



30分でわかる Cisco NGFW (次世代ファイアウォール)

2020年11月5日

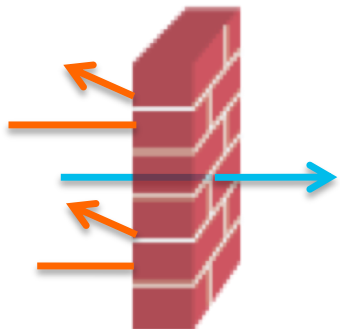
シスコシステムズ合同会社

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)

現在の脅威対策にこのような課題はありませんか？

- 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
- 次世代ファイアウォールは導入しているが、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



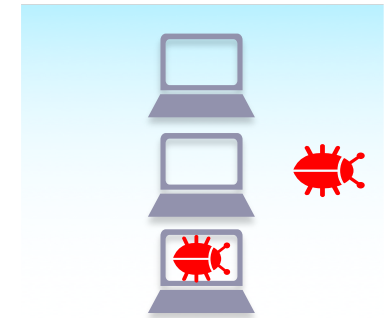
Web アプリケーション、ユーザ、
脅威の可視化

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

Firepower シリーズ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
- ✓ スレッドグリッドサンドボックス



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	0 (No Code) / icmp	Unknown (Unknown)	0	PROTOCOL-ICMP Unk
2020-07-30 15:38:19	low	3	↓	146.112.41.2	NLD 192.168.20.102	443 (https) / tcp	49850 / 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	80 (http) / tcp	Unknown (Unknown)	0	SERVER-OTHER Nove

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

表示 [コンテキストエクスプローラ](#) | [接続イベント](#) | [侵入イベント](#) | [ファイアウォール](#) | [Malwareイベント](#)

ホストのスクリーンショット

ホ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

▼ 侵入の痕跡 (1)

侵入の痕跡

User History

Users

Discovered Identities\setsuko.overton (LDAP)

armando zuniga (dcloud.cisco.com)\azuniga, LDAP

ユーザ履歴

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	ssh	
tcp	1		

脆弱性 (1022)

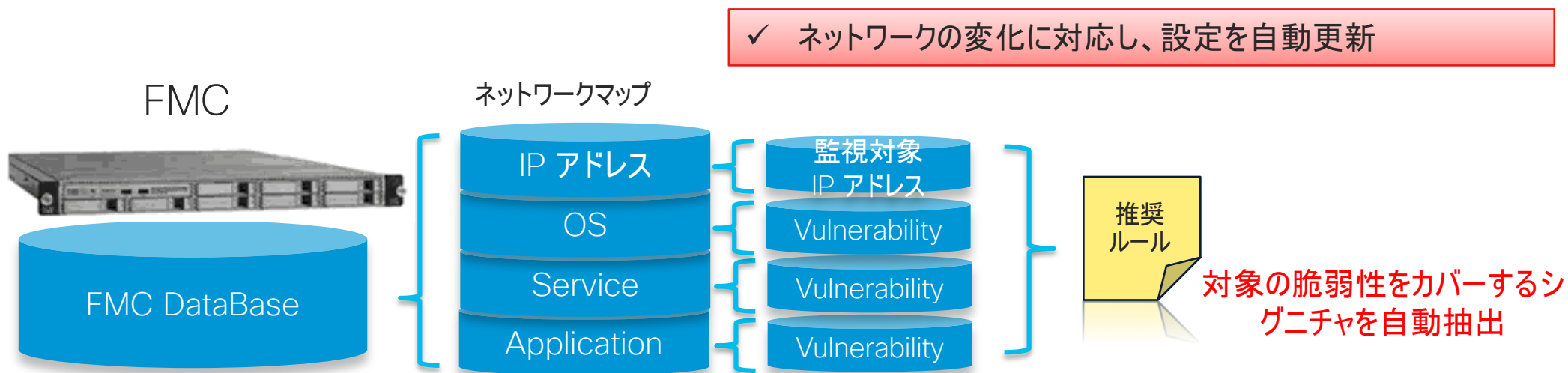
該当脆弱性リスト

名前	ポート
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



- ✓ 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 OS、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

自動チューニングとインパクト解析

自動チューニング
ネットワーク環境を学習し、
最適な推奨設定を自動生成

一般的な侵入検知機器 (IPS) の
運用者が抱える問題

環境に合わせて設定を調整したいが、運用が大変...

沢山のログが出るが、本当に重要なものがわからない...

Firepower Management Center
ポリシー / アクセス制御 / ポリシーの編集

Firepower推奨ルール構成

Firepowerは1ホストに対して23259ルール状態設定を推奨しています

- 360個のルールをイベントを生成するよう設定します
- ⊙ 8473個のルールをドロップおよびイベントを生成するよう設定します
- 14426個のルールを無効にするよう設定します

ポリシーは生成された推奨項目を使用していません。クリックすると推奨項目を変更できます
最終生成日: 2020 Aug 3 18:14:38

ポリシーレポートで推奨とルール状態の間のすべての差を含む

推奨項目をアップデート 推奨項目を使用する



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

Intrusion Events

Last 180 days

Category	Total
①	141
②	0
③	110
④	29

Impact 1 Events by Application Protocol

Application	Impact 1 Events
HTTP	77
DNS	21
HTTPS	7
FTP	4
Twitter	2

Dropped Intrusion Events

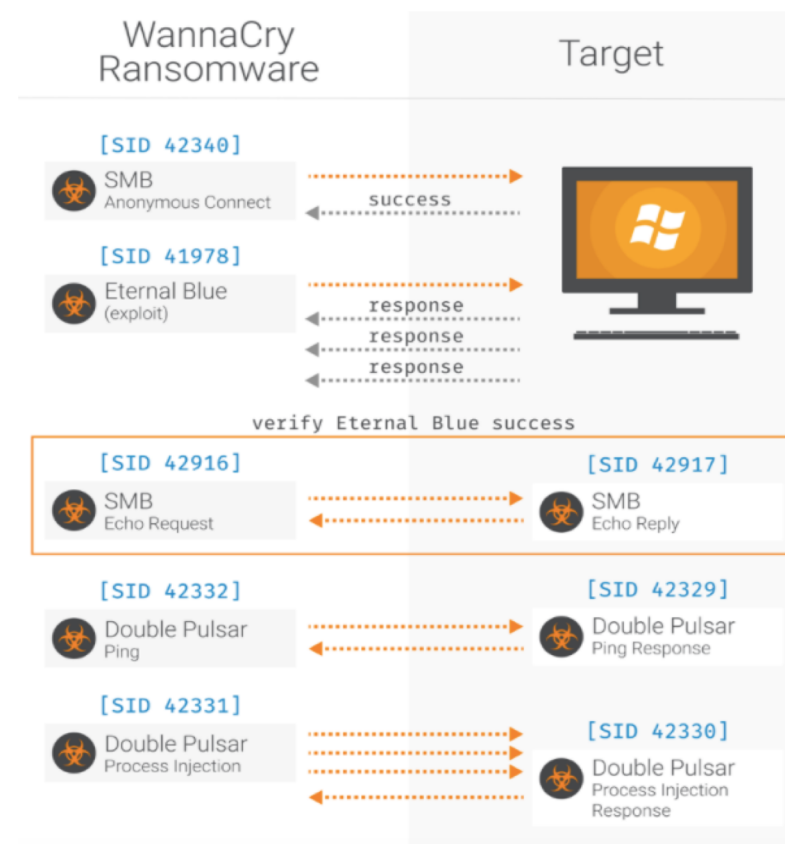
Classification	Count
A Network Trojan was Detected	119
Attempted Administrator Privilege Gain	13
Attempted Information Leak	6
Attempted User Privilege Gain	5

Impact 2 Events by Application Protocol

Application	Impact 2 Events
NetBIOS-ssn (SMB)	21
FTP	7
HTTP	1

Snort IPS ルール

- 単なる脆弱性を突く攻撃だけでなく一連の攻撃プロセスに沿った豊富な検知ルール
 - ✓ 外部だけでなく内部通信からも脅威検出
- Exploit-Kit / Malware-Backdoor / MS 脆弱性情報などカテゴリーごとに Snort IPS ルール分類
- Snort 言語と正規表現により内容確認可能
 - ✓ 全ルールの検知ロジック開示が可能
- 推奨ルール、自動チューニング
 - ✓ Cisco Talos 推奨ルール利用、もしくはホストプロファイル から学習した脆弱性情報に基いてチューニング

