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

2024年5月

シスコシステムズ合同会社
セキュリティ事業 ソリューションズエンジニア
小林 達哉 (tatskoba@cisco.com)

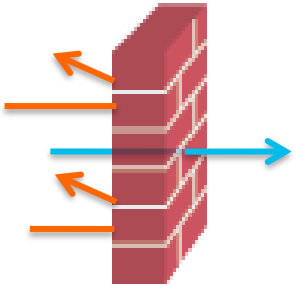
アジェンダ

- Firewall Threat Defense の概要
- Firewall プラットホーム
- まとめ

Firewall Threat Defense の概要

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

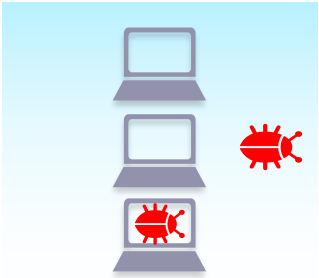
Web アプリケーション、ユーザ、脅威の可視化

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

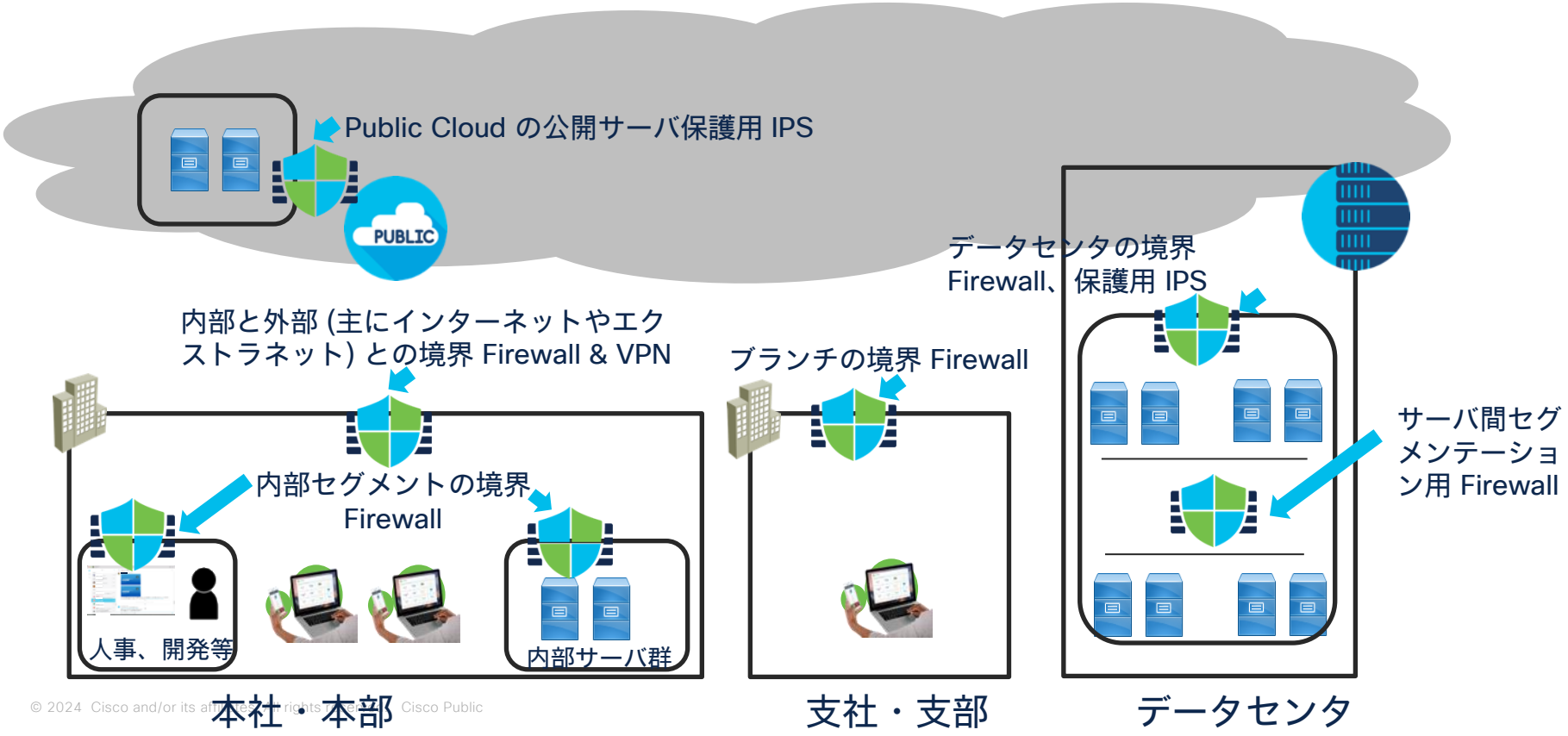
・「とりあえず動かすだけ」の IPS からの卒業。本当に必要な脅威対策を IPS で実施

- **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

2024-05-16 11:16:08	medium	脆弱	Block	192.168.10.71	192.168.150.72	65040 / udp	53 (domain) / udp	INDICATOR-SCAN DNS version.bind string information disclosure attempt (1:42785:4)
2024-05-16 11:13:59	medium	脆弱	Block	192.168.10.71	192.168.150.72	64492 / udp	53 (domain) / udp	INDICATOR-SCAN DNS version.bind string information disclosure attempt (1:42785:4)
2024-05-16 11:08:23	medium	脆弱	Block	192.168.10.71	192.168.150.72	62623 / udp	53 (domain) / udp	INDICATOR-SCAN DNS version.bind string information disclosure attempt (1:42785:4)

ホストプロファイル

ホストのスキャン　許可リストプロ

IPアドレス 192.168.150.72
NetBIOS名
デバイス (Hop) FTDv74-1 (1)
MACアドレス(TTL) 00:50:56:8F:9B:76 (VMware, Inc.) (255)
ホストタイプ NAT Device
最後の発見 2024-05-20 16:03:09
現在のユーザ Discovered Identities\anonymous (FTP)
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 | ファイルイベント | マルウェアイベ

クライアント アプリケーション

アプリケーション (16)

アプリケーションプロトコル	クラ		ーション
YouTube	Chrome		
QUIC	Chrome		
HTTP/3	Chrome		
HTTP/3	Chrome	123.0.0.0	
DNS	DNS		
HTTPS	Firefox		
HTTPS	Java Update		
HTTPS	Office 365		
SSL	SSL client		
HTTPS	SSL client		
HTTP	BITS	7.8	Web Browsing
HTTP			
HTTP			
HTTP			
HTTP			
HTTP			

侵入の痕跡

侵入の痕跡 (2)　ルール状態を編集する　すべ

カテゴリ	イベントタイプ	説明	最初の発見	最後の発見
Suspicious Activity	Encrypted Visibility Engine	Probable Malware Communication	2024-05-15 17:20:11	2024-0 16:03:1
Impact 2 Attack	Impact 2 Intrusion Event - attempted-user	The host was attacked and is potentially vulnerable	2024-05-15 18:18:05	2024-0 18:18:0

該当脆弱性リスト

脆弱性 (684)　脆弱性を編集する

名前		ポート
<p>A remote code execution vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling applicat		Windows 10 20h2.x, 10 21h1.x, 10 21h2.x, 10 22h2.x, 11 21h2.x, 11 22h2.x
<p>An elevation of privilege vulnerability exists because of overly permissive Access Control Lists (ACLs) on multiple system files, including the Security Accounts Manager (SAM) database. An attacker who successfully exploited this vulnerability could ru		Windows 10 20h2.x, 10 21h1.x, 10 21h2.x, 10 22h2.x, 11 21h2.x, 11 22h2.x
<p>Microsoft is investigating reports of a remote code execution vulnerability in MSHTML that affects Microsoft Windows. Microsoft is aware of targeted attacks that attempt to exploit this vulnerability by using specially-crafted Microsoft Office document	Yes	Windows 10 20h2.x, 10 21h1.x, 10 21h2.x, 10 22h2.x, 11 21h2.x, 11 22h2.x
A buffer overflow vulnerability while parsing "application/http-index-format" format content when the header contains improperly formatted data. This allows for an out-of-bounds read of data from memory.	Yes	Firefox

端末 OS

システム (1)　オペレーティングシ

ハードウェア	OSベンダー	OS製品	OSバージョン	送信元
	Microsoft	Windows	10 20h2.x, 10 21h1.x, 10 21h2.x, 10 22h2.x, 11 21h2.x, 11 22h2.x	Firepower

サーバ アプリケーション

サーバ (25)

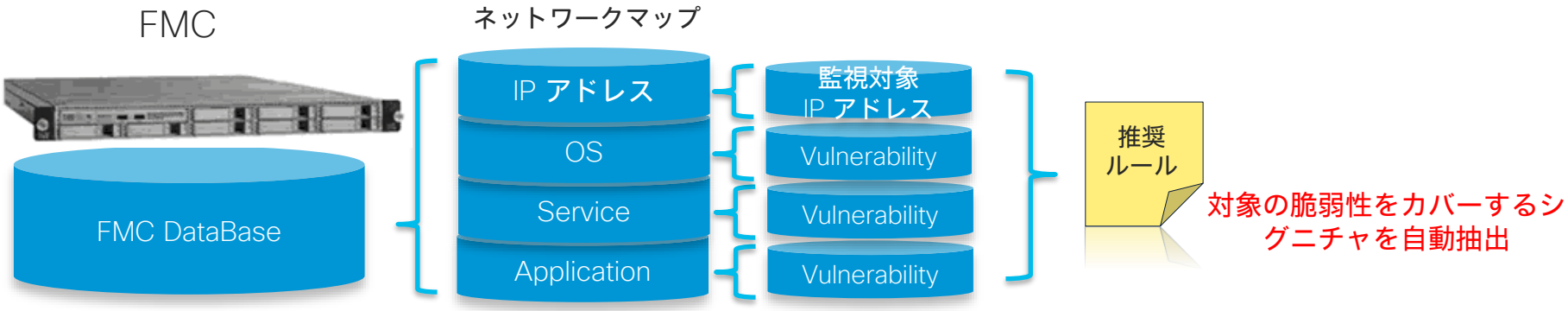
プロトコル	ポート	アプリケーションプロトコル	製造元およびバージョン
udp	5060	SIP	
tcp	49668	Kerberos	
tcp	4		
udp	1		

