本当に必要な脅威対策
Cisco Firewall Threat Defense のご紹介

2024年1月

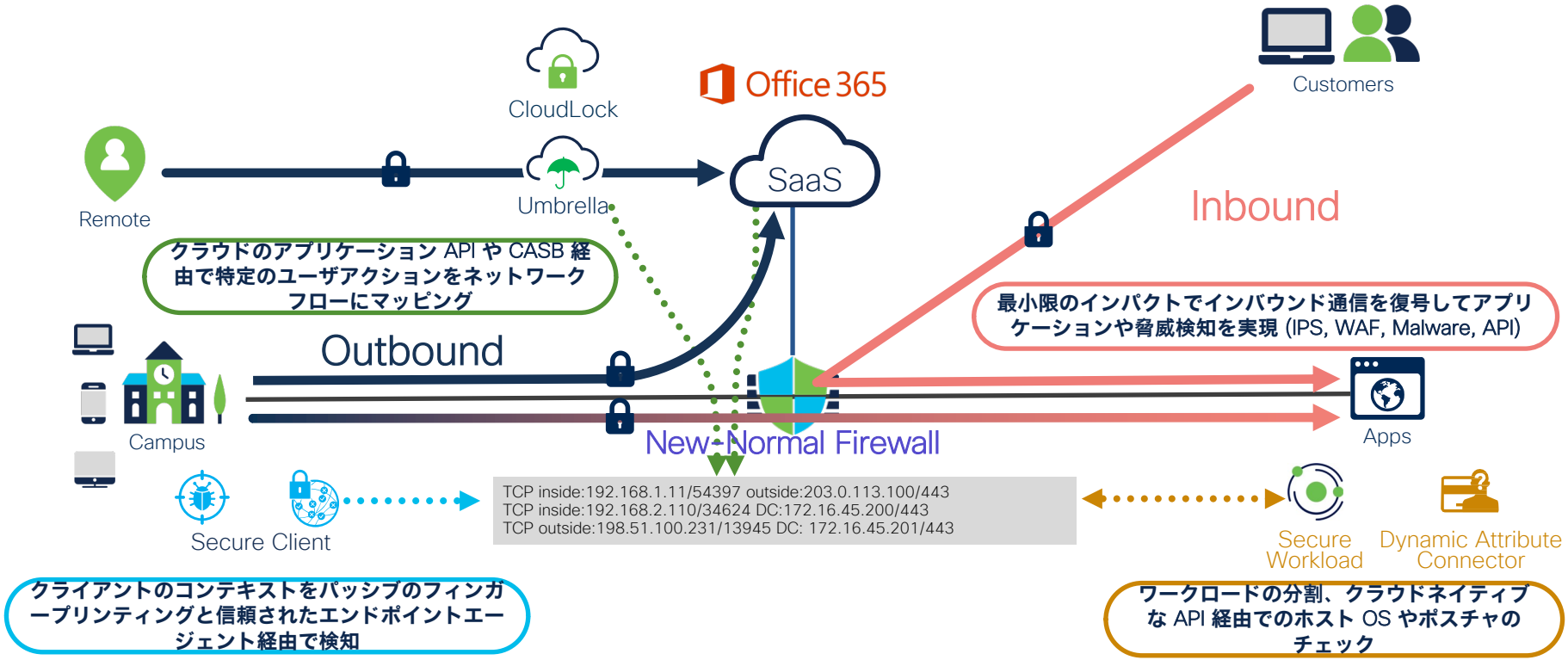
シスコシステムズ合同会社
セキュリティ事業 テクニカルソリューションズアーキテクト
小林 達哉 (tatskoba@cisco.com)

アジェンダ

- Firewall Threat Defense の概要
- Firewall プラットホーム
- Firewall Threat Defense のアーキテクチャ
- まとめ

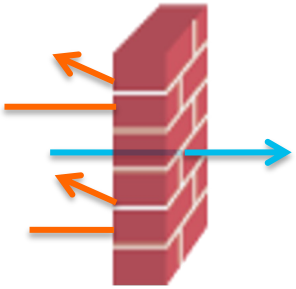
Firewall Threat Defense の概要

Secure Firewall Threat Defense でのインスペクション



Basic 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

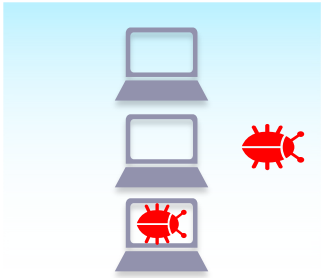
Web アプリケーション、
ユーザ、脅威の可視化

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
- ✓ サンドボックス

FTD の機能と課題との対応付け

L7 情報の可視化によるネットワーク制御

- 業務に不要な、危険なアプリケーション利用の排除
  - AVC
  - URL フィルタ
- 意図しない通信の可視化や制御
  - IDFW (Identity Firewall)
  - Geo Location DB

本当に必要な脅威対策としての IPS

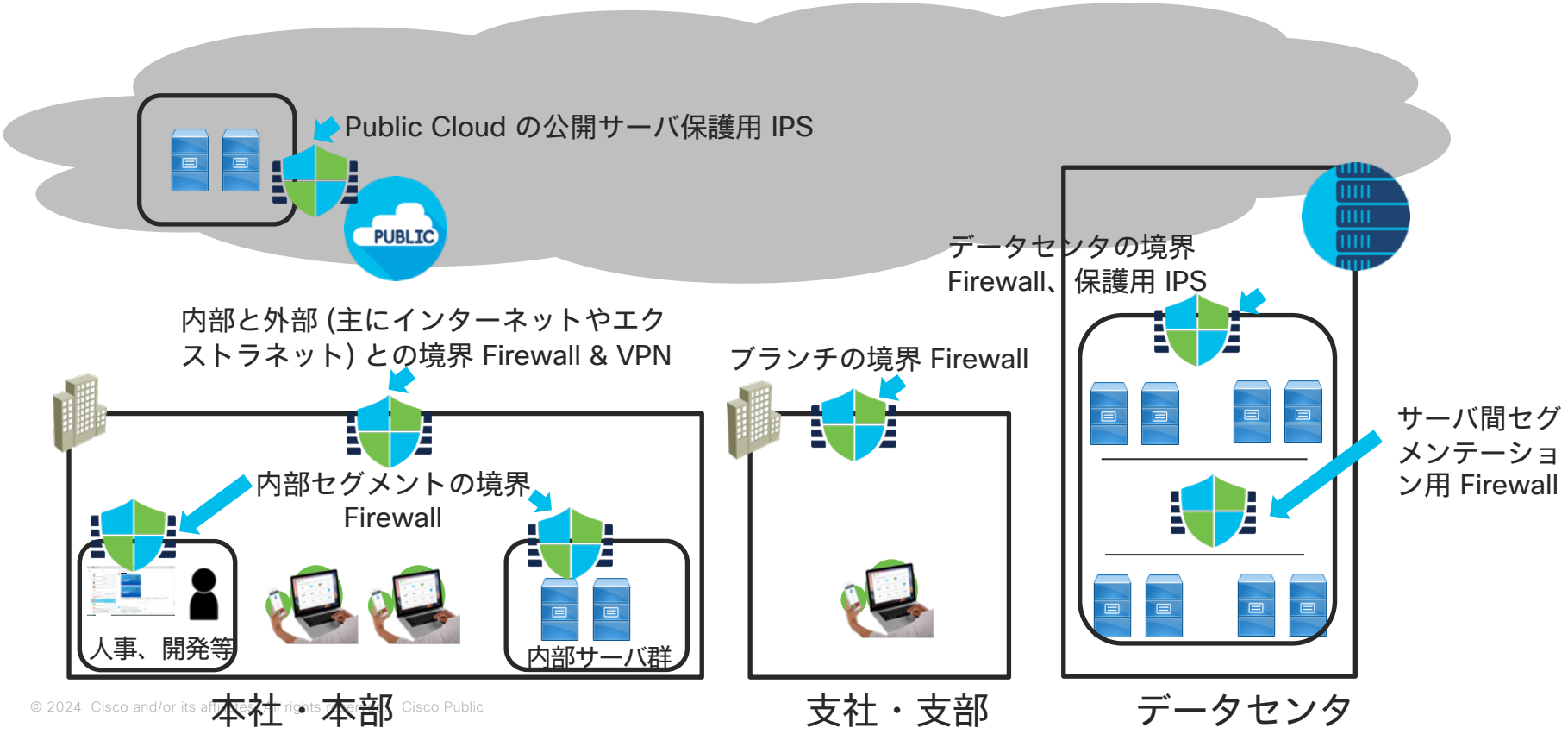
・「とりあえず動かすだけ」の IPS からの卒業。本当に必要な脅威対策を IPS で実施

- 自動チューニング
- インパクト解析
- ネットワークの可視化による状況把握
  - ネットワークとホスト学習
  - TLS 復号
  - Encrypted Visibility Engine
- Cisco Talos からの脅威情報を利用
  - Snort Rule
  - Security Intelligence

Endpoint だけでなく Network での Malware対策を実現

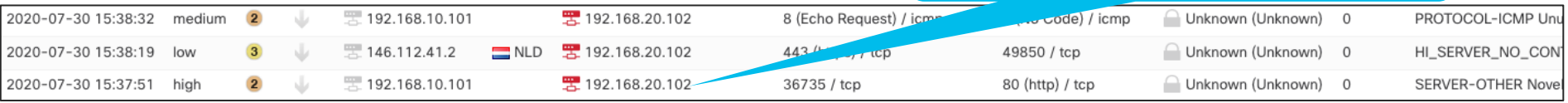
- Firewall で動く軽いエンジン
  - ファイルのハッシュ値による検知
  - ClamAV エンジン利用
- 時間の経過で Malware だとわかるファイルの特定
  - クラウドリコール
- 必要に応じてファイルそのものの振る舞いを確認
  - Threat Grid Sandbox

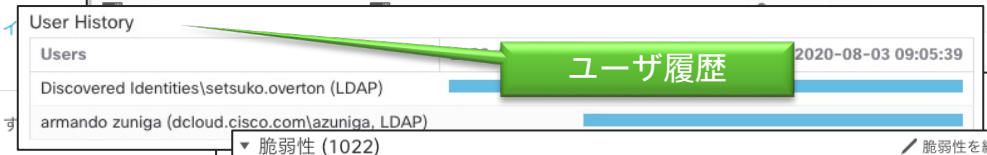
一般的なネットワーク構成図における FTD の位置付け

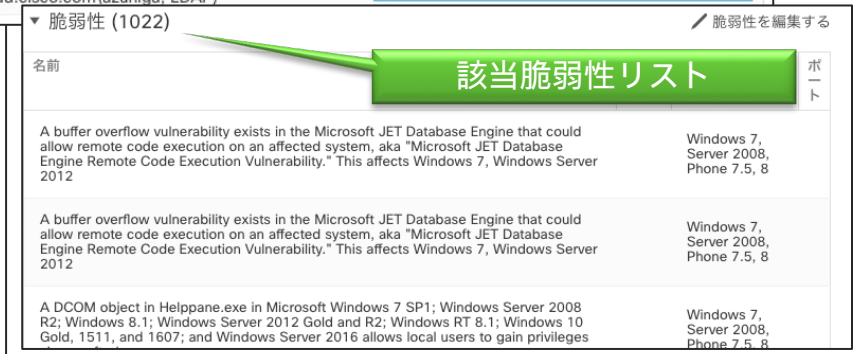


ホストプロファイルの例

例)アラートが発生したホストの情報を確認したい







クライアント アプリケーション

ユーザ履歴

侵入の痕跡

該当脆弱性リスト

端末 OS

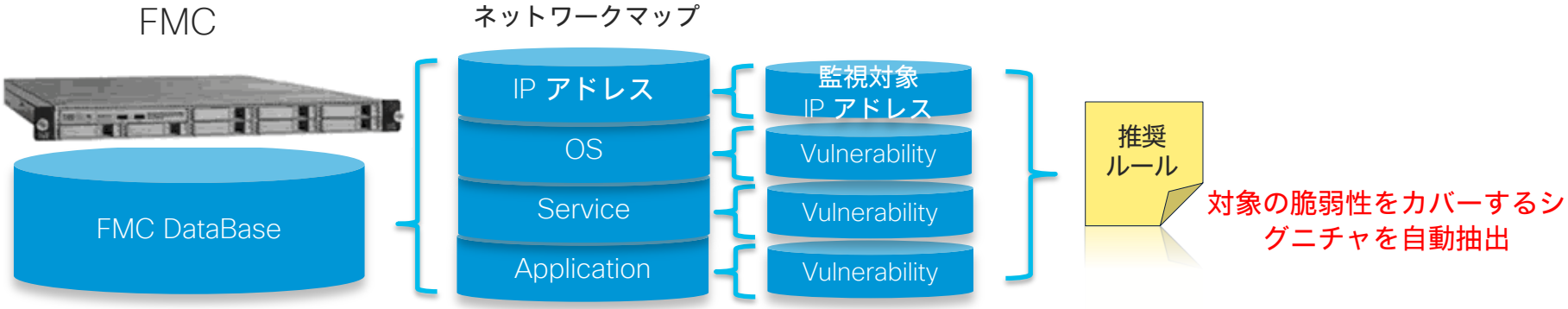
サーバ アプリケーション

✓ 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

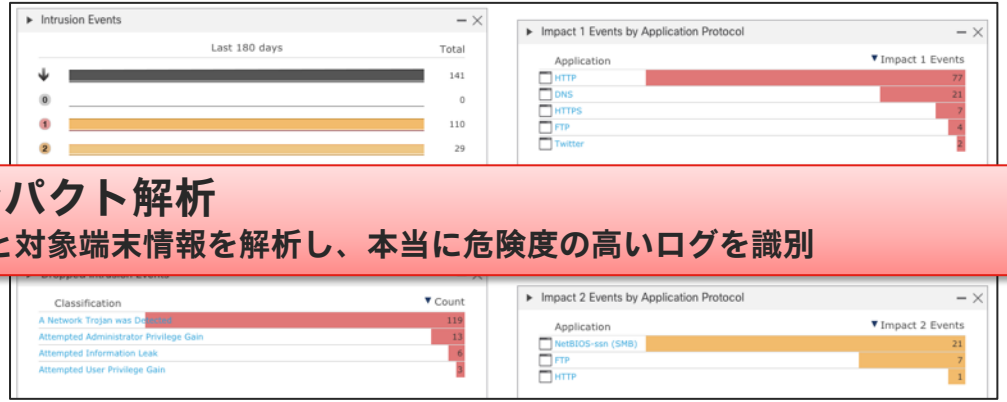
自動チューニング(推奨設定)とインパクト解析

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・・・

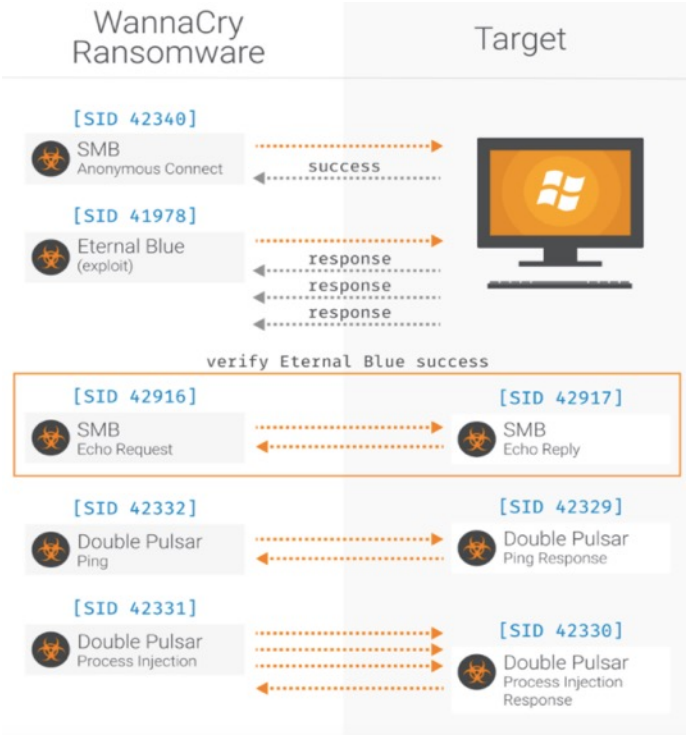
自動チューニング(推奨設定)
ネットワーク環境を学習し、
最適な推奨設定を自動生成



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 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

