



# Cisco Firepower Next-Generation Firewall 6.3 Features Lab v1.2のご紹介

2019年4月18日

シスコシステムズ合同会社 セキュリティ事業

稲澤 敏

# 本日のアジェンダ

- Cisco Firepower Next-Generation Firewall概要
- 最新バージョン (Firepower 6.3) での新機能概要
- dCloud Lab 利用方法
- Cisco Firepower Next-Generation Firewall 6.3 Features Lab v1.2 シナリオ概要

Cisco Firepower

Next-Generation Firewall概要

# 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 (CiscoISE 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



# ネットワークマップ

- 対象ネットワーク上のホストに関する情報を収集し管理
- インシデント解析や自動チューニングのベースとなる情報

## 収集情報例

- 存在するホスト (IPv4, IPv6)
- ホップ数
- オペレーティングシステム
- アプリケーション
- ポート
- プロトコル
- 脆弱性

The screenshot displays a network management interface with the following sections:

- ホスト**: Global \ Cisco\_Backend \ Cisco\_SOC
- ドメイン**: Global \ Cisco\_Backend \ Cisco\_SOC
- IPアドレス**: 10.131.10.11
- NetBIOS名**: vNGIPS.dcloud.cisco.com (0)
- デバイス (Hop)**: vFTD.dcloud.cisco.com (0)
- MACアドレス (TTL)**: 00:11:F5:1:68:8E:13 (Hon Hai Precision Ind. Co.,Ltd.) (128)
- EC:F0:0E:17F:23:08 (AboCom) (64)**
- ホストタイプ**: Host
- 最後の発見**: 2018-07-23 12:02:06
- 現在のユーザ**: CAMIE HARGROVE (DCLLOUD-SOC\kharg, LDAP)
- 表示**: コンテキストエクスプローラ | 検知イベント | 侵入イベント | ファイルイベント | Malwareイベント

**侵入の痕跡 (0)**

**オペレーティングシステム**

ベンダー	製品	バージョン	ソース
Microsoft	Windows	7	Firepower

**アプリケーション (2)**

アプリケーションプロトコル	クライアント	バージョン	ウェブアプリケーション
<input type="checkbox"/> NetBIOS-dgm	<input type="checkbox"/> NetBIOS-dgm		
<input type="checkbox"/> NetBIOS-ns	<input type="checkbox"/> NetBIOS-ns		

**ユーザ履歴**

ユーザ	2018-07-22 12:17:33	2018-07-23 12:17:33
JANFAN RUST (DCLLOUD-SOC\orust, LDAP)		
TONISHA KIDDER (DCLLOUD-SOC\okidjd, LDAP)		
MARYETTA WFATHERFORD (DCLLOUD-SOC\wfeat, LDAP)		
FARAH DESMARAIS (DCLLOUD-SOC\odesm, LDAP)		
JANN MAZZOLA (DCLLOUD-SOC\hmazz, LDAP)		
BIRGIT GAGNON (DCLLOUD-SOC\ggagn, LDAP)		
CAMIE HARGROVE (DCLLOUD-SOC\kharg, LDAP)		

# インシデント解析例

例)アラートが発生したホストの情報を確認したい

2018-07-23 11:04:10	medium	1	10.0.12.190	10.0.10.12	(snmp) / udp	32923 / udp	Unknown (Unknown)	0	PROTOCOL-SNM
2018-07-23 11:04:10	medium	1	10.0.12.190	ホストアドレスを調く	161 (snmp) / udp	32923 / udp	Unknown (Unknown)	0	PROTOCOL-SNM
2018-07-23 11:04:09	medium	2	10.112.3.7	222.195.195.8	CHN 8 (Echo Request) / icmp	0 (No Code) / icmp	Unknown (Unknown)	0	PROTOCOL-ICM

## ホストプロフィール

ドメイン Global \ Cisco\_Backend \ Cisco\_SOC  
IPアドレス 10.0.10.12  
NetBIOS名  
デバイス (Hop) VFTD.dcloud.cisco.com (1)  
vNGIPS.dcloud.cisco.com (128)  
MACアドレス(TTL) 00:00:28:12:CF:0E (PRODIGY SYSTEMS CORPORATION) (128)  
00:06:29:40:A5:E5 (IBM Corp) (128)  
02:1A:C5:01:00:00 (255)  
... (すべてを表示)  
ホストタイプ Host  
最後の発見 2018-07-23 11:16:44  
現在のユーザ PEARLINE EARNEST (DCLLOUD-SOC\bearn, LDAP)  
表示 コンテキストエクスプローラ | 接続イベント | 侵入イベント | ファイルイベント | Malwareイベント

### アプリケーション (2) ▼

アプリケーションプロトコル	クライアント	バージョン	ウ
NetBIOS-dgm	NetBIOS-dgm		
NetBIOS-ns	NetBIOS-ns		

クライアントアプリケーション

### ユーザ履歴 ▼

ユーザ	2018-07-22 12:05:53	2018-07-23 12:05:53
IVEY PAQUIN (DCLLOUD-SOC\bpaqu, LDAP)		
GENOVEVA PRICKETT (DCLLOUD-SOC\gprick, LDAP)		
PILAR MCVAY (DCLLOUD-SOC\pncvay, LDAP)		
RAYMONDE HITT (DCLLOUD-SOC\ehitt, LDAP)		
INES HUNTLEY (DCLLOUD-SOC\ihunt, LDAP)		

