



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

2024年1月

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

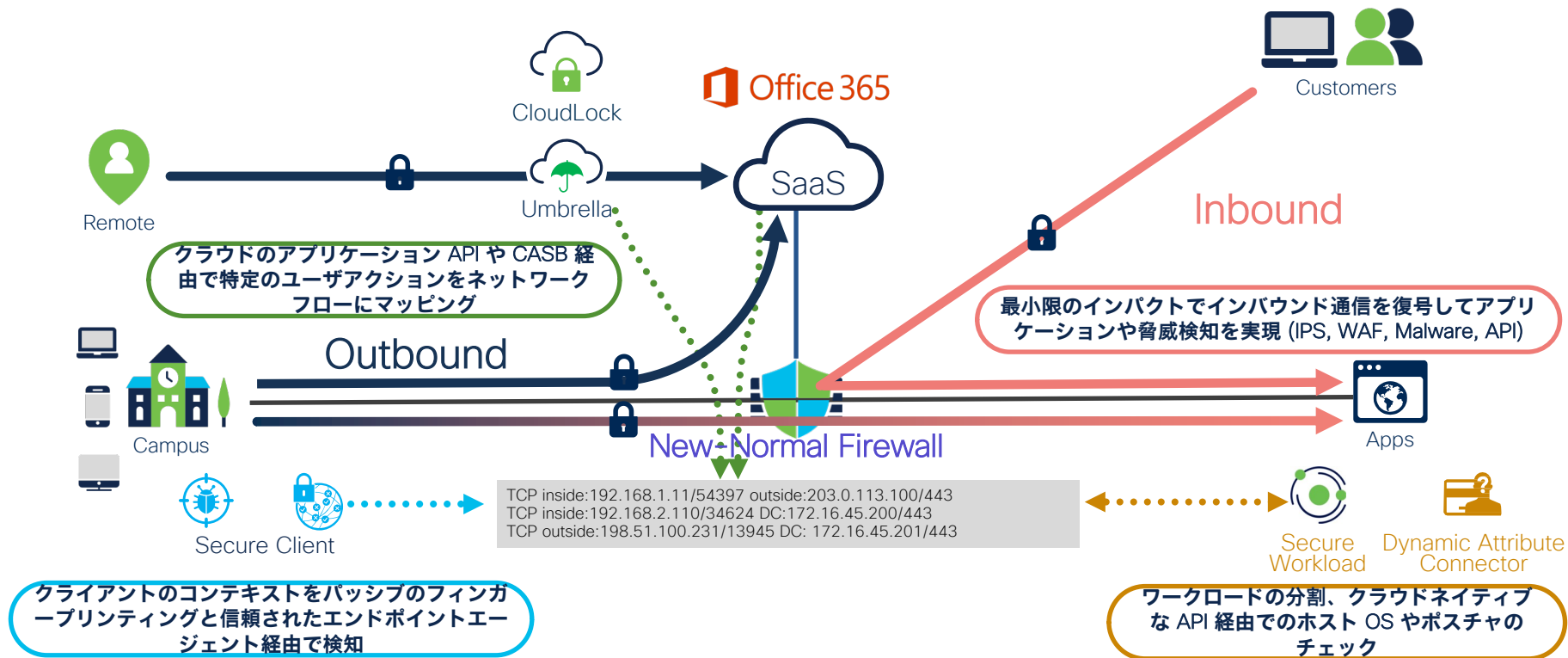
小林 達哉 (tatskoba@cisco.com)

アジェンダ

- Firewall Threat Defense の概要
- Firewall プラットホーム
- Firewall Threat Defense のアーキテクチャ
- まとめ

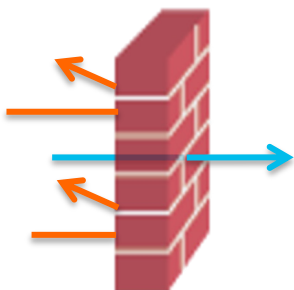
Firewall Threat Defense の概要

Secure Firewall Threat Defense でのインスペクション



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



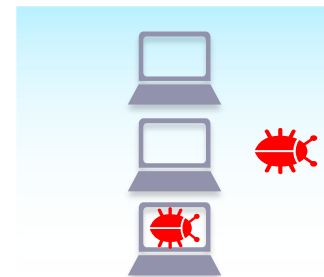
Web アプリケーション、
ユーザ、脅威の可視化

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

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

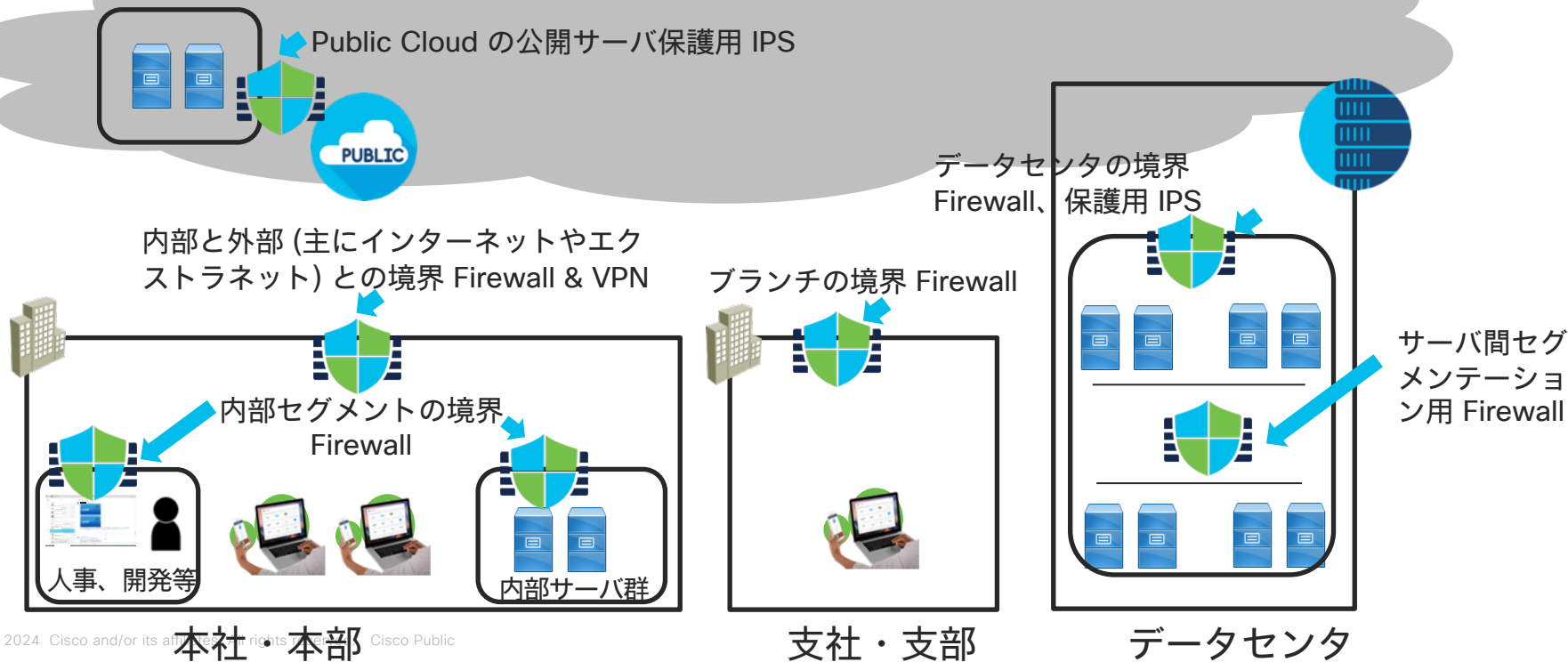
Cisco 提供脅威情報活用
3rd パーティとの脅威情報連携

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り舞いを確認
 - 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

2020-07-30 15:38:32	medium	2	↓	192.168.10.101	192.168.20.102	8 (Echo Request) / icmp	Unknown (Unknown)	0	PROTOCOL-ICMP Un
2020-07-30 15:38:19	low	3	↓	146.112.41.2	192.168.20.102	443 (https) / tcp	Unknown (Unknown)	0	HI_SERVER_NO_CON
2020-07-30 15:37:51	high	2	↓	192.168.10.101	192.168.20.102	36735 / tcp	Unknown (Unknown)	0	SERVER-OTHER Nov

ホストプロフィール

IPアドレス 192.168.20.102
NetBIOS名
デバイス (Hop) FTDv66-1 (0)
MACアドレス(TTL) 00:0C:29:1D:47:5E (VMware, Inc.) (128)
ホストタイプ Host
最後の発見 2020-08-03 17:01:57
現在のユーザ

ホストのスキャン

ホワイトリストプロファイル

アプリケーション (60)

アプリケーションプロトコル	クライアントアプリケーション
<input type="checkbox"/> DNS over HTTPS	<input type="checkbox"/> DNS over HTTPS
<input type="checkbox"/> SSL	<input type="checkbox"/> SSL client
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client
<input type="checkbox"/> SSL	<input type="checkbox"/> SSL client
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client

クライアントアプリケーション

User History

Users	2020-08-03 09:05:39
Discovered Identities\setsuko.overton (LDAP)	
armando zuniga (dcloud.cisco.com\azuniga, LDAP)	

ユーザ履歴

侵入の痕跡 (1)

侵入の痕跡

カテゴリ	イベントタイプ	説明	最初の発見	最後の発見
Impact 2 Attack	Impact 2 Intrusion Event - attempted-user	The host was attacked and is potentially vulnerable	2020-07-30 15:37:51	2020-07-30 15:37:51

オペレーティングシステム

端末 OS

ベンダー	製品	バージョン	送信元
Microsoft	Windows	7, Server 2008, Phone 7.5, 8	Firepower

サーバ (15)

サーバ アプリケーション

プロトコル	ポート	アプリケーションプロトコル	製造元およびバージョン
tcp	8000
tcp	1
tcp	443

脆弱性 (1022)

該当脆弱性リスト

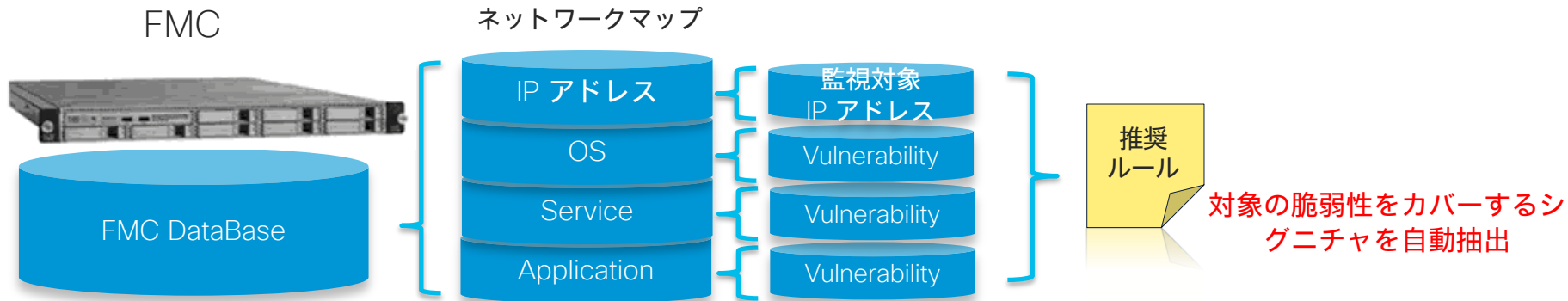
A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system, aka "Microsoft JET Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012	Windows 7, Server 2008, Phone 7.5, 8
A buffer overflow vulnerability exists in the Microsoft JET Database Engine that could allow remote code execution on an affected system, aka "Microsoft JET Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012	Windows 7, Server 2008, Phone 7.5, 8
A DCOM object in Helppane.exe in Microsoft Windows 7 SP1; Windows Server 2008 R2; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows local users to gain privileges	Windows 7, Server 2008, Phone 7.5, 8

✓ 端末のセキュリティに関連する様々な情報を自動収集し、解析に活用

自動チューニング

- 対象ネットワークの保護に必要なシグネチャおよびアクション(イベント生成、ドロップ)を抽出
- 推奨設定の生成および適用は、オンデマンドまたはスケジューリングに対応

✓ ネットワークの変化に対応し、設定を自動更新



✓ 必要なシグネチャをのみを有効化することにより、誤検知を大幅削減

インパクトフラグ

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

		攻撃の危険度		インパクトフラグ		
2020-08-03 09:22:00	medium	3		3	10.1.120.17	62.51.0.36
2020-08-03 09:17:52	high	1	↓	1	10.1.108.15	144.76.133.38
2020-08-03 09:17:32	high	2	↓	2	10.1.114.34	10.100.9.4
2020-08-03 09:11:25	high	1	↓	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

自動チューニング(推奨設定)とインパクト解析

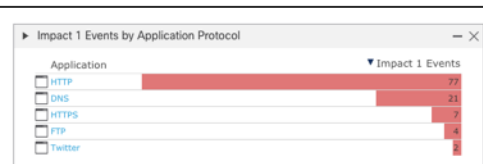
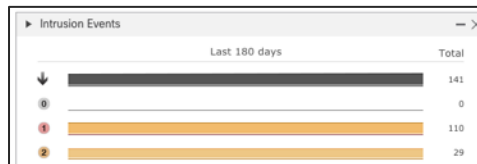
一般的な侵入検知機器 (IPS) の
運用者が抱える問題

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
要なものが見えない・・・

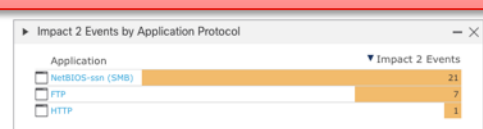
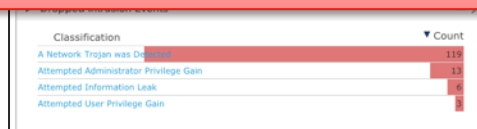