今後リリースされる新機能の多くは Snort 3 が必要

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		✔

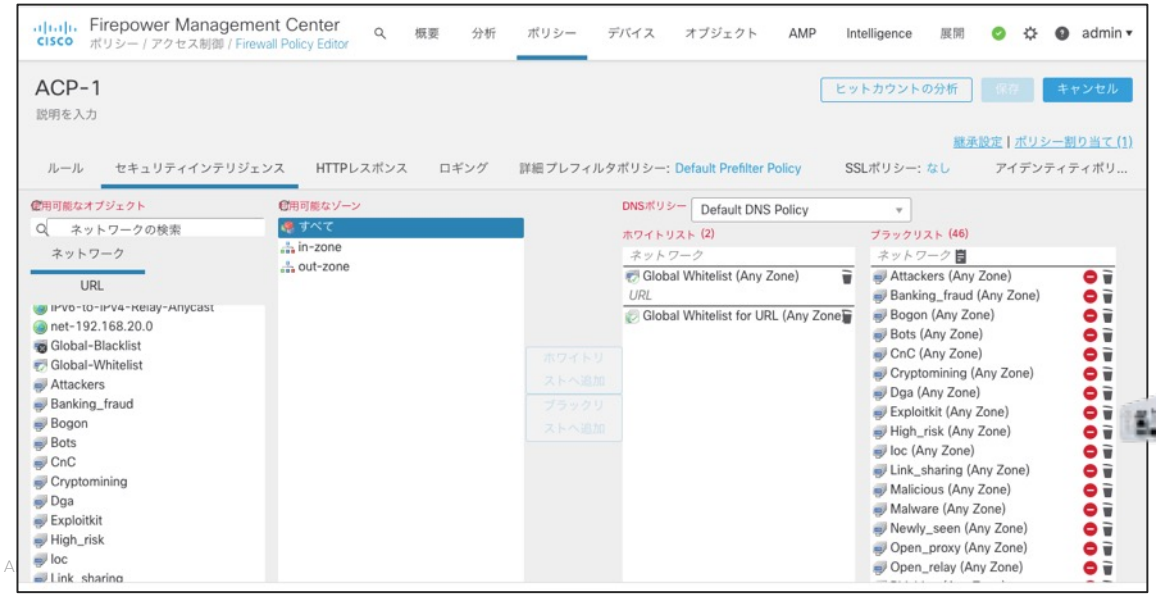
Snort 2 に比べて Snort Process Restart の必要なケースが大幅に減少
通常のポリシー設定や DB 更新においては Snort Process Restart が不要

Snort Process Restart が必要なケース一覧

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

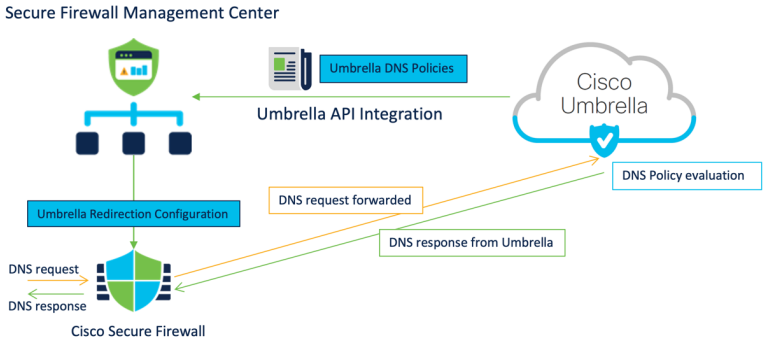
    など



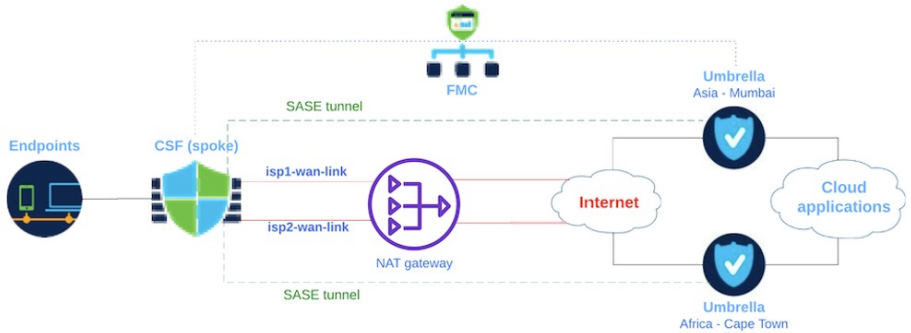
Umbrella とのインテグレーション

自動トンネルを使った SASE デプロイと共通の DNS セキュリティポリシー

- 全拠点での共通セキュリティポリシー
- 複数レイヤでの DNS セキュリティ
- 早い段階でのプロテクション
- インターネット接続の速度向上
- ハイブリッド勤務での共通セキュリティ



- SASE ユースケース
- Umbrella SIG – Cloud-delivered Firewall と連携
- FTD と Umbrella の間の接続と設定を自動化

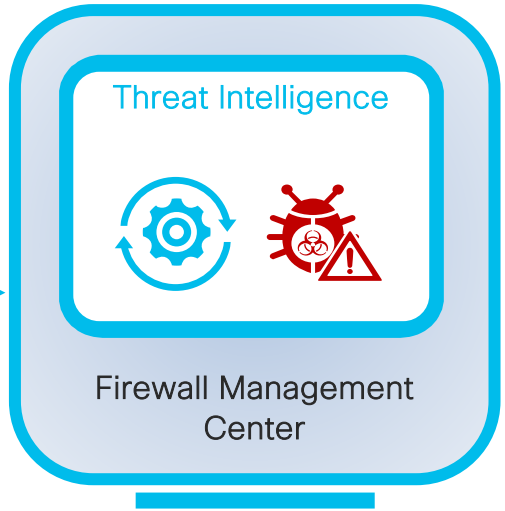


Threat Intelligence Director

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
- 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		Jul 24, 2018 6:18 AM EDT	Completed

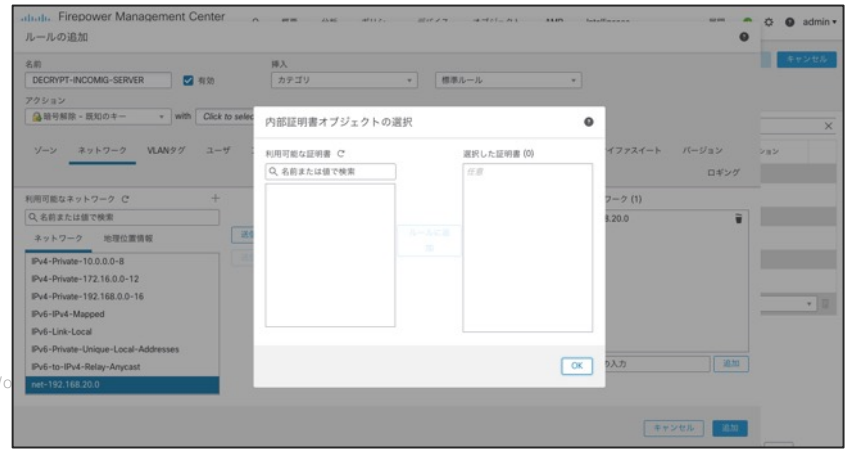
Block
Monitor

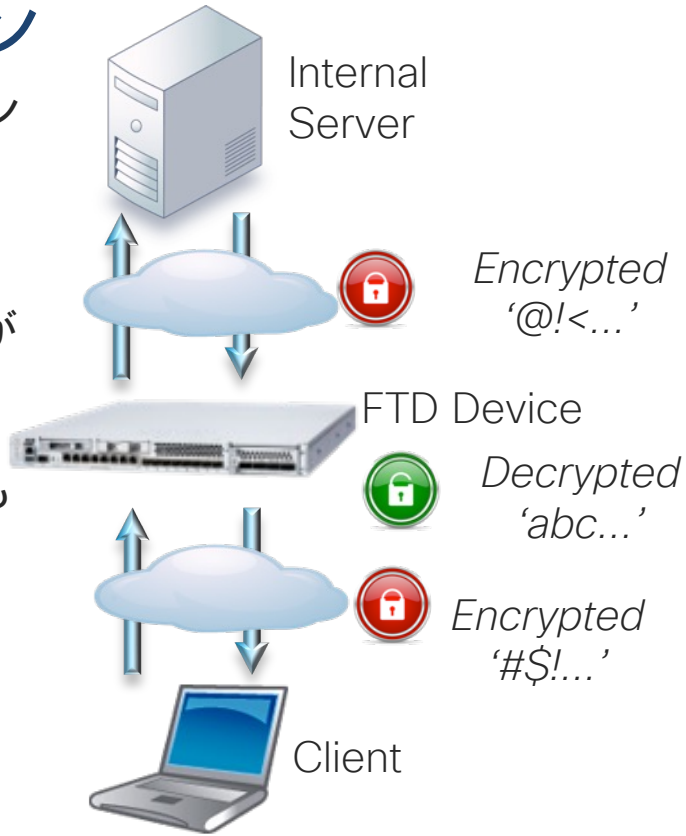
ジオロケーション

- 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

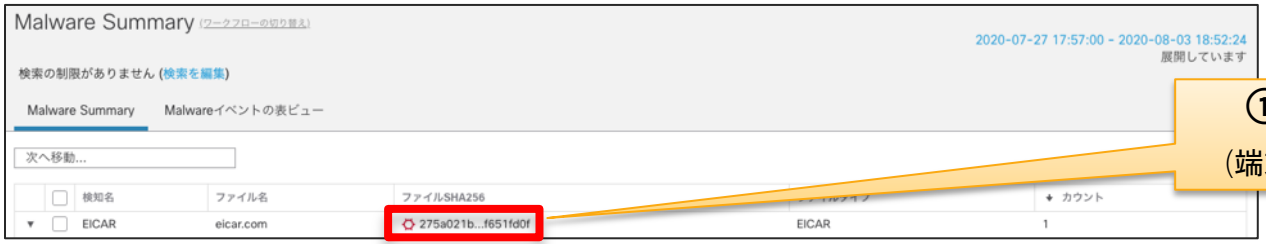
TLS 暗号化アクセラレーション

- 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 ネイティブにも Version 7.2 にて対応済み。TLS 1.2 にダウングレードしてのインスペクションも可能

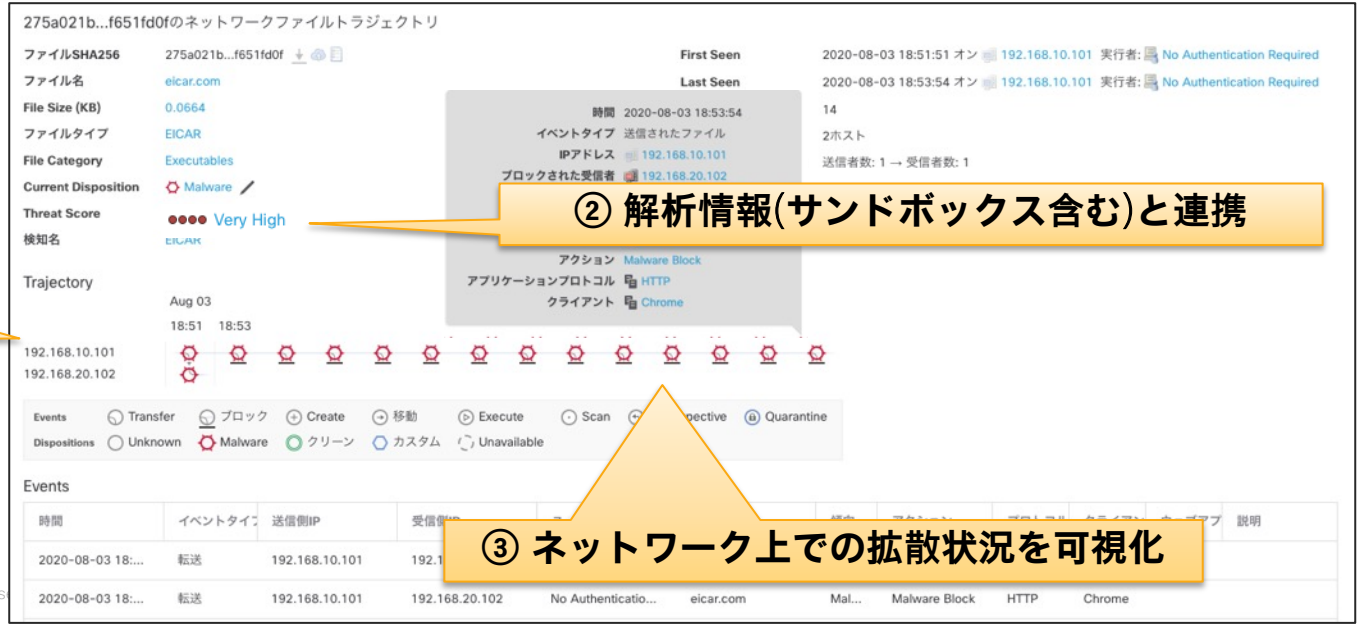




Malware Defense マルウェアの可視化と制御、トラッキング



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)