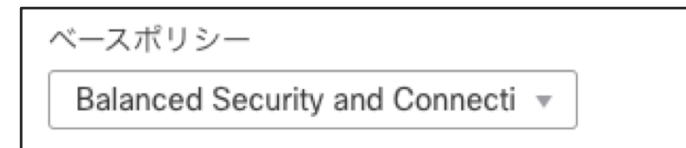


```
rule alert udp $HOME_NET any -> any 53 (msg:"APP-DETECT 12P DNS request attempt"; flow:to_server; byte_test:1,!&,0xF8,2; content:"|03|b32|03|i2p|00|"; fast_pattern:only; metadata:policy max-detect-ips drop, service dns; reference:url,geti2p.net; classtype:misc-activity; sid:37062; rev:2; gid:1; )
```


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 ↑ 防御優先
- Balanced
- Connectivity Over Security ↓ 通信優先

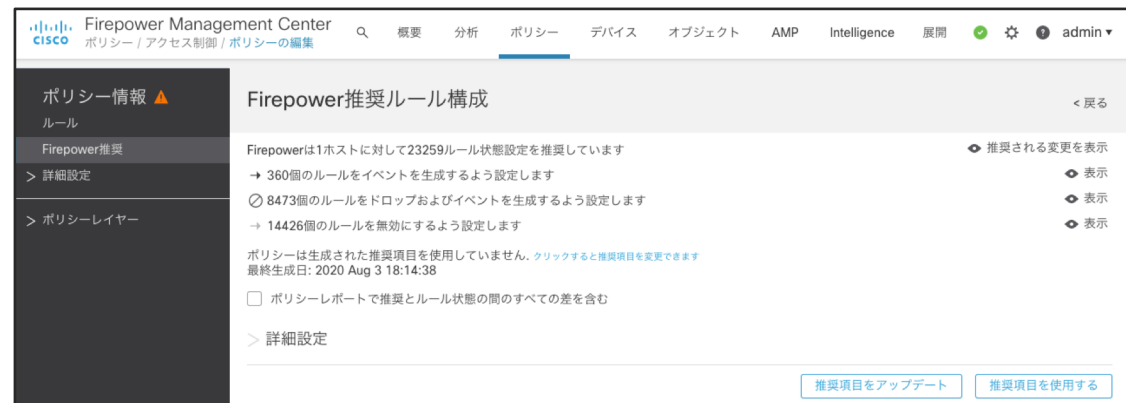


- 自動チューニングの利用

- FMC が推奨設定を生成
- ベースポリシーを上書き

- カスタムチューニング

- ベースポリシーおよび推奨設定を上書き



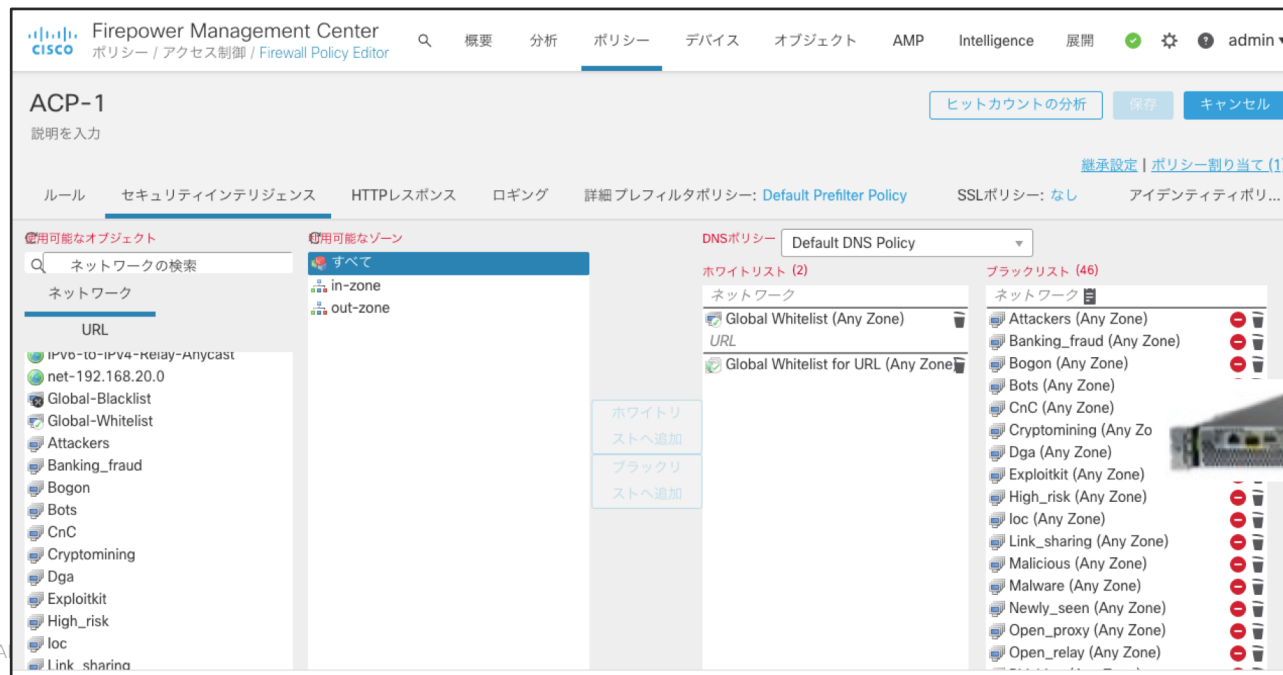
Security Intelligence 脅威情報フィルタ



- Cisco Collective Security Intelligence 提供のブラックリスト 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)
- 既知のブラックリスト宛て 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



ジオロケーション

- IP アドレスと国や地域を紐づけたジオロケーションデータベース
- IPS、アプリケーション制御、ファイルポリシー等の任意の設定と組み合わせて利用可

The screenshot displays the 'ルール追加' (Add Rule) configuration page. The rule name is 'Monitoring from some countries', which is active (有効). It is assigned to 'ルールの下' (Under Rule) with a priority of 2. The action is set to '承認' (Allow). The time range is 'なし' (None).