自動チューニング(推奨設定)
ネットワーク環境を学習し、
最適な推奨設定を自動生成



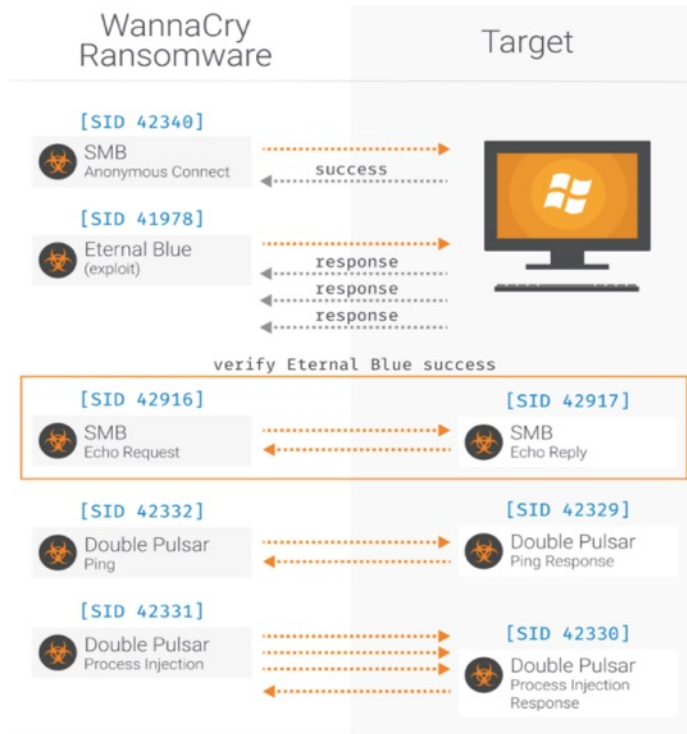
インパクト解析

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づいてチューニング



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



- 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		✓

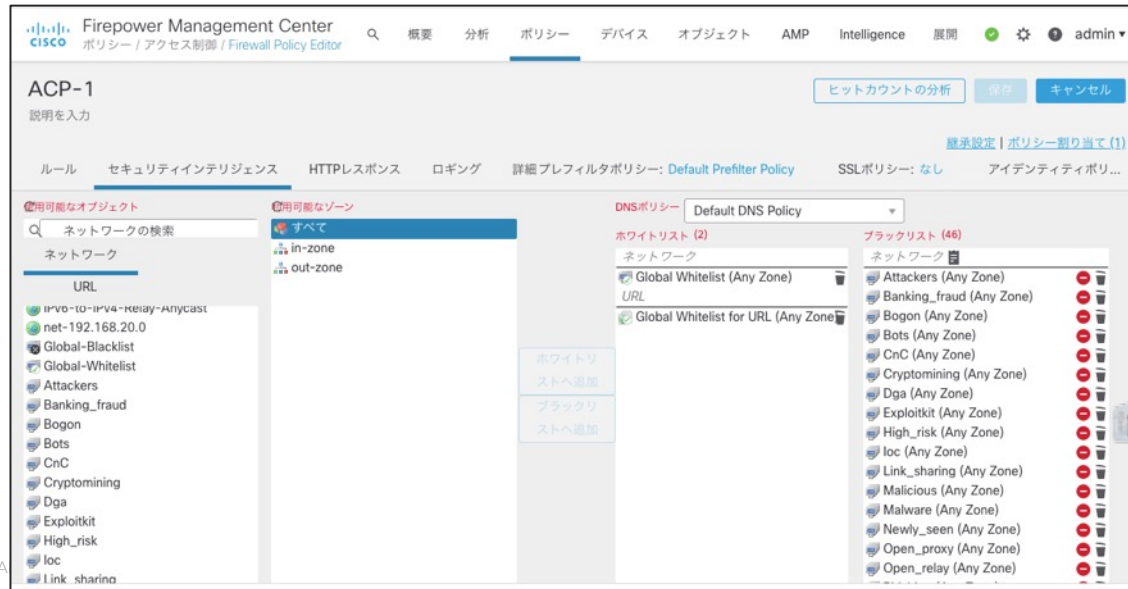
Snort 2 に比べて Snort Process Restart の必要なケースが大幅に減少
通常のポリシー設定や DB 更新においては Snort Process Restart が不要

[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 からの接続を モニターもしくはブロック
- カテゴリー
 - CnC
 - Malware
 - Phishing
 - Bots
 - Attackers など



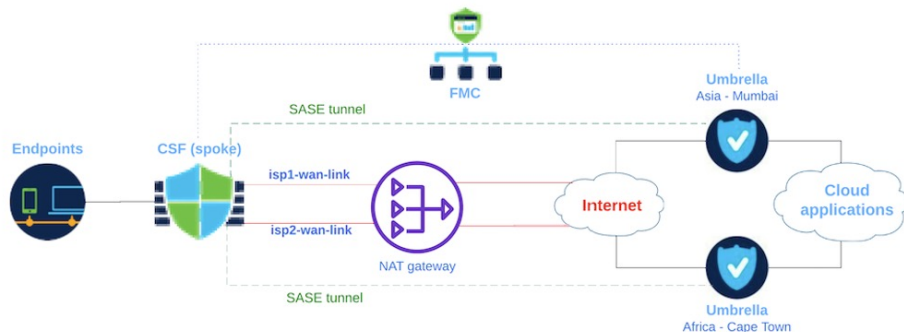
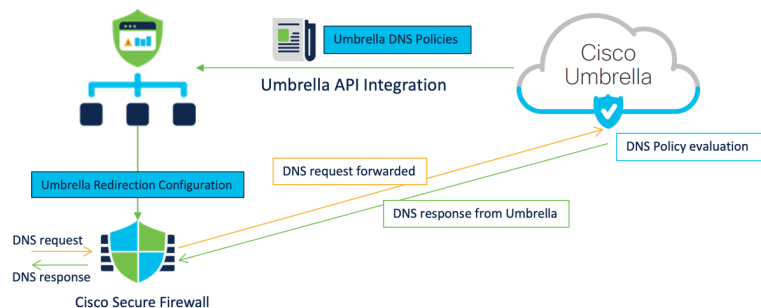
Umbrella とのインテグレーション

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

Secure Firewall Management Center



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

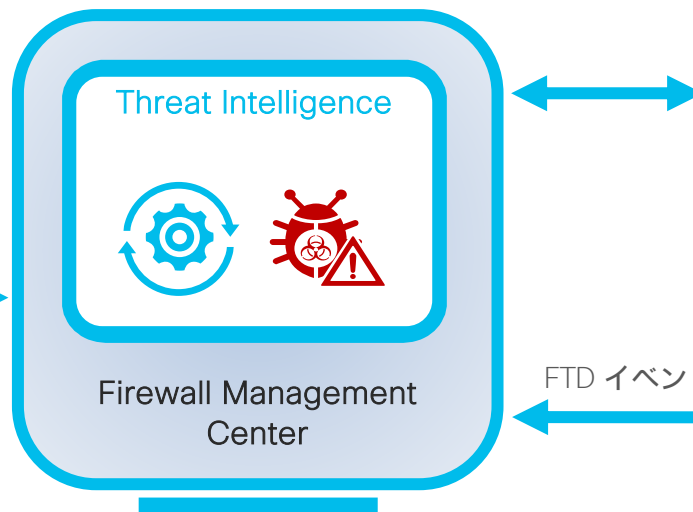
サードパーティ:

- CrowdStrike
- Flashpoint
- Soltra Edge
- Eclectiq
- 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 <i>Indicator Imported From a Flat File</i>	test	1	Monitor	Block Monitor	Jul 24, 2018 6:18 AM EDT	Completed

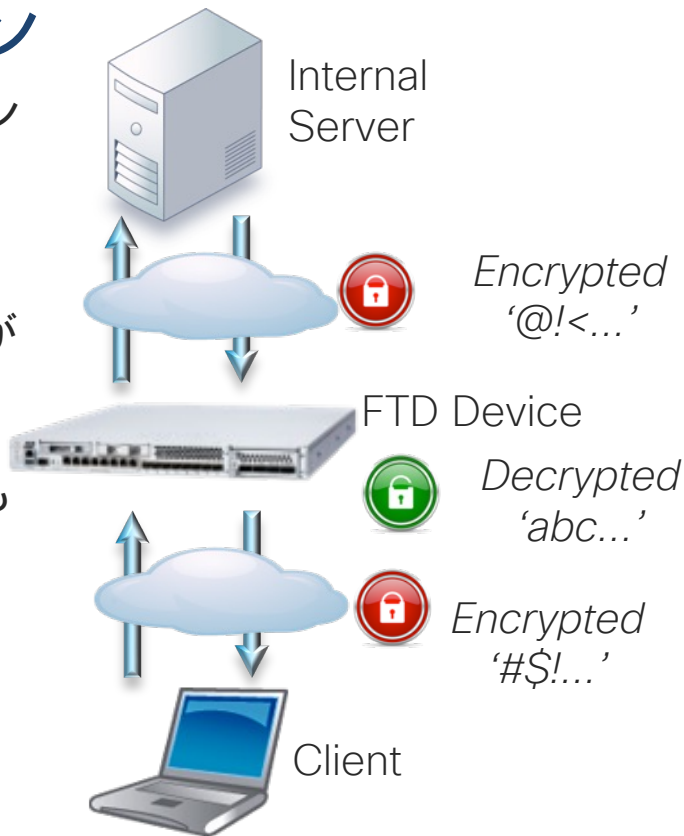
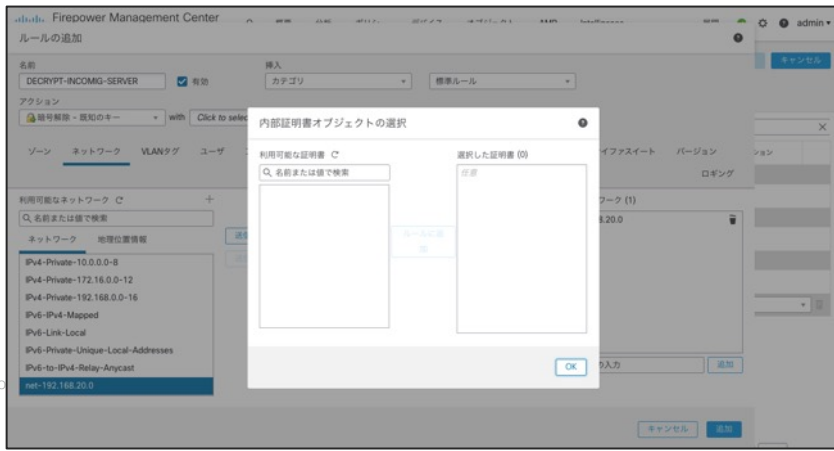
ジオロケーション

- 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、ファイアポリシー等の任意の設定と組み合わせて利用可

The screenshot displays the 'Rule Addition' (ルールの追加) configuration window. At the top, the rule name is 'Monitoring from some countries', which is checked as active (有効). The rule is applied to 'Rule's Sub' (ルールの下) and has a priority of 2. The action is set to 'Allow' (承認), and the time range is 'None' (なし). Below the configuration, there are tabs for various attributes: Zone, Network, VLAN Tag, User, Application, Port, URL, SGT/ISE Attribute, Check, Logging, and Comment. The 'Network' tab is selected, showing a search bar and two columns: 'Available Networks' (利用可能なネットワーク) and 'Destination Networks' (送信先ネットワーク). The 'Available Networks' column lists geographical regions: Africa (58 countries), Antarctica (3 countries), and Asia (50 countries). Under Asia, several countries are listed with their respective flags: Afghanistan, Armenia, Azerbaijan, Bahrain, and Bangladesh. There are buttons to add networks to the 'Destination Networks' list: 'Add to Destination Networks' (送信元ネットワークに追加) and 'Add to Destination' (送信先に追加). The 'Destination Networks' column currently contains three entries: China, United States, and Russian Federation, each with a trash icon for removal. At the bottom, there are input fields for 'IP Address Input' (IPアドレスの入力) and 'Add' (追加) buttons for both columns.

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 Version 7.2 にて対応済み。TLS 1.2 にダウングレードしてのインスペクションも可能



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	First Seen	2020-08-03 18:51:51 オン	192.168.10.101	実行者: No Authentication Required
ファイル名	eicar.com	Last Seen	2020-08-03 18:53:54 オン	192.168.10.101	実行者: No Authentication Required
File Size (KB)	0.0664	時間	2020-08-03 18:53:54	14	
ファイルタイプ	EICAR	イベントタイプ	送信されたファイル	2ホスト	
File Category	Executables	IPアドレス	192.168.10.101	送信者数: 1 → 受信者数: 1	
Current Disposition	Malware	ブロックされた受信者	192.168.20.102		
Threat Score	Very High	アクション	Malware Block		
検知名	EICAR	アプリケーションプロトコル	HTTP		
Trajectory		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	送信者	ファイル名	ファイルタイプ	検出	アクション	説明
2020-08-03 18:...	転送	192.168.10.101	192.168.20.102	No Authentication...	eicar.com	Mal...	Malware Block	HTTP	Chrome
2020-08-03 18:...	転送	192.168.10.101	192.168.20.102	No Authentication...	eicar.com	Mal...	Malware Block	HTTP	Chrome