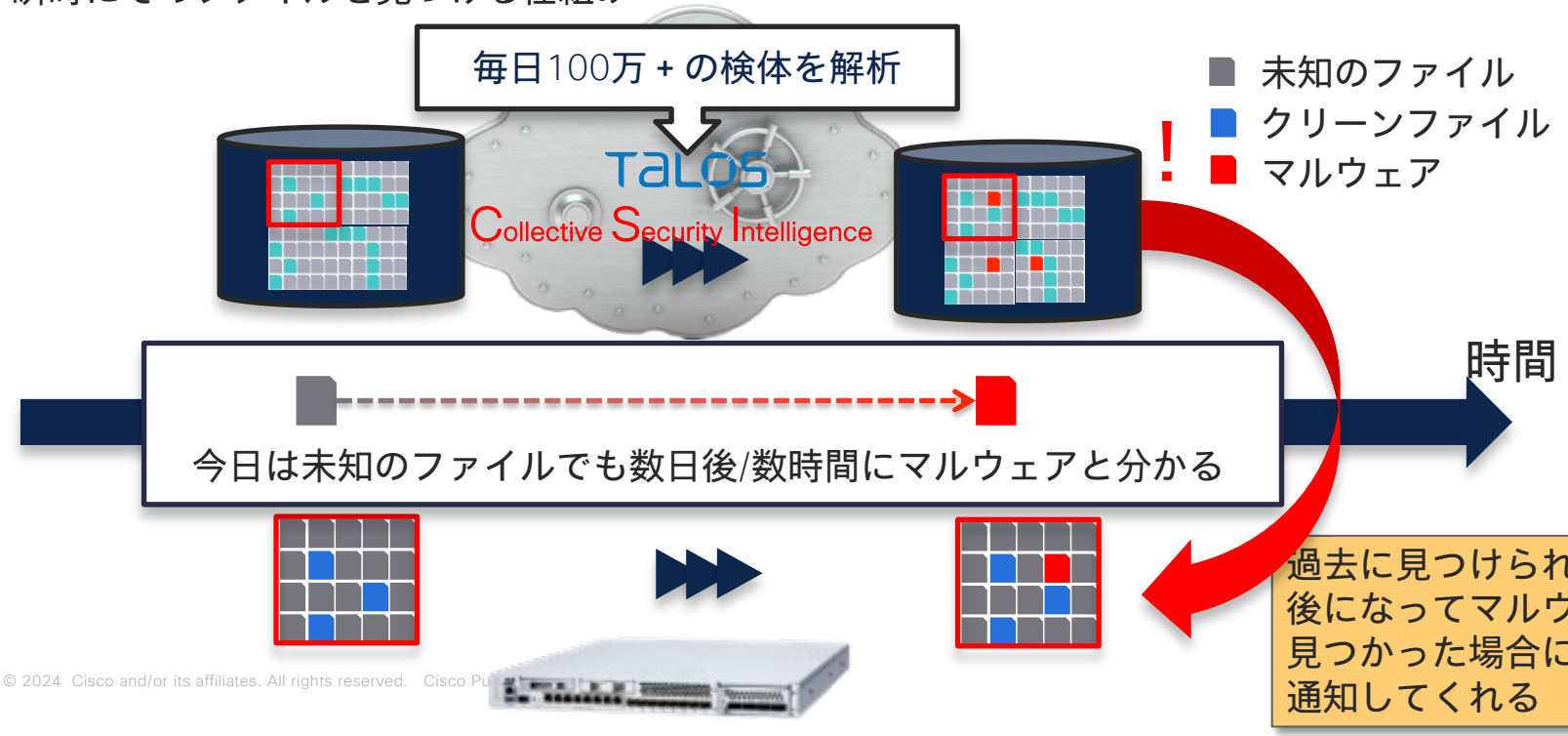
② 解析情報(サンドボックス含む)と連携

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

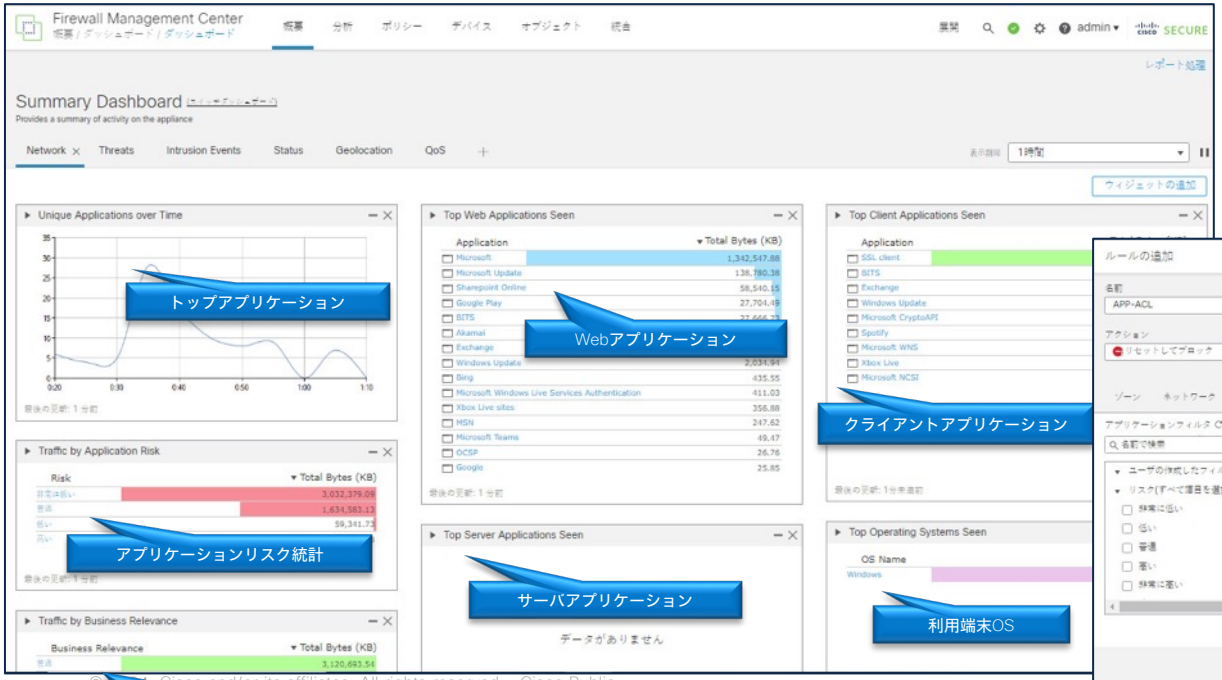
一度調査したファイルを覚えておき、合致するマルウェアが見つかった場合に
瞬時にそのファイルを見つける仕組み



クラウドリコールによるゼロデイマルウェア検知例

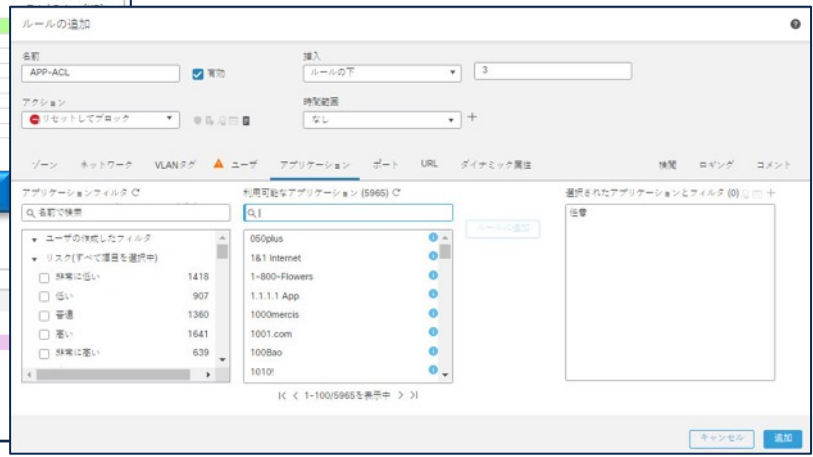
Application Visibility Control
アプリケーションの可視化と制御

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



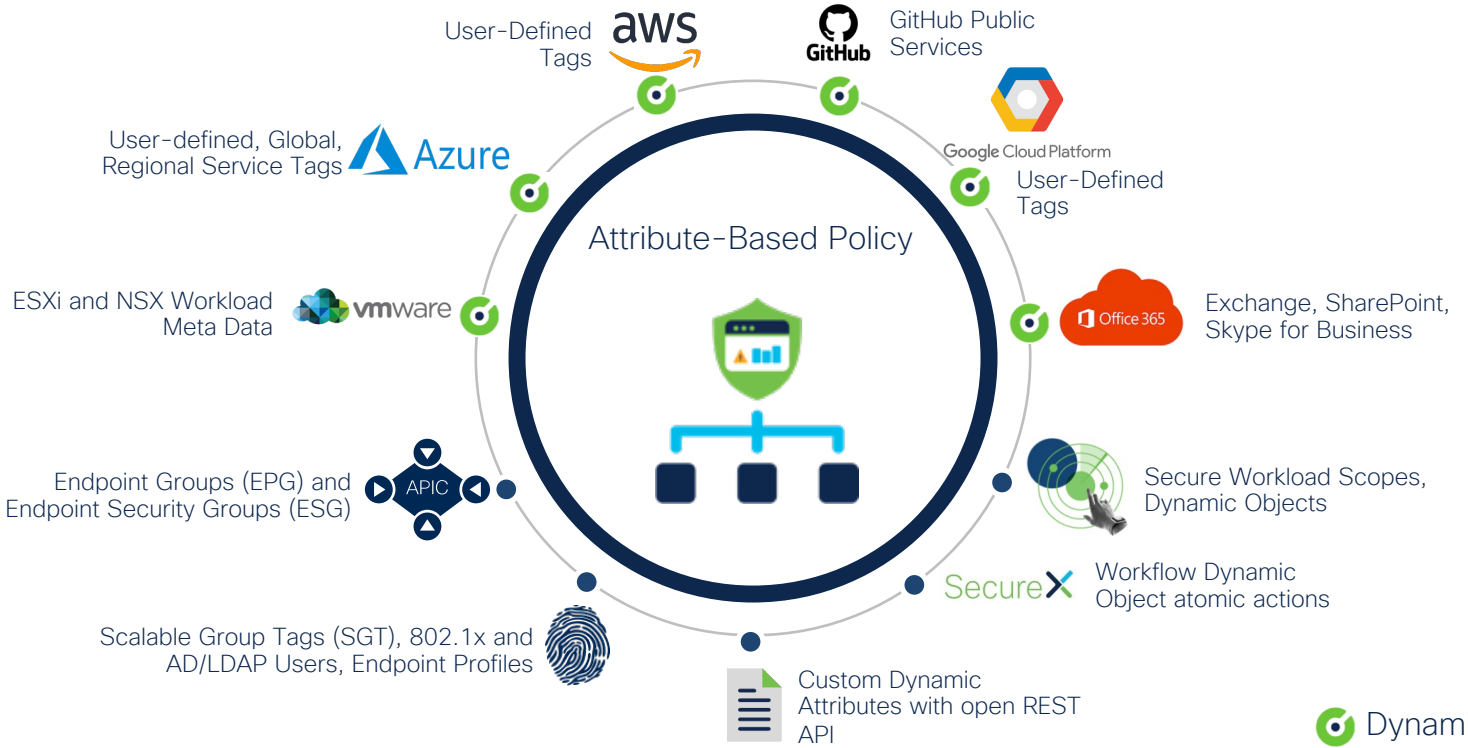
6,000 近くのアプリケーションから、利用状況をチェック

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/

Firewall Policy の抽象化



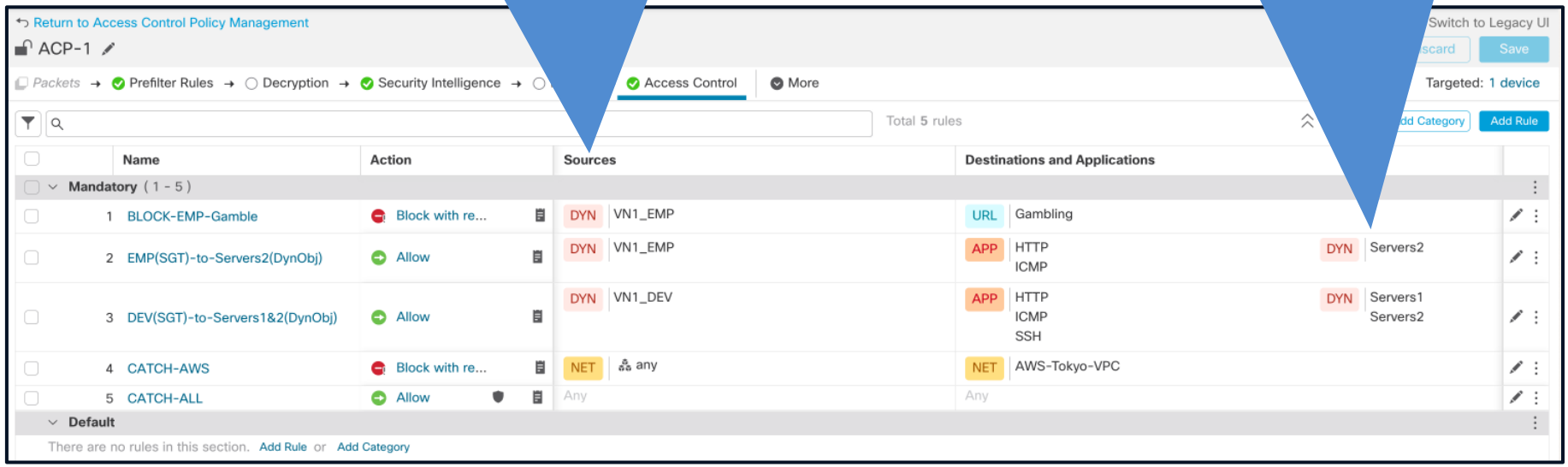
Dynamic Attribute Connector

Firewall Management Center

Firewall Policy 抽象化の例

Source にはユーザ認証情報で得た Security Group Tag を条件として指定
認証に応じて動的に変わるエンドポイントの端末の IP アドレスを指定する必要無し

Destination には Dynamic Attribute Connector を介して得た Public Cloud のインスタンス情報を条件として指定
静的に指定ができないインスタンスの IP アドレスを調べる必要無し



Firewall の Security Policy (FTD では Access Control Policy) において
IP アドレスが動的に変わる Source / Destination を抽象化して指定可能

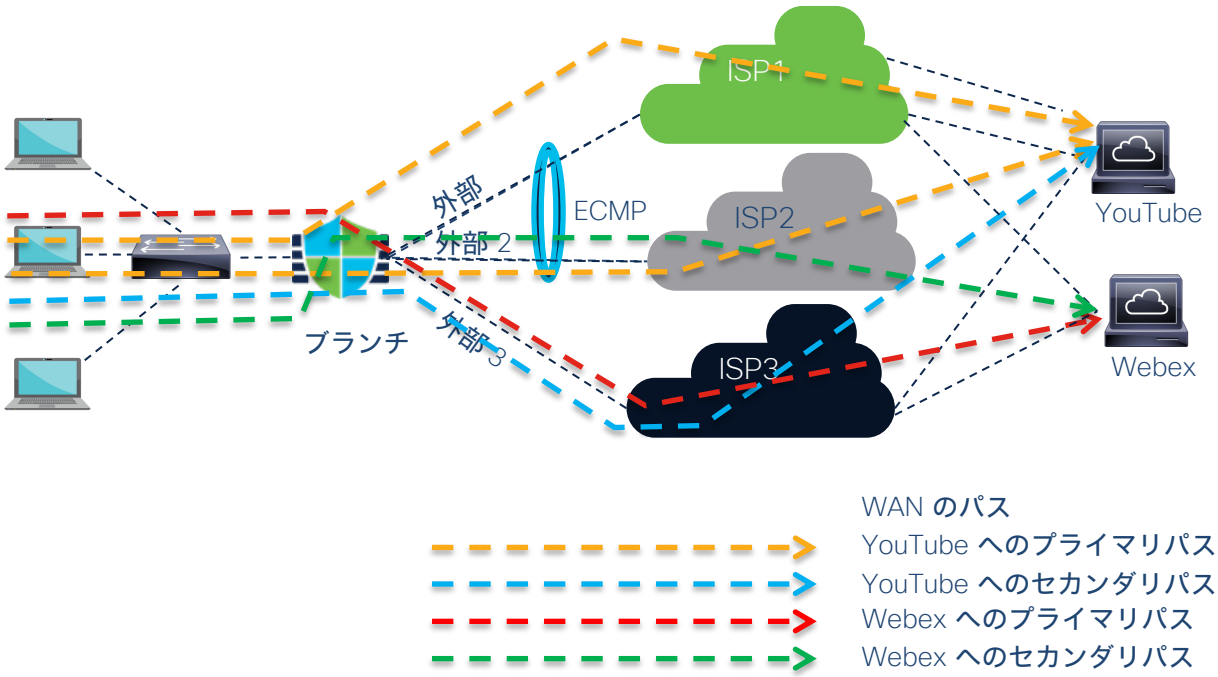
インテリジェントルーティング

展開シナリオ

- パスモニタリングを使用したアプリケーションベースまたはポリシーベースのルーティング
- リアルタイムメトリックを使用した動的パス選択

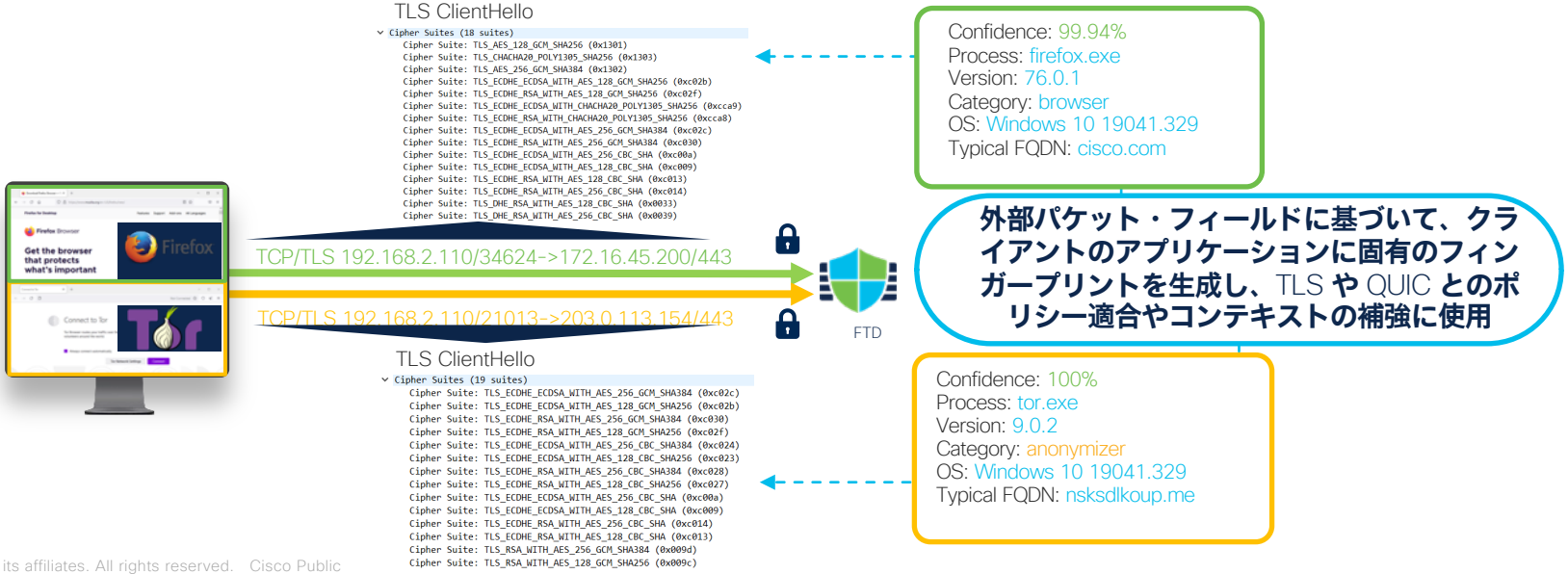
メリット

- インテリジェント アプリケーション ルーティング
- リアルタイムメトリックを使用した動的パス選択
- 手動による介入なしで保証される最良の出力パス
- リンクの正常性とネットワーク状態の継続的なモニタリング
- 複数の属性に基づく出力インターフェイスの選択



