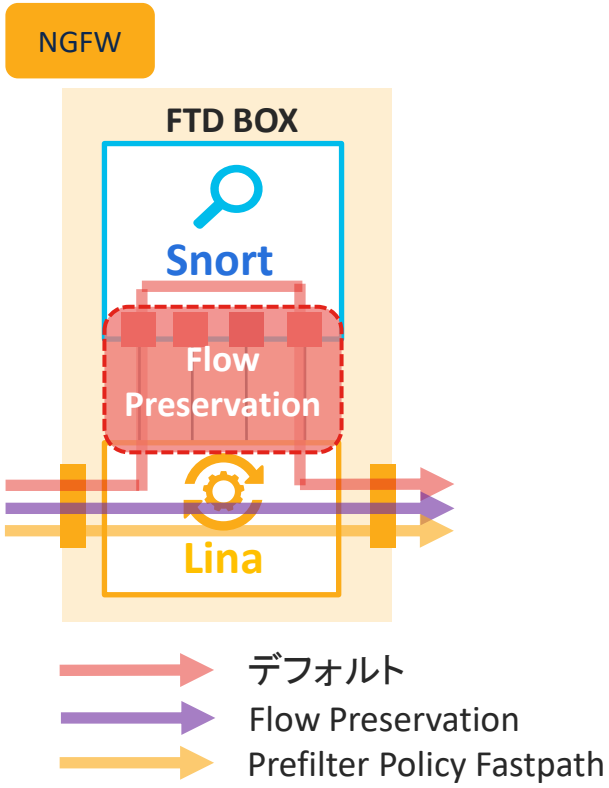
デフォルト
Fail-Open
Prefilter Policy Fastpath

- 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 エンジンをバイパス
- 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 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、既存コネクションのみ 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 されたコネクションは、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


CISCO