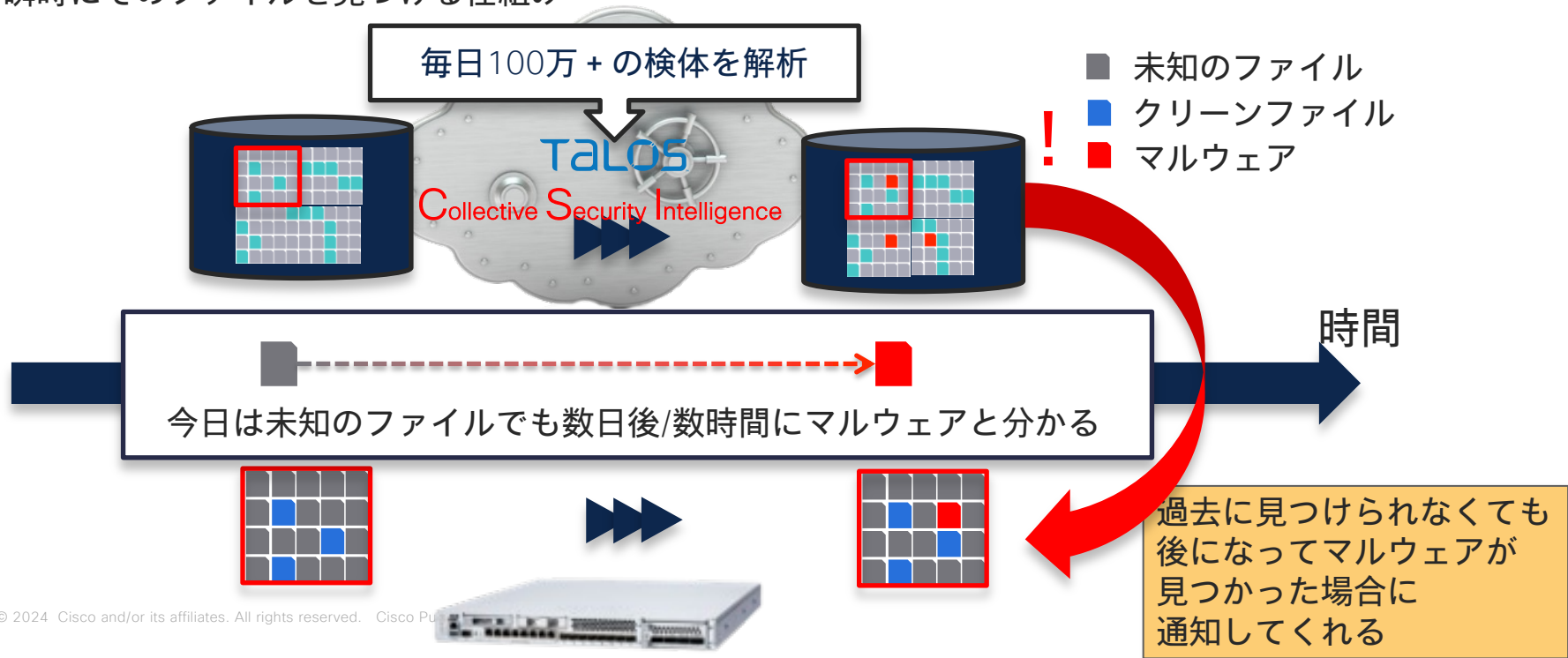
② 解析情報(サンドボックス含む)と連携

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



クラウドリコールによるゼロデイマルウェア検知例

Firepower Management Center
分析 / ファイル / ネットワークファイルトラジェクトリ

4b061e78...4d18e0b0のネットワークファイルトラジェクトリ

ファイルSHA256 4b061e78...4d18e0b0
ファイル名 malware.exe
File Size (KB) 136.2607
ファイルタイプ MSEXE
File Category Executables
Current Disposition Malware
Threat Score None

First Seen 2020-08-04 17:56:37 オン 192.168.10.101 実行者: No Authentication Required
Last Seen 2020-08-04 17:57:38 オン 192.168.20.102 実行者: No Authentication Required
イベント 2
Seen On 3ホスト (2件表示)
Seen On Breakdown 送信者数: 2 → 受信者数: 2 (1 → 1件表示)

Trajectory

Aug 04
17:56 17:57

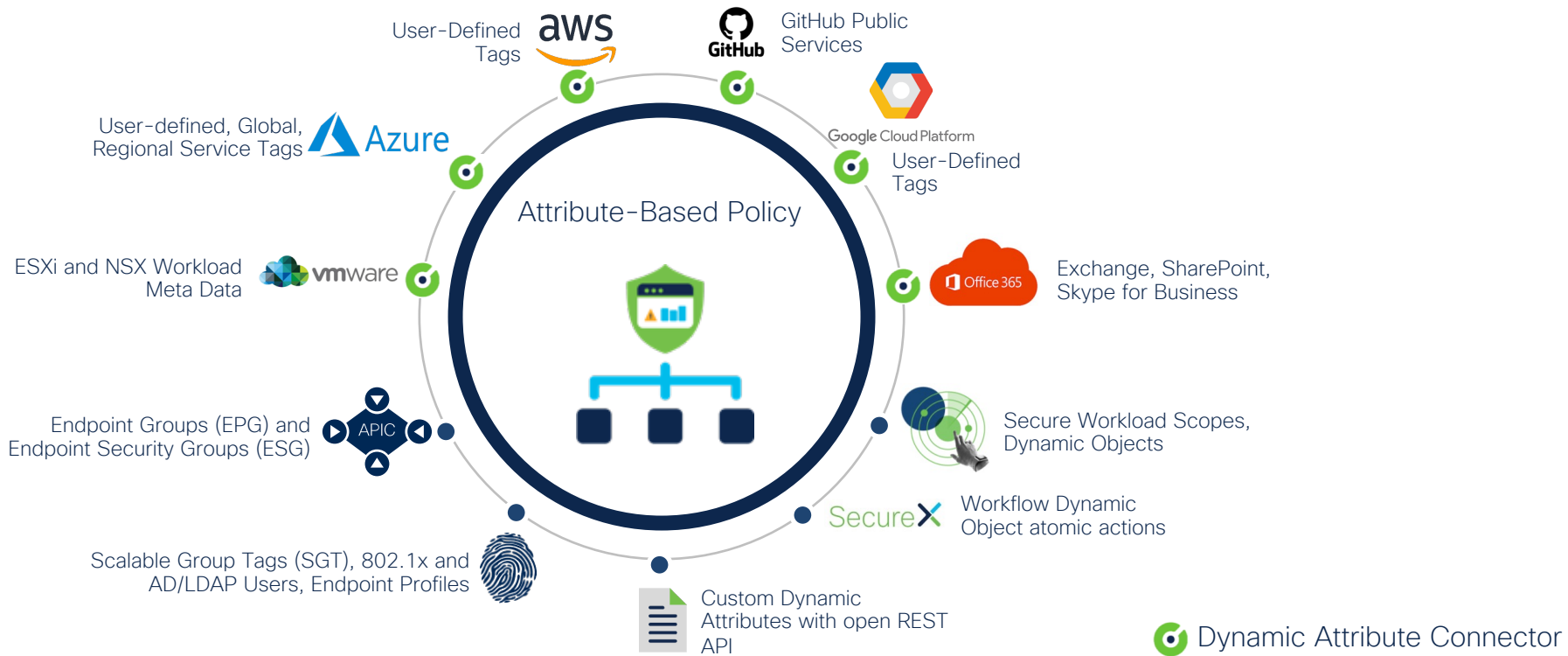
192.168.10.101
192.168.20.102

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

Events

時間	イベントタイプ	送信側IP	受信側IP	ユーザ	ファイル名	傾向	アクション	プロトコル	クライアント	ウェアアプリケ	説明
2020-08-04 17:56:37	転送	192.168.10.101	192.168.20.102	No Authentication Required	malware.exe	Unknown	Malware Cloud Look...	HTTP	Chrome		Retrospective Event (L...
2020-08-04 17:57:38	回顧的イベント					Malware					Malware Detected by ...

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 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

Return to Access Control Policy Management

ACP-1

Packets → Prefilter Rules → Decryption → Security Intelligence → Access Control

Total 5 rules

Name	Action	Sources	Destinations and Applications
Mandatory (1 - 5)			
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 DYN Servers1 SSH Servers2
4 CATCH-AWS	Block with re...	NET any	NET AWS-Tokyo-VPC
5 CATCH-ALL	Allow	Any	Any

Default

There are no rules in this section. Add Rule or Add Category

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

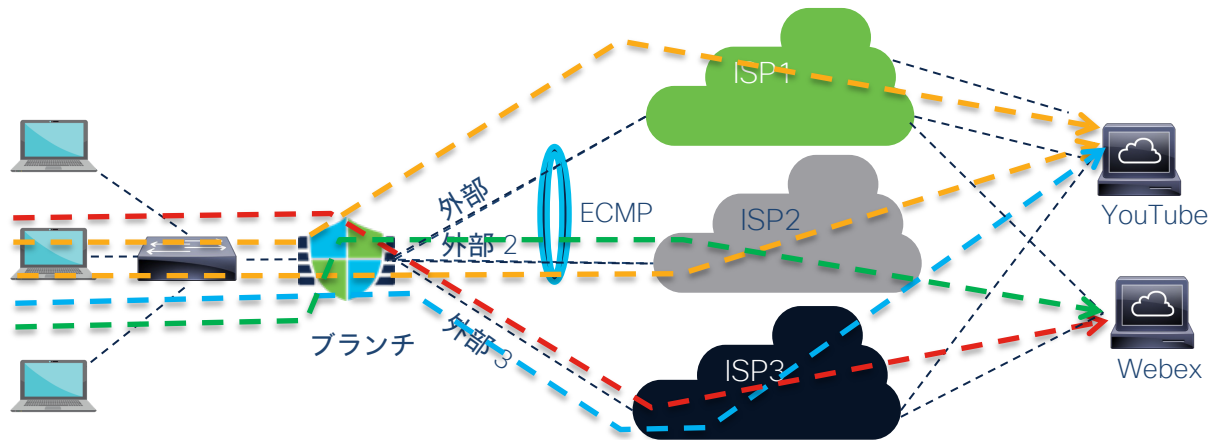
インテリジェントルーティング

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

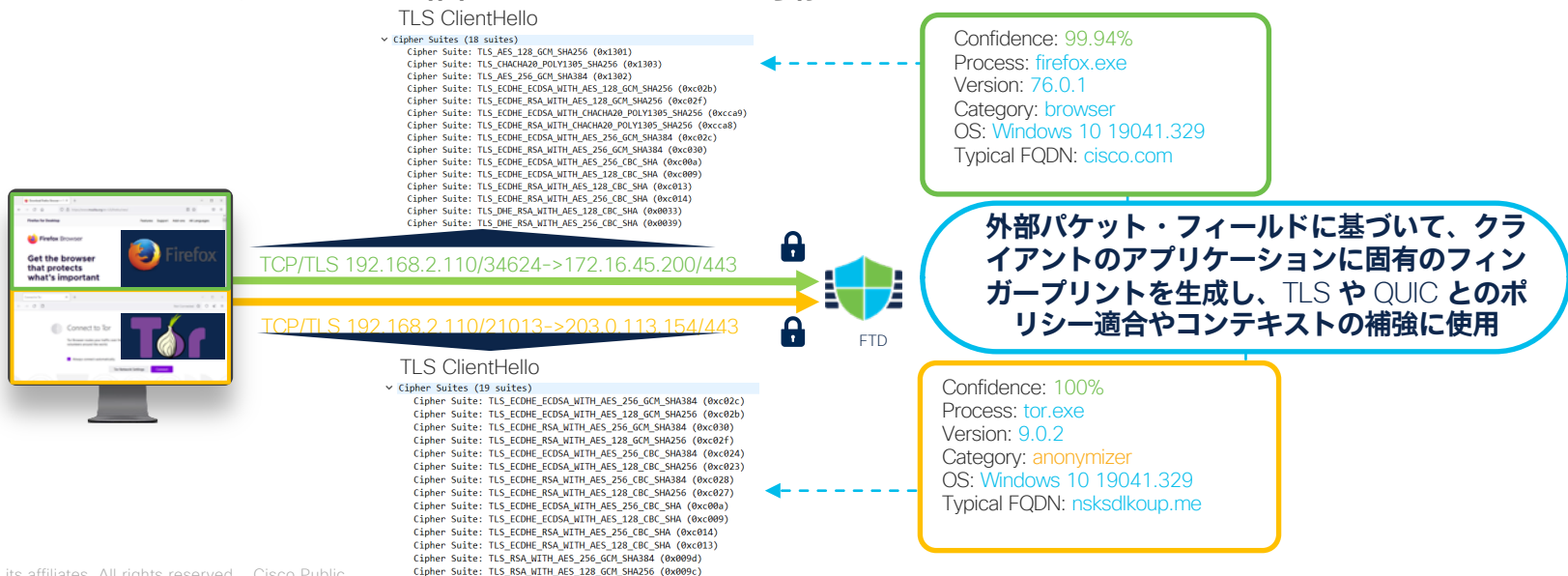


WAN のパス

- > YouTube へのプライマリパス
- > YouTube へのセカンダリパス
- > Webex へのプライマリパス
- > Webex へのセカンダリパス

Encrypted Visibility Engine

- 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



FMC での VPN ダッシュボード

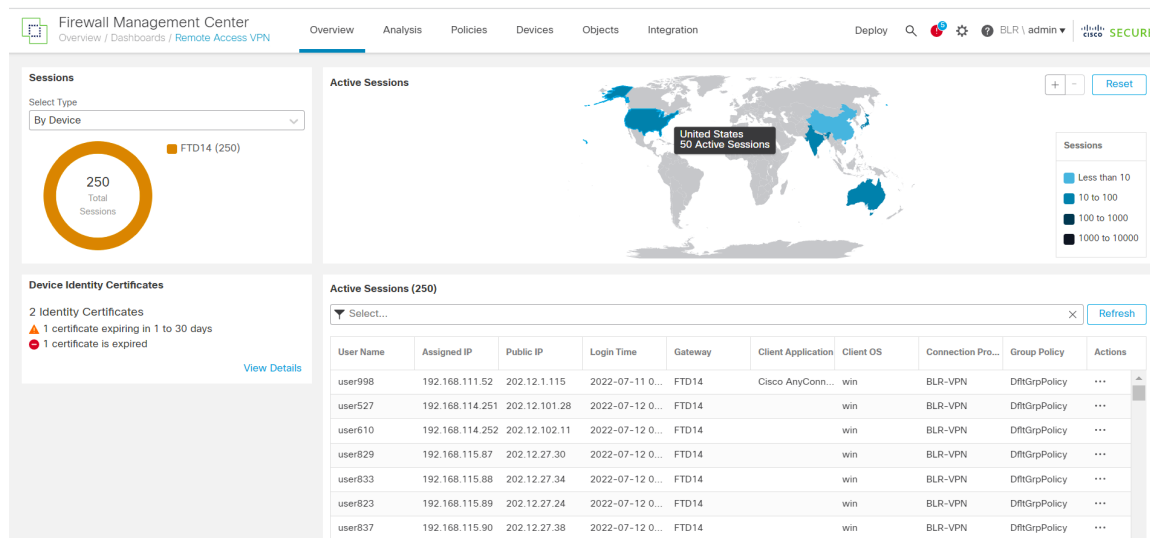
アプリケーション認識型ファイアウォールポリシーの適用、パスの選択、および復号

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



Custom Report レポート機能

柔軟なレポート機能：レポートデザイナー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

概要

シスコは、シスコシステムズ：eCloudが最新のデータに基づいて分析しました。その結果は、ビジネスの成長を促進するもの、潜在的なリスクを特定するもの、およびネットワークの脆弱性を明らかにするものを含みます。これらのデータは、ネットワークの脆弱性を特定し、脆弱性を減らすためのアクションを推奨します。マルウェアも検出され、脆弱性を減らすためのアクションがあります。

