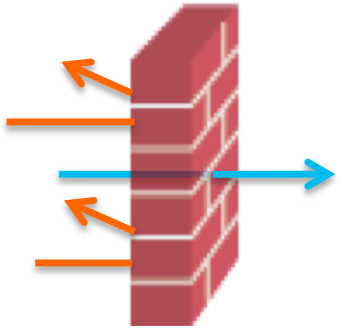
30分でわかる
Cisco NGFW (次世代ファイアウォール)

2020年11月5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)

現在の脅威対策にこのような課題はありませんか?

- 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
- 次世代ファイアウォールは導入しているが、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

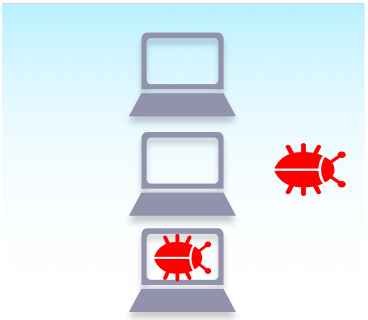
Web アプリケーション、ユーザ、脅威の可視化

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

Firepower シリーズ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_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 Nove

ホストプロフィール　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		
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

▼ 侵入の痕跡 (1)　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

端末 OS

▼ オペレーティングシステム　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 アプリケーション

サーバ (15)

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		

▼ 脆弱性 (1022)　脆弱性を編集する

該当脆弱性リスト

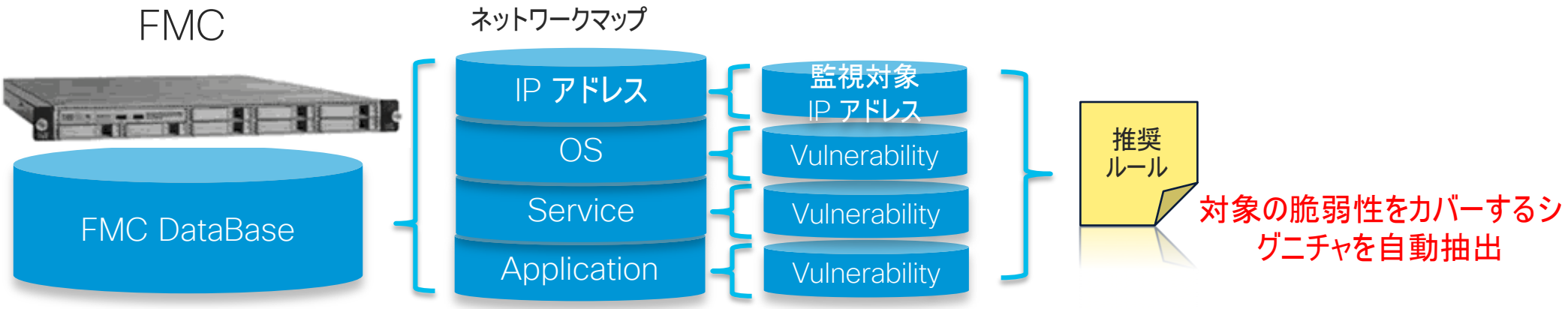
名前	ポート
A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system, aka "Microsoft JET Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012	Windows 7, Server 2008, Phone 7.5, 8
A 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

✓ 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 OS、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

