cisco SECURE

cisco The bridge to possible

Cisco Secure Firewall 新製品と利用ケースのご紹介

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)

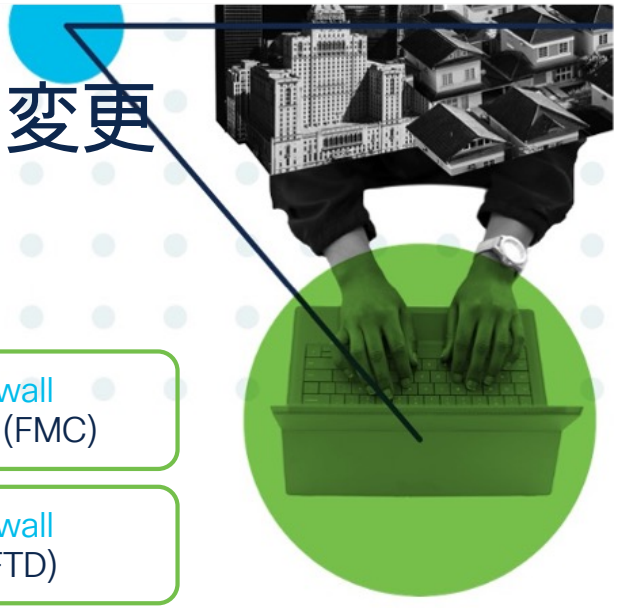
2023年9月14日

アジェンダ

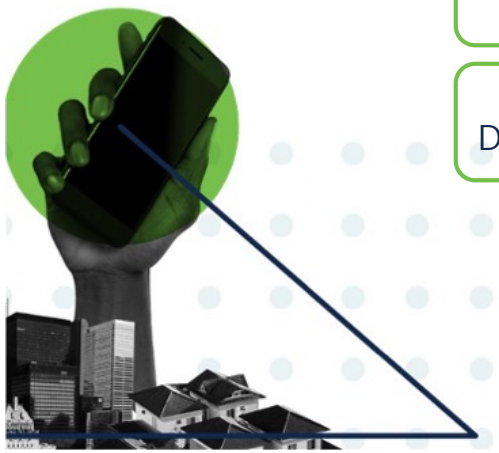
- Introduction & Software Release
- Platforms
- Threat Protection
- Connectivity
- Private & Public Cloud
  (Cisco Multicloud Defense 含む)
- Management
- 参考資料

Introduction & Software Release

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)



Hardware Appliance の名前も “Firepower” から “Secure Firewall” に変更
ただし、型番には FPR の名前が残る

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

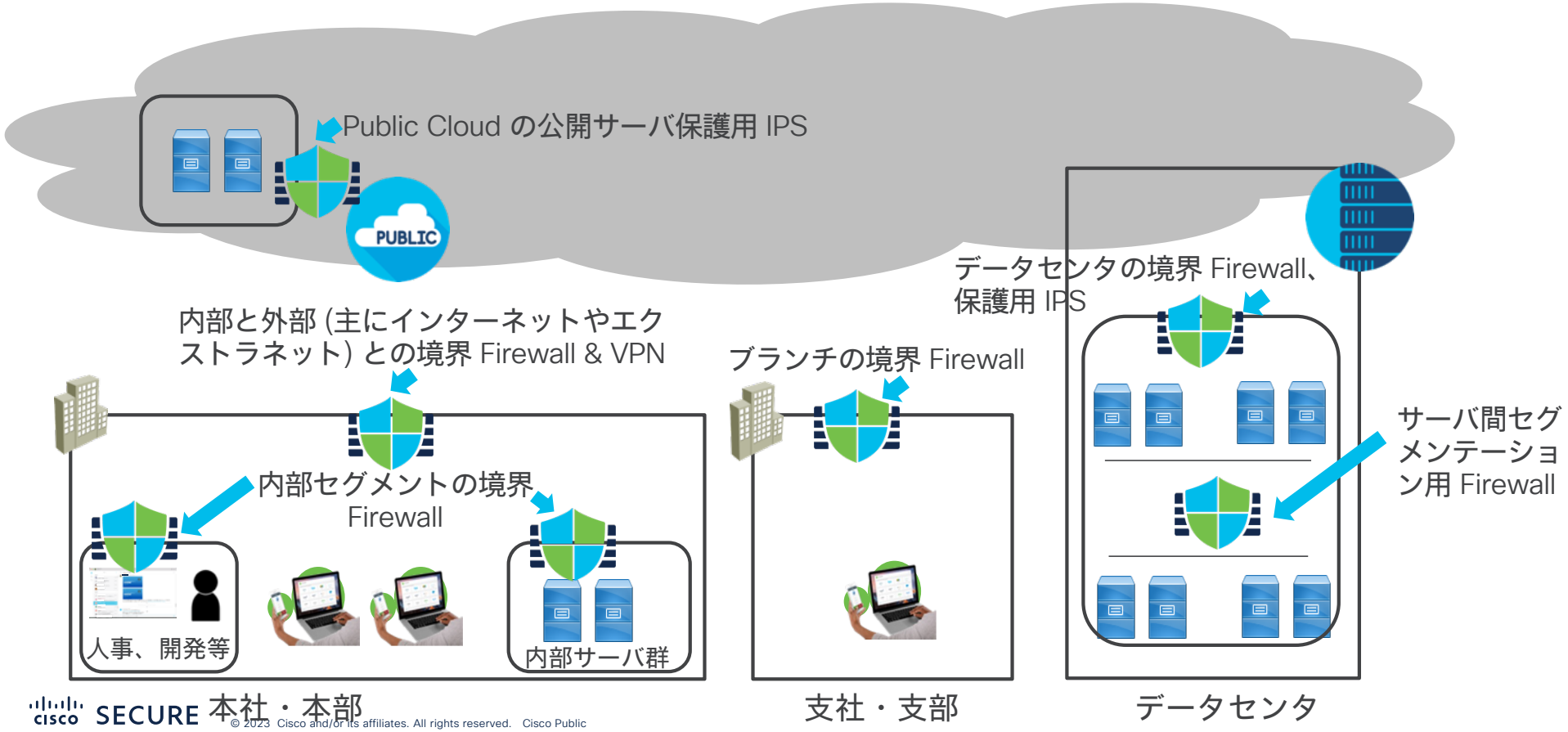
・「とりあえず動かすだけ」の IPS からの卒業。本当に必要な脅威対策を IPS で実施

- **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

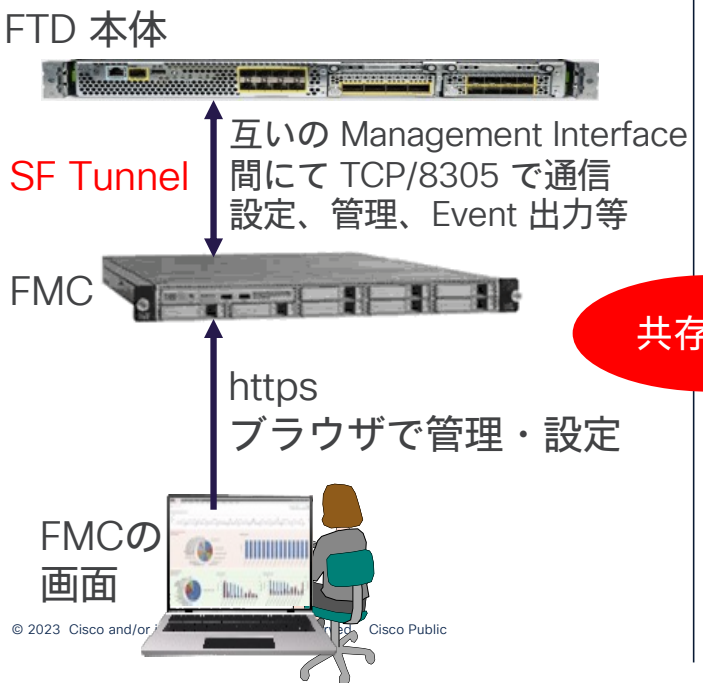


FTD の管理・設定アーキテクチャ (On Premise)

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

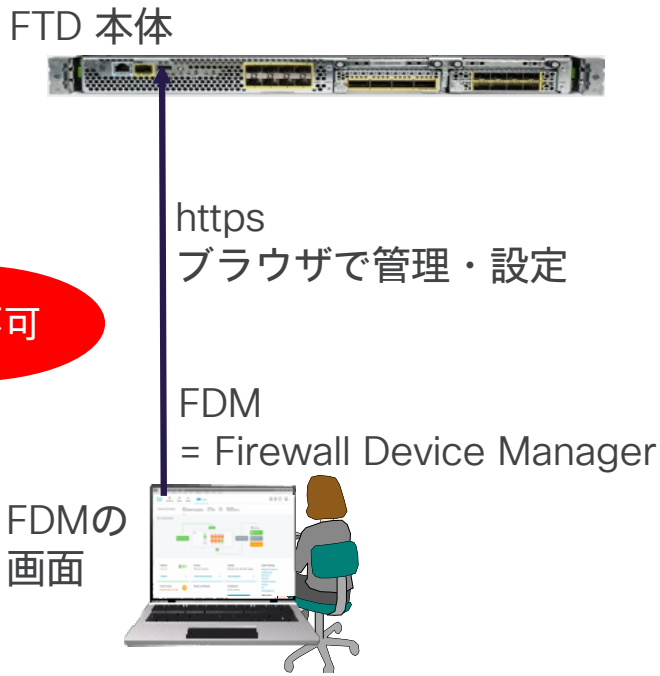
FMC (On Premise) 管理

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



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



共存不可

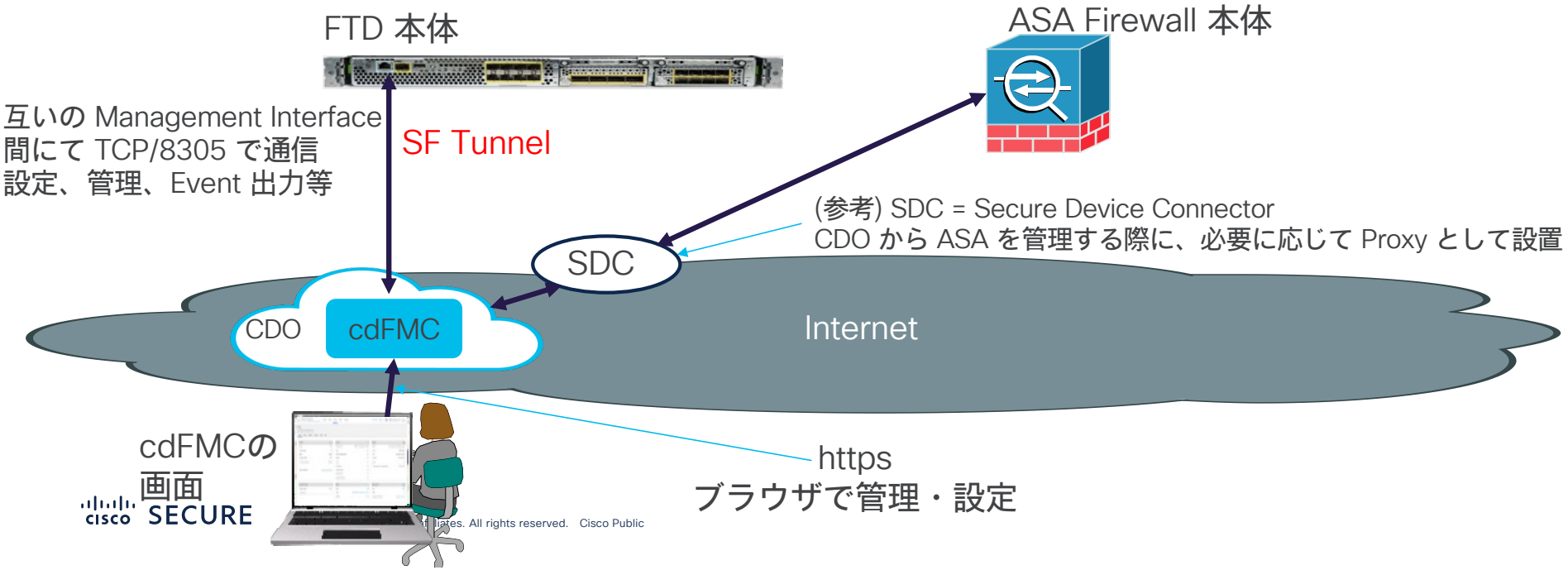
FTD の管理・設定アーキテクチャ (Cloud)

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)

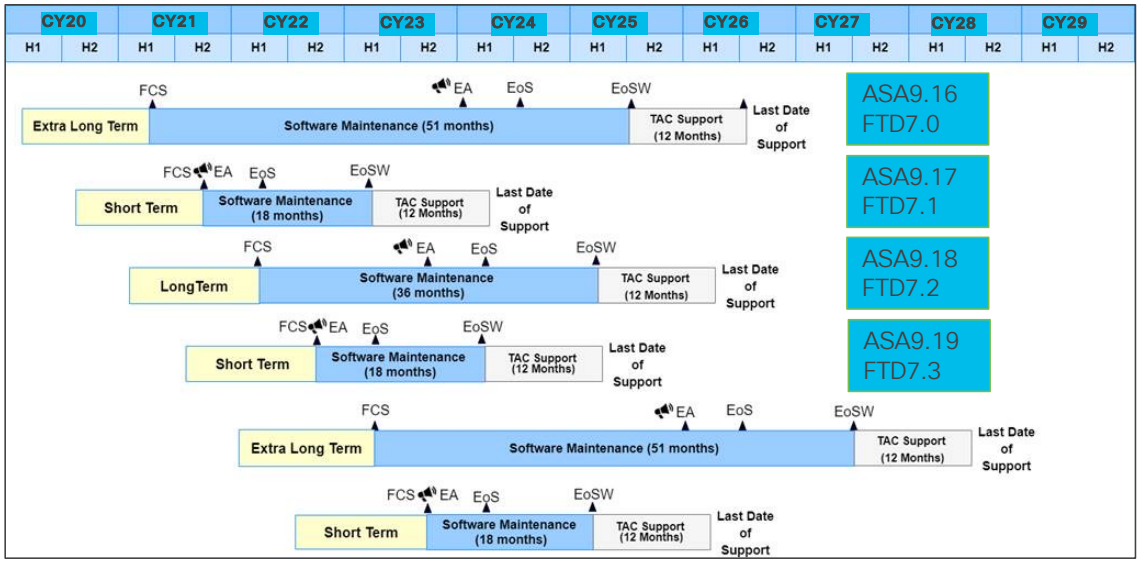
On Premise FMC を Event 出力先として同時利用可能



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 および ASA 9.20.1 は、2023年6月時点で Firewall 4200 シリーズ専用リリースとなり、他のモデル向けには2023年12月にリリース予定



Firewall Threat Defense 7.2.5 ソフトウェア

FTD 7.2.5

- 品質を高めるために FTD 7.2 に行われた改良
  - FTD と FMC のデータベースエンジンの堅牢化
  - Snort 3 の運用における残課題を解決
  - 3種類の自動化されたシステム試験にて問題を解決
- 顧客での体験と成果を重視
  - 100 以上の実運用環境での検証
  - デプロイ時間とスケールを改善するための機能拡張を選択
- 7.0.x へのバックポートと 7.4.x トレインのリリースへの準備

FTD 7.2.5 (と ASA 9.18.3 interim) が Suggested Release に

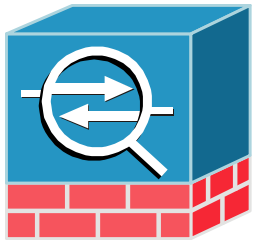
今後のソフトウェアリリース予定について

- FTD 7.4.0 と ASA 9.20.1 が 2023年9月にリリース済
  - Firewall 4200 シリーズ (後述) 専用ソフトウェアとしてリリース
  - FMC にも対応 (販売終了モデルを除く)
- FTD 7.4.1 と ASA 9.20.2 が 2023年12月頃にリリース予定
  - その他の Firewall / Firepower アプライアンス (販売終了モデルを除く) にも対応
- FTD 7.4.x と ASA 9.20.x は Extra Long Term Release (XLTR) になる予定

- 全ては予定であり、予告無く変更される可能性有り

[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
  - 19年目のロングセラー
    (PIX まで遡ると29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)
  - 17年目のロングセラー
    (Cisco VPN Client まで遡ると23年)

どちらもまだまだシスコのセキュリティ製品の中核かつ主力

Firewall は ASA か FTD か？

- Firepower アプライアンスは ASA ソフトウェアか FTD ソフトウェアを選択して動作させることができる。また、ASA も FTD もそれぞれ仮想版ソフトウェアが存在する

	ASA	FTD
Basic (L4まで) Firewall, Routing / Switching, NAT	◎	○
RA VPN 終端	◎	◎
Site-to-Site VPN (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

Platforms

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

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

cisco SECURE

Cisco Secure Firewall Hardware のポートフォリオ

650 Mbps
AVC+IPS

1.5-2.2 Gbps
AVC+IPS

2.3-20 Gbps
AVC+IPS

17-45 Gbps AVC+IPS
8 - 22.4 Gbps IPsec VPN
8 Node Cluster:
With 3140, up to
AVC+IPS(1024B) = 288 Gbps