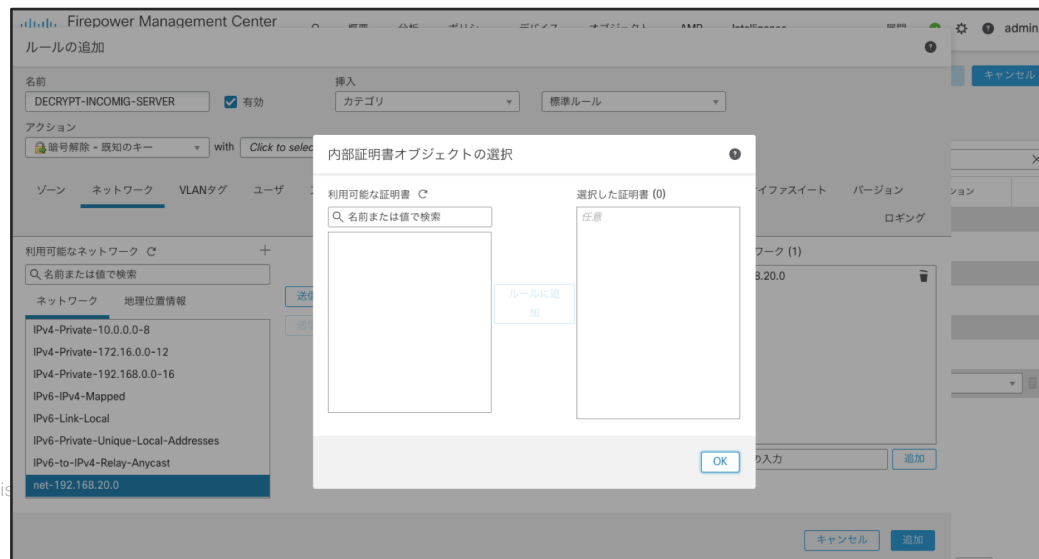
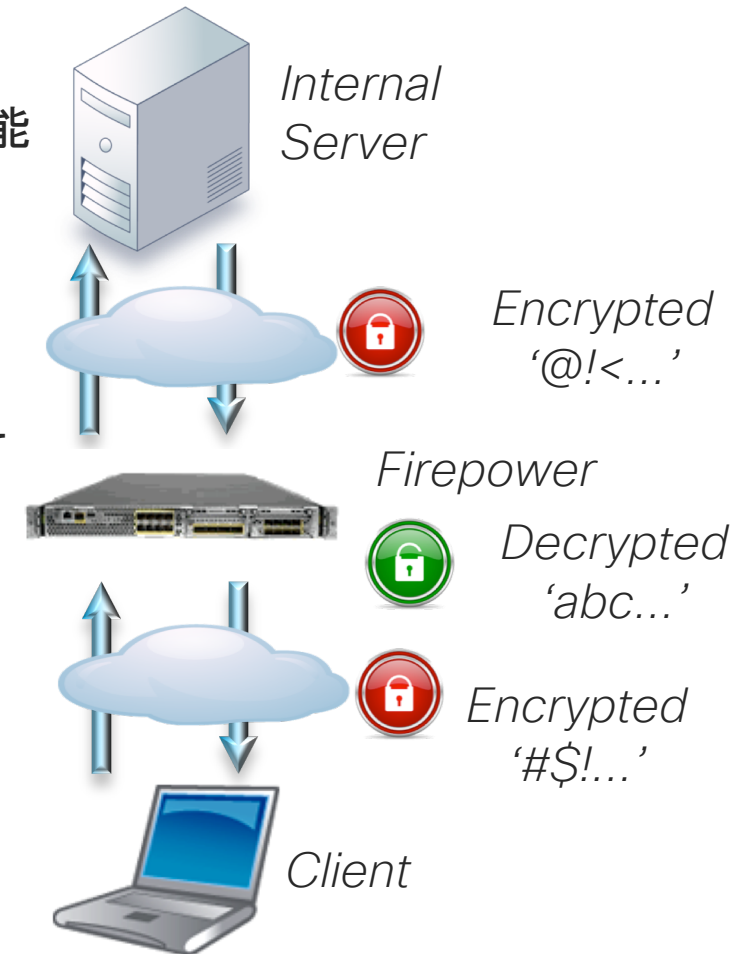
The configuration is divided into three main sections:

- 利用可能なネットワーク (Available Networks):** A search bar is present. Under the '地理位置情報' (Geographic Information) tab, a list of regions is shown: Africa (58 countries), Antarctica (3 countries), and Asia (50 countries). Under the 'Asia' section, several countries are listed: Afghanistan, Armenia, Azerbaijan, Bahrain, and Bangladesh. There are buttons to '送信元ネットワークに追加' (Add to Source Network) and '送信先に追加' (Add to Destination).
- 送信元ネットワーク (Source Networks):** Labeled '(3)', it contains 'China', 'United States', and 'Russian Federation'. Each entry has a trash icon for removal. There is an input field for 'IPアドレスの入力' (IP Address Input) and an '追加' (Add) button.
- 送信先ネットワーク (Destination Networks):** Labeled '(0)', it is currently empty and labeled '任意' (Optional). There is an input field for 'IPアドレスの入力' (IP Address Input) and an '追加' (Add) button.

Navigation tabs at the top include: ゾーン, ネットワーク, VLANタグ, ユーザ, アプリケーション, ポート, URL, SGT/ISE属性, 検閲, ロギング, コメント.

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 ネイティブには未対応、TLS 1.2 にダウングレードしてのインスペクションは可能



AMP4N (Advanced Malware Protection for Network) 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

属性	値	First Seen	Last Seen
ファイルSHA256	275a021b...f651fd0f	2020-08-03 18:51:51 オン	2020-08-03 18:53:54 オン
ファイル名	eicar.com	192.168.10.101	192.168.10.101
File Size (KB)	0.0664		14
ファイルタイプ	EICAR		2ホスト
File Category	Executables		送信者数: 1 → 受信者数: 1
Current Disposition	Malware		
Threat Score	Very High		
検知名	EICAR		

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	アクション	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	Malware Block	HTTP	Chrome	
2020-08-03 18:53:54	転送	192.168.10.101	192.168.20.102	EICAR	eicar.com	EICAR	Malware Block	HTTP	Chrome	

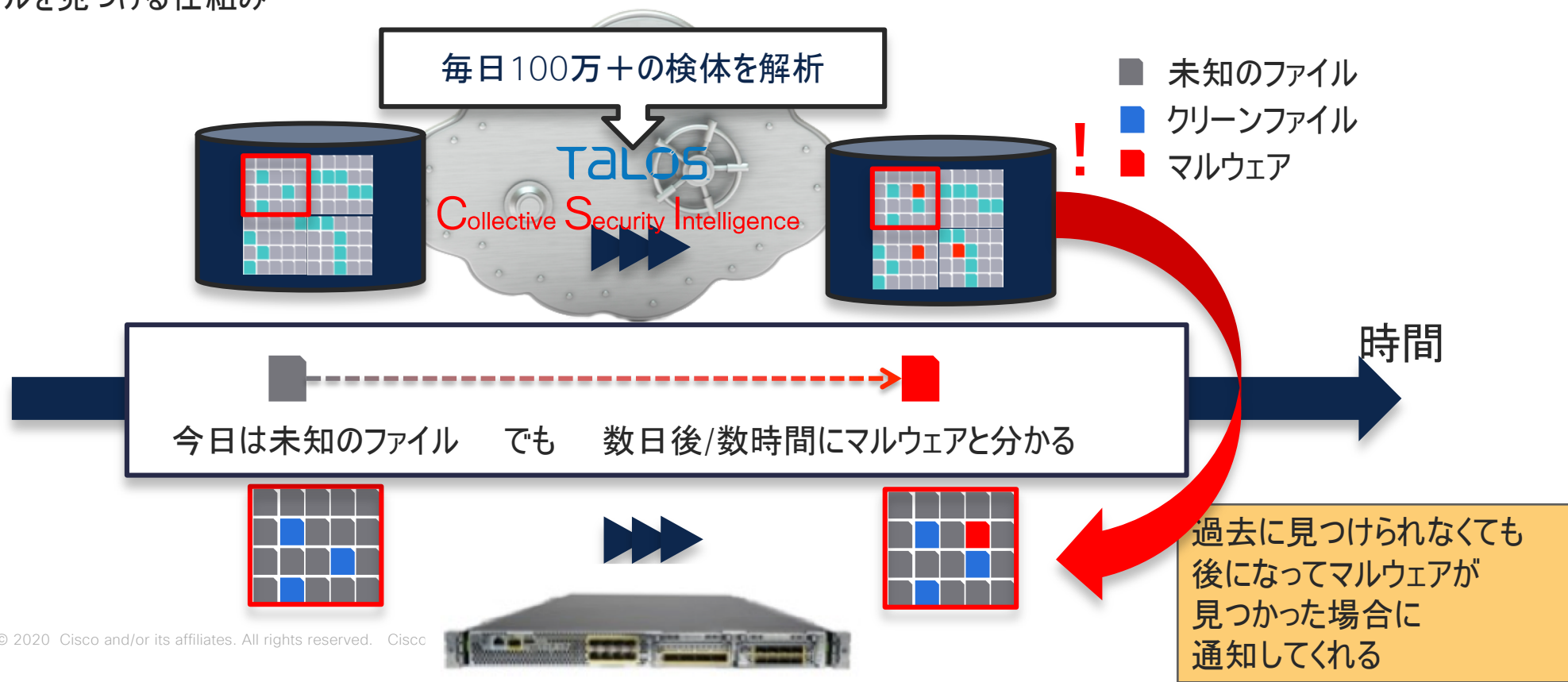
② 解析情報(サンドボックス含む)と連携

④ 端末の特定

③ ネットワーク上での拡散状況を可視化

AMP4N (Advanced Malware Protection for Network) 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

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	ウェブアプリケ	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 ...