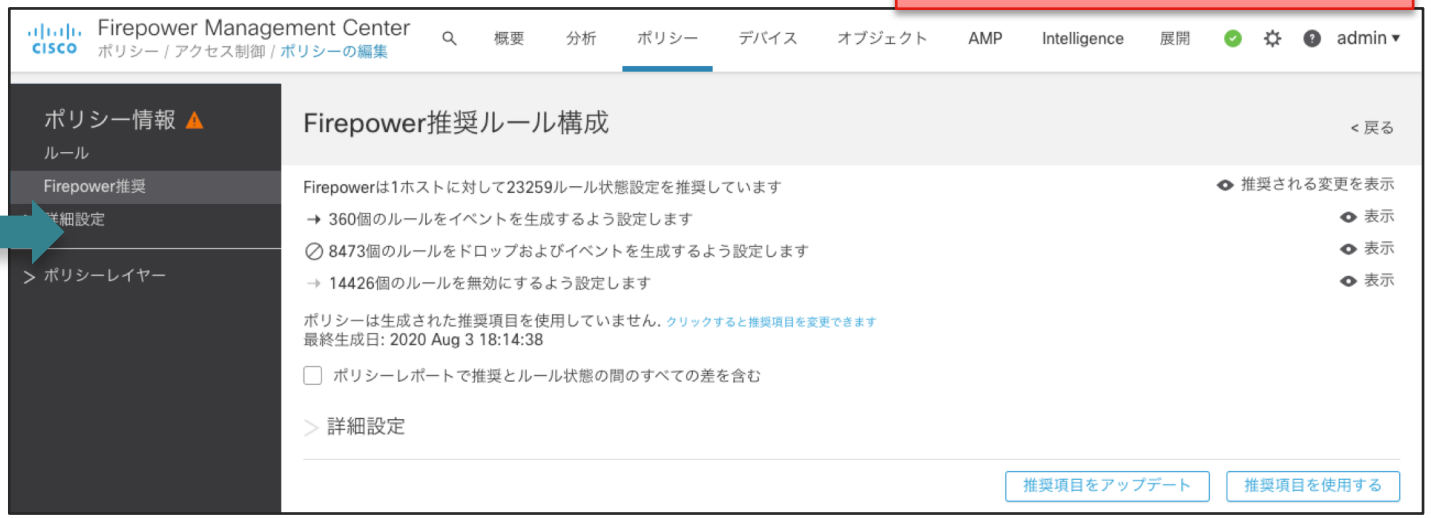
自動チューニングとインパクト解析

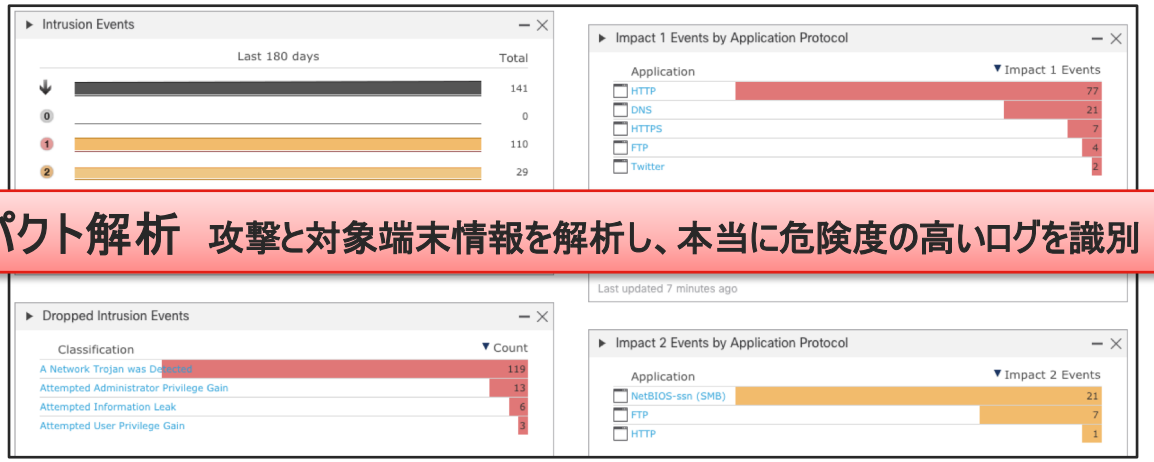
自動チューニング
ネットワーク環境を学習し、最適な推奨設定を自動生成

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・・・

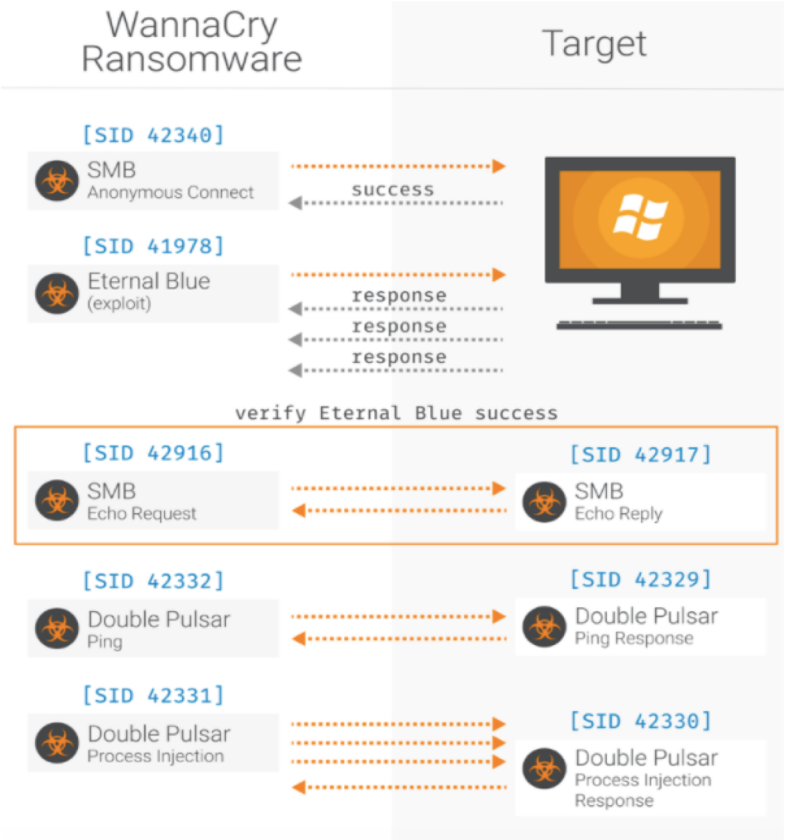




インパクト解析 攻撃と対象端末情報を解析し、本当に危険度の高いログを識別

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



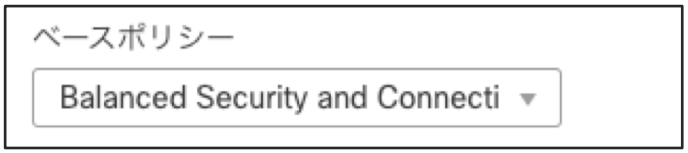

```
rule    alert udp $HOME_NET any -> any 53 (msg:"APP-DETECT 12P DNS request attempt"; flow:to_server; byte_test:1,!&,0xF8,2; content:"|03|b32|03|i2p|00|"; fast_pattern:only; metadata:policy max-detect-ips
        drop, service dns; reference:url,geti2p.net; classtype:misc-activity; sid:37062; rev:2;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

IPSポリシーの設定

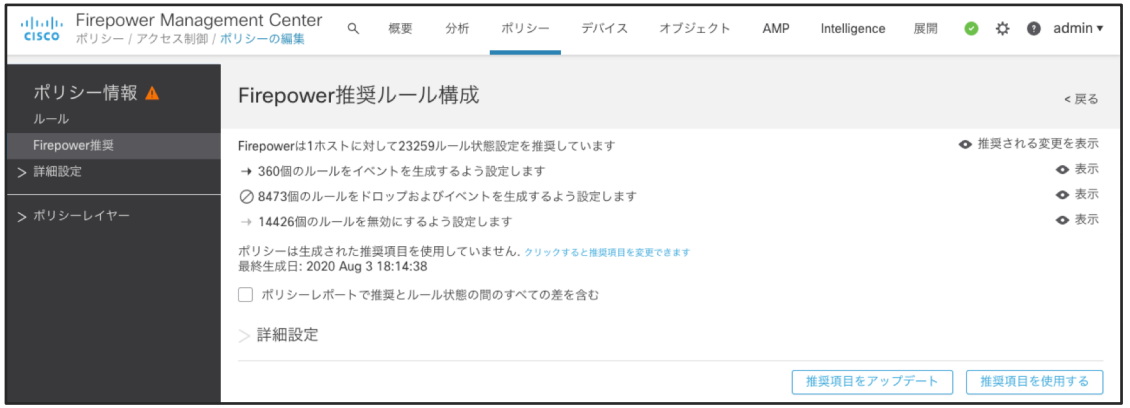
- ベースポリシー（ベンダー推奨ポリシー）の選択
  - Security Over Connectivity
  - Balanced
  - Connectivity Over Security

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

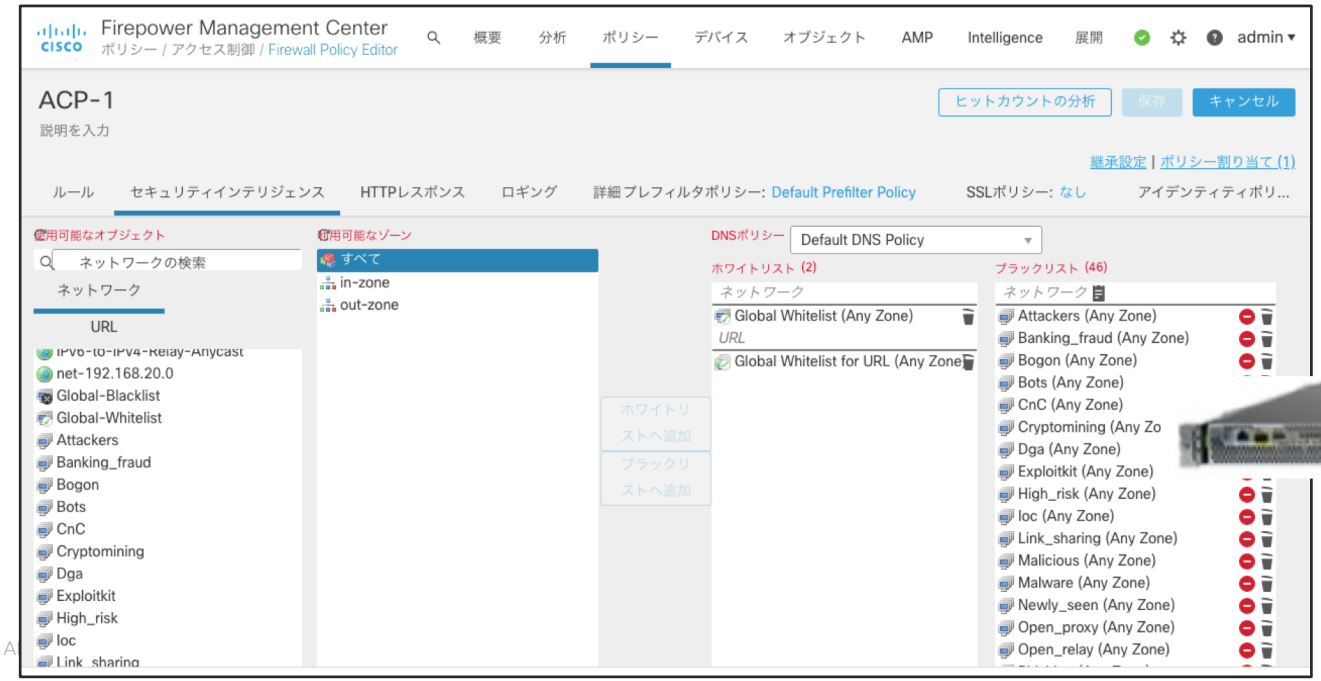


- カスタムチューニング