Stand-alone device:
12-53 Gbps AVC
10-47 Gbps AVC+IPS
Sixteen node cluster:
Up to 680 Gbps AVC
Up to 675 Gbps
AVC+IPS

Stand-alone device:
65-145 Gbps AVC
65-145 Gbps AVC+IPS
Sixteen node cluster:
Up to 1.7 Tbps AVC
Up to 1.6 Tbps AVC+IPS

One Module:
30-70 Gbps AVC
24-64 Gbps AVC+IPS
Sixteen node cluster:
AVC+IPS
SM40*16n = 704 Gbps
SM48*16n = 830 Gbps
SM56*16n = 950 Gbps


1010


1120/40/50


2110/20/30/40


3105/10/20/30/40


4112/15/25/45

NEW

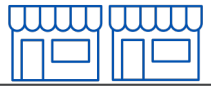

4215/25/45


9300 Series
SM-40
SM-48
SM-56


SMB


Branch Office


Mid Enterprise


Large Enterprise


Data Center


Service Provider

全てのハードウェアには ASA or FTD ソフトウェアを搭載可能

cisco SECURE

Secure Firewall 4200 Overview

FTD 7.4

ASA 9.20

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

SFP Data Interfaces

- 8x1/10/25GE/50GE

1RU

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)

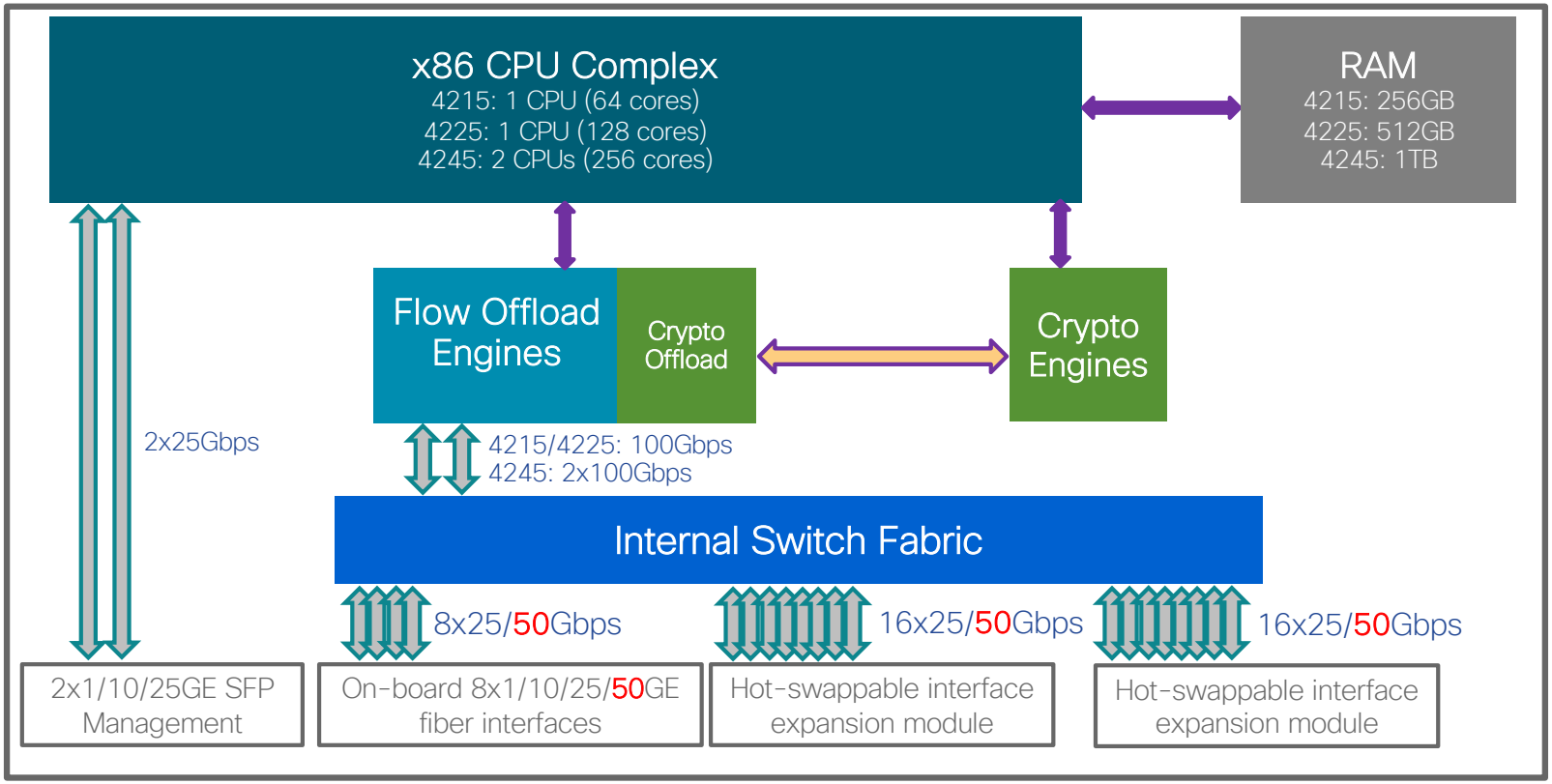
cisco SECURE

赤字は将来対応予定

Secure Firewall 4200 Architecture

FTD 7.4

ASA 9.20



System Bus

Ethernet

Chip-to-Chip Link

Secure Firewall 4200 パフォーマンス

FTD 7.4

ASA 9.20

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 7.1

ASA 9.17

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

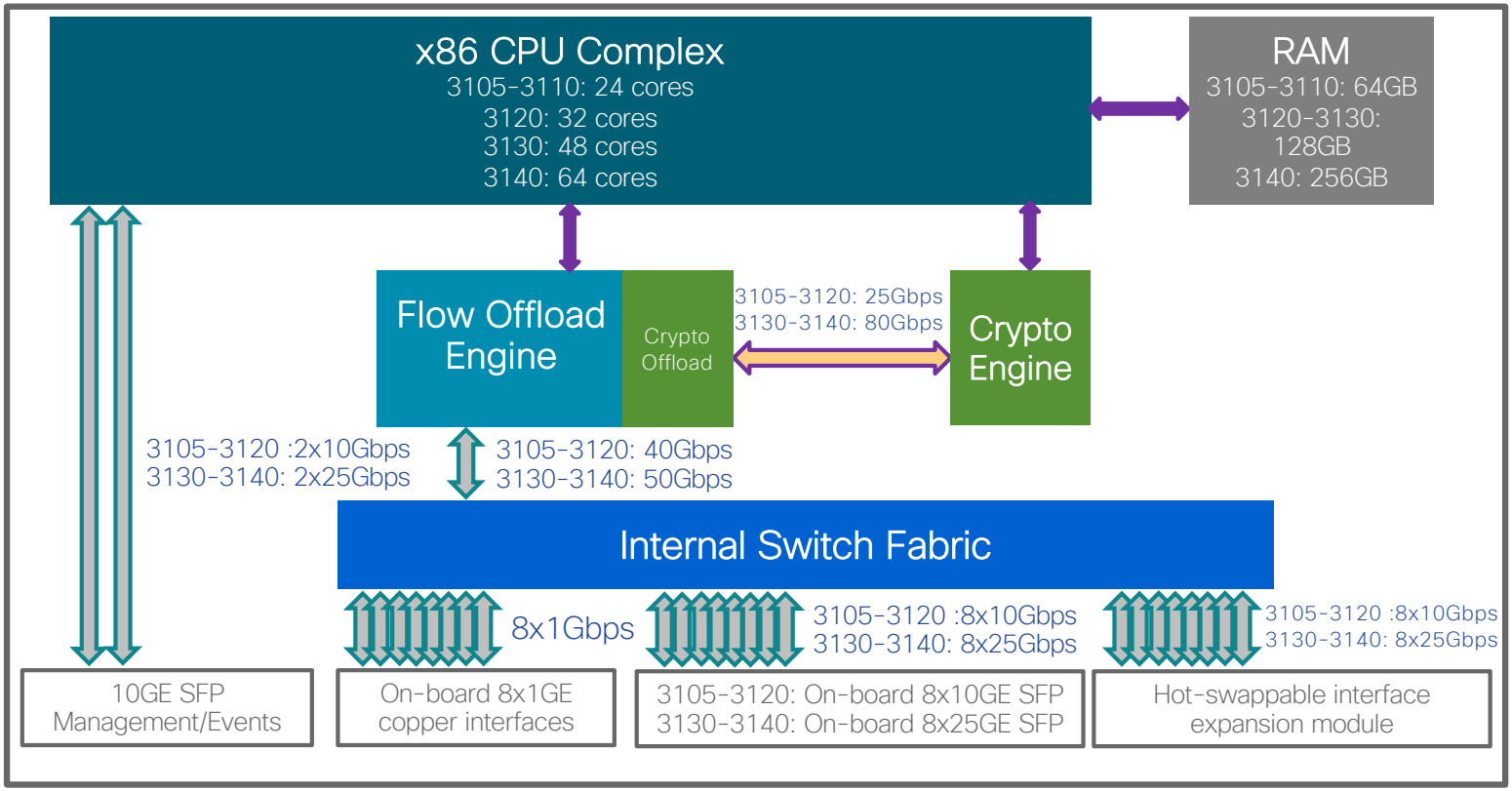
- 8x1/10/25GE or 6x10/25GE FTW on Firewall 3105-3120
- 4x40GE or 2x40GE FTW on Firewall 3130-3140

赤字は将来対応予定 (3105 除く)

Secure Firewall 3100 Architecture

FTD 7.1

ASA 9.17



System Bus

Ethernet

Chip-to-Chip Link

cisco SECURE

Secure Firewall 3100 Performance

FTD 7.2

ASA 9.18

	3105	3110	3120	3130	3140
FW+AVC+IPS 1024B Avg Packet	10Gbps	17Gbps	21Gbps	38Gbps	45Gbps
IPsec VPN 1024B Avg Packet	5.5Gbps	11Gbps	13.5Gbps	33Gbps	39Gbps

最大で 7x FW+AVC+IPS 利用時

最大で 17x IPsec VPN 利用時

最大で 14x TLS 利用時

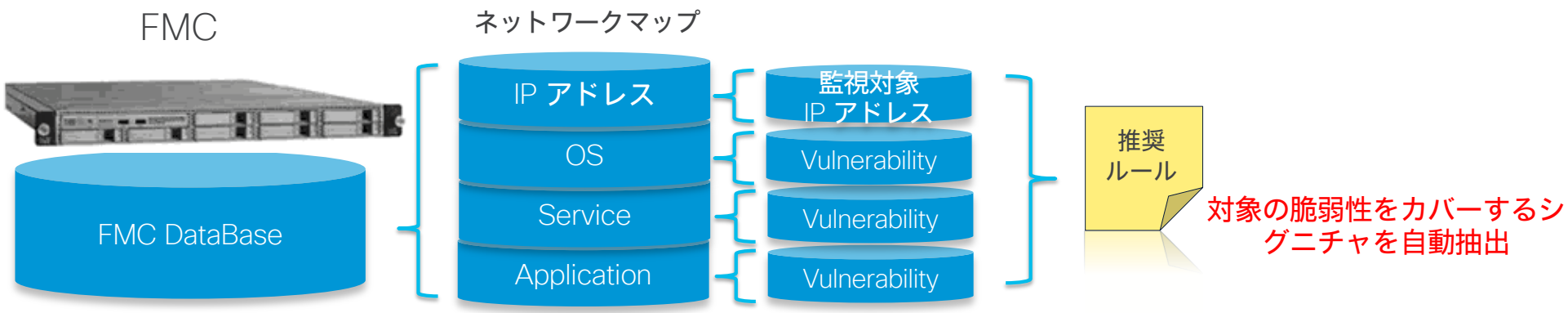
Threat Protection

自動チューニング

FTD Basic

- 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

FTD Basic

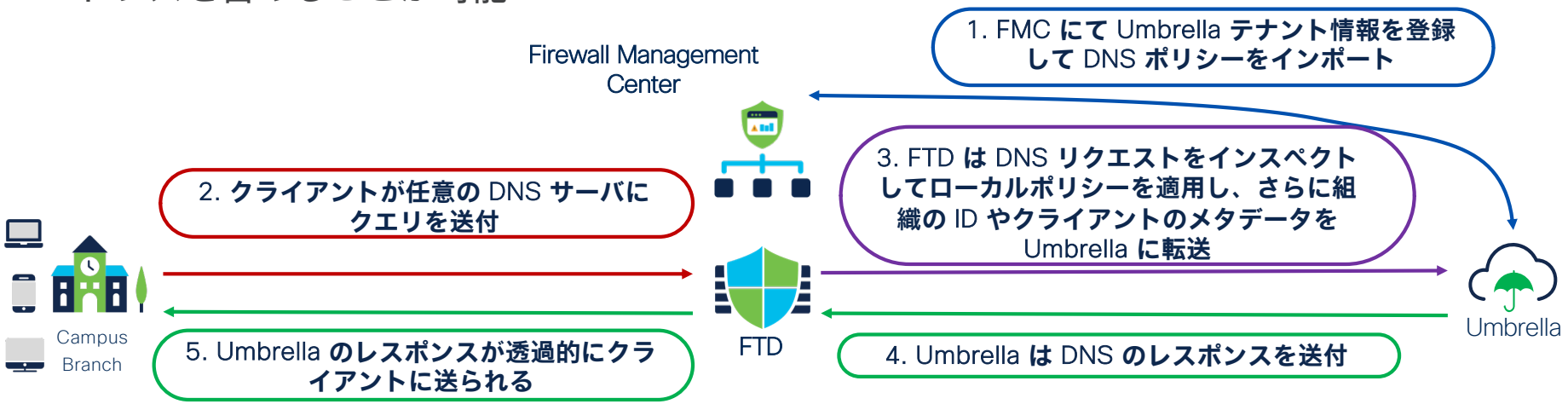
- 全ての IPS イベントを、ターゲットホストの脆弱性情報と関連づけて解析
- 緊急度の高いイベントのみに、高インパクトのフラグを付けてアラート
  - インパクトフラグ1 – 即時対応が必要
    ※ IDS (パケットドロップなし) の場合
  - インパクトフラグ2 – 要調査
  - インパクトフラグ3 – 対応の必要なし

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

Umbrella への DNS リダイレクト

FTD 7.2

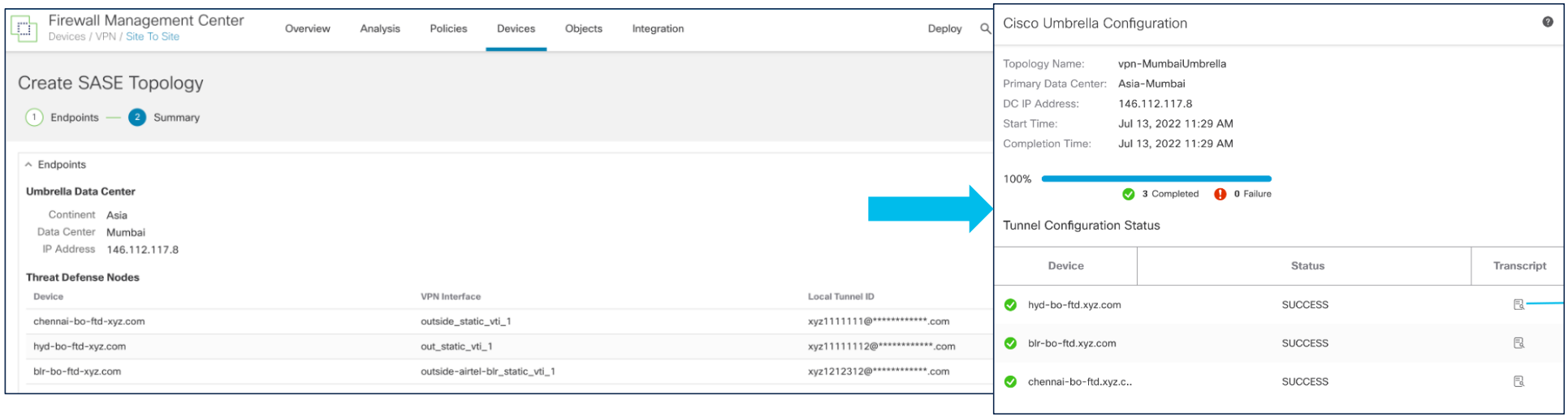
- Umbrella をレジストした FMC は双方向でインテグレーションされる
  - Umbrella DNS ポリシーを FTD の Access Control Policy に適用可能
  - FTD はインラインにて組織の ID やデバイスの認証情報、オリジナルのクライアントの IP アドレスを含めることが可能



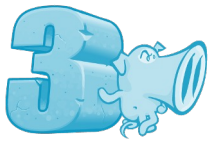
Umbrella への SASE トポロジー自動トンネル

FTD 7.3

- FMC の SASE トポロジーにて全ポートのトラフィックを Umbrella SIG に転送
  - 双方向プロビジョニングを簡略化するために DNS コネクタを設定
  - ポリシーベースの転送のために Virtual Tunnel Interface (VTI) を設定
  - トンネル毎のカスタム IKE ID を使った複数トンネルへのロードバランス