✓ 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

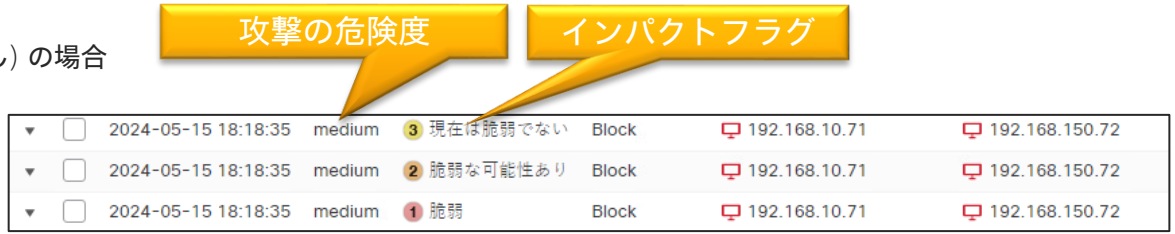
✓ ネットワークの変化に対応し、設定を自動更新



✓ 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

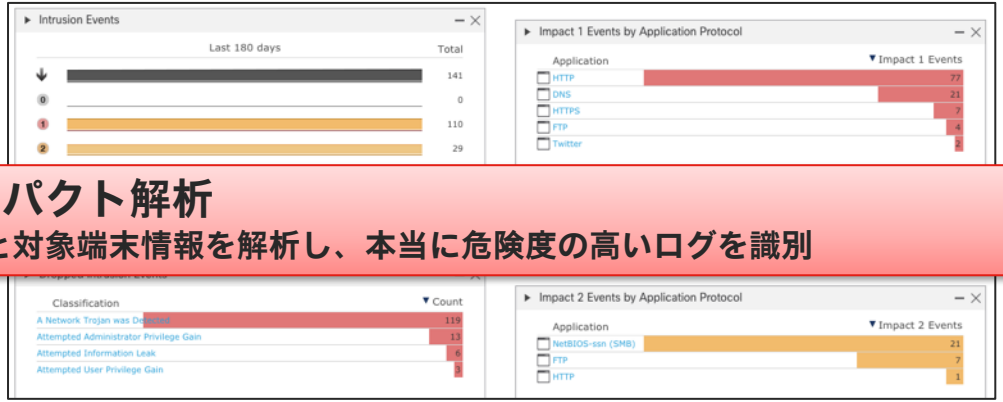
自動チューニング(推奨設定)とインパクト解析

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・・・

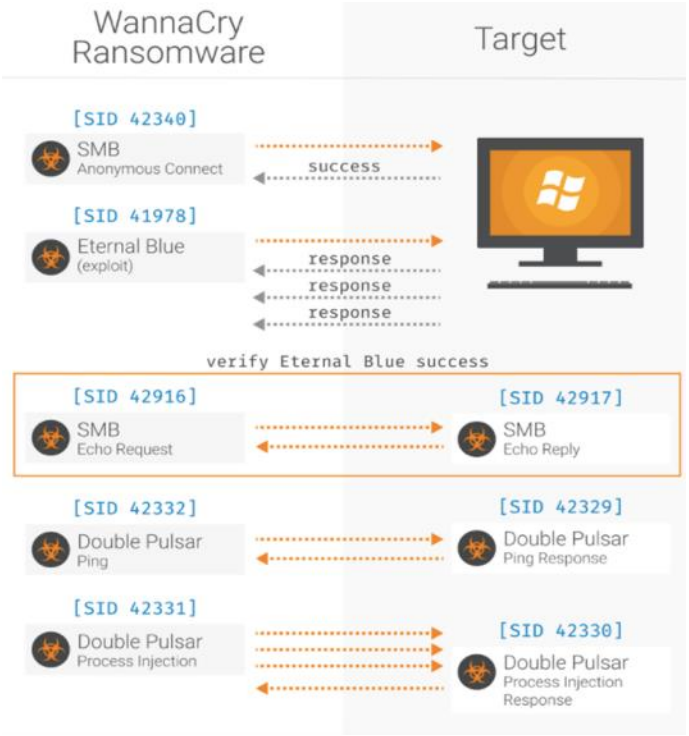
自動チューニング(推奨設定)
ネットワーク環境を学習し、
最適な推奨設定を自動生成



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 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		✔

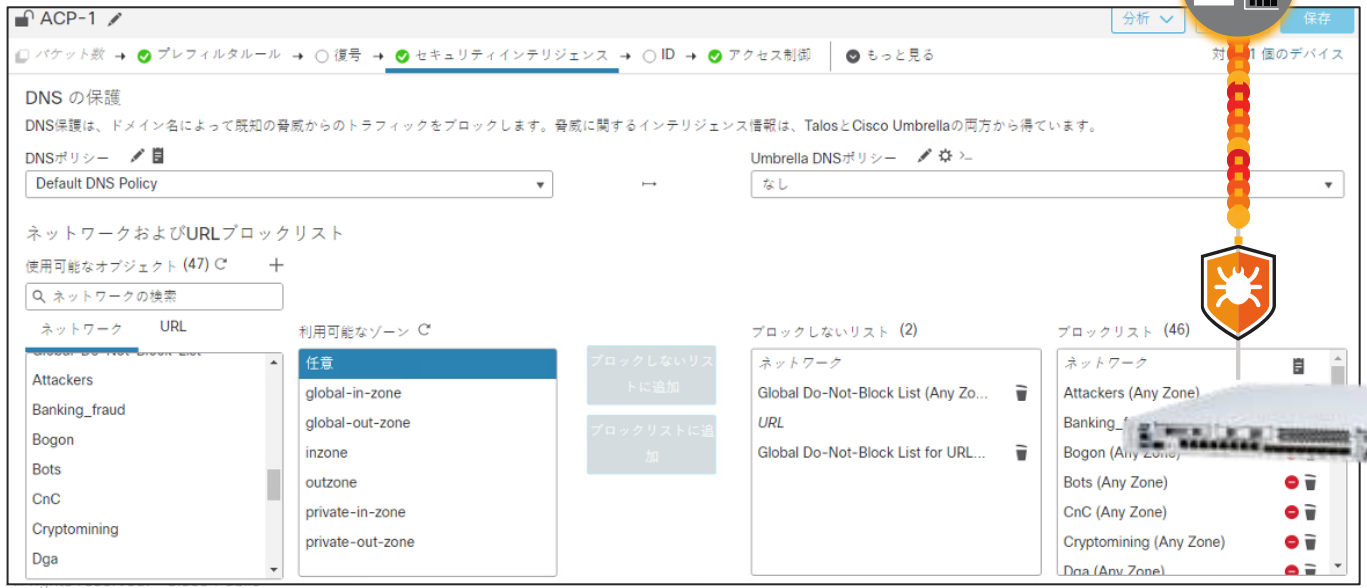
Snort 2 に比べて Snort Process Restart の必要なケースが大幅に減少
通常のポリシー設定や DB 更新においては Snort Process Restart が不要

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

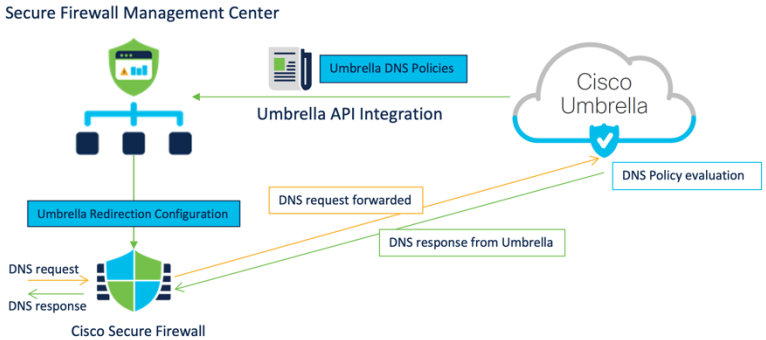
    など



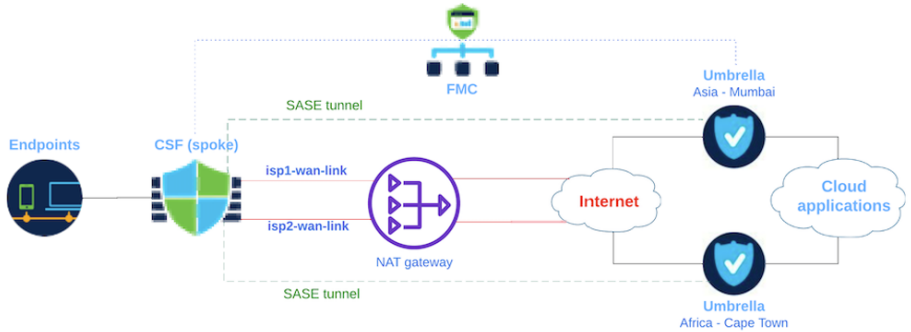
Umbrella とのインテグレーション

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

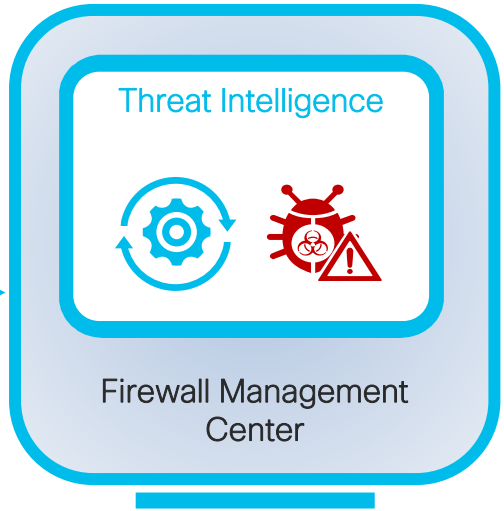


Threat Intelligence Director

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

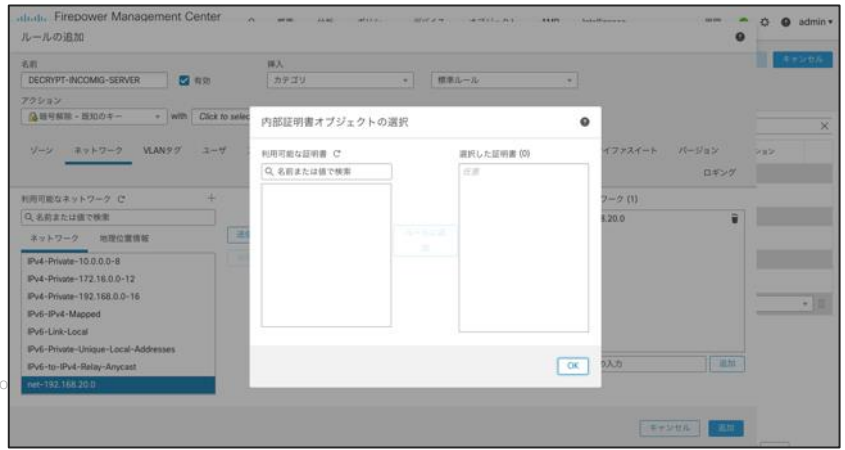
Type	Name	Source	Incidents	Action	Publish	Last Updated	Status
IPv4	1.1.1.1 *Indicator Imported From a Flat File*	test	1	Monitor (Block / Monitor)		Jul 24, 2018 6:18 AM EDT	Completed

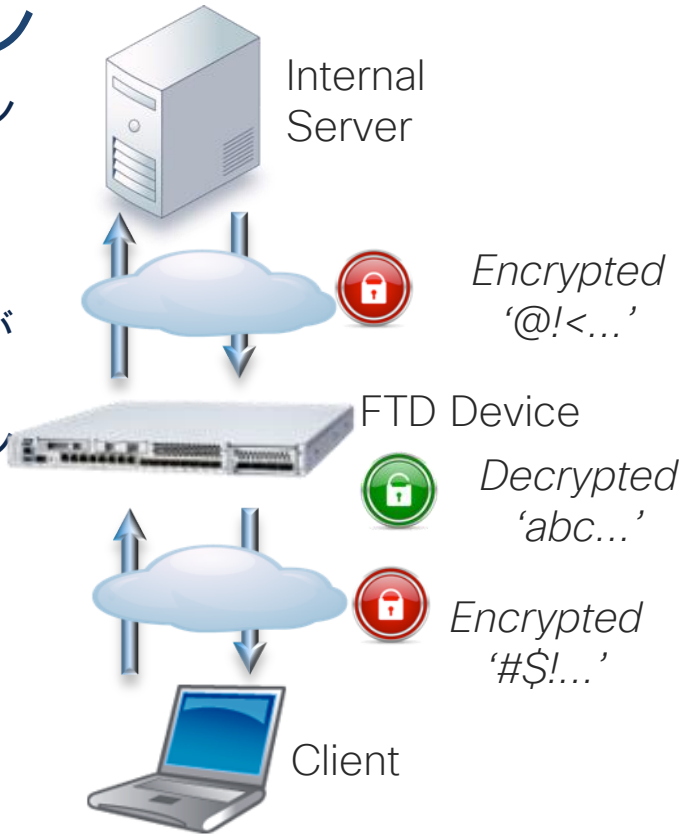
ジオロケーション

- 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 ネイティブにも 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)