ユーザ履歴

## 侵入の痕跡 (1) ▼

カテゴリ	イベントタイプ	説明	2018-07-23 11:22:56	2018-07-23 11:22:56
Impact 2 Attack	Impact 2 Intrusion Event - attempted-admin	The host was attacked and is potentially vulnerable		

侵入の痕跡

## オペレーティングシステム ▼

ベンダー	製品	バージョン	ソース
Microsoft	Windows	Vista, 7, Server 2008, Phone R2, 10	Firepower

端末 OS

## サーバ (2) ▼

プロトコル	ポート	アプリケーションプロトコル	製造元およびバージョン
udp	67	DHCP	
udp	0	保留中	

サーバアプリケーション

## 脆弱性 (614) ▼

名前	リモート	コンポーネント	ポート
* RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.		Windows Vista, 7, Server 2008, Phone 7.5, Phone 8.0, 8, Server 2012, Server 2012 R2, 10	
* RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.		Windows Vista, 7, Server 2008, Phone 7.5, Phone 8.0, 8, Server 2012, Server 2012 R2, 10	
** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.		Vista, 7, Server 2008, Phone 7.5, Phone 8.0, 8, Server 2012, Server 2012 R2, 10	
** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.		Windows Vista, 7, Server 2008, Phone 7.5, Phone 8.0, 8, Server 2012, Server 2012 R2, 10	

該当脆弱性リスト

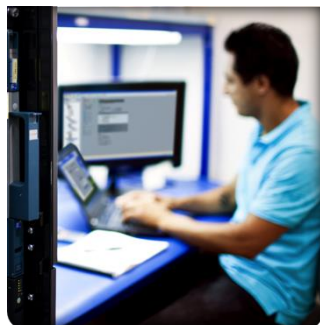
✓ 端末のセキュリティに関連する様々な情報を自動収集し、解析に活用

# 自動チューニングとインパクト解析

一般的な侵入検知機器 (IPS) の  
運用者が抱える問題

環境に合わせて設定を調整  
したいが、運用が大変...

沢山のログが出るが、本当に  
重要なものがわからない...



Overview 分析 **ポリシー** デバイス オブジェクト

アクセス制御 ▶ 侵入 ネットワーク検知 アプリケーションディテクタ コリレーション アクション ▼

### ポリシーの編集: [0] Corporate Production IPS Policy

ポリシー情報 ⚠

- ルール
- Firepower推奨
- ⊕ 詳細設定
- ⊕ ポリシーレイヤー

#### Firepower推奨ルール構成

Firepowerは2637ホストに対して30924ルール状態設定を推奨しています

- ➡ 1052個のルールをイベントを生成するよう設定します
- ✖ 71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
- ➡ 29801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せん  
最終生成日: 2018 Jul 23 14:13:32

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

⊕ 詳細設定

推奨項目を使用する

推奨項目をアップデート

**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

**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

Priority	Count
low	41
medium	627
high	1,433

Impact	Count
1	106
2	374

攻撃の緊急度 "High" のアラート数: 1433      実インパクト "High(1)" のアラート数: 106

10分の1以下に減少

# Security Intelligence 脅威情報フィルタ



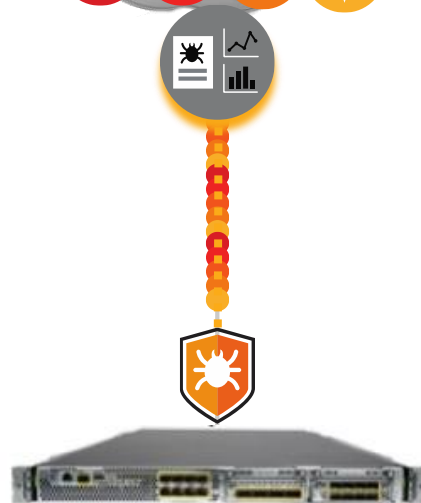
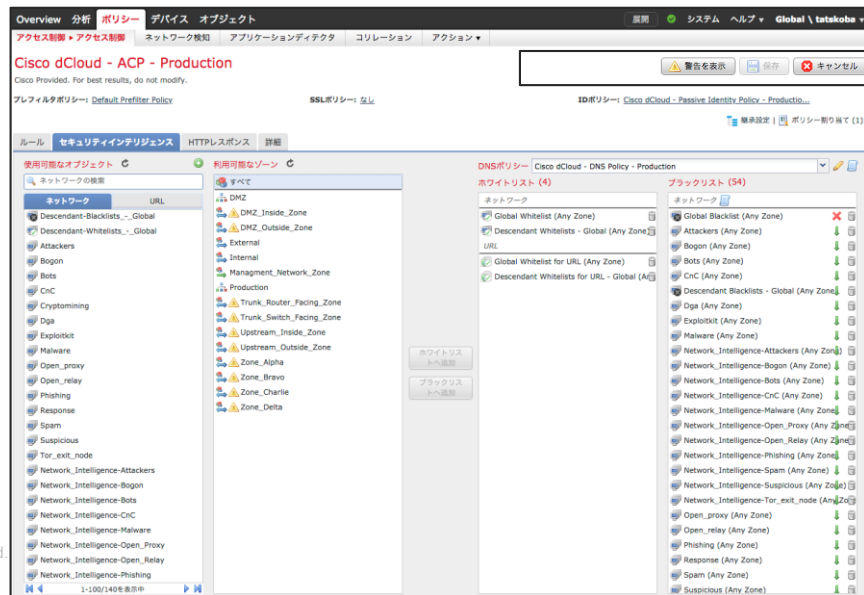
- Cisco Collective Security Intelligence 提供のブラックリスト IP アドレス、URL、ドメインに基づく制御 (i.e. レピュテーション)

