

CISCO
SECURE



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)



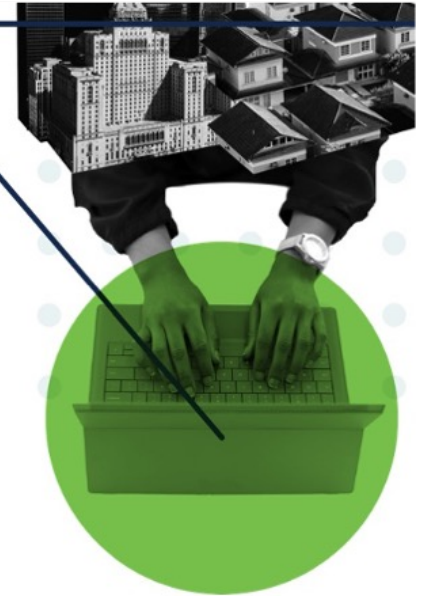
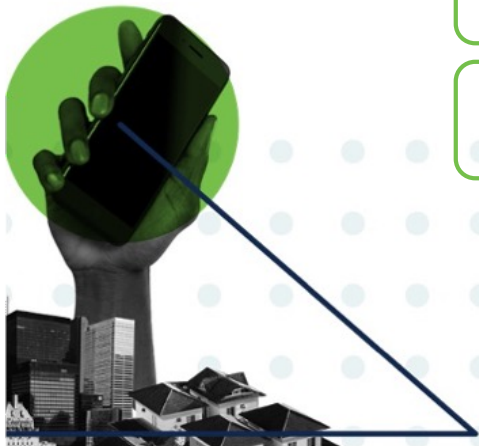
Cisco Secure Firewall ASA

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



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

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)

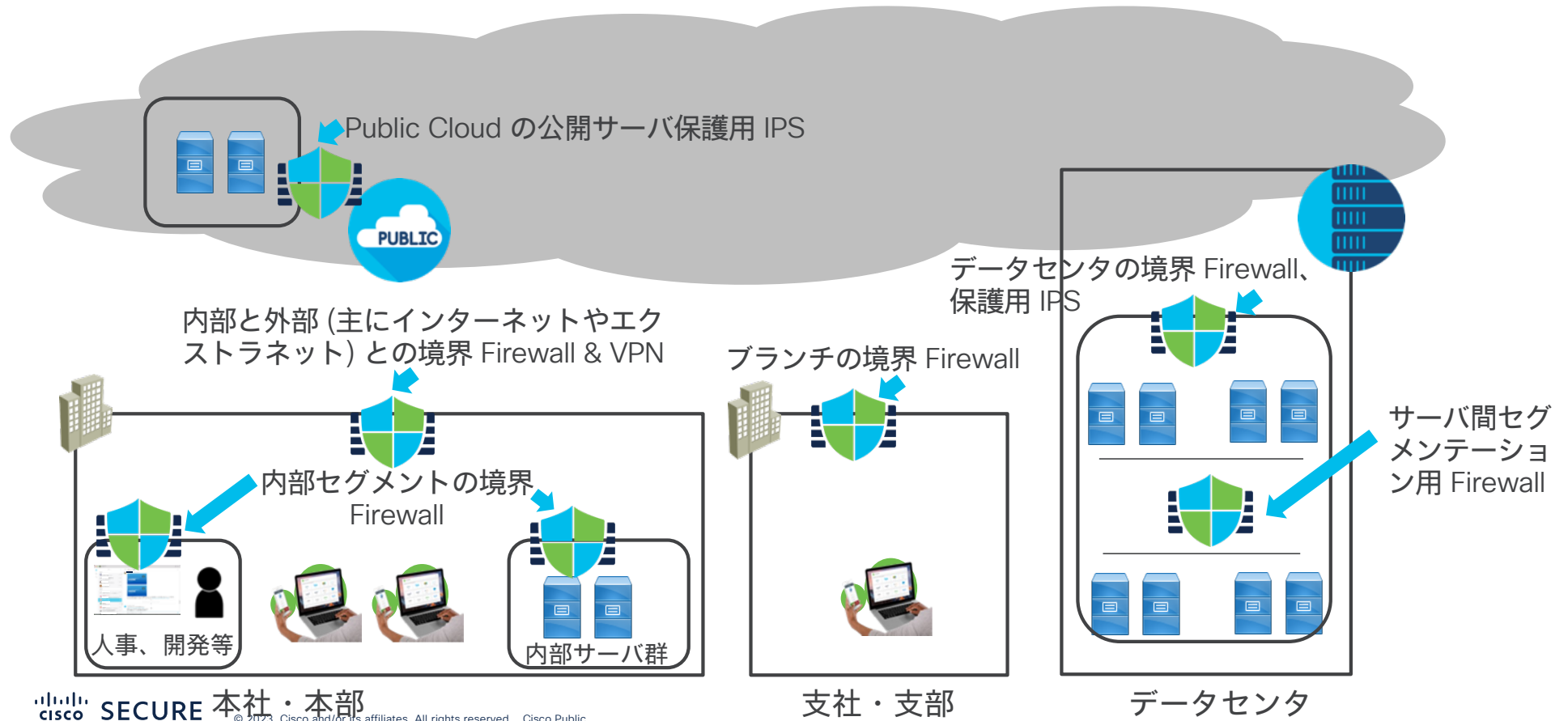
Cisco 提供脅威情報活用、3rd パーティとの脅威情報連携

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

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



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

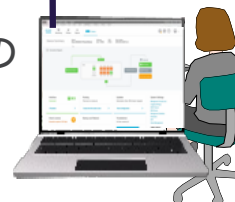
FTD 本体



https
ブラウザで管理・設定

FDM
= Firewall Device Manager

FDMの
画面



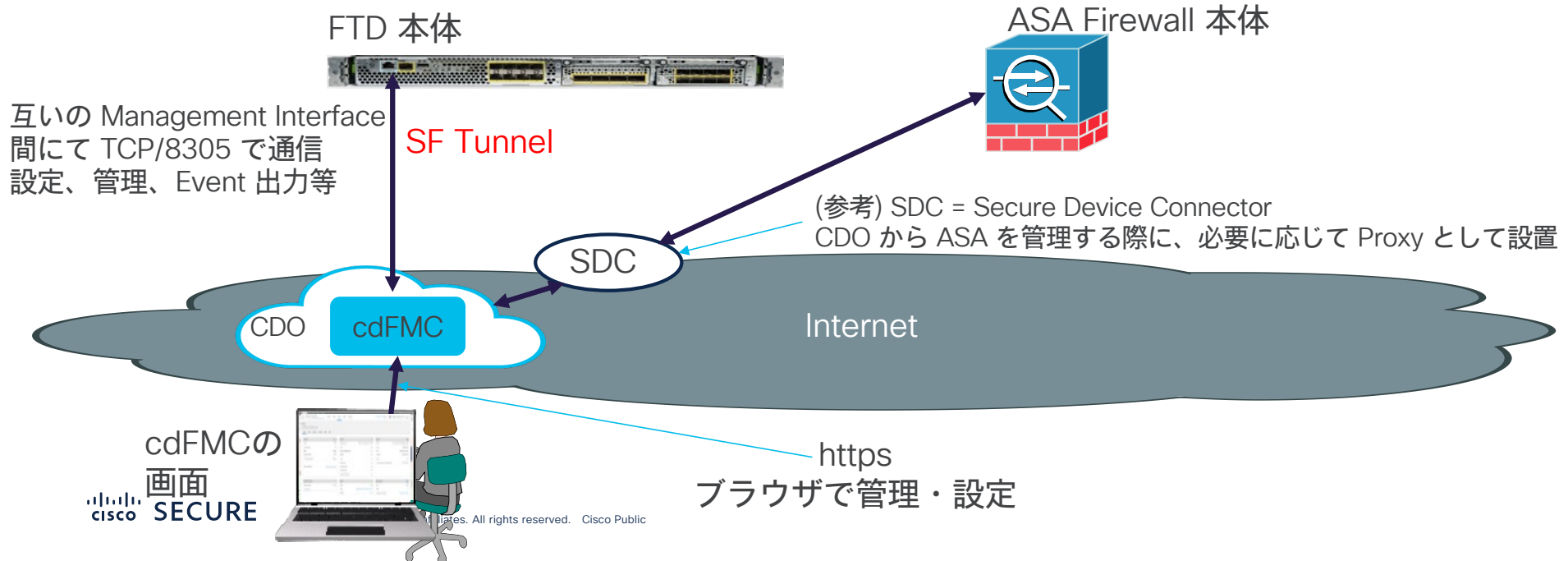
共存不可

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

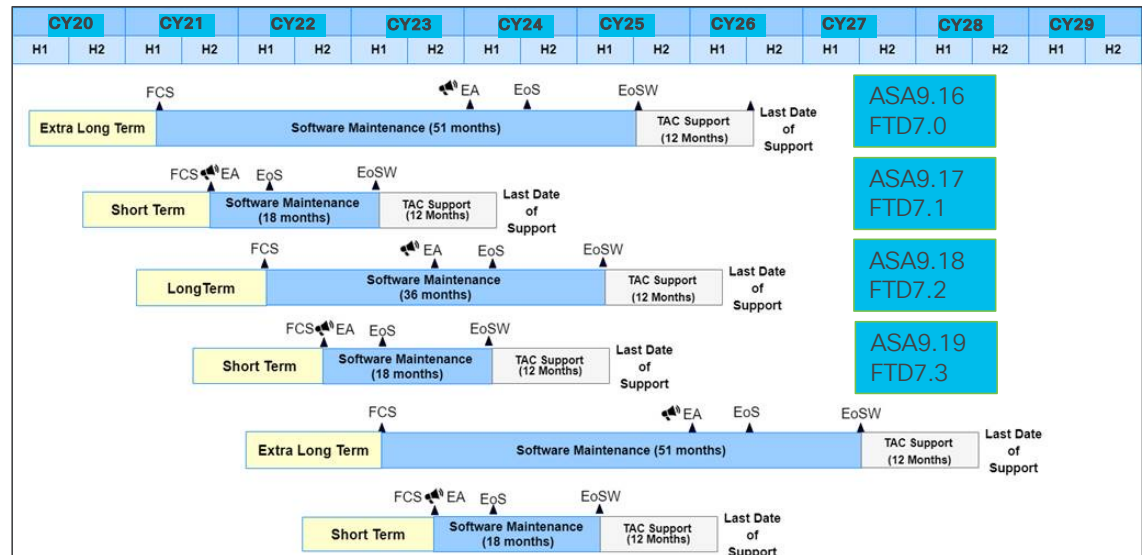


ソフトウェアライフサイクルポリシー

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



- 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

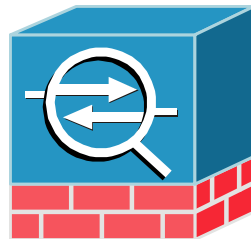
- 全ては予定であり、予告無く変更される可能性有り

[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)