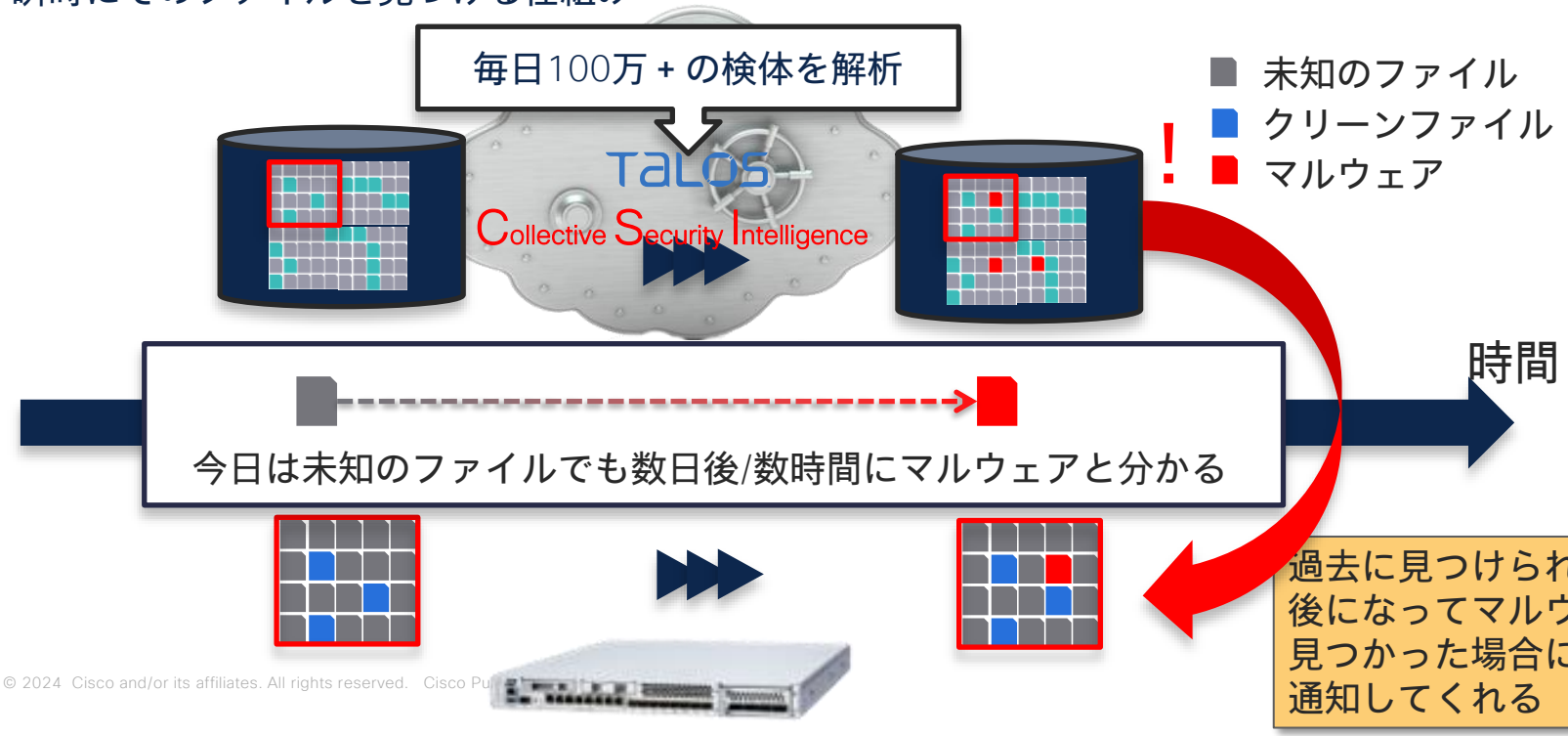
② 解析情報(サンドボックス含む)と連携

③ ネットワーク上での拡散状況を可視化

④ 端末の特定

Malware Defense クラウドリコール

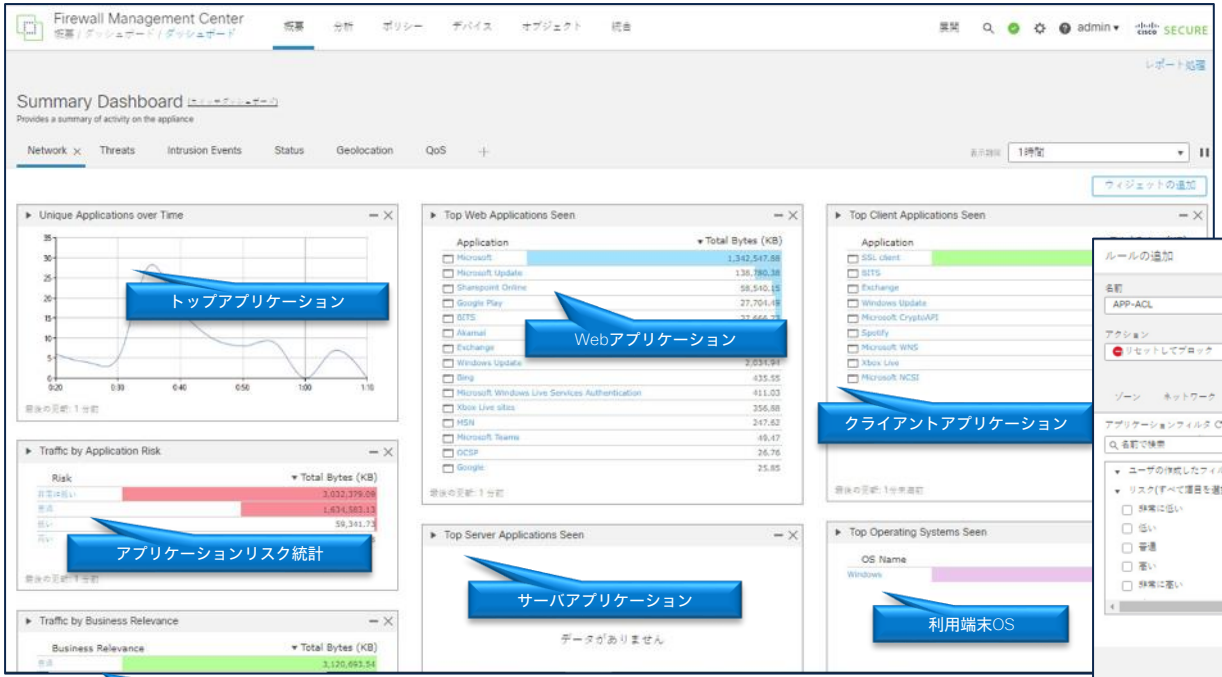
一度調査したファイルを覚えておき、合致するマルウェアが見つかった場合に
瞬時にそのファイルを見つける仕組み



クラウドリコールによるゼロデイマルウェア検知例

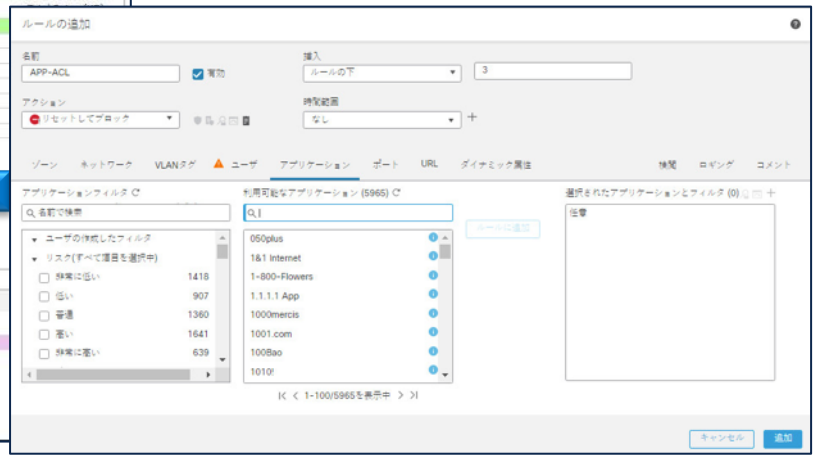
Application Visibility Control
アプリケーションの可視化と制御

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

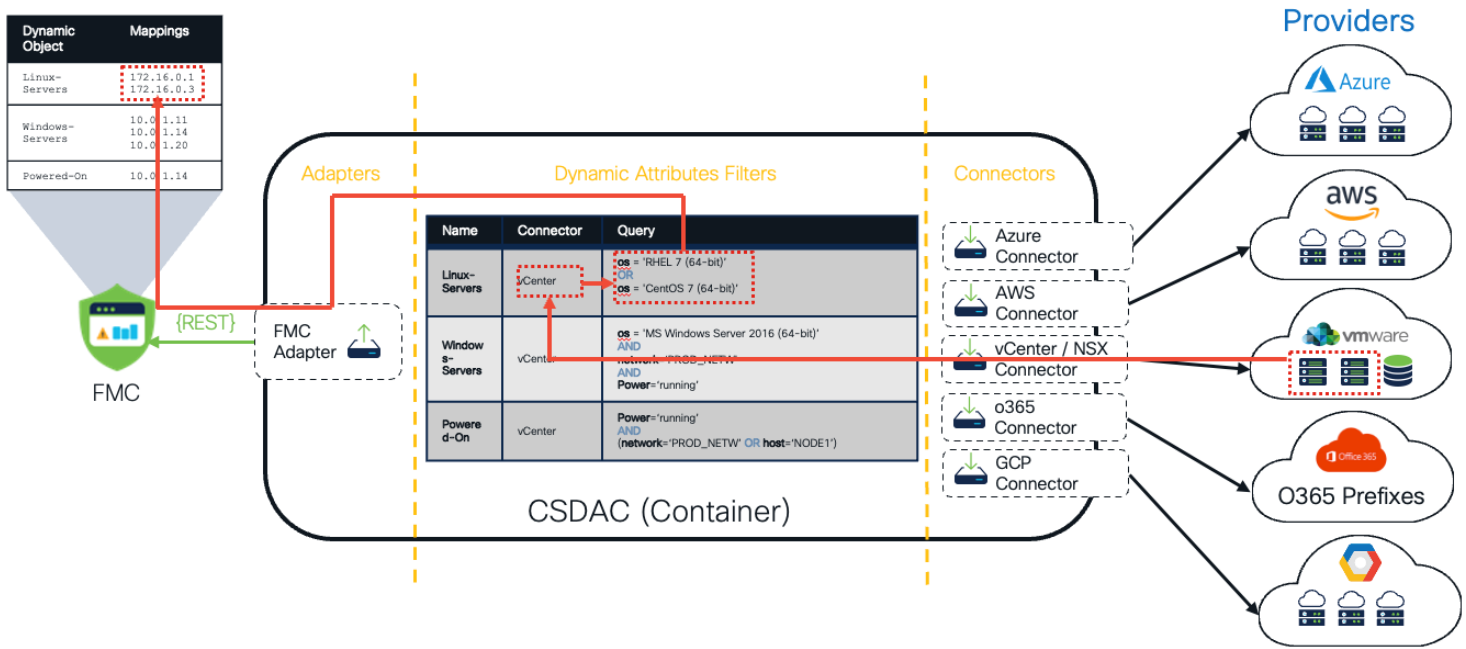
問題のあるアプリケーション、利用している端末を割り出し、利用の制限を実施し内在するリスクを軽減