- 既知のブラックリスト宛て or からのコネクションを モニターもしくはブロック

## • カテゴリー

- CnC
- Malware
- Phishing
- Bots
- Attackers

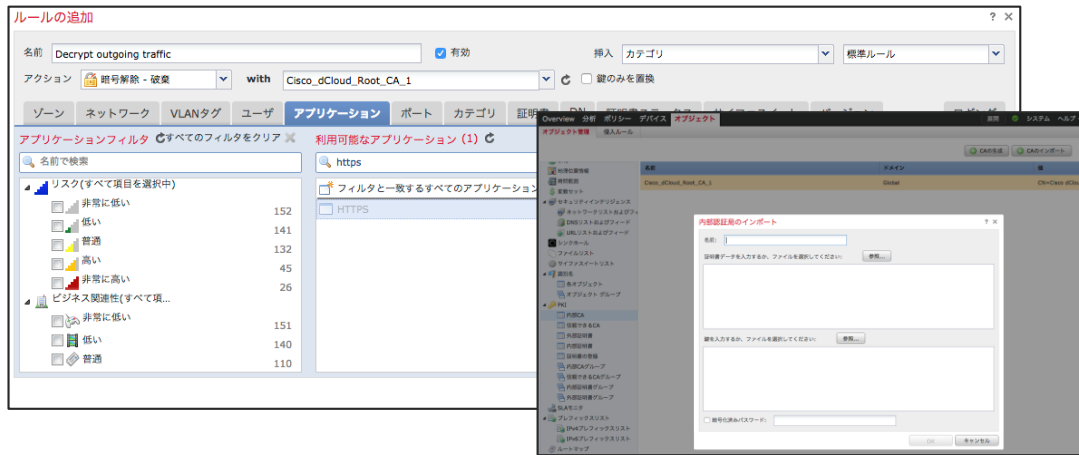
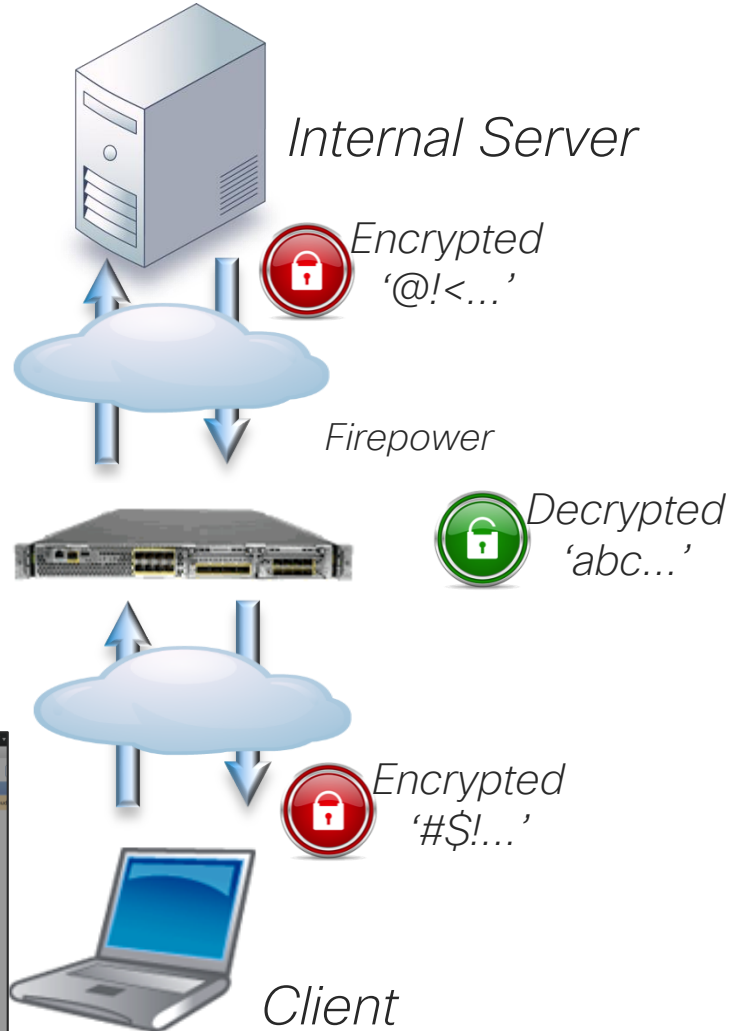
など





# SSL / TLS 復号

- SSL / TLS で暗号化された通信のインスペクションを行う機能
  - inbound passive
  - inbound inline
  - outbound inline
- Version 6.3.0 以降の FP2100/4100/9300 はハードウェア処理となり処理能力が向上



# 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)

Malware Summary > Malware イベントの表示

検索の制限がありません (検索を編集)

検知名	ファイル名	ファイルタイプ	カテゴリ
W32.697FA5A1DE-95.SBX.TG	70ca2b97-ff39-4a0b-87af-8cb4f49ee7b-grd4.xls	MSOLE2	NEW_OFFICE
Doc.Downloader.Donoff::100.sbx.tg	4f116d3b-e274-404b-bb2a-928dee88727-lockv.docm	NEW_OFFICE	261
Doc.Downloader.Donoff::100.sbx.tg	f7cc3eb9-8f59-4a7e-a815-f496348c4a07-lockv.docm	NEW_OFFICE	42
Doc.Downloader.Generic::95.sbx.tg	vizsla.origo.hu	NEW_OFFICE	16

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)