詳細期間: Sat Apr 29 2017 04:23:53 ~ Mon May 29 2017 04:23:53

リスクのあるアップリケーション	リスクのあるユーザー	高権限アップリケーション
9	18	1
権限化アップリケーション	セキュリティ関連機能を持つアップリケーション	危険なwebブラウザ
9	2	56

ネットワークプロファイル

10	8	83	5
オペレーティングシステム	モバイルデバイス	使用時のアプリケーション	転送されるファイルタイプ

概要

シスコは、シスコシステムズ：eCloudが最新のデータに基づいて分析しました。その結果は、ビジネスの成長を促進するもの、潜在的なリスクを特定するもの、およびネットワークの脆弱性を明らかにするものを含みます。これらのデータは、ネットワークの脆弱性を特定し、脆弱性を減らすためのアクションを推奨します。マルウェアも検出され、脆弱性を減らすためのアクションがあります。

アタックレポート

概要

シスコはシスコシステムズ：eCloudが最新のデータに基づいて分析しました。その結果は、悪意のあるホストを特定し、脆弱性を減らすためのアクションを推奨します。リスクを軽減するためのアクションを推奨します。マルウェアも検出され、脆弱性を減らすためのアクションがあります。

詳細期間: Sat Apr 29 2017 04:24:22 ~ Mon May 29 2017 04:24:22

合計攻撃数	警告する攻撃数	脆弱となったホスト
28,675	0	0
無関係な攻撃	注意が必要なイベント	CUCサーバに接続されているホスト
100%	0%	0

関連の攻撃によりもたらされるリスク

攻撃	ホスト
PrivateBot Bot Traffic	5,888
Advanced Information Leak	8,903
Ultimate Traffic	5,889
Site Activity	2,257
Malicious Leak	5,961

シスコは、シスコシステムズ：eCloudがCisco Firepowerプライマリスをインストールして実行することを勧めます。
1. プライマリスをインストールして実行することをお勧めします。
2. ネットワークの脆弱性を特定し、脆弱性を減らすためのアクションを推奨します。
3. このリスクの軽減を推奨するために自動的に生成された脆弱性を減らす

マルウェアレポート

概要

シスコは、シスコシステムズ：eCloudが最新のデータに基づいて分析しました。その結果は、悪意のあるマルウェアファミリーによる攻撃を特定し、脆弱性を減らすためのアクションを推奨します。リスクを軽減するためのアクションを推奨します。マルウェアも検出され、脆弱性を減らすためのアクションがあります。

詳細期間: Sat Apr 29 2017 04:24:27 ~ Mon May 29 2017 04:24:27

マルウェアを検出	IOCを示しているホスト	脆弱プロトコル
36	19	2
CUCサーバに接続されているホスト	マルウェアの送信	マルウェアのURL
0	22	2

マルウェアのプロファイル: 30日

27	ダウンロード元: 3	ダウンロードの実行数: 3	ダウンロード先: 7
さまざまなマルウェアファミリーがダウンロード	独自の固有のホスト	独自のユーザー	独自のデバイス

シスコは、Advanced Malware Protectionをインストールして実行することを勧めます。
1. 高度なマルウェアの検出能力の可用性を確保する。
2. このリスクを軽減するために自動的に生成された脆弱性を減らす

Cisco AI Assistant for Security

Return to Access Control Policy

ACP - Production

Analyze Rule Heartbeat Reset Save

Packets + Prefilter Rules + Decryption + Security Intelligence + Identity + Access Control + More

Targeted: 3 device

Total 9 rules Add Category Add Rule Ask AI

Name	Action	Source				Destination			
		Zones	Networks	Ports	Dynamic Attributes	Zones	Networks	Ports	Applications
Mandatory									
There are no rules in this section Add Rule Add Category									
Default (1-9)									
<input type="checkbox"/> 1 External	Block	Any	any-ipv4 -1 more	Any	Any	Any	Any	TCP_47001	Any
<input type="checkbox"/> 2 Internal	Allow	Any	any -1 more	Any	Any	Any	Any	TCP_8302	Cisco
<input type="checkbox"/> 3 Block Malwares	Block	Any	any-ipv4 -1 more	Any	Any	Any	Any	Any	Tiny
<input type="checkbox"/> 4 Block Torrent	Block	Any	Germany -8 more	Any	Any	Any	Any	Bit-torrent	Torrent

Default Action: Intrusion Prevention: Balanced Security and Con...

Ask Cisco AI

Show me access policies related to the user group lmn-vendor

Cisco Assistant 8:12 AM

Absolutely! There are **3 Access Control Policies** related to user group lmn-vendor. There are **10 Access Control Rules** across these 3 policies.

- 4 rules are about **Sensitive Data**
- 4 rules are about **Internet Access**
- 2 rules are about **Internal Application Access**

Regenerate

Ask a question or request, or type "?" for suggestions

Privacy policy Terms of service

Assist



Firewall ポリシーの構成

Augment



トラブルシューティング

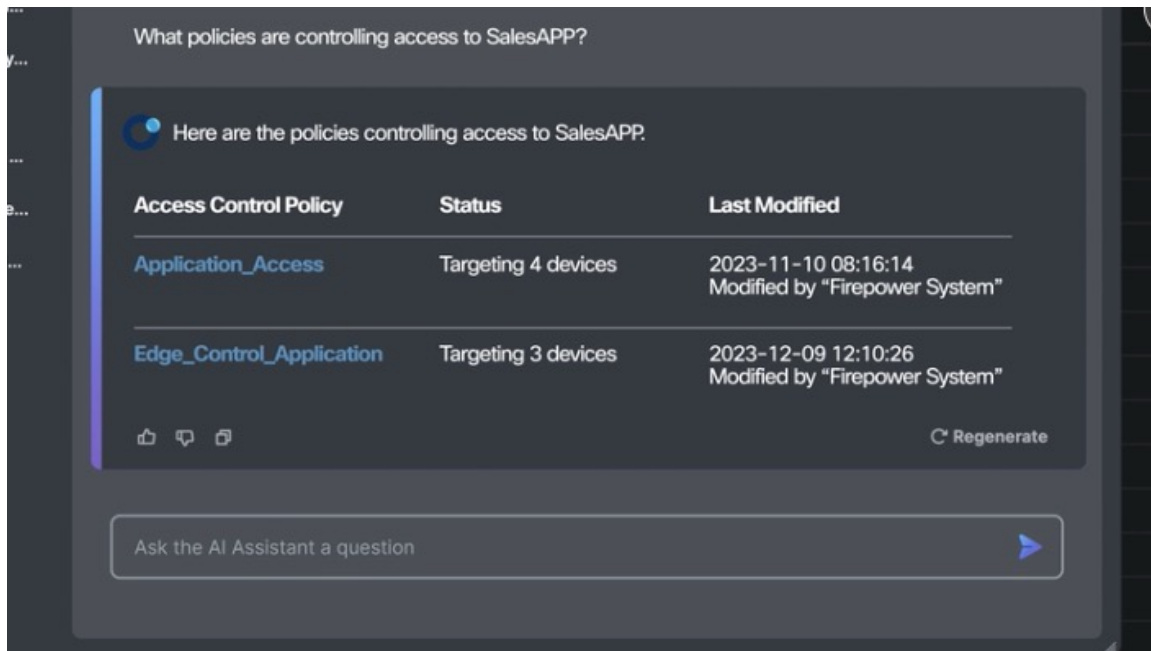
Automate



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/en/us/products/security/artificial-intelligence-ai.html?socialshare=lightbox-security-ai>



What policies are controlling access to SalesAPP?

Here are the policies controlling access to SalesAPP.

Access Control Policy	Status	Last Modified
Application_Access	Targeting 4 devices	2023-11-10 08:16:14 Modified by "Firepower System"
Edge_Control_Application	Targeting 3 devices	2023-12-09 12:10:26 Modified by "Firepower System"

👍 🗨️ 📄 🔄 Regenerate

Ask the AI Assistant a question ➔

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

FTD Virtual 版と FP2110 を 1台の FMC で管理している例

The screenshot shows the FMC web interface with a table of managed devices. A red box highlights two specific entries: FP2110-b1 and FTDv66-1.

名前	モデル	バージョン	シャーシ	ライセンス
FP2110-b1 10.71.153.56 - Routed	FTD on Firepower 2110	6.4....	N/A	ベース、脅威 (2 more...)
FTDv66-1 10.71.132.199 - Routed	FTD for VMWare	6.6.0	N/A	ベース、脅威 (2 more...)

✓ FP2110-b1 10.71.153.56 - Routed	FTD on Firepower 2110	6.4....
✓ FTDv66-1 10.71.132.199 - Routed	FTD for VMWare	6.6.0

Firewall Management Center (On Premise) プラットフォーム一覧



FMC1700
最大 50個のセンサー管理
最大イベント数 3,000万件
900GB のイベントストレージ
最大 5万ホスト、5万ユーザの
ネットワークマップ
HA対応



FMC2700
最大 300個のセンサー管理
最大イベント数 6,000万件
1.8TB のイベントストレージ
最大 15万ホスト、15万ユーザの
ネットワークマップ
HA対応



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



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

FTD の機能を最大限に引き出す管理サーバ

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



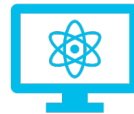
テナント毎に25%以上の
Firewall をサポート



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

無料で提供される 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

The screenshot displays the Cisco Firepower Device Manager (FDM) web interface. At the top, it shows the device name 'FTDv66-2' and various system status indicators like 'モデル: Cisco Firepower Threat Defense for VMWare...', 'ソフトウェア: 6.6.0-90', and 'VDB: 335.0'. The main area features a network diagram with a central FTD device connected to an internal network and an ISP/WAN. Below the diagram are several configuration panels: 'インターフェイス' (Interfaces) showing 9 active ports, 'ルーティング' (Routing) with 1 static route, '更新' (Updates) with system update information, 'システム設定' (System Settings) for management access, 'スマート ライセンス' (Smart Licenses) with registration status, 'バックアップと復元' (Backup and Restore), 'トラブルシューティング' (Troubleshooting) with a file creation button, 'サイト間VPN' (Site-to-Site VPN), 'リモート アクセス VPN' (Remote Access VPN), '詳細設定' (Advanced Settings) with FlexConfig and Smart CLI, and 'デバイス管理' (Device Management) for monitoring and deployment.

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

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



* FTD 側は Data Interface
で管理することも可能

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

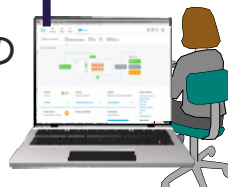
FTD 本体



https
ブラウザで管理・設定

FDM
= Firewall Device Manager

FDMの
画面



共存
不可

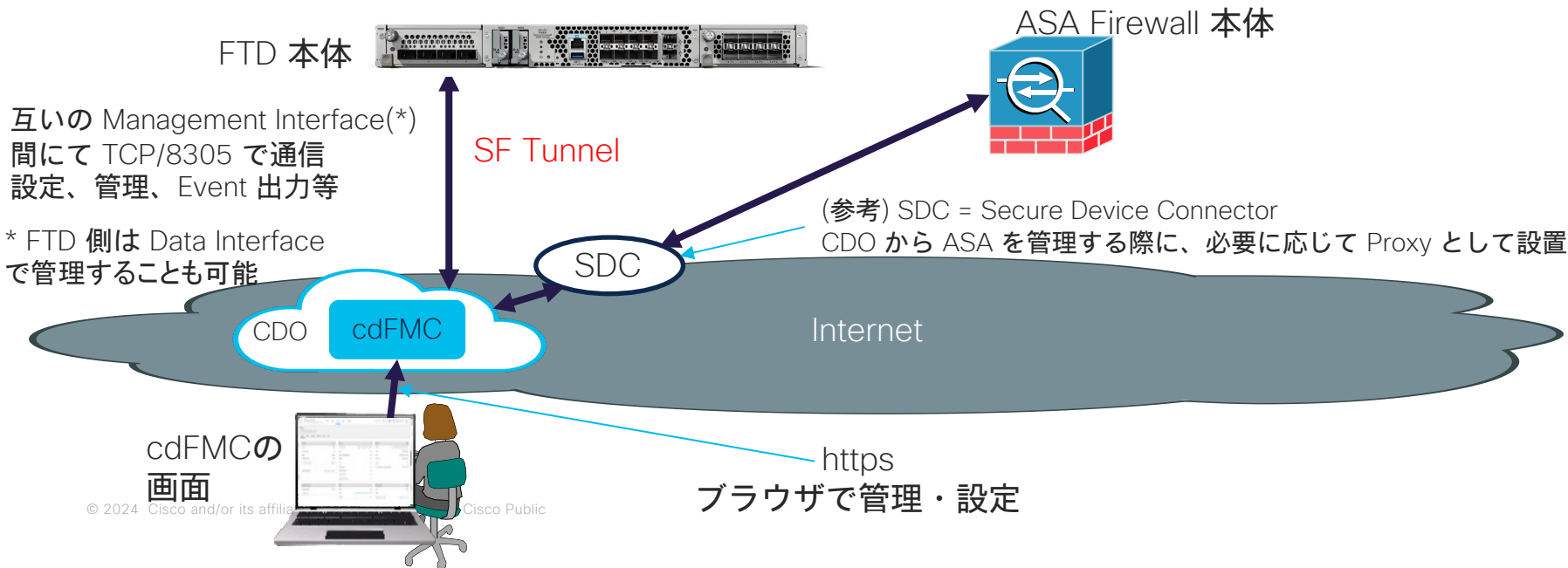
FTD の管理・設定アーキテクチャ (Cloud)