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

Public Cloud



Hardware



FPR 1010



FPR 1120/40/50



FPR 2110/20/30/40



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

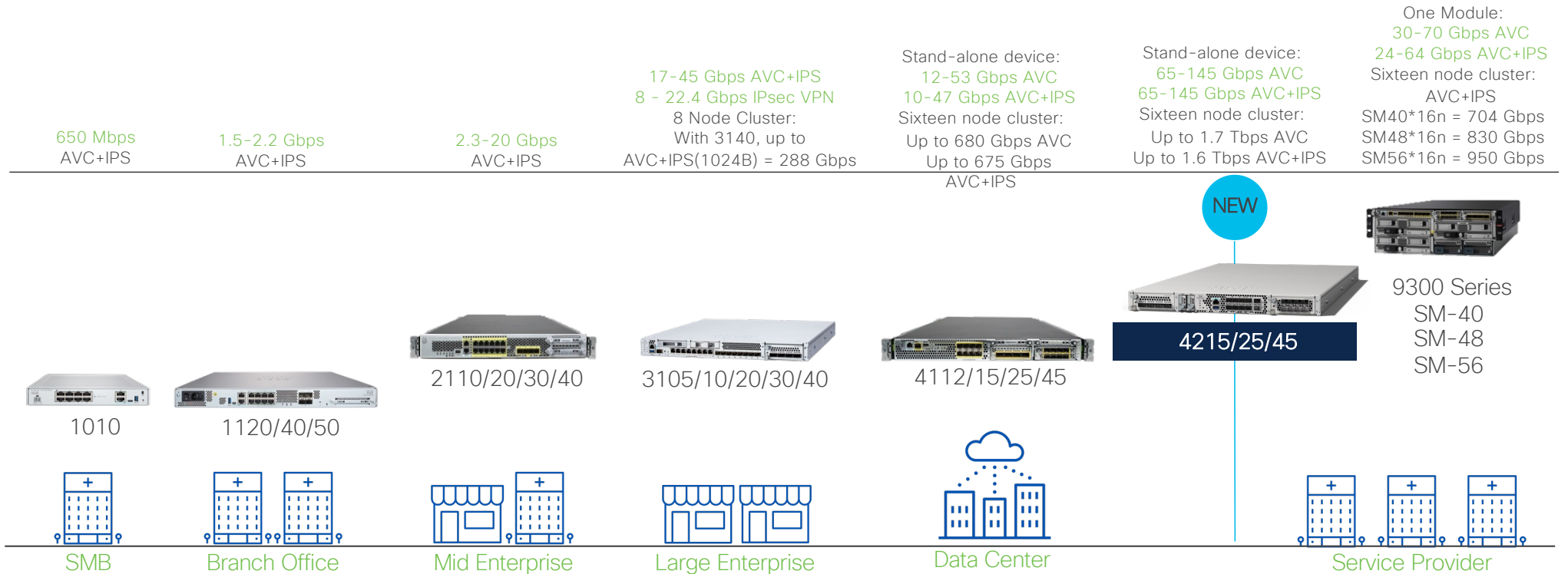
Small Enterprises /
Branch Deployments

Mid and Large Enterprises /
Campus Deployments

Datacenter / Service
Providers



Cisco Secure Firewall Hardware のポートフォリオ



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

Secure Firewall 4200 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フォーム

- 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

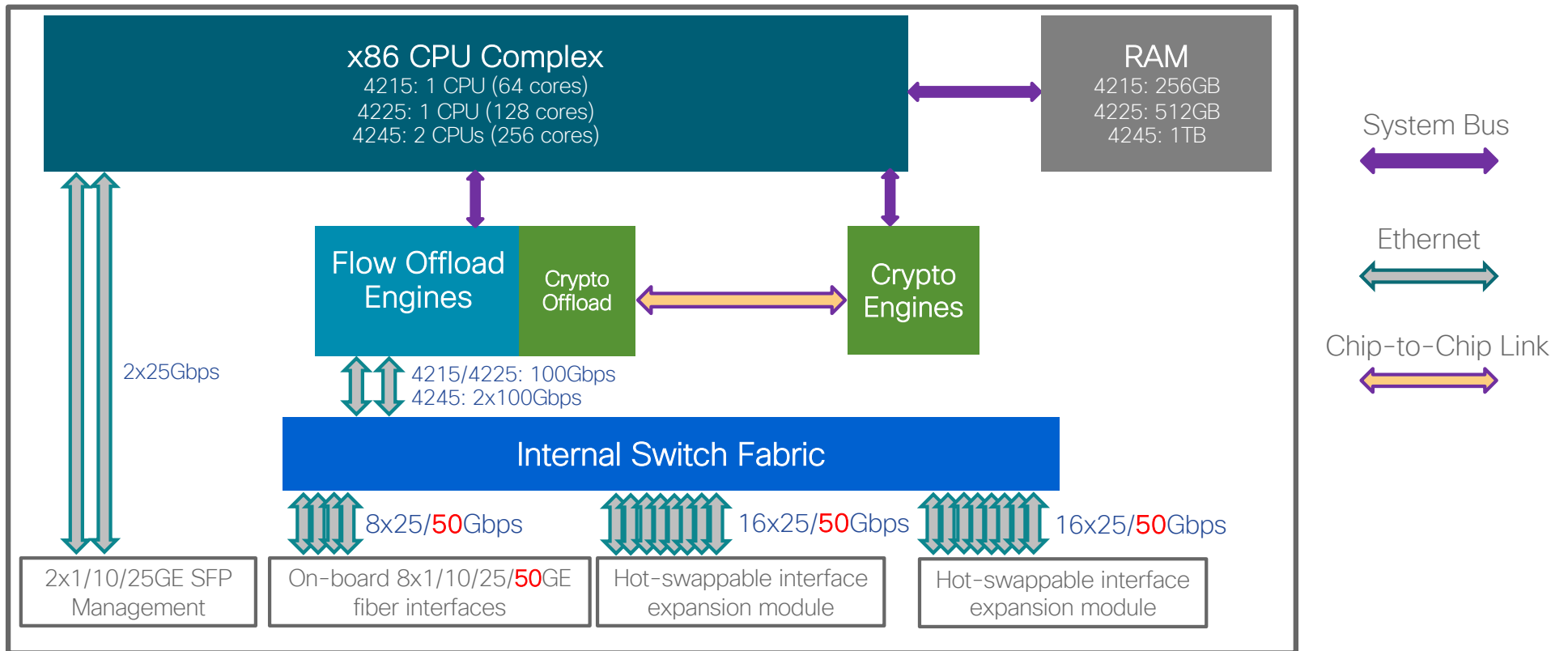
- Standard: 8x1/10GE, 8x1/10/25/**50GE**, 4x10/40GE, 2x100GE, 4x40/100/200GE, **2x200/400GE SFP+**
Fail-to-Wire: 8x1GE Copper; 6x10GE or 6x25GE SFP+ (SR and LR variants)



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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フォーム

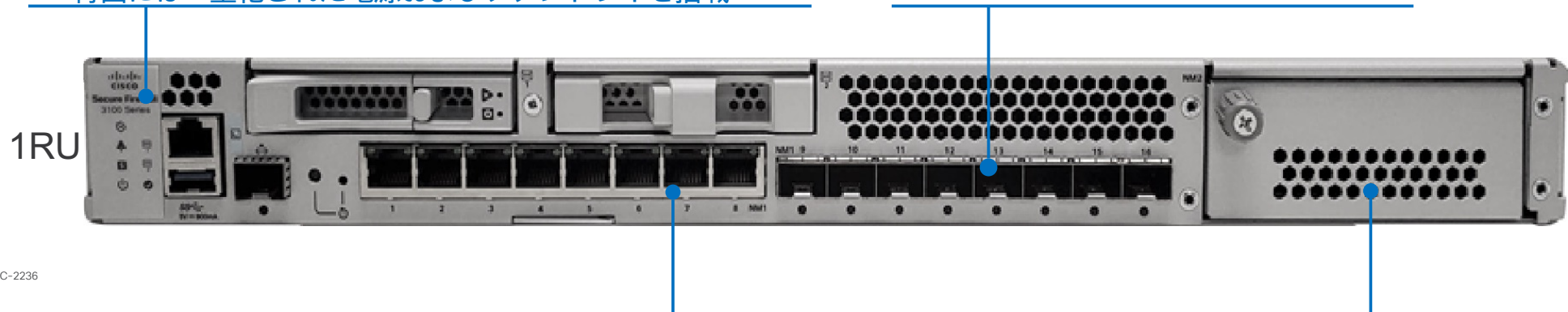
- 固定構成の5つのモデル: 3105, 3110, 3120, 3130, 3140
- **マルチインスタンス**およびクラスタリングが可能な