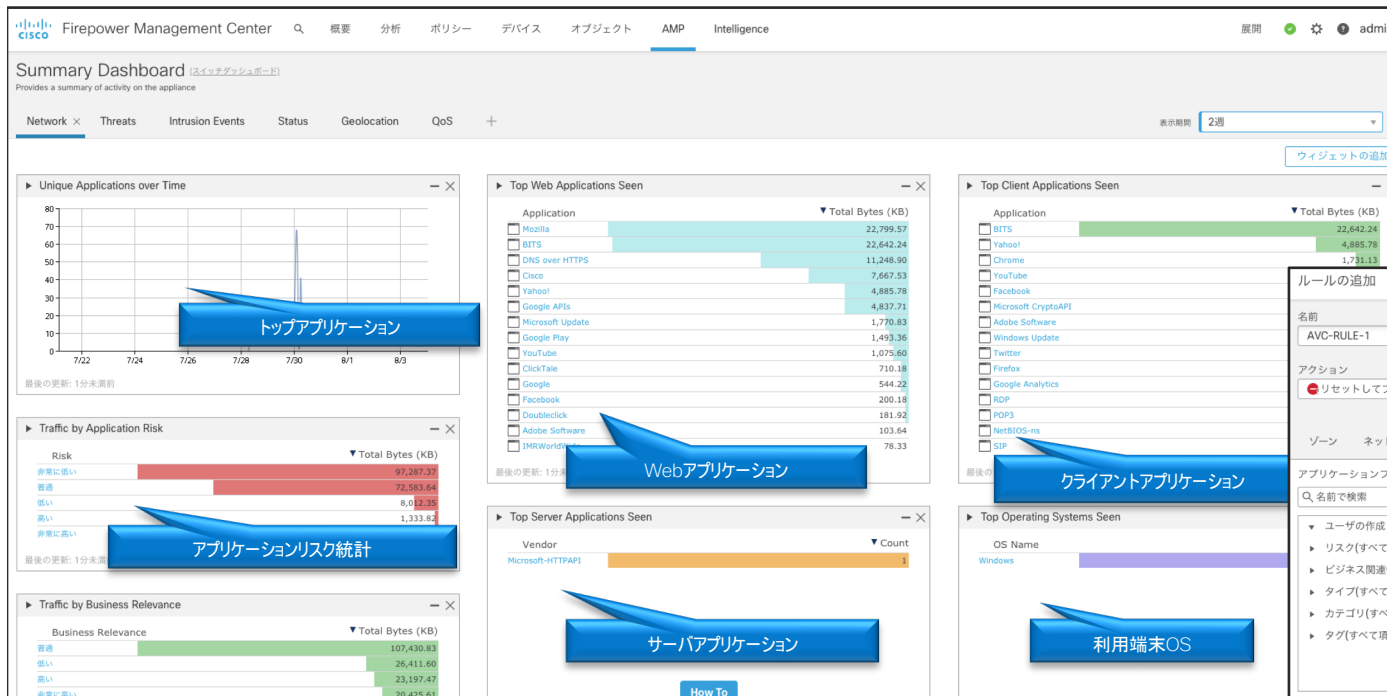
このケースでは最初の時点では既存セキュリティをすり抜けてしまったマルウェアを、1分後にリコールで検知している

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

利用されている Web アプリケーション、クライアントアプリケーション、サーバアプリケーション、
利用量、リスク統計から、問題点を的確に捉え、アプリケーション制限を実施し、リスクを軽減することが可能

3,500 以上のアプリケーションから、利用状況を
チェック

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



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

5292017 ネットワーク リスクレポート

I. 概要

シスコは、シスコシステムズ: eCloudが高リスクの状態にあると判断しました。その理由は、ビジネスとの関連性は低いものの、会社にとってリスクになる可能性があるアプリケーションを使用しているためです。これらのアプリケーションは、ネットワークを攻撃に対して脆弱なままにしたり、マルウェアをインストールし、帯域幅を消費したがる可能性があります。

評価期間: Sat Apr 29 2017 04:23:53~Mon May 29 2017 04:23:53

リスクのあるアプリケーション 9	リスクのあるユーザー 18	高帯域幅アプリケーション 1
暗号化アプリケーション 9	セキュリティ回避機能を持つアプリケーション 2	危険な Web ブラウザ 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	使用中のアプリケーション	転送されるファイルタイプ

推奨

シスコは、シスコシステムズ: eCloudがアプリケーション制御とURLフィルタリングを備えたCisco Firepowerアプリケーション/NICの導入を促して次のことをお勧めします。

- アプリケーション攻撃の出現を減らす
- アプリケーション、帯域幅、URLアクセス、およびアクティブユーザーポリシーをきめ細かく制御する
- モバイルデバイスやNICのリスクを含むネットワークのリスクと使用状況を可視化する

アタックレポート

5292017 攻撃リポート

I. 概要

シスコはシスコシステムズ: eCloudが高リスクの状態にあると判断しました。その理由は、悪質なホストを標的とした攻撃がネットワーク上で検出されたからです。リスクを軽減するためには、これらの攻撃とホストをさらに調査する必要があります。

評価期間: Sat Apr 29 2017 04:24:10~Mon May 29 2017 04:24:10

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

関連の攻撃によりもたらされるリスク

分類	カウント
Potentially Bad Traffic	9,884
Attempted Information Leak	8,960
Unknown Traffic	5,889
Misc Activity	2,257
Information Leak	1,961

シスコは、シスコシステムズ: eCloudがCisco Firepowerアプリケーションを導入して次を行うことをお勧めします。

- ネットワーク攻撃のリスクに対する継続的な可視性を確立する
- このリスクの発生を軽減するために自動化された制御を実施する

マルウェアレポート

5292017 高度なマルウェアリポート

I. 概要

シスコは、シスコシステムズ: eCloudが別の異なるマルウェアファミリーによる攻撃を受けており、高いリスクにあると判断しました。評価期間の30日の間、Cisco Advanced Malware Protection (AMP)が導入されました。このレポートは、この期間にネットワークで検出された記録を示すものです。

評価期間: Sat Apr 29 2017 04:24:27~Mon May 29 2017 04:24:27

マルウェアを検出 36	IOCを示しているホスト 19	感染プロトコル 2
CNCサーバに接続されているホスト 0	マルウェアの送信 22	マルウェアのURL 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者: 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	台の固有のホスト	人のユーザー	台のデバイス

シスコは、Advanced Malware Protectionを導入して次を行うことをお勧めします。

- 高度なマルウェアの継続的な可視性を確立する
- このリスクを軽減するために既存の制御を強化する

FTD の市場評価

2018年に続き、2019年の Gartner Magic Quadrant で、ネットワーク向けファイアウォール分野のリーダーにシスコが選出

さらに、2020年の Forrester Wave で、エンタープライズ ファイアウォール分野のリーダーにシスコが選出

詳しくは以下の2つの記事を参照

<https://gblogs.cisco.com/jp/2019/10/cisco-named-a-leader-in-the-2019-gartner-magic-quadrant-for-network-firewalls/>

<https://gblogs.cisco.com/jp/2020/08/cisco-named-a-leader-in-the-2020-forrester-wave-for-enterprise-firewalls/>

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Japan Blog > セキュリティ

セキュリティ

2019 年度の Gartner Magic Quadrant で、ネットワーク向けファイアウォール分野のリーダーにシスコが選出される

小林 達哉
2019年10月4日

この記事は、シスコのセキュリティデバイスプレジデント兼ジェネラル、*Geer Rittenhouse* によるブログ「*Cisco Named a Leader in the 2019 Gartner Magic Quadrant for Network Firewalls*」(2019/9/19) の抄訳です。

デジタル変革の中核をなすのはネットワークです。そのネットワークは、しかしネットワークが進化し続ける中で、シスコにとっての使命は、ポリシーの統合と脅威の可視化を実現するネットワークセキュリティを提供することです。この使命を果たすために、シスコは、