参考サイト (日本語 Cisco Community 記事):
https://community.cisco.com/t5/-/-/ta-p/4800965



Snort 3 IPS エンジン

FTD 7.0+

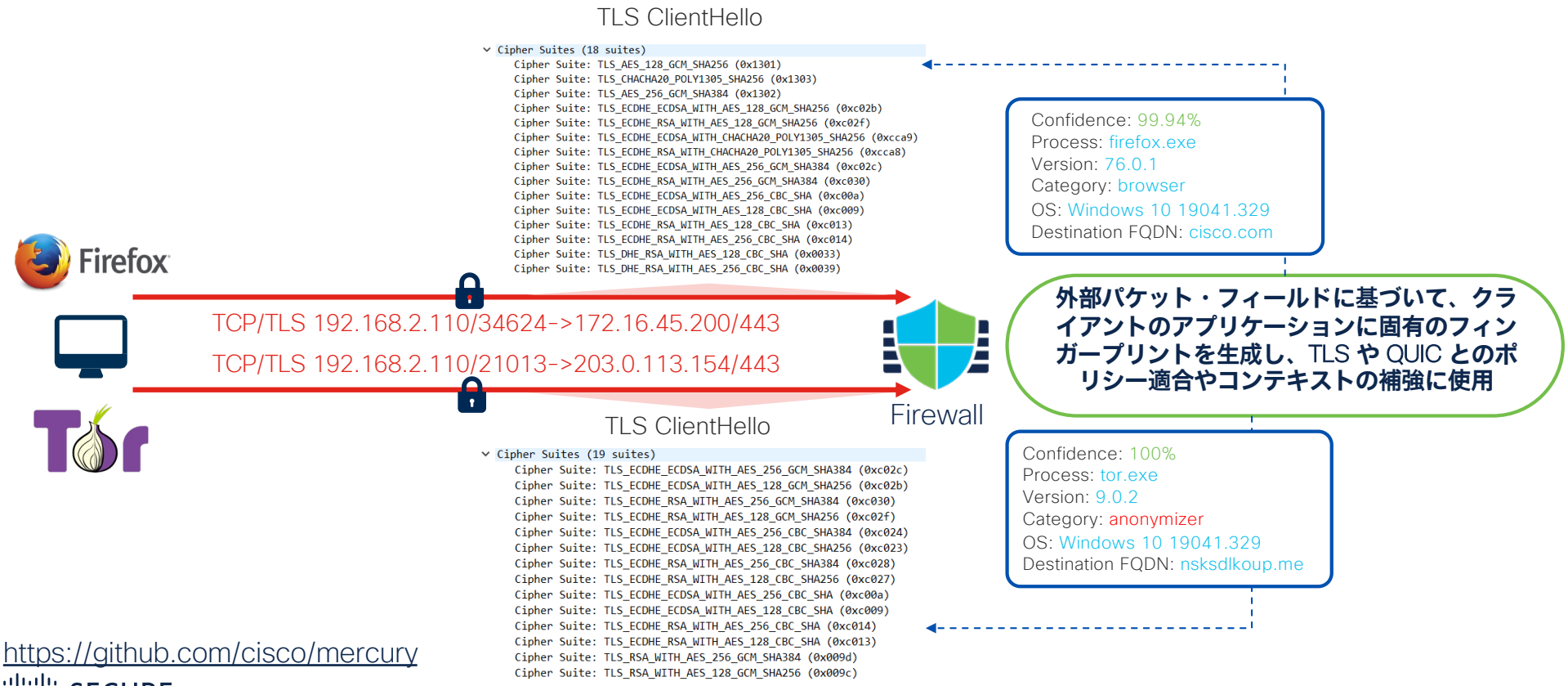
- 信頼性の高い NGIPS エンジンのアップデートにより、最新の脅威を阻止
  - マルチスレッドアーキテクチャにより、有効性とパフォーマンスが大幅に向上
  - HTTP/2 や QUIC などの最新プロトコルをネイティブでサポート
  - 人間が読めるシグニチャ・ルールの記述方法
  - ルールグループにより 1つのポリシー内で検査レベルを調整可能
- 利用価値が高い Snort 3 が必要な新機能
  - 機械学習が可能な Encrypted Visibility Engine (EVE) でのセキュリティ機能
  - 包括的なポートスキャン攻撃検知と防止
  - ネイティブでの TLS 1.3 復号
  - エレファントフローの検知とインパクト軽減機能

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

Encrypted Visibility Engine (EVE)

FTD 7.1



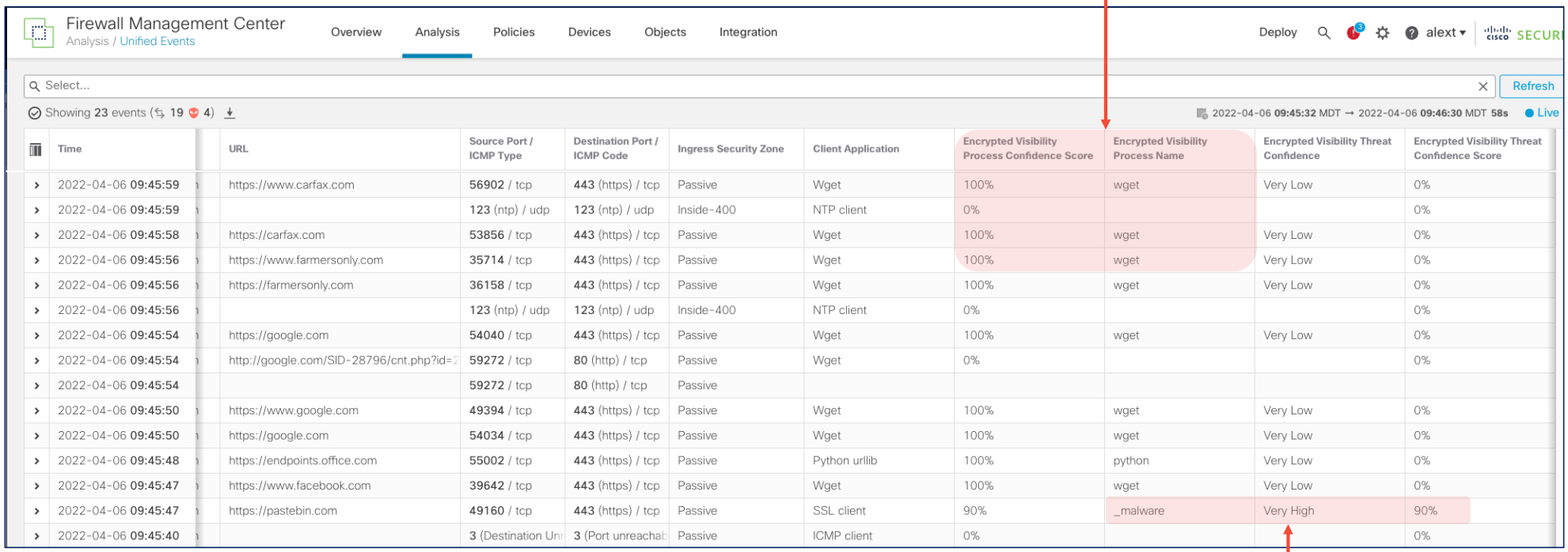
https://github.com/cisco/mercury

cisco SECURE

EVE - Unified Events

FTD 7.1

クライアントのプロセス名と検知の信頼度スコア; プロセス名には FTD 7.2 よりカスタム AppID 作成へのリンクが張られる



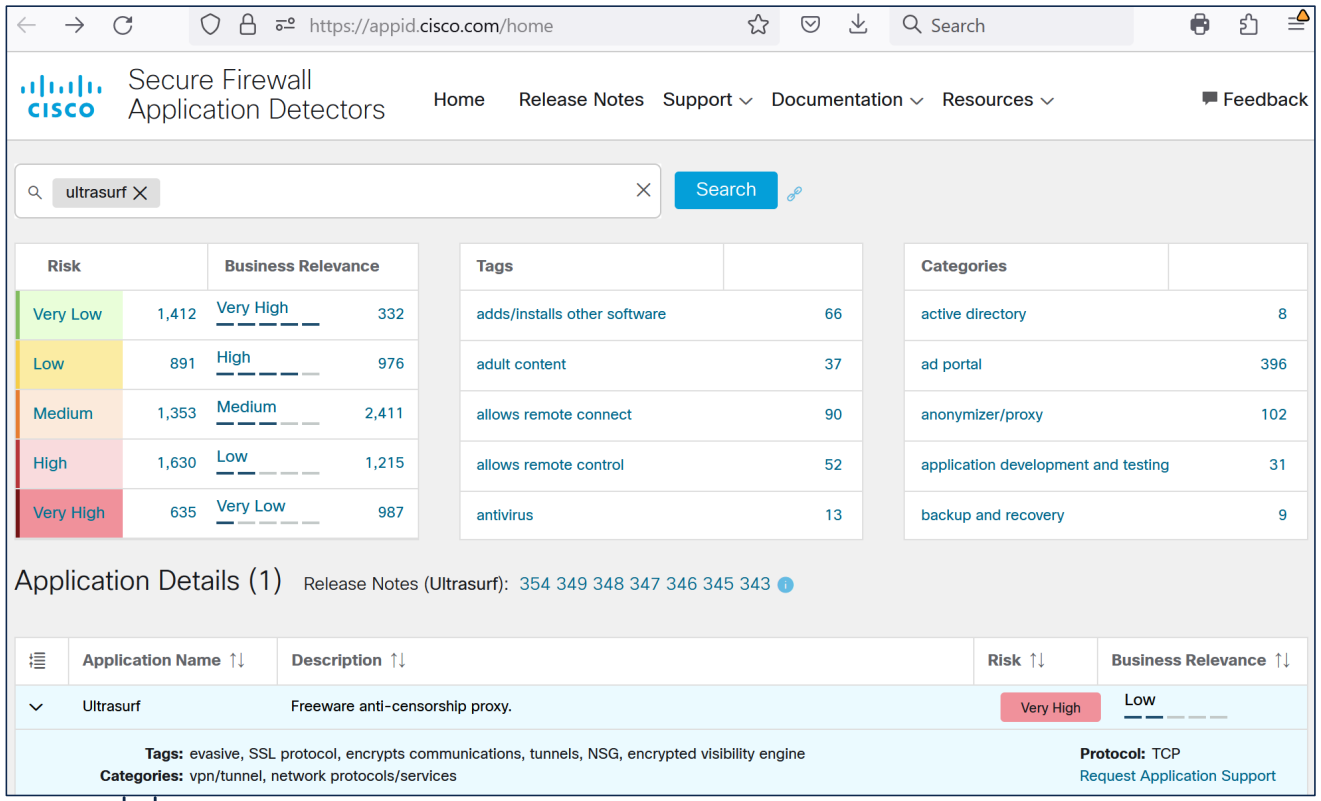
Time	URL	Source Port / ICMP Type	Destination Port / ICMP Code	Ingress Security Zone	Client Application	Encrypted Visibility Process Confidence Score	Encrypted Visibility Process Name	Encrypted Visibility Threat Confidence	Encrypted Visibility Threat Confidence Score
2022-04-06 09:45:59	https://www.carfax.com	56902 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:59		123 (ntp) / udp	123 (ntp) / udp	Inside-400	NTP client	0%			0%
2022-04-06 09:45:58	https://carfax.com	53856 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:56	https://www.farmersonly.com	35714 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:56	https://farmersonly.com	36158 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:56		123 (ntp) / udp	123 (ntp) / udp	Inside-400	NTP client	0%			0%
2022-04-06 09:45:54	https://google.com	54040 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:54	http://google.com/SID-28796/cnt.php?id=	59272 / tcp	80 (http) / tcp	Passive	Wget	0%			0%
2022-04-06 09:45:54		59272 / tcp	80 (http) / tcp	Passive					
2022-04-06 09:45:50	https://www.google.com	49394 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:50	https://google.com	54034 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:48	https://endpoints.office.com	55002 / tcp	443 (https) / tcp	Passive	Python urllib	100%	python	Very Low	0%
2022-04-06 09:45:47	https://www.facebook.com	39642 / tcp	443 (https) / tcp	Passive	Wget	100%	wget	Very Low	0%
2022-04-06 09:45:47	https://pastebin.com	49160 / tcp	443 (https) / tcp	Passive	SSL client	90%	_malware	Very High	90%
2022-04-06 09:45:40		3 (Destination Un	3 (Port unreachab	Passive	ICMP client	0%			0%

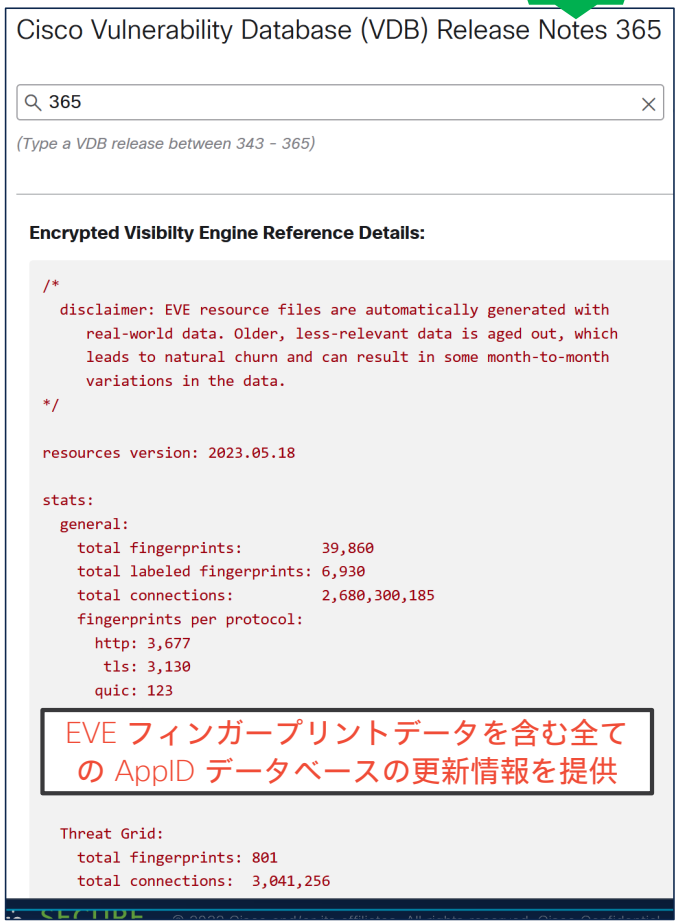
推測されるアラートレベルとその信頼度

AppID ポータル: https://appid.cisco.com

Now

Firewall Management Center で設定可能な全てのアプリケーションリストを提供

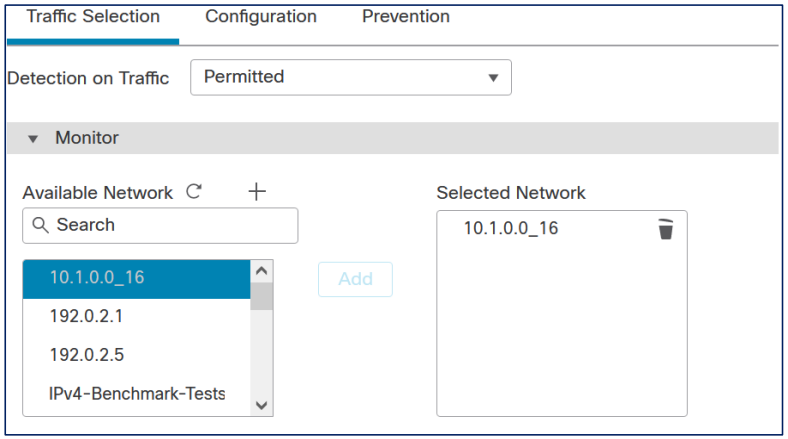


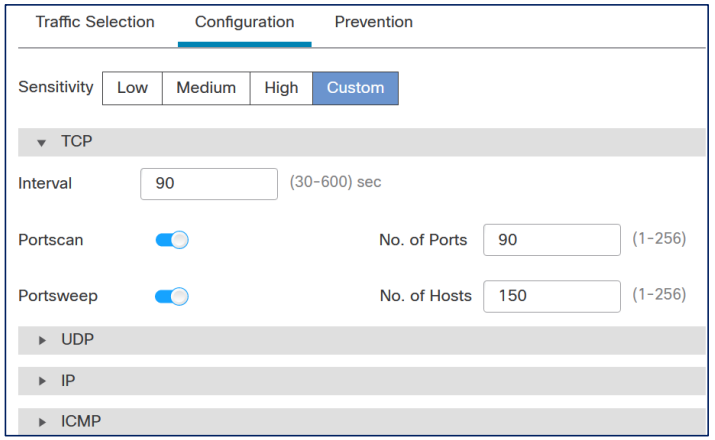


Portscan の検知と防止

FTD 7.2

- 進化した Portscan の検知エンジンをデータプレーンに直接搭載
  - パフォーマンスと検出効果が大幅に向上
  - シングルホスト、デコイ、分散型、ポートスイープスキャンを認識
  - オプションで潜在的な攻撃者を時間ベースでブロック
- Access Control Policy レベルできめ細かいプロファイル設定が可能