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



Copper Data Interfaces

- 8x10M/100M/1GE Ethernet

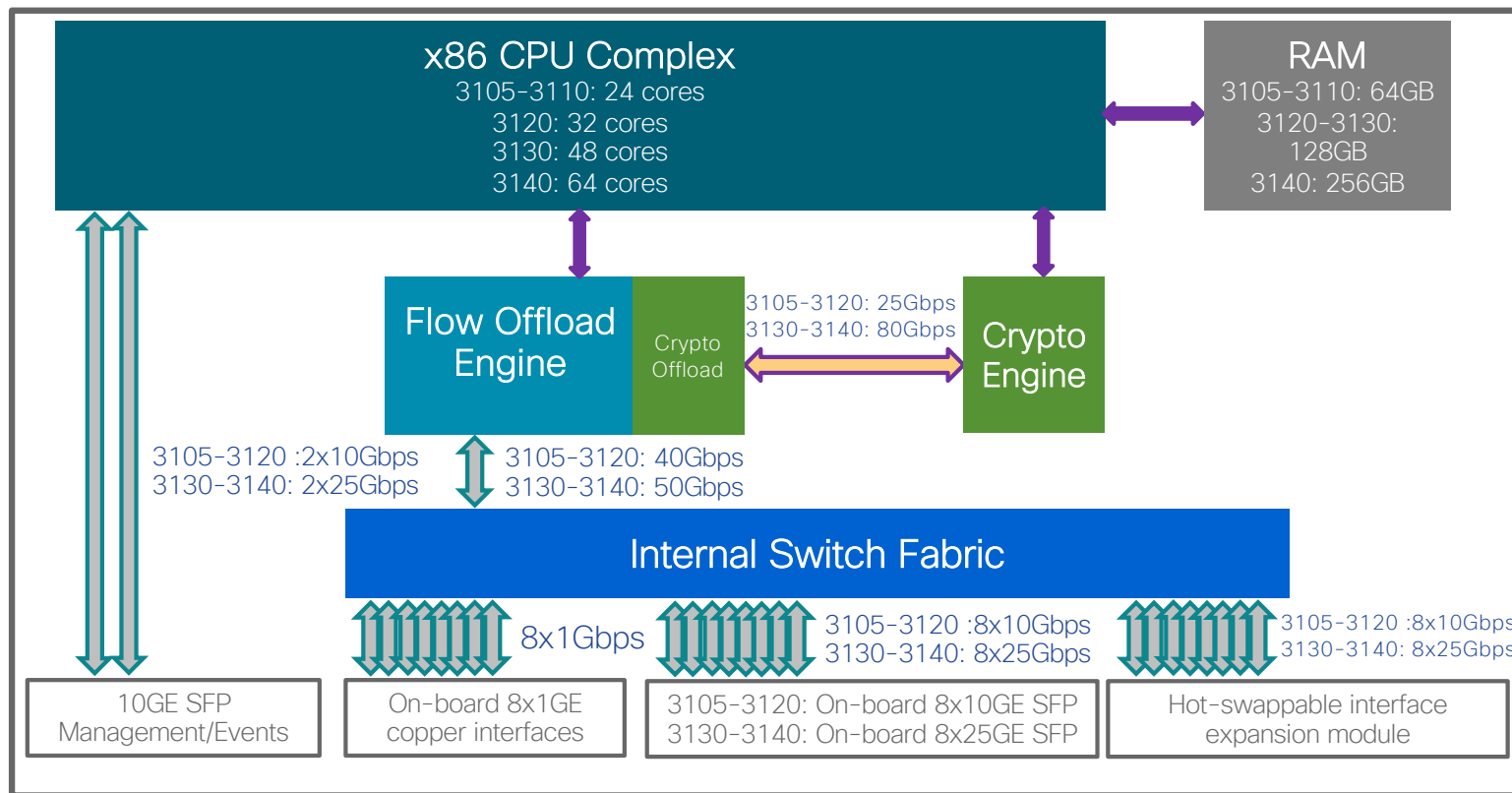
Network Module

- 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



Secure Firewall 3100 Performance



	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

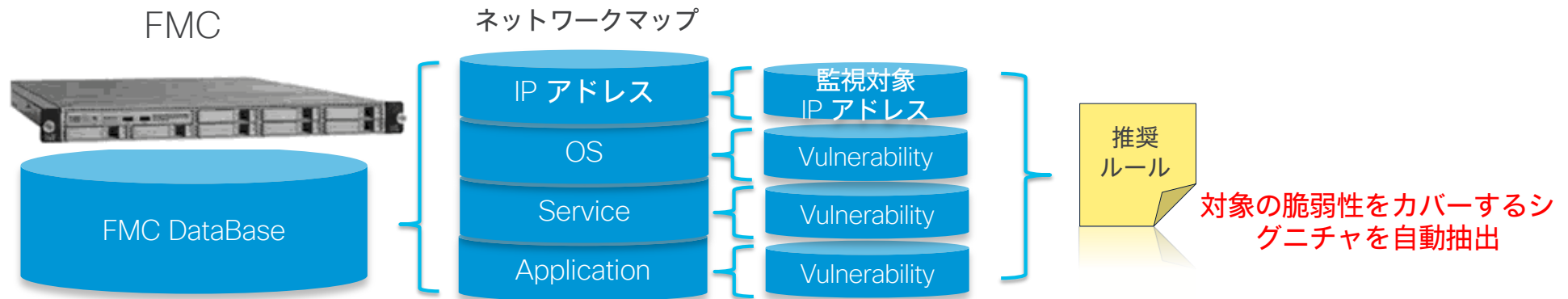
Threat Protection



自動チューニング

- 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



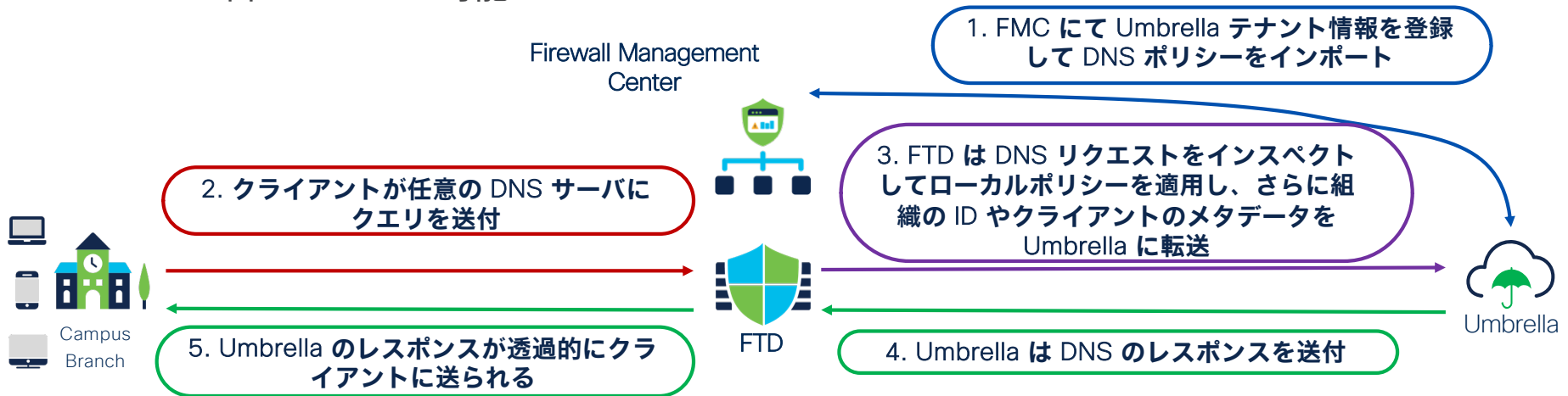
2020-08-03 09:22:00	medium	3		10.1.120.17	62.51.0.36
2020-08-03 09:17:52	high	1	↓	10.1.108.15	144.76.133.38
2020-08-03 09:17:32	high	2	↓	10.1.114.34	10.100.9.4
2020-08-03 09:11:25	high	1	↓	10.1.104.115	188.120.225.17

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



- 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



- 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

The screenshot displays the Cisco Firewall Management Center (FMC) interface. The main panel is titled "Create SASE Topology" and shows the "Summary" step. It lists the "Umbrella Data Center" (Continent: Asia, Data Center: Mumbai, IP Address: 146.112.117.8) and "Threat Defense Nodes" (chennai-bo-ftd-xyz.com, hyd-bo-ftd-xyz.com, blr-bo-ftd-xyz.com). A table shows the mapping of devices to VPN interfaces and local tunnel IDs. A blue arrow points from this table to a "Cisco Umbrella Configuration" panel on the right. This panel shows the configuration details for the topology, including the name "vpn-MumbaiUmbrella", primary data center "Asia-Mumbai", DC IP address "146.112.117.8", start time "Jul 13, 2022 11:29 AM", and completion time "Jul 13, 2022 11:29 AM". A progress bar indicates 100% completion with 3 successful and 0 failed configurations. Below this, a "Tunnel Configuration Status" table lists the devices and their status.

Device	Status	Transcript
hyd-bo-ftd.xyz.com	SUCCESS	📄
blr-bo-ftd.xyz.com	SUCCESS	📄
chennai-bo-ftd.xyz.c..	SUCCESS	📄

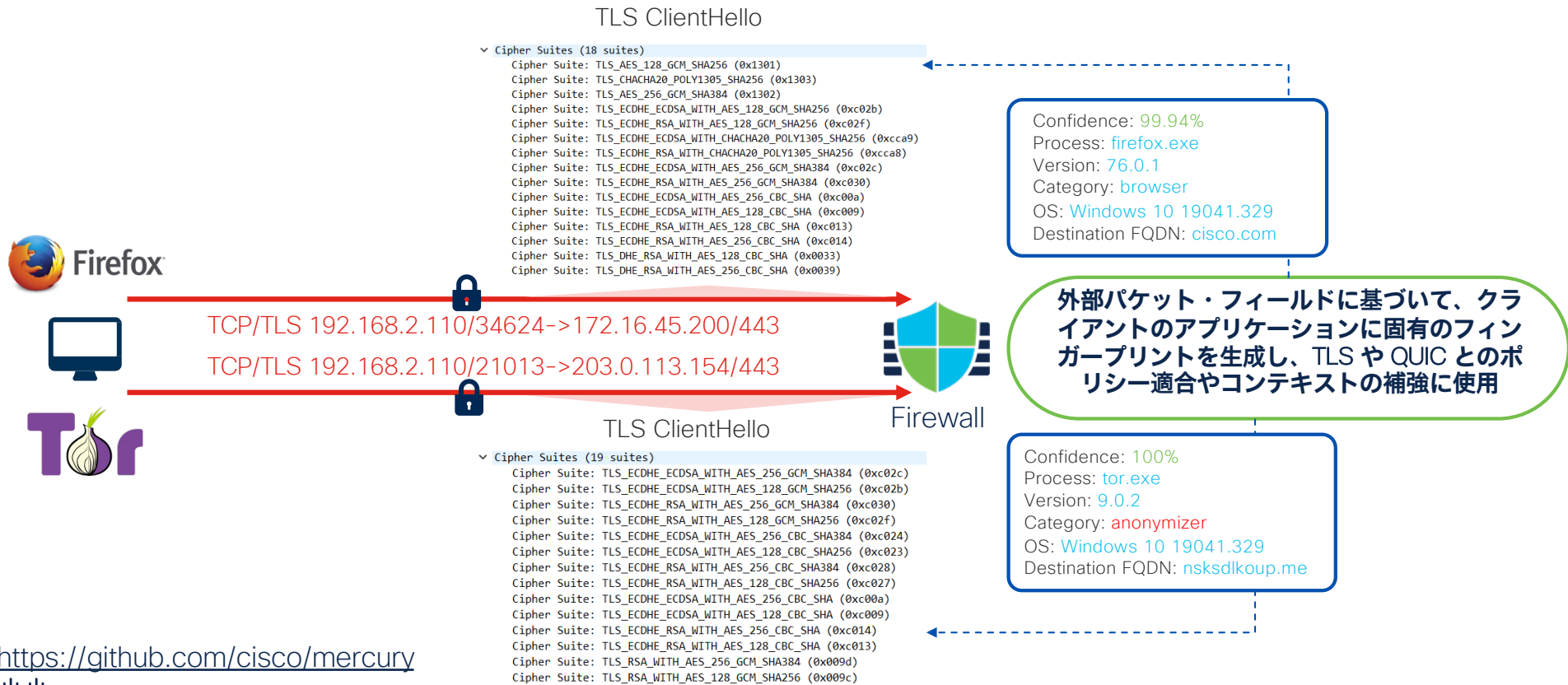
3 Snort 3 IPS エンジン



- 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

Encrypted Visibility Engine (EVE)



<https://github.com/cisco/mercury>



EVE - Unified Events



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=2	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 Unr	3 (Port unreacha	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>



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

Secure Firewall Application Detectors

Home Release Notes Support Documentation Resources Feedback

Search: ultrasurf

Risk	Business Relevance	Tags	Categories
Very Low	1,412 Very High 332	adds/installs other software 66	active directory 8
Low	891 High 976	adult content 37	ad portal 396
Medium	1,353 Medium 2,411	allows remote connect 90	anonymizer/proxy 102
High	1,630 Low 1,215	allows remote control 52	application development and testing 31
Very High	635 Very Low 987	antivirus 13	backup and recovery 9

Application Details (1) Release Notes (Ultrasurf): 354 349 348 347 346 345 343

Application Name	Description	Risk	Business Relevance
Ultrasurf	Freeware anti-censorship proxy.	Very High	Low

Tags: evasive, SSL protocol, encrypts communications, tunnels, NSG, encrypted visibility engine
Categories: vpn/tunnel, network protocols/services
Protocol: TCP
Request Application Support

Cisco Vulnerability Database (VDB) Release Notes 365

Search: 365

(Type a VDB release between 343 - 365)

Encrypted Visibility Engine Reference Details:

```
/*
 disclaimer: EVE resource files are automatically generated with
 real-world data. Older, less-relevant data is aged out, which
 leads to natural churn and can result in some month-to-month
 variations in the data.
*/
resources version: 2023.05.18

stats:
 general:
  total fingerprints: 39,860
  total labeled fingerprints: 6,930
  total connections: 2,680,300,185
 fingerprints per protocol:
  http: 3,677
  tls: 3,130
  quic: 123
```

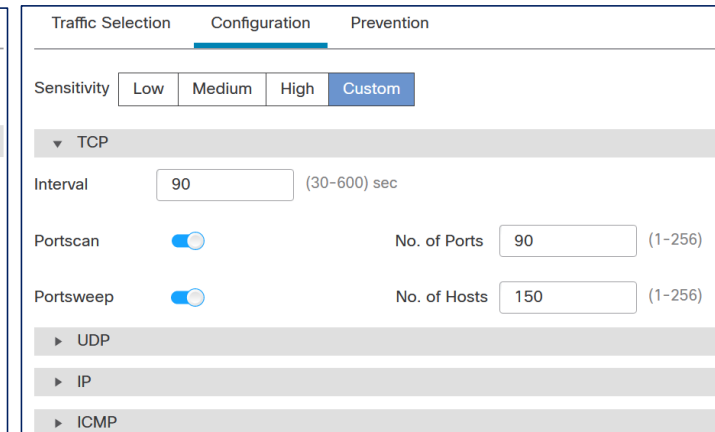
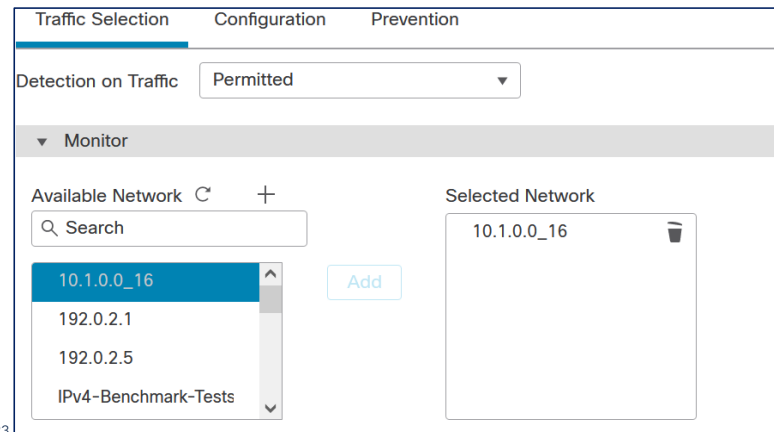
EVE フィンガープリントデータを含む全ての AppID データベースの更新情報を提供

Threat Grid:
total fingerprints: 801
total connections: 3,041,256

Portscan の検知と防止



- 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



- 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
- ウィ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ロールが可能

Create Decryption Policy

1 A decryption policy is not required to only perform application or URL discovery; instead, you can use TLS 1.3 Server Identity Discovery on the access control policy.