Cisco Japan Blog > セキュリティ

セキュリティ

エンタープライズ ファイアウォール分野の Forrester Wave 2020 年版でシスコがリーダーに選出

小林 達哉
2020年8月25日

この記事は、*Network, Cloud and Workload Security* の Senior Director Product Management 担当である *Chandrodaya Prasad* によるブログ「*Cisco Named a Leader in the 2020 Forrester Wave for Enterprise Firewalls*」(2020/8/11) の抄訳です。

『The Forrester Wave™: Enterprise Firewalls, Q3 2020』をダウンロードしてご覧ください

組織のセキュリティ体制の根幹は、長らくファイアウォールが支えてきました。しかし、単一のネットワーク制御ポイントで対応するという旧来の考え方は、もはや通用しなくなっています。アプリケーションとデータがクラウドに移行し、ユーザがあらゆる場所で業務をするようになったためです。組織は、各種の物理アプライアンスと仮想アプライアンスを追加することで、従来型ファイアウォールの強化を進めています。これらはネットワークに組み込まれる場合もあれば、サービスとして提供される場合もあります。ホストベースの場合もあれば、パブリッククラウドの環境に制御機能として直接実装される場合もあります。

Cisco Firepower シリーズ提供形態

- Firepower NGIPS / Firepower **単独アプライアンス**
Sourcefire 時代から販売している Firepower 専用機
(仮想アプライアンス以外全て販売終了アナウンス済み)
- ASA with Firepower Services
Cisco ASA5500-X と Firepower module のハイブリッド
(多くの機種で販売終了アナウンス済み)
- Cisco NGFW / Firepower Threat Defense (FTD)
Firepower に ASA 基本機能を統合した一体型ソフトウェア
- Firepower Management Center (FMC)
Firepower 製品の機能をフルに利用するための管理サーバ



監視カメラ／
センサー



監視モニター／
経験豊富な監視者

Firepower Management Center (FMC) 概要

- Firepower 専用機や Firepower Services (on ASA) と、FTD を全てまとめて管理
- Access Control Policy 等、各 Policy を共有可能



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

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...)

Firepower Management Center プラットフォーム一覧



FMC1600

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

FMC2600

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

FMC4600

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

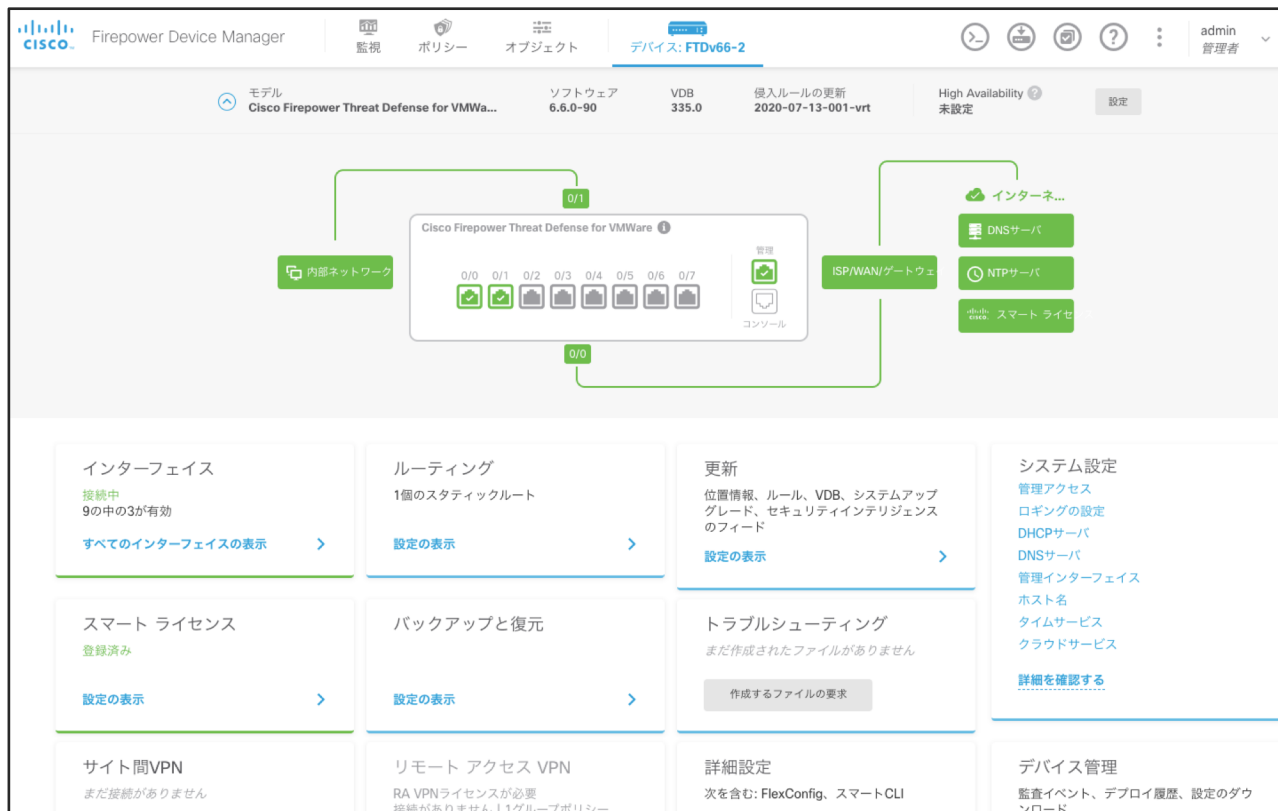
最大 25個のセンサー管理
最大イベント数 1,000万件
250GB のイベントストレージ
最大 5万ホスト、5万ユーザの
ネットワークマップ
300個のセンサー管理対応
モデルも有り (FMCv300)

Firepower の機能を最大限に引き出す管理サーバ

Firepower 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



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
- AMP4N 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

Firepower 管理方法一覧

11/12 14:00から
ウェビナー開催予定

Centralized

Firepower Management
Center (FMC)

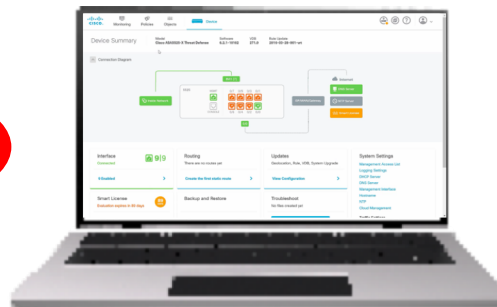


複数デバイスに対し、高度なセキュリティ監視・管理と自動化を実現

共存
不可

On-box

Firepower Device
Manager (FDM)