### 697fa5a1...457fcd80のネットワークファイルトラジェクトリ

ファイルSHA256	697fa5a1...457fcd80	First Seen	2018-04-25 07:03:34 オン 172.16.1.128 実行者: BLANCHE TYNDALL (DCLOUD-SOC\etvnd_LDAP)
ファイル名	70ca2b97-ff39-4a0b-87af-8cb4f49ee7b-grd4.xls, affe5843-dddd-4e9b-abd1-fb772bb44cff-grd4.xls	Last Seen	2018-07-25 20:43:59 オン 10.110.10.11 実行者: ANNALÉE SWINDELL (DCLOUD-SOC\swin_LDAP)
File Size (KB)	57,500	イベント	784 (250件表示)
ファイルタイプ	MSOLE2	Seen On	429ホスト (160件表示)
File Category	Executables	Seen On Breakdown	送信者数: 255 → 受信者数: 324 (85 → 118件表示)
Current Disposition	Malware		
Threat Score	Very High		
検知名	W32.697FA5A1DE-95.SBX.TG		

### Trajectory

② 解析情報(サンドボックス含む)と連携

時間	2018-04-25 07:05:44	20:02	20:03
イベントタイプ	送信されたファイル		
IPアドレス	10.0.1.178		
送信先	10.0.1.128		
ユーザ	JANITA KOLB (DCLOUD-SOC\tkolb_LDAP)		
ファイル名	affe5843-dddd-4e9b-abd1-fb772bb44cff-grd4.xls		
傾向	Malware		
Action	Malware Cloud Lookup		
アプリケーションプロトコル	HTTP		
クライアント	Web browser		

③ ネットワーク上での拡散状況を可視化

④ 端末の特定

Events Transfer ブロック Create 移動 Execute Scan Retrospective Quarantine

# クラウドリコールによるゼロデイマルウェア検知例

概要 分析 ポリシー デバイス オブジェクト FireAMP 動作状況 システム ヘルプ admin

コンテキスト エクスプローラ 接続 Intrusions ファイル ネットワーク ファイル トラジェクトリ ホスト ユーザー 脆弱性 コリレーション カスタム 検索

### 3706b205...b08480b4のネットワーク ファイル トラジェクトリ

ファイルSHA-256 3706b205...b08480b4

ファイル名

ファイルタイプ [MSEXE](#)

File Category [Executables](#)

Current Disposition [Malware](#)

Threat Score None

First Seen 2014-06-08 00:39:19 オン [23.75.24.57](#)

Last Seen 2014-06-08 17:29:39 オン [45.0.132.198](#)

イベント 2

Seen On ホスト数: 2

Seen On Breakdown 送信者数: 1 → 受信者数: 1

#### Trajectory

Jun 08

00:39 17:29

23.75.24.57

45.0.132.198

このケースでは17時間ほど遅れて、既存セキュリティを抜けてしまったマルウェアを検知

Events Transfer [ブロック](#) Create 移動 Execute Scan Retrospective Quarantine

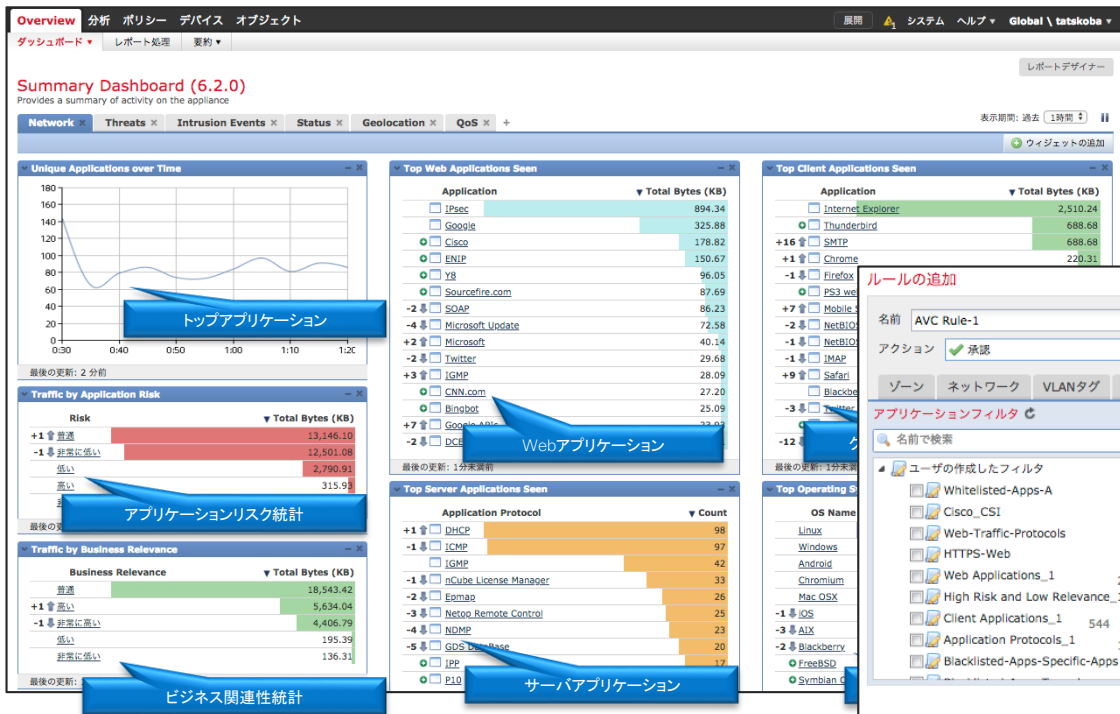
Dispositions Unknown [Malware](#) クリーン カスタム Unavailable

