ざっくり FTD
(Firewall Threat Defense)

2024年2月

シスコシステムズ合同会社

イチオシの機能

アジェンダ

- 用語集
- FTD とは
- ターゲットとゴール
- FTD が必要となる背景と課題
- FTD の主要機能の紹介
- FTD の機能と課題との対応付け
- 一般的なネットワーク構成図における FTD の位置付け
- Firewall は ASA か FTD か?
- FTD の代表的な機能の紹介
  - ネットワークの学習と可視化
  - IPS 自動チューニング
  - IPS インパクトフラグ
  - Security Intelligence
  - TLS Decryption
  - Malware Defense
  - アプリケーションの可視化と制御
  - Encryption Visibility Engine
  - Unified Event Viewer
- 第三者評価補足資料
- FTD のまとめ
- ネクストステップ
- 補足資料

用語集-1

- IPS – Intrusion Prevention System の略。パケット単体や複数の中身や振る舞いまでを見て、シグニチャとのパターンマッチングで攻撃を検知し、防御するシステム。検知とアラートだけの場合には IDS (Intrusion Detection System) となる
- NGFW – Next Generation Firewall (次世代ファイアウォール) の略。ベーシックファイアウォールは、IP アドレス、ポート番号、プロトコルで識別してフィルタリングを行うが、NGFW は L7 の情報となるアプリケーション識別やユーザアカウント情報等とも連携してフィルタリングを行うことができる
- FTD – Firewall Threat Defense の略。旧名称は Firepower Threat Defense。詳細は「FTD とは」のページを参照
- Firepower – 現在は FPR1k,2k,4k(4100),9k のハードウェアのブランド名を指す。以前は、旧 Sourcefire 社が販売していた IPS のソフトウェアの名称であり、最近までは FTD の正式名称にも使われていた。現在、ハードウェアブランドの名称は Cisco Firewall となっており、最新の 3100 と 4200 シリーズは Firepower ではなく、Firewall 3100 / 4200 シリーズという名称である

用語集-2

- FMC – Firewall Management Center の略。旧名称は Firepower Management Center。複数の FTD デバイスをまとめて管理し、ポリシーの共有化を行うことができる。ネットワークの学習機能を備えており、IPS の自動チューニングやインパクトフラグといった FTD に非常に大事な機能の中枢を担う。本資料全体で詳しく説明
- FDM – Firewall Device Manager の略。旧名称は Firepower Device Manager。FTD 単体管理のために FTD に内蔵された管理ソフトウェアであり、管理者は FTD の管理ポートに https でアクセスして FDM を利用する
- CDO – Cisco Defense Orchestrator の略。シスコが提供するクラウドサービスであり、ASA, FTD, Umbrella, Meraki デバイス等の Firewall 機能を統合管理することが可能。CDO には Cloud Delivered FMC (cdFMC) の機能が含まれており、FTD 管理を CDO に含まれた cdFMC から行うことで、On Premise の FMC とほぼ同じ GUI で設定が可能

用語集-3

- サンドボックス - ここでは、仮想マシンにて動作可能なファイルを実行し、どのように振る舞うかを解析する機能を指す。FTD では、Dynamic Analysis という機能名称にて、シスコが提供するクラウドサービス (プライベートクラウドも可) の Threat Grid をサンドボックスとして利用する
- Talos – シスコが運営する世界最大規模のセキュリティ研究・調査基幹の名称。世界中のトラフィックやファイルを監視しており、ここで得た脅威情報をシスコの様々な製品で利用している。FTD も Talos が作った Snort Rule やセキュリティインテリジェンス情報を使っている
- CnC – Command and Control の略。ボットクライアントへの司令塔として動作するサイトやサーバのこと。ボットクライアントが侵入してしまったホストからこの CnC に接続することで、CnC からクライアントの操作や情報収集を行う
- VDB – Vulnerability Data Base の略。Talos が FTD に提供する脆弱性情報のデータベースであり、脆弱性情報以外にアプリケーション識別情報や暗号化通信パターンも含むため、FTD の根幹を構成する DB のひとつ

用語集-4

- ClamAV -オープンソースで提供されているクロスプラットフォームのアンチウイルスソフトウェアであり、Talos が作成している。FTD の Malware Defense 機能の中でも使われている
- ISE – Identity Services Engine の略。シスコが提供する高機能の RADIUS サーバであり、認証・認可が必要なあらゆる場面で利用可能

FTD とは

- Cisco の Firewall ソフトウェアのひとつ。正式名称は Firewall Threat Defense、旧名称は Firepower Threat Defense。
- 従来の Basic Firewall 兼 VPN 終端装置である ASA と、世界でいちばん使われているオープンソースの IPS エンジンである Snort ベースをベースにした NGFW + IPS + Malware 対策を足して1つのソフトウェアにしたもの。
- ハードウェアアプライアンスとバーチャルマシン (Public Cloud 含む) で稼働する
- 管理ツールとして Firewall Management Center (旧名称は Firepower Management Center、略称は FMC) を使うことで、複数の FTD をまとめて管理したり、FTD にある全ての機能を利用できるなどのメリットがある。On Premise の FMC を使わずに Firewall Device Manager (旧名称は Firepower Device Manager) や CDO (Cisco Defense Orchestrator) で管理することも可能。
- On Premise FMC で管理された FTD を利用することで、FTD のすべての機能を利用可能。

ターゲットとゴール

<ターゲット(前提知識)>

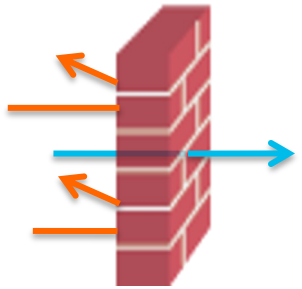
- 基本的な Firewall のことはわかっているが、それ以上のことはわからない方向け

<ゴール>

- 次世代 Firewall (NGFW) だったり、IPS といった高度なレイヤのセキュリティ対策をその Firewall に含めたいといった要件に対して、FTD の基本と特長を簡単に説明できるようになること。