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



Cisco Firewall プラットホーム

FTD / ASA どちらも利用可能

Private Cloud

Public Cloud

HyperFlex

vmware ESXi

aws

Google Cloud Platform

Microsoft Azure

rackspace technology

NUTANIX

KVM

openstack

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

機種選定のポイント (2024年1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>

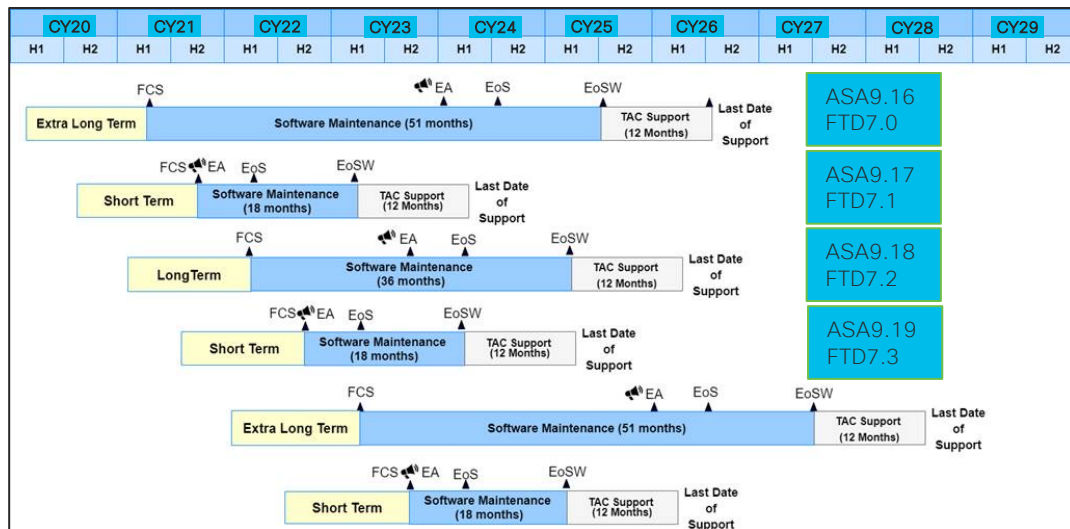
- FTD (ASA も) のバージョンの数字の小
数点1桁目が偶数ならロングタームサ
ポート、奇数ならショートタームサ
ポートとなる

FTD 7.3 → ショートタームサポート

FTD 7.2 → 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 & ASA 推奨ソフトウェアバージョン

- 2024年1月時点で一般的な推奨バージョンは FTD 7.2.5 / ASA 9.18.3 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 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

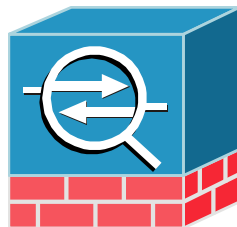
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

[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)

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

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、データベースに組み込まれた 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



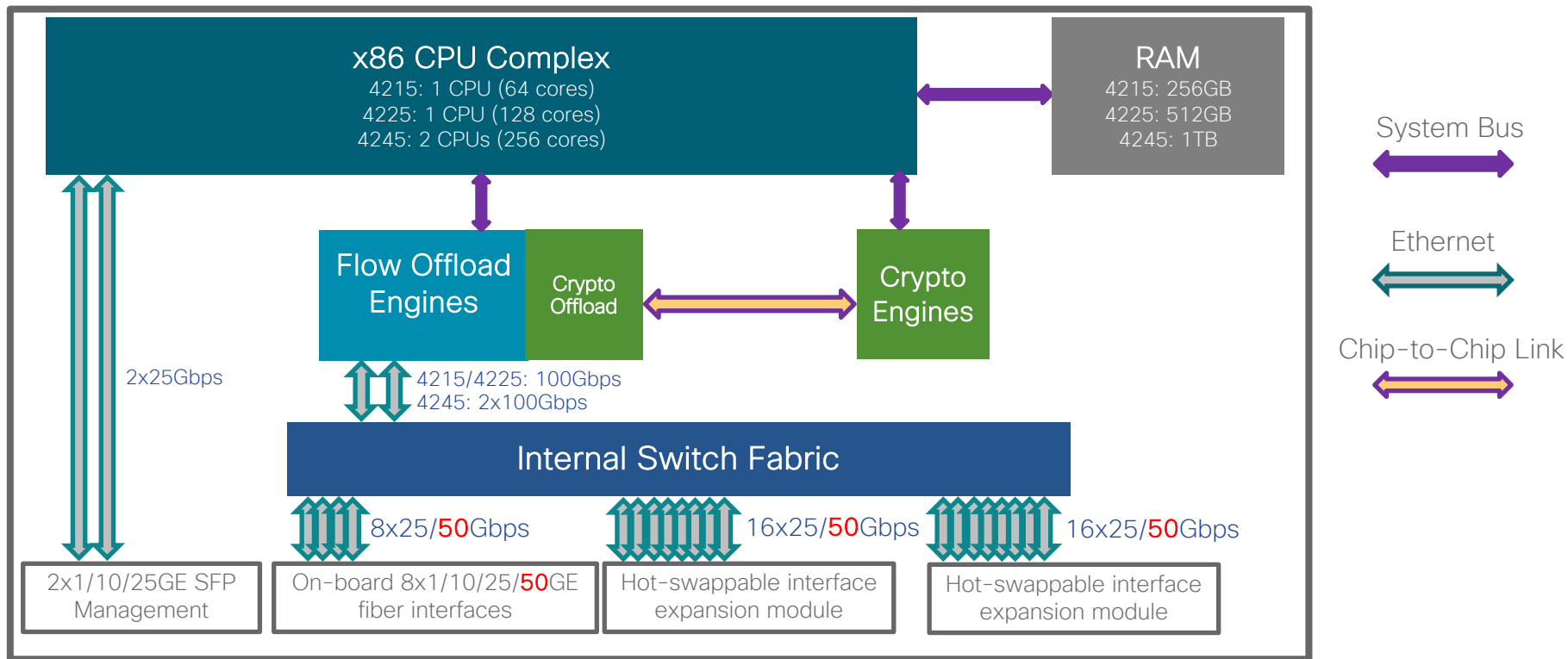
NVMe Drives

- 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)

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

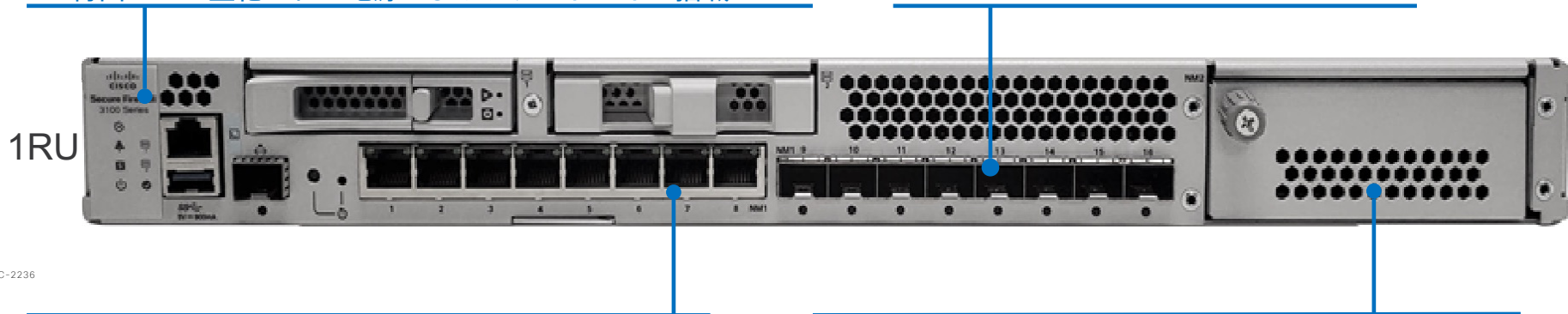
- Flow Offload や Crypto Engine の機能を持つ、データパスに

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

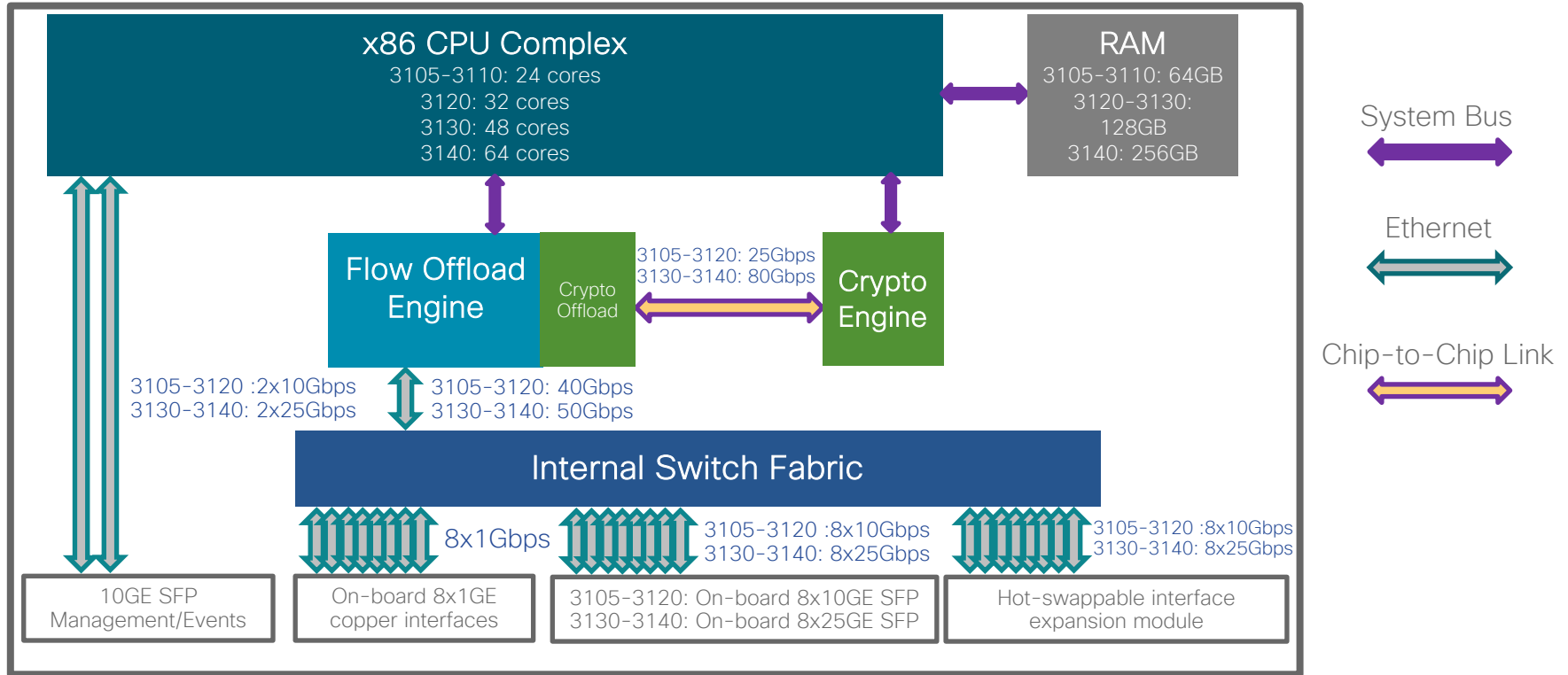
Network Module

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

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

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

FTD ライセンスの概要

FTD はスマートライセンス必須

Airgap 環境では License Reservation or Cisco Smart Software Manager On-Prem を利用

最低限必要なライセンスは？

FTD デバイス毎に必要な機能が含まれる 1,3,5年のサブスクリプションライセンス

冗長構成ではどの FTD デバイスにもライセンスが必要。2台目のサブスクリプションは半額になるバンドル型番有り

管理方法による追加費用

On Premise FMC → FMC そのものの購入が必要

cdFMC / CDO → CDO でのサブスクリプションライセンスとデバイスライセンスが必要

FDM → 購入不要

ライセンスの管理を行うデバイス・システムは？

On Premise FMC で管理時は FMC でまとめてライセンスを管理、それ以外は FTD 毎にデバイス内でライセンスを管理

どちらの場合も初期インストール後、90日間の評価ライセンスが利用可能 (Smart Software Manager への接続不要)

FTD デバイスに必要な機能のライセンス一覧

- Base (FTDv のみモデル毎に 1,3,5年のサブスクリプション、Firepower アプライアンスは無償)
AVC, Basic Firewall, Routing & Switching
- Threat (モデル毎に1,3,5年のサブスクリプション) ライセンス型番は **T**
IPS / IDS, Security Intelligence, Encrypted Visibility Engine
- Malware (モデル毎に1,3,5年のサブスクリプション) ライセンス型番は **M** or **AMP**
Malware Defense, Threat Grid (Dynamic File Analysis), ファイル保存
- URL Filtering (モデル毎に1,3,5年のサブスクリプション) ライセンス型番は **C** or **URL**
カテゴリ、reputation
- Secure Client (旧 AnyConnect)
サイト単位で Premier (旧 Apex) or Advantage (旧 Plus) ライセンスを適用 or デバイス単位で VPN-Only ライセンスを利用

FTD デバイス管理に必要なライセンス一覧

- FDM で直接管理

追加ライセンス不要

- On Premise FMC で管理

FMC Appliance → ライセンス不要 (FMC Appliance の購入が必要)

FMC Virtual → 管理デバイス数 (2,10,25,300) 毎に永続ライセンスの購入が必要 (初期の 90日間評価ライセンス有り)

- CDO (cdFMC) からの管理

テナントごとの Base License を 1,3,5年のサブスクリプションライセンスで購入

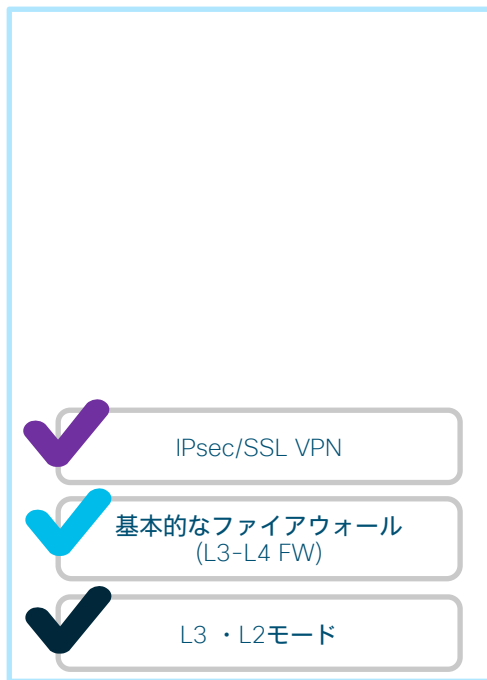
管理する FTD の数をデバイスのモデル別にそれぞれ 1,3,5年のサブスクリプションライセンスで購入

[詳細はオーダーガイド参照](#)