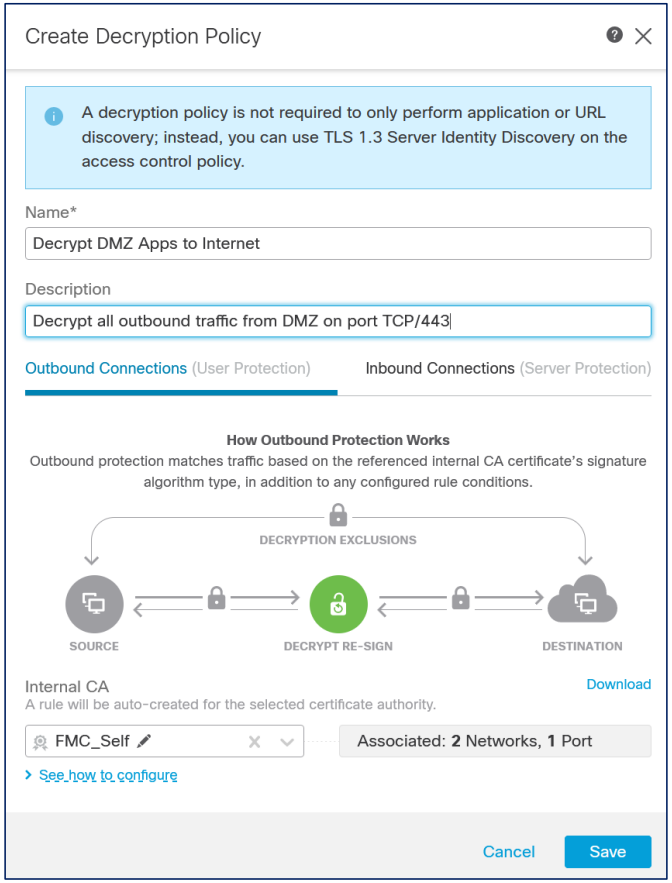




簡素化された TLS Decryption Policy

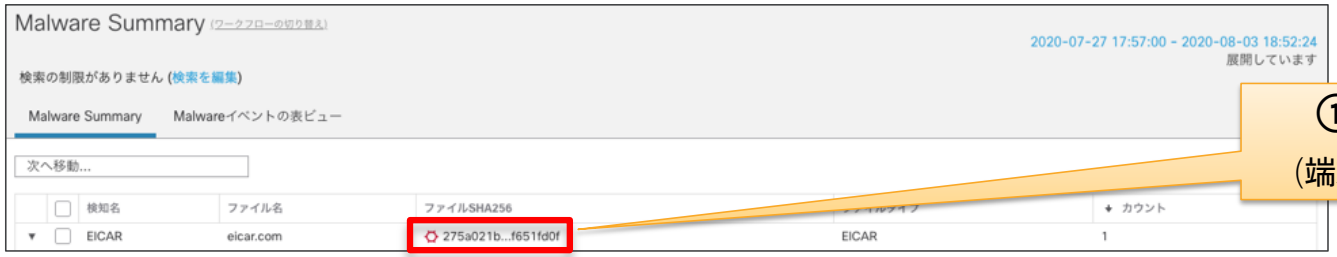
FTD 7.3

- 復号は可視化のために必ずしも必要とは限らない
  - 復号しなくても URL フィルタやいくつかの AppID は動く
  - IPS と File/Malware ポリシーには復号が必要
- ネイティブで TLS 1.2 と 1.3 を復号可
- ウイザードスタイルでの Decryption Policy
  - Outbound は、多くのSaaS アプリケーションに対して効果が無い
  - Inbound はアプリケーションサーバに対してコントールが可能

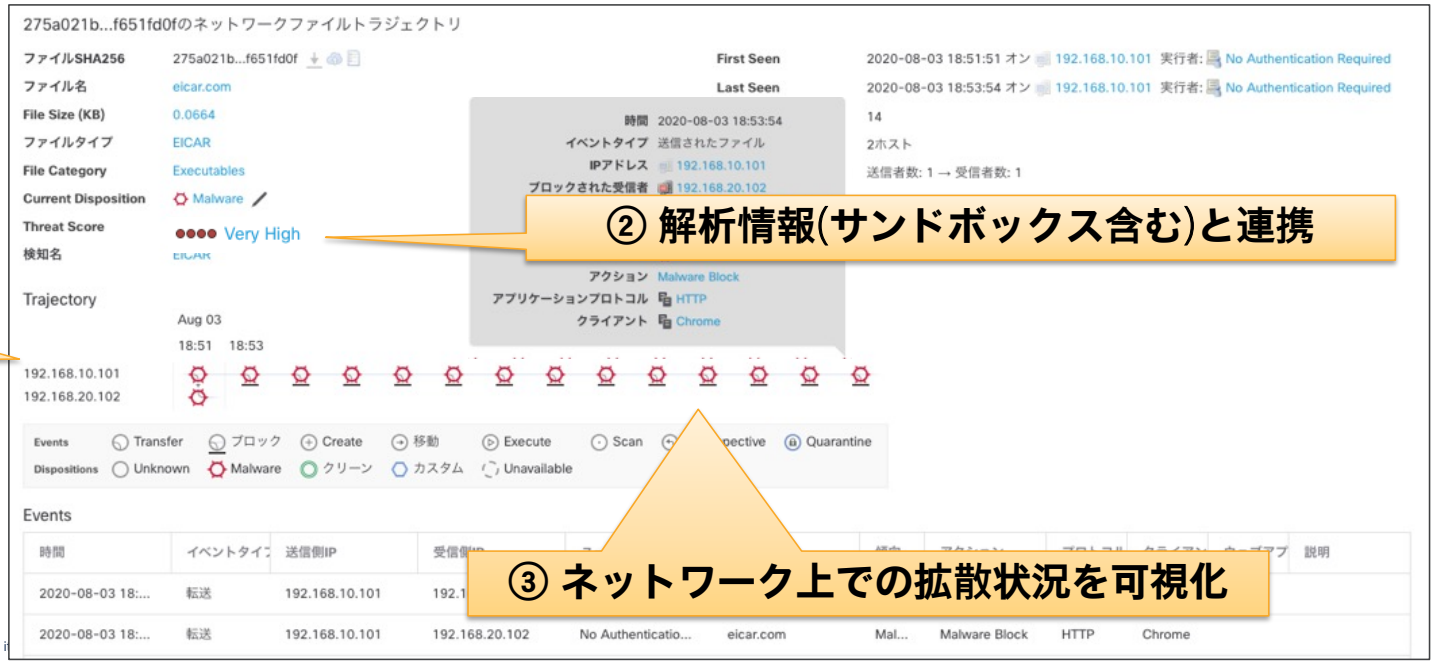


Malware Defense マルウェアの可視化と制御、トラッキング

FTD Basic



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

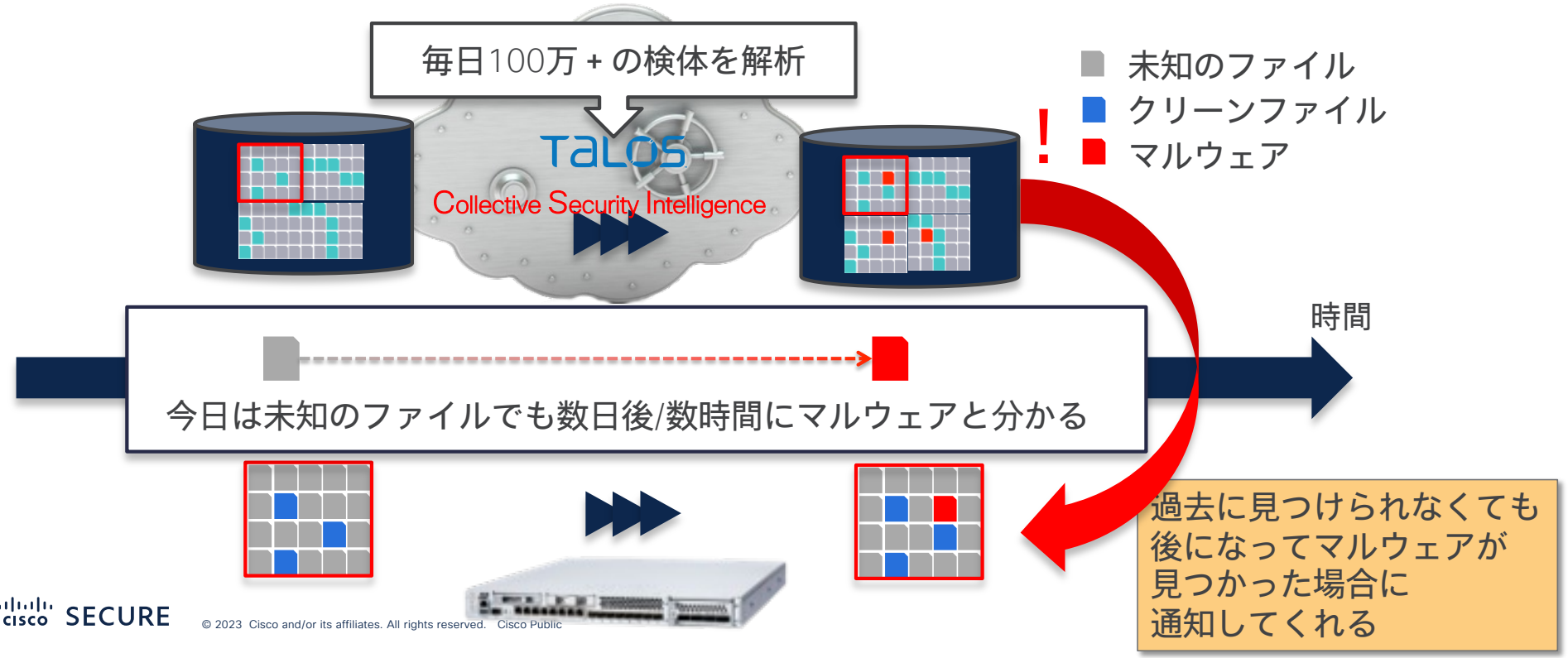
③ ネットワーク上での拡散状況を可視化

④ 端末の特定

Malware Defense クラウドリコール

FTD Basic

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

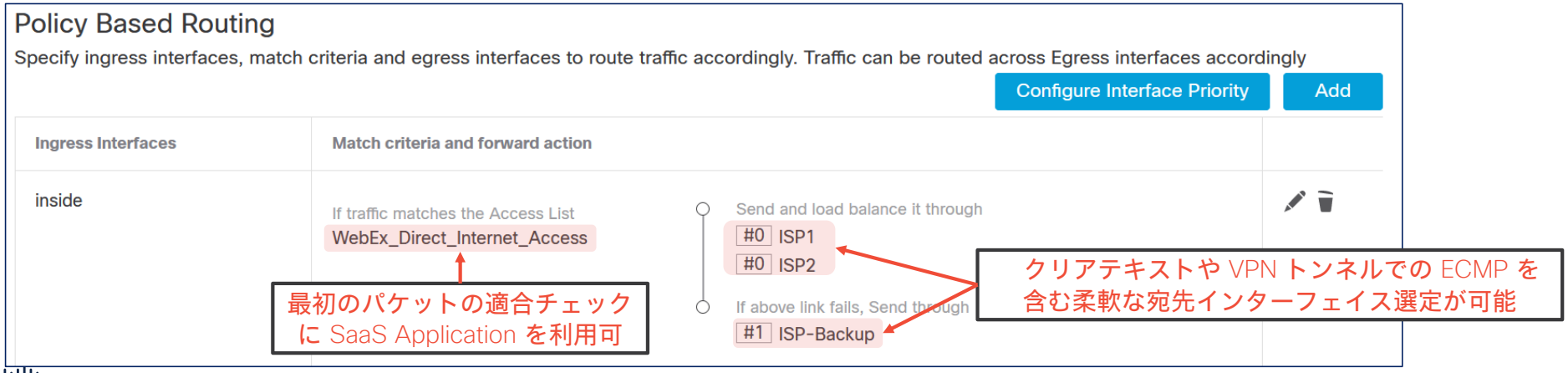


Connectivity

Application Base の Policy Based Routing

FTD 7.1

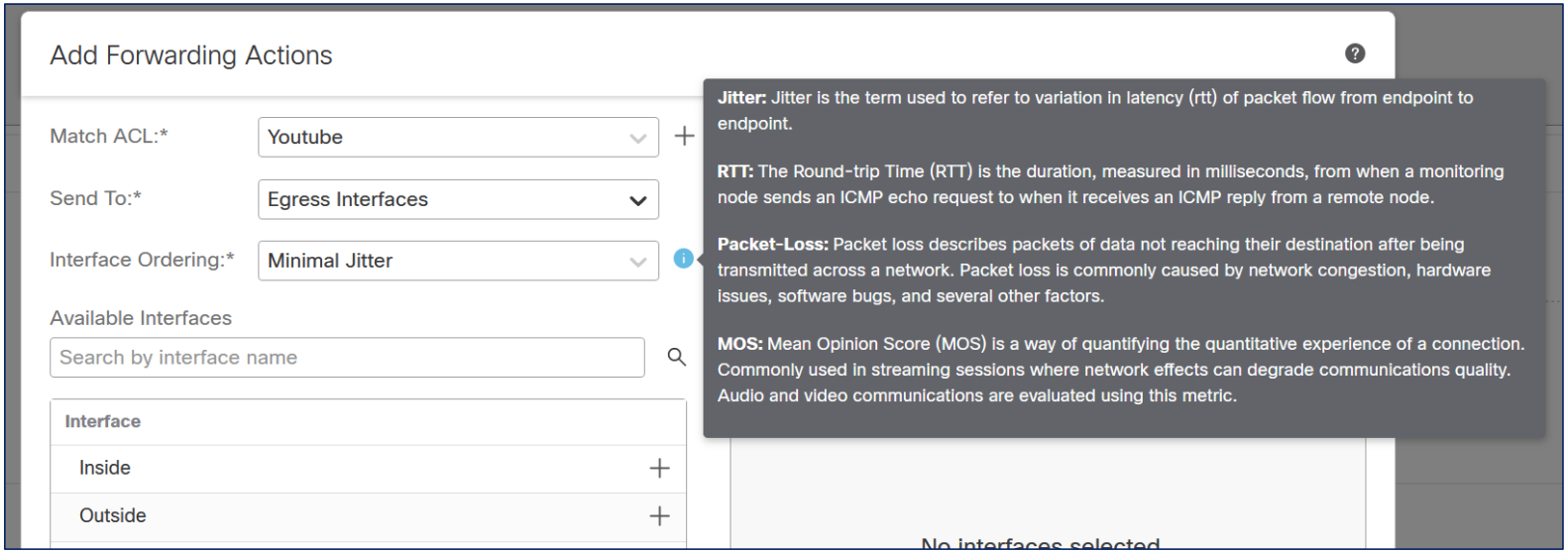
- FMC での Policy Based Routing をネイティブでサポート
  - 一般的に SaaS Application 利用時の条件として利用
  - ドメインパターンマッチングのための Trusted Server 用に DNS スヌーピングを利用
  - Data Plane は Network Service Group 用のアプリケーションと IP アドレスのマッピングを実施
- WAN での Direct Internet Access (DIA) のブレークアウトとして利用される



Path Monitoring および Quality-Based Routing

FTD 7.2

- ポリシーベースのインターフェイス選定はパスの品質を条件に含むことが可能
  - インターフェイス毎の ICMP ベースのネクストホップや外部 IP アドレスのモニタリング
  - HTTP(S) ベースの SaaS Application トラッキングは FTD 7.4 でサポート