  - ベースポリシーおよび推奨設定を上書き

Security Intelligence 脅威情報フィルタ

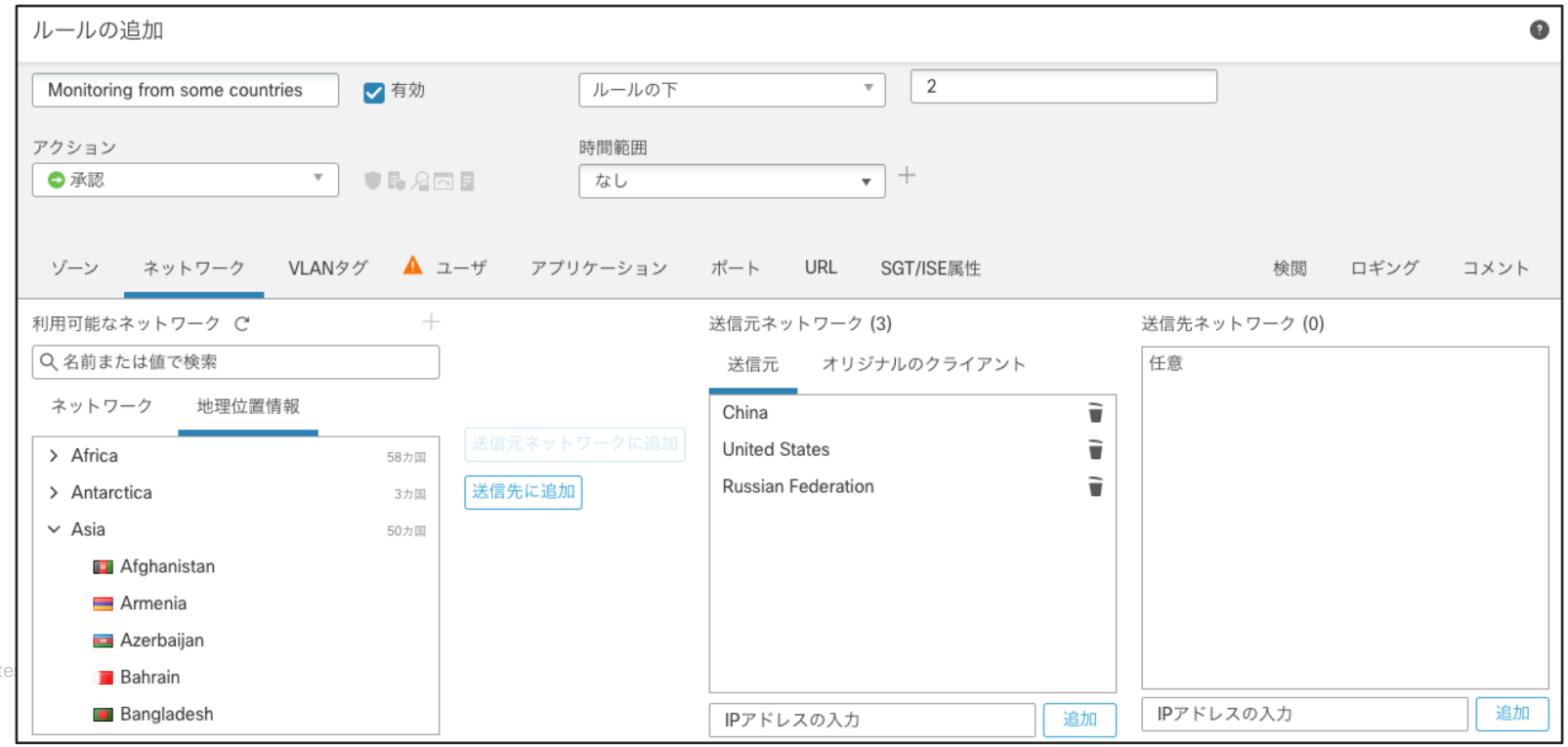
- Cisco Collective Security Intelligence 提供のブラックリスト IP アドレス、URL、ドメインに基づく制御 (i.e. レピュテーション)
- 既知のブラックリスト宛て or からのコネクションを　モニターもしくはブロック
- カテゴリー
  - CnC
  - Malware
  - Phishing
  - Bots
  - Attackers

    など



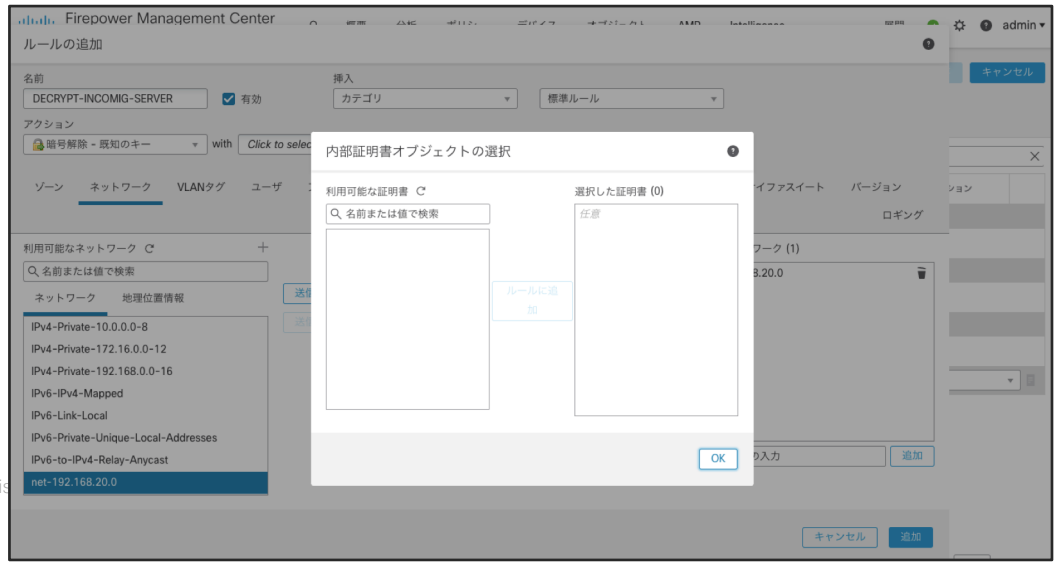
ジオロケーション

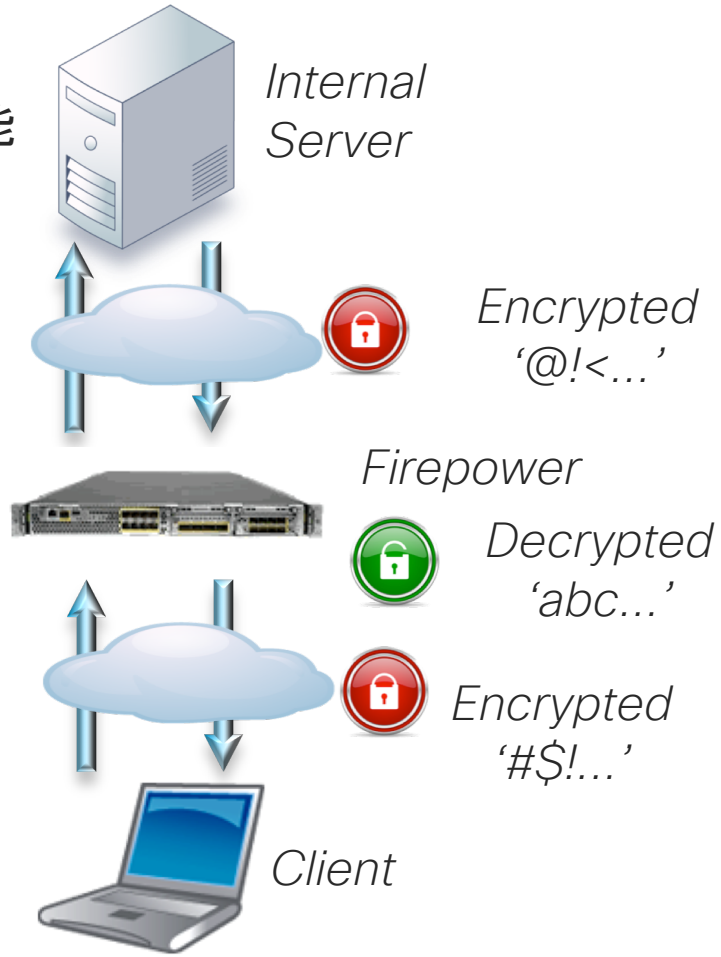
- IP アドレスと国や地域を紐づけたジオロケーションデータベース
- IPS、アプリケーション制御、ファイルポリシー等の任意の設定と組み合わせて利用可



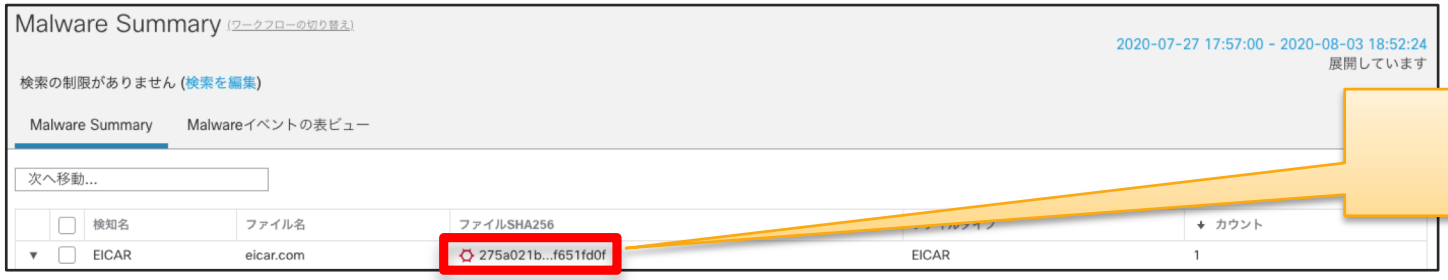
TLS 暗号化アクセラレーション

- 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、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



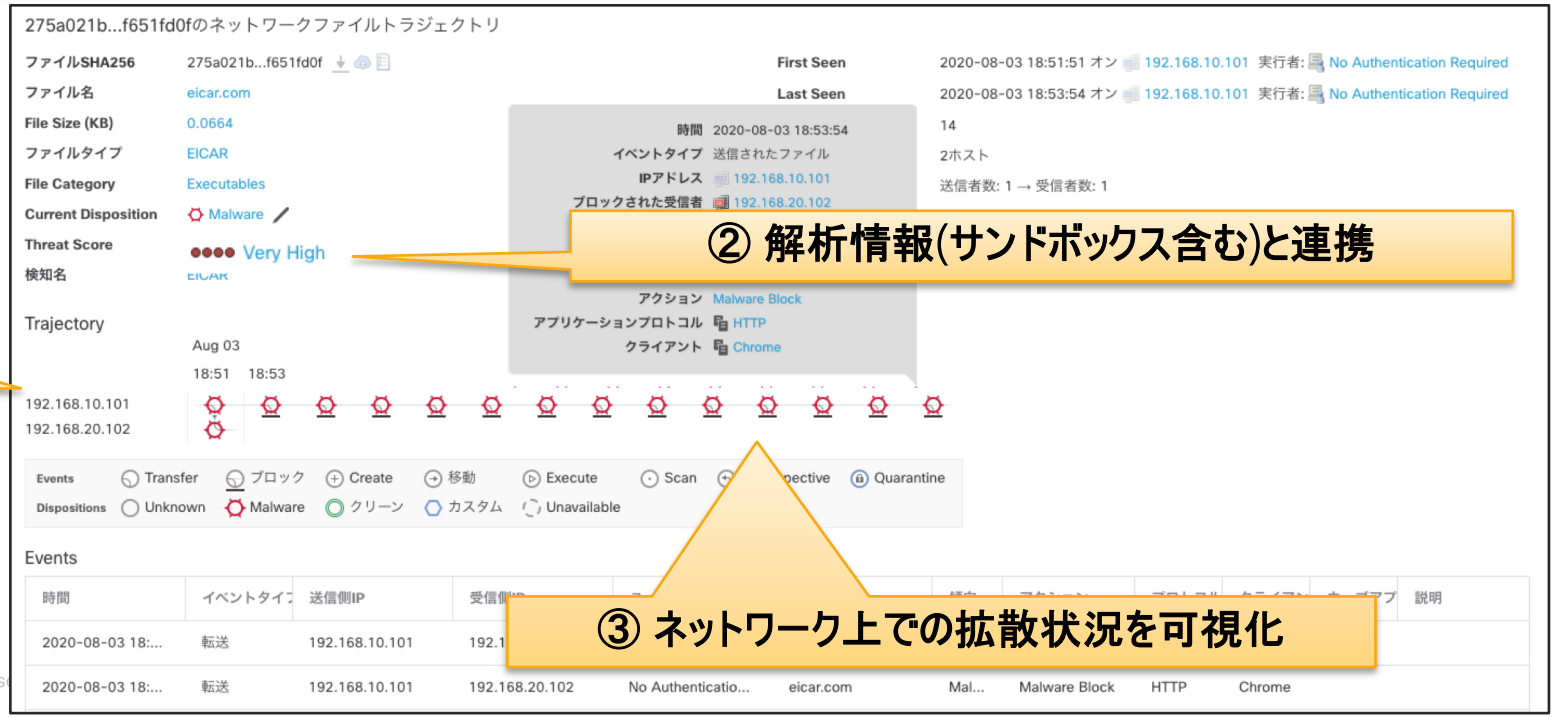


AMP4N (Advanced Malware Protection for Network)
マルウェアの可視化と制御、トラッキング



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)



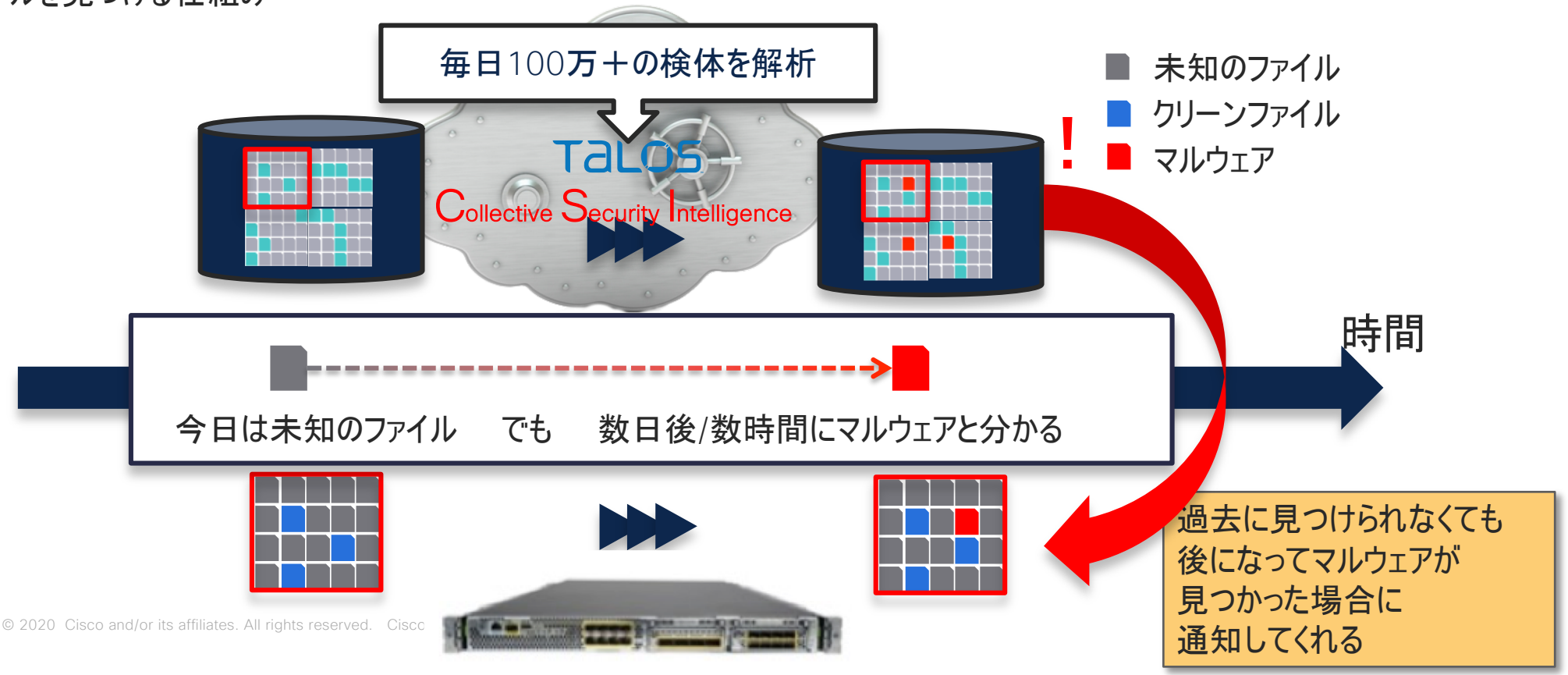
② 解析情報(サンドボックス含む)と連携

③ ネットワーク上での拡散状況を可視化

④ 端末の特定

AMP4N (Advanced Malware Protection for Network)
クラウドリコール

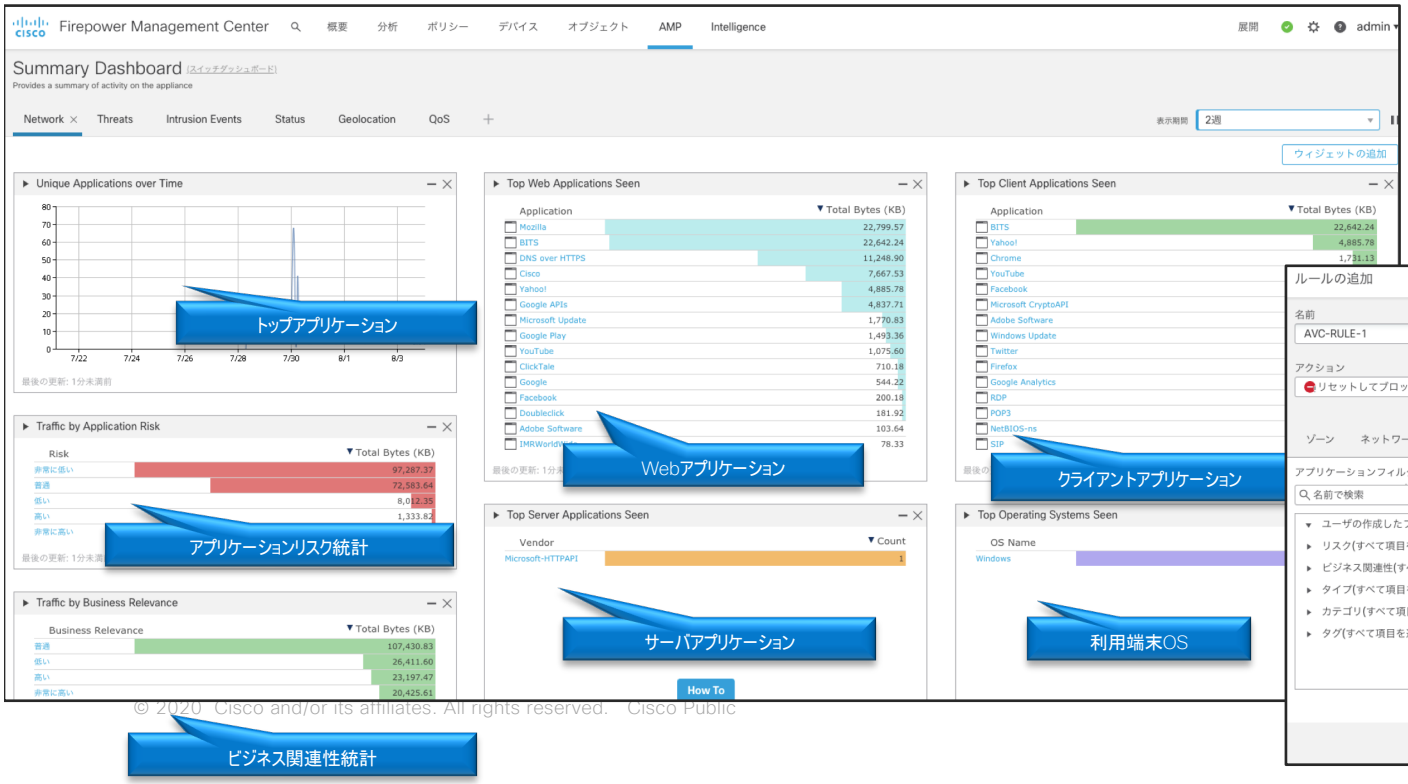