#### Events

時間	イベントタイプ	送信側IP	受信側IP	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 アブ...	説明
2014-06-08 00:39:19	転送	23.75.24.57	45.0.132.198		Unkno...	Malware Cloud Loo...	HTTP	Internet Ex...	CNET	Retrospective Event, Sun Jun 8 08:...
2014-06-08 17:29:39	回顧的イベント				Malware					

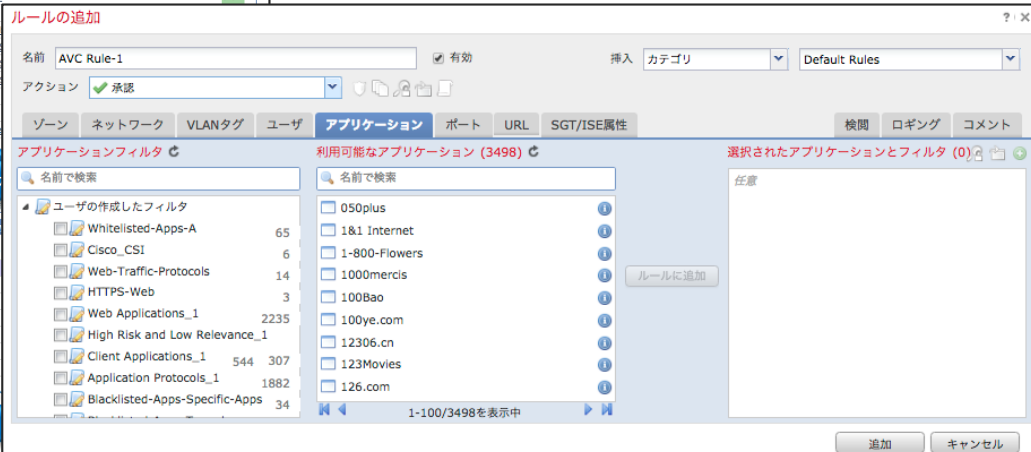
# Application Visibility Control アプリケーションの可視化と制御

- 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 (v6.3時点) 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

ネットワーク リポート

**I. 概要**

シスコは、シスコシステムズ: eDmEdがネットワークの状態にあると判断しました。その理由は、ビジネスの継続性があるため、適切なリスクのある状態に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ており、マルウェアを伝播したり、侵害を誘発したりする可能性があります。

詳細期間: Sat Apr 29 2017 04:24:20~Mon May 29 2017 04:24:25

リスクのあるアプリケーション <b>9</b>	リスクのあるユーザ <b>18</b>	高権限アプリケーション <b>1</b>
暗号化アプリケーション <b>9</b>	セキュリティ関連機能を持つアプリ <b>2</b>	危険な Web ブラウザ <b>56</b>

ネットワークプロファイル

<b>10</b> オペレーティングシステム	<b>8</b> モバイルデバイス	<b>83</b> 使用中のアプリケーション	<b>5</b> 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: eDmEdがアプリケーション脆弱性と脆弱なファイルタイプを継続してCisco Firepowerアプリケーション脆弱性検出エンジンを使用して検出しました。アプリケーション脆弱性の出現を減らすアプリケーション、脆弱性、脆弱なOS、および脆弱なソフトウェアのリリースを定期的に更新する。モバイルデバイスやWebのリスクを自己ネットワークのリスクと脆弱性を同様に減らす。

## アタックレポート

攻撃 リポート

**I. 概要**

シスコはシスコシステムズ: eDmEdがネットワークの状態にあると判断しました。その理由は、脆弱なホストを脆弱化した攻撃がネットワーク上で検出されたためです。リスクを軽減するために、これらの攻撃を減少させる必要があります。

詳細期間: Sat Apr 29 2017 04:24:20~Mon May 29 2017 04:24:25

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

関連の攻撃によりもたらされるリスク

分類	カウント
Prevalent host traffic	6,888
Attempted Information Leak	8,960
Unknown Traffic	5,889
Site activity	2,257
Information Leak	1,561

シスコは、シスコシステムズ: eDmEdがCisco Firepowerアプリケーションを導入して実行することを勧めます。

- ネットワーク脆弱性のリスクに対する継続的な脆弱性検出
- このリスクの出現を軽減するために自動化された保護を実装する

## マルウェアレポート

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: eDmEdが脆弱なマルウェアファミリーによる攻撃を検出しており、高いリスクであると判断しました。侵害を防ぐために、Cisco Advanced Malware Protection (AMP)を導入されました。このレポートは、この期間にネットワークで検出された攻撃を示しています。

詳細期間: Sat Apr 29 2017 04:24:20~Mon May 29 2017 04:24:27

マルウェアを検出 <b>36</b>	IOCを求めているホスト <b>19</b>	継続プロトコル <b>2</b>
CnCサーバに接続されているホスト <b>0</b>	マルウェアの通信 <b>22</b>	マルウェアのURL <b>2</b>

マルウェアのプロファイル: 30 日

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

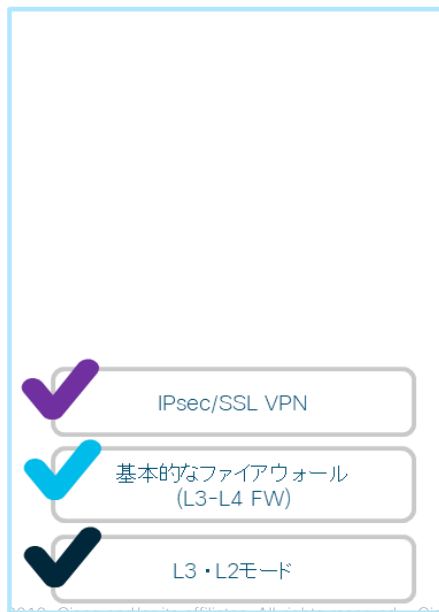
シスコは、Advanced Malware Protectionを導入して実行することを勧めます。