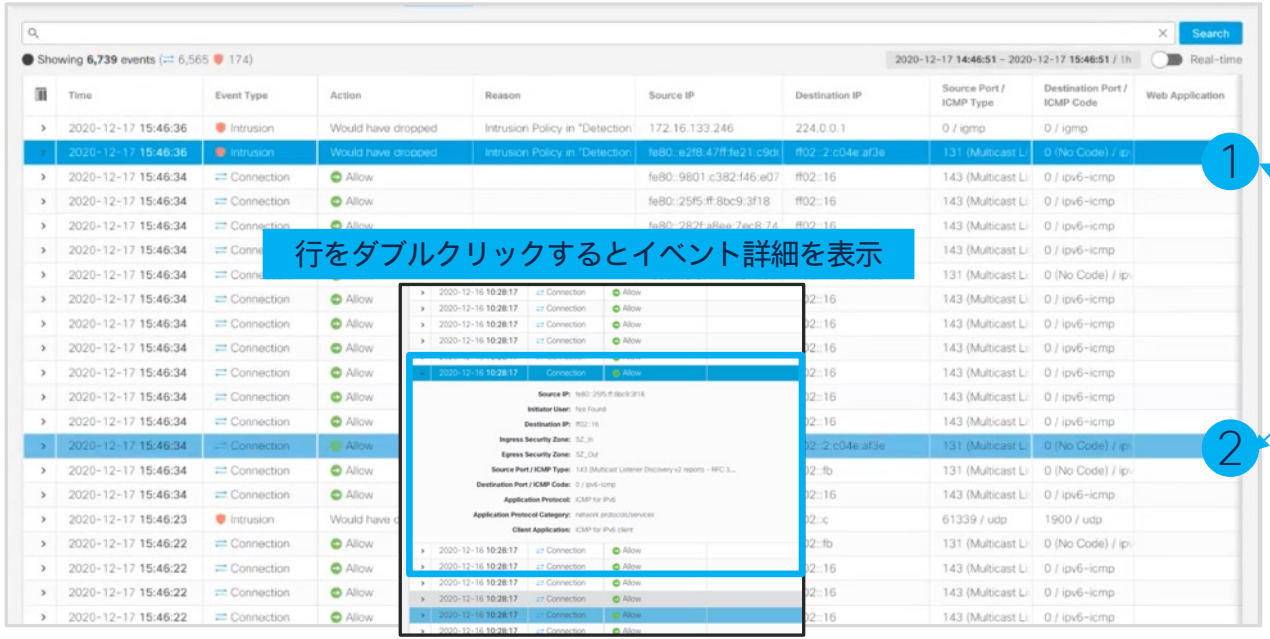
Encrypted Visibility Engine

- 暗号化通信の OS や アプリケーション、リスクを、復号せずに高精度で特定
- 検知には、Talos が作成した VDB に含まれたフィンガープリントを利用
- リスクのレベルに応じて通信のブロックも可能



Unified Event Viewer

- Unified Event 画面は複数種別のイベントを一つのビューで参照できるイベント調査画面
- 例えばマルウェアイベントと IPS イベントの関連性調査や、通信ログのリアルタイムな効果確認において有用なビュー



真の相関分析
Intrusion Event を選択すると、関連する Connection Event もハイライトされる

FMC での VPN ダッシュボード

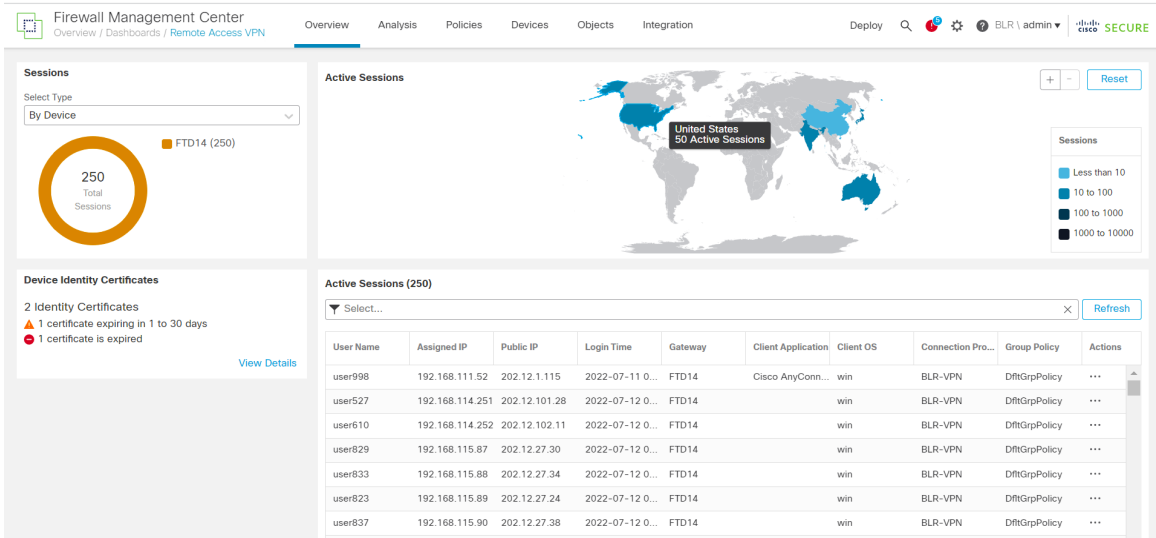
アプリケーション認識型ファイアウォールポリシーの適用、パスの選択、および復号

展開シナリオ

- 中規模から大規模の VPN 展開ベース
- ユーザーアクティビティとセッションの詳細をモニタリング
- キャパシティプランニングと可用性統計情報

メリット

- 統合ダッシュボード
- ユーザーの地理位置情報
- 展開ベース（一般的なワークステーション OS プラットフォームなど）の分析
- アップグレードの計画/トラブルシューティングのために、1 つまたはすべての VPN セッションを終了



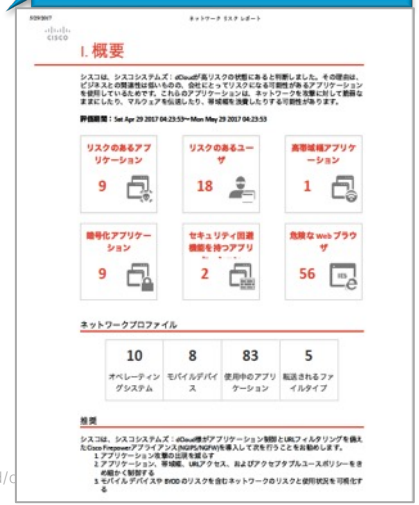
Custom Report レポート機能

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

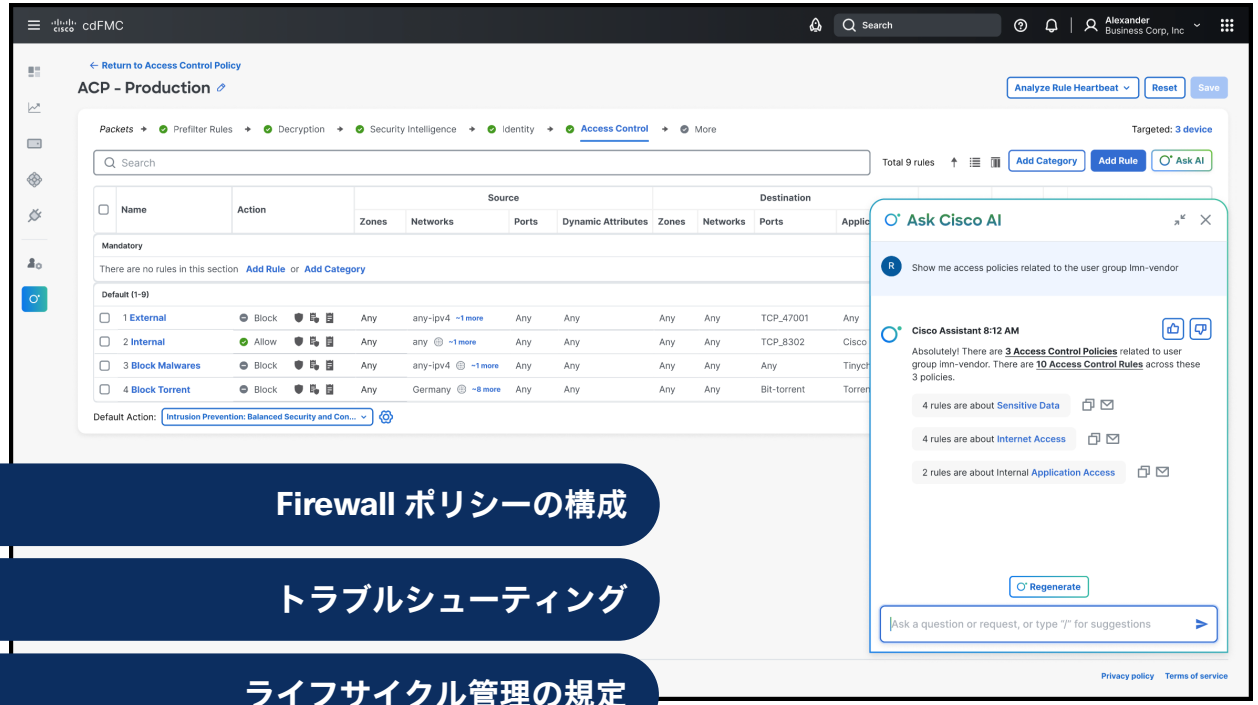
ネットワークレポート



アタックレポート

マルウェアレポート

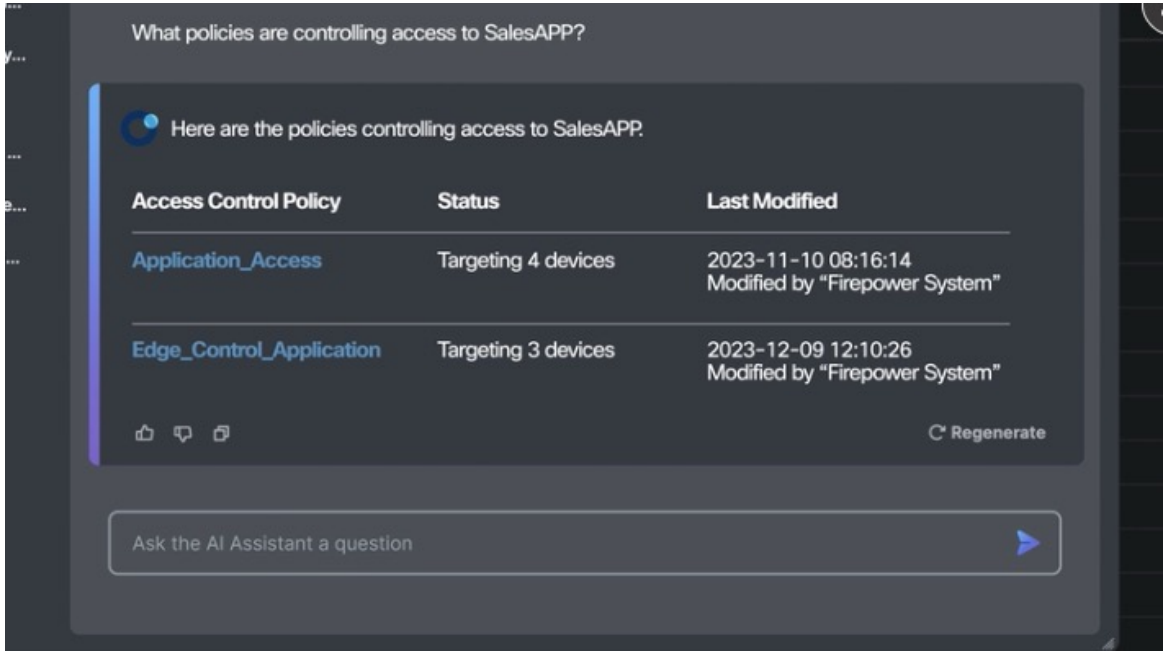
Cisco AI Assistant for Security



- Assist ＋ Firewall ポリシーの構成
- Augment ＋ トラブルシューティング
- Automate ＋ ライフサイクル管理の規定

AI Assistant を使った Firewall ポリシー管理デモ

https://www.cisco.com/c/en/us/products/security/artificial-intelligence-ai.html?socialshare=lightbox-security-ai

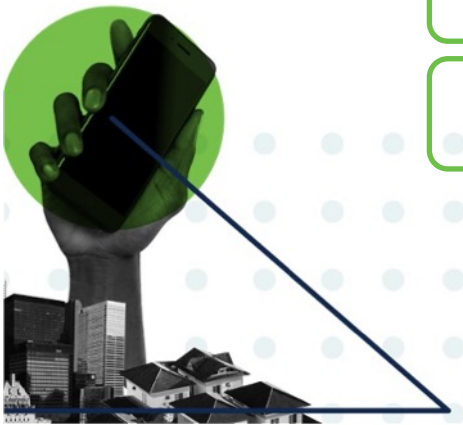


Cloud Delivered FMC にて近日サポート開始

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) On Premise 概要

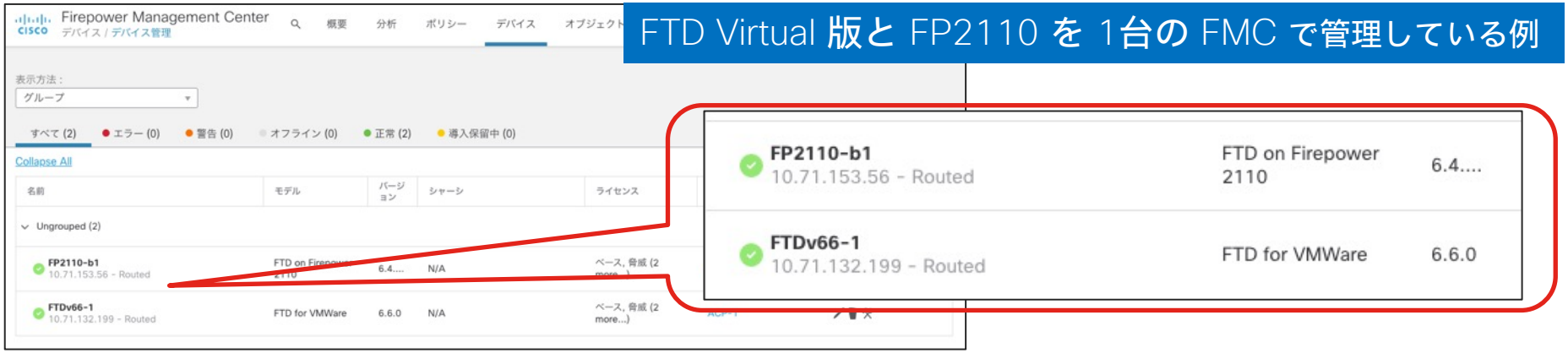
- FTD デバイスをまとめて管理
- Access Control Policy 等、各 Policy を共有可能