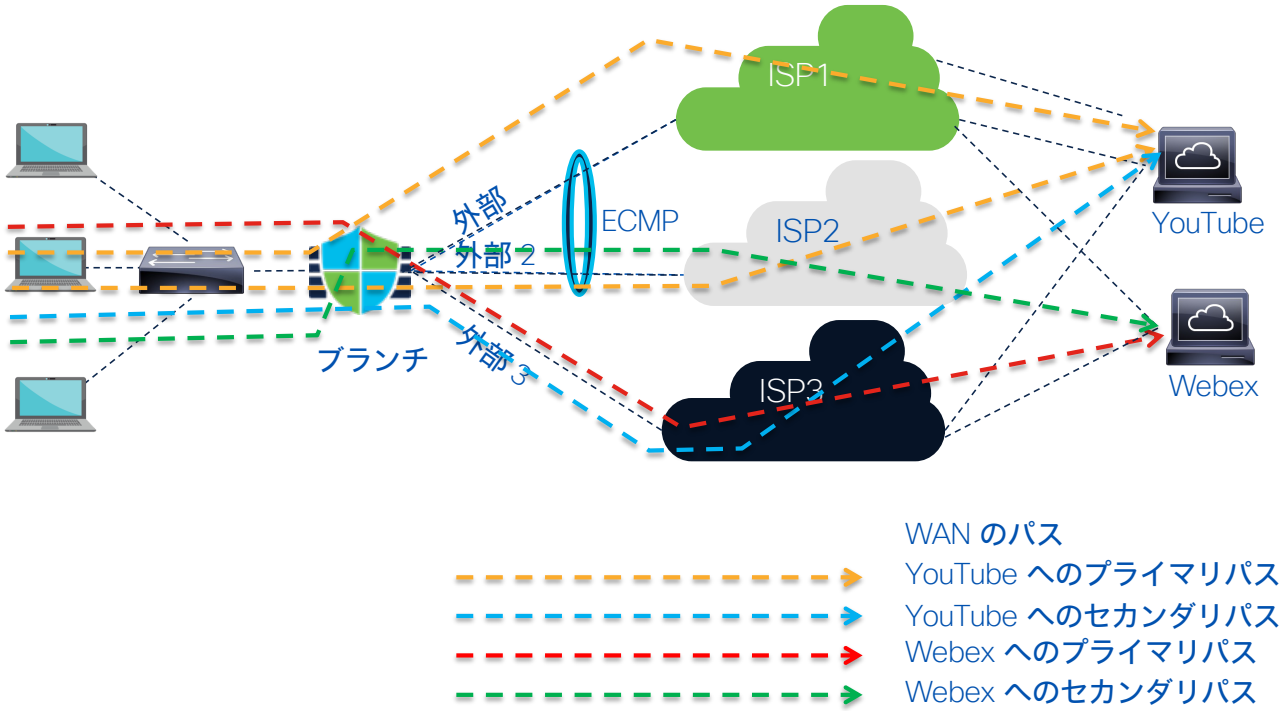
Application Routing の例

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

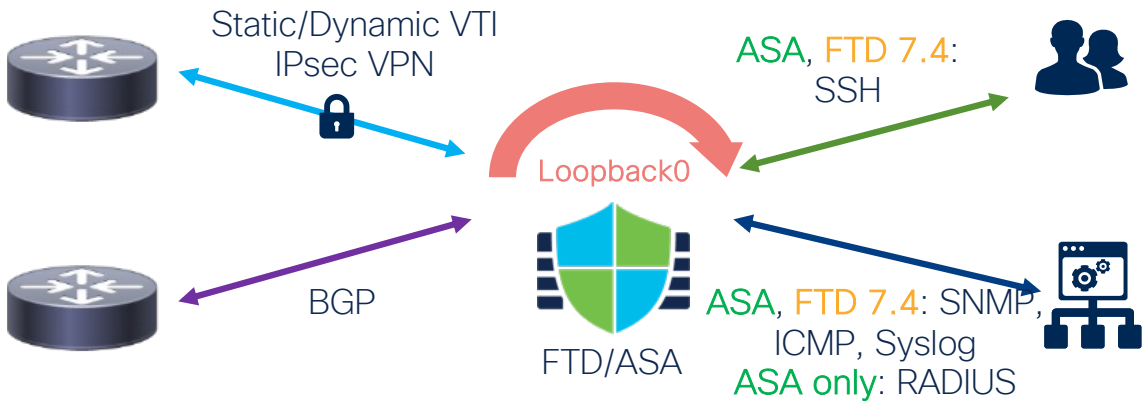


Loopback Interface

FTD 7.3+

ASA 9.18.2

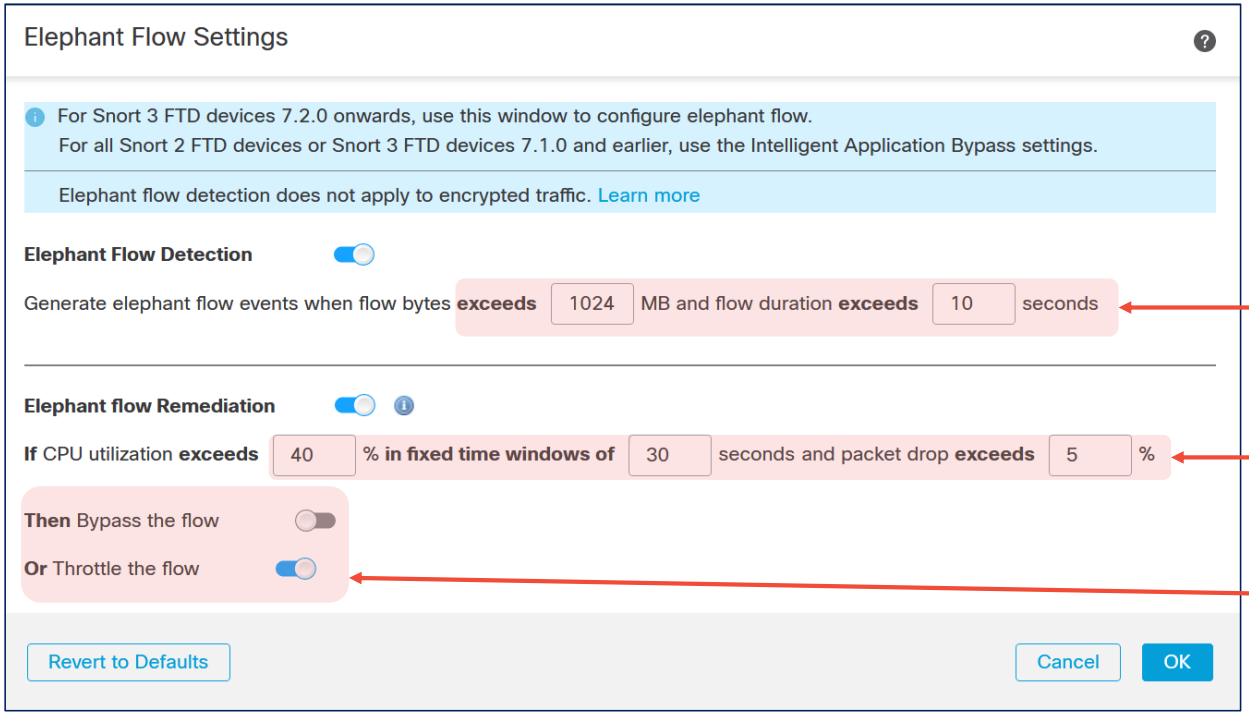
- 物理インターフェイスを経由した To / From デバイスの概念的なインターフェイス
  - ルーテッド・トランスペアレント (VTI 除く) モードでの IPv4/IPv6 アドレス
  - HA/failover および clustering (VTI 除く) をサポート



Elephant Flow Detection

FTD 7.2

- フロー毎のトラッキングは Intelligent Application Bypass (IAB) に代わって当機能で実現



エレファントフローと判断するスループットの閾値

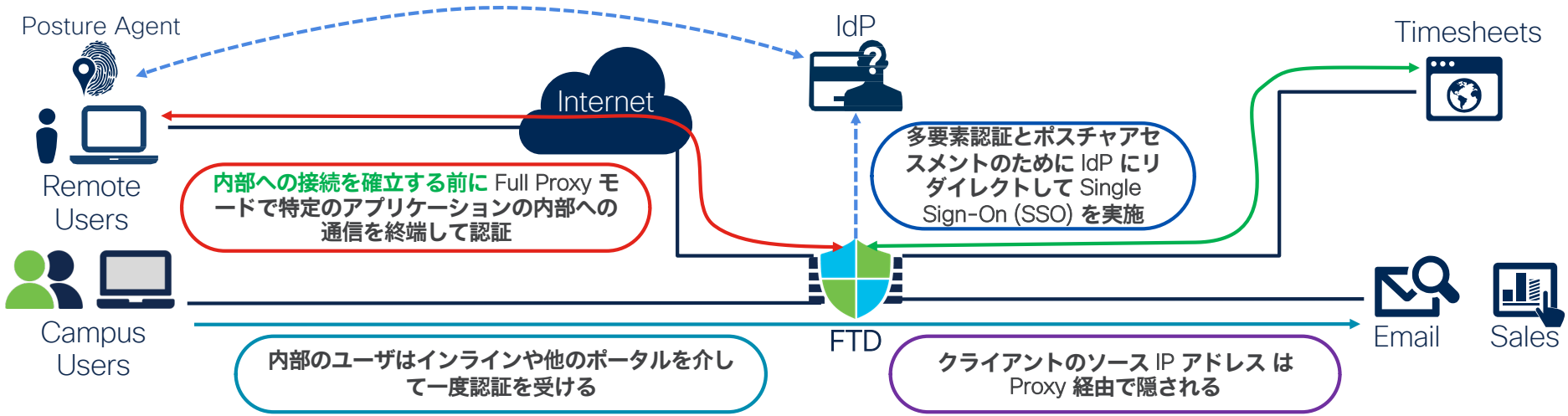
オプションで CPU リソースの使用率やパケットドロップ率を条件としてエレファントフローを制御可能

オプションでのフロー制御アクションの設定

Clientless Zero Trust App Access (ZTAA)

FTD 7.4

- Captive Portal の機能を Full Reverse Proxy に拡張
  - ポスチャアセスメントの機能を含む 外部の Identity Provider (IdP) と連携



Private & Public Cloud
(Cisco Multicloud Defense 含む)

cisco SECURE

Hybrid Cloud での継続的なプロテクション

FTD 7.2

Private Cloud

HyperFlex

vmware ESXi

KVM

NUTANIX

openstack.

Public Cloud

Microsoft Azure

Google Cloud Platform

aws

rackspace technology

EQUINIX

ORACLE CLOUD INFRASTRUCTURE

Alibaba Cloud

alkira

Secure Firewall Capabilities

- ネットワーキングの拡張
- スナップショットを使った導入の簡素化
- Gateway Load-Balancer の入れ込みと FWaaS
- Clustering & Auto Scaling
- 機敏性のためのInfrastructure-as-Code と自動化
- クラウドサービスや管理とのインテグレーション
- Dynamic Policy
- Smart & Tiered Licensing

cisco SECURE

Automation with Infrastructure-as-Code

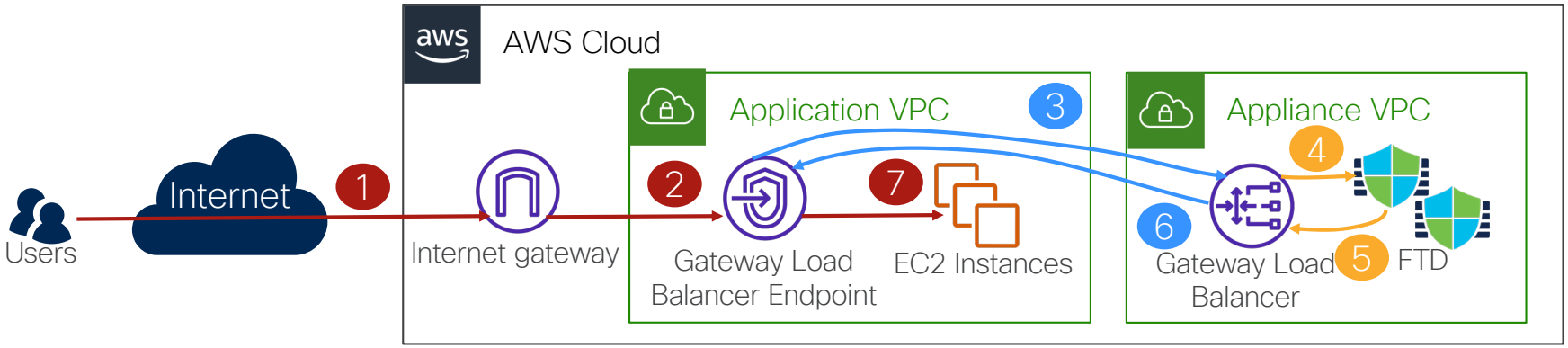
- Public Cloud のテンプレートを使った Secure Firewall のインスタンス
- ASA と FTD (FMC 経由) 用の宣言型 Teraform テンプレート
  - HashiCorp Consul と連携した FTD Dynamic Object
- ASA と FTD (FDM と FMC) 用の Ansible タスク
- Cisco DevNet のリポジトリは継続して更新
  - https://developer.cisco.com/secure-firewall/cloud-resources/
  - https://github.com/CiscoDevNet/secure-firewall
  - https://github.com/CiscoDevNet/FMCAnsible

Gateway Load-Balancer in aws and Azure

FTD 7.1+

ASA 9.17+

- インバウンド・アウトバウンドフローへの Network firewall service の入れ込み
  - GEneric NEtwork Virtualization Encapsulation (GENEVE) でのリダイレクト
  - ソフトウェアで実現可能な Bring-your-own TLS 復号

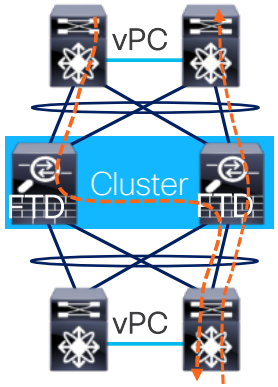


- Autoscale およびスナップショットを使ったインスタンス化は FTD 7.2 と ASA 9.18 からサポート

Clustering for Virtual Firewalls

FTD 7.1+ ASA 9.17+

- Clustering で複数の Firewall を論理的な1つの Firewall として利用可能
  - トラフィックを止めることなくシームレスに 16ユニットの FTD までスケールアップ
  - 非対称トラフィックや障害時のリカバリーをステートフルに実現
  - シングルポイントでの管理と統合レポーティング



- Hybrid Cloud における Clustering による弾力性と障害処理の向上
  - aws Google Cloud Platform Azure KVM vmware
  - 1つの Port-channel に代わって Individual data interface への IP アドレス付与
  - Control Plane へのユニキャスト通信のための VxLAN を使った Cluster Control Link
  - 非対称通信のハンドリング用の ソース NAT は不要
  - サポートされている環境での障害発生時に既存フローを再ホスト

Attribute-Based Policies

FTD 7.0+

Custom Orchestrator

Push Model: Attribute Mapping の同期を作成・更新するための FMC REST API

vmware aws Azure Office 365 GitHub

Dynamic Attribute Connector

Pull Model: ほぼリアルタイムでの更新を行うための特定のオーケストレータへの接続

		Source		Destination		
Name	Action	Networks	Dynamic Attributes	Networks	Dynamic Attributes	Applications
Allow Windows Updates	Allow	Any	Windows_OS	Any	Any	Windows Update
Allow WebApp to DB	Allow	Any	WebApp_Logic	Any	DB_Cluster	Any

FMC

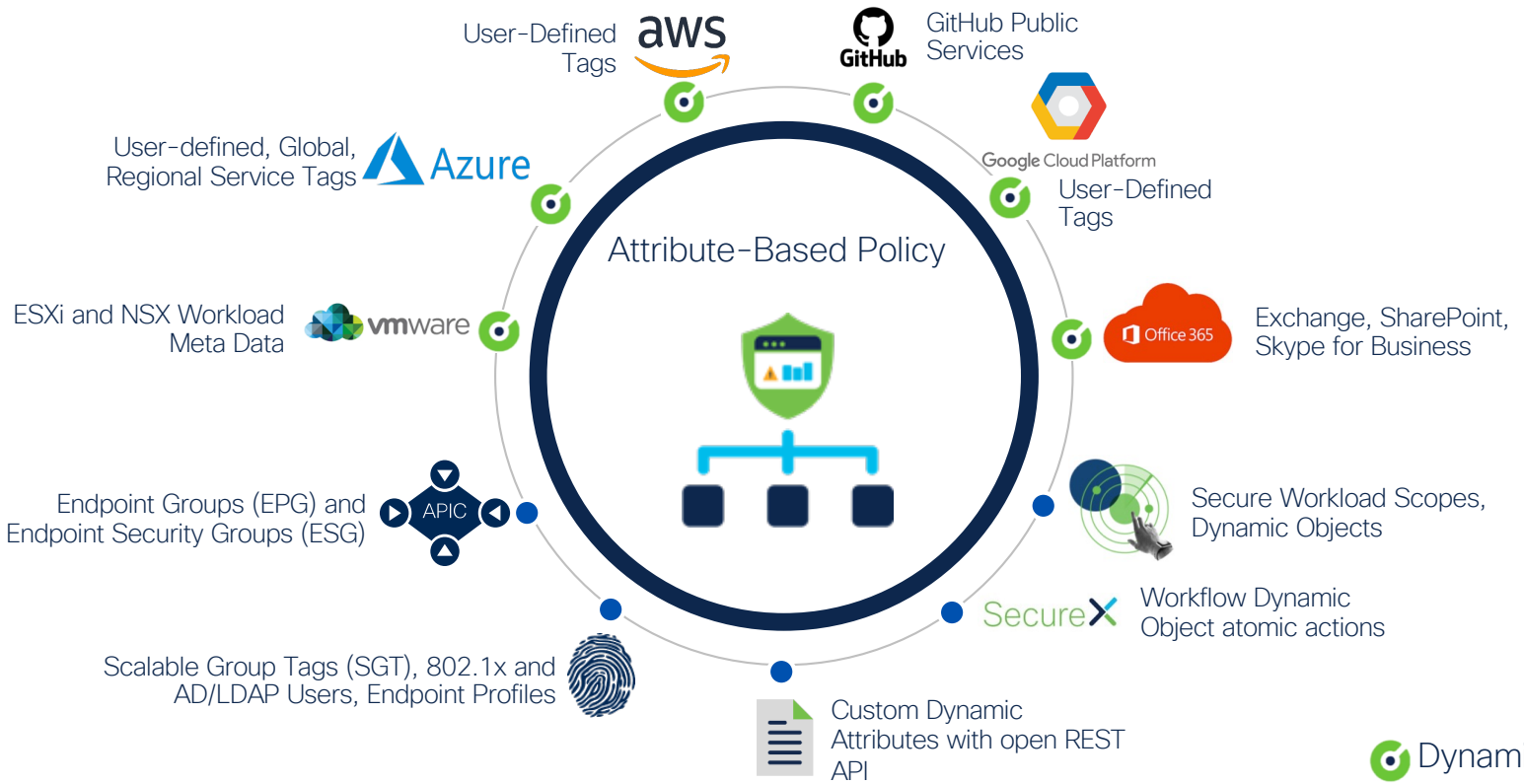
Label	IP Address
WebApp_Logic	192.168.1.151
Windows_OS	192.168.1.120-130
DB_Cluster	172.16.45.90