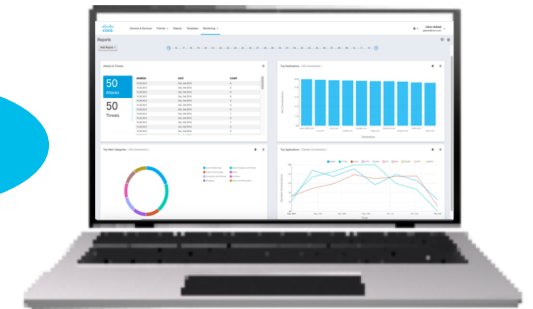


基本的なセキュリティポリシーを、シンプルに1つのデバイスに対して実施

共存
可能

Cloud-based

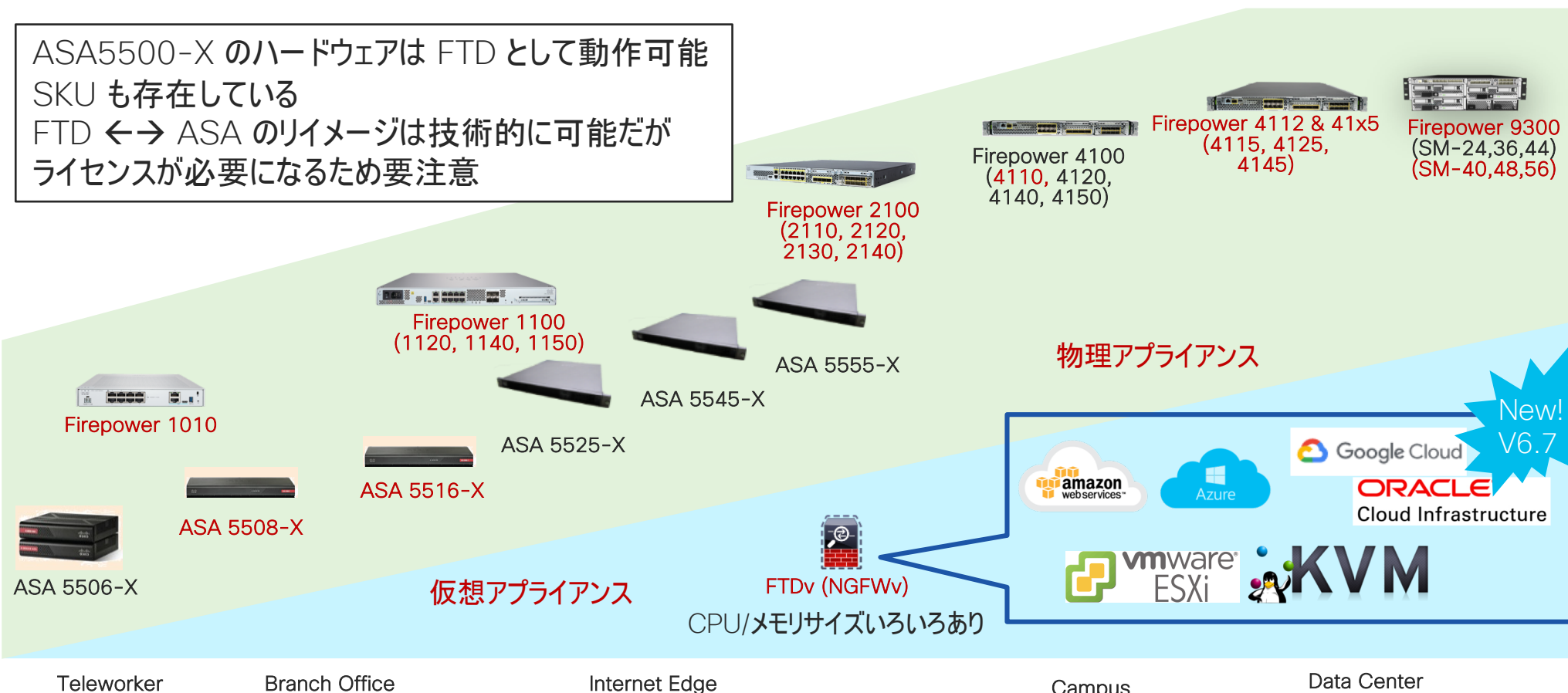
Cisco Defense
Orchestrator (CDO)



複数デバイスに対し、クラウドからセキュリティポリシーを管理
FTD だけでなく ASA や Meraki MX も同時に管理可能で、共有オブジェクトも利用可能

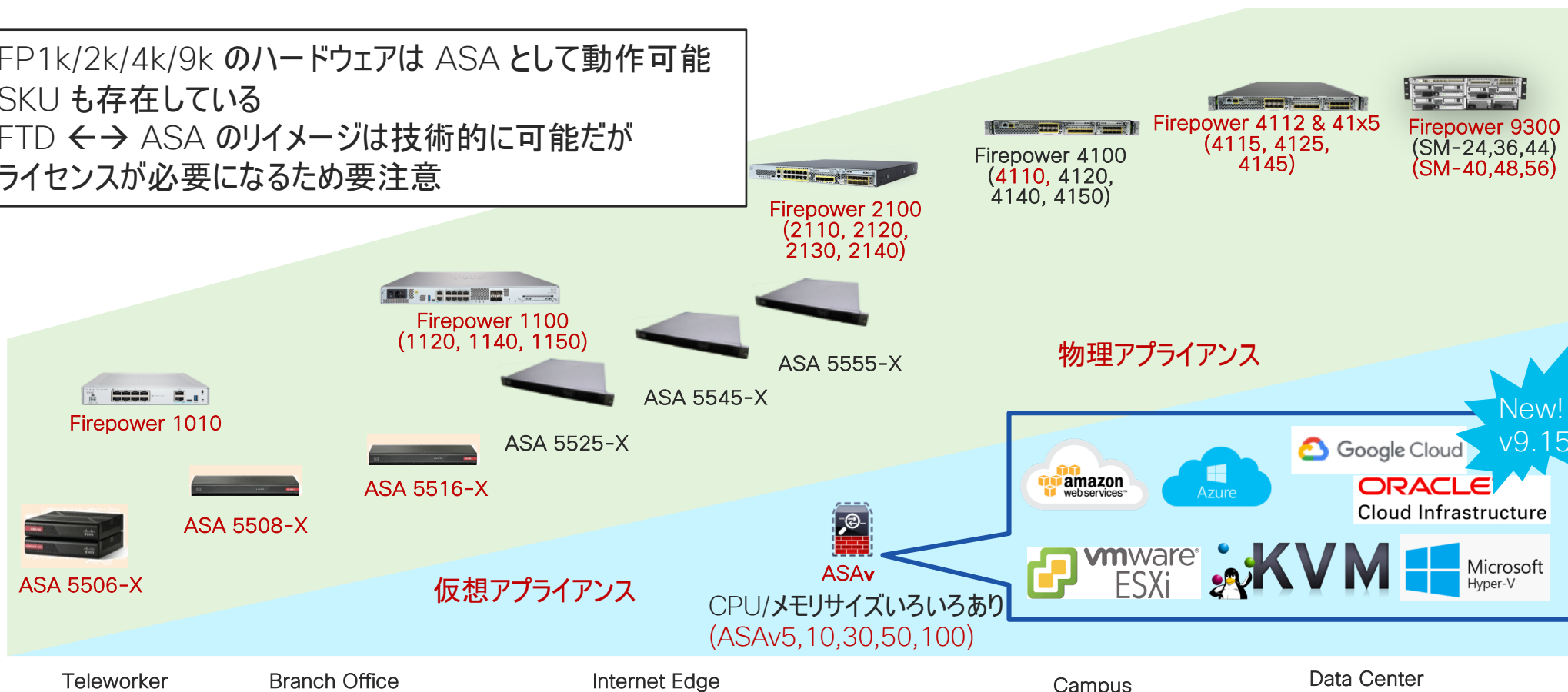
Firepower Threat Defense が動くプラットフォーム

ASA5500-X のハードウェアは FTD として動作可能
SKU も存在している
FTD ↔ ASA のリイメージは技術的に可能だが
ライセンスが必要になるため要注意



[参考] ASA ソフトウェアが動くプラットフォーム

FP1k/2k/4k/9k のハードウェアは ASA として動作可能
SKU も存在している
FTD ↔ ASA のリイメージは技術的に可能だが
ライセンスが必要になるため要注意

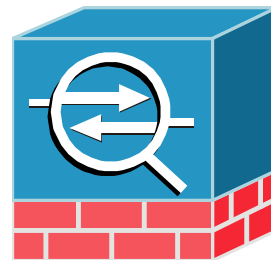


[参考] ASA と AnyConnect



• 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
- 16年目のロングセラー
(PIX まで遡ると27年!)



• AnyConnect の特長

- どこからでも安全なアクセスを提供
- 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, AMP enabler, Umbrella)
- 14年目のロングセラー
(Cisco VPN Client まで遡ると21年!)