一度調査したファイルを覚えておき、合致するマルウェアが見つかった場合に瞬時にそのファイルを見つける仕組み



クラウドリコールによるゼロデイマルウェア検知例

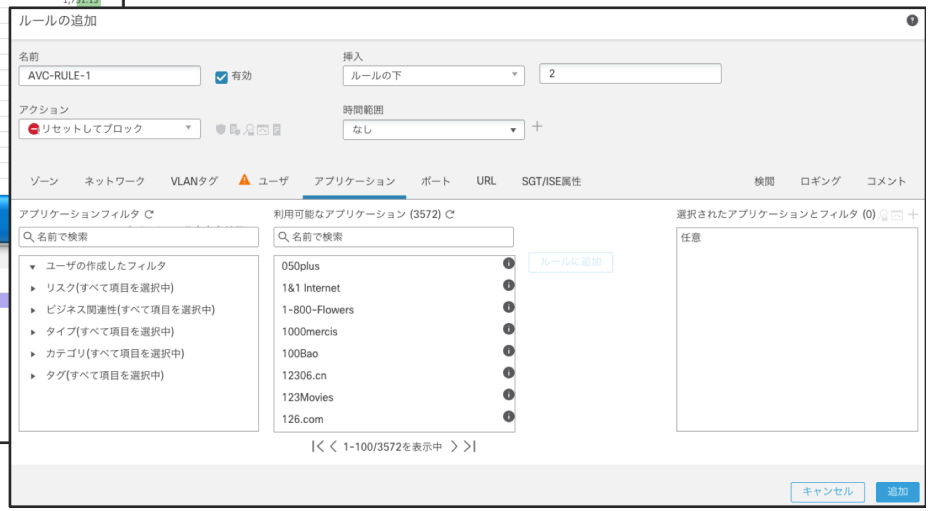
Application Visibility Control アプリケーションの可視化と制御

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



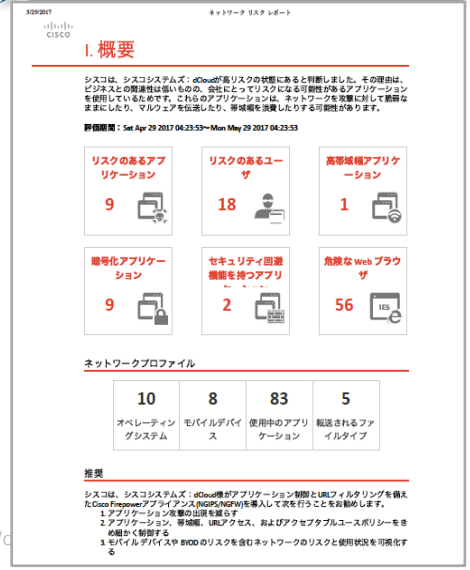
Custom Report レポート機能

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

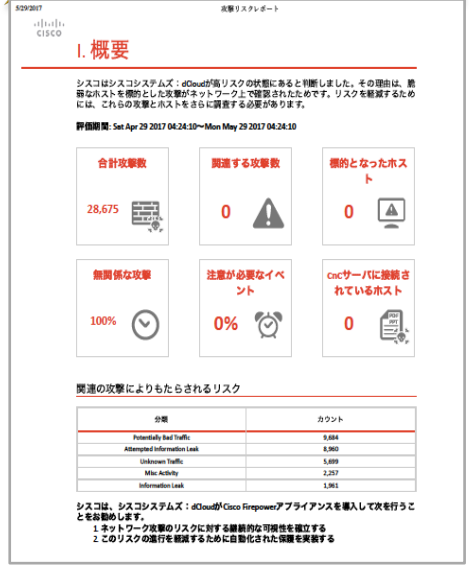
作成したレポートを任意のメールアドレスへ自動転送

PDF、HTML、CSV形式をサポート

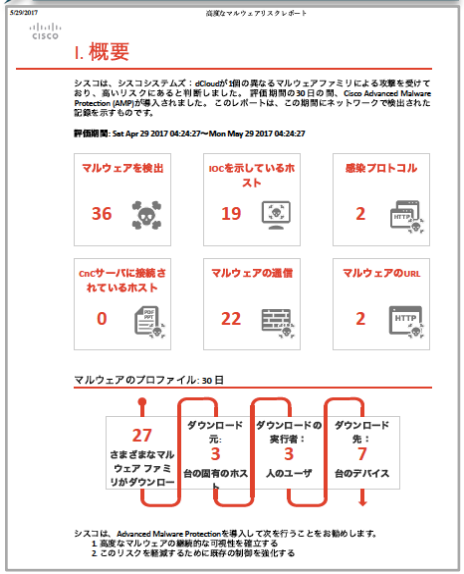
ネットワークレポート



アタックレポート



マルウェアレポート



FTD の市場評価

2018年に続き、2019 年の Gartner Magic Quadrant で、ネットワーク向けファイアウォール分野のリーダーにシスコが選出

さらに、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2つの記事を参照
https://gblogs.cisco.com/jp/2019/10/cisco-named-a-leader-in-the-2019-gartner-magic-quadrant-for-network-firewalls/

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

Cisco Firepower シリーズ提供形態

- Firepower NGIPS / Firepower 単独アプライアンス

  Sourcefire 時代から販売している Firepower 専用機

  (仮想アプライアンス以外全て販売終了アナウンス済み)

- ASA with Firepower Services