deploy を行うことなくリアルタイムでのマッピング情報の更新を実現

FTD FTD FTD

Firewall Policy の抽象化

FTD 7.0+



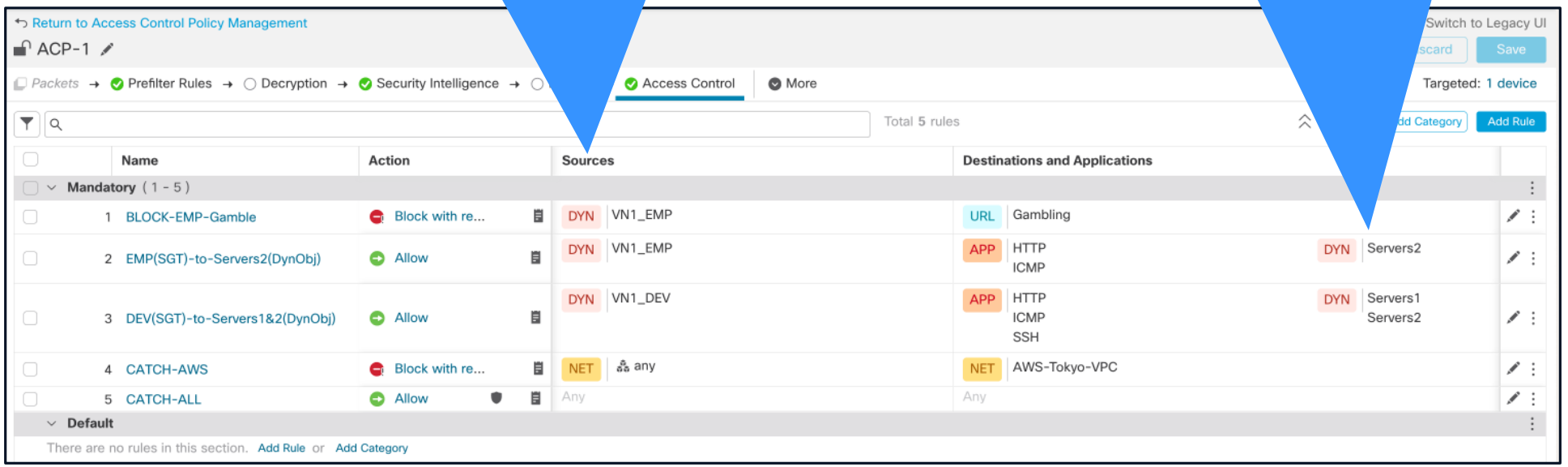
Dynamic Attribute Connector

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

Cisco Multicloud Defense の登場

バラバラになっている箇所を集中管理

Now

クラウド間で共通セキュリティ

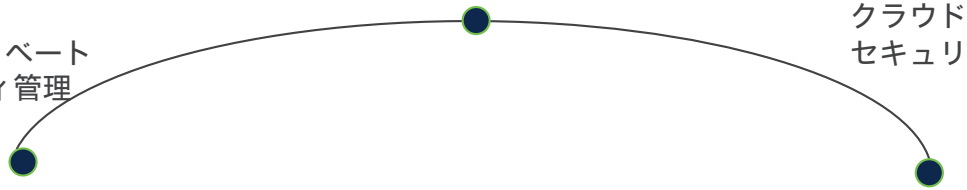
単一ポリシーで、
AWS, Azure GCP, OCI とプライベート
クラウドを跨いでセキュリティ管理

あらゆる方向の保護

アプリを狙った攻撃や、C&C 通信だけで
なく、ラテラルムーブメントも阻止可能

リスクとコストを一緒に軽減
作業の効率性重視

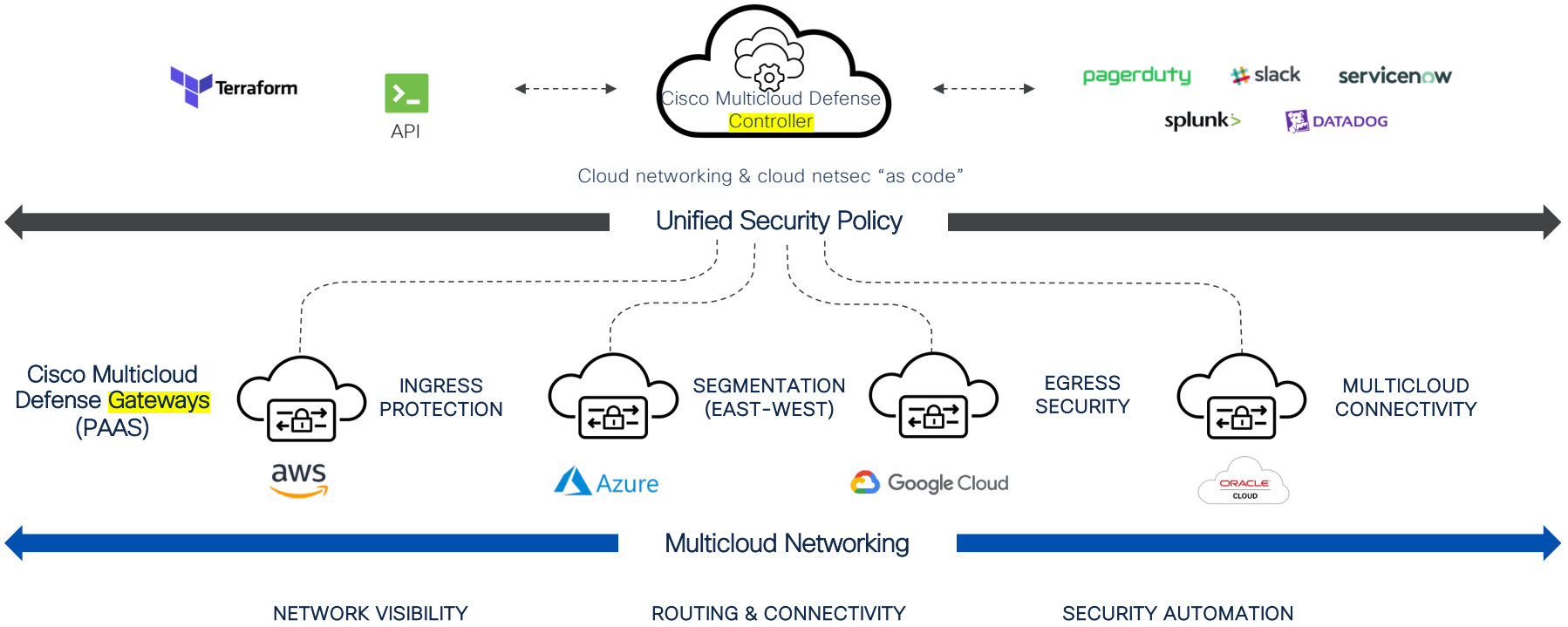
クラウドアンダーレイの自動化により、
セキュリティと共に作業の効率化も実現



Cisco Multicloud Defense

マルチクラウドネットワーク、 自動化、Cloud-nativeなネットワークセキュリティ制御を一元化

Now



Multicloud Defense Gateways

Now

Ingress Gateway

- ✓ Reverse Proxy
- ✓ TLS decrypt
- ✓ WAF – L7 DoS
- ✓ IDS / IPS
- ✓ Antivirus
- ✓ Geo IP
- ✓ Malicious IP

Egress Gateway

Egress

- ✓ URL filtering
- ✓ Forward proxy
- ✓ TLS decrypt
- ✓ FQDN filtering*
- ✓ FQDN-based firewall policy
- ✓ DLP
- ✓ IDS / IPS
- ✓ Antivirus

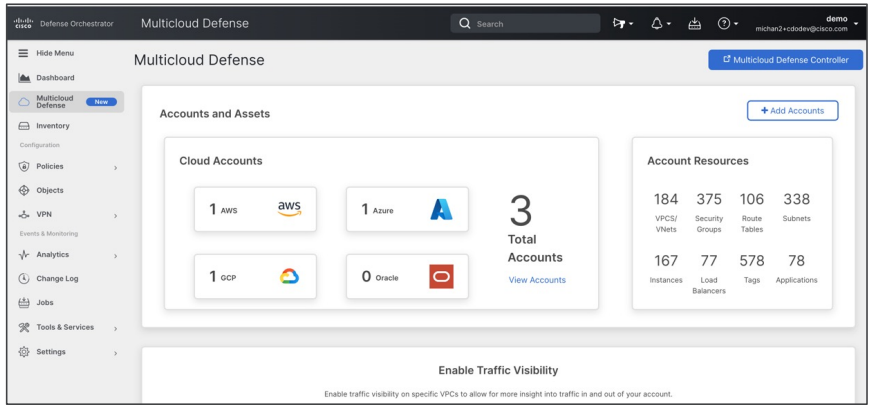
East/West

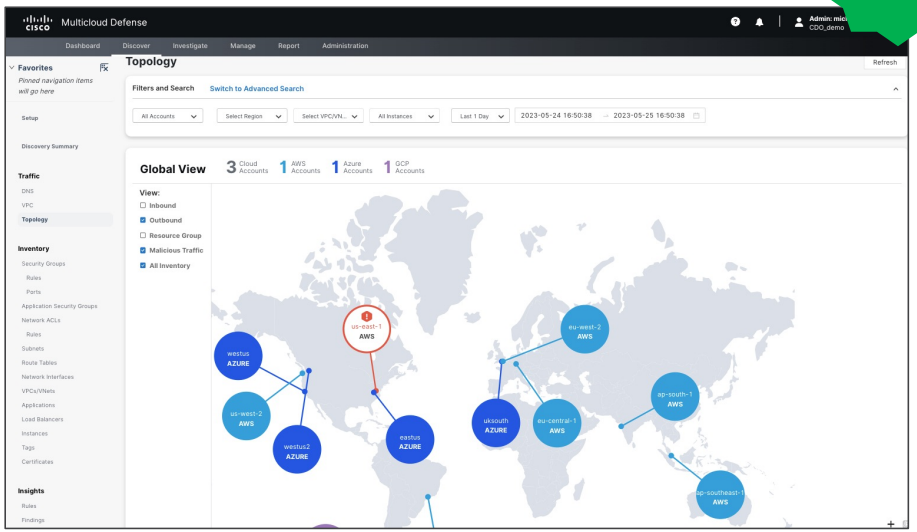
- ✓ FQDN filtering
- ✓ IPS / IDS
- ✓ Antivirus
- ✓ L4 firewall
- ✓ Micro-segmentation
- ✓ FQDN-based firewall policy