FTD が必要となる背景と課題

- 基本の Firewall に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

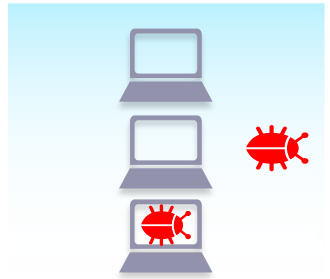
ファイアウォール

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



サンドボックス

FTD の主要機能の紹介

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

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

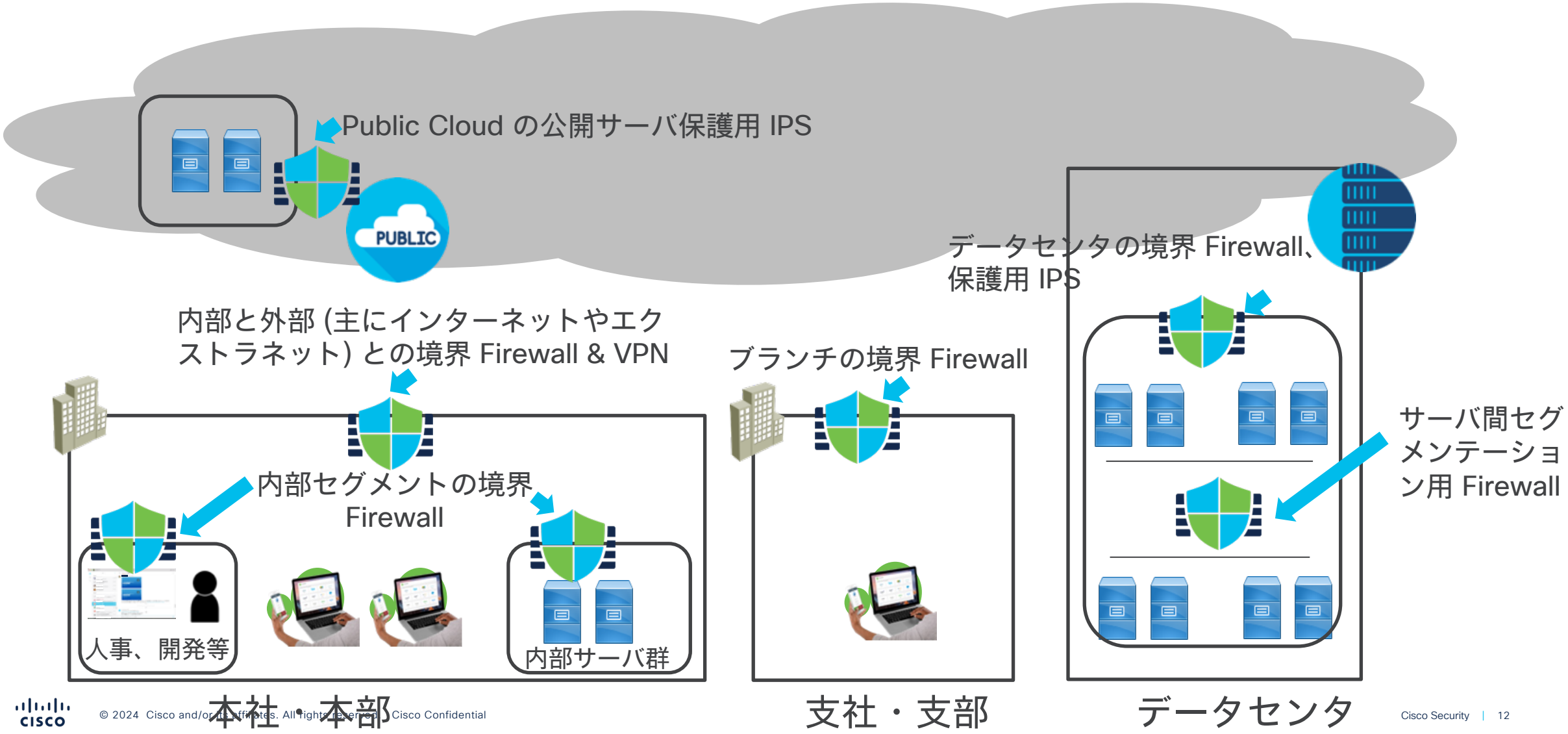
本当に必要な脅威対策としての IPS

・「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



Firewall は ASA か FTD か？

- Firewall ハードウェアアプライアンスは 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 (ルータの方が高性能)	○	○
IPS / IDS	X	◎
AVC, URL Filter	X	◎
Malware 対策	X	◎
暗号化通信対策 (SSL / TLS 復号, EVE*)	X	◎
CLI での設定	◎	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

EVE* = Encrypted Visibility Engine, 復号せずに暗号化通信の一部を特定

FTD の代表的な機能の紹介
ネットワークの学習と可視化

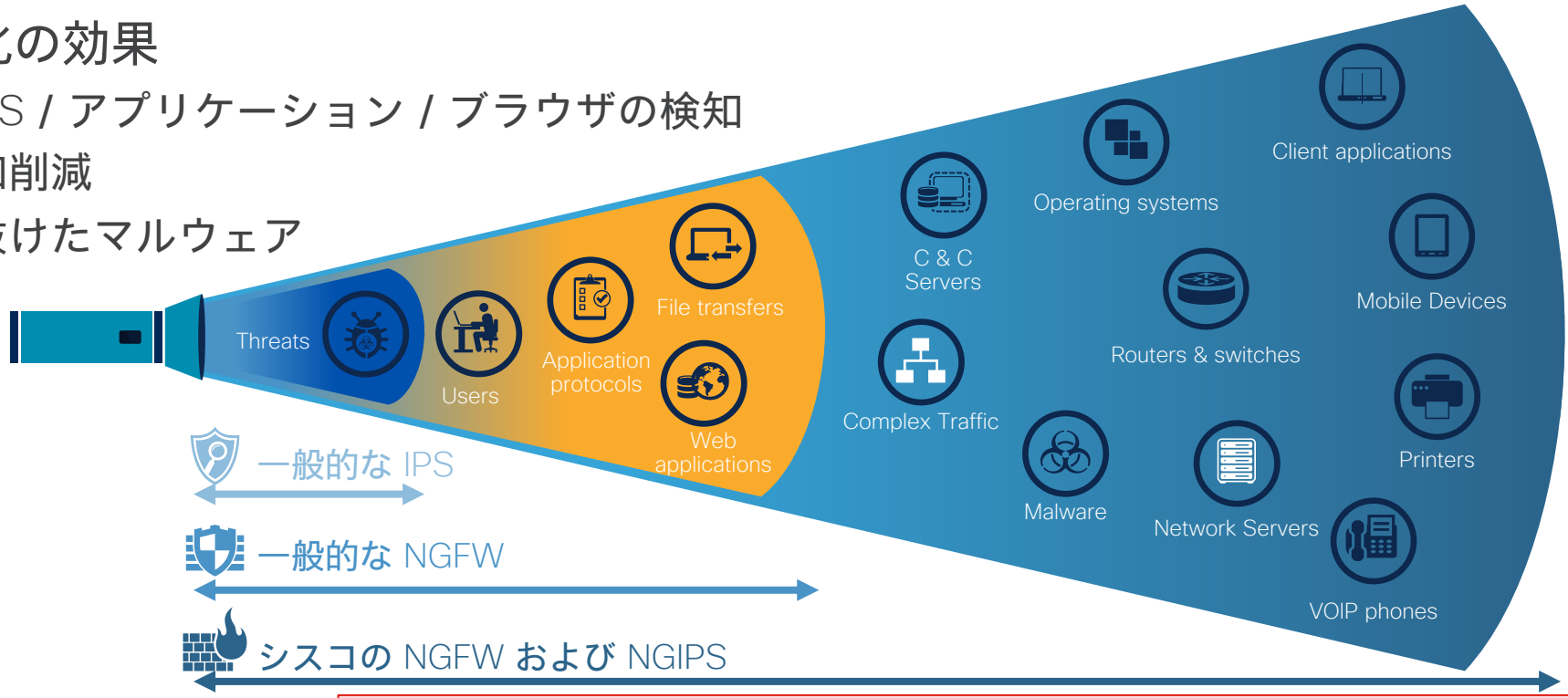
- 決められたネットワークの範囲内で、FTD が流れているトラフィック情報を FMC に送る。FMC はその情報を各種データベースに照らし合わせ、どのような OS やアプリケーションが使われているか、どのようなユーザが利用しているか等の情報を学習し、可視化する

- 可視化の効果

  古いOS / アプリケーション / ブラウザの検知

  誤検知削減

  すり抜けたマルウェア



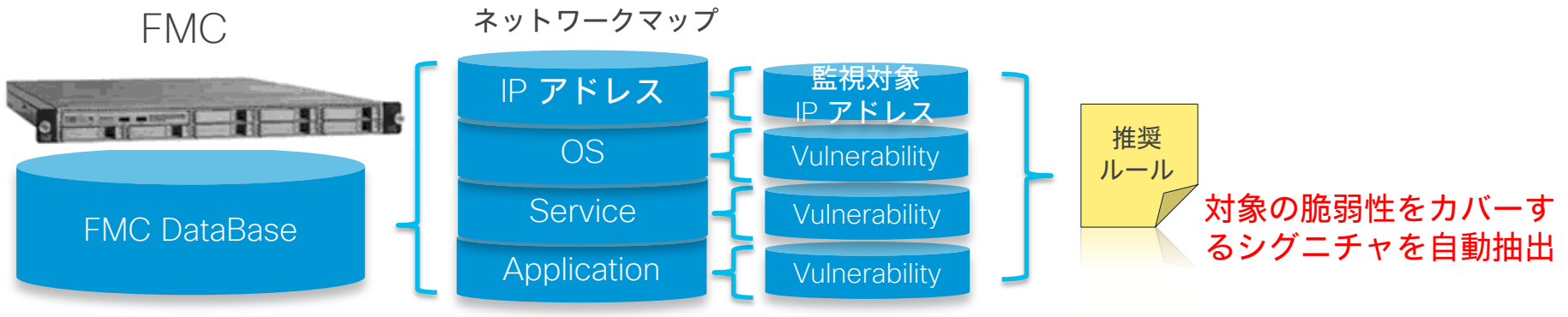
✓ 守るネットワークの範囲に存在する OS やアプリケーション情報を学習することで、後述の IPS 自動チューニングやインパクト解析に利用

FTD の代表的な機能の紹介
IPS 自動チューニング

イチオシ!!

- 学習した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/・ルールをのみを有効化することにより、誤検知を大幅削減

FTD の代表的な機能の紹介
IPS インパクトフラグ

イチオシ!!

- 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	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				
0				

✓ 同じ攻撃でもターゲットによって異なる危険度であることを瞬時に判断可能

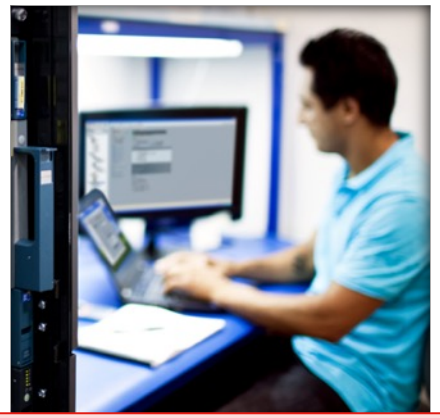
FTD の代表的な機能の紹介
IPS 運用の悩みを解決

イチオシ!!