  Cisco ASA5500-X と Firepower module のハイブリッド

  (多くの機種で販売終了アナウンス済み)

- Cisco NGFW / Firepower Threat Defense (FTD)

  Firepower に ASA 基本機能を統合した一体型ソフトウェア

- Firepower Management Center (FMC)

  Firepower 製品の機能をフルに利用するための管理サーバ

監視カメラ／
センサー

監視モニター／
経験豊富な監視者

Firepower Management Center (FMC) 概要

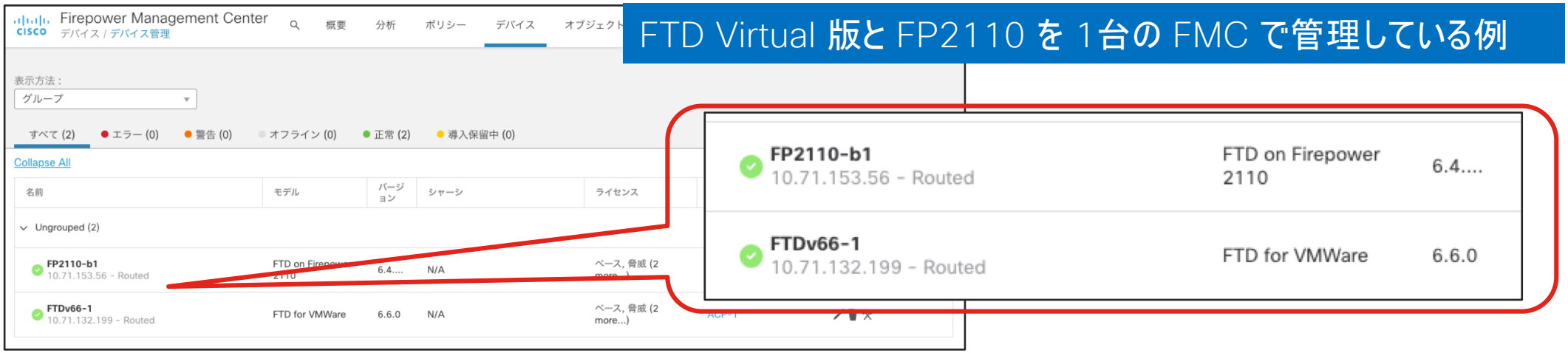
- Firepower 専用機や Firepower Services (on ASA) と、FTD を全てまとめて管理
- Access Control Policy 等、各 Policy を共有可能

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



Firepower 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

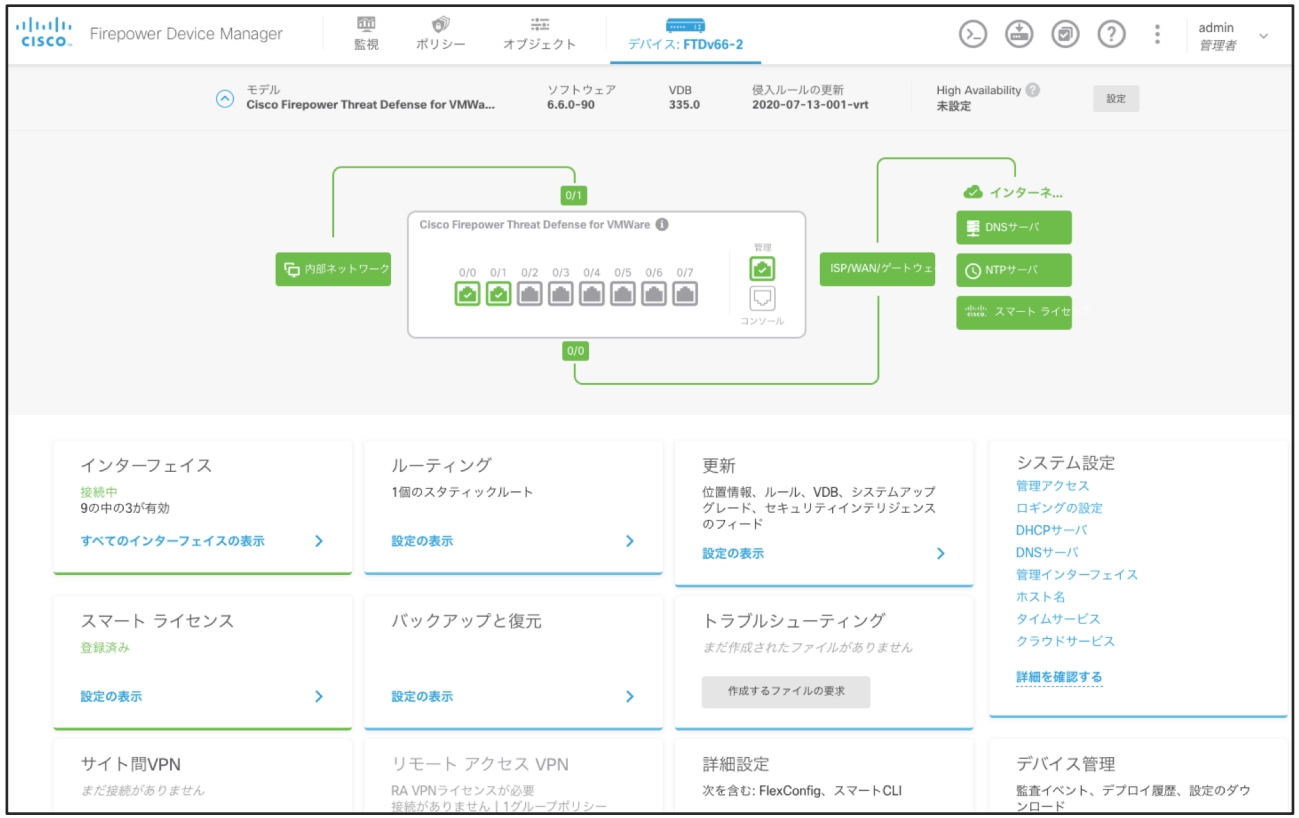
Virtual FMC
最大 25個のセンサー管理
最大イベント数 1,000万件
250GB のイベントストレージ
最大 5万ホスト、5万ユーザのネットワークマップ
300個のセンサー管理対応モデルも有り (FMCv300)

Firepower の機能を最大限に引き出す管理サーバ

Firepower 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
- AMP4N 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

Firepower 管理方法一覧

11/12 14:00から
ウェビナー開催予定

Centralized

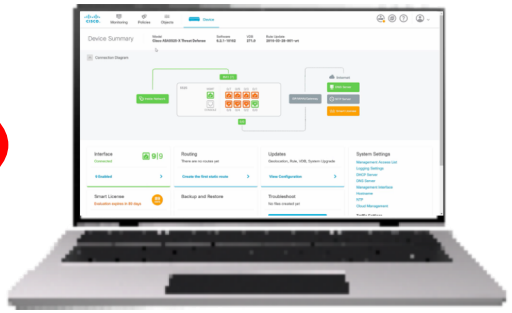