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

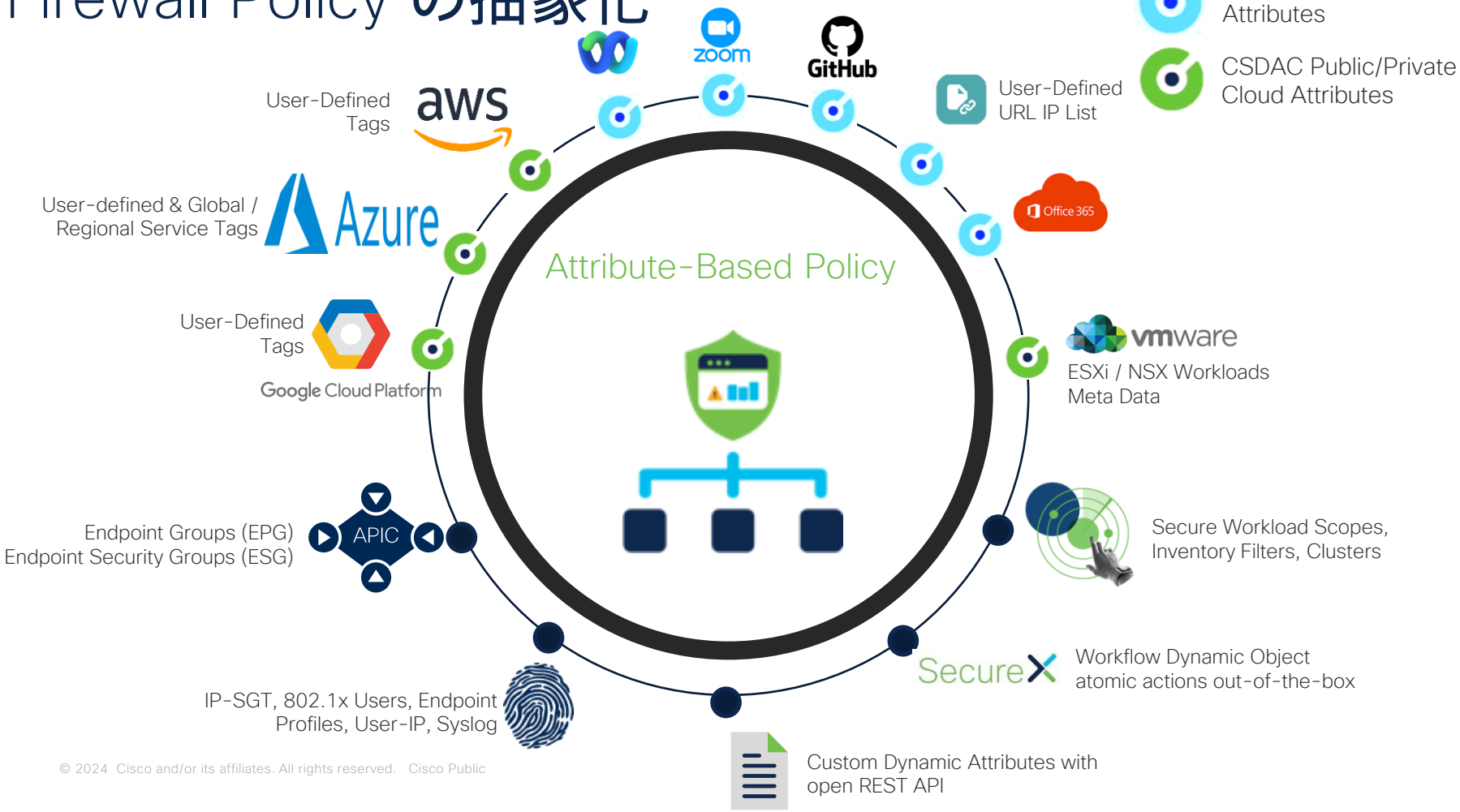
Cisco Secure Dynamic Attributes Connector (CSDAC)

FTD にすぐに Dynamic Object の変更を反映、ポリシーのデプロイは必要無し



CSDAC は cdFMC および On Premise FMC (version 7.4) に包含 (CSDAC 専用 VM も利用可能)

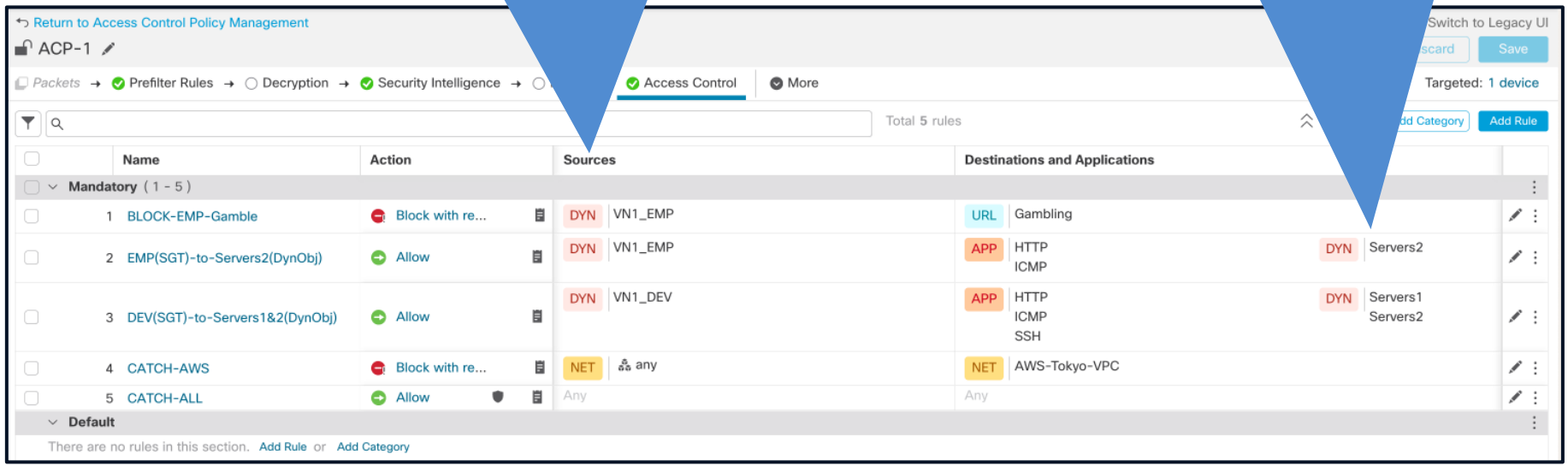
Firewall Policy の抽象化



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 CSDAC 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

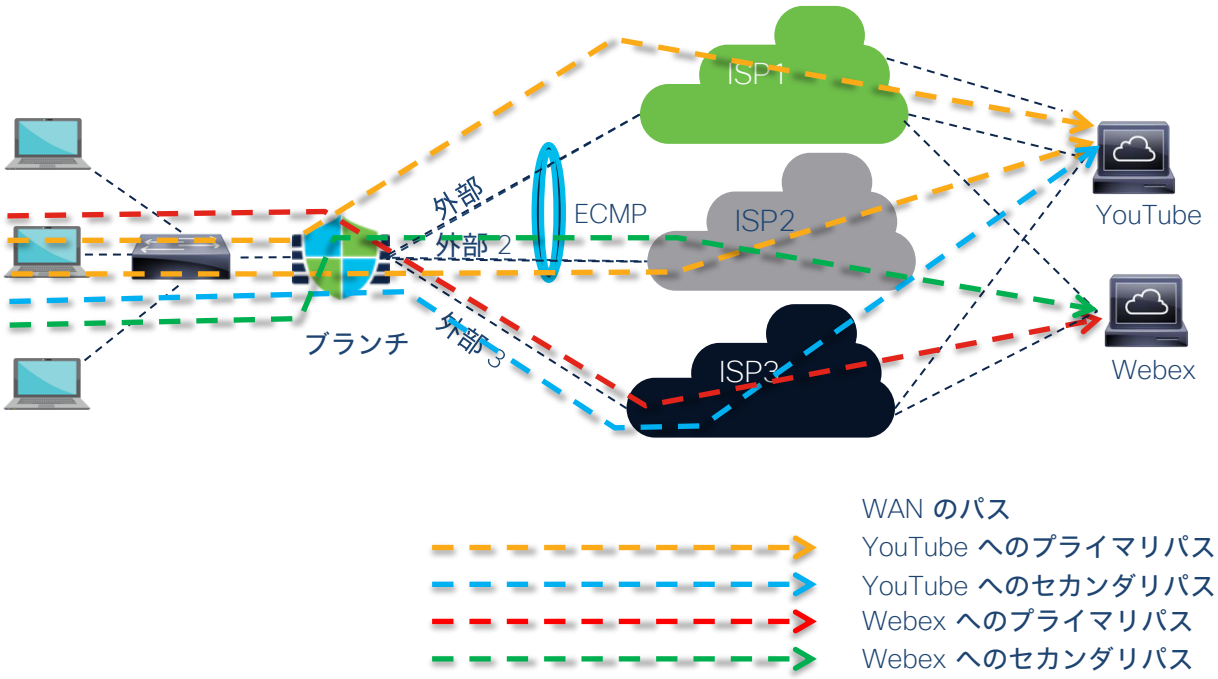
インテリジェントルーティング

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

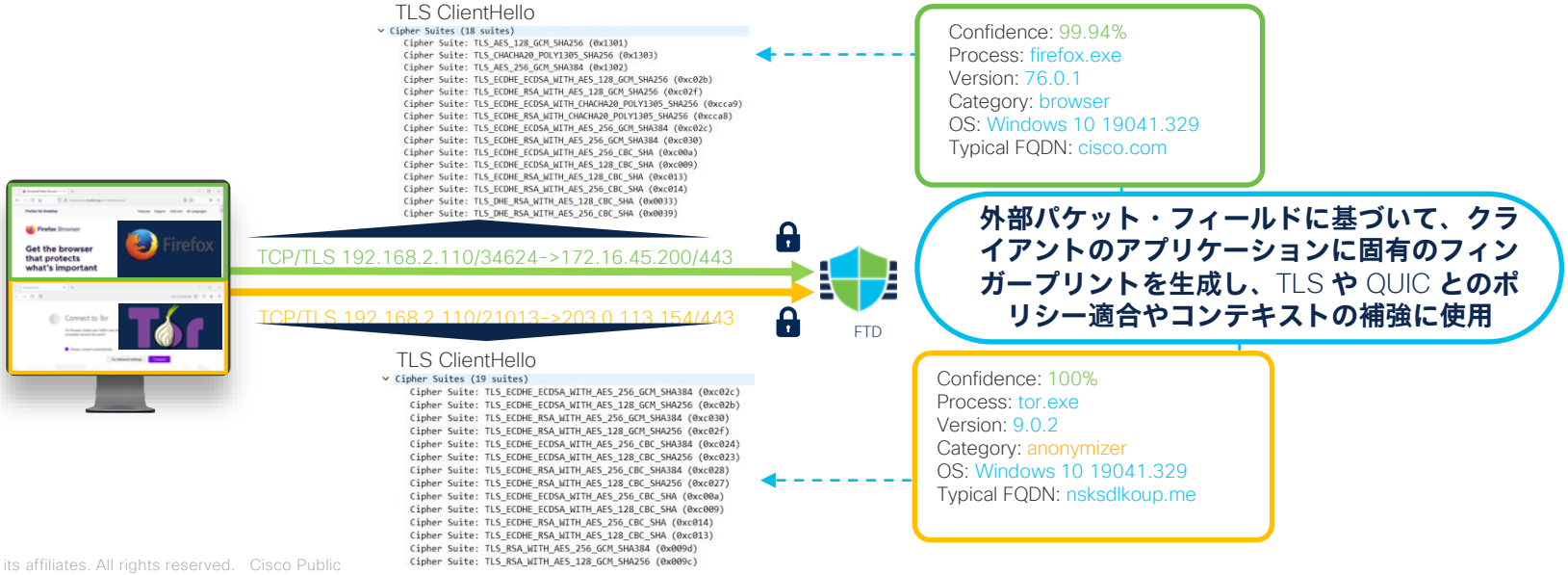
メリット

- 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 (EVE)