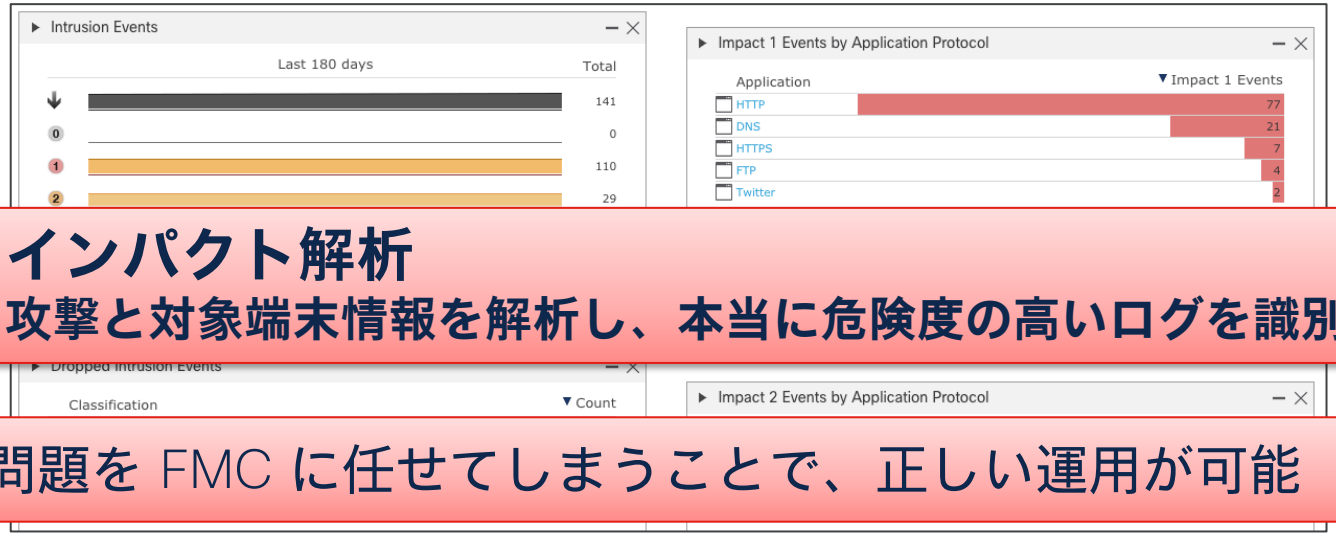
一般的な侵入検知機器 (IPS) の運用者が抱える問題

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

✓ IPS を導入しても運用しきれない問題を FMC に任せてしまうことで、正しい運用が可能

FTD の代表的な機能の紹介
Security Intelligence 脅威情報フィルタ

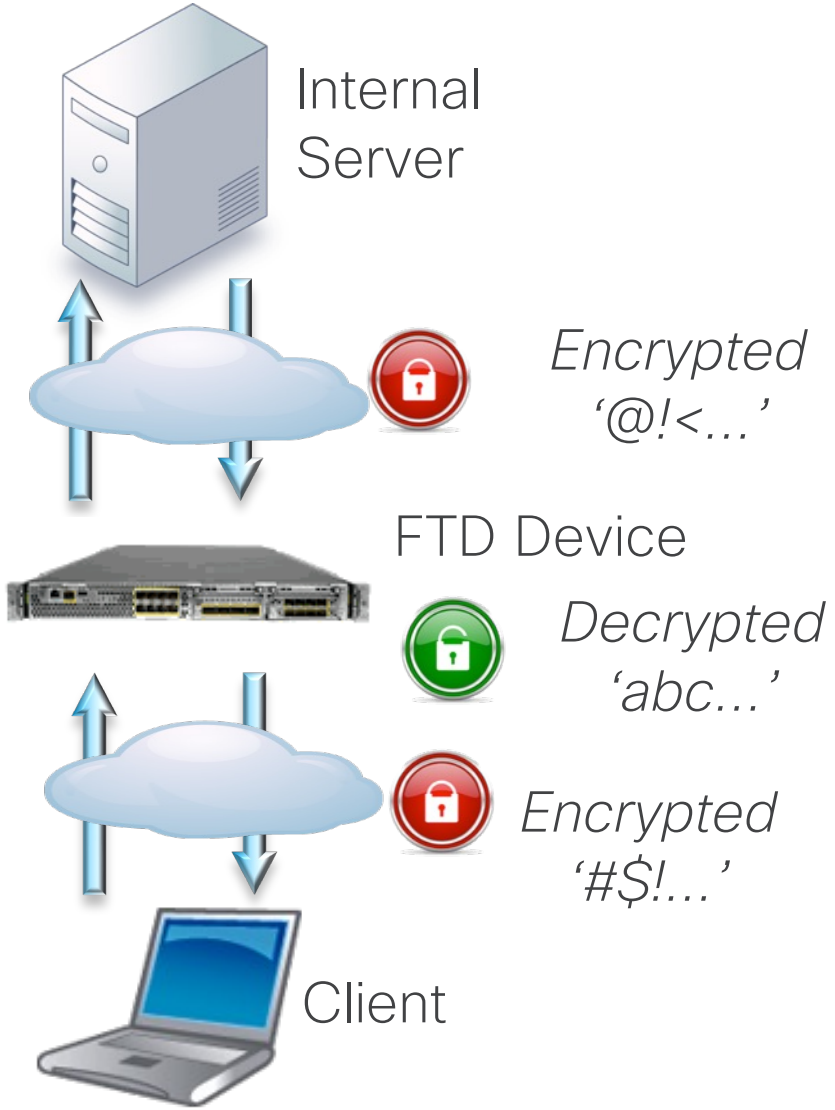
- Cisco Collective Security Intelligence 提供のブロックリスト IP アドレス、URL、ドメインに基づく制御 (i.e. レピュテーション)
- 既知のブロックリスト宛て or からのコネクションを　モニターもしくはブロック
- カテゴリー
  - CnC
  - Malware
  - Phishing
  - Bots
  - Attackers

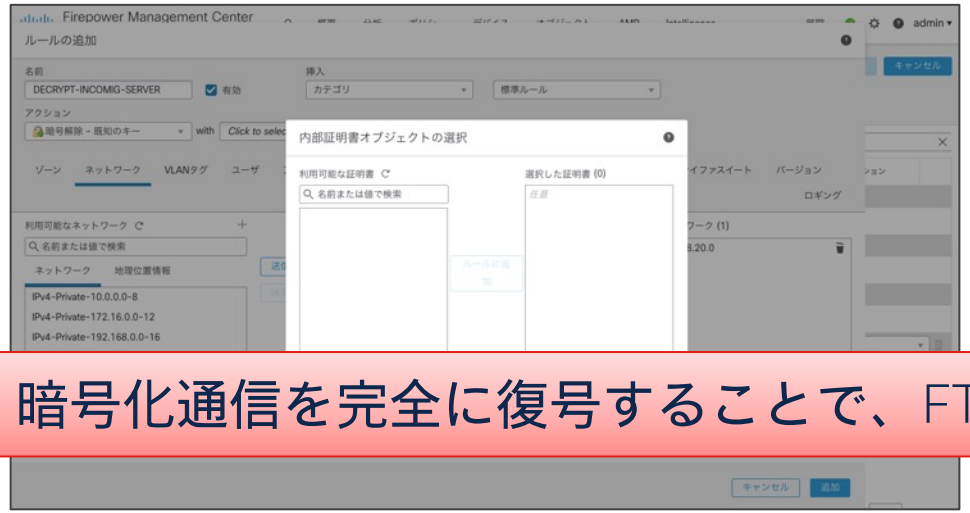
    など

✓ パケットヘッダだけでインスペクションが行われるため FTD の処理負荷が軽い

FTD の代表的な機能の紹介
TLS Decryption

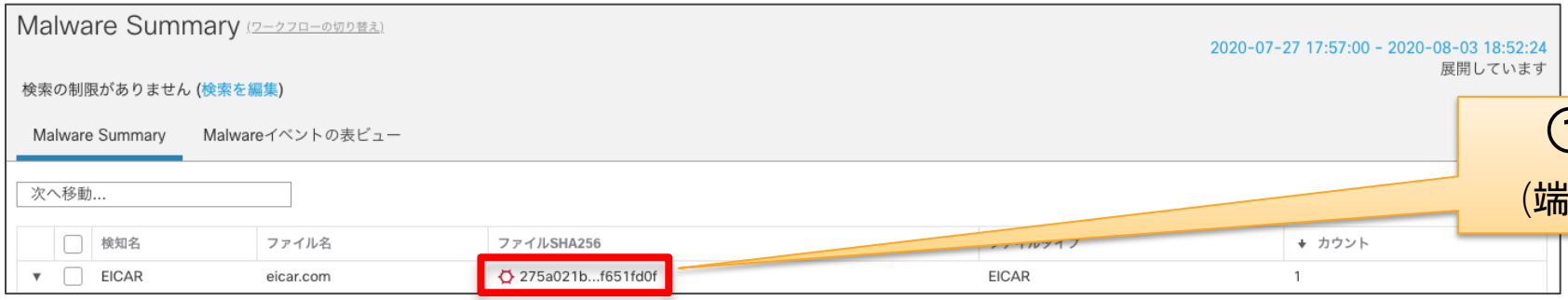
- TLS で暗号化された通信を復号してインスペクションを行う機能
  - inbound inline
  - outbound inline
- ハードウェア処理が可能なモデルと不可能なモデルがあるため、パフォーマンス見積もりに注意
- TLS 1.3 ネイティブにも最新バージョンにて対応済み。TLS 1.2 にダウングレードしてのインスペクションも可能