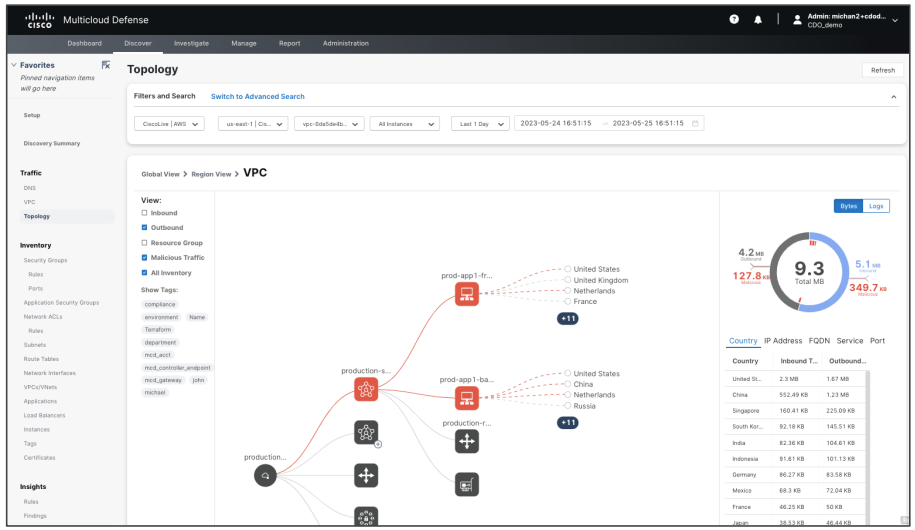
** TLS decryption **無しで動作可能***

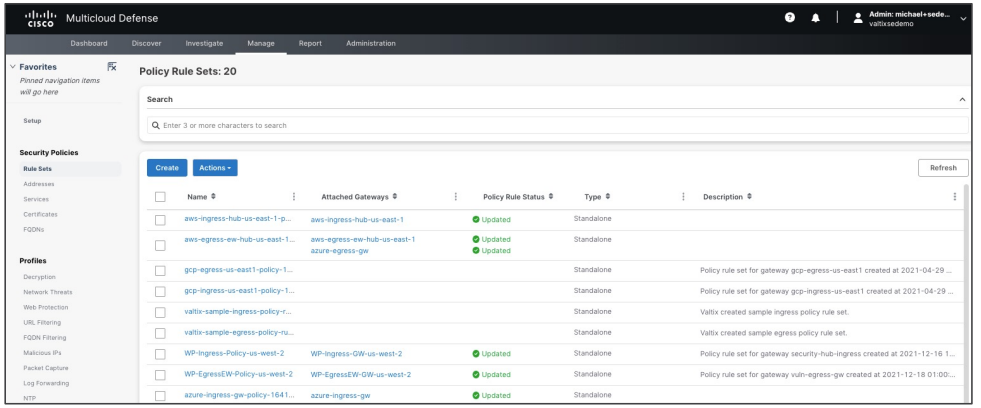
Multicloud Defense Controller

Now





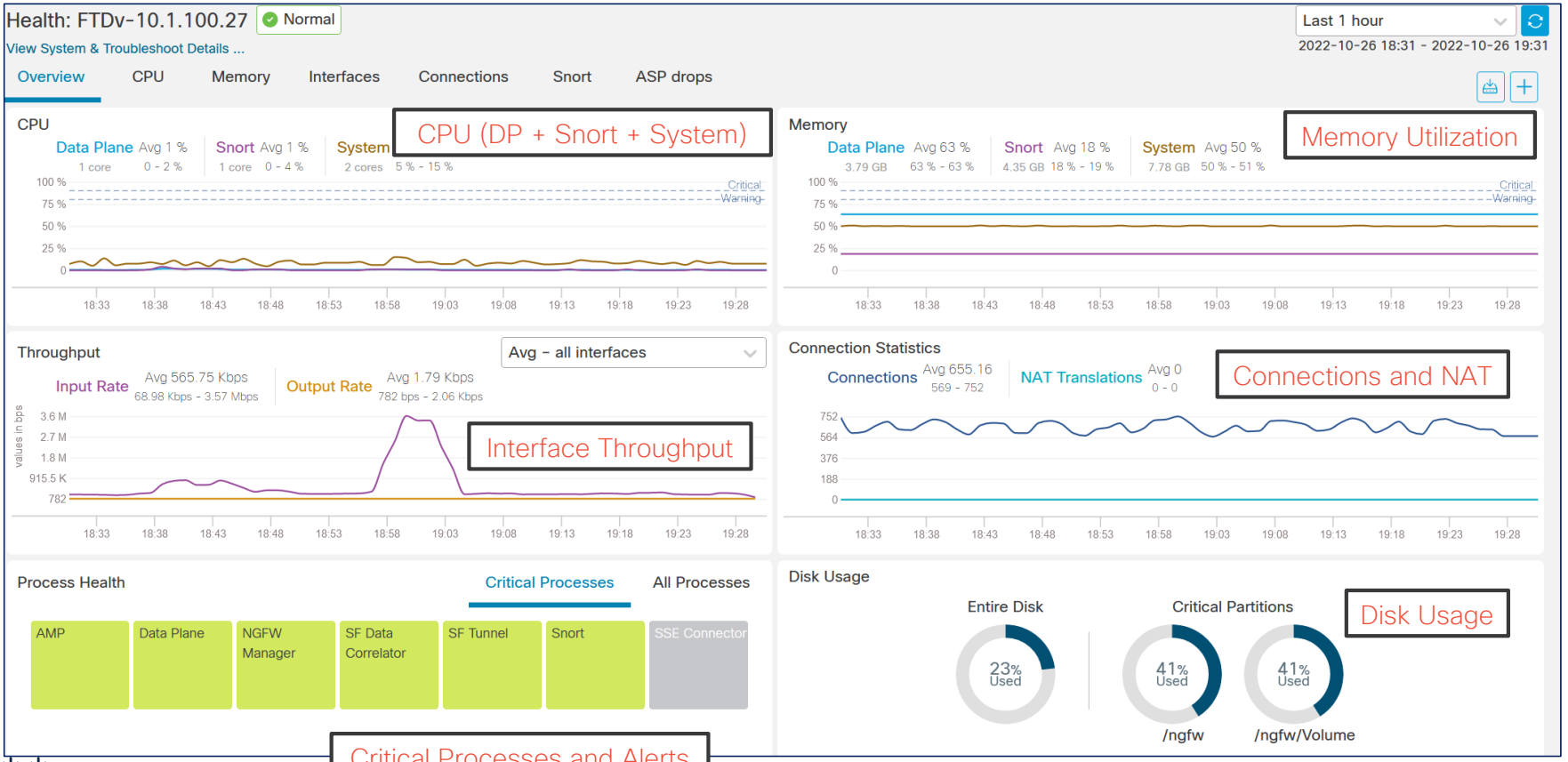




Management

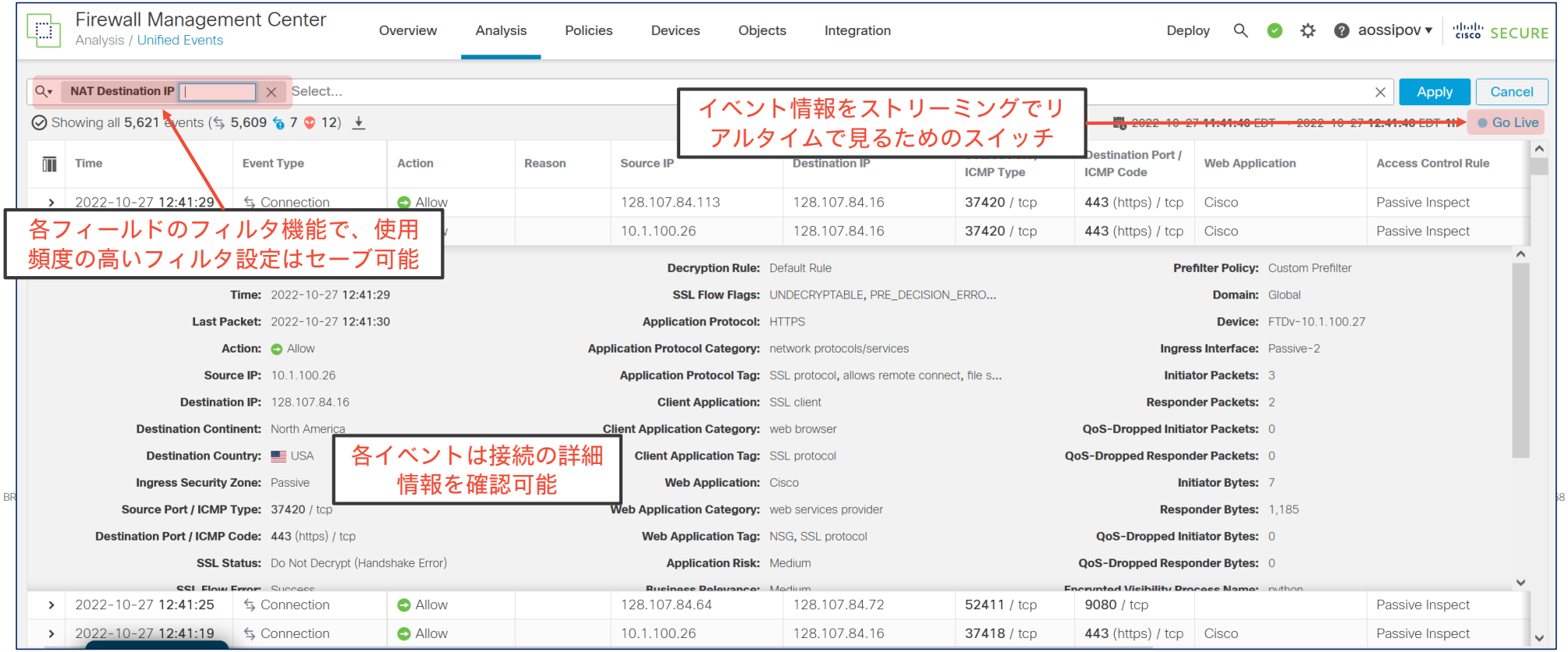
FTD Health Dashboard

FMC 6.7+



Unified Events with Live View

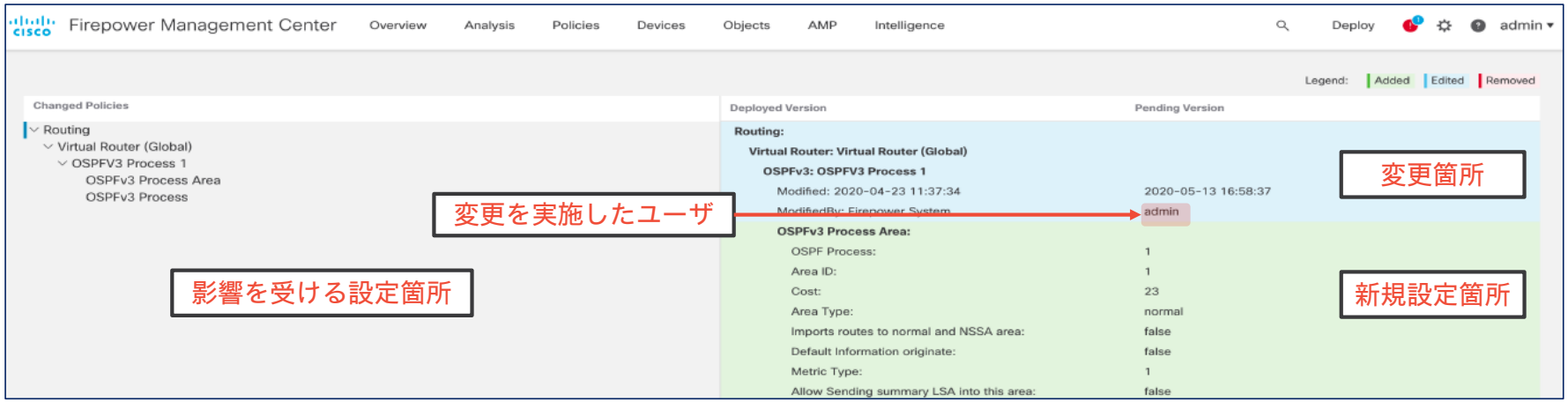
FMC 7.0



変更管理

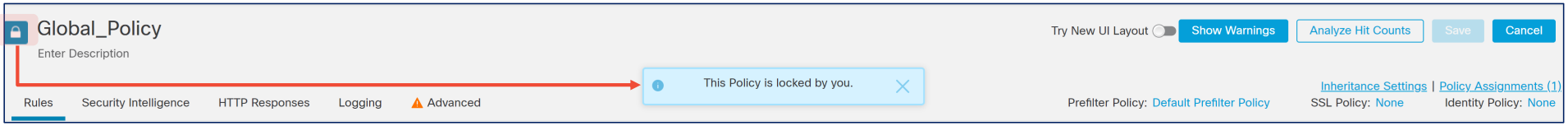
FMC 7.0

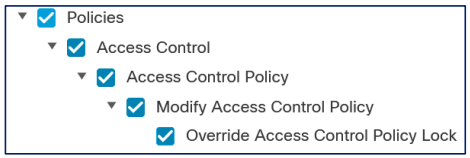
- 変更箇所を選択してデプロイ可能、かつ FMC で詳細を監査可能
  - ユーザが設定変更箇所をフィルタしてデプロイ可能
  - 過去10回分の設定に緊急ロールバック可能
  - 将来はチケットベースの変更管理モードをサポート予定