Name*
Decrypt DMZ Apps to Internet

Description
Decrypt all outbound traffic from DMZ on port TCP/443

Outbound Connections (User Protection) Inbound Connections (Server Protection)

How Outbound Protection Works
Outbound protection matches traffic based on the referenced Internal CA certificate's signature algorithm type, in addition to any configured rule conditions.

Internal CA
A rule will be auto-created for the selected certificate authority. [Download](#)

FMC_Self Associated: 2 Networks, 1 Port
[See how to configure](#)

Cancel Save

Malware Defense マルウェアの可視化と制御、トラッキング



Malware Summary (ワークフローの切り替え)

2020-07-27 17:57:00 - 2020-08-03 18:52:24 展開しています

検索の制限がありません (検索を編集)

Malware Summary Malwareイベントの表ビュー

次へ移動...

<input type="checkbox"/>	検知名	ファイル名	ファイルSHA256	ファイルタイプ	カウント
▼ <input type="checkbox"/>	EICAR	eicar.com	275a021b...f651fd0f	EICAR	1

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)

275a021b...f651fd0fのネットワークファイルトラジェクトリ

ファイルSHA256: 275a021b...f651fd0f
ファイル名: eicar.com
File Size (KB): 0.0664
ファイルタイプ: EICAR
File Category: Executables
Current Disposition: Malware
Threat Score: Very High
検知名: EICAR

First Seen: 2020-08-03 18:51:51 オン 192.168.10.101 実行者: No Authentication Required
Last Seen: 2020-08-03 18:53:54 オン 192.168.10.101 実行者: No Authentication Required

時間: 2020-08-03 18:53:54
イベントタイプ: 送信されたファイル
IPアドレス: 192.168.10.101
ブロックされた受信者: 192.168.20.102

アクション: Malware Block
アプリケーションプロトコル: HTTP
クライアント: Chrome

Aug 03
18:51 18:53

192.168.10.101
192.168.20.102

Events: Transfer, ブロック, Create, 移動, Execute, Scan, 検出, Quarantine
Dispositions: Unknown, Malware, クリーン, カスタム, Unavailable

時間	イベントタイプ	送信側IP	受信側IP	検知名	ファイル名	ファイルタイプ	アプリケーションプロトコル	クライアント	説明
2020-08-03 18:51:51	転送	192.168.10.101	192.168.20.102	EICAR	eicar.com	EICAR	HTTP	Chrome	
2020-08-03 18:53:54	転送	192.168.10.101	192.168.20.102	EICAR	eicar.com	EICAR	HTTP	Chrome	

② 解析情報(サンドボックス含む)と連携

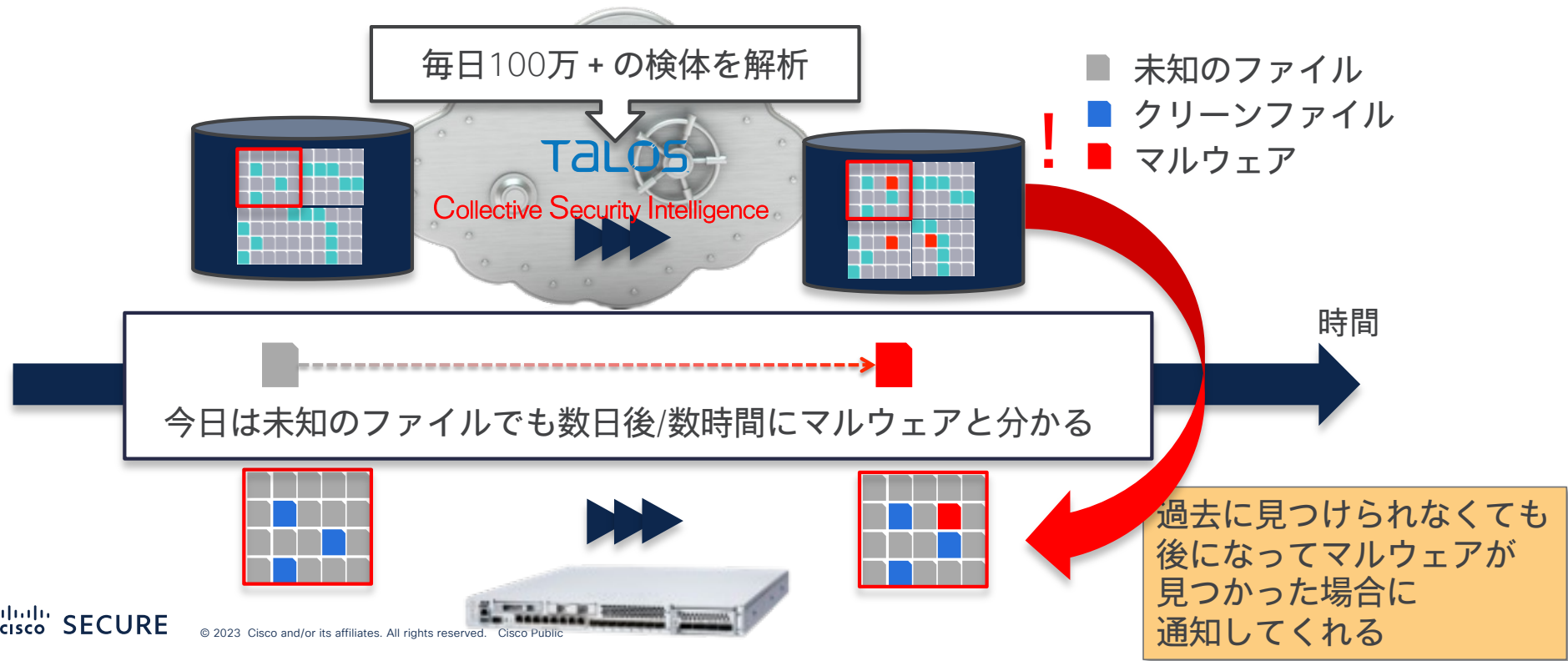
④ 端末の特定

③ ネットワーク上での拡散状況を可視化

Malware Defense クラウドリコール



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



Connectivity

Application Base の Policy Based Routing



- 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) のブレイクアウトとして利用される

Policy Based Routing
Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly

[Configure Interface Priority](#) [Add](#)

Ingress Interfaces	Match criteria and forward action
inside	<p>If traffic matches the Access List WebEx_Direct_Internet_Access</p> <p>Send and load balance it through #0 ISP1 #0 ISP2</p> <p>If above link fails, Send through #1 ISP-Backup</p>

最初のパケットの適合チェックに SaaS Application を利用可

クリアテキストや VPN トンネルでの ECMP を含む柔軟な宛先インターフェイス選定が可能

Path Monitoring および Quality-Based Routing



- 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

Add Forwarding Actions

Match ACL:* Youtube +

Send To:* Egress Interfaces

Interface Ordering:* Minimal Jitter ⓘ

Available Interfaces

Search by interface name 🔍

Interface	
Inside	+
Outside	+

No interfaces selected

Jitter: Jitter is the term used to refer to variation in latency (rtt) of packet flow from endpoint to endpoint.

RTT: The Round-trip Time (RTT) is the duration, measured in milliseconds, from when a monitoring node sends an ICMP echo request to when it receives an ICMP reply from a remote node.

Packet-Loss: Packet loss describes packets of data not reaching their destination after being transmitted across a network. Packet loss is commonly caused by network congestion, hardware issues, software bugs, and several other factors.

MOS: Mean Opinion Score (MOS) is a way of quantifying the quantitative experience of a connection. Commonly used in streaming sessions where network effects can degrade communications quality. Audio and video communications are evaluated using this metric.