Firewall Threat Defense の アーキテクチャ

ASA FW, Firepower IPS, FTD の関係性

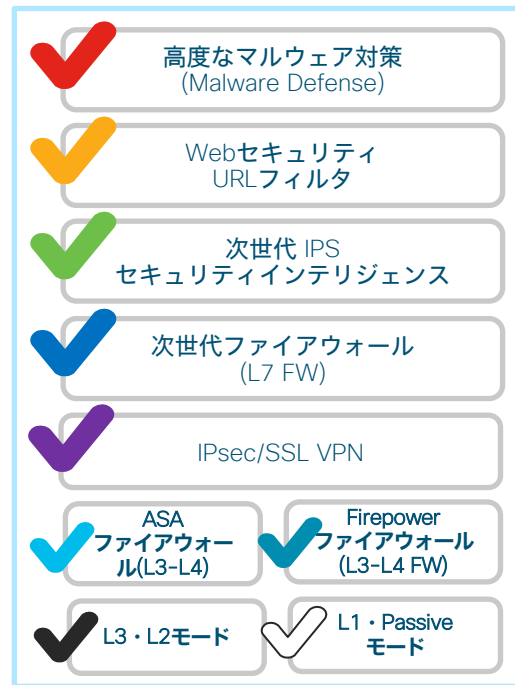
ASA Firewall



Firepower IPS



Firewall Threat Defense



FTD インターフェースモード



ASAから継承



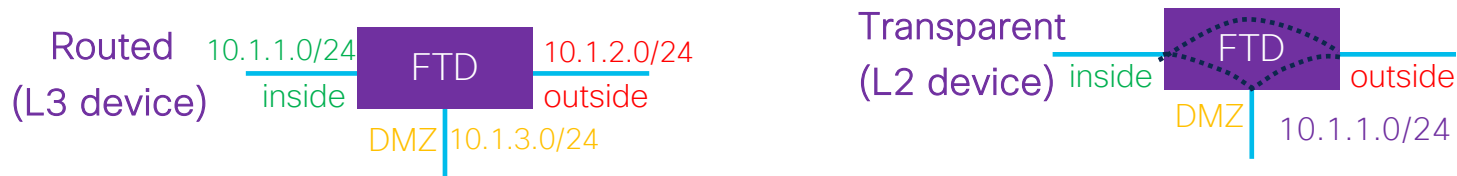
Firepowerから継承



※Inline / Inline Tapのみ、ハードウェアバイパス
モジュールにて、Fail-to-Wire 機能利用可能

FTD Firewall モードとそれぞれのインターフェイス

- FTD 新規デプロイ時にその FTD の Firewall としてのモードについて、Routed Firewall か Transparent Firewall の選択が**必須**



- Transparent Mode での BVI には IP アドレス設定が**必須**
- Routed インターフェイスと IRB (Integrated Routing and Bridging) の併用が可能



- FTD の全機能の利用が可能 (i.e. Firewall 機能と IPS 機能の両方が利用可能)

- VLAN or VxLAN ID は FTD を越える際に変更が**必須**

FTD の NGIPS インターフェイスモード

- Routed / Transparent Firewall にて未使用のインターフェイスは NGIPS モードのインターフェイスとして利用可能

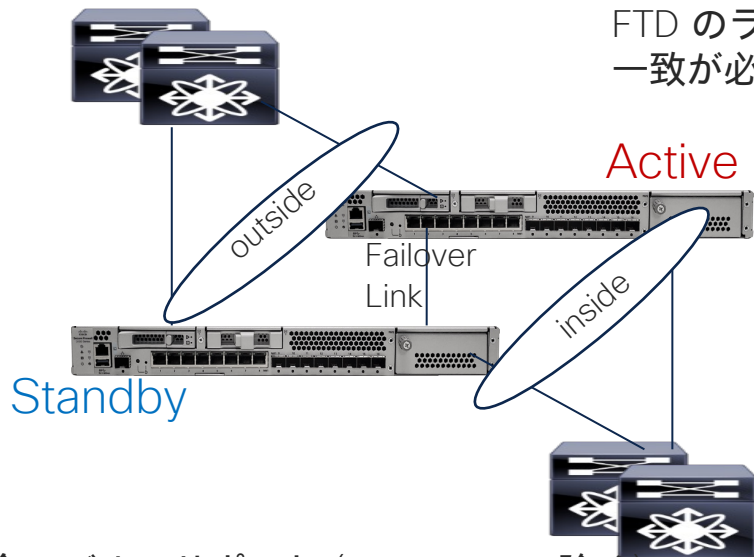


- Inline は Intelligence なケーブルとして動作 (L1 mode とも言う)
- 物理 / EtherChannel での Inline Pair が利用可能: Inline Sets は非対称通信をサポート
- VLAN と LACP はパススルー可能。Q-in-Q のパススルーは不可。
- 全ての Security Policy は有効。Inline モードではブロック可、Inline TAP と Passive モードはブロック不可
- データプレーンは HA / Clustering 時にコネクションをトラック (データプレーンでの Block は無い)
- NAT、アプリケーションインスペクション等の ASA の機能は無効
- Flow Offload も使われない

注1) FTD 7.0 より ASA と同じ仕組みの VPN Load Balancing もサポート開始

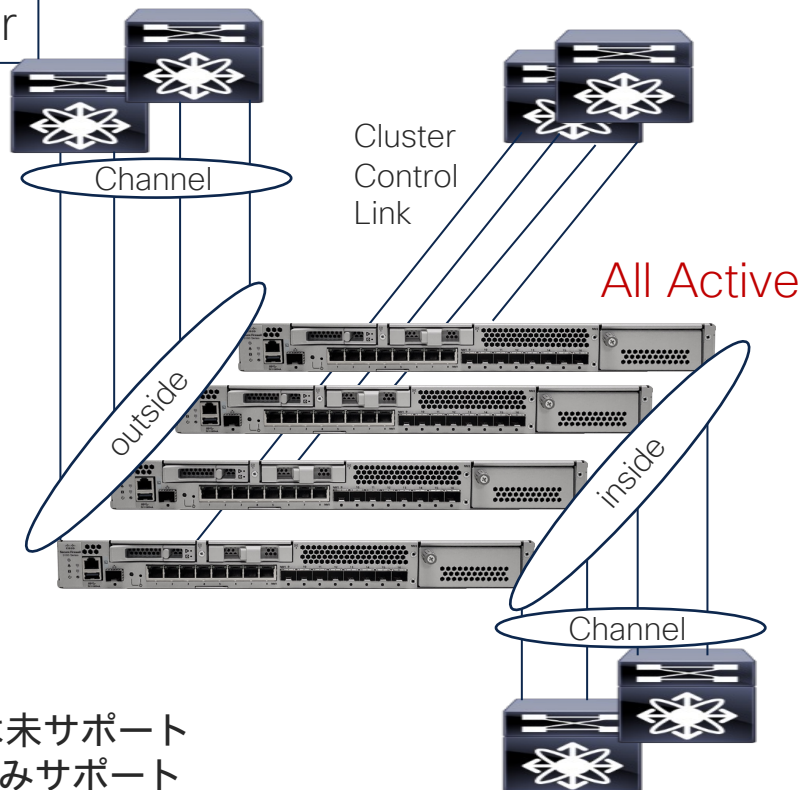
FTD の高可用性

Active - Standby



注2) どちらの構成でも
FTD のライセンスは
一致が必要

Cluster



全モデルでサポート (public cloud 除く)
FMC 管理 / FDM 管理どちらも可
同一モデル同士でペアを組む
ASA での Active - Standby と全く同じ仕組み
Routed / Transparent / Inline IPS で動作可

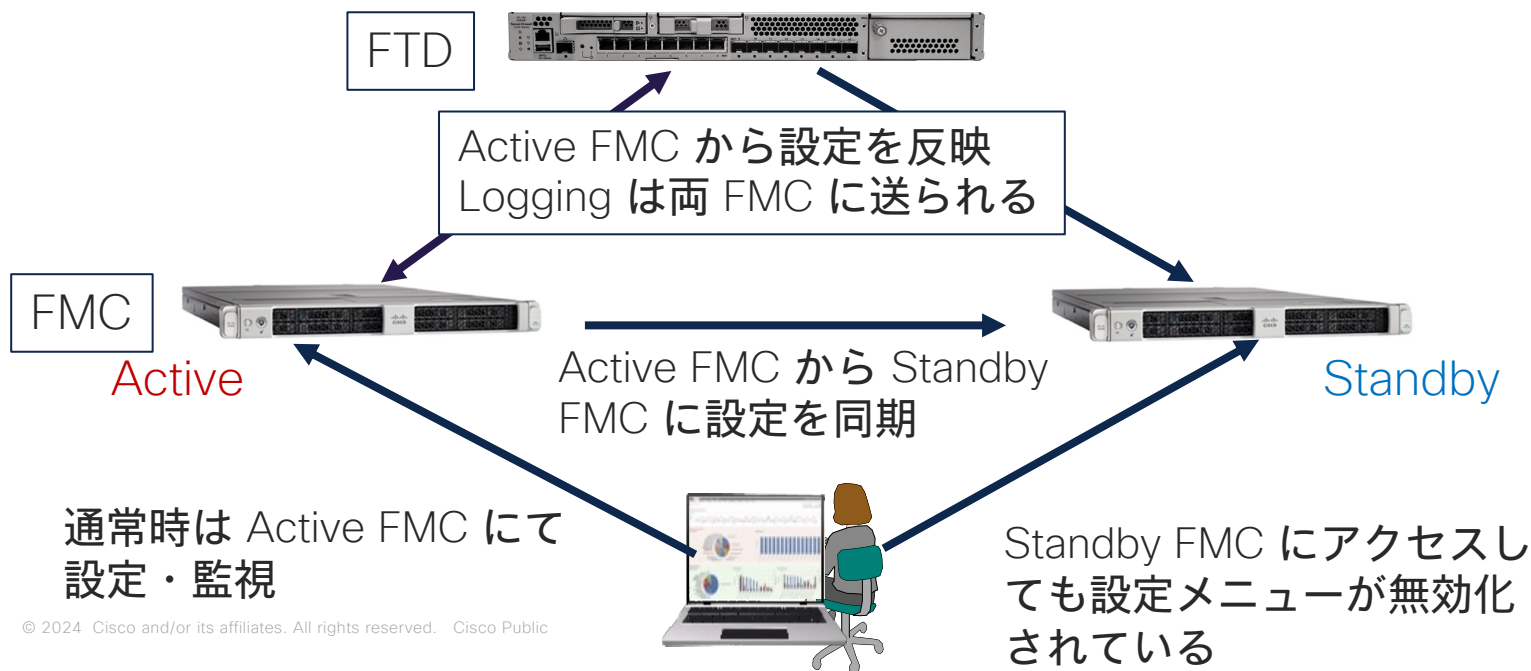
FPR1k/2k は未サポート
FMC 管理のみサポート
同一モデル or 同一インスタンスサイズでメンバーを組む
ASA での Shared Interface 利用時の Cluster と同じ仕組み
Routed / Transparent / Inline IPS で動作可

FMC (On Premise) の高可用性

FMC は Active / Standby での冗長化が可能

FMCv も version 6.7 より VMware 版のみで可能になった (FMCv2 除く)

FMC には Active / Standby 自動切り替わり機能は無く、手動で切り替える必要がある



Logging

FTD から直接出力される syslog と FMC からサブされる eStreamer がある

FMC 管理 FTD

FTD からの syslog 出力は、管理インターフェイスでもデータインターフェイスでもどちらも可

FDM 管理 FTD

SF Tunnel

FMC

eStreamer

eStreamer クライアント

互いの Management Interface
間にて TCP/8305 で通信
FTD から FMC に Event 出力

FMC が介在した
syslog (impact flag 等)