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

FTD

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

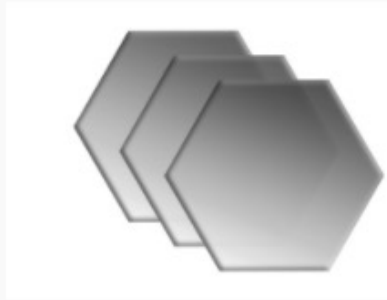


Firewall Management Center (On Premise)
プラットホーム一覧

FMC1700
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

FMC2700
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

FMC4700
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

Cloud Delivered Firewall Management Center

CDO (Cisco Defense Orchestrator) にて Cloud Delivered FMC が登場

FMC を On Premise で別途構築せずにクラウドから利用可能

変更管理と更新のオーバーヘッドを排除

テナント毎に25%以上の Firewall をサポート

ラックスペースと光熱費が不要となり、オペレーションコストを削減

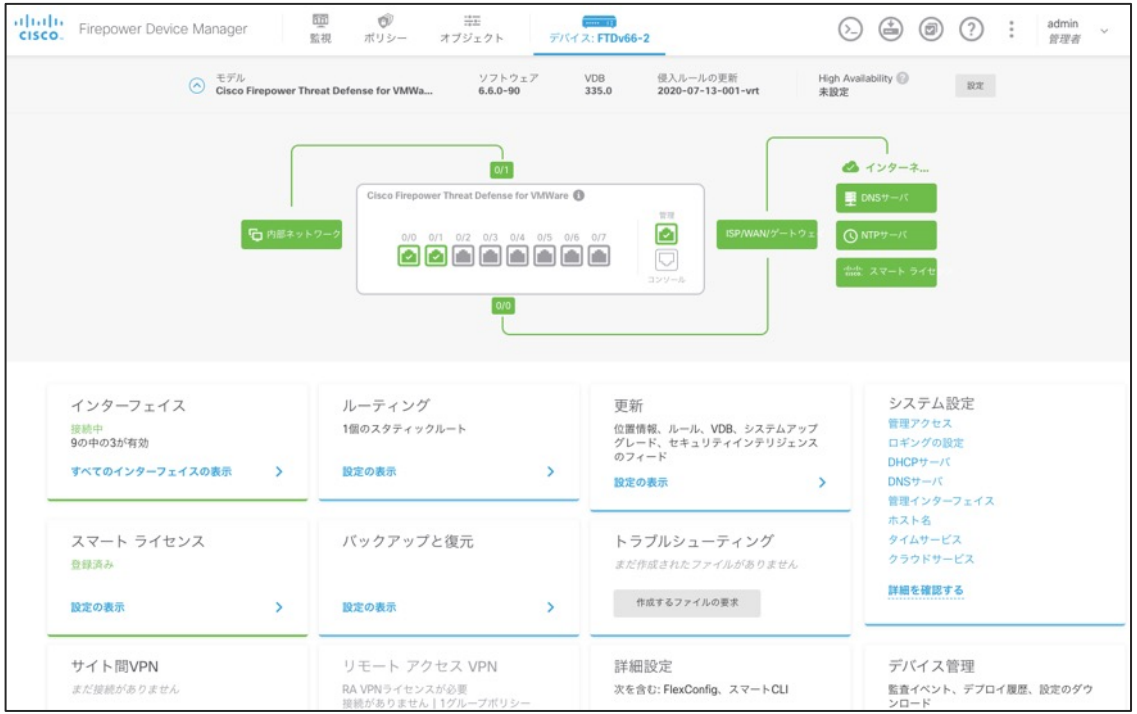
シスコがアップタイムを確保し、柔軟性を向上

既存の操作性と変わらず、既存利用者が新たに操作方法を覚える必要無し

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 (On Premise)

FTD デバイスを On Premise で設定・管理するには以下のどちらかが必要。
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 (On Premise) 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

* FTD 側は Data Interface で管理することも可能

共存不可

FDM 管理

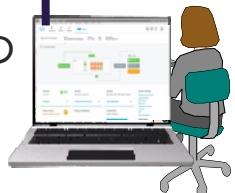
基本的なセキュリティポリシーを、シンプルに1つの FTD に対して実施

FTD 本体

https
ブラウザで管理・設定

FDM
= Firewall Device Manager

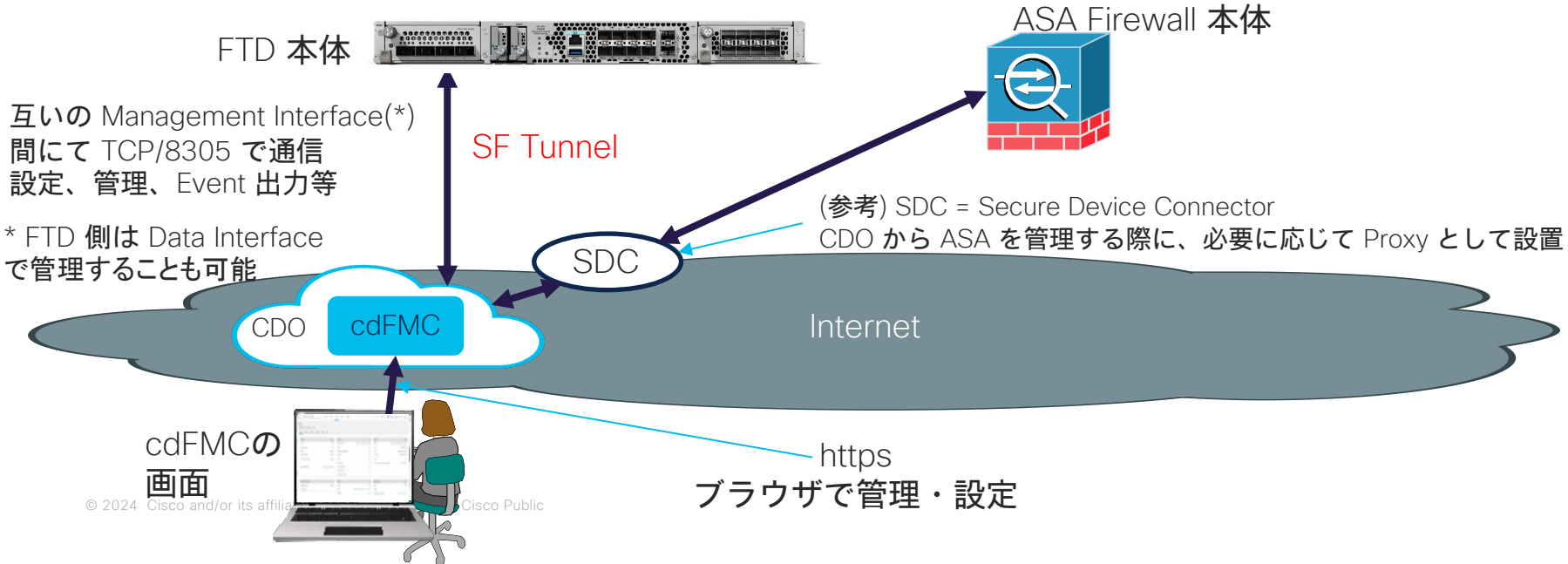
FDMの画面



FTD の管理・設定アーキテクチャ (Cloud)

FTD デバイスを Cloud から設定・管理するには CDO (Cisco Defense Orchestrator) に含まれる Cloud Delivered FMC (cdFMC) を利用する。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

Cloud Delivered FMC (cdFMC) 管理
On Premise FMC と同様の UI や多くの同様の機能を提供 (ホスト学習や自動チューニングは近日対応予定)
On Premise FMC を Event 出力先として同時利用可能



Cisco Firewall プラットホーム

FTD / ASA どちらも利用可能

Private Cloud

HyperFlex
vmware ESXi
NUTANIX
KVM
openstack

Public Cloud

aws
Google Cloud Platform
Microsoft Azure
rackspace technology
EQUINIX
ORACLE CLOUD INFRASTRUCTURE
Alibaba Cloud
alkira

Hardware


FPR 1010


FPR 1120/40/50


FPR2110/20/30/40


FPR 3105/10/20/30/40


FPR 4112/15/25/45

NEW!


FPR 4215/25/45


FPR 9300 Series SM-40/48/56

Small & Home Offices / Small Branch Deployments

Small Enterprises / Branch Deployments

Mid and Large Enterprises / Campus Deployments

Datacenter / Service Providers

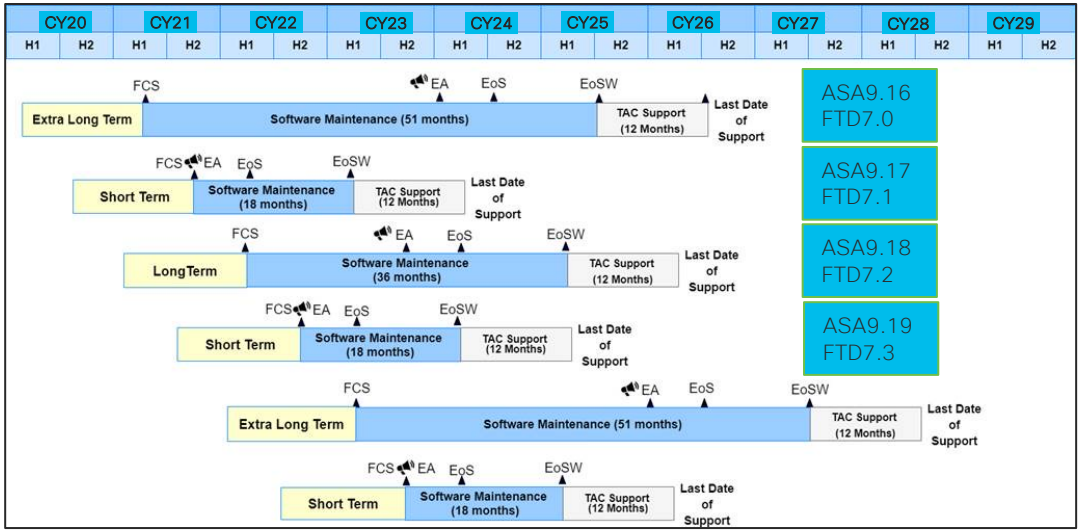
機種選定のポイント (2024年1月現在)

- Firewall 2100 シリーズは、製品寿命を考えると、1140/50 か 3100 シリーズを選定することを推奨
- Firewall 9300 シリーズは、製品寿命とコストパフォーマンスを考えると、4200 シリーズを選定した方が良い場合が多い

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

- 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 7.3 → ショートタームサポート
  - FTD 7.2 → ロングタームサポート
- ロングタームサポートの中でも、2年に1度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 エクストラロングタームサポート



FTD & ASA 推奨ソフトウェアバージョン

- 2024年1月時点で一般的な推奨バージョンは FTD 7.2.5 / ASA 9.18.3 系
- 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

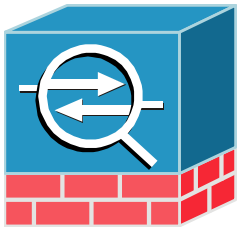
安定度の面からも、既存 FTD 環境の
Version 7.2.5 への VersionUP を強く推奨

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
  - 20年目のロングセラー

  (PIX まで遡ると30年)



- AnyConnect の特長
  - Cisco Secure Client としてリブランディング
  - 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, Umbrella, Secure Endpoint)
  - 18年目のロングセラー

  (Cisco VPN Client まで遡ると24年)

NEW!

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 (ルータの方が高機能)	○	○
IPS / IDS	X	◎
AVC, URL Filter, SSL / TLS 復号	X	◎
Malware 対策	X	◎
CLI での設定	◎	X
コストパフォーマンス	◎	○

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

当資料は以降 FTD にフォーカス

Secure Firewall 4200 Overview

ソフトウェアは FTD と ASA の選択が可能

FTD および ASA ソフトウェア用の 1RU アプライアンスモードのセキュリティプラットホーム

- 固定構成の3つのモデル: 4215, 4225, 4245
- **マルチインスタンス**およびクラスタリングが可能な軽量型仮想スーパーバイザモジュール
- Flow Offload や Crypto Engine の機能を持つ、データパスに組み込まれた FPGA
- 背面には二重化電源および3つのファントレイを搭載

1RU

SFP Data Interfaces

- 8x1/10/25GE/50GE

NVMe Drives

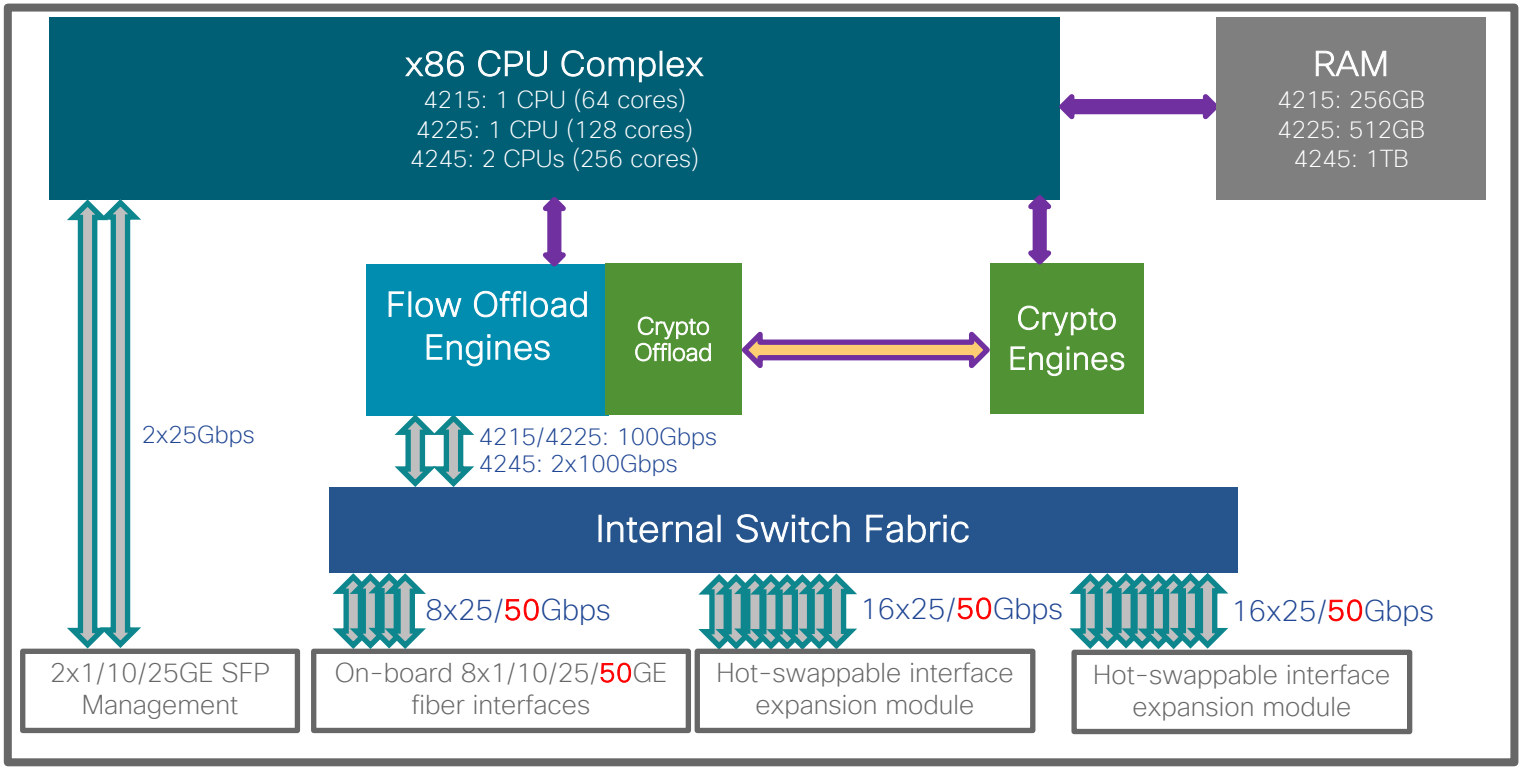
- Up to 2x900GB in RAID1 on 4215/4225
- Up to 2x1.8TB in RAID1 on 4245

Expansion Network Modules

- Standard: 8x1/10GE, 8x1/10/25/50GE, 4x10/40GE, 2x100GE, 4x40/100/200GE, 2x200/400GE SFP+
- Fail-to-Wire: 8x1GE Copper; 6x10GE or 6x25GE SFP+ (SR and LR variants)

赤字は将来対応予定

Secure Firewall 4200 Architecture



Secure Firewall 4200 パフォーマンス

Metric	4215	4225	4245
Throughput* FW+AVC+IPS	65 Gbps	85 Gbps	145 Gbps
Throughput* IPsec VPN (Fastpath)	50 Gbps	85 Gbps	145 Gbps
Maximum number of VPN peers	20000	25000	30000
Maximum concurrent connections with AVC	15 M	30 M	60 M
Maximum new connections per second (ASA code)	1.5 M	1.8 M	2.1 M

* 1024 Bytes のパケットでの数値

Secure Firewall 3100 Overview

FTD および ASA ソフトウェア用のアプライアンスモードのセキュリティプラットホーム

- **固定構成の5つのモデル**: 3105, 3110, 3120, 3130, 3140
- **マルチインスタンス*** **およびクラスタリングが可能な**