- 高度なマルウェアの継続的な脆弱性を検出する
- このリスクを軽減するために適切な制御を強化する

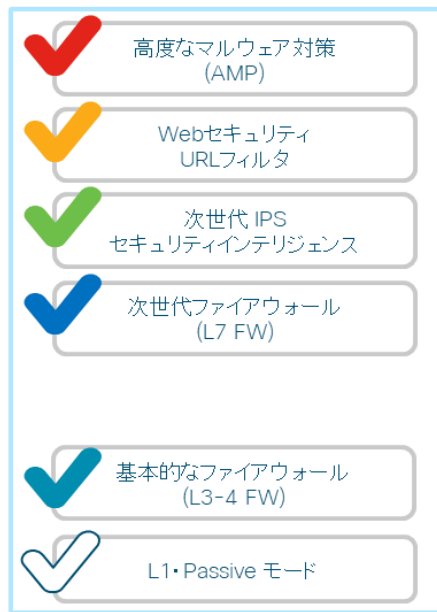
# ソフトウェア – Firepower Threat Defense (FTD)

- ASA基本機能とFirepower(NGIPS)を統合した一体型ソフトウェア
- FTDはスマートライセンスが必須

ASA Firewall



Firepower IPS

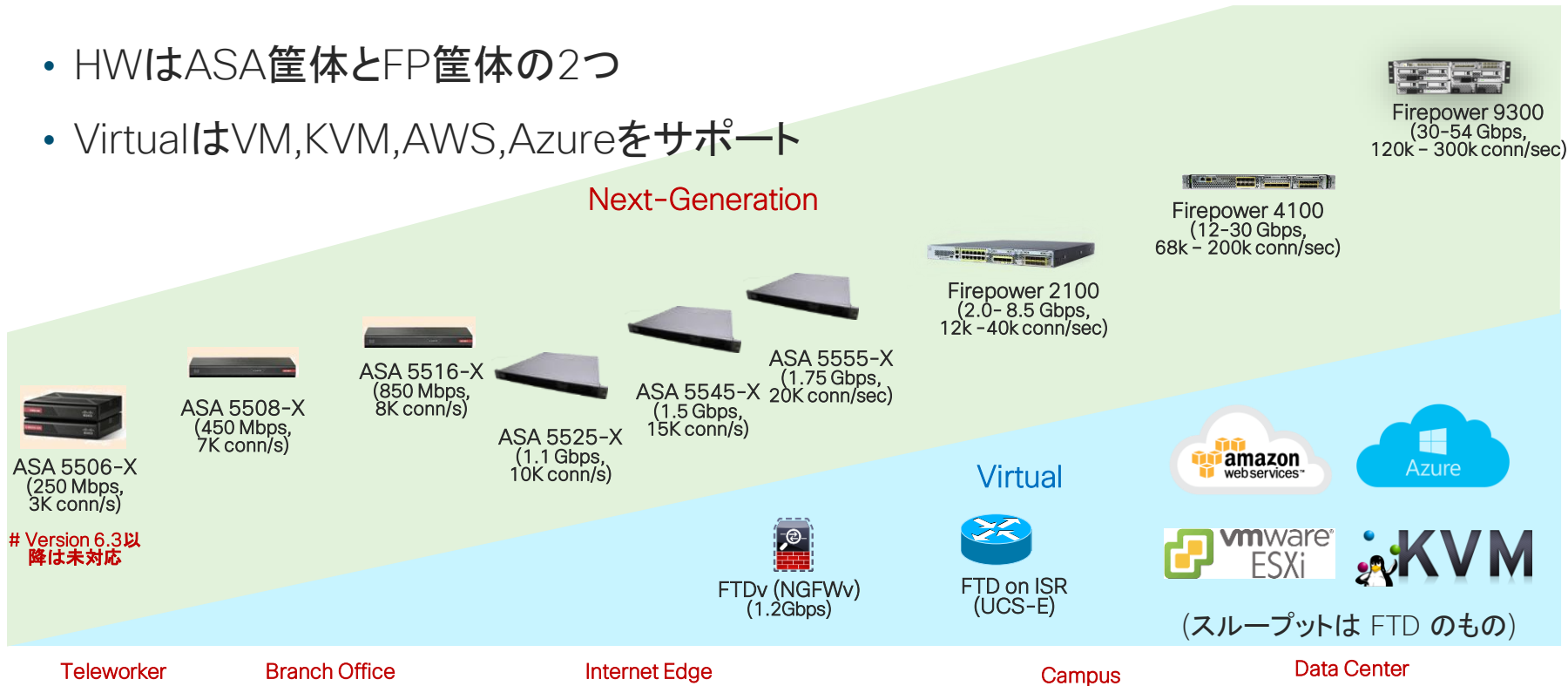


Firepower Threat Defense



# Firepower Threat Defense が動くプラットフォーム

- HWはASA筐体とFP筐体の2つ
- VirtualはVM,KVM,AWS,Azureをサポート



# Version 6.3以降は未対応

# Off-Box管理 - Firepower Management Center (FMC)

- FTD 管理サーバ (FP41xx/93xx 利用時は必須)
- 各種設定・ポリシーの適用と管理・レポートの生成
- ネットワークマップ、IPSルールの自動チューニングやインパクトフラグはFMCで実施
- 日本語対応