Event / System log は一時的に
FTD 内部に保存するが、保存可
能なデータ量は非常に少ない

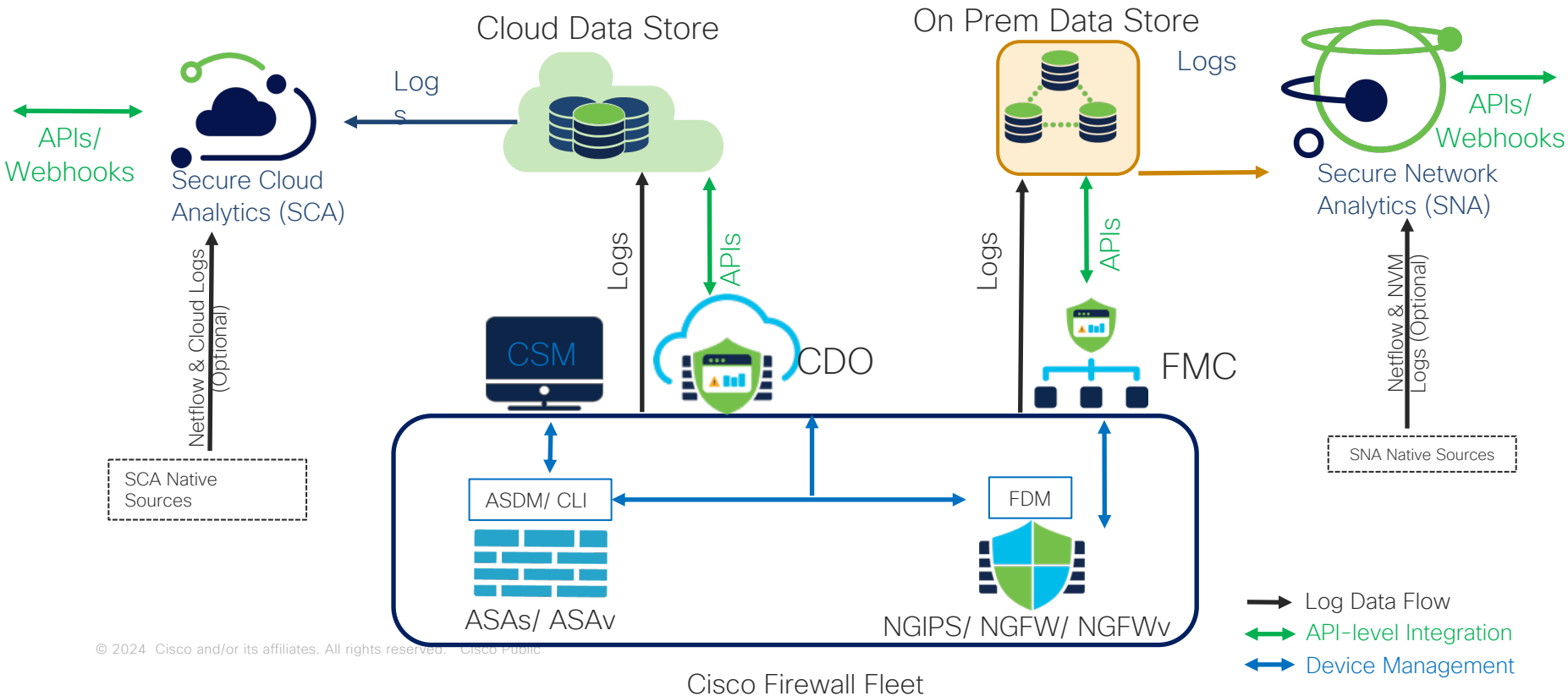
FMC は通常は
TCP/8302 で待受

注) その他、FTD から NSEL
(Netflow) でのイベント出力も可
能。要 FlexConfig

Event / System log は一時的に FMC
内部に保存するが、Event 量が多い
場合にはすぐに容量がいっぱい
になって、FIFO で破棄される

SAL (Security Analytics Logging) アーキテクチャ

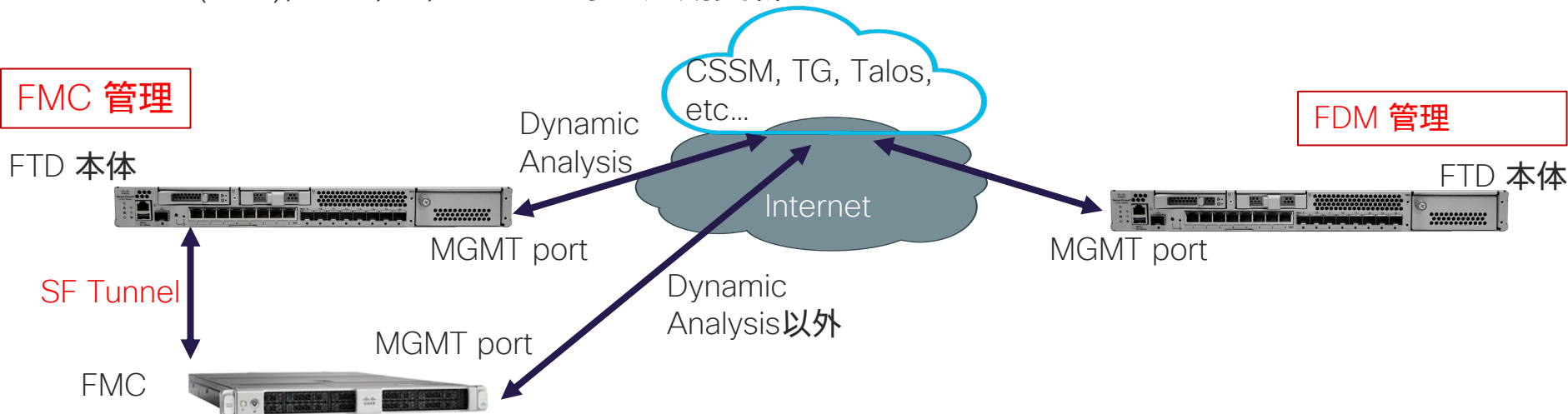
Firewall の logging をクラウド or オンプレミスに実施し、そのデータを有効活用



インターネットアクセスの必要性

FMC, FTD デバイス自身からインターネットへのアクセスが必要

- ライセンス管理のための Cisco Smart Software Manager (CSSM) へのアクセス
- Malware 機能における Cloud Lookup と Dynamic Analysis
- SRU (LSP), VDB, SI, GeoDB 等の定期更新

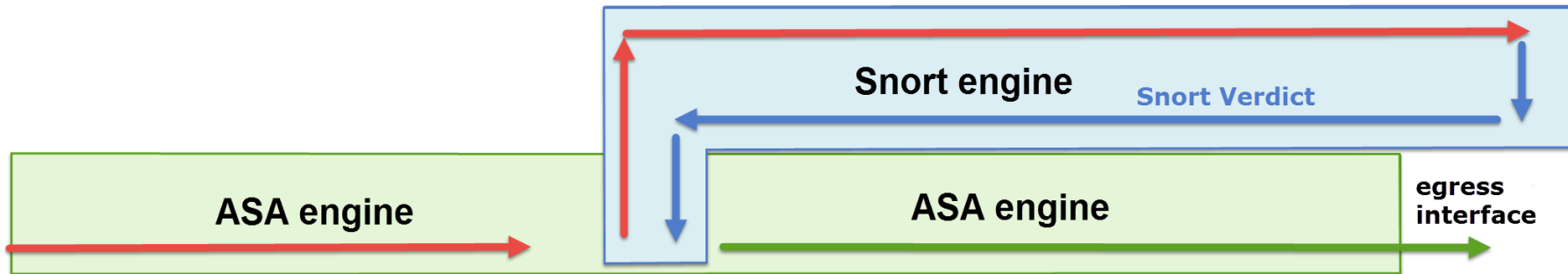


FMC 管理の場合、CSSM へのアクセスも含め、ほとんどのインターネットアクセスは FMC が実施する
ただし、Cloud の Threat Grid にファイルを送信する (Dynamic Analysis) のは FTD から行われる

本当に Air Gap 環境か？

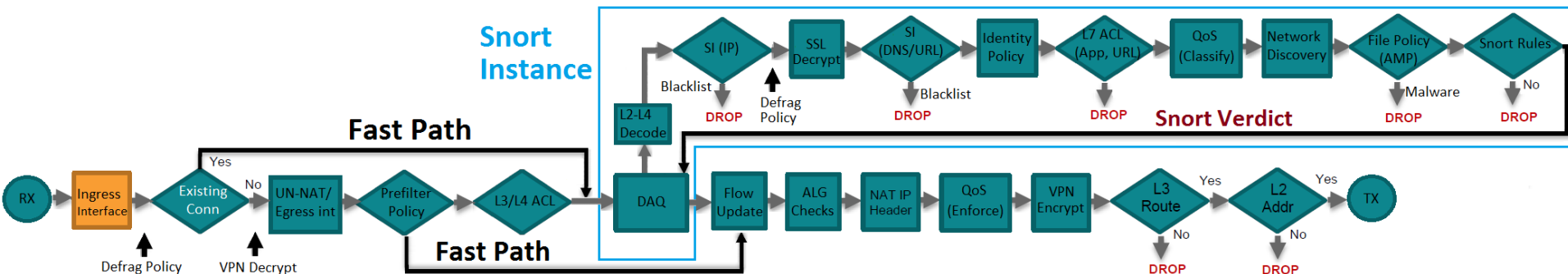
- そもそも本当に Air Gap 環境で使うのか？再度検討する必要がある
- Air Gap 環境だと、Malware Cloud Lookup / Dynamic Analysis や URL Filter, Security Intelligence 等が使えず、SRU (LSP) や Geo DB, VDB 更新も完全にマニュアルで実行する必要がある。本当にそのような環境で FTD を使うのか？
- License Reservation にしても、初期セットアップ時にオフラインでスマートアカウントに登録し、エンジニアがオフライン環境で CSSM から必要な情報入手しなくてはならない
- License Reservation のメリットは、FMC や FDM の管理インターフェイスから、定期的に CSSM にアクセスしなくても良いこと、のみ
- 「なんとなく License Reservation を申請」しないこと

FTD パケット処理の大まかなプロセス



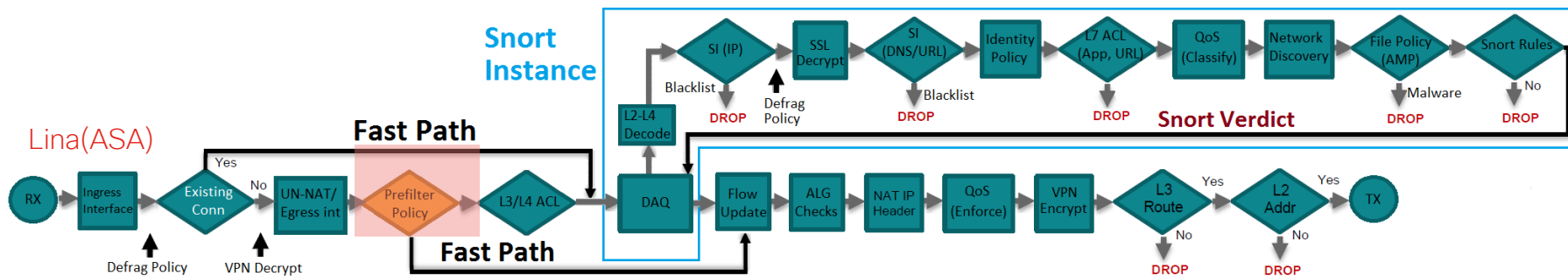
1. Ingress Interface に入ってきたパケットはまずは ASA エンジン (通称 LINA) にて処理される
 2. ポリシーに適合すれば、パケットは Snort エンジンにてインスペクションされる
 3. Snort エンジンがパケット転送の許可/破棄を決定
 4. ASA エンジンは Snort の判断に従ってパケットを転送するか破棄する
- Snort エンジンは従来の Firepower IPS のコードをベースとして動作
 - ASA エンジンは ASA Firewall 9.x のコードで動作

FTD パケット処理 詳細



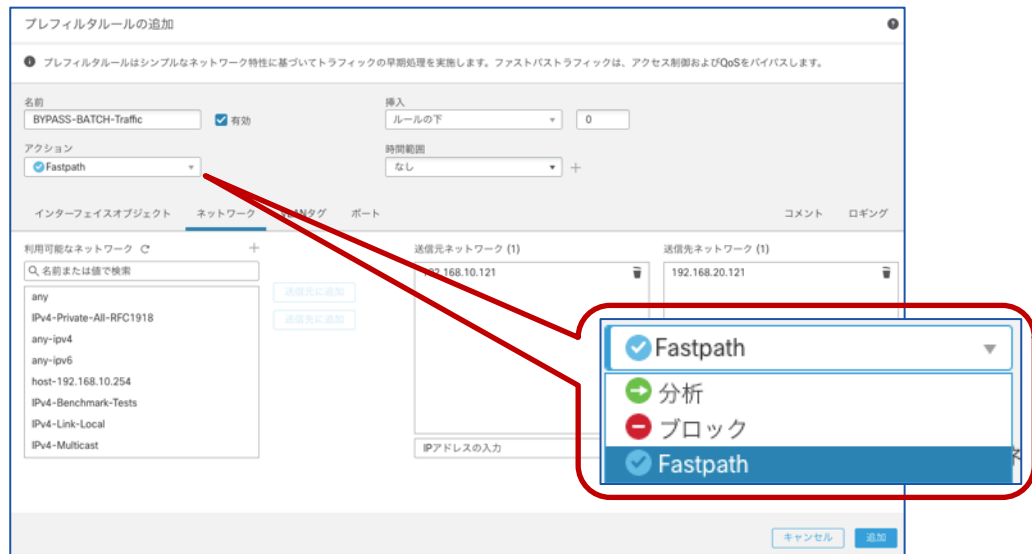
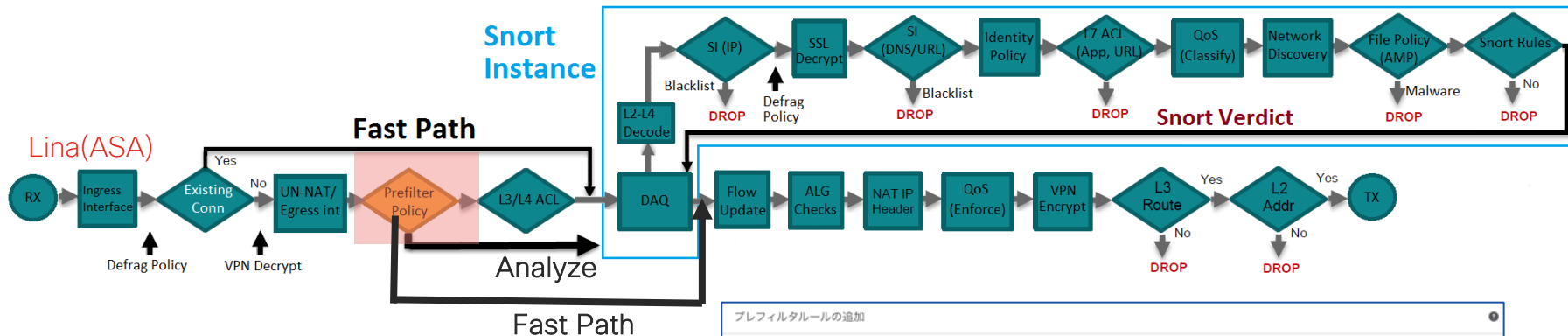
Routed / Switched(Transparent) mode: ASA + Snort フル機能
その他: ASA 一部機能 (L3-4ACL)

Prefilter ポリシーの役割



- Prefilter ポリシーは主に2つの役割を提供
 - 1. トンネル内のパケットに対するインスペクション処理
 - GRE、IP-in-IP、IPv6-in-IP、Teredo Port 3544
 - 2. Snort 処理前のアクセスコントロール
 - 監視系 / バックアップなど L7 レベルでの検査が不要な信頼された通信をバイパスする、等

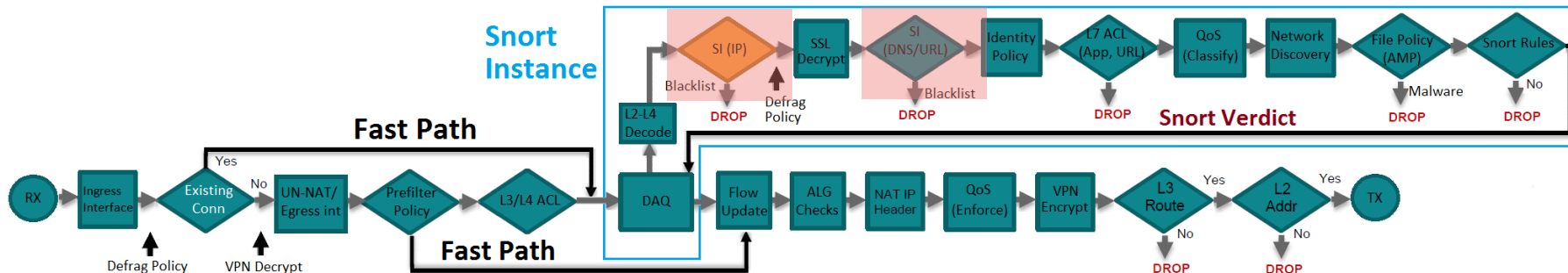
Prefilter ポリシーの役割 (続き)



- Snort 処理前のアクセスコントロール、3つのアクション

1. ブロック (Block): パケットをドロップ処理 (L4 レベルで判定できる Deny アクセスリスト など)
2. Fastpath: Snort 側へパケットを渡さずバイパス処理 (監視通信、夜間のバッチ処理 など)
3. 分析 (Analyze): Snort 側へパケットを通過処理 (デフォルト設定)