軽量型仮想スーパーバイザモジュール

- Flow Offload **や** Crypto Engine **の機能を持つ、データパスに**

組み込まれた FPGA

- **背面には二重化された電源およびファントレイを搭載**

SFP Data Interfaces

- 8x1/10GE on Firewall 3105-3120
- 8x1/10/25GE on Firewall 3130-3140

1RU

Copper Data Interfaces

- 8x10M/100M/1GE Ethernet

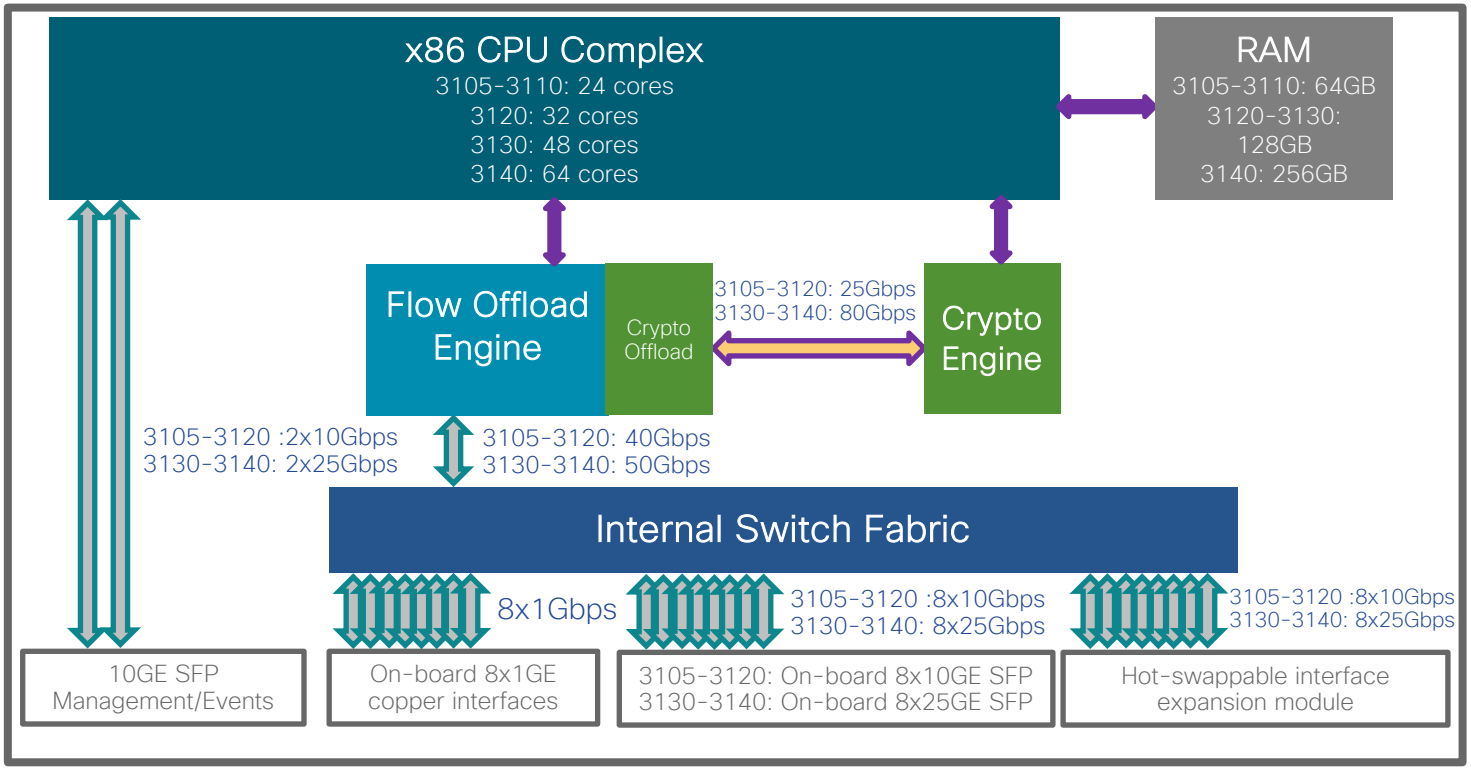
Network Module

- 8x1/10/25GE or 6x10/25GE FTW on Firewall 3105-3120
- 4x40GE or 2x40GE FTW on Firewall 3130-3140

ソフトウェアは FTD **と** ASA **の選択が可能**

* **マルチインスタンスは** Firewall 3105 **は未サポート**

Secure Firewall 3100 Architecture



Secure Firewall 3100 パフォーマンス

Metric	3105	3110	3120	3130	3140
Throughput* FW+AVC+IPS	10 Gbps	17 Gbps	21 Gbps	38 Gbps	45 Gbps
Throughput* IPsec VPN (Fastpath)	5.5 Gbps	8 Gbps	10 Gbps	17.8 Gbps	22.4 Gbps
Maximum number of VPN peers	2,000	3,000	6,000	15,000	20,000
Maximum concurrent connections with AVC	1.5 M	2 M	4 M	6 M	10 M
Maximum new connections per second (ASA code)	150,000	300,000	500,000	875,000	1,100,000

* ステートフルインスペクションのパケットサイズは 1024 Bytes

ソフトウェアは FTD と ASA の選択が可能

Firepower 1000 シリーズ

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

FTD ライセンスの概要

FTD はスマートライセンス必須

Airgap 環境では License Reservation or Cisco Smart Software Manager On-Prem を利用

最低限必要なライセンスは?

FTD デバイス毎に必要な機能が含まれる 1,3,5年のサブスクリプションライセンス

冗長構成ではどの FTD デバイスにもライセンスが必要。2台目のサブスクリプションは半額になるバンドル型番有り

管理方法による追加費用

- On Premise FMC → FMC そのものの購入が必要
- cdFMC / CDO → CDO でのサブスクリプションライセンスとデバイスライセンスが必要
- FDM → 購入不要

ライセンスの管理を行うデバイス・システムは？

On Premise FMC で管理時は FMC でまとめてライセンスを管理、それ以外は 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)

FTD デバイスに必要な機能のライセンス一覧

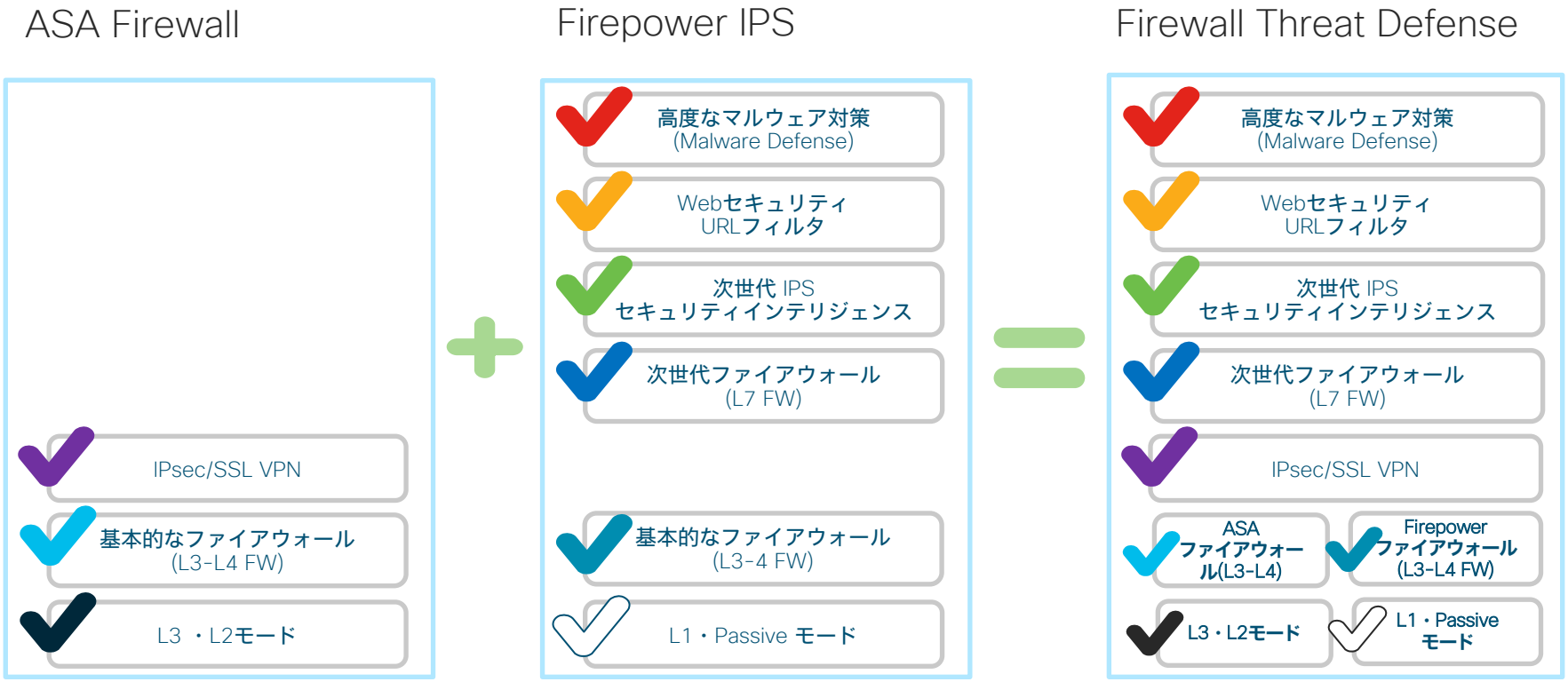
- Base (FTDv のみモデル毎に 1,3,5年のサブスクリプション、Firepower アプライアンスは無償)
  AVC, Basic Firewall, Routing & Switching
- Threat (モデル毎に1,3,5年のサブスクリプション) ライセンス型番は T
  IPS / IDS, Security Intelligence, Encrypted Visibility Engine
- Malware (モデル毎に1,3,5年のサブスクリプション) ライセンス型番は M or AMP
  Malware Defense, Threat Grid (Dynamic File Analysis), ファイル保存
- URL Filtering (モデル毎に1,3,5年のサブスクリプション)ライセンス型番は C or URL
  カテゴリ、reputation
- Secure Client (旧 AnyConnect)
  サイト単位で Premier (旧 Apex) or Advantage (旧 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
  評価には Smart License が必要 (初期の 90日間評価ライセンスには含まれない)

FTD デバイス管理に必要なライセンス一覧

- FDM で直接管理
  - 追加ライセンス不要
- On Premise FMC で管理
  - FMC Appliance → ライセンス不要 (FMC Appliance の購入が必要)
  - FMC Virtual → 管理デバイス数 (2,10,25,300) 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)
- CDO (cdFMC) からの管理
  - テナントごとの Base License を 1,3,5年のサブスクリプションライセンスで購入
  - 管理する FTD の数をデバイスのモデル別にそれぞれ 1,3,5年のサブスクリプションライセンスで購入
  - 詳細はオーダーガイド参照

Firewall Threat Defense のアーキテクチャ

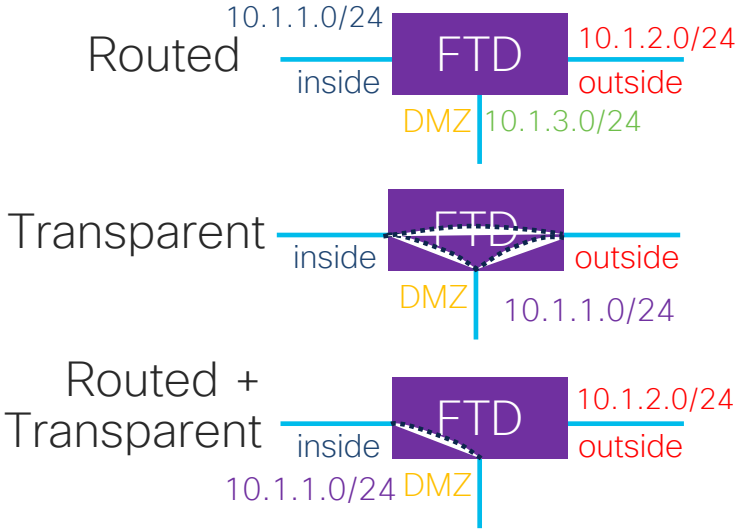
ASA FW, Firepower IPS, FTD の関係性



FTD インターフェースモード

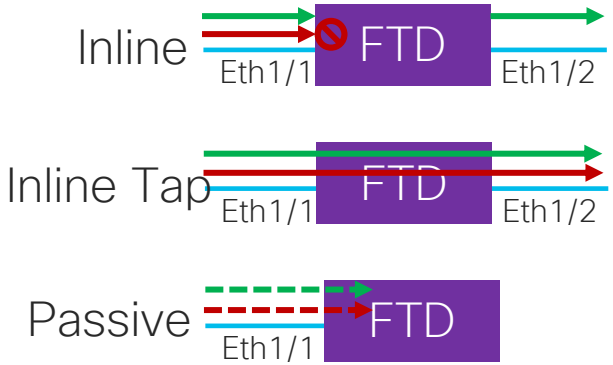
NGFW

ASAから継承



Firepowerから継承

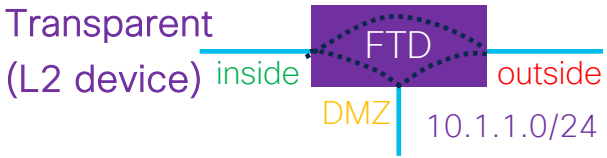
NGIPS



※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

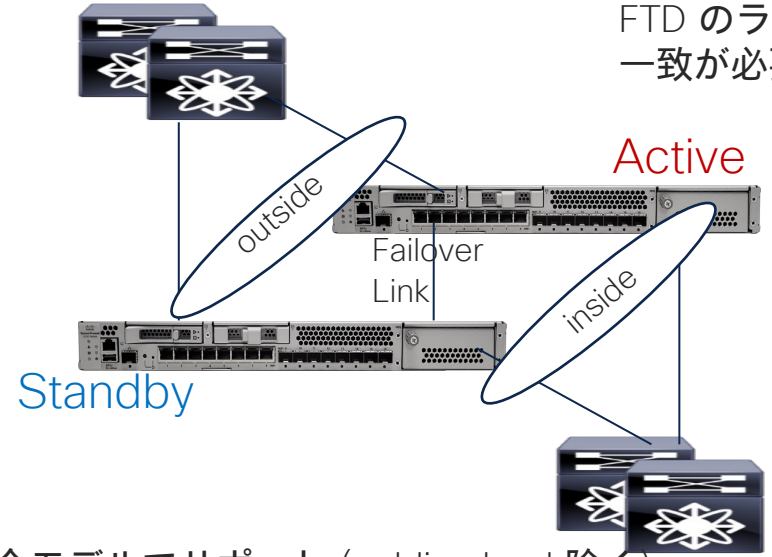
- Routed / Transparent Firewall にて未使用のインターフェイスは NGIPS モードのインターフェイスとして利用可能