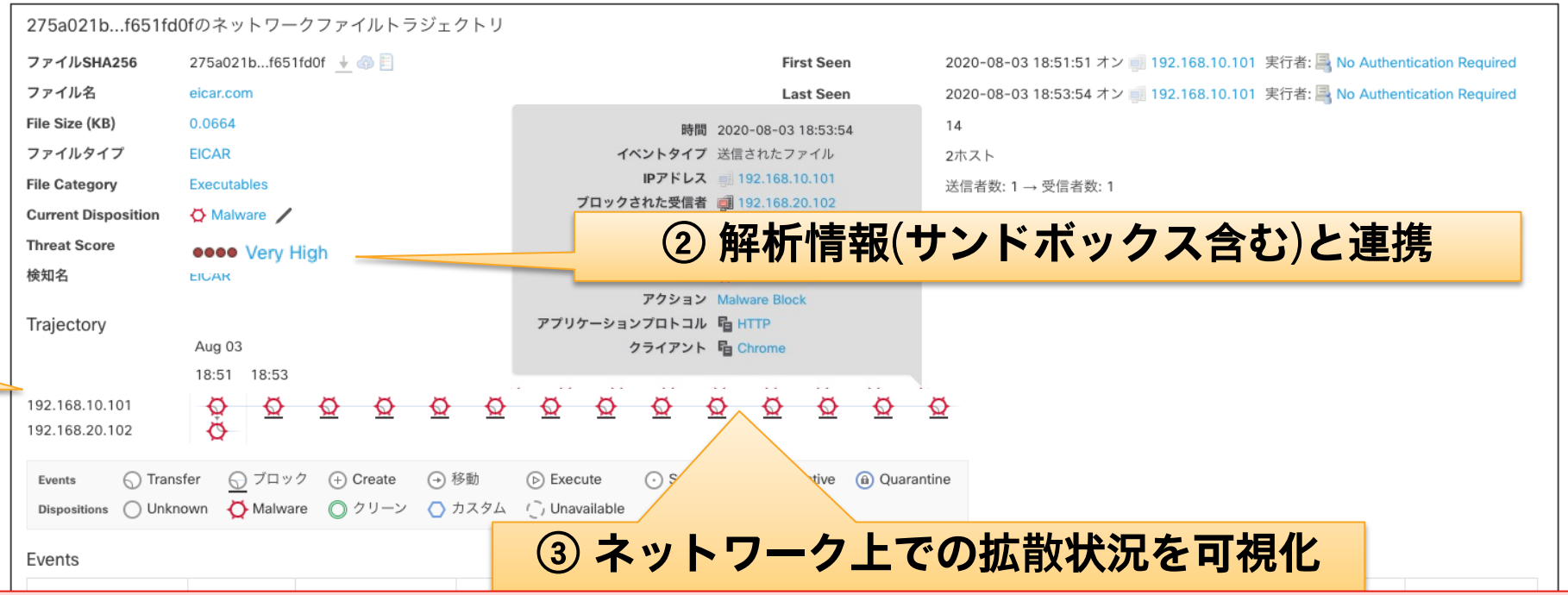


✓ 暗号化通信を完全に復号することで、FTD のセキュリティ機能を全て利用可

FTD の代表的な機能の紹介
Malware Defense – 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

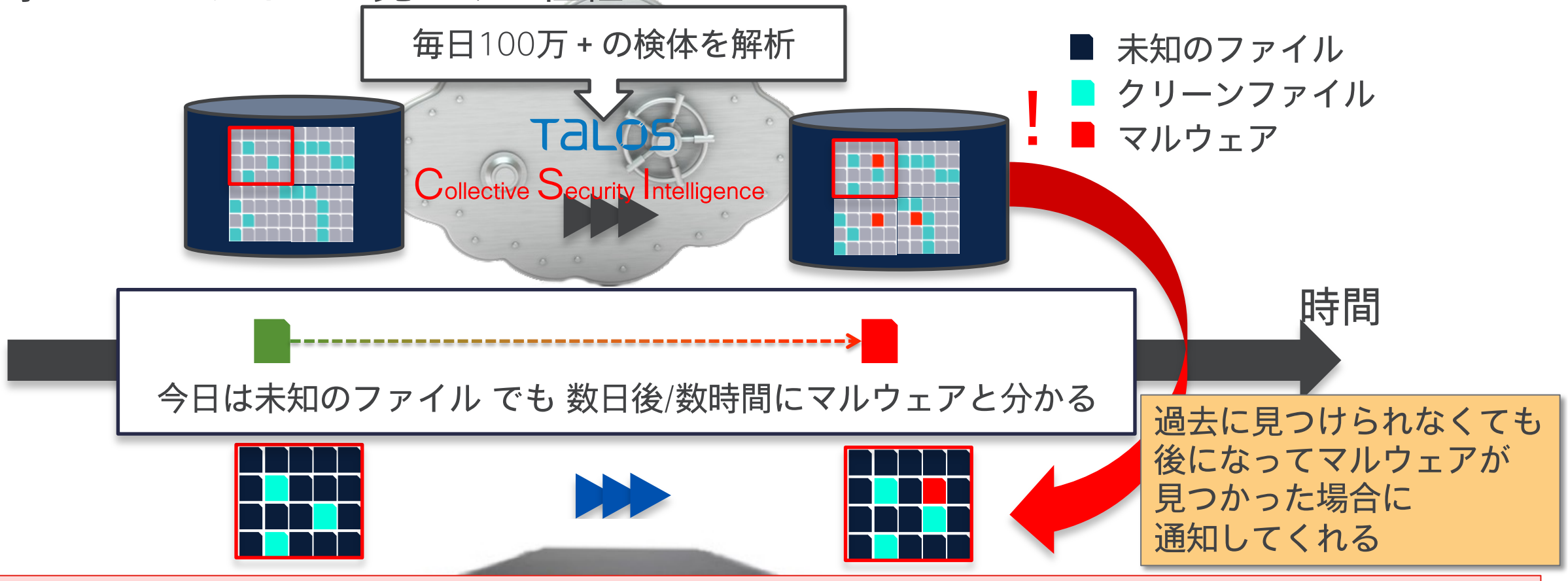
③ ネットワーク上での拡散状況を可視化

④ 端末の特定

✓ネットワーク側でもマルウェアの検知を行うことで、エージェントが導入できないエンドポイントや IoT デバイス宛てのマルウェアも含め、ファイルの行方を追跡することが可能