Security Intelligence (IP/URL/DNS)



Security Intelligence (IP Address / URL) :

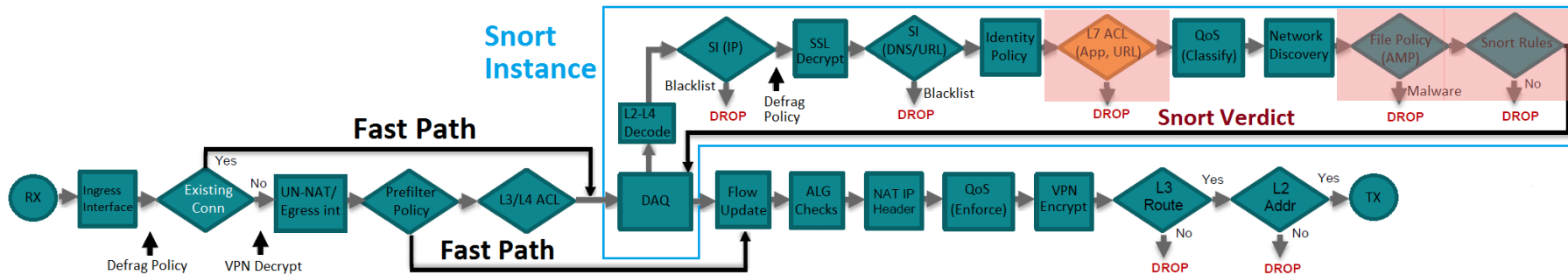
- Security Intelligence に指定された IP アドレス & URL 群への / からの通信を Blocklist or Allowlist に従って処理
- Blocklist は 手動設定 or 自動設定 (Intelligence Feed by Talos or custom)

Security Intelligence (DNS) :

- Security Intelligence に指定された DNS 群を以下の処理を実施可能
 1. Whitelist
 2. Monitor
 3. Domain Not Found (NXDOMAIN)
 4. Drop (DNSクエリー)
 5. Sinkhole (IP リダイレクト)
- Blocklist は 手動設定 or 自動設定 (Intelligence Feed by Talos or custom)



L7 ACL (Access Control Policy)



Access Control Policy:

アプリケーションコントロール、URL フィルタリング、IPS、Malware Defense を設定するポリシー
 IPS / File Policy など個別に作成したポリシーが紐づく根本となるポリシー

Firewall Management Center
 ポリシー / アクセス制御 / Policy Editor

概要 分析 ポリシー デバイス オブジェクト 統合

ACP-1
 説明を入力

新しいUIレイアウトを試す ヒットカウントの分析 保存 キャンセル

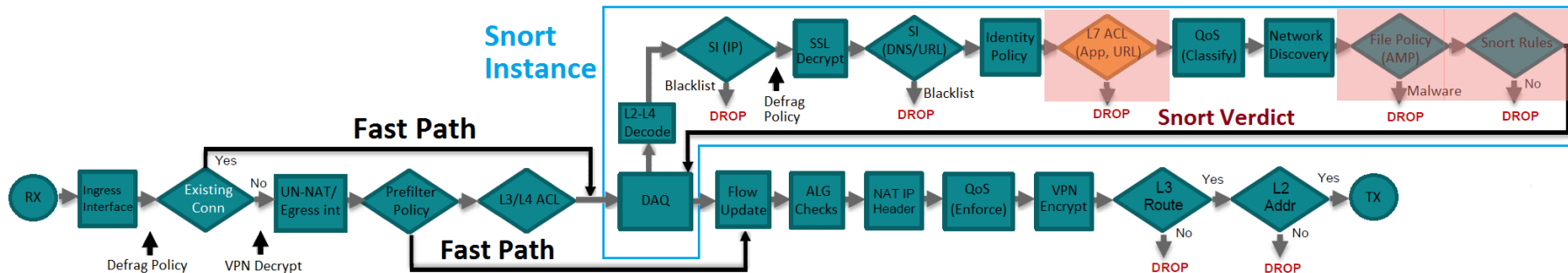
ルール セキュリティインテリジェンス HTTPレスポンス ログング ▲ 詳細

プレフィルタポリシー: Default Prefilter Policy SSLポリシー: なし 継承設定 | ポリシー割り当て(1) アイデンティティポリシー: なし

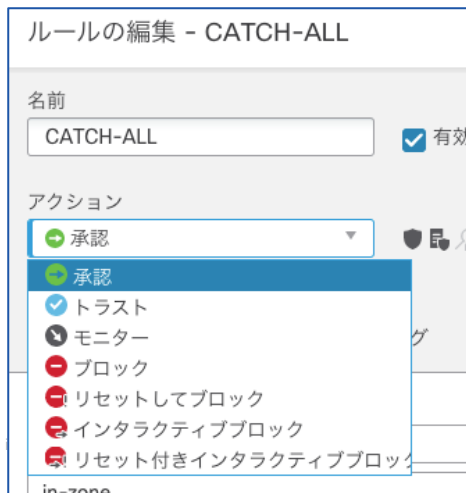
デバイスごとのフィルタ 検索ルール

#	名前	送信元ゾーン	送信先ゾーン	送信元ネットワーク	送信先ネットワーク	VLANタグ	ユーザ	アプリケーション	送信元ポート	宛先ポート	URL	送信元のダイナミック属性	宛先のダイナミック属性	アクション	監視	ヘルプ	複製	削除	リセット	0
▼ Mandatory - ACP-1 (1-2)																				
1	BLOCK-BOX-AV	すべて	すべて	すべて	すべて	すべて	すべて	Box	すべて	すべて	すべて	すべて	すべて	リセット	監視	ヘルプ	複製	削除	リセット	0
2	Block-Sports-UF	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	Sports and Rei	すべて	すべて	リセット	監視	ヘルプ	複製	削除	リセット	0
▼ Default - ACP-1 (3-3)																				
3	CATCH-ALL	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	すべて	承認	監視	ヘルプ	複製	削除	リセット	0

L7 ACL (Access Control Policy) (続き)

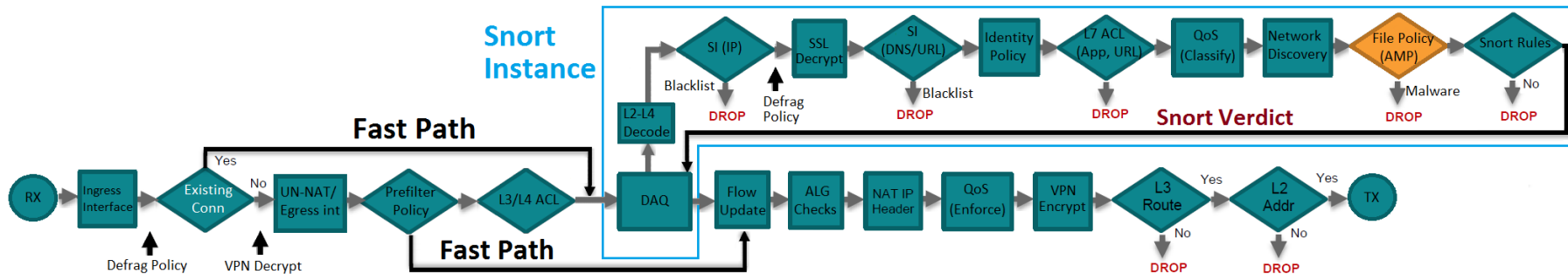


Access Control ルール、7つのアクション



1. 承認 (Allow): パケットを許可、IPS / File 検査可能
2. トラスト (Trust): パケットを信頼、IPS / File 検査スキップ
3. モニター (Monitor): パケットのログ取得、次のルールへ処理を回す
4. ブロック (Block): パケットを破棄
5. リセットしてブロック (Block with reset): パケットを破棄、送信元へリセットパケット送信
6. インタラクティブブロック (Interactive Block): 警告画面表示
7. リセット付きインタラクティブブロック (Interactive Block with reset): 警告画面表、送信元へリセットパケット送信

Malware & File Policy



- Malware & File Policy :
通過するファイルを検査するためのポリシー
クラウド上のデータベースからマルウェアを発見することや、ファイル拡張子に応じてキャプチャやブロックなど設定可能

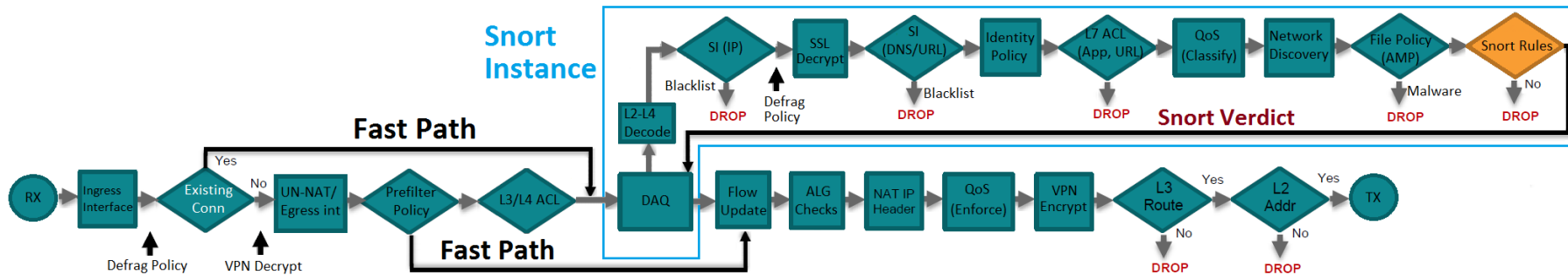
The screenshot shows the configuration for a rule named "Malwareのブロック". The configuration includes the following sections:

- アプリケーションプロトコル:** すべて
- 転送方向:** すべて
- アクション:**
 - Malwareのブロック
 - MSEXE向け SPERO 分析
 - ダイナミック分析
 - 容量処理
 - ローカルMalware分析
 - 接続をリセットする
- ファイルの保存:**
 - Malware
 - 不明
 - クリーン
 - カスタム
- ファイルタイプカテゴリ:**
 - Office Documents (18)
 - Archive (19)
 - Multimedia (4)
 - Executables (10)
 - PDF files (1)
 - Encoded (0)
 - Graphics (1)
- ファイルタイプ:**
 - 7Z (7-Zip compressed file)
 - ACCDB (Microsoft Access 20...)
 - ALZ (Archive file for Microsof...)
 - ARJ (Compressed archive file)
 - BINARY_DATA (Universal Bin...)
 - RINHEX (Macintosh RinHex 4 ...)
- 選択されたファイルカテゴリとタイプ:**
 - カテゴリ: Local Malware Anal...
 - カテゴリ: Dynamic Analysis C...
 - カテゴリ: System files
 - カテゴリ: Graphics
 - カテゴリ: Encoded
 - カテゴリ: PDF files
 - カテゴリ: Executables

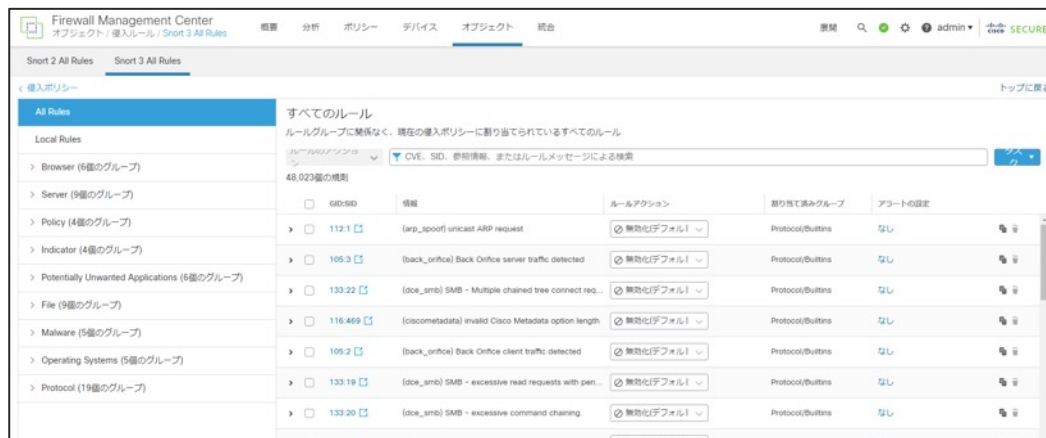
A dropdown menu is open, showing the following options:

- Malwareのブロック
- ファイルの検知
- ファイルのブロック
- Malwareのクラウド検索
- Malwareのブロック

Intrusion Policy



- Intrusion Policy :
Snort IPS を用いたパケット検査
ポリシー
推奨ルール、カスタムルール、
独自に作成したルールなど設定
が可能



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

- Cisco Secure Firewall への cisco.comでのショートカット
<http://cisco.com/go/ngfw>
- 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>
- [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 (ドキュメントまとめサイト)
<https://secure.cisco.com/secure-firewall>

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
NetSec Community
SECURE
FIREWALL

Firepower 1000 Series
CISCO

Cisco Secure Firewall
チャンネル登録者数 4340人

登録済み

ホーム 動画 再生リスト コミュニティ チャンネル 概要

Introducing the Cisco Secure 3100 Series Firewall!
Cisco Secure Firewall • 375 回視聴 • 3 週間前
Interested to learn more about what the 3100 series has to offer? Find additional details here!
<https://www.cisco.com/c/en/us/products/security/secure-firewall-3100-series/index.html> Ask Questions...

1:37

Cisco Secure Firewall 7.2 Release ▶ すべて再生

RELEASE 7.2 OVERVIEW 23:05

TRANSPORT LAYER SECURITY TLS - 1.3 SUPPORT 4:36

VIRTUAL FIREWALL CLUSTERING 15:01

EIGRP WITH FMC 5:42

PBR WITH PATH MONITORING 7:27

ENCRYPTED VISIBILITY ENGINE 16:50

Cisco Secure Firewall Release 7.2 - Overview

Cisco Secure Firewall 7.2 Release - TLS 1.3 Support

Cisco Secure Firewall 7.2 Release - Virtual Firewall...

Cisco Secure Firewall 7.2 Release - EIGRP with Firewa...

Cisco Secure Firewall 7.2 Release - Policy Based...

Cisco Secure Firewall Release 7.2 - Encrypted...

多くの動画で日本語への自動翻訳が有効