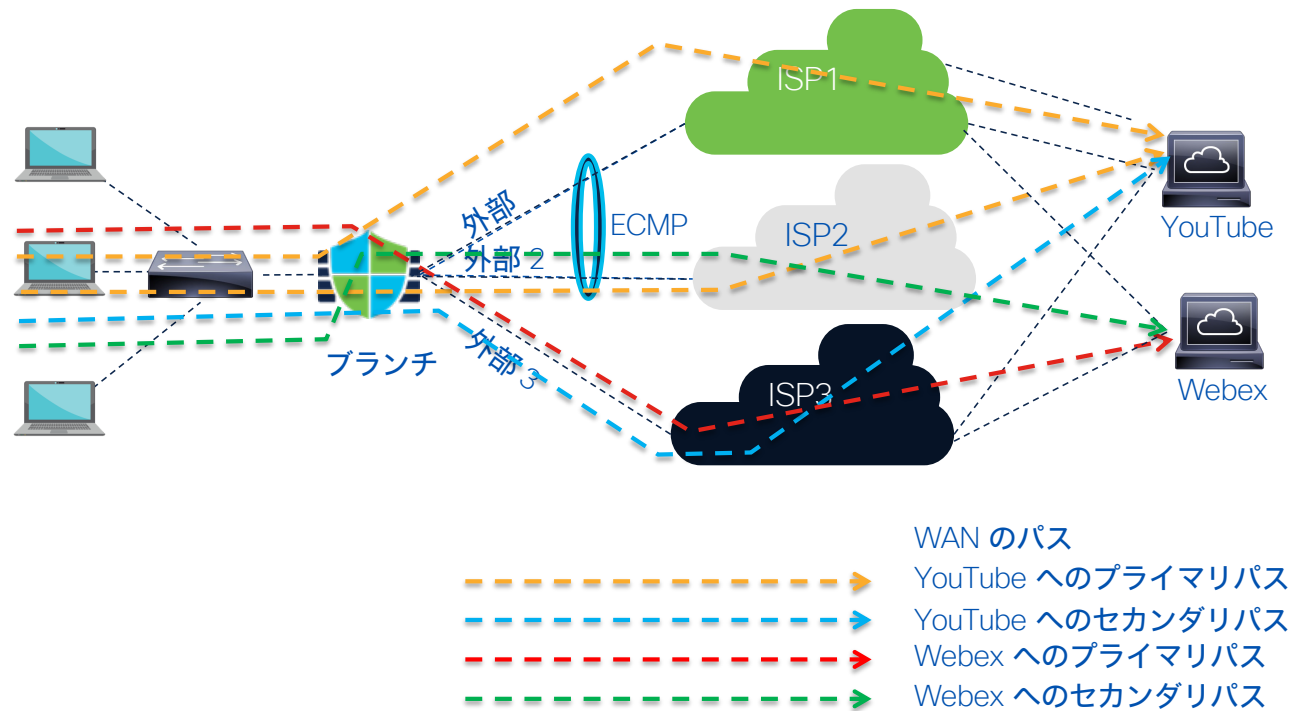
Application Routing の例

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

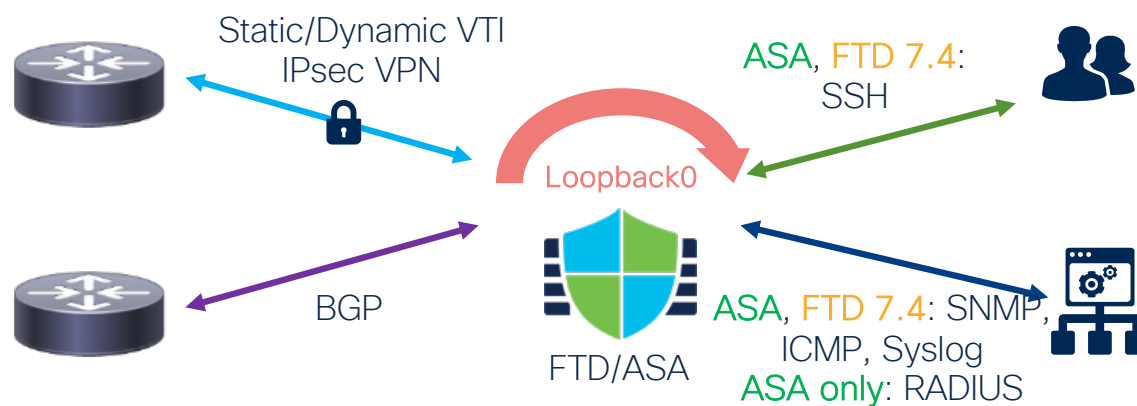
- インテリジェント アプリケーションルーティング
- リアルタイムメトリックを使用した動的パス選択
- 手動による介入なしで保証される最良の出力パス
- リンクの正常性とネットワーク状態の継続的なモニタリング
- 複数の属性に基づく出力インターフェイスの選択



Loopback Interface



- 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



- 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

Elephant Flow Settings

For Snort 3 FTD devices 7.2.0 onwards, use this window to configure elephant flow.
For all Snort 2 FTD devices or Snort 3 FTD devices 7.1.0 and earlier, use the Intelligent Application Bypass settings.

Elephant flow detection does not apply to encrypted traffic. [Learn more](#)

Elephant Flow Detection

Generate elephant flow events when flow bytes **exceeds** MB and flow duration **exceeds** seconds

Elephant flow Remediation ⓘ

If CPU utilization **exceeds** % in fixed time windows of seconds and packet drop **exceeds** %

Then Bypass the flow

Or Throttle the flow

[Revert to Defaults](#) [Cancel](#) [OK](#)

エレファントフローと判断するスループットの閾値

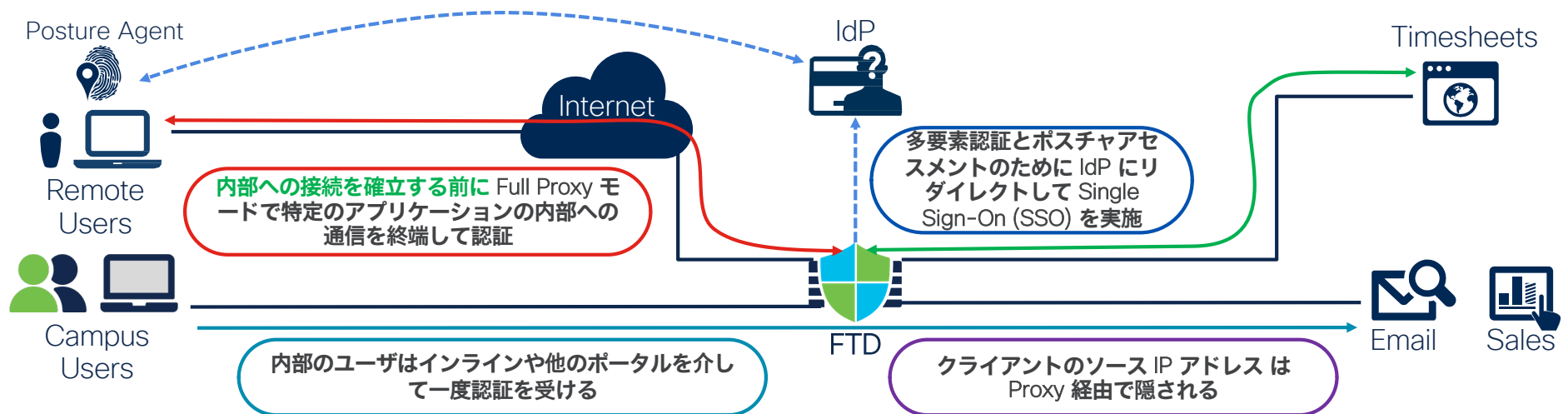
オプションで CPU リソースの使用率やパケットドロップ率を条件としてエレファントフローを制御可能

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)



- 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)

Hybrid Cloud での継続的なプロテクション



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

- ネットワークの拡張
- 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

Automation with Infrastructure-as-Code



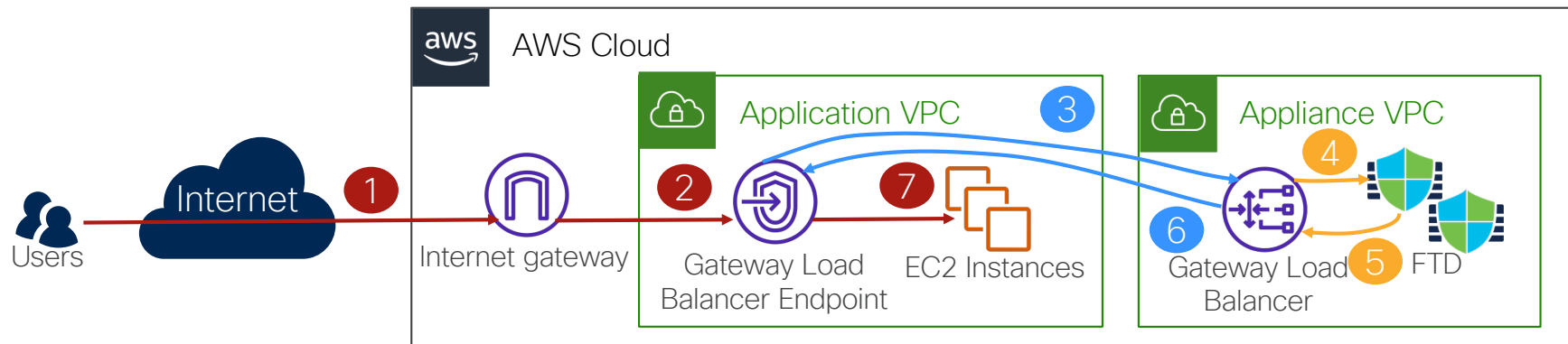
- Public Cloud のテンプレートを使った Secure Firewall のインスタンス
- ASA と FTD (FMC 経由) 用の宣言型 Terraform テンプレート
 - HashiCorp Consul と連携した FTD Dynamic Object
- ASA と FTD (FDM と FMC) 用の Ansible タスク
- Cisco DevNet のリポジトリは継続して更新
 - <https://developer.cisco.com/secure-firewall/cloud-resources/>
 - <https://github.com/CiscoDevNet/secure-firewall>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



Gateway Load-Balancer in and Azure



- 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

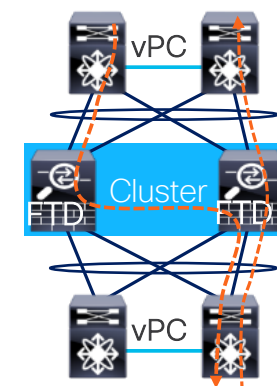


- Autoscale およびスナップショットを使ったインスタンス化は **FTD 7.2** と **ASA 9.18** からサポート

Clustering for Virtual Firewalls



- 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ト
- Hybrid Cloud における Clustering による弾力性と障害処理の向上
 -     
 - 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



Custom Orchestrator

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

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



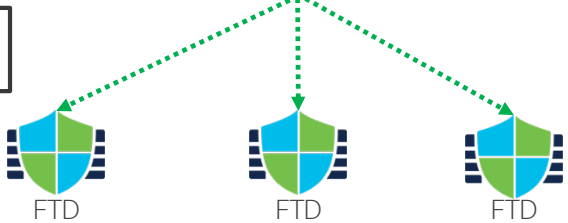
Dynamic Attribute Connector

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

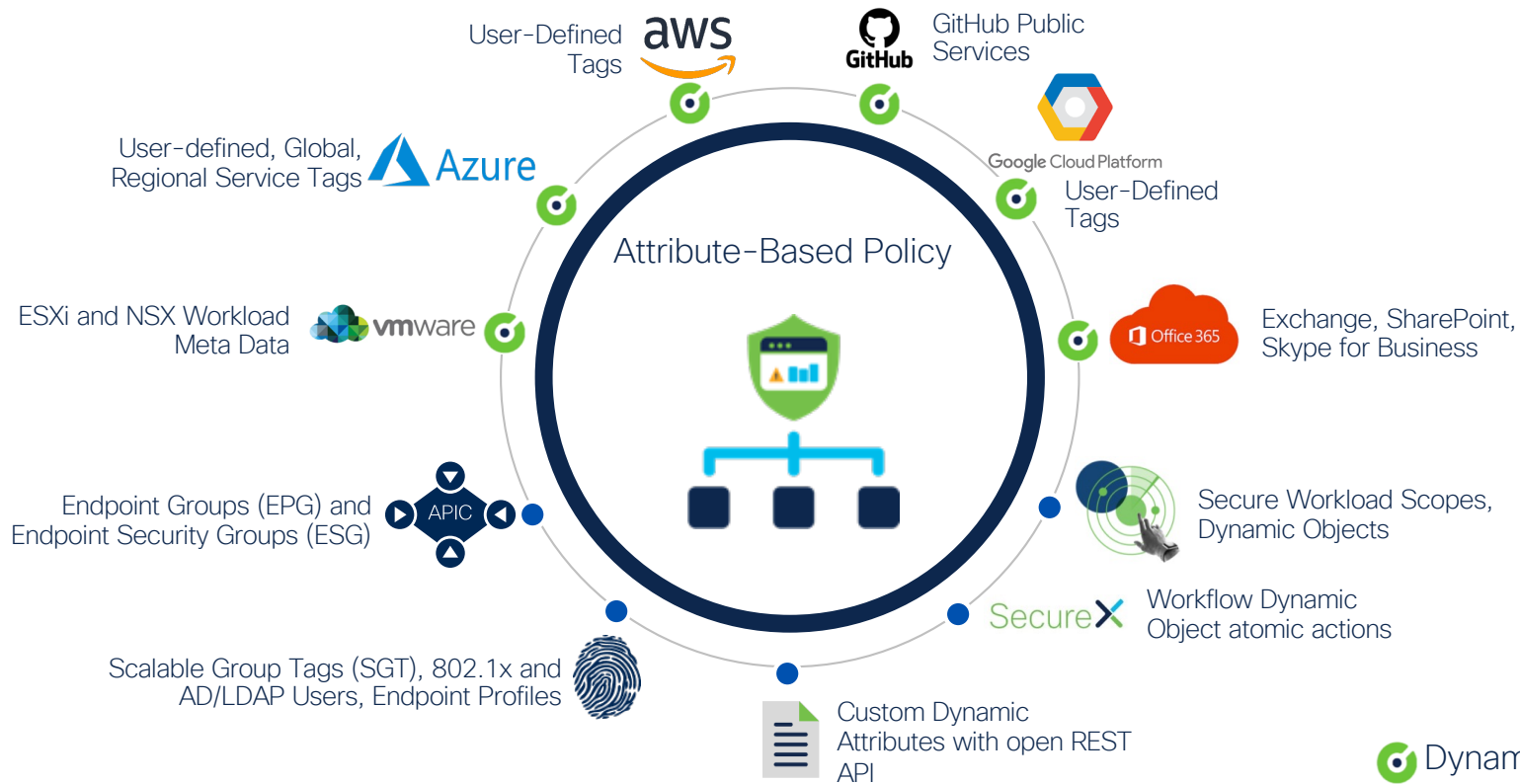


Label	IP Address
WebApp_Logic	192.168.1.151
Windows_OS	192.168.1.120-130
DB_Cluster	172.16.45.90