FTD の代表的な機能の紹介
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



✓ 一度チェック済みのファイルでも、後からマルウェアと判断されることで、内部での追跡に役立つ

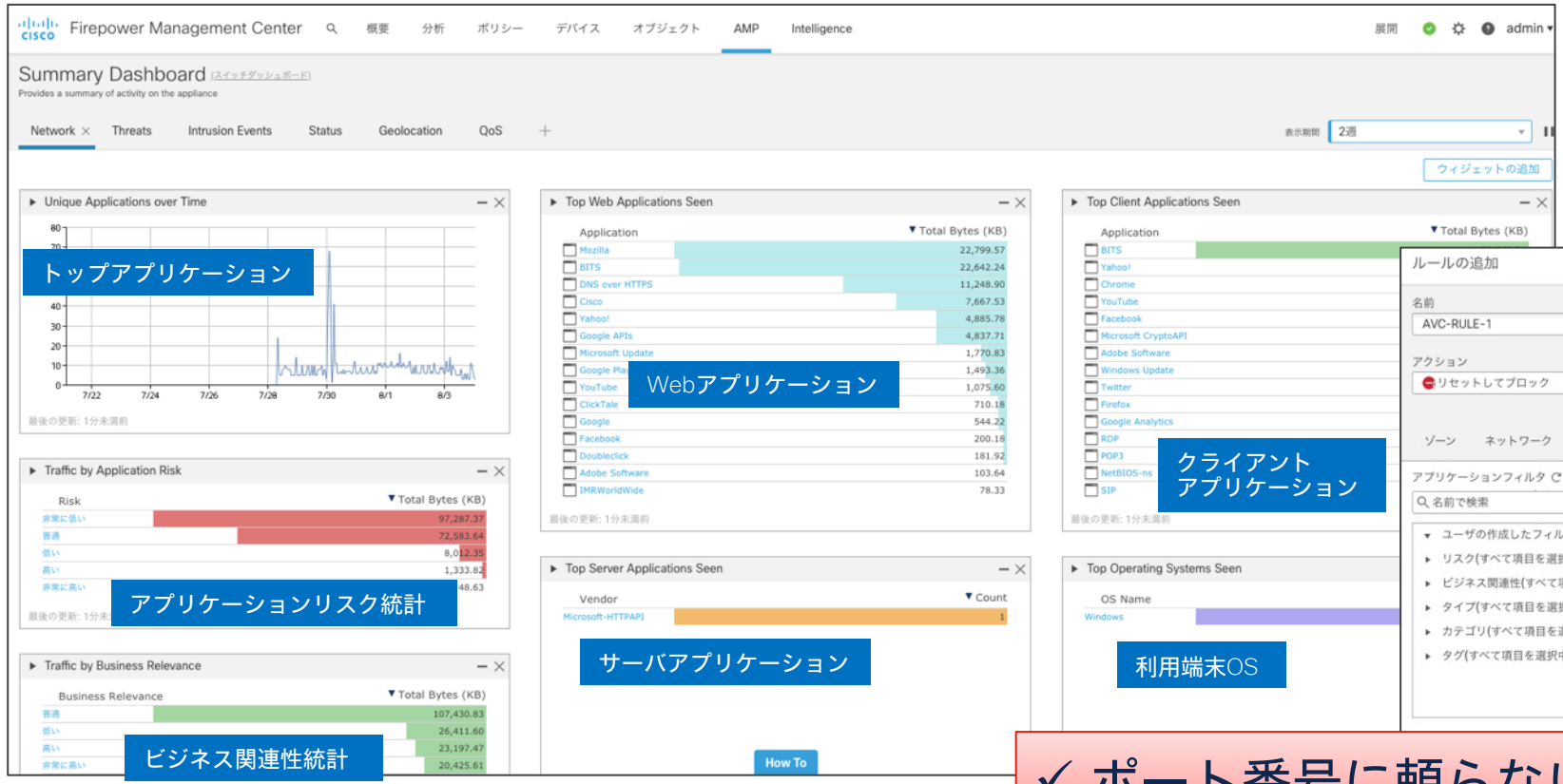
FTD の代表的な機能の紹介

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 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



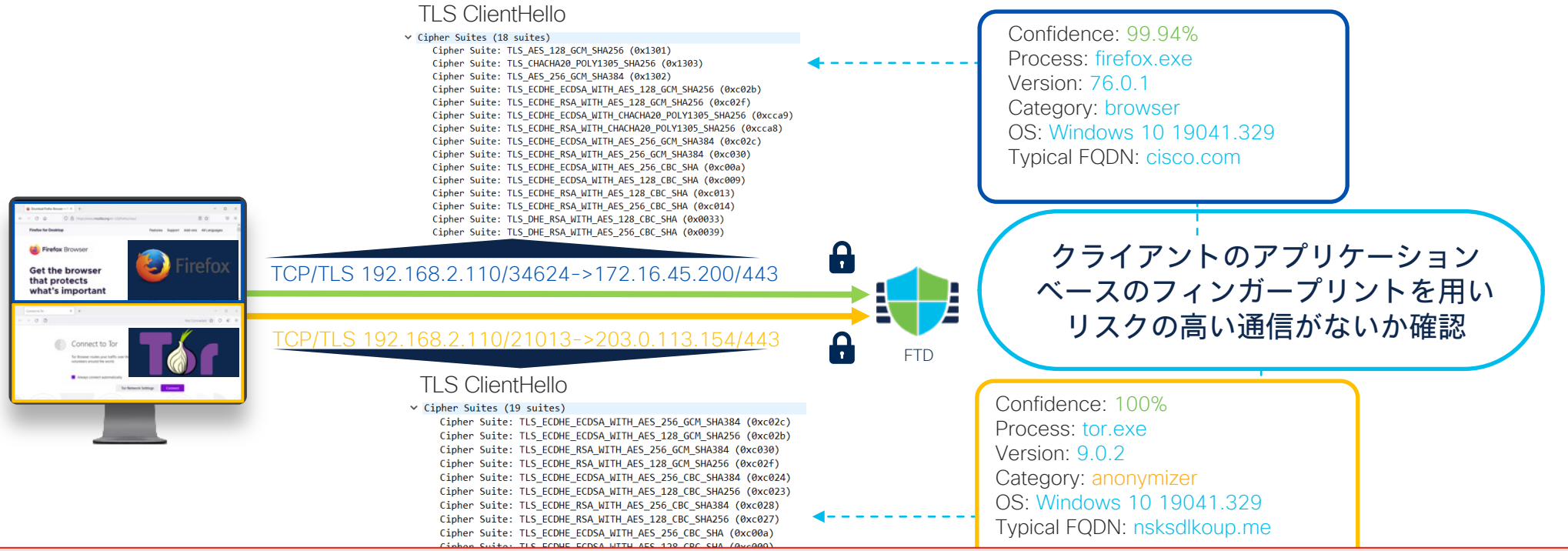
✓ ポート番号に頼らないアプリケーションの検知が可能

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

FTD の代表的な機能の紹介
Encrypted Visibility Engine

イチオシ!!

- 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

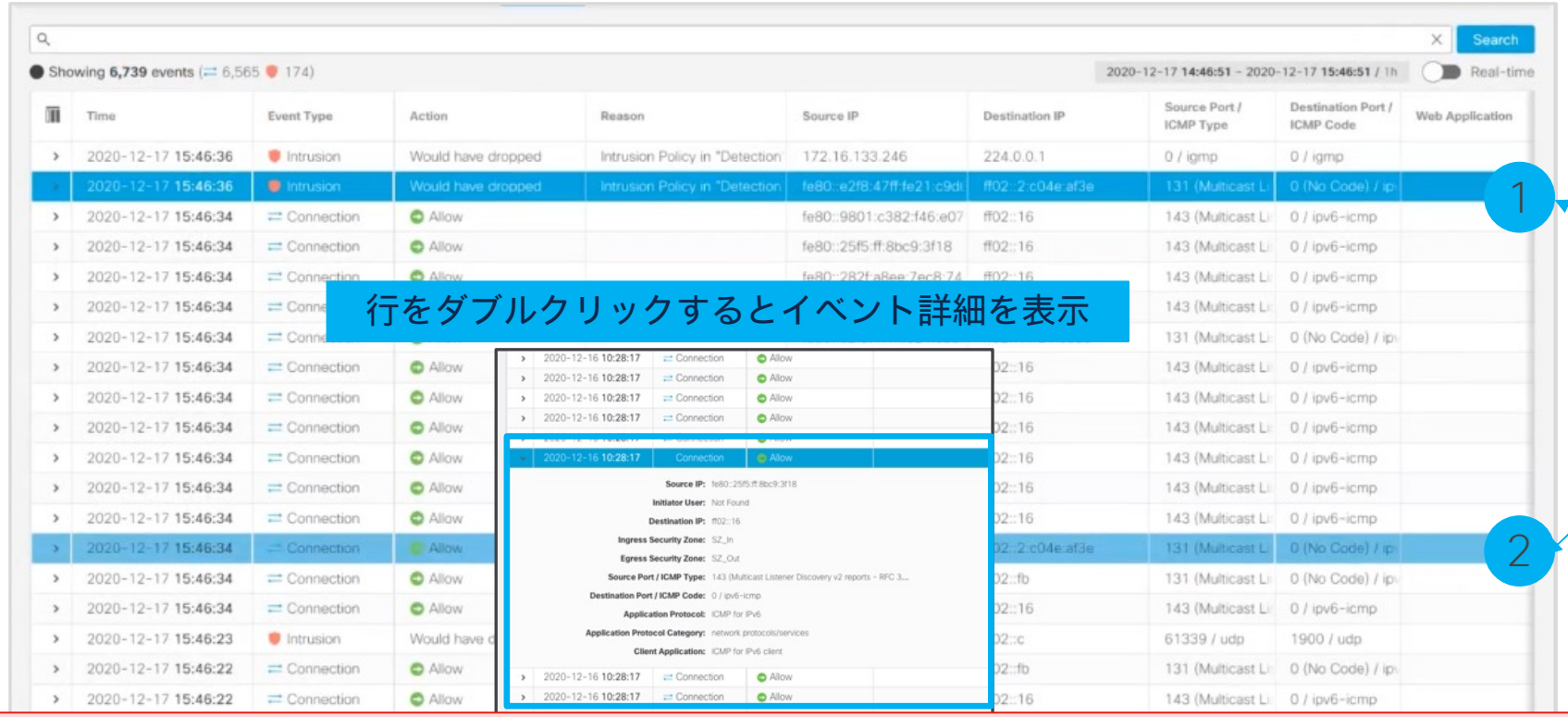


✓ FTD の負荷が上昇する TLS Decryption を使うことなく、危険なクライアントやアプリケーションを検知することが可能

FTD の代表的な機能の紹介
Unified Event Viewer

イチオシ!!