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



FP Sensor

FTD Virtual 版と FP 専用機 (Virtual 版) を 1 台の FMC で管理している例

Overview	分析	ポリシー	デバイス	オブジェクト
デバイス管理	NAT	VPN	QoS	プラットフォーム設定
				FlexConfig
				証明書
デバイス管理				
List of all the devices currently registered on the Firepower Management Center.				
View By:	ドメイン別	すべて (2)	エラー (0)	警告 (0)
			Offline (0)	正常 (2)
				Deployment Pending (0)
名前	モデル	Version	ライセンスタイプ	
Global (1)				
Cisco_Backend (1)				
Cisco_SOC (2)				
<input checked="" type="checkbox"/> vFTD.dcloud.cisco.com 198.18.133.10 - Routed	Cisco Firepower Threat Defense for VMWare	6.2.3	ベース、脅威、Malware、URL Filtering	<a href="#">Cisco dCloud - ACP - SOC NGFW</a>
<input checked="" type="checkbox"/> vNGIPS.dcloud.cisco.com 198.18.133.11	NGIPSv for VMWare	6.2.3	保護、制御、Malware、URL Filtering	<a href="#">Cisco dCloud - ACP - SOC NGIPS</a>

<input checked="" type="checkbox"/> vFTD.dcloud.cisco.com 198.18.133.10 - Routed	Cisco Firepower Threat Defense for VMWare	6.2.3
<input checked="" type="checkbox"/> vNGIPS.dcloud.cisco.com 198.18.133.11	NGIPSv for VMWare	6.2.3



# On-Box管理 - Firepower Device Manager (FDM)

- Web ブラウザで FTD デバイスにアクセス、FTDv,ASA55xx-X,FP21xx で動作
- シンプルなUIで直感的な操作が可能 ※ただし機能制限あり
- 日本語対応

Cisco  
監視 ポリシー オブジェクト **デバイス**

デバイス概要  
モデル Cisco Firepower Threat Defense for VMWare  
ソフトウェア 6.2.3.2-45  
VDB 299.0  
ルールアップデート 2018-07-02-001-vrt

接続図

内部ネットワーク  
FTDv  
0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7 0/8  
管理  
コンソール  
ISP/WAN/ゲートウェイ  
インターネット...  
DNSサーバ  
NTPサーバ  
スマート ライセンス

インターフェイス **3/10**  
接続中  
3 有効

ルーティング  
まだルートがありません  
最初のスタティックルートの作成

更新  
位置情報、ルール、VDB、システムアップグレード、セキュリティインテリジェンスのフィード  
設定の表示

システム設定  
管理アクセス  
ロギングの設定  
DHCPサーバ  
DNSサーバ  
管理インターフェイス  
ホスト名  
NTP  
クラウドサービス  
トラフィックの設定  
URLフィルタリングの設定

スマート ライセンス  
登録解除済み  
設定の表示

バックアップと復元  
設定の表示

トラブルシューティング  
まだ作成されたファイルがありません  
作成するファイルの要求

# Firepower Version 6.3新機能概要

# Firepower 6.3.0 新機能一覧

## プラットフォームの拡張性

### マルチインスタンス for 4100/9300

- 最大14台の仮想インスタンス\*
- 冗長構成のサポート

\*機種により最大数は異なります。

### 100GEネットワークモジュール for 9300

- 2x100GE, 4x100GE Module
- シャーシ当たり最大8x100GEまでサポート

### HWによるTLS復号化対応

- より高速なTLSインスペクションスループット
- すべてのFirepowerプラットフォームでサポート(2100/4100/9300)

### Fail-to-wireネットワークモジュール for FP2100

- 2100でもFTWの利用が可能に

### NGIPSからの移行

- 新しいマイグレーションツール

## 操作性

### エアギャップ環境でのライセンス利用

- License Reservationにより、エアギャップ環境でのFTDの利用が可能に

### ローカル管理FTDの機能拡張

- ハイアベイラビリティ、パッシブ認証、SmartCLI(Routing、ACL等)、RAVPN認証関連等

### FMCで管理されている全FTDのフルバックアップが可能に

### Syslogイベントの統合

- ASAとSnortからまとめて一つのSyslogを送信

## 可視性 & セキュリティ

### イベントログから他製品との容易な連携

- 他のCisco製品やサードパーティSIEMsとのシームレスな統合

### FQDNベースのアクセスコントロール

- ASA機能のFTDへのマイグレーション
- 動的クラウドベースアプリケーションのためのコントロール有効化

### FMCにおける2FA & RADIUS CoA for RA VPN

- ASA機能のFTDへのマイグレーション

# Firepower 6.3.0 新機能一覧

今回のLabで操作可能な機能

## プラットフォームの拡張性

### マルチインスタンス for 4100/9300

- 最大14台の仮想インスタンス\*
- 冗長構成のサポート

\*機種により最大数は異なります。

### 100GEネットワークモジュール for 9300

- 2x100GE, 4x100GE Module
- シャーシ当たり最大8x100GEまでサポート

### HWによるTLS復号化対応

- より高速なTLSインスペクションスループット
- すべてのFirepowerプラットフォームでサポート(2100/4100/9300)