- 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



EVE によるトラフィック識別

Process Confidence:
発信元のプロセスに対する EVE の判断がどの程度確かであるかを表示

Threat Confidence and Score:
フローがマルウェアに感染している可能性を計算して表示

Time	Action	Event Type	Destination IP	Destination Port / ICMP Code	Encrypted Visibility Process Confidence Score	Encrypted Visibility Process Name	Encrypted Visibility Threat Confidence	Encrypted Visibility Threat Confidence Score	Client Application	Detection Type
2022-05-04 17:14:10	Allow	Connection	199.58.81.140	443 (https) / tcp	100%	tor	Very Low	0%	TOR	TLS Fingerprint
2022-05-04 17:13:53	Allow	Connection	163.172.21.117	443 (https) / tcp	100%	tor	Very Low	0%	TOR	TLS Fingerprint
2022-05-04 17:13:49	Allow	Connection	45.66.33.45	443 (https) / tcp	100%	tor	Very Low	0%	TOR	TLS Fingerprint
2022-05-04 17:13:32	Allow	Connection	131.188.40.189	443 (https) / tcp	100%	tor	Very Low	0%	TOR	TLS Fingerprint
2022-05-04 17:13:27	Allow	Connection	45.14.233.149	443 (https) / tcp	100%	tor	Very Low	0%	TOR	TLS Fingerprint

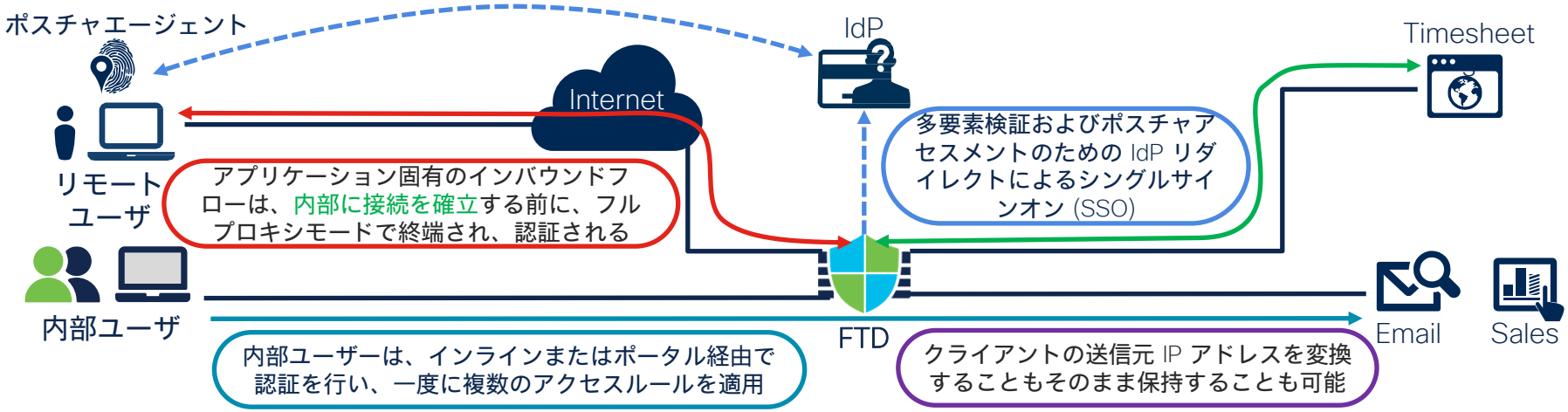
Process Name:
このフローを生成したホスト上のプロセス名を表示

Client Application:
EVE によって検出され、発信元の Host Profile に追加されたクライアントアプリケーションを表示

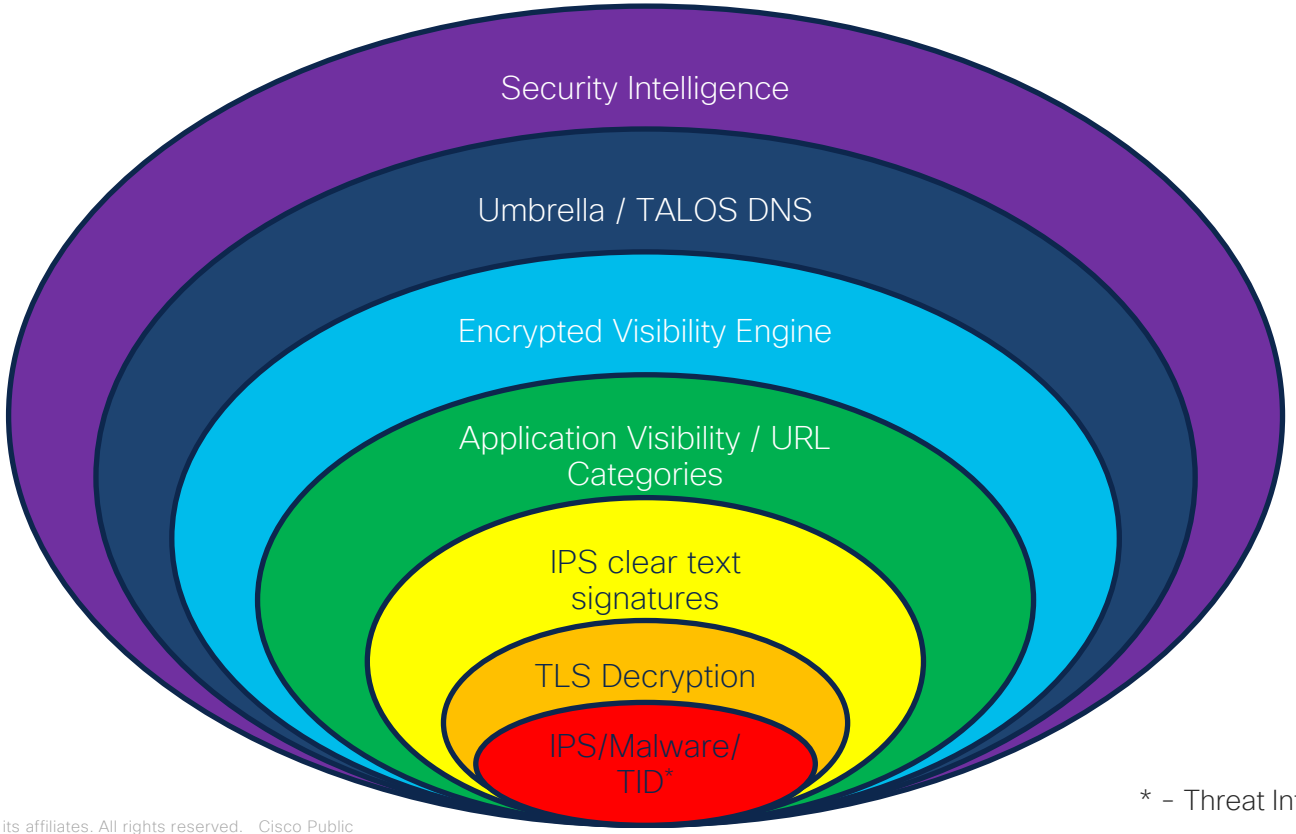
Detection Type は TLS Fingerprint として表示される

Clientless Zero Trust App Access (ZTAA)

- Captive Portal の機能をフルリバースプロキシに拡張
  - ポスチャアセスメントを行うことができる外部 Identity Provider (IdP) と連携
  - 従来の Clientless SSL-VPN からの置き換え



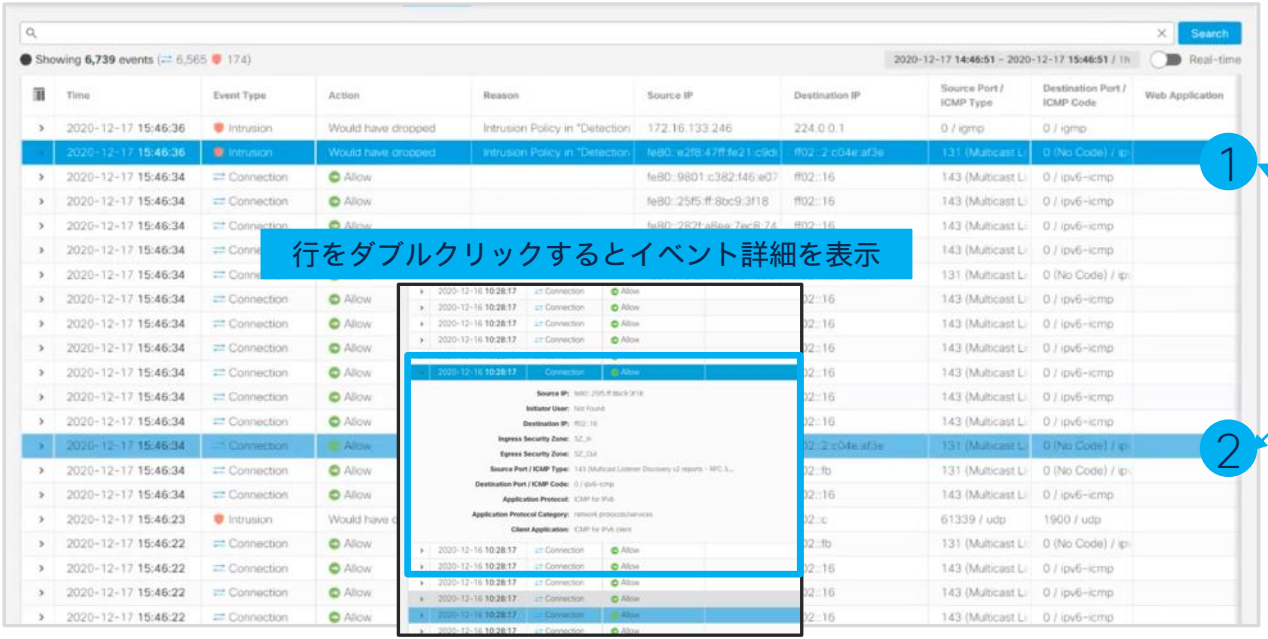
多層で行われる防御 – 本当に必要な脅威対策



* – Threat Intelligence Director (TID)