Firepower Management Center (FMC)

複数デバイスに対し、高度なセキュリティ監視・管理と自動化を実現

共存不可

On-box

Firepower Device Manager (FDM)

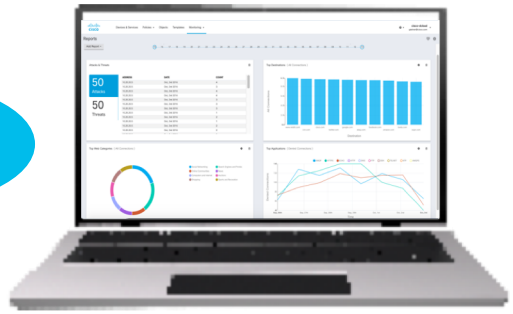


基本的なセキュリティポリシーを、シンプルに1つのデバイスに対して実施

共存可能

Cloud-based

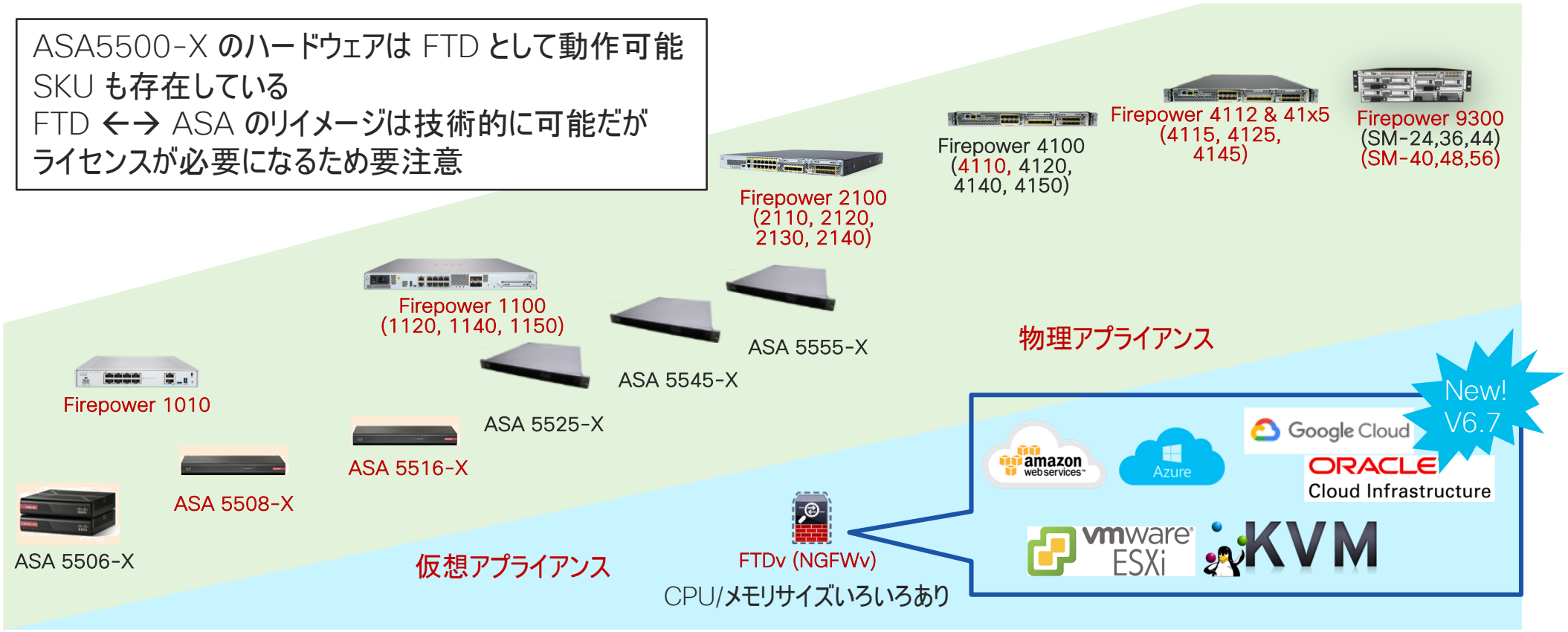
Cisco Defense Orchestrator (CDO)



複数デバイスに対し、クラウドからセキュリティポリシーを管理
FTD だけでなく ASA や Meraki MX も同時に管理可能で、共有オブジェクトも利用可能

Firepower Threat Defense が動くプラットホーム

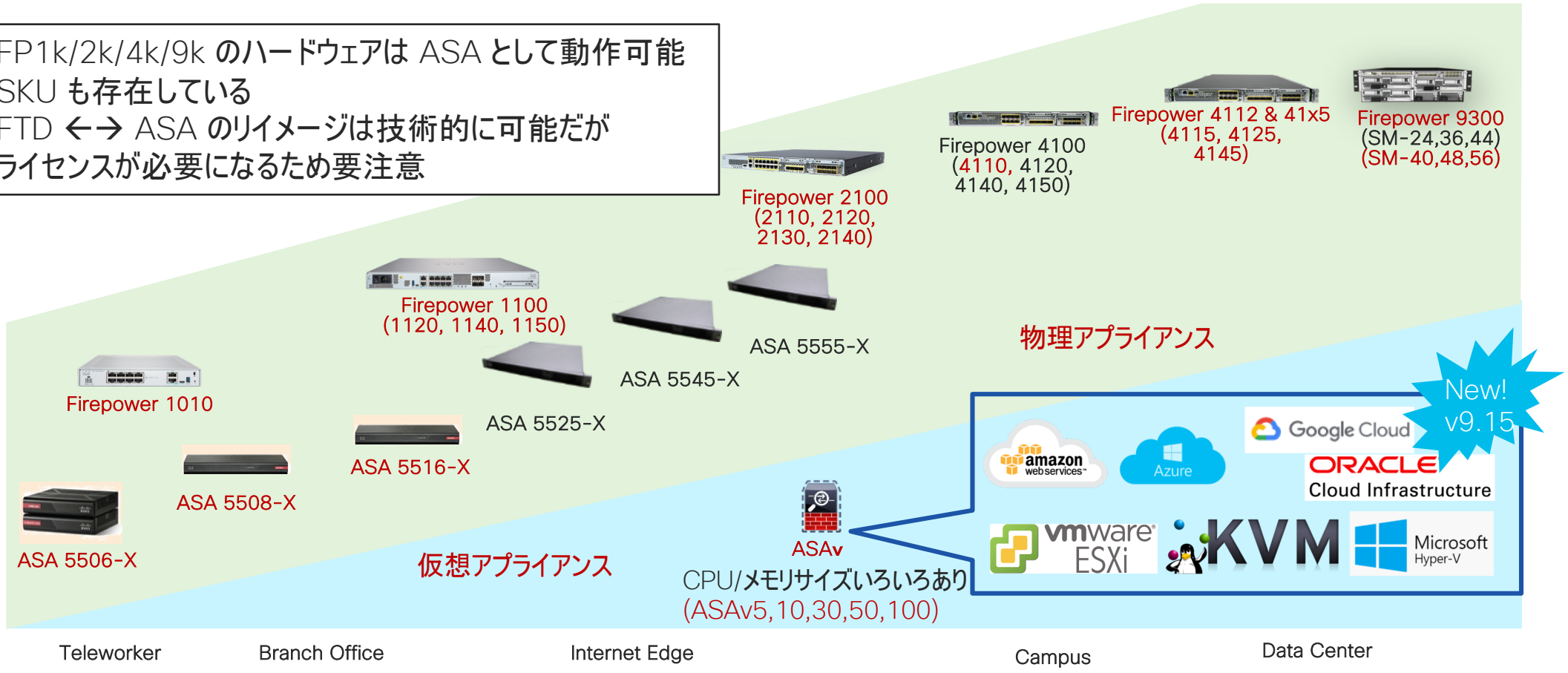
ASA5500-X のハードウェアは FTD として動作可能
SKU も存在している
FTD ←→ ASA のリイメージは技術的に可能だが
ライセンスが必要になるため要注意



黒字のモデルは販売終了アナウンス済み

[参考] ASA ソフトウェアが動くプラットホーム

FP1k/2k/4k/9k のハードウェアは ASA として動作可能
SKU も存在している
FTD ←→ ASA のリイメージは技術的に可能だが
ライセンスが必要になるため要注意

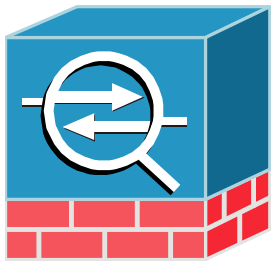


黒字のモデルは販売終了アナウンス済み

[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
  - 16年目のロングセラー

  (PIX まで遡ると27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)
  - 14年目のロングセラー

  (Cisco VPN Client まで遡ると21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

まとめ