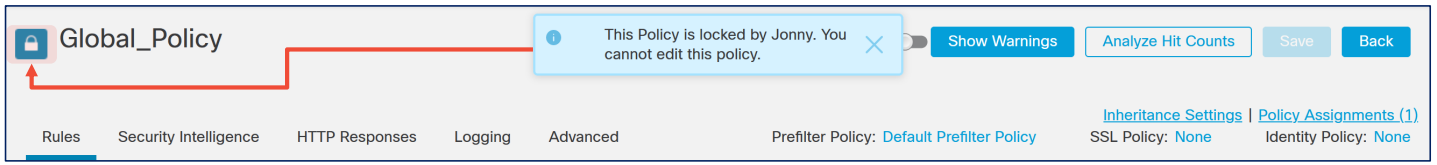


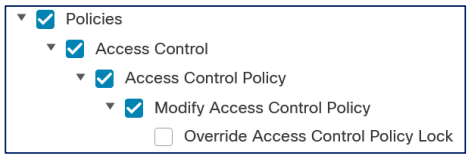
Access Policy Locking

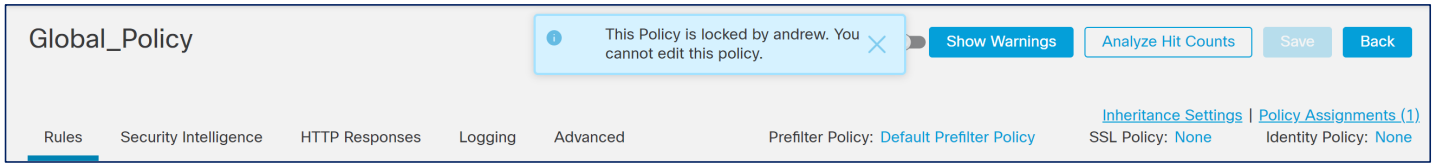
FMC 7.2





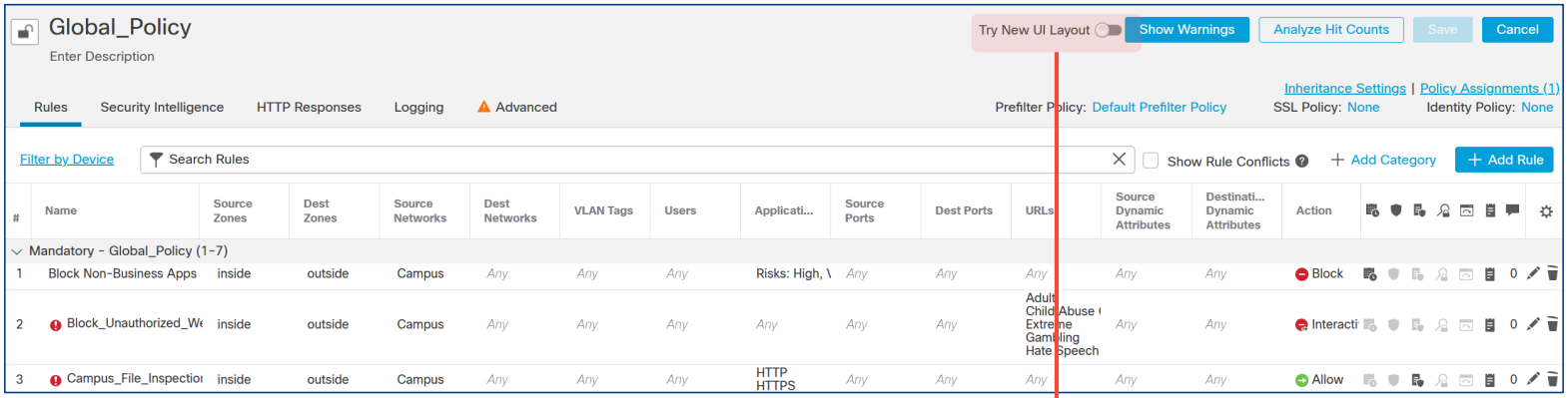


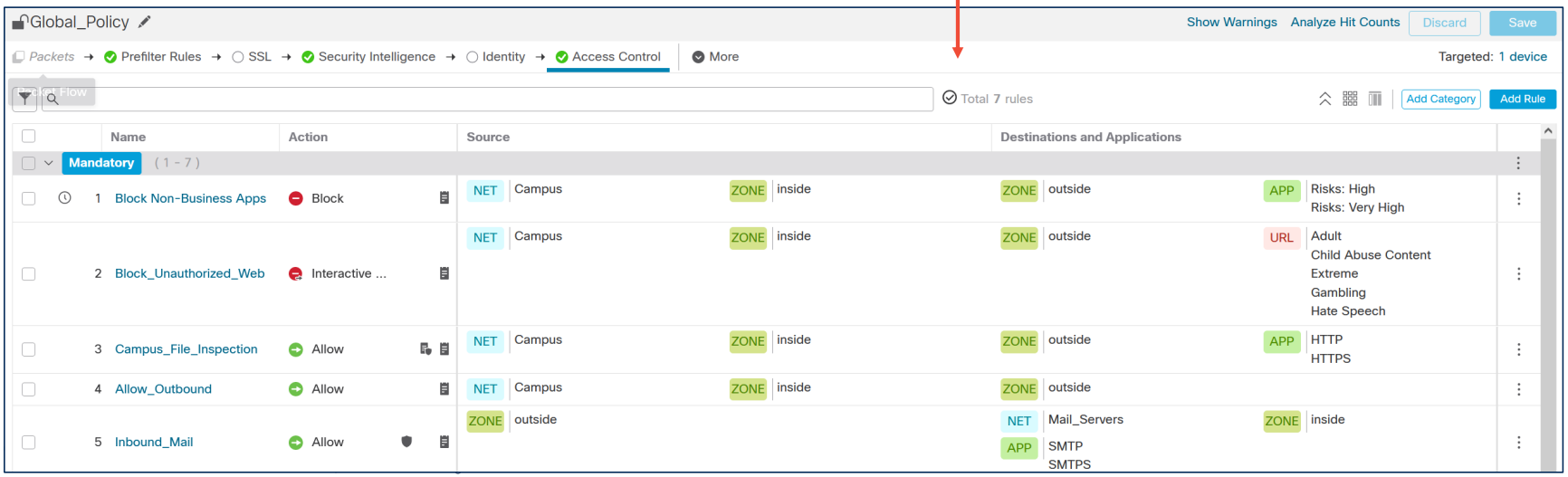




Access Control Policy (ACP) のシンプル化された UI

FMC 7.2



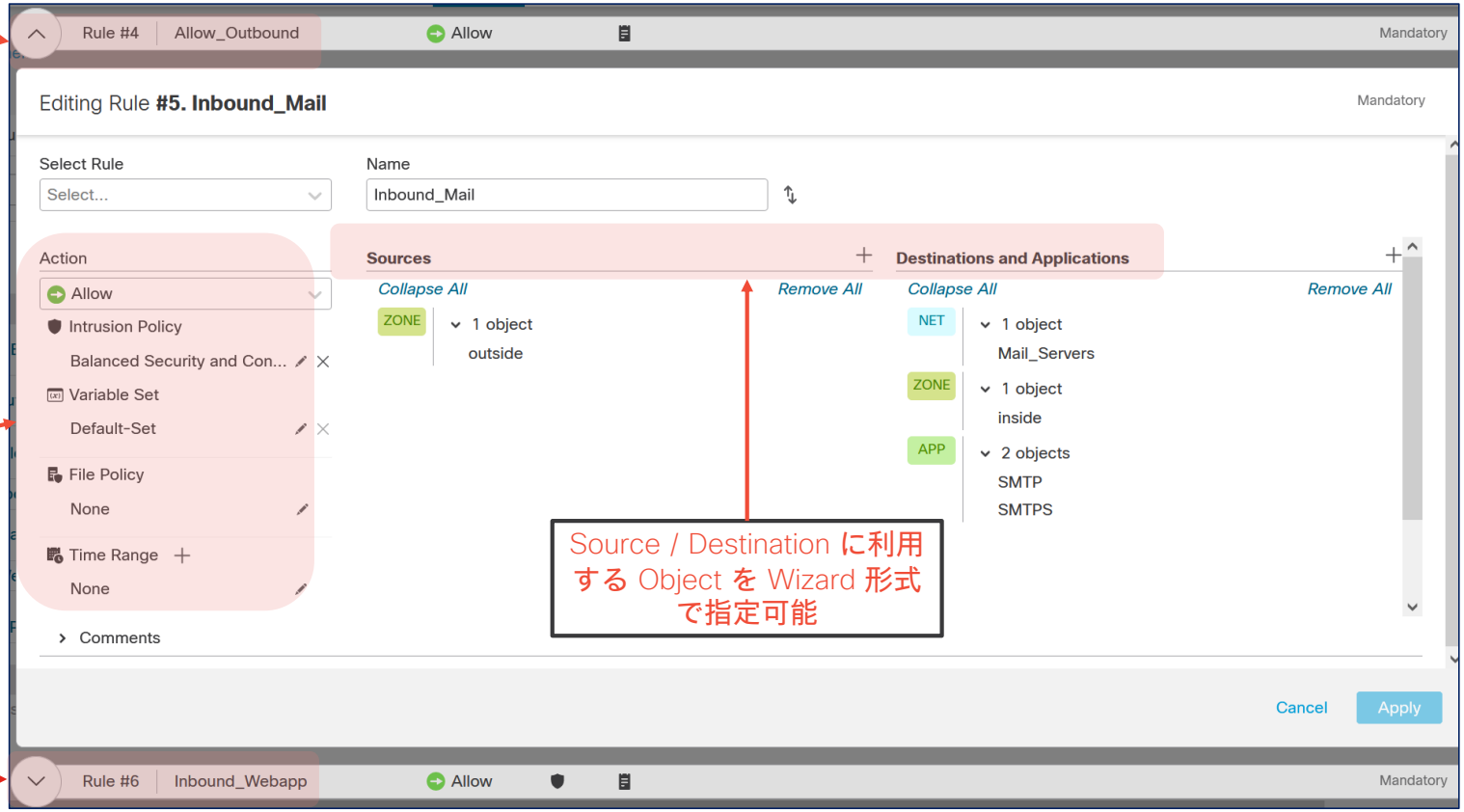


シンプル化された ACP ルールエディタ

FMC 7.2

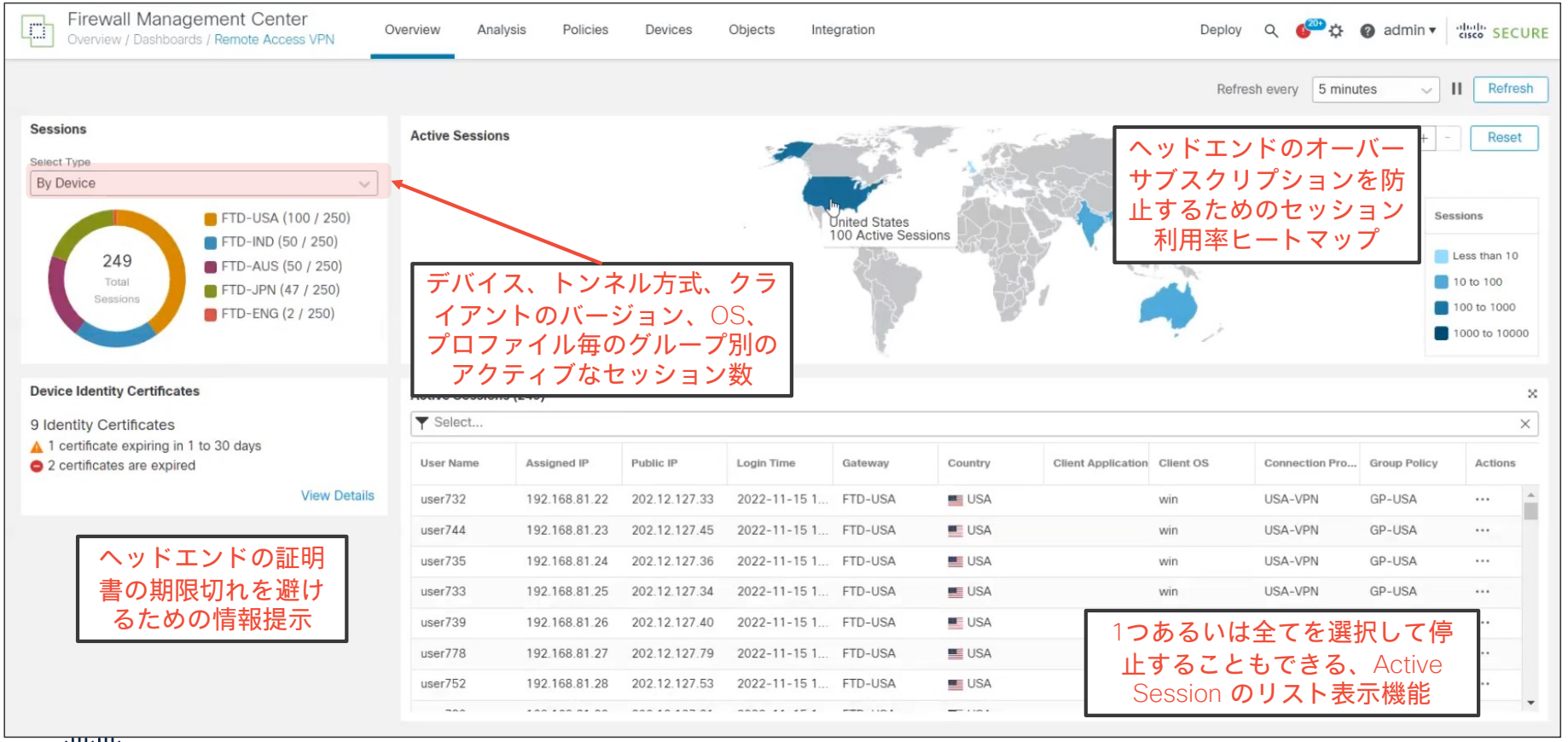
インラインルール ナビゲーション

全ての Advanced Setting に直接アクセス可能



VPN Monitoring Dashboard

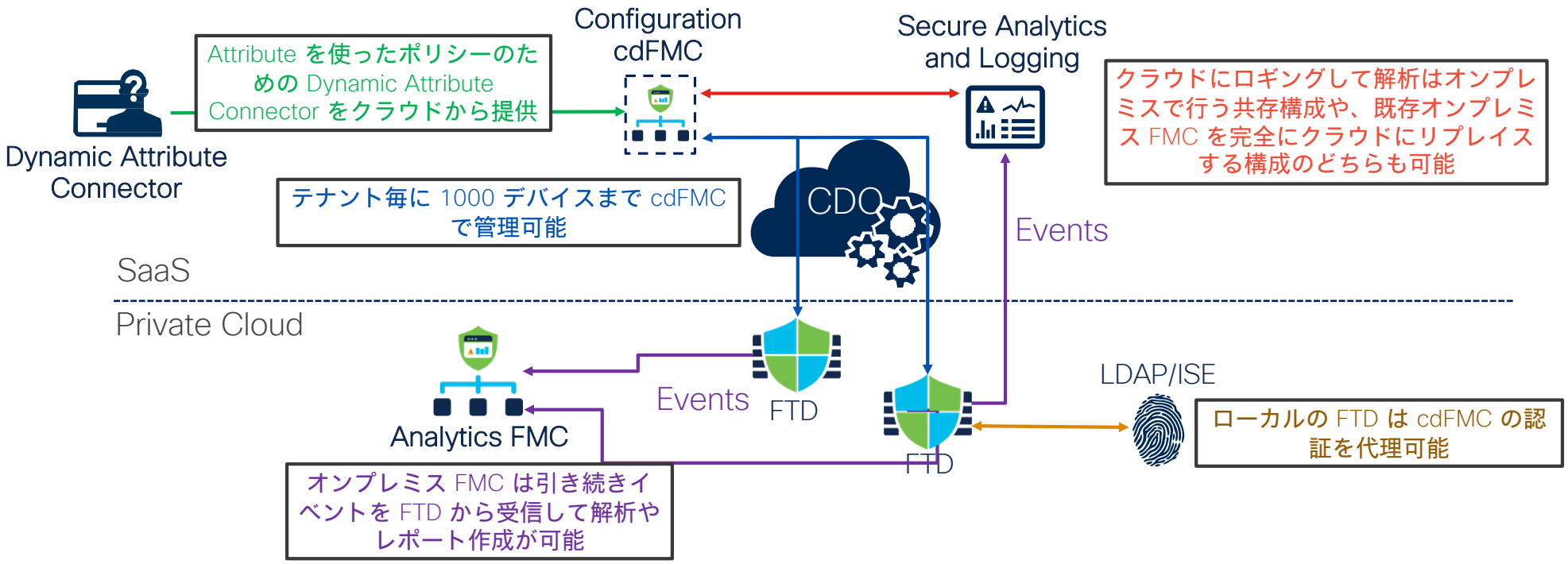
FMC 7.3



Cloud-Delivered Firewall Management Center

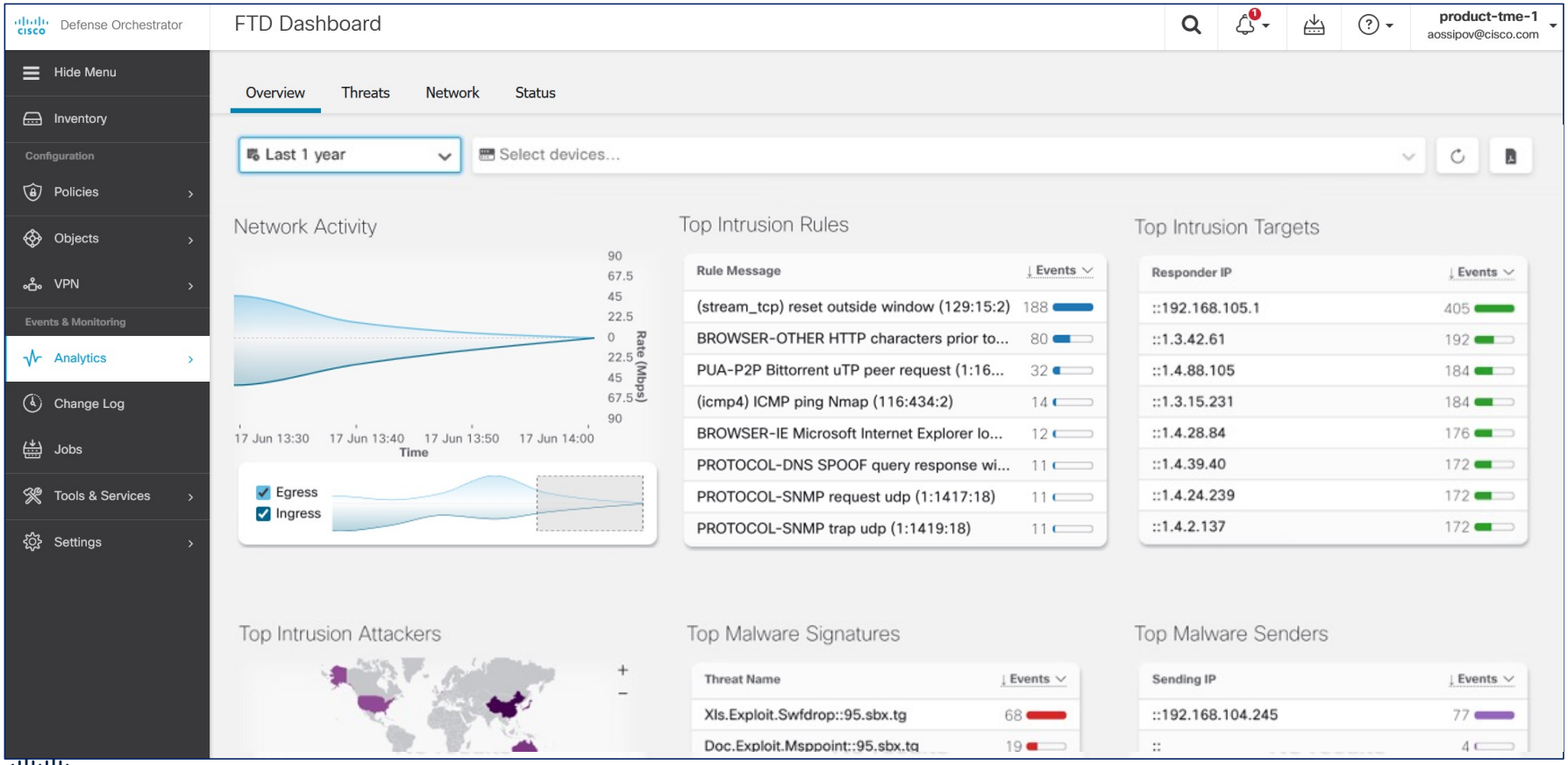
cdFMC 7.2

- Cisco Defense Orchestrator から FMC と同じ UI を提供



Cloud Analytics Dashboard

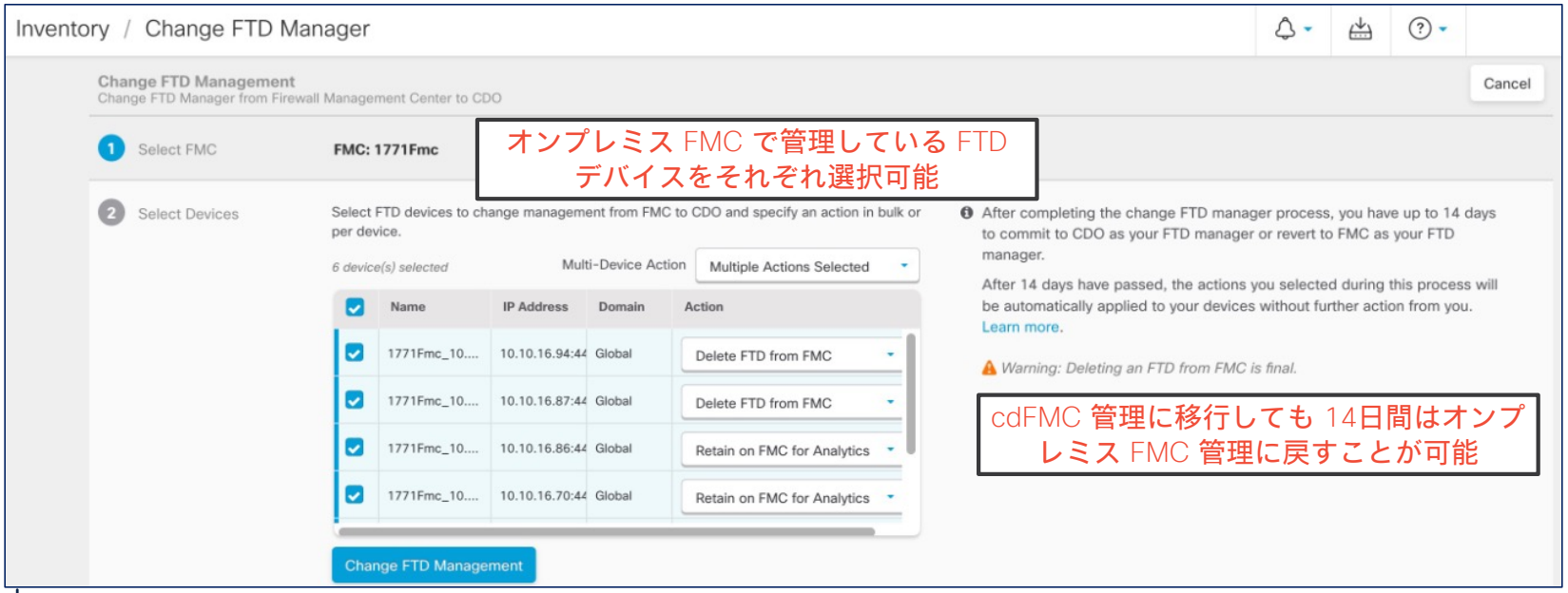
cdFMC 7.2



簡単に FTD をクラウド管理に移行可能

cdFMC 7.2

- 新しいデバイスはシリアル番号を使って簡単にオンボーディングが可能
- オンプレミス FMC で管理している FTD デバイスは簡単に cdFMC に移行可能



参考資料

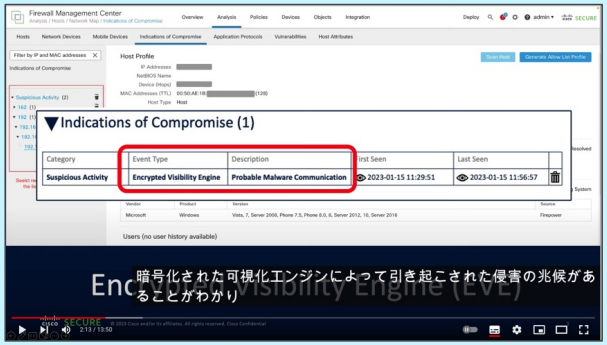
参考資料

- [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
  https://secure.cisco.com/
- Japan Partner Community : セキュリティ
  https://salesconnect.cisco.com/APJCPartnerCommunity/s/japan-partner-community-sec
- シスコ セキュリティ パートナー ガイド
  https://www.cisco.com/c/m/ja_jp/partners/documents/security-guide.html
- パートナー向け技術資料 (Firewall 基本説明動画、FTD 初期設定ガイド、FDM 初期設定ガイド等、いろいろ公開中)
  https://www.cisco.com/c/m/ja_jp/partners/documents.html

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

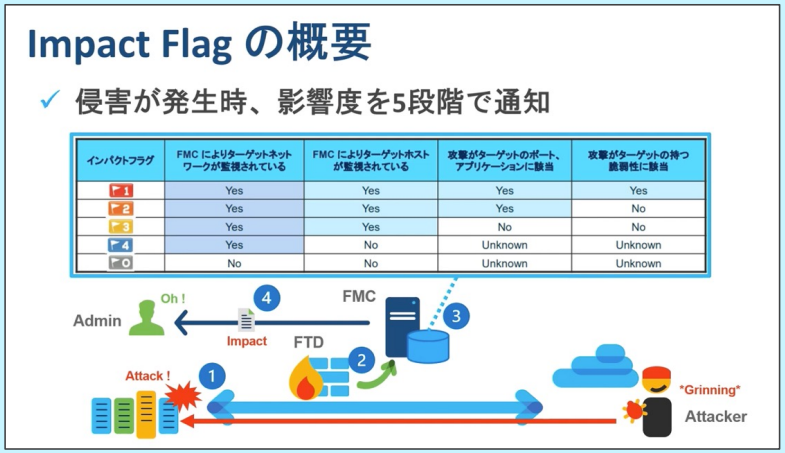
多くの動画で日本語への自動翻訳が有効



Cisco サクセスちゃんねる

- Cisco Customer Success / Customer Experience チームが日本語で運営
- サービス・製品使いこなしテクニックの動画が多数有り

  https://www.youtube.com/@Cisco-Success-Channel



Cisco Security オンラインセミナー
資料と録画のご案内

https://www.cisco.com/c/m/ja_jp/training-events/events-webinars/security.html

cisco SECURE


cisco SECURE