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

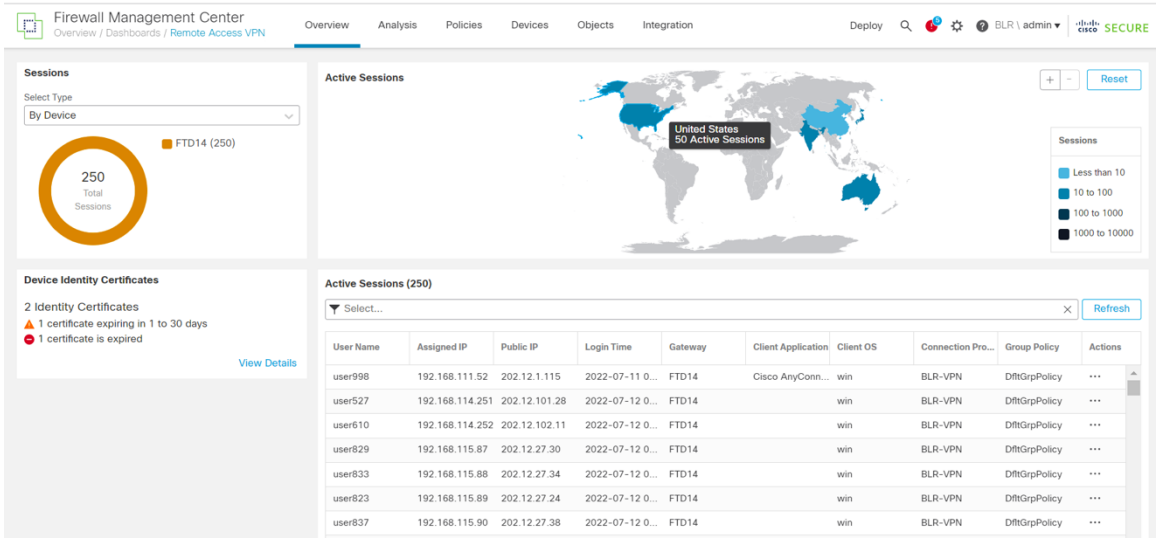
アプリケーション認識型ファイアウォールポリシーの適用、パスの選択、および復号

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

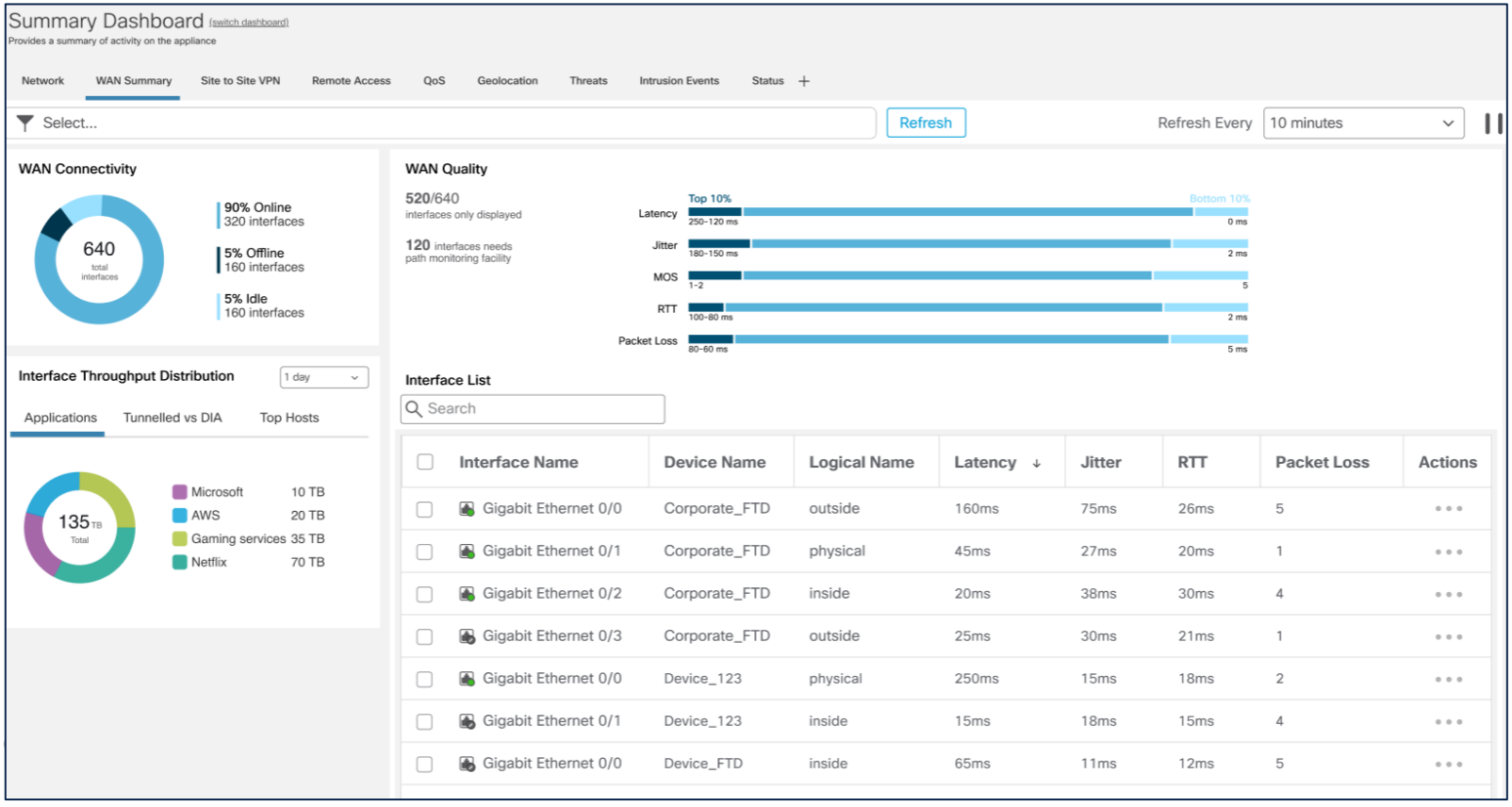
メリット

- 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



SD-WAN モニタリングダッシュボード

SD-WAN の状況を一目で確認可能なダッシュボード



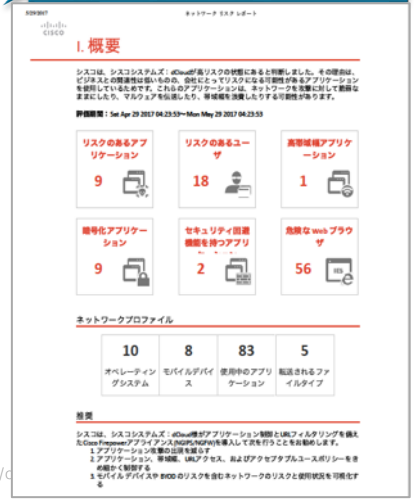
Custom Report レポート機能

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

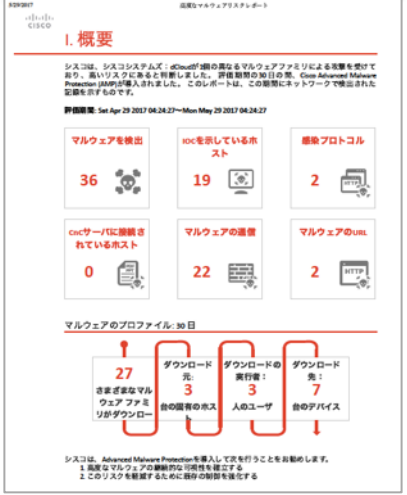
PDF、HTML、CSV形式をサポート

ネットワークレポート

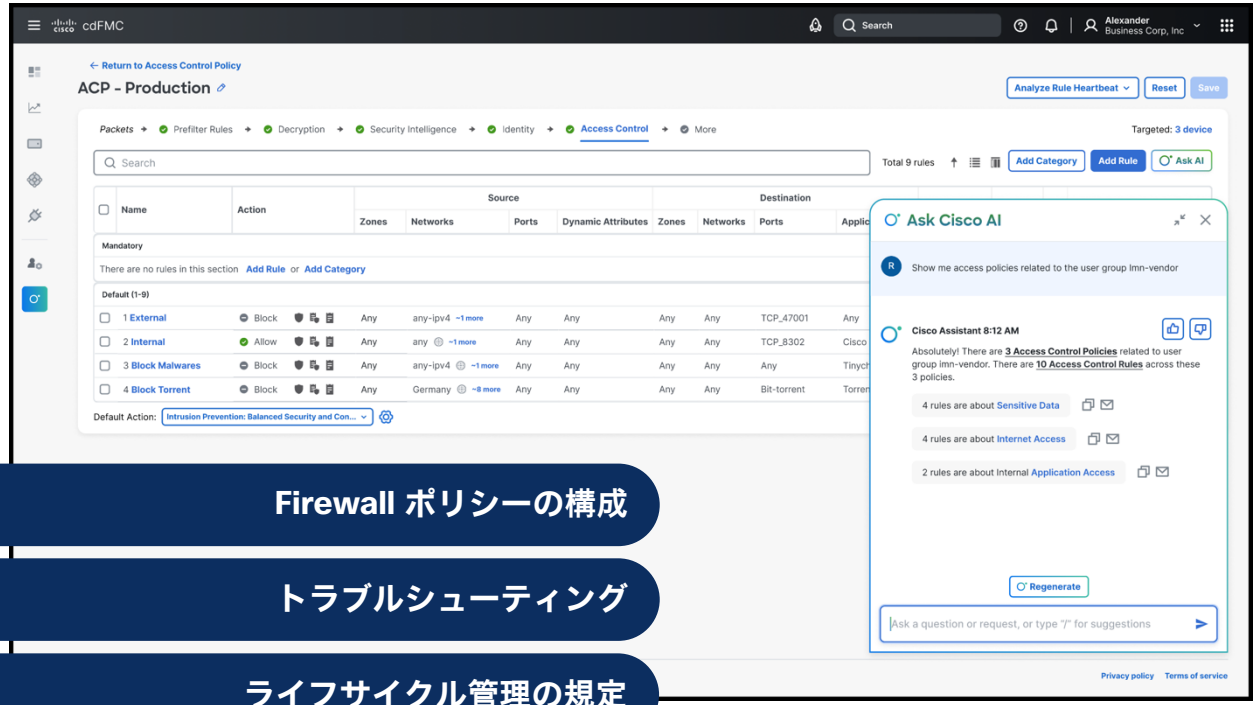


アタックレポート

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

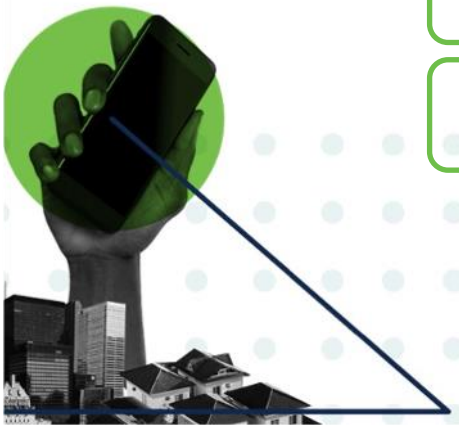
https://www.cisco.com/c/ja_jp/products/security/artificial-intelligence-ai.html

Cloud Delivered FMC にて近日サポート開始 (On Premise FMC でもサポート予定有り)

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

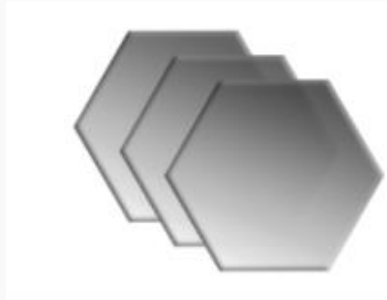
FPR1150 と FTD 仮想版 を 1台の FMC で管理している例

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

FMC1700
最大 50台の Firewall 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台の Firewall 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 1000台の Firewall 管理
最大イベント数 4億件
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台の Firewall 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台の Firewall 管理対応モデルも有り (FMCv300)
HA対応 (Vmware, AWS, OCI 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