- Firepower 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
- “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
- 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
- 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

参考資料 (1)

- Firepower への cisco.comでのショートカット

  http://cisco.com/go/ngfw

- ASA への cisco.comでのショートカット

  http://cisco.com/go/asa

- パートナー向け技術資料 (Firepower 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

- [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

参考資料 (2)

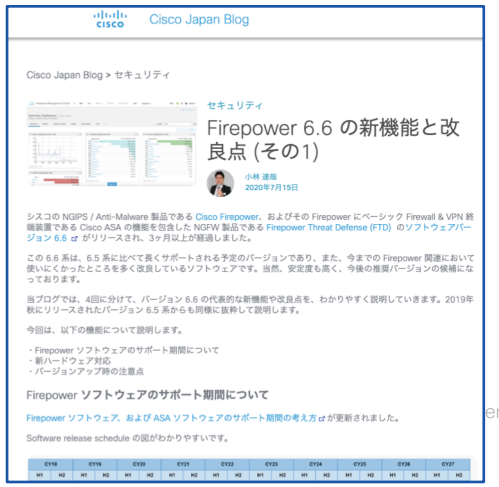
- シスコシステムズ合同会社 コーポレートブログにて、Firepower 6.6 (一部 6.5 を含む) の機能解説を、4回に渡って掲載
  - Firepower 6.6 の新機能と改良点 (その1-4)

    https://gblogs.cisco.com/jp/2020/07/fp66-release-1/

    https://gblogs.cisco.com/jp/2020/07/fp66-release-2/

    https://gblogs.cisco.com/jp/2020/07/fp66-release-3/

    https://gblogs.cisco.com/jp/2020/07/fp66-release-4/

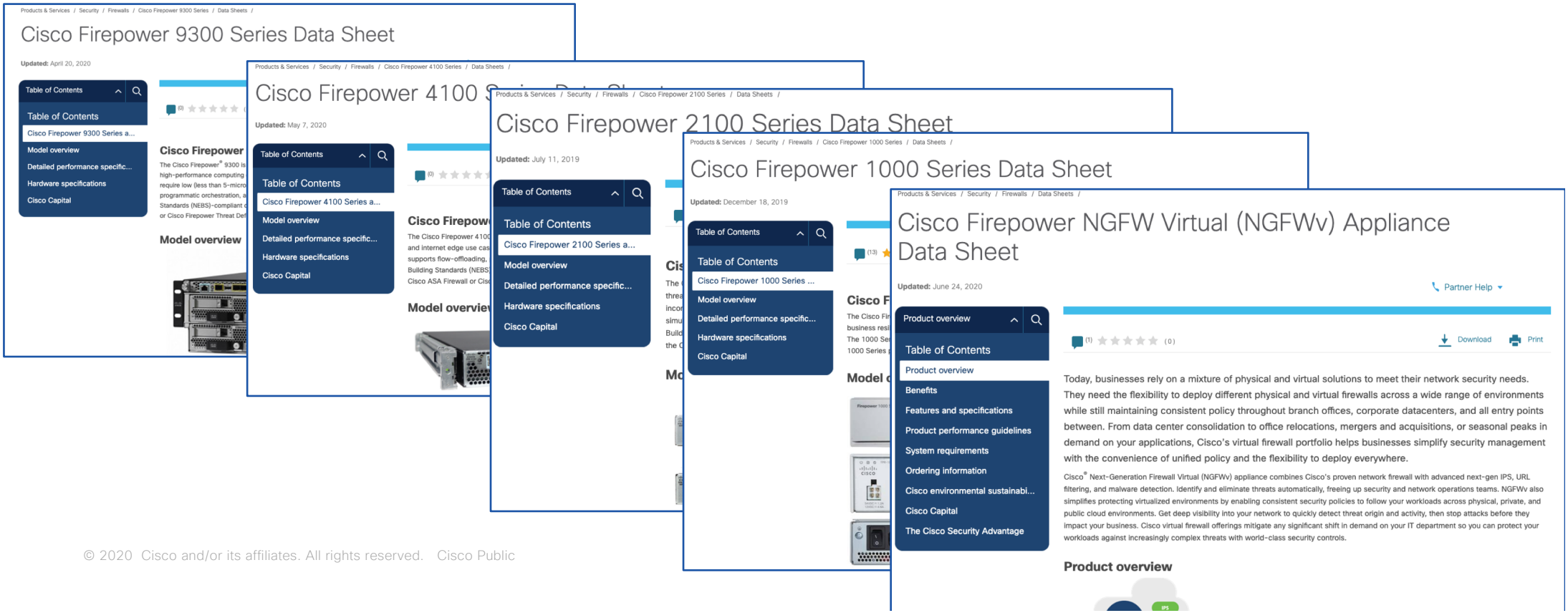


Appendix

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 Smart Software Manager Satellite 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 ★