- 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

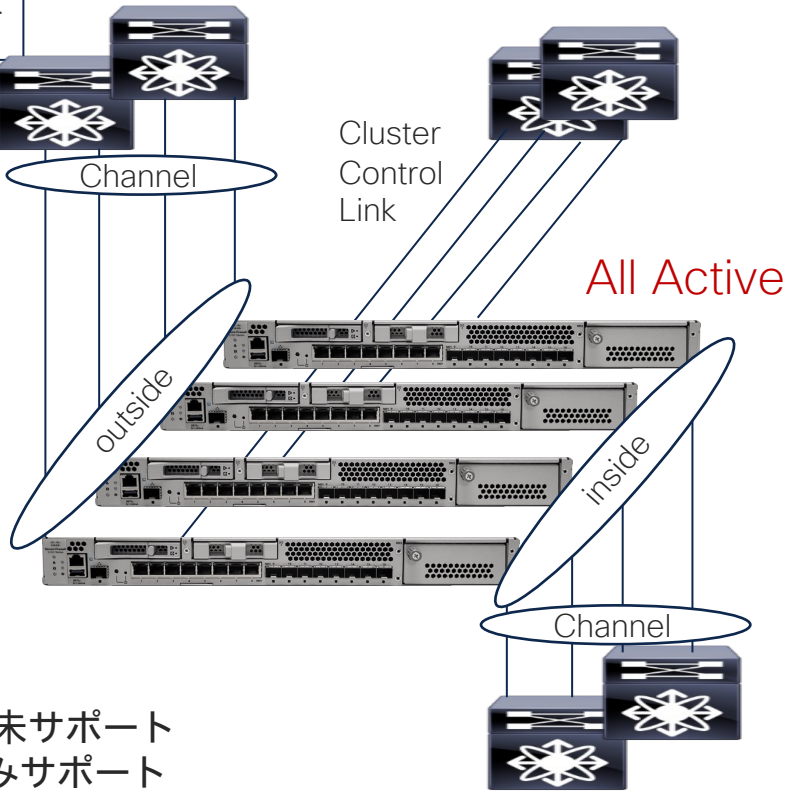
Active - Standby



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

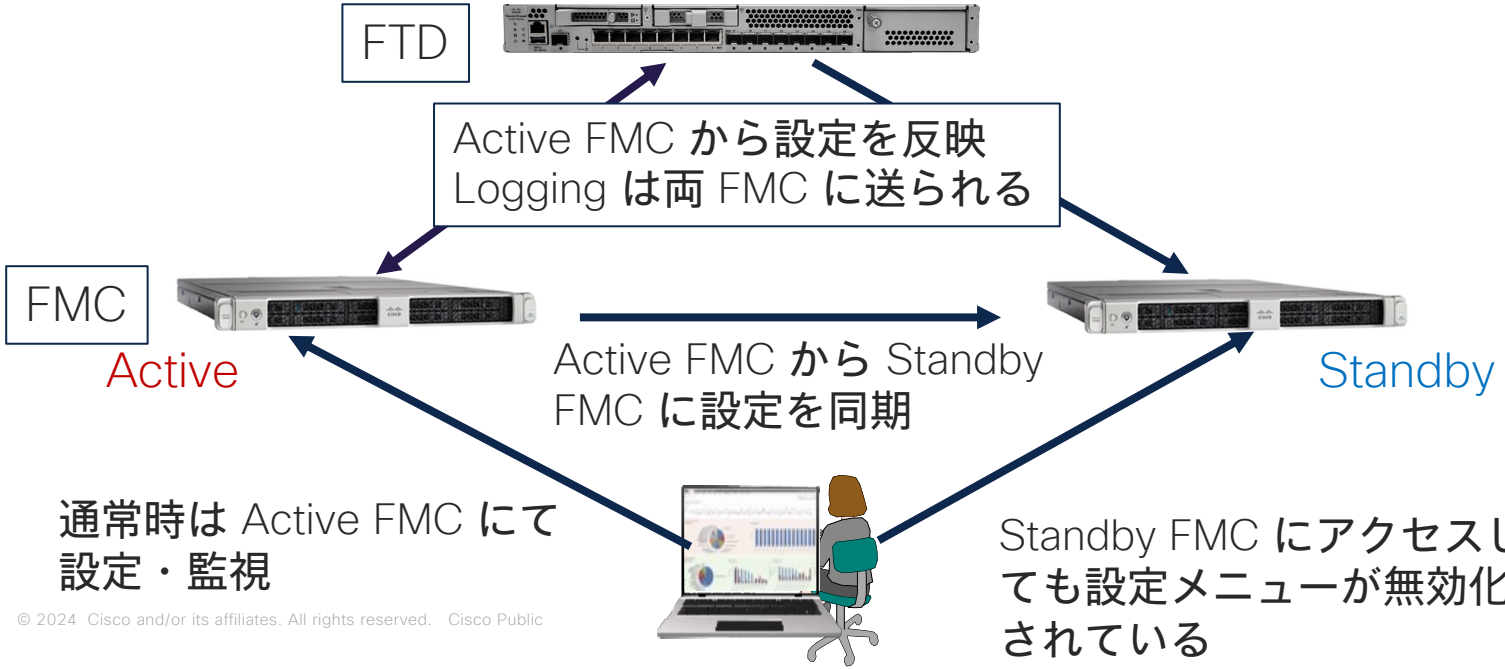
Cluster



FPR1k/2k は未サポート
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

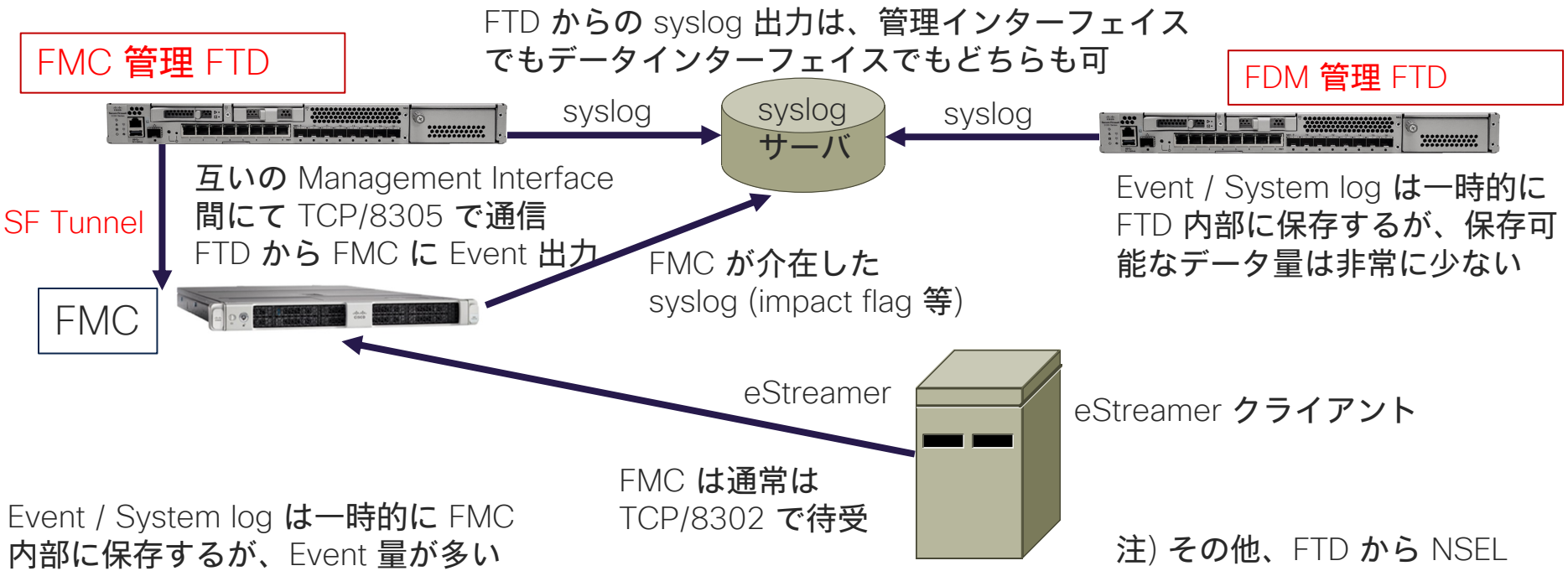
FMC (On Premise) の高可用性

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



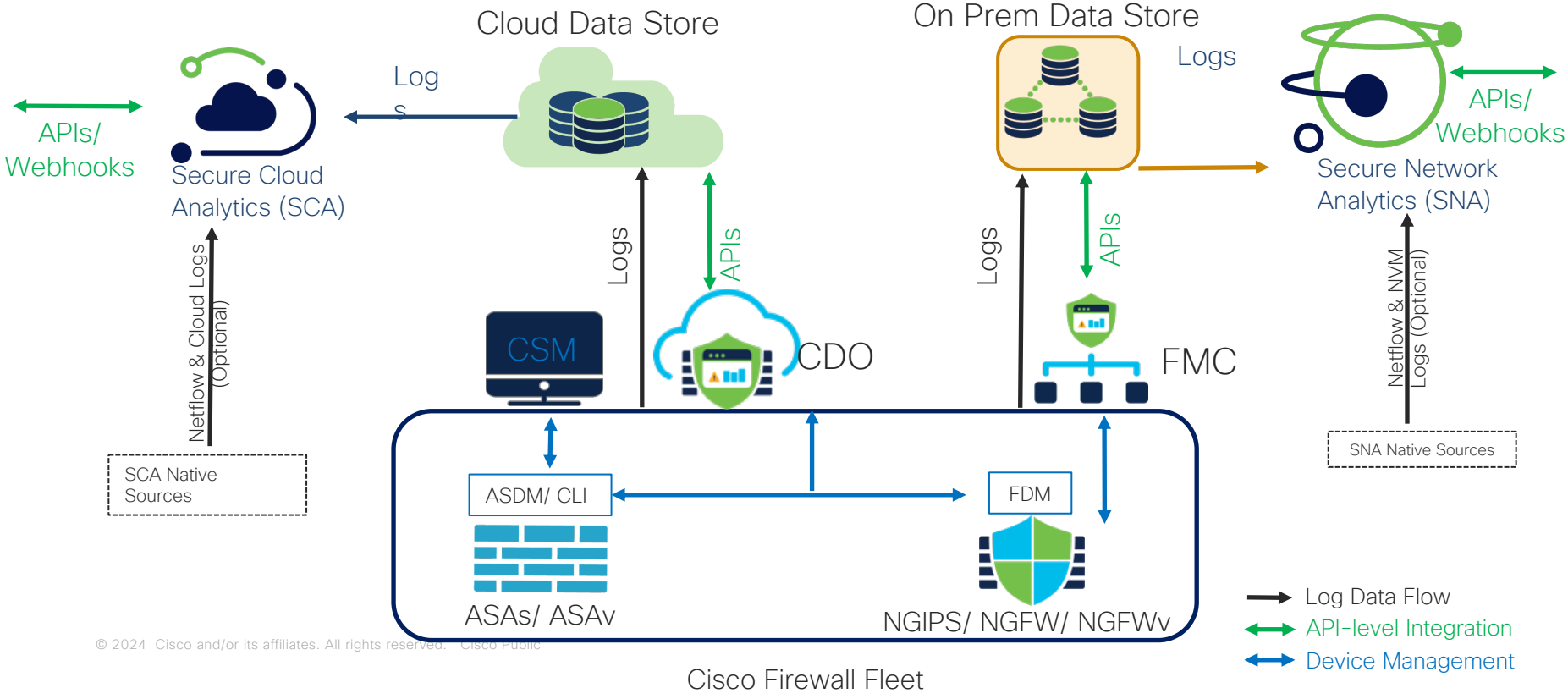
Logging

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

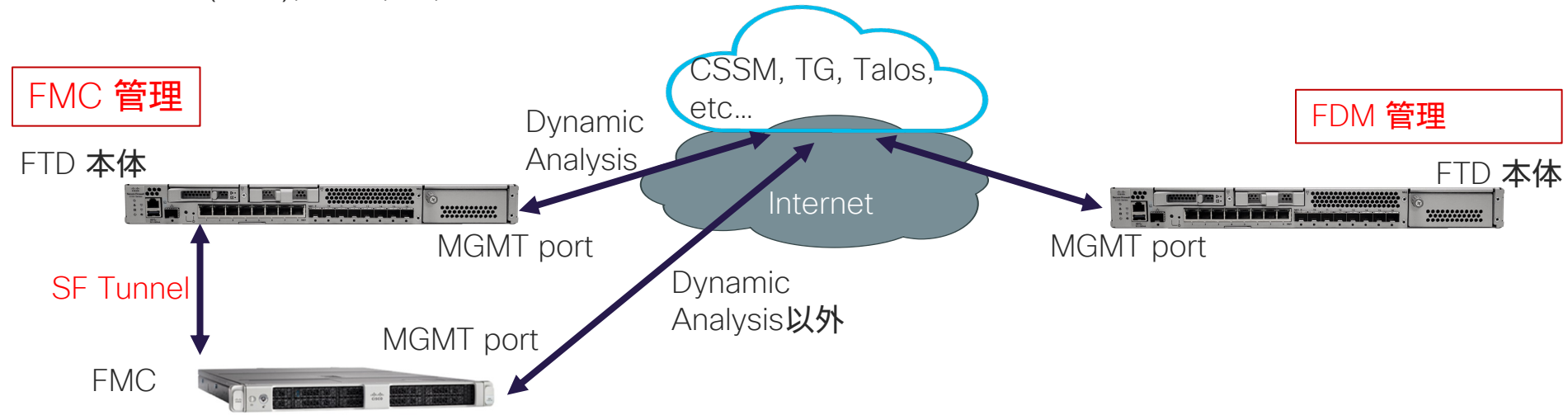
Firewall の logging をクラウド or オンプレミスに実施し、そのデータを有効活用



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

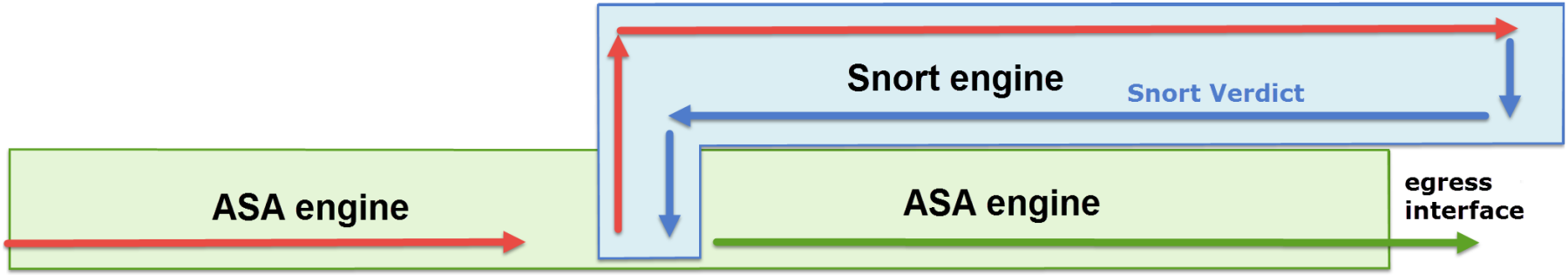


FMC 管理の場合、CSSM へのアクセスも含め、ほとんどのインターネットアクセスは FMC が実施する
ただし、Cloud の Threat Grid にファイルを submit する (Dynamic Analysis) のは FTD から行われる
Proxy 経由、NAT 越えはサポート
CSSM へのアクセスが不可な場合 (Air Gap 環境)、License Reservation を利用

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

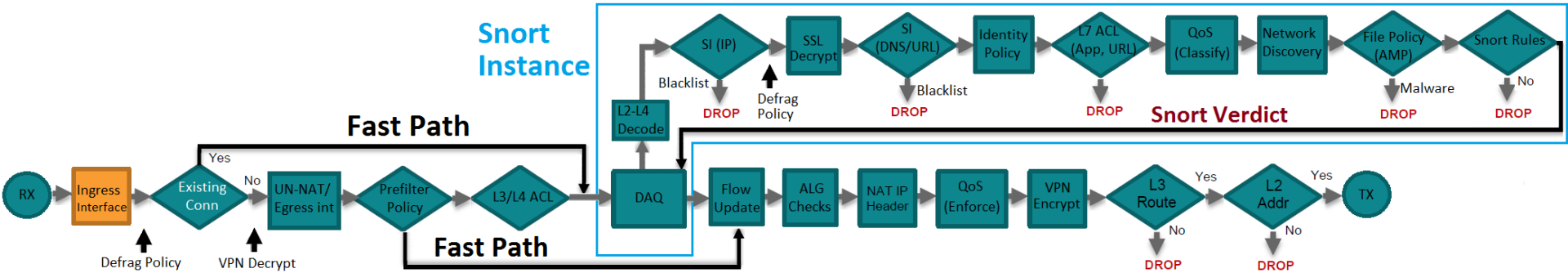
FTD パケット処理の大まかなプロセス



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

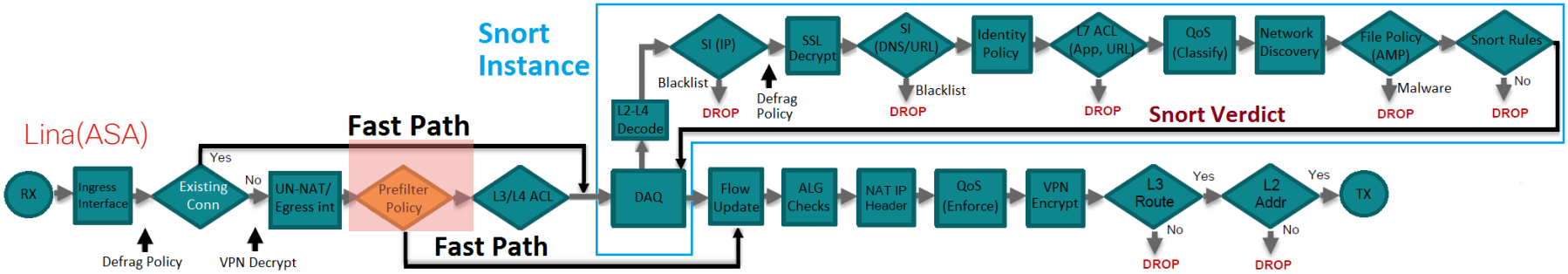
- Snort エンジンは従来の Firepower IPS のコードをベースとして動作
- ASA エンジンは ASA Firewall 9.x のコードで動作