### Fail-to-wireネットワークモジュール for FP2100

- 2100でもFTWの利用が可能に

### NGIPSからの移行

- 新しいマイグレーションツール

## 操作性

### エアギャップ環境でのライセンス利用

- License Reservationにより、エアギャップ環境でのFTDの利用が可能に

### ローカル管理FTDの機能拡張

- ハイアベイラビリティ、パッシブ認証、SmartCLI(Routing、ACL等)、RAVPN認証関連等

### FMCで管理されている全FTDのフルバックアップが可能に

### Syslogイベントの統合

- ASAとSnortからまとめて一つのSyslogを送信

## 可視性 & セキュリティ

### イベントログから他製品との容易な連携

- 他のCisco製品やサードパーティSIEMsとのシームレスな統合

### FQDNベースのアクセスコントロール

- ASA機能のFTDへのマイグレーション
- 動的クラウドベースアプリケーションのためのコントロール有効化

### FMCにおける2FA & RADIUS CoA for RA VPN

- ASA機能のFTDへのマイグレーション

## 参考) マルチインスタンスの概要

- Firepower 4100 と 9300 **のみでサポート**
- 1つのモジュール or アプライアンスで複数の論理デバイスが稼働
  - まずは FTD のみでサポート、FTD と ASA の混在は**将来サポート予定**
  - Docker インフラとコンテナのパッケージングを活用
- トラフィックも管理も完全に分離
- 物理/論理インターフェイスと VLAN は Supervisor で実施



## 参考) マルチインスタンスの利点

- Network Security 製品におけるユニークで新しいアプローチ
- ハードウェアレベルでのトラフィックの処理と管理プロセスの完全な分離
- シングルコンテキストで完結する機能はすべてサポート
- ソフトウェア管理や再起動を完全に独立して実施可能
- **将来は** FTD と ASA のインスタンスの共存が可能
- **将来は** ハードウェアから Docker コンテナとして FTD と ASA を持ち出し可能
- 品質と導入コストの双方にメリット

## 参考) Airgap 環境での FTD ライセンス

- FTD は**必ずスマートライセンスが必要**
- FMC の管理インターフェイスからインターネットにアクセス不可な環境ではスマートライセンスサテライトサーバにて対応
- スマートライセンスサテライトサーバの利用が何らかの理由で不可能な場合には、FTD 6.3.0 からサポートされる以下のどちらかを選択し、事前にシスコからの承認を得る必要がある。いずれもインストール時に Cisco Smart Software Manager (CSSM) に管理者がアクセスし、ライセンスを確保することで、**FMC からの定期的な CSSM へのアクセスを省くことが可能**
  - **UPLR** – Universal Permanent License Reservation  
全機能が利用可能なため、利用については厳密な審査が行われる
  - **SLR** – Specific License Reservation  
機能を選択して利用可能、UPLR ほど厳密ではないが、事前に申請が必要
- **どの選択を行ってもスマートアカウントの作成、利用は必要なことに注意**

## 参考)品質のさらなる向上 - Snort リスタート 機能改善

- 6.3.0 にてさらにいくつかのシナリオにて Snort リスタートが不要に
  - テキストに加えてバイナリのルールも含めた**すべての SRU**
  - 実際にデプロイする前の VDB 更新インストール
- Snort リスタートが起きるシナリオは、**あとはこれだけ**
  - Talos が関係しない VDB 更新やカスタムアプリケーションディテクタの変更
  - File Policy のオプション変更 (Snort のインスタンス数が変わる際のみ)
  - TLS or Captive Portal Policy の有効化/無効化
  - HA ペアの作成/破棄時
  - Network Discovery での Traffic-Based Detection で HTTP, FTP, or MDNS の有効化/無効化
  - 全データインターフェイスでの最大 MTU の変更

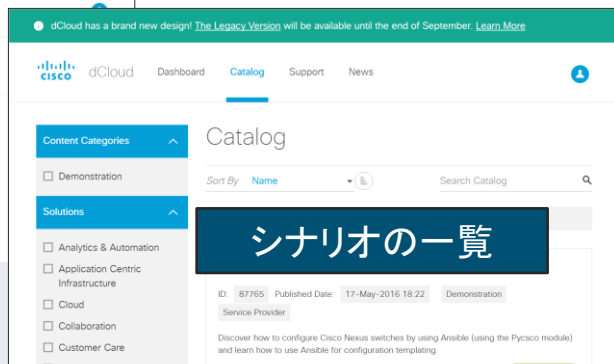
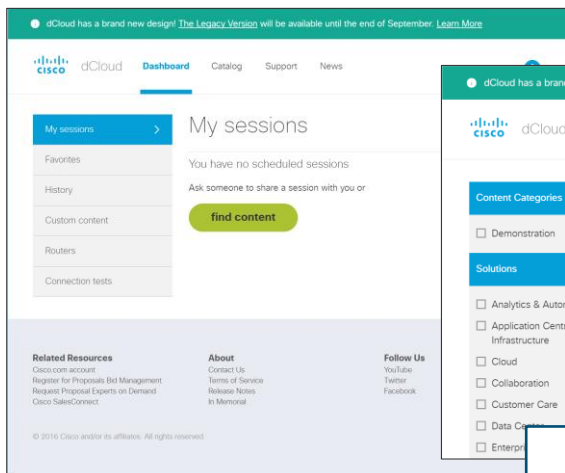


# dCloud利用方法

# dCloud (Demo Cloud)

<http://dcloud.cisco.com/>

いつでもどこでもインターネット経由で呼び出せる「**デモ環境**」、「**PoV環境**」、「**ラボ環境**」です。  
デモ環境はセットアップ済で提供されるため、すぐにデモができるため、準備 (機材の入手やセットアップ、シナリオ作成) にかかる時間が省略できます。



日本語シナリオも充実

## システムズエンジニアリング