まとめ

- Firepower 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
- “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
- 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
- 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

参考資料 (1)

- Firepower への cisco.comでのショートカット
<http://cisco.com/go/ngfw>
- ASA への cisco.comでのショートカット
<http://cisco.com/go/asa>
- パートナー向け技術資料 (Firepower 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
- [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>

参考資料 (2)

- シスコシステムズ合同会社 コーポレートブログにて、Firepower 6.6 (一部 6.5 を含む) の機能解説を、4回に渡って掲載

- Firepower 6.6 の新機能と改良点 (その1-4)

<https://gblogs.cisco.com/jp/2020/07/fp66-release-1/>

<https://gblogs.cisco.com/jp/2020/07/fp66-release-2/>

<https://gblogs.cisco.com/jp/2020/07/fp66-release-3/>

<https://gblogs.cisco.com/jp/2020/07/fp66-release-4/>

Cisco Japan Blog > セキュリティ

Firepower 6.6 の新機能と改良点 (その1)

小林 達哉
2020年7月15日

シスコの NGIPS / Anti-Malware 製品である Cisco Firepower、およびその Firepower にベースック Firewall & VPN 終端装置である Cisco ASA の機能を包含した NGFW 製品である Firepower Threat Defense (FTD) のソフトウェアバージョン 6.6 がリリースされ、3ヶ月以上が経過しました。

この 6.6 系は、6.5 系に比べて長くサポートされる予定のバージョンであり、また、今までの Firepower 関連において使えなかったところを多く改良しているソフトウェアです。当然、安定度も高く、今後の推奨バージョンの候補になっております。

当ブログでは、4回に分けて、バージョン 6.6 の代表的な新機能や改良点を、わかりやすく説明していきます。2019年秋にリリースされたバージョン 6.5 系からも同様に変更が説明します。

今回は、以下の機能について説明します。

- Firepower ソフトウェアのサポート期間について
- 新しいソフトウェア対応
- バージョンアップ時の注意事項

Firepower ソフトウェアのサポート期間について

Firepower ソフトウェア、および ASA ソフトウェアのサポート期間の考え方が更新されました。

Software release schedule の図がわかりやすいです。

6.11	6.10	6.9	6.8	6.7	6.6	6.5	6.4	6.3	6.2	6.1	6.0
●	●	●	●	●	●	●	●	●	●	●	●

Cisco Japan Blog > セキュリティ

Firepower 6.6 の新機能と改良点 (その2)

小林 達哉
2020年7月15日

NGIPS / NGFW / Anti-Malware である Cisco Firepower のソフトウェアバージョン 6.6 がリリースされました。前回に引き続き、今回は、FMC 管理 / FDM 管理のどちらにも該当する以下の新機能や改良点をピックアップします。

- URL Filter のデータベース変更
- Firepower 1010 だけの特別な機能のサポート
- 次世代検疫 / クラウドラングでの設定同期の改善
- VRF をサポート
- アップグレードファイルの柔軟な指定
- リーポートアクセス VPN での DTLS 1.2 サポート
- Object Group Search のサポート
- AWS と Azure での FMCv と FTDv の大型インスタンス対応および FTDv のオートスケール対応

URL Filter のデータベース変更

バージョン 6.5 から、URL Filter のデータベースが、Cisco Talos がネイティブにも変更されました。カテゴリも数分、新規追加等変わっておりますので、改めて URL Filter の設定を見直すことをおすすめします。

Firepower 1010 だけの特別な機能のサポート

Firepower 1010 は、デスクトップに置けるような小型サイズのアプライアンスであり、L2 Switching Port や PoE 対応 Port といった、他のアプライアンスには無い機能があります。バージョン 6.5 からこれらの設定が可能になりました。

Cisco Japan Blog > セキュリティ

Firepower 6.6 の新機能と改良点 (その3)

小林 達哉
2020年7月17日

NGIPS / NGFW / Anti-Malware である Cisco Firepower のソフトウェアバージョン 6.6 がリリースされました。全4回の連載のうち、第3回となる今回は、FMC 管理の環境のみに該当する以下の新機能や改良点をピックアップして解説します。過去の記事はこちらです (第1回、第2回)。

- セキュリティポリシーの設定と管理の利便性向上
- Time-Based Rule
- FMC イベントデータベースの変更
- FMC の新しい UI
- デプロイ画面
- インストール時に各種タスクを自動スケジューリング
- FMC バージョンアップ作業残時間の表示
- マルチインスタンスとクラウドラングの併用

セキュリティポリシーの設定と管理の利便性向上

Access Control Policy や Prefilter 等の設定や管理の利便性があること向上しています。文字列のサーチが複数条件でできたり、ルール設定画面内で Object の中身や使用状況の確認、あるいはそのまま編集が可能、等の機能拡張がなされています。複数のルールを選択し、同時に編集することも可能になりました。例えば、複数のルールのロギングのタイミングをまとめて変更したい、等といった場合にとても便利です。

Cisco Japan Blog > セキュリティ

Firepower 6.6 の新機能と改良点 (その4) 最終回

小林 達哉
2020年7月20日

NGIPS / NGFW / Anti-Malware である Cisco Firepower のソフトウェアバージョン 6.6 がリリースされました。全4回の連載の最終回となる今回は、FDM (Firepower Device Manager) 管理の FTD (Firepower Threat Defense) のみに該当する以下の新機能や改良点をピックアップして解説します。過去の記事はこちらです (第1回、第2回、第3回)。

- FTDv on AWS / Azure の FDM 管理
- Intrusion Rule のステータスの上書き
- 侵入ポリシーの検知モード
- IPDPS
- 管理インターフェイスの Proxy サーバ指定
- エアギャップ環境でのスマートライセンス (PLR)

FTDv on AWS / Azure の FDM 管理

AWS と Azure で動作させている FTDv の管理ツールに、FDM が使えるようになりました。AWS や Azure で稼働している FTDv の管理ツールに FMC を使うだけでなく、という要件の場合にご利用ください。CDO (Cisco Defense Orchestrator) からの管理も FDM と同じ仕組みなので可能です。

Intrusion Rule のステータスの上書き

FDM で FTD に適用するセキュリティポリシーにおいて、Intrusion policy (侵入ポリシー) のレベルを選択可能ですが、この「レベル」内でセットされたルールのステータスを上書きする、ということが可能になりました。すなわち、この「レベル」で設定している各ルールのステータスについて、無効化されているルールを有効化したり、有効化されているルールを無効化できるようになった、ということになります。

Appendix

Firepowerシリーズのデータシート

- モデル別に存在、英語/日本語ともに公開 (英語版の方が最新)

[FP9300](#), [FP4100](#), [FP2100](#), [FP1000](#), [Virtual Appliance](#)

Products & Services / Security / Firewalls / Cisco Firepower 9300 Series / Data Sheets /

Cisco Firepower 9300 Series Data Sheet

Updated: April 20, 2020

Table of Contents

- Cisco Firepower 9300 Series a...
- Model overview
- Detailed performance specific...
- Hardware specifications
- Cisco Capital

Cisco Firepower

The Cisco Firepower® 9300 is high-performance computing require low (less than 5-micro programmatic orchestration, a Standards (NEBS)-compliant c or Cisco Firepower Threat Def

Model overview

Products & Services / Security / Firewalls / Cisco Firepower 4100 Series / Data Sheets /

Cisco Firepower 4100 Series Data Sheet

Updated: May 7, 2020

Table of Contents

- Cisco Firepower 4100 Series a...
- Model overview
- Detailed performance specific...
- Hardware specifications
- Cisco Capital

Cisco Firepow

The Cisco Firepower 4100 and internet edge use cas supports flow-offloading, building Standards (NEBS) Cisco ASA Firewall or Cis

Model overview

Products & Services / Security / Firewalls / Cisco Firepower 2100 Series / Data Sheets /

Cisco Firepower 2100 Series Data Sheet

Updated: July 11, 2019

Table of Contents

- Cisco Firepower 2100 Series a...
- Model overview
- Detailed performance specific...
- Hardware specifications
- Cisco Capital

Cis

The thre inco simu the C

Mo

Products & Services / Security / Firewalls / Cisco Firepower 1000 Series / Data Sheets /

Cisco Firepower 1000 Series Data Sheet

Updated: December 18, 2019

Table of Contents

- Cisco Firepower 1000 Series ...
- Model overview
- Detailed performance specific...
- Hardware specifications
- Cisco Capital

Cis

The Cisco Fir business res The 1000 Ser 1000 Series

Model o

Products & Services / Security / Firewalls / Data Sheets /

Cisco Firepower NGFW Virtual (NGFWv) Appliance Data Sheet

Updated: June 24, 2020

Partner Help

Download Print

(1) ★★★★★ (0)

Product overview

Table of Contents

- Product overview
- Benefits
- Features and specifications
- Product performance guidelines
- System requirements
- Ordering information
- Cisco environmental sustainabi...
- Cisco Capital
- The Cisco Security Advantage

Today, businesses rely on a mixture of physical and virtual solutions to meet their network security needs. They need the flexibility to deploy different physical and virtual firewalls across a wide range of environments while still maintaining consistent policy throughout branch offices, corporate datacenters, and all entry points between. From data center consolidation to office relocations, mergers and acquisitions, or seasonal peaks in demand on your applications, Cisco's virtual firewall portfolio helps businesses simplify security management with the convenience of unified policy and the flexibility to deploy everywhere.