- 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

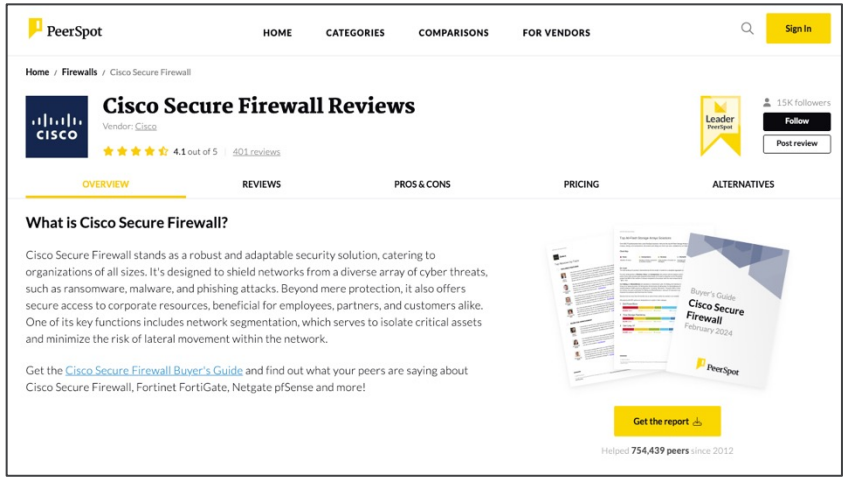


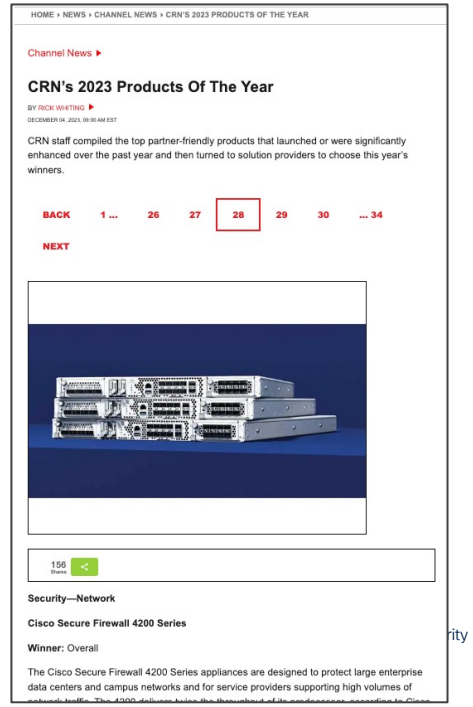
真の相関分析
Intrusion Event を選択すると、関連する Connection Event もハイライトされる

✓ 複数のイベントビューワをまたいでチェックすることなく、起きた事象を確認することが可能

第三者評価補足資料

- SE Labs の年次レポート 2023 にて次世代ファイアウォール部門最優秀賞に選出
  https://gblogs.cisco.com/jp/2023/08/se-labs-2023-annual-security-report-names-cisco-as-best-next-generation-firewall/
- Cisco Secure Firewall が 2023 PeerSpot Tech Leader Award を受賞
  https://www.peerspot.com/products/cisco-secure-firewall-reviews
- Cisco Secure Firewall 4200 シリーズが CRN's 2023 Products of the Year の Overall Winner に選出
  https://www.crn.com/news/channel-news/crn-s-2023-products-of-the-year?page=28





FTD のまとめ

- 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

ネクストステップ

- 全体説明、概要説明、デモガイド

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

  PSU-VoD-SEC-Cisco Secure Firewall Threat Defenseライセンス解説-FTD license

  PSU-VoD-SEC-dCloud を利用した Firewall Management Center 7.1 デモ-Firewall DEMO

- 設定資料

  Firewall Threat Defense (FMC 管理) Version 7.0 初期セットアップガイド Vol. 1 初期インストール編

  Firewall Threat Defense (FMC 管理) Version 7.0 初期セットアップガイド Vol. 2 基本セキュリティポリシー設定編

  Firewall Threat Defense (FMC 管理) Version 7.0 初期セットアップガイド Vol. 3 応用設定編

  Firewall Threat Defense (FMC 管理) Version 7.0 初期セットアップガイド Vol. 4 管理・監視・冗長構成編

  PSU-VoD-SEC-FTDで始めよう RAVPN 各機能の設定例-Remote Access VPN

  Cisco Firewall Threat Defense V7.0 FDM管理用 設定パラメータシート

  PSU-VoD-SEC-Firewall Threat Defense を Cisco Defense Orchestrator に簡単に登録する方法

  PSU-VoD-SEC-Cloud Delivered Firewall Management Center 設定サンプルガイド

  [必見!] シスコサポートコミュニティ セキュリティ – Firewall Threat Defense テクニカルドキュメント

補足資料

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

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

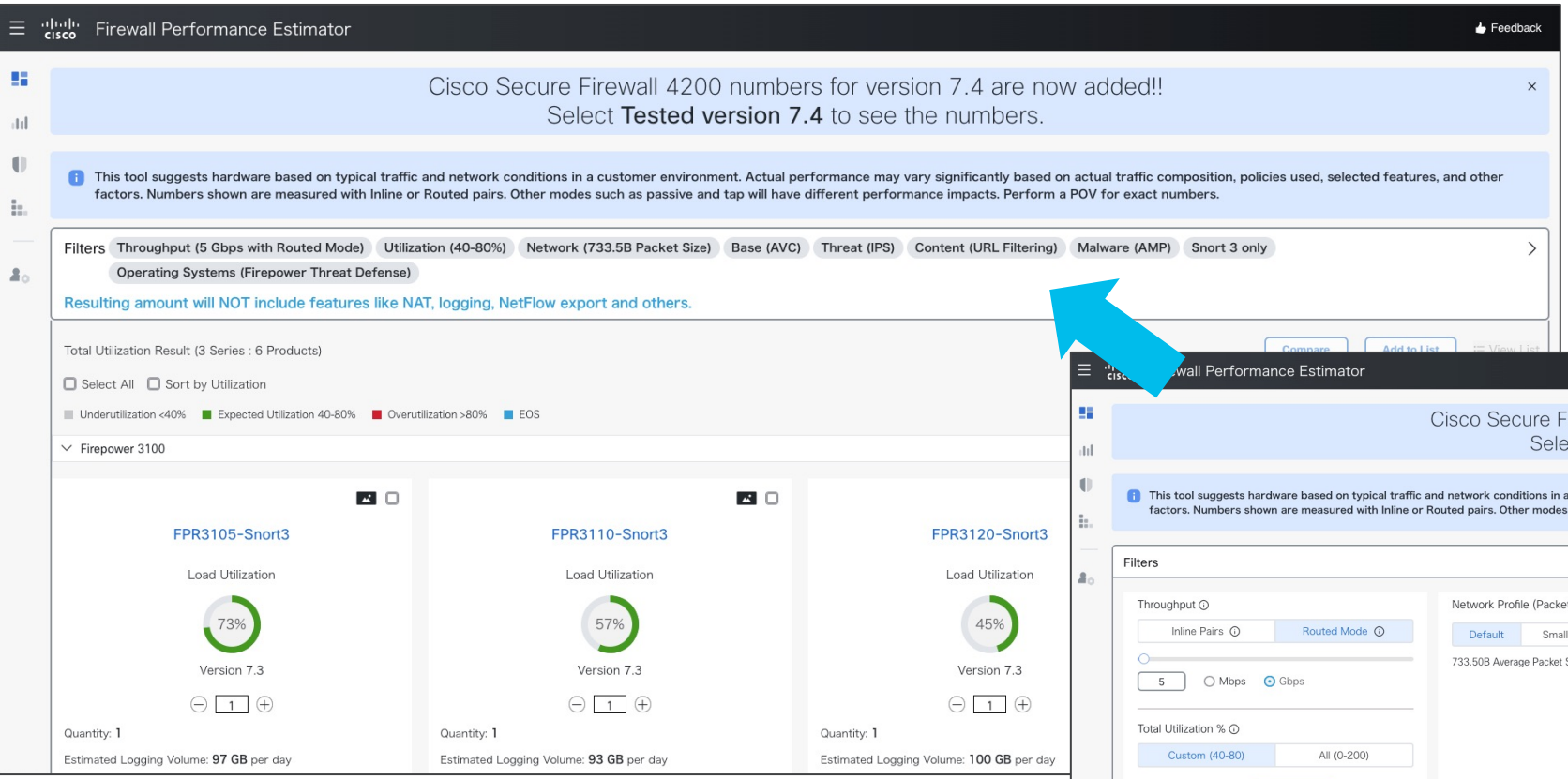
FMC4700
最大 750個のセンサー管理
最大イベント数 3億件
3.2TB のイベントストレージ
最大 60万ホスト、60万ユーザのネットワークマップ
HA対応