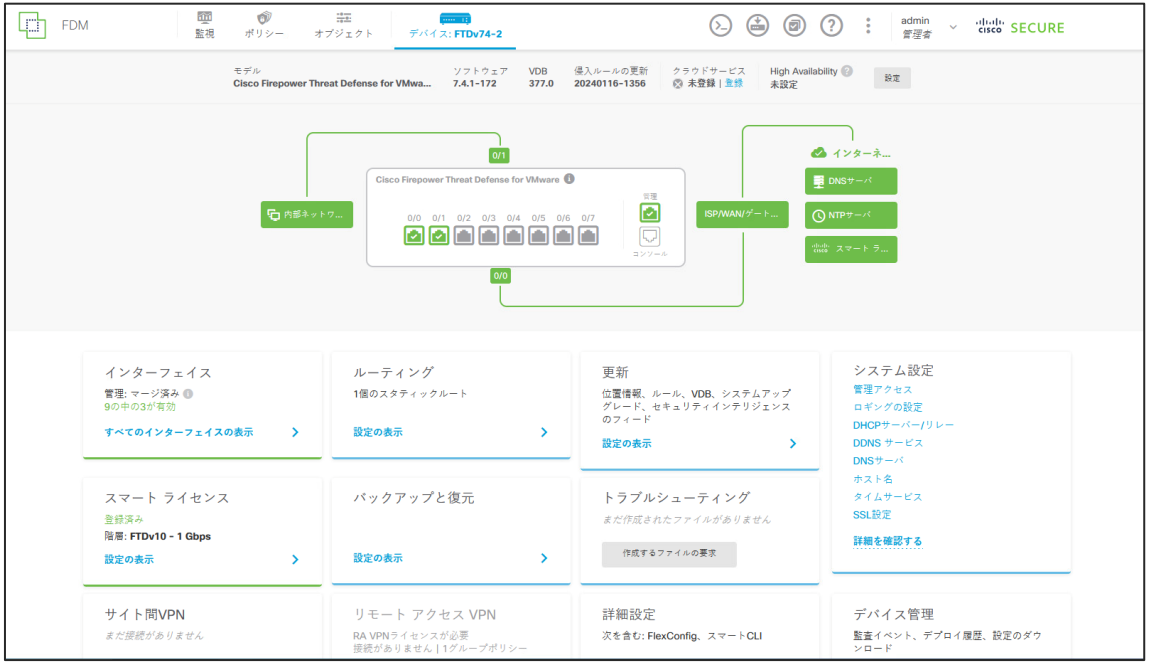
シスコがアップタイムを確保し、柔軟性を向上

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
- Firewall 4200 シリーズの管理

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

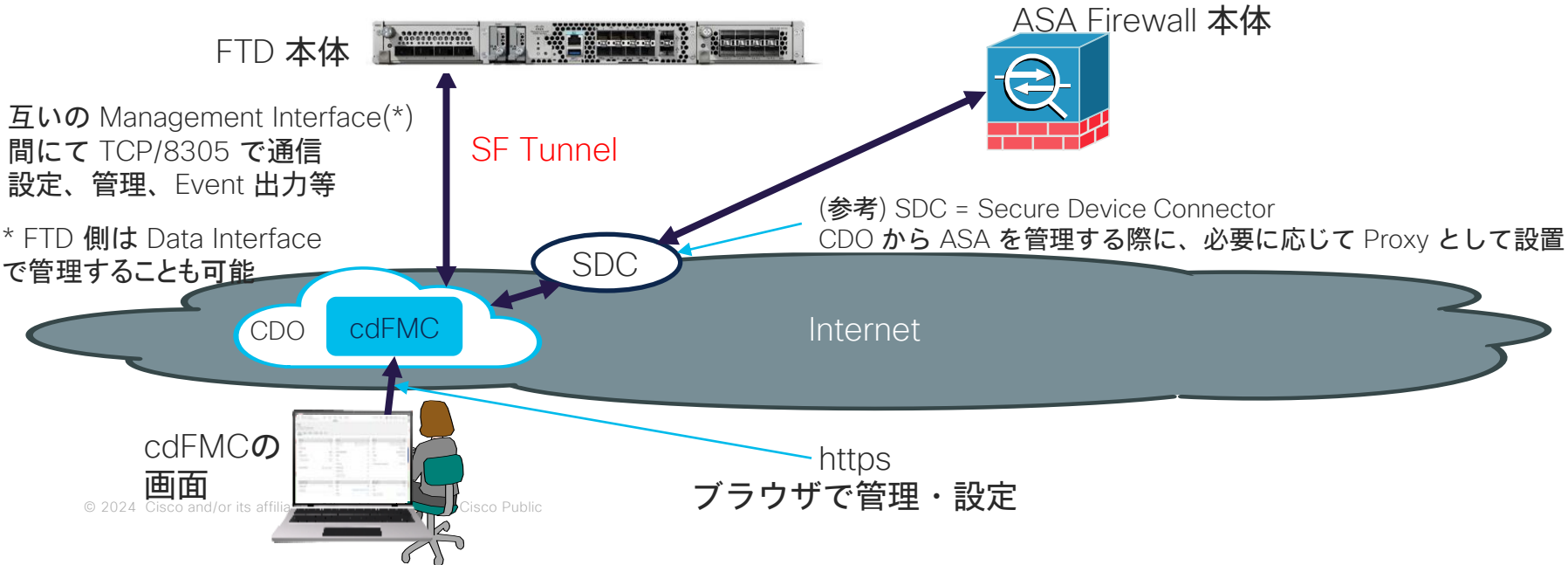
FDM
= Firewall Device Manager

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5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

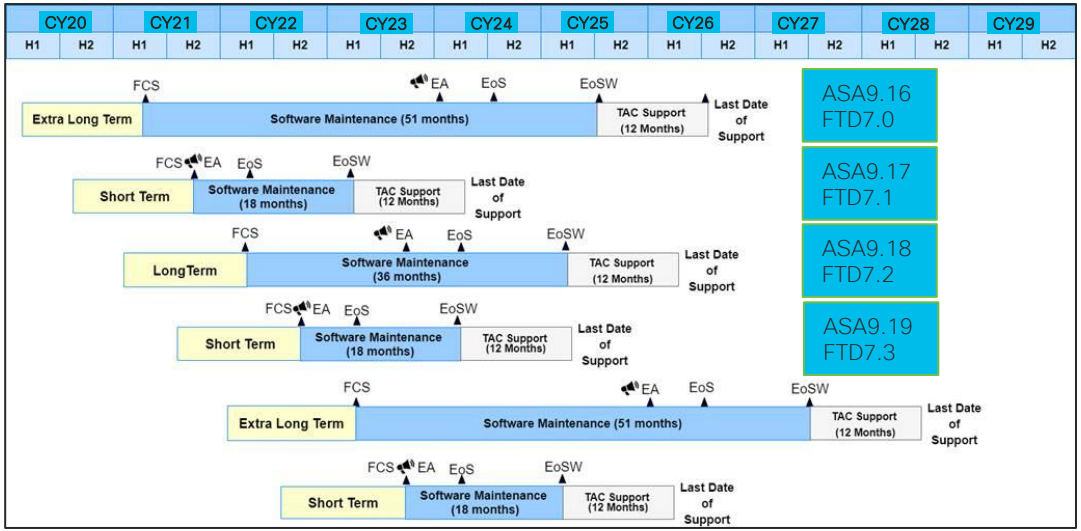
- FTD (ASA も) のバージョンの数字の小数点1桁目が偶数ならロングタームサポート、奇数ならショートタームサポートとなる

  FTD 7.3 → ショートタームサポート

  FTD 7.4 → 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 7.4 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5月時点で一般的な推奨バージョンは FTD 7.2.5 / ASA 9.18.4 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

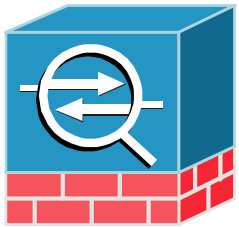
安定度の面からも、既存 FTD 環境の Version 7.2.5.x or 7.2.7 への VersionUP を強く推奨

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？

- 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 を選択してもよい

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

当資料は FTD の説明にフォーカス

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

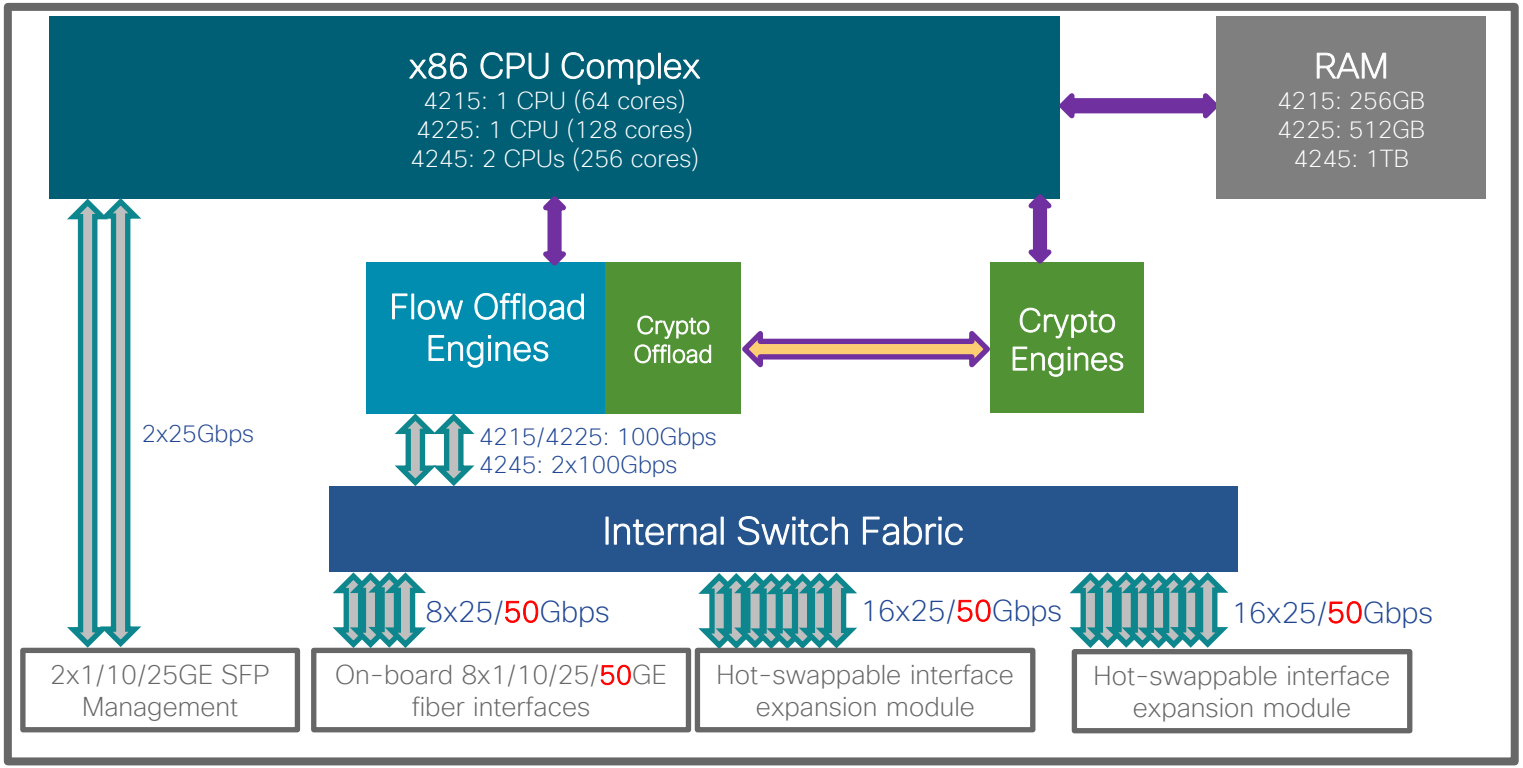
- Up to 2x900GB in RAID1 on 4215/4225
- Up to 2x1.8TB in RAID1 on 4245