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



Firewall Policy の抽象化



- Dynamic Attribute Connector
- Firewall Management Center

Firewall Policy 抽象化の例

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

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

The screenshot shows the 'Access Control' section of the FTD configuration interface. It displays a list of 5 rules under the 'Mandatory' category. The rules are:

Name	Action	Sources	Destinations and Applications
1 BLOCK-EMP-Gamble	Block with re...	DYN VN1_EMP	URL Gambling
2 EMP(SGT)-to-Servers2(DynObj)	Allow	DYN VN1_EMP	APP HTTP, ICMP, DYN Servers2
3 DEV(SGT)-to-Servers1&2(DynObj)	Allow	DYN VN1_DEV	APP HTTP, ICMP, SSH, DYN Servers1, Servers2
4 CATCH-AWS	Block with re...	NET any	NET AWS-Tokyo-VPC
5 CATCH-ALL	Allow	Any	Any

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



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

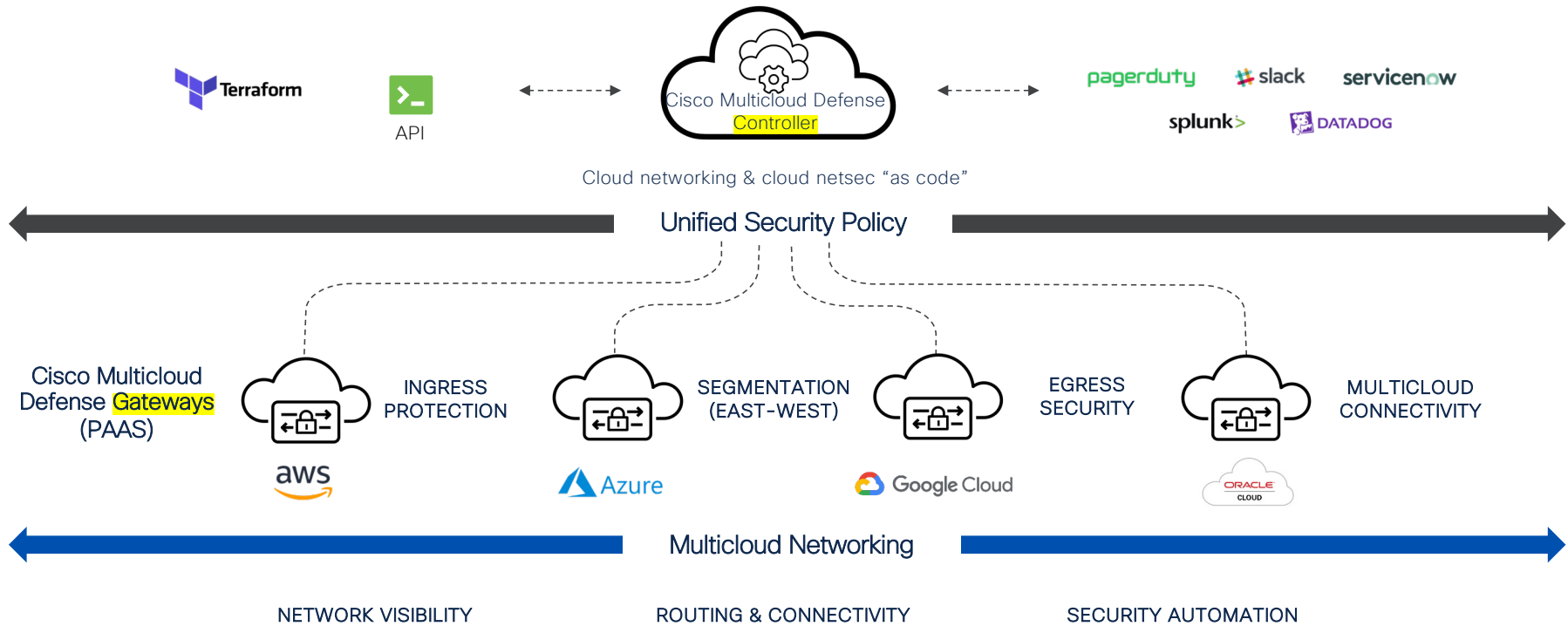


リスクとコストを一緒に軽減 作業の効率性重視

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



Multicloud Defense Gateways



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



Multicloud Defense

Accounts and Assets

Cloud Accounts

- 1 AWS
- 1 Azure
- 3 Total Accounts
- 1 GCP
- 0 Oracle

Account Resources

184	375	106	338
VPCs/ VNETs	Security Groups	Route Tables	Subnets
167	77	578	78
Instances	Load Balancers	Tags	Applications

Enable Traffic Visibility

Enable traffic visibility on specific VPCs to allow for more insight into traffic in and out of your account.

Multicloud Defense

Topology

Global View

3 Cloud Accounts, 1 AWS Accounts, 1 Azure Accounts, 1 GCP Accounts

View: Inbound, Outbound, Resource Group, Malicious Traffic, All Inventory

Multicloud Defense

Topology

Global View > Region View > VPC

View: Inbound, Outbound, Resource Group, Malicious Traffic, All Inventory

4.2 us Total, 127.8 MB Inbound, 9.3 Total MB, 5.1 MB Outbound, 349.7 MB

Country	IP Address	FQDN	Service	Port
United St...				1.67 MB
China				1.23 MB
Singapore				225.09 KB
South Kor...				145.51 KB
India				104.61 KB
Indonesia				101.13 KB
Germany				83.58 KB
Mexico				72.04 KB
France				50 KB
Japan				48.44 KB

Multicloud Defense

Policy Rule Sets: 20

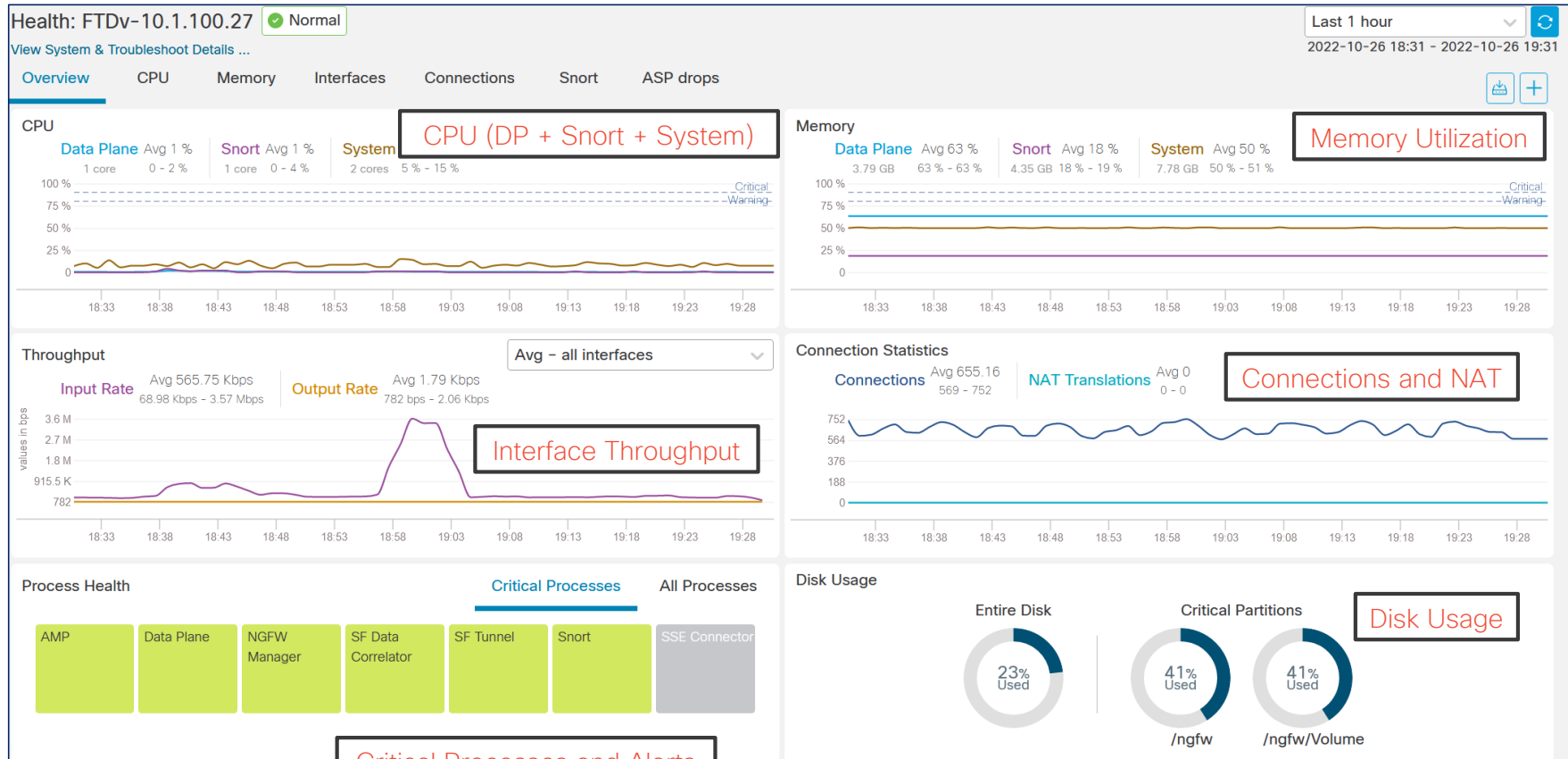
Search

Enter 3 or more characters to search

Name	Attached Gateways	Policy Rule Status	Type	Description
aws-ingress-hub-us-east-1-p...	aws-ingress-hub-us-east-1	Updated	Standalone	
aws-egress-ew-hub-us-east-1...	aws-egress-ew-hub-us-east-1, azure-egress-gw	Updated	Standalone	
gcp-egress-us-east1-policy-1...		Updated	Standalone	Policy rule set for gateway gcp-egress-us-east1 created at 2021-04-29 ...
gcp-ingress-us-east1-policy-1...		Updated	Standalone	Policy rule set for gateway gcp-ingress-us-east1 created at 2021-04-29 ...
va1ix-sample-ingress-policy-r...		Updated	Standalone	va1ix created sample ingress policy rule set.
va1ix-sample-egress-policy-r...		Updated	Standalone	va1ix created sample egress policy rule set.
WP-Ingress-Policy-us-west-2	WP-Ingress-GW-us-west-2	Updated	Standalone	Policy rule set for gateway security-hub-ingress created at 2021-12-16 1...
WP-EgressEW-Policy-us-west-2	WP-EgressEW-GW-us-west-2	Updated	Standalone	Policy rule set for gateway vult-egress-gw created at 2021-12-18 01:00...
azure-ingress-gw-policy-1641...	azure-ingress-gw	Updated	Standalone	