  AMP for Networks, Threat Grid, ファイル保存

- 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

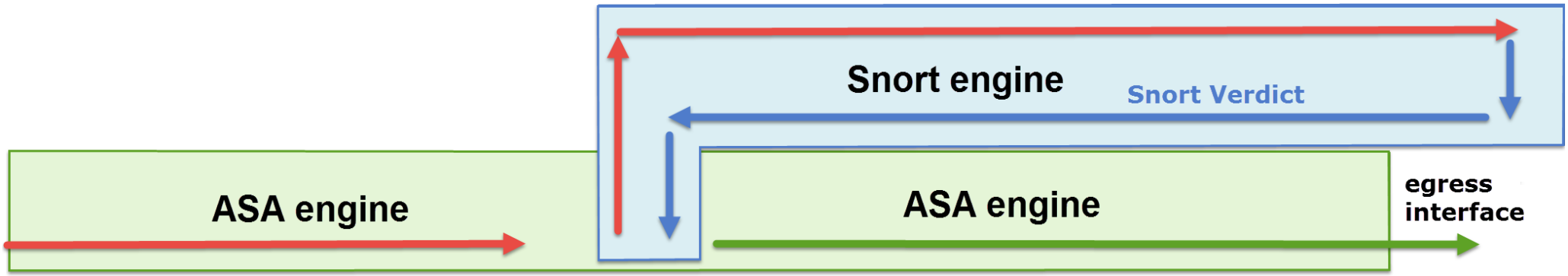
  評価ライセンス利用のためには別途申請が必要 (初期の 90日間評価ライセンスには含まれない)

- 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)

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

ソフトウェアライフサイクルポリシー

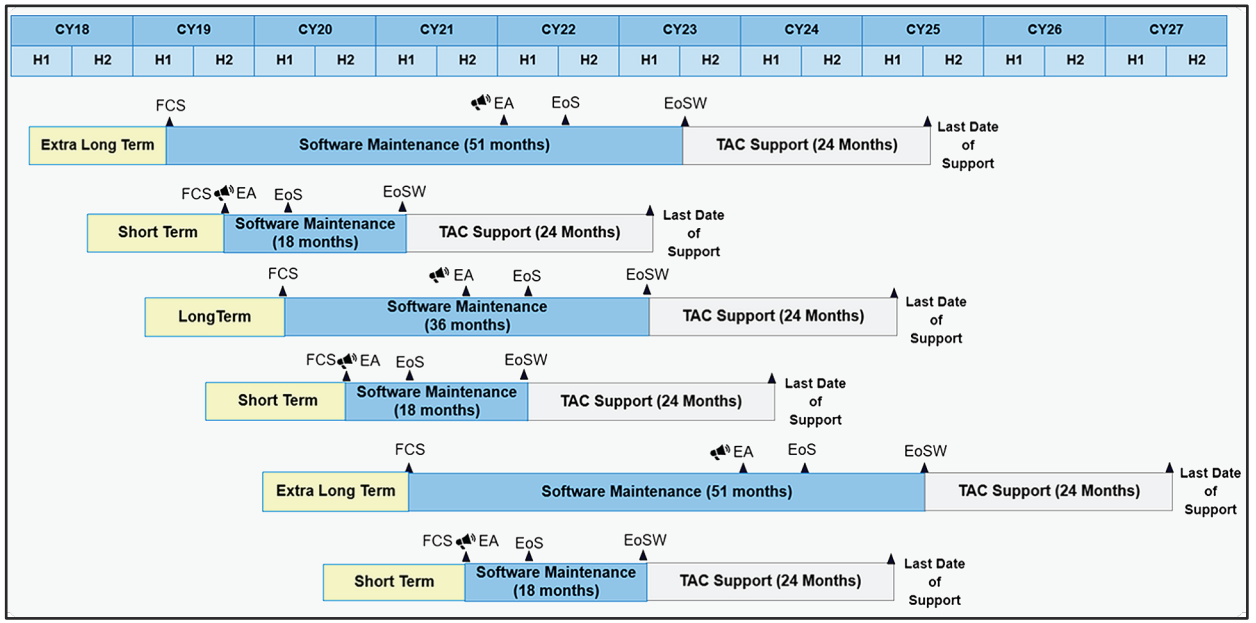
Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin
https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html

- 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

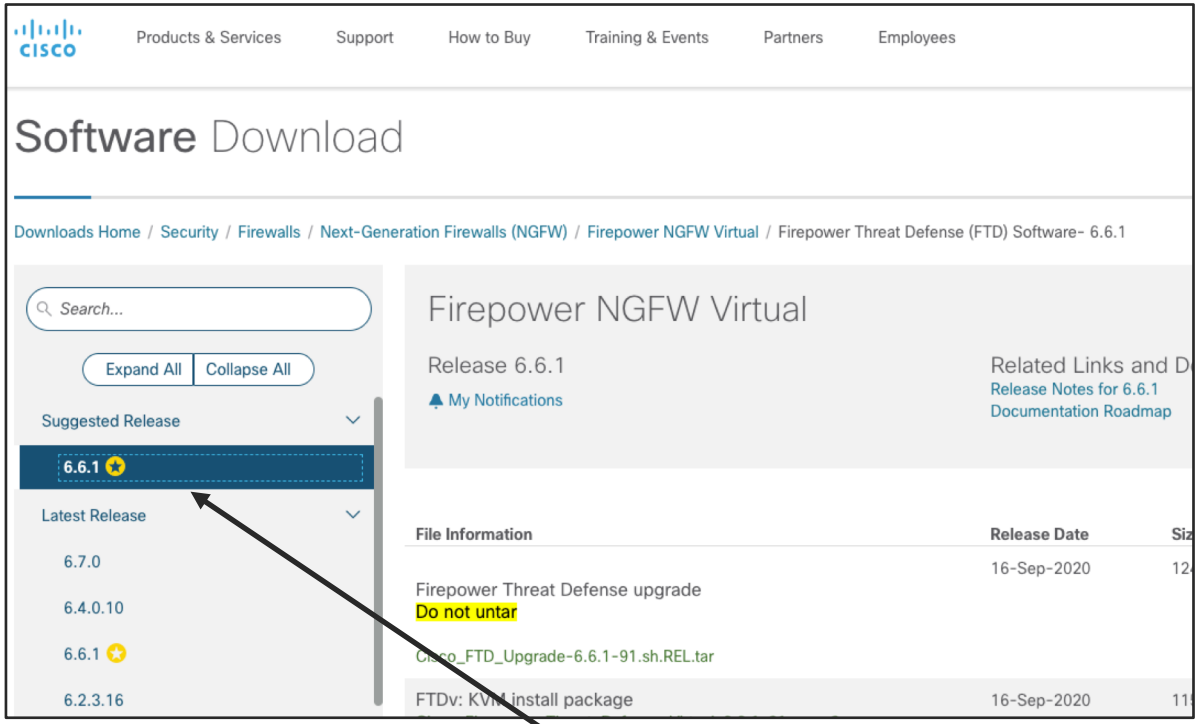
  FTD 6.6 → ロングタームサポート
- ロングタームサポートの中でも、2019年前半、2021年前半(予定)にリリースされるものはエクストラロングタームサポートとなる

  FTD 6.4 → 2019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

- 2020年11月時点で一般的な推奨バージョンは 6.6.1
  - 6.4 系の最新版も十分に利用されているが、いくつかのセキュリティアドバイザリに該当しているので要注意
  - 6.5 系はショートタームサポートであり、すでにサポート終了スケジュール発表済み
- 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



★マークに注目


CISCO