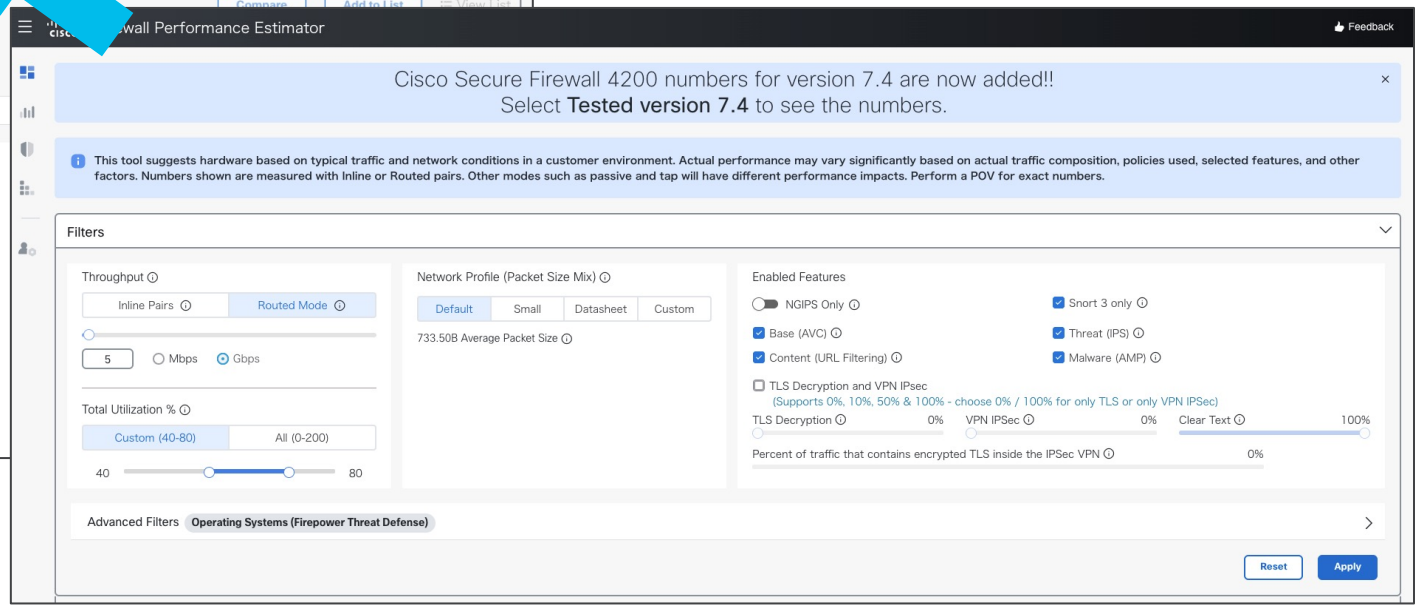
Virtual FMC
最大 25個のセンサー管理
最大イベント数 1,000万件
250GB のイベントストレージ
最大 5万ホスト、5万ユーザのネットワークマップ
300個のセンサー管理対応モデルも有り (FMCv300)
HA対応 (VMware のみ)

FTD の機能を最大限に引き出す管理サーバ

NGFW Performance Estimator

- 様々なトラフィックパターンや条件を組み合わせ、実測値に近い (データシートよりもより現実的な) サイジングが可能





パートナー権限以上の cisco.com アカウントが必要

https://ngfwpe.cisco.com

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

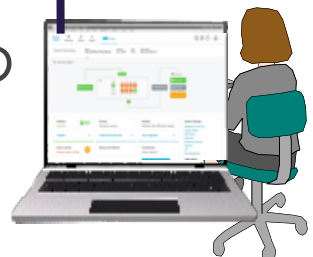
基本的なセキュリティポリシーを、シンプルに1つの FTD に対して実施

FTD 本体

https
ブラウザで管理・設定

FDM
= Firewall Device Manager

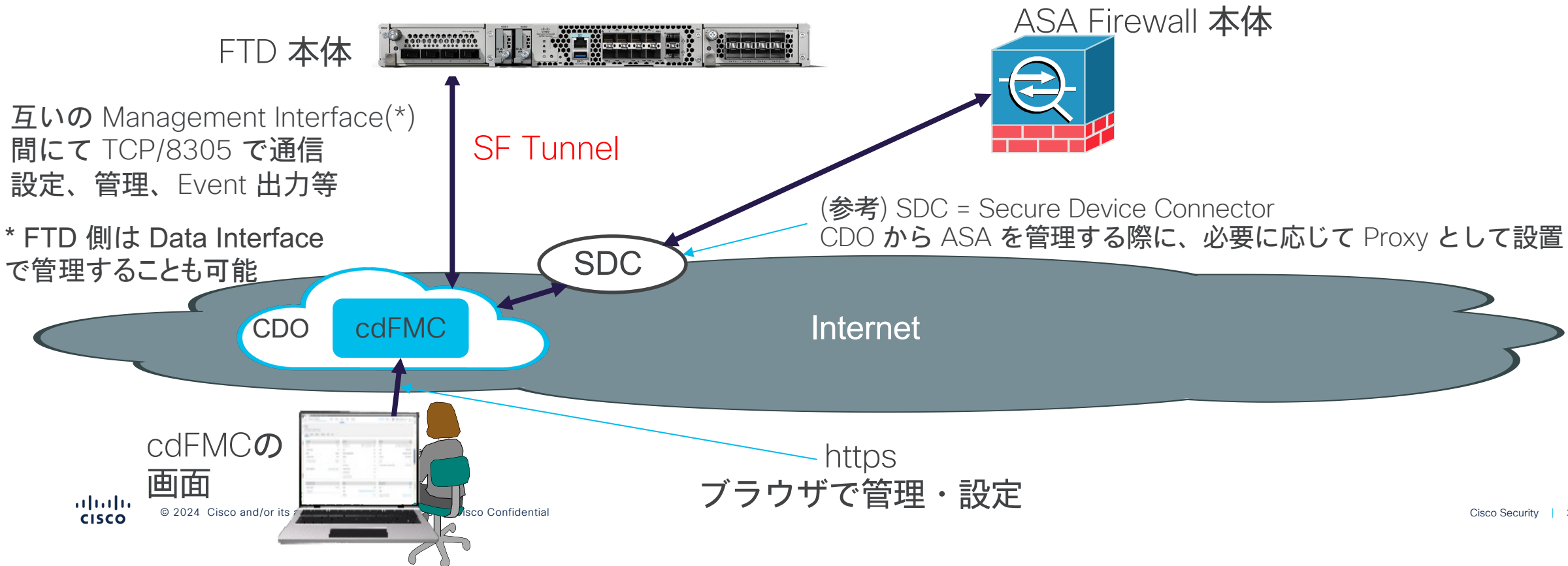
FDMの画面



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



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、Firewall ハードウェア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