Management

FTD Health Dashboard



Unified Events with Live View



Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ⓘ aossipov 🔒 cisco SECURE

🔍 NAT Destination IP [] Select... [Apply] [Cancel]

Showing all 5,621 events (🔄 5,609 📊 7 📌 12) ⏏️

📅 2022-10-27 11:40 EDT → 2022-10-27 12:40 EDT → [Go Live]

Time	Event Type	Action	Reason	Source IP	Destination IP	ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule
2022-10-27 12:41:29	Connection	Allow		128.107.84.113	128.107.84.16	37420 / tcp	443 (https) / tcp	Cisco	Passive Inspect
				10.1.100.26	128.107.84.16	37420 / tcp	443 (https) / tcp	Cisco	Passive Inspect

各フィールドのフィルタ機能で、使用頻度の高いフィルタ設定はセーブ可能

イベント情報をストリーミングでリアルタイムで見るためのスイッチ

各イベントは接続の詳細情報を確認可能

Decryption Rule: Default Rule
SSL Flow Flags: UNDECRYPTABLE, PRE_DECISION_ERRO...
Application Protocol: HTTPS
Application Protocol Category: network protocols/services
Client Application: SSL client
Client Application Category: web browser
Client Application Tag: SSL protocol
Web Application: Cisco
Web Application Category: web services provider
Web Application Tag: NSG, SSL protocol
Application Risk: Medium
Business Relevance: Medium

Prefilter Policy: Custom Prefilter
Domain: Global
Device: FTDv-10.1.100.27
Ingress Interface: Passive-2
Initiator Packets: 3
Responder Packets: 2
QoS-Dropped Initiator Packets: 0
QoS-Dropped Responder Packets: 0
Initiator Bytes: 7
Responder Bytes: 1,185
QoS-Dropped Initiator Bytes: 0
QoS-Dropped Responder Bytes: 0
Encrypted Visibility Process Name: authen

Time: 2022-10-27 12:41:29
Last Packet: 2022-10-27 12:41:30
Action: Allow
Source IP: 10.1.100.26
Destination IP: 128.107.84.16
Destination Continent: North America
Destination Country: USA
Ingress Security Zone: Passive
Source Port / ICMP Type: 37420 / tcp
Destination Port / ICMP Code: 443 (https) / tcp
SSL Status: Do Not Decrypt (Handshake Error)
SSL Flow Error: Success

2022-10-27 12:41:25	Connection	Allow		128.107.84.64	128.107.84.72	52411 / tcp	9080 / tcp		Passive Inspect
2022-10-27 12:41:19	Connection	Allow		10.1.100.26	128.107.84.16	37418 / tcp	443 (https) / tcp	Cisco	Passive Inspect

変更管理



- 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

Legend: ■ Added ■ Edited ■ Removed

Deployed Version	Pending Version
Routing:	
Virtual Router: Virtual Router (Global)	
OSPFv3: OSPFv3 Process 1	
Modified: 2020-04-23 11:37:34	2020-05-13 16:58:37
Modified By: Firepower System	admin
OSPFv3 Process Area:	
OSPF Process:	1
Area ID:	1
Cost:	23
Area Type:	normal
Imports routes to normal and NSSA area:	false
Default information originate:	false
Metric Type:	1
Allow Sending summary LSA into this area:	false

Access Policy Locking



Global_Policy

Enter Description

Try New UI Layout Show Warnings Analyze Hit Counts Save Cancel

Rules Security Intelligence HTTP Responses Logging **Advanced**

This Policy is locked by you.

Prefilter Policy: Default Prefilter Policy Inheritance Settings | Policy Assignments (1) SSL Policy: None Identity Policy: None

- Policies
 - Access Control
 - Access Control Policy
 - Modify Access Control Policy
 - Override Access Control Policy Lock

Global_Policy

This Policy is locked by Jonny. You cannot edit this policy.

Show Warnings Analyze Hit Counts Save Back

Rules Security Intelligence HTTP Responses Logging **Advanced**

Prefilter Policy: Default Prefilter Policy Inheritance Settings | Policy Assignments (1) SSL Policy: None Identity Policy: None

- Policies
 - Access Control
 - Access Control Policy
 - Modify Access Control Policy
 - Override Access Control Policy Lock

Global_Policy

This Policy is locked by andrew. You cannot edit this policy.

Show Warnings Analyze Hit Counts Save Back

Rules Security Intelligence HTTP Responses Logging **Advanced**

Prefilter Policy: Default Prefilter Policy Inheritance Settings | Policy Assignments (1) SSL Policy: None Identity Policy: None

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



Global_Policy

Enter Description

Rules Security Intelligence HTTP Responses Logging **Advanced**

Try New UI Layout Show Warnings Analyze Hit Counts Save Cancel

Inheritance Settings | Policy Assignments (1)
 Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None

Filter by Device Search Rules Show Rule Conflicts + Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destinati... Dynamic Attributes	Action	Icons
Mandatory - Global_Policy (1-7)															
1	Block Non-Business Apps	inside	outside	Campus	Any	Any	Any	Risks: High, \	Any	Any	Any	Any	Any	Block	Icons
2	Block_Unauthorized_Wt	inside	outside	Campus	Any	Any	Any	Any	Any	Any	Any	Any	Any	Interacti	Icons
3	Campus_File_Inspector	inside	outside	Campus	Any	Any	Any	HTTP HTTPS	Any	Any	Any	Any	Any	Allow	Icons

Global_Policy

Show Warnings Analyze Hit Counts Discard Save

Packets → Prefilter Rules → SSL → Security Intelligence → Identity → **Access Control** → More Targeted: 1 device

Flow Total 7 rules Add Category Add Rule

Name	Action	Source	Destinations and Applications
Mandatory (1 - 7)			
1 Block Non-Business Apps	Block	NET Campus	ZONE inside ZONE outside APP Risks: High Risks: Very High
2 Block_Unauthorized_Web	Interactive ...	NET Campus	ZONE inside ZONE outside URL Adult Child Abuse Content Extreme Gambling Hate Speech
3 Campus_File_Inspection	Allow	NET Campus	ZONE inside ZONE outside APP HTTP HTTPS
4 Allow_Outbound	Allow	NET Campus	ZONE inside ZONE outside
5 Inbound_Mail	Allow	ZONE outside	NET Mail_Servers ZONE inside APP SMTP SMTPS

シンプル化された ACP ルールエディタ



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

Source / Destination に利用する Object を Wizard 形式で指定可能

The screenshot displays the Cisco ACP Rule Editor interface. At the top, a navigation bar shows 'Rule #4 Allow_Outbound' with an 'Allow' status and 'Mandatory' priority. Below this, the main editing area is titled 'Editing Rule #5. Inbound_Mail' with a 'Mandatory' priority. The interface includes a 'Select Rule' dropdown, a 'Name' field containing 'Inbound_Mail', and an 'Action' dropdown set to 'Allow'. The 'Sources' and 'Destinations and Applications' sections are visible, each with a 'Collapse All' and 'Remove All' option. The 'Sources' section shows a 'ZONE' object named 'outside'. The 'Destinations and Applications' section shows three objects: 'NET' (Mail_Servers), 'ZONE' (inside), and 'APP' (SMTP, SMTPS). A 'Comments' section is at the bottom. At the very bottom, a navigation bar shows 'Rule #6 Inbound_Webapp' with an 'Allow' status and 'Mandatory' priority. Red arrows point from the callout boxes to the navigation bar, the 'Advanced Setting' list, and the 'Sources' section.

VPN Monitoring Dashboard



Firewall Management Center
Overview / Dashboards / Remote Access VPN

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ? admin ▼ 🔒 cisco SECURE

Refresh every 5 minutes Refresh

Reset

Sessions

Select Type
By Device

249 Total Sessions

- FTD-USA (100 / 250)
- FTD-IND (50 / 250)
- FTD-AUS (50 / 250)
- FTD-JPN (47 / 250)
- FTD-ENG (2 / 250)

Active Sessions

United States
100 Active Sessions

Sessions

- Less than 10
- 10 to 100
- 100 to 1000
- 1000 to 10000

デバイス、トンネル方式、クライアントのバージョン、OS、プロファイル毎のグループ別のアクティブなセッション数

Device Identity Certificates

9 Identity Certificates

- ▲ 1 certificate expiring in 1 to 30 days
- 2 certificates are expired

View Details

ヘッドエンドの証明書
の期限切れを避
けるための情報提示

User Name	Assigned IP	Public IP	Login Time	Gateway	Country	Client Application	Client OS	Connection Pro...	Group Policy	Actions
user732	192.168.81.22	202.12.127.33	2022-11-15 1...	FTD-USA	USA		win	USA-VPN	GP-USA	...
user744	192.168.81.23	202.12.127.45	2022-11-15 1...	FTD-USA	USA		win	USA-VPN	GP-USA	...
user735	192.168.81.24	202.12.127.36	2022-11-15 1...	FTD-USA	USA		win	USA-VPN	GP-USA	...
user733	192.168.81.25	202.12.127.34	2022-11-15 1...	FTD-USA	USA		win	USA-VPN	GP-USA	...
user739	192.168.81.26	202.12.127.40	2022-11-15 1...	FTD-USA	USA		win	USA-VPN	GP-USA	...
user778	192.168.81.27	202.12.127.79	2022-11-15 1...	FTD-USA	USA		win	USA-VPN	GP-USA	...
user752	192.168.81.28	202.12.127.53	2022-11-15 1...	FTD-USA	USA		win	USA-VPN	GP-USA	...

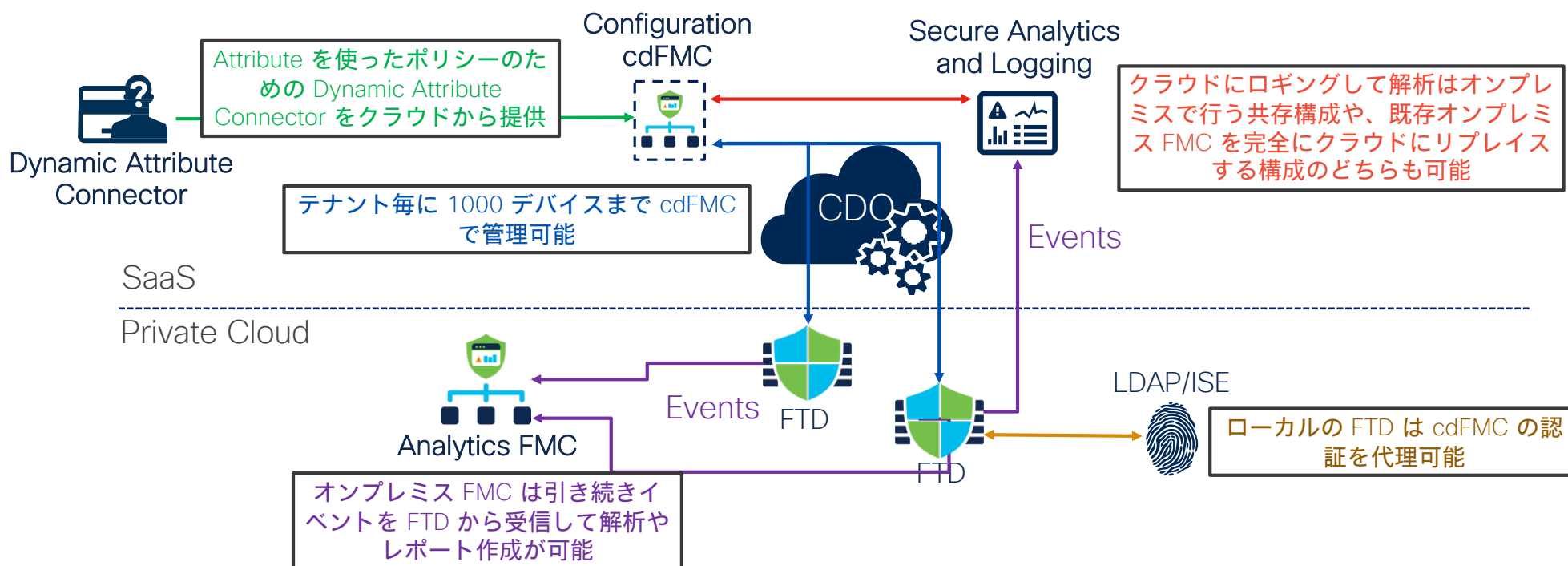
ヘッドエンドのオーバ
サブスクリプションを
防止するためのセッション
利用率ヒートマップ