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

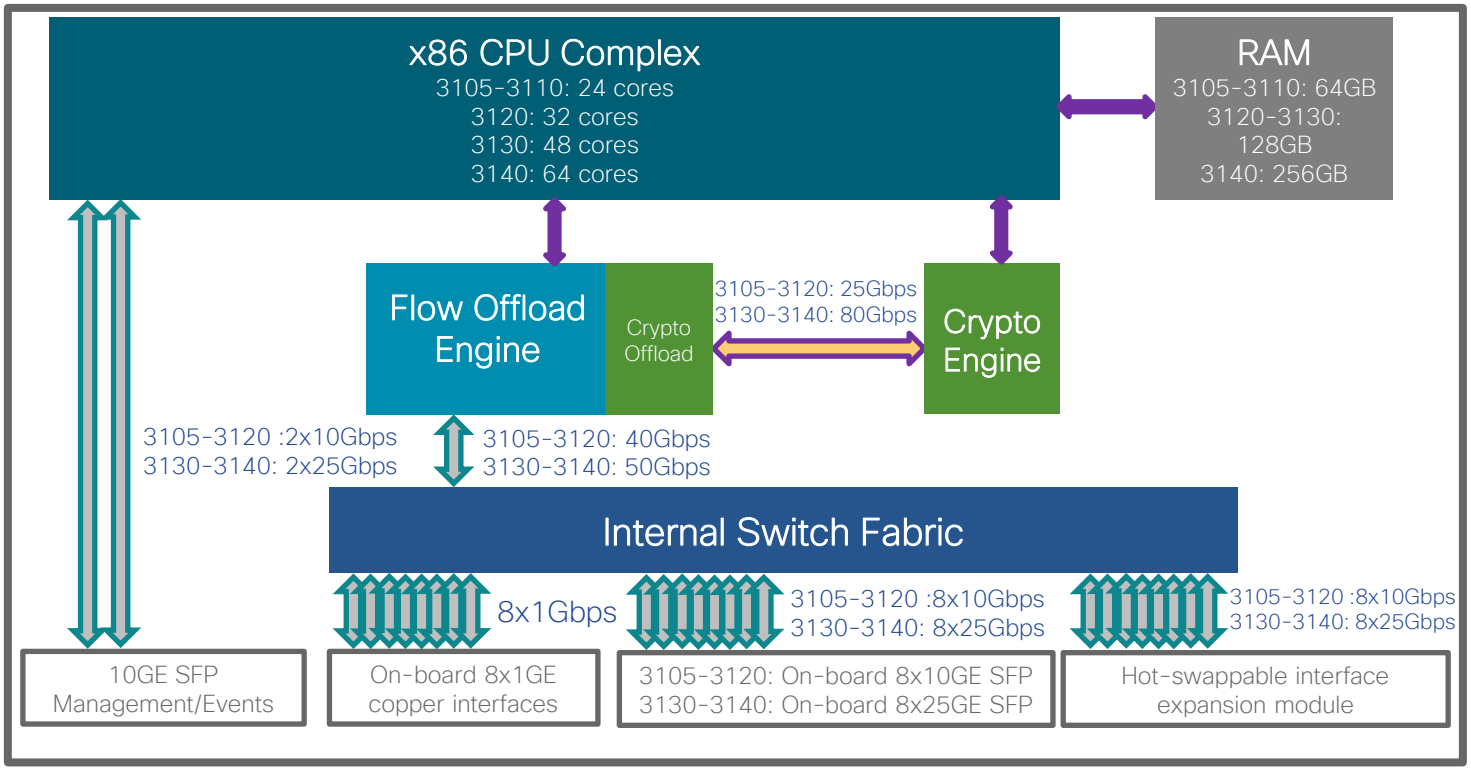
Copper Data Interfaces
- 8x10M/100M/1GE Ethernet

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

まとめと参考資料

まとめ

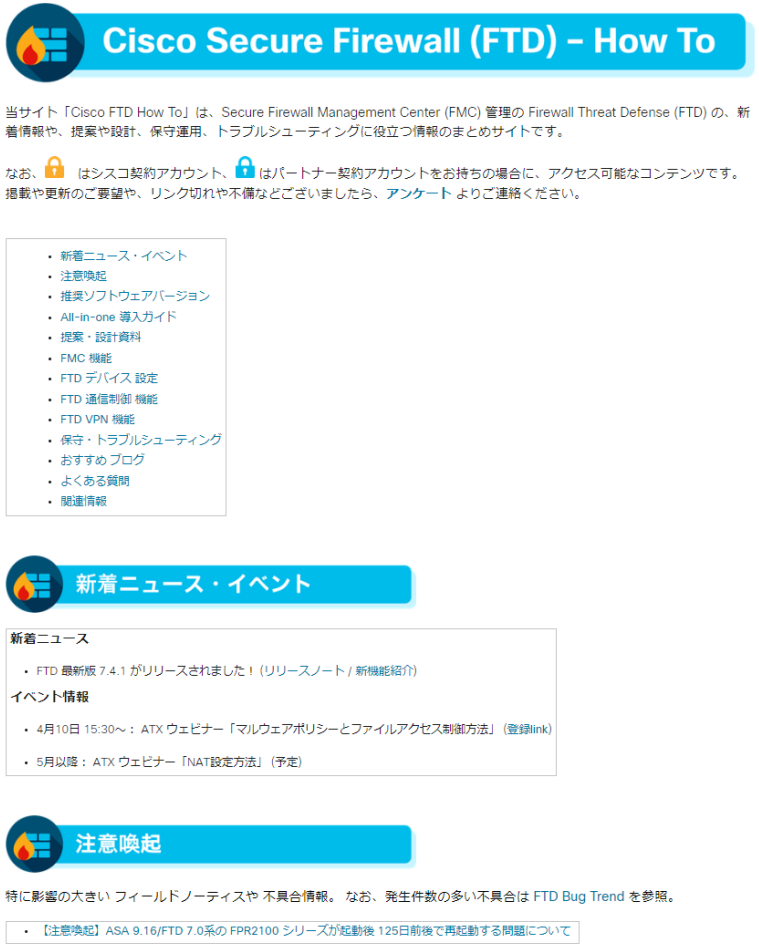
- Firewall Threat Defense (FTD) が上位レイヤの脅威対策を行う NGFW & IPS 製品として位置づけられ、市場で認知されている
- L4 までの Basic Firewall である ASA と L7 Security の FTD を適材適所で使い分ける
- “本当に使える” 脅威対策として FTD は優れた機能や管理性を持つ
- FTD は ASA の機能を包含した新たな NGFW + IPS + Malware Defense 製品として利用可能
- FTD も ASA も同一ハードウェアで動作し、豊富なラインナップがある
- FTD と ASA の明確な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

- [必見] FTD まとめサイト (FMC 管理の FTD の全てをまとめた日本のサイト)
  https://community.cisco.com/t5/-/-/ta-p/5024782
- 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
- 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

FTD まとめサイト のご案内

2024年2月 公開！
毎月更新！



Cisco Secure Firewall (FTD) – How To

当サイト「Cisco FTD How To」は、Secure Firewall Management Center (FMC) 管理の Firewall Threat Defense (FTD) の、新着情報や、提案や設計、保守運用、トラブルシューティングに役立つ情報のまとめサイトです。

なお、 はシスコ契約アカウント、 はパートナー契約アカウントをお持ちの場合に、アクセス可能なコンテンツです。
掲載や更新のご要望や、リンク切れや不備などございましたら、アンケート よりご連絡ください。

- 新着ニュース・イベント
- 注意喚起
- 推奨ソフトウェアバージョン
- All-in-one 導入ガイド
- 提案・設計資料
- FMC 機能
- FTD デバイス 設定
- FTD 通信制御 機能
- FTD VPN 機能
- 保守・トラブルシューティング
- おすすめ ブログ
- よくある質問
- 関連情報

新着ニュース・イベント

新着ニュース

- FTD 最新版 7.4.1 がリリースされました！(リリースノート / 新機能紹介)

イベント情報

- 4月10日 15:30～： ATX ウェビナー「マルウェアポリシーとファイルアクセス制御方法」(登録link)
- 5月以降： ATX ウェビナー「NAT設定方法」(予定)

注意喚起

特に影響の大きい フィールドノーティスや 不具合情報。 なお、発生件数の多い不具合は FTD Bug Trend を参照。

- 【注意喚起】ASA 9.16/FTD 7.0系の FPR2100 シリーズが起動後 125日前後で再起動する問題について

FTD の提案や設計、導入・保守運用に
必要な情報が揃った、オールインワン サイト！

Cisco SE や TAC・CSが 総力をあげて作成・監修

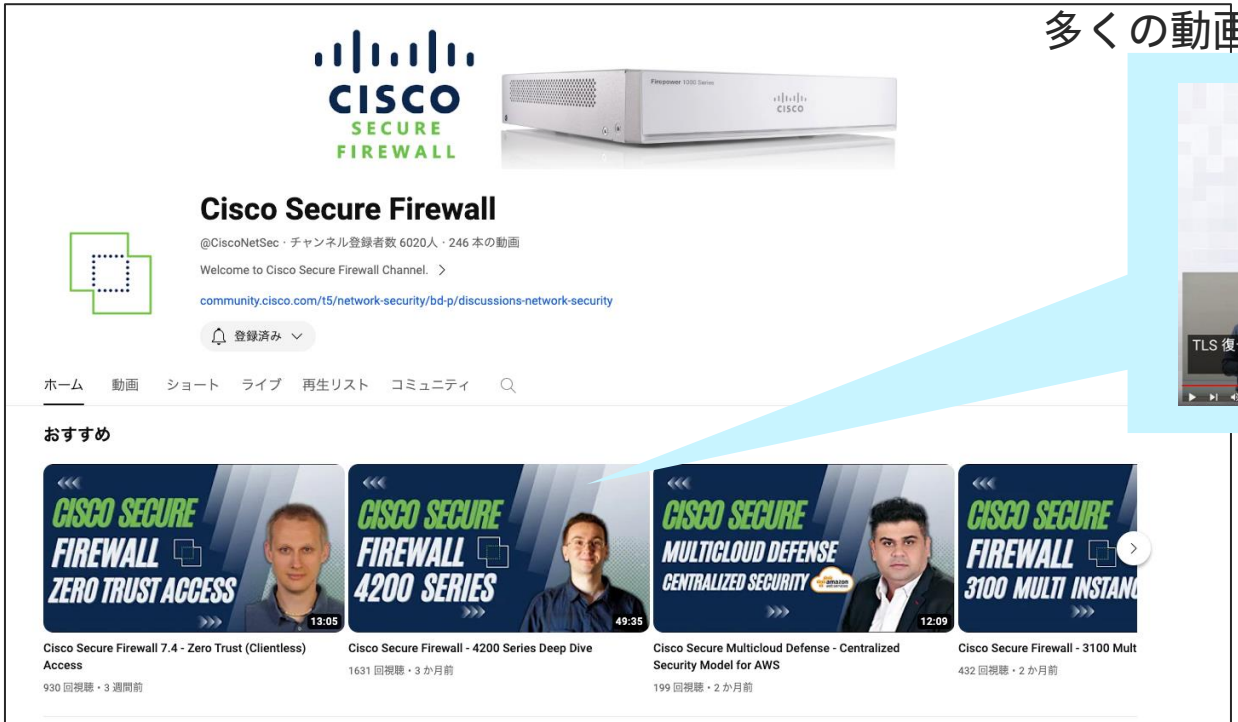
- ✓ 新着ニュースや イベント、推奨バージョン情報
- ✓ 注意喚起情報
- ✓ 提案・設計 資料
- ✓ 主要機能の設定やデモガイド
- ✓ 運用や保守ガイド
- ✓ おすすめブログ記事、など

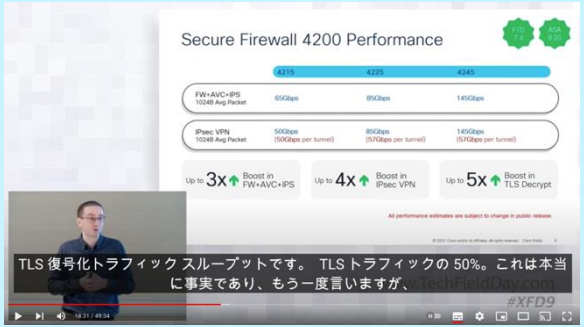
https://community.cisco.com/t5/-/-/ta-p/5024782

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