FTD パケット処理 詳細



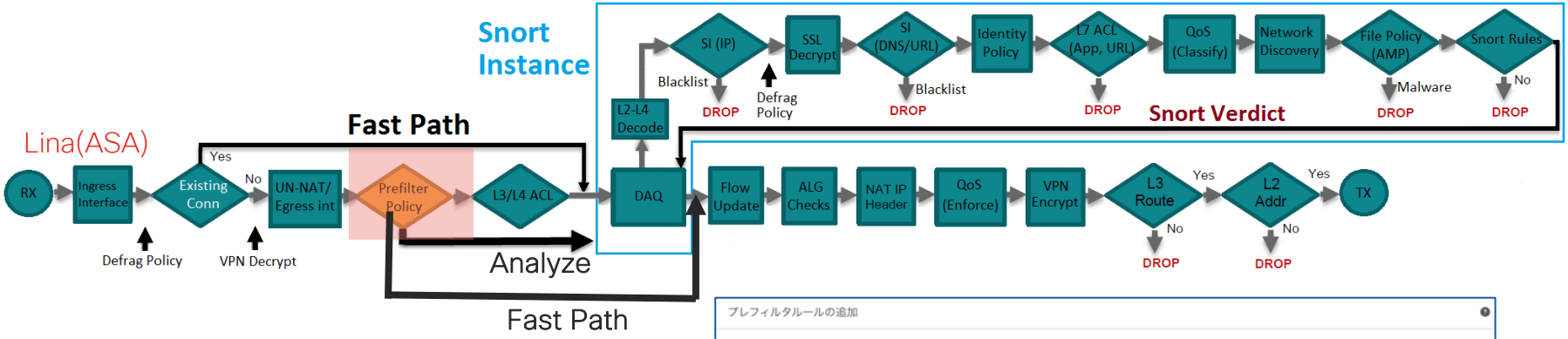
Routed / Switched(Transparent) mode: ASA + Snort **フル機能**
その他: ASA **一部機能** (L3-4ACL)

Prefilter ポリシーの役割



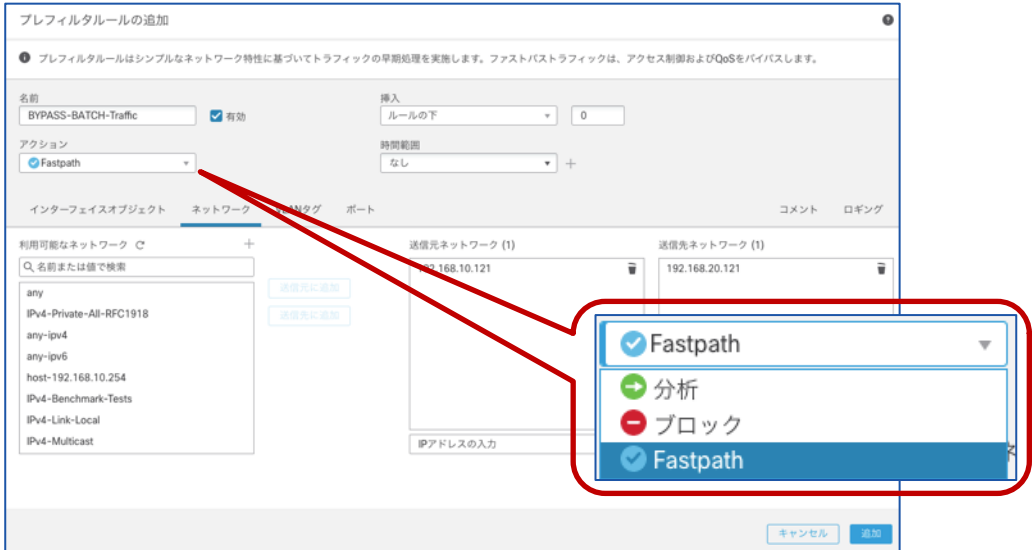
- Prefilter ポリシーは主に2つの役割を提供
  1. トンネル内のパケットに対するインスペクション処理
     - GRE、IP-in-IP、IPv6-in-IP、Teredo Port 3544
  2. Snort 処理前のアクセスコントロール
     - 監視系 / バックアップなど L7 レベルでの検査が不要な信頼された通信をバイパスする、等

Prefilter ポリシーの役割 (続き)

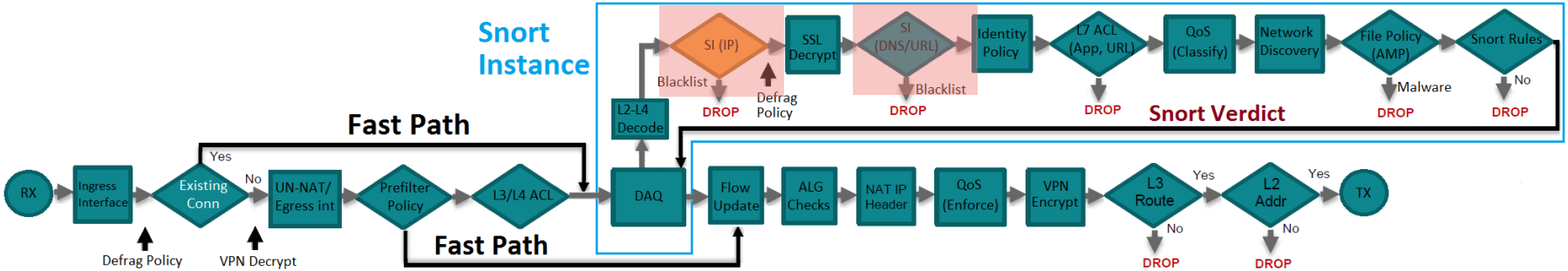


- Snort 処理前のアクセスコントロール、3つのアクション

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)



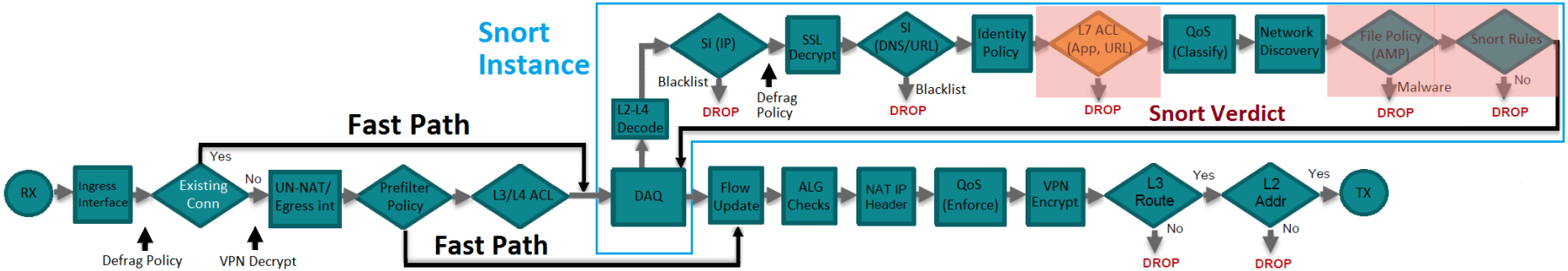
Security Intelligence (IP Address / URL)：

- 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)

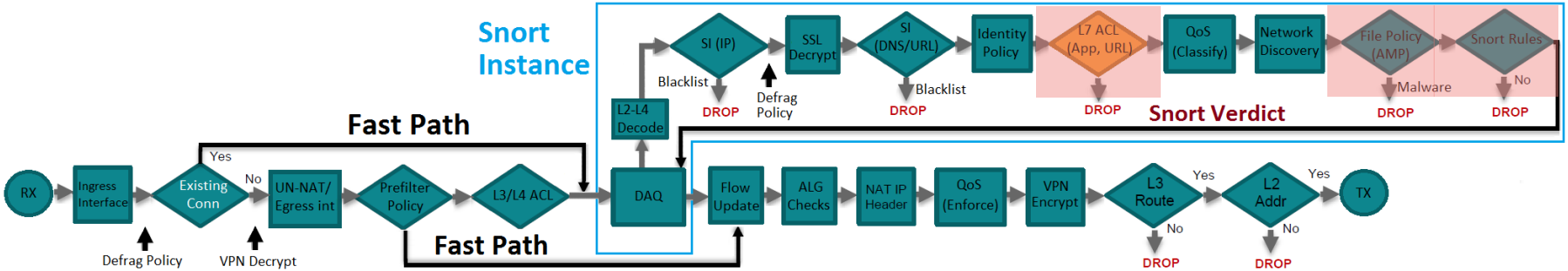


Access Control Policy:

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

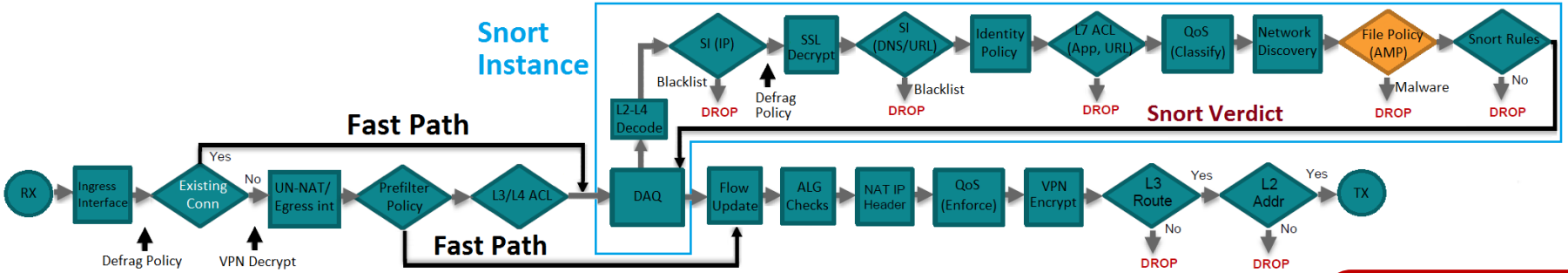
L7 ACL (Access Control Policy) (続き)



- Access Control ルール、 7 つのアクション

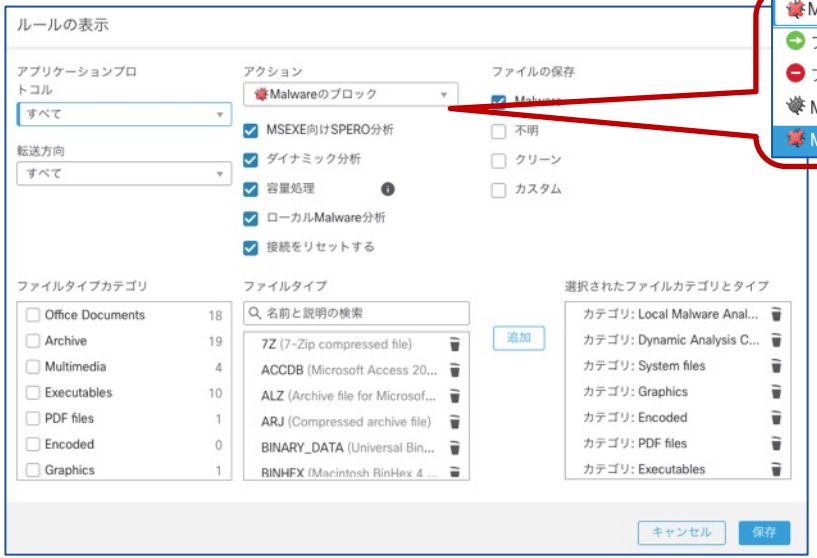
1. 承認 (Allow): パケットを許可、IPS / File 検査可能
2. トラスト (Trust): パケットを信頼、IPS / File 検査スキップ
3. モニター (Monitor): パケットのログ取得、次のルールへ処理を回す
4. ブロック (Block): パケットを破棄
5. リセットしてブロック (Block with reset): パケットを破棄、送信元へリセットパケット送信
6. インタラクティブブロック (Interactive Block)： 警告画面表示
7. リセット付きインタラクティブブロック (Interactive Block with reset):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

Malware & File Policy

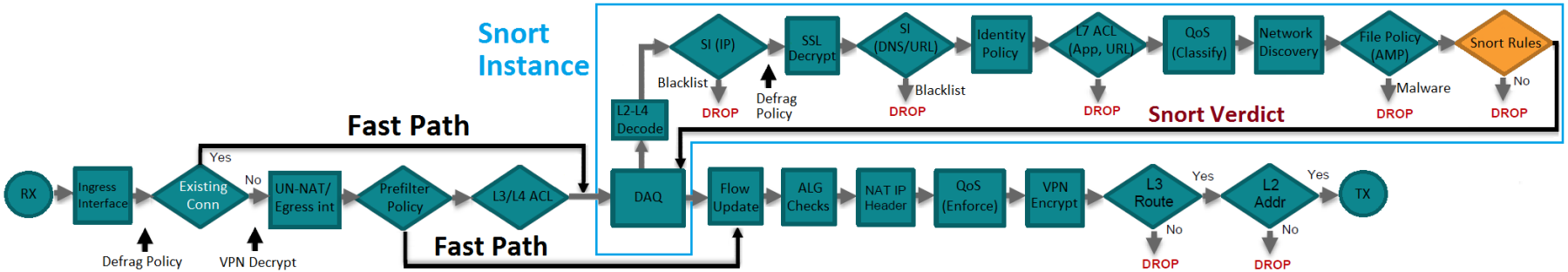


- Malware & File Policy：

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

まとめと参考資料

まとめ

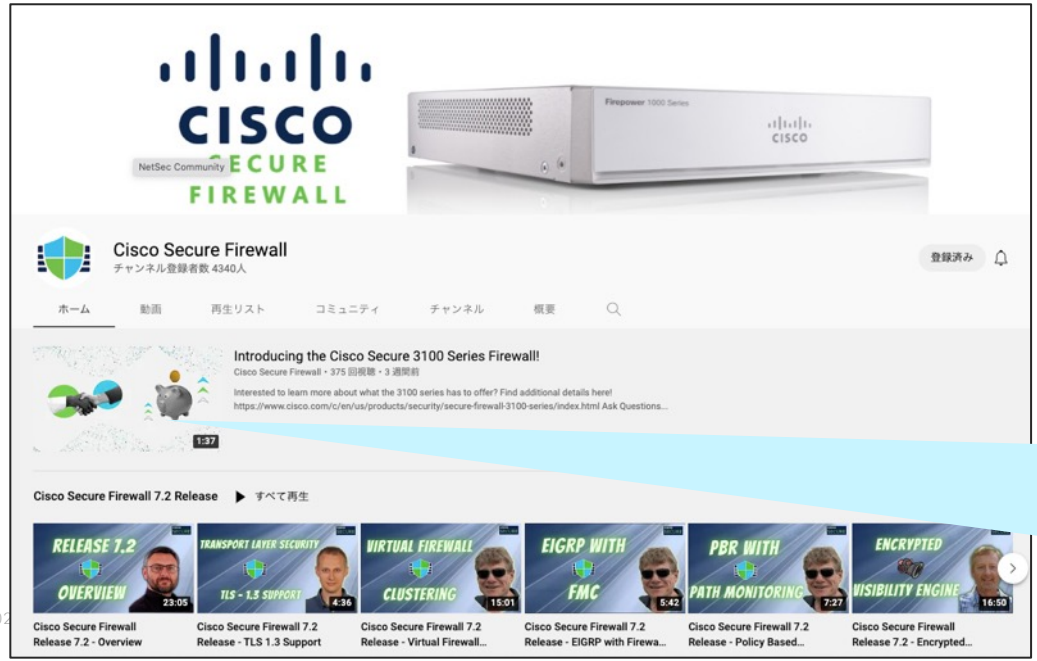
- Firewall Threat Defense (FTD) が上位レイヤの脅威対策を行う NGFW & IPS 製品として位置づけられ、市場で認知されている
- L4 までの Basic Firewall である ASA と L7 Security の FTD を適材適所で使い分ける
- “本当に使える” 脅威対策として FTD は優れた機能や管理性を持つ
- FTD は ASA の機能を包含した新たな NGFW + IPS + Malware Defense 製品として利用可能
- FTD も ASA も同一ハードウェアで動作し、豊富なラインナップがある
- FTD と ASA の明確な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 初期設定ガイド等を公開中)
  https://www.cisco.com/c/m/ja_jp/partners/documents.html
- Japan Partner Community : セキュリティ
  https://salesconnect.cisco.com/APJCPartnerCommunity/s/japan-partner-community-sec
- [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/
- The Cisco Secure Firewall Essentials Hub (ドキュメントまとめサイト)
  https://secure.cisco.com/secure-firewall

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