1つあるいは全てを選択して停
止することもできる、Active
Session のリスト表示機能

Cloud-Delivered Firewall Management Center



- Cisco Defense Orchestrator から FMC と同じ UI を提供



Cloud Analytics Dashboard



Defense Orchestrator
FTD Dashboard
product-tme-1
aossipov@cisco.com

- Hide Menu
- Inventory
- Configuration
- Policies
- Objects
- VPN
- Events & Monitoring
- Analytics
- Change Log
- Jobs
- Tools & Services
- Settings

Overview | Threats | Network | Status

Last 1 year
Select devices...

Network Activity

Top Intrusion Rules

Rule Message	Events
(stream_tcp) reset outside window (129:15:2)	188
BROWSER-OTHER HTTP characters prior to...	80
PUA-P2P Bittorrent uTP peer request (1:16...	32
(icmp4) ICMP ping Nmap (116:434:2)	14
BROWSER-IE Microsoft Internet Explorer lo...	12
PROTOCOL-DNS SPOOF query response wi...	11
PROTOCOL-SNMP request udp (1:1417:18)	11
PROTOCOL-SNMP trap udp (1:1419:18)	11

Top Intrusion Targets

Responder IP	Events
::192.168.105.1	405
::1.3.42.61	192
::1.4.88.105	184
::1.3.15.231	184
::1.4.28.84	176
::1.4.39.40	172
::1.4.24.239	172
::1.4.2.137	172

Top Intrusion Attackers

Top Malware Signatures

Threat Name	Events
Xls.Exploit.Swfdrop::95.sbx.tg	68
Doc.Exploit.Mspoint::95.sbx.ta	19

Top Malware Senders

Sending IP	Events
::192.168.104.245	77
::	4

簡単に FTD をクラウド管理に移行可能



- 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

Inventory / Change FTD Manager

Change FTD Management
Change FTD Manager from Firewall Management Center to CDO

1 Select FMC FMC: 1771Fmc

2 Select Devices

Select FTD devices to change management from FMC to CDO and specify an action in bulk or per device.

6 device(s) selected Multi-Device Action Multiple Actions Selected

<input checked="" type="checkbox"/>	Name	IP Address	Domain	Action
<input checked="" type="checkbox"/>	1771Fmc_10...	10.10.16.94:44	Global	Delete FTD from FMC
<input checked="" type="checkbox"/>	1771Fmc_10...	10.10.16.87:44	Global	Delete FTD from FMC
<input checked="" type="checkbox"/>	1771Fmc_10...	10.10.16.86:44	Global	Retain on FMC for Analytics
<input checked="" type="checkbox"/>	1771Fmc_10...	10.10.16.70:44	Global	Retain on FMC for Analytics

Change FTD Management

After completing the change FTD manager process, you have up to 14 days to commit to CDO as your FTD manager or revert to FMC as your FTD manager.

After 14 days have passed, the actions you selected during this process will be automatically applied to your devices without further action from you. [Learn more.](#)

Warning: Deleting an FTD from FMC is final.

Cancel

オンプレミス FMC で管理している FTD デバイスをそれぞれ選択可能

cdFMC 管理に移行しても 14日間はオンプレミス FMC 管理に戻すことが可能

參考資料

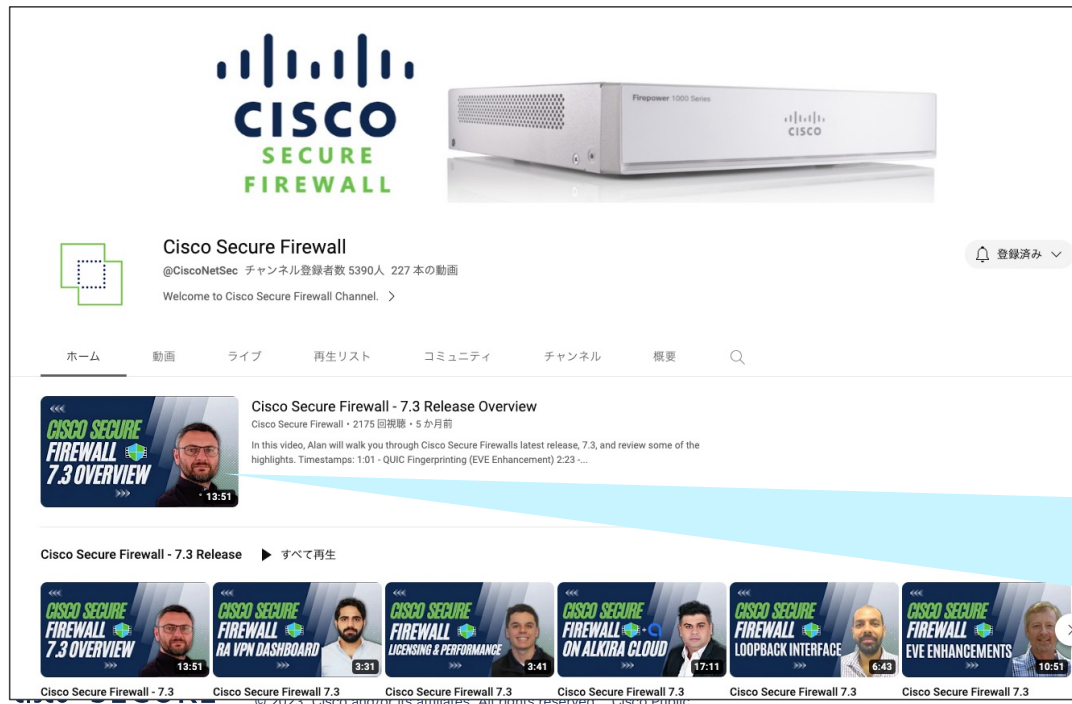
参考資料

- [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>



CISCO
SECURE
FIREWALL

Firepower 1000 Series
CISCO

Cisco Secure Firewall
@CiscoNetSec チャンネル登録者数 5390人 227本の動画
Welcome to Cisco Secure Firewall Channel >

ホーム 動画 ライブ 再生リスト コミュニティ チャンネル 概要

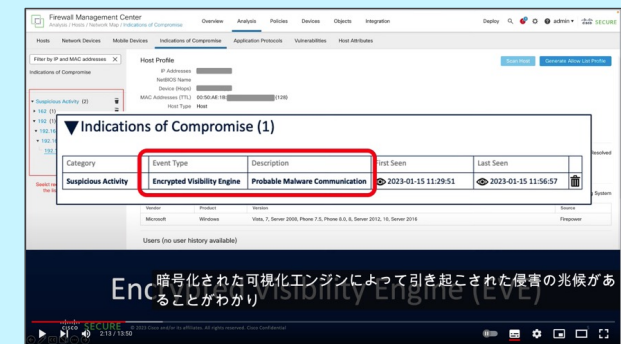
CISCO SECURE FIREWALL 7.3 OVERVIEW
Cisco Secure Firewall - 7.3 Release Overview
Cisco Secure Firewall • 2175 回視聴 • 5 か月前
In this video, Alan will walk you through Cisco Secure Firewalls latest release, 7.3, and review some of the highlights. Timestamps: 1:01 - QUIC Fingerprinting (EVE Enhancement) 2:23 ...

Cisco Secure Firewall - 7.3 Release ▶ すべて再生

CISCO SECURE FIREWALL 7.3 OVERVIEW 13:51
CISCO SECURE FIREWALL RA VPN DASHBOARD 3:31
CISCO SECURE FIREWALL LICENSING & PERFORMANCE 3:41
CISCO SECURE FIREWALL ON ALKIRA CLOUD 17:11
CISCO SECURE FIREWALL LOOPBACK INTERFACE 6:43
CISCO SECURE FIREWALL EVE ENHANCEMENTS 10:51

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

多くの動画で日本語への自動翻訳が有効



Firewall Management Center
Overview Analysis Policies Devices Objects Integration
Hosts Network Devices Mobile Devices Indications of Compromise Application Protocols Vulnerabilities Host Attributes

Filter by IP and MAC addresses X

Host Profile
IP Address: [REDACTED]
HostID Name: [REDACTED]
Device Group: [REDACTED]
MAC Address (F1): [REDACTED]
Host Type: Host

Indications of Compromise (1)

Category	Event Type	Description	First Seen	Last Seen
Suspicious Activity	Encrypted Visibility Engine	Probable Malware Communication	2023-01-15 11:29:51	2023-01-15 11:56:57

Users (No user history available)

Encrypted Visibility Engine (EVE)
暗号化された可視化エンジンによって引き起こされた侵害の兆候があることがわかり

Cisco サクセスちゃんねる

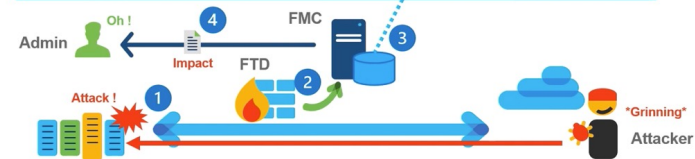
- Cisco Customer Success / Customer Experience チームが日本語で運営
- サービス・製品使いこなしテクニックの動画が多数有り

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

Impact Flag の概要

✓ 侵害が発生時、影響度を5段階で通知

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



Cisco Security オンラインセミナー 資料と録画のご案内



The screenshot shows the Cisco Engage website interface. At the top, there is a navigation bar with the Cisco logo and links for '製品とサービス', 'ソリューション', 'サポート', and '学び'. On the right, there are links for 'サイトマップ' and '検索'. The main header area features the 'CISCO Engage' logo and the text 'Cisco Security オンラインセミナー'. Below this, a message states: '最新のシスコセキュリティセミナー登録や開催済セミナーのコンテンツをご覧いただけます。' (You can view the content of the latest Cisco Security seminars and completed seminars.) A blue button labeled 'セミナーへお申し込みはこちら' (Click here to register for the seminar) is positioned below the message. At the bottom, a table lists seminar sessions with columns for '日時' (Date/Time), 'セッションタイトル' (Session Title), 'セッション資料' (Session Materials), and 'セッション録画' (Session Recording). Two sessions are listed, each with a corresponding 'オンデマンド録画' (On-demand recording) button.

日時	セッションタイトル	セッション資料	セッション録画
2023.4.20	既存 SASE の課題を解決する、Cisco 最新型 SASE のご紹介		オンデマンド録画
2023.3.2	セキュリティレジリエンスを実現するには：最新のシスコセキュリティ成果レポートからの教訓		オンデマンド録画

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


CISCO SECURE