Cisco® Next-Generation Firewall Virtual (NGFWv) appliance combines Cisco's proven network firewall with advanced next-gen IPS, URL filtering, and malware detection. Identify and eliminate threats automatically, freeing up security and network operations teams. NGFWv also simplifies protecting virtualized environments by enabling consistent security policies to follow your workloads across physical, private, and public cloud environments. Get deep visibility into your network to quickly detect threat origin and activity, then stop attacks before they impact your business. Cisco virtual firewall offerings mitigate any significant shift in demand on your IT department so you can protect your workloads against increasingly complex threats with world-class security controls.

Product overview

FTD ライセンス一覧 (1)

FTD はスマートライセンス必須

Airgap 環境では License Reservation を申請するか Smart Software Manager Satellite を構築

★ は FTD のモデル毎に1,3,5年のライセンスを購入

FMC 利用時は FMC でまとめてライセンスを管理

FDM 利用時は 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)

- Base (無償)

AVC, Basic Firewall, Routing & Switching

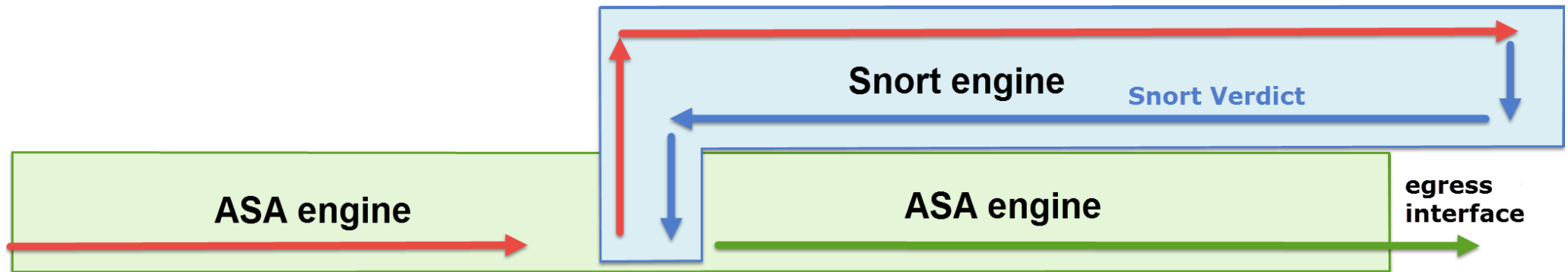
- Threat ★

IPS / IDS, Security Intelligence

FTD ライセンス一覧 (2)

- URL Filtering ★
カテゴリ、reputation
- Malware ★
AMP for Networks, Threat Grid, ファイル保存
- AnyConnect
サイト単位で APEX or Plus ライセンスを適用 or デバイス単位で VPN-Only ライセンスを利用
評価ライセンス利用のためには別途申請が必要 (初期の 90日間評価ライセンスには含まれない)
- FMC Virtual
管理デバイス数 (2,10,25) 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)
300デバイス管理が可能な大型モデルもあり (FMCv300)

FTD パケット処理の大まかなプロセス



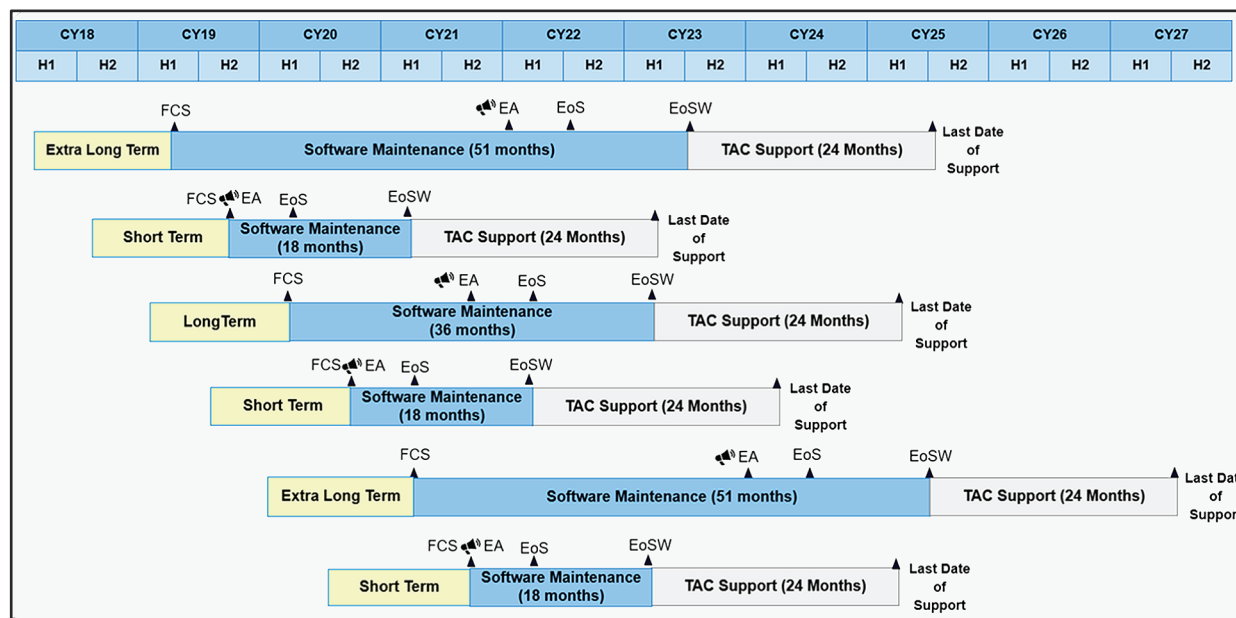
1. Ingress Interface に入ってきたパケットはまずは ASA エンジン (通称 LINA) にて処理される
 2. ポリシーに適合すれば、パケットは Snort エンジンにてインスペクションされる
 3. Snort エンジンがパケット転送の許可/破棄を決定
 4. ASA エンジンは Snort の判断に従ってパケットを転送するか破棄する
- Snort エンジンは Firepower 6.x のコードで動作
 - ASA エンジンは ASA 9.x のコードで動作

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>

- 年の前半と後半にそれぞれ新しいソフトウェアをリリースする
- 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 6.5 → ショートタームサポート
 - FTD 6.6 → ロングタームサポート
- ロングタームサポートの中でも、2019年前半、2021年前半(予定)に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 6.4 → 2019年前半リリースなのでエクストラロングタームサポート



FTD / FMC 推奨ソフトウェアバージョン

- 2020年11月時点で一般的な推奨バージョンは 6.6.1
 - 6.4 系の最新版も十分に利用されているが、いくつかのセキュリティアドバイザリに該当しているので要注意
 - 6.5 系はショートタームサポートであり、すでにサポート終了スケジュール発表済み
- 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

The screenshot shows the Cisco Software Download page for Firepower NGFW Virtual. The page includes a search bar, expand/collapse buttons, and a list of releases. The 'Suggested Release' section highlights version 6.6.1 with a star icon. The 'Latest Release' section lists versions 6.7.0, 6.4.0.10, 6.6.1 (with a star), and 6.2.3.16. The right side of the page shows details for the 6.6.1 release, including a table of file information.

File Information	Release Date	Size
Firepower Threat Defense upgrade Do not untar Cisco_FTD_Upgrade-6.6.1-91.sh.REL.tar	16-Sep-2020	12
FTDv: KVM install package	16-Sep-2020	11

★マークに注目