- Cisco 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

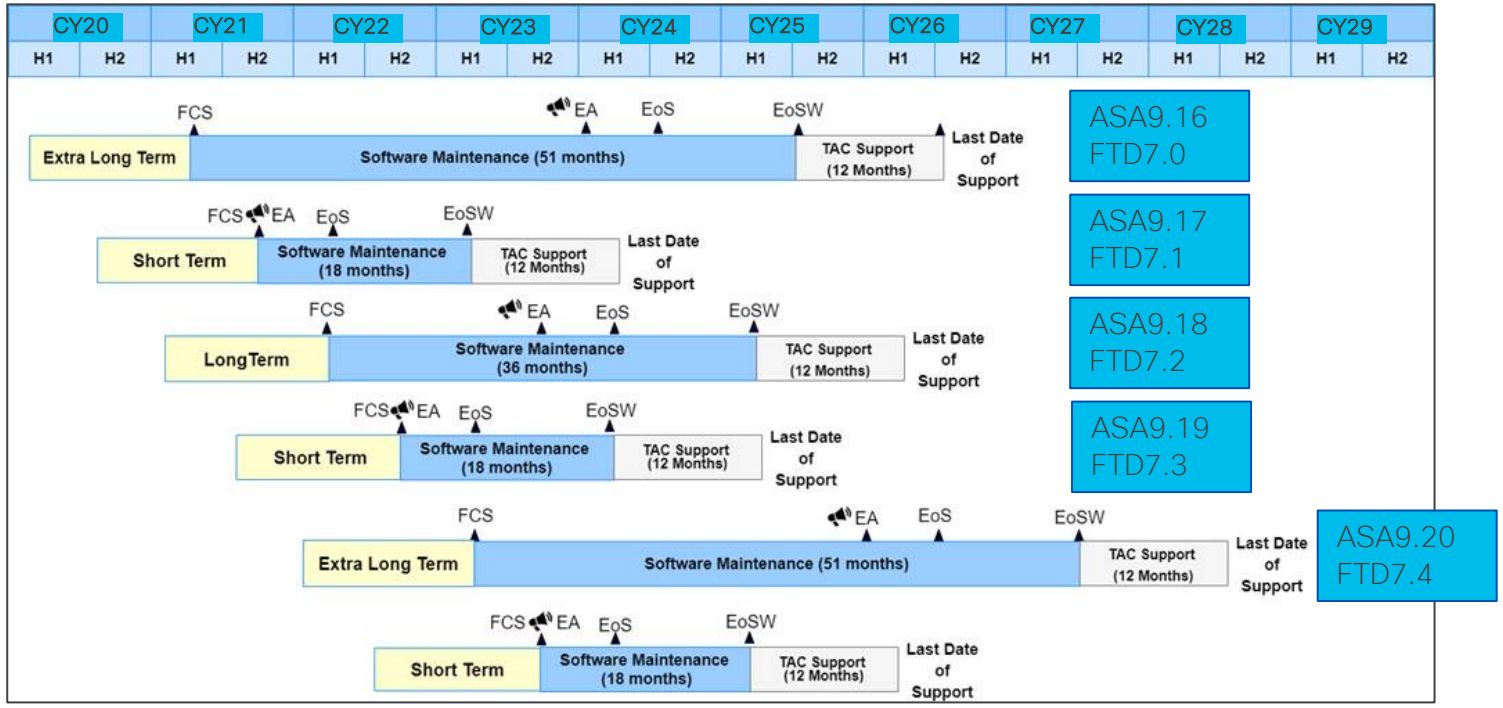
  管理する FTD の数をデバイスのモデル別にそれぞれ 1,3,5年のサブスクリプションライセンスで購入

  詳細はオーダーガイド参照

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

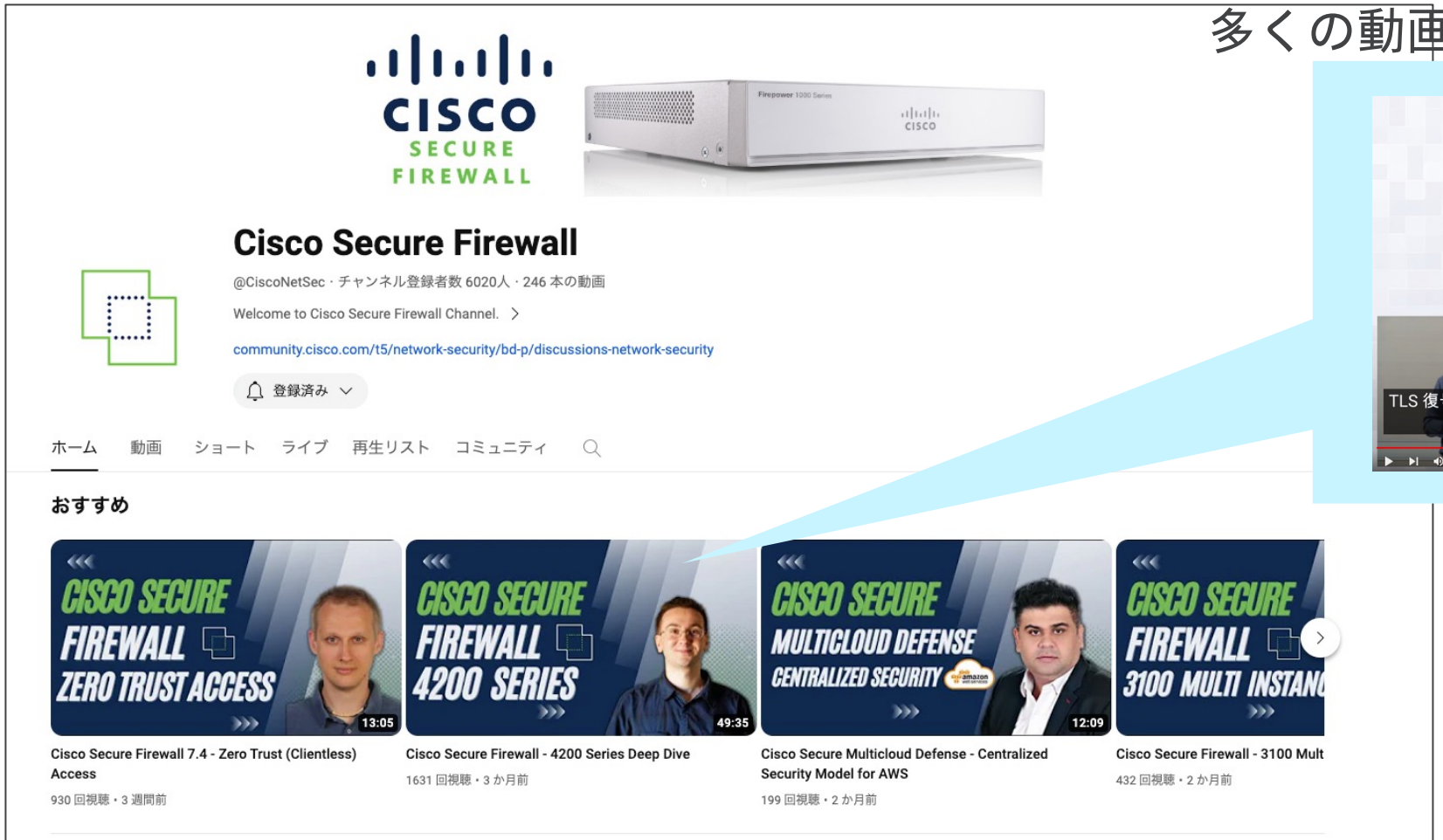
- FTD (ASA も) のバージョンの数字の小数点1桁目が偶数ならロングタームサポート、奇数ならショートタームサポートとなる
  - FTD 7.3 → ショートタームサポート
  - FTD 7.2 → ロングタームサポート
- ロングタームサポートの中でも、2年に1度リリースされるものはエクストラロングタームサポートとなる
  - FTD 7.0 → エクストラロングタームサポート
  - FTD 7.4 は次のエクストラロングタームサポートの候補

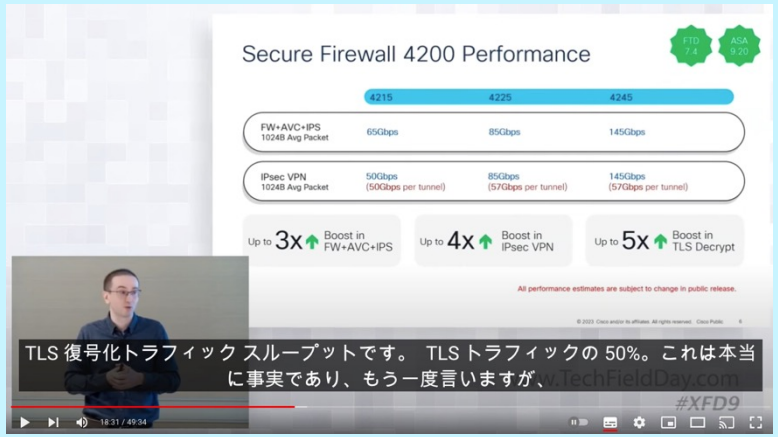


Cisco Secure Firewall 新機能解説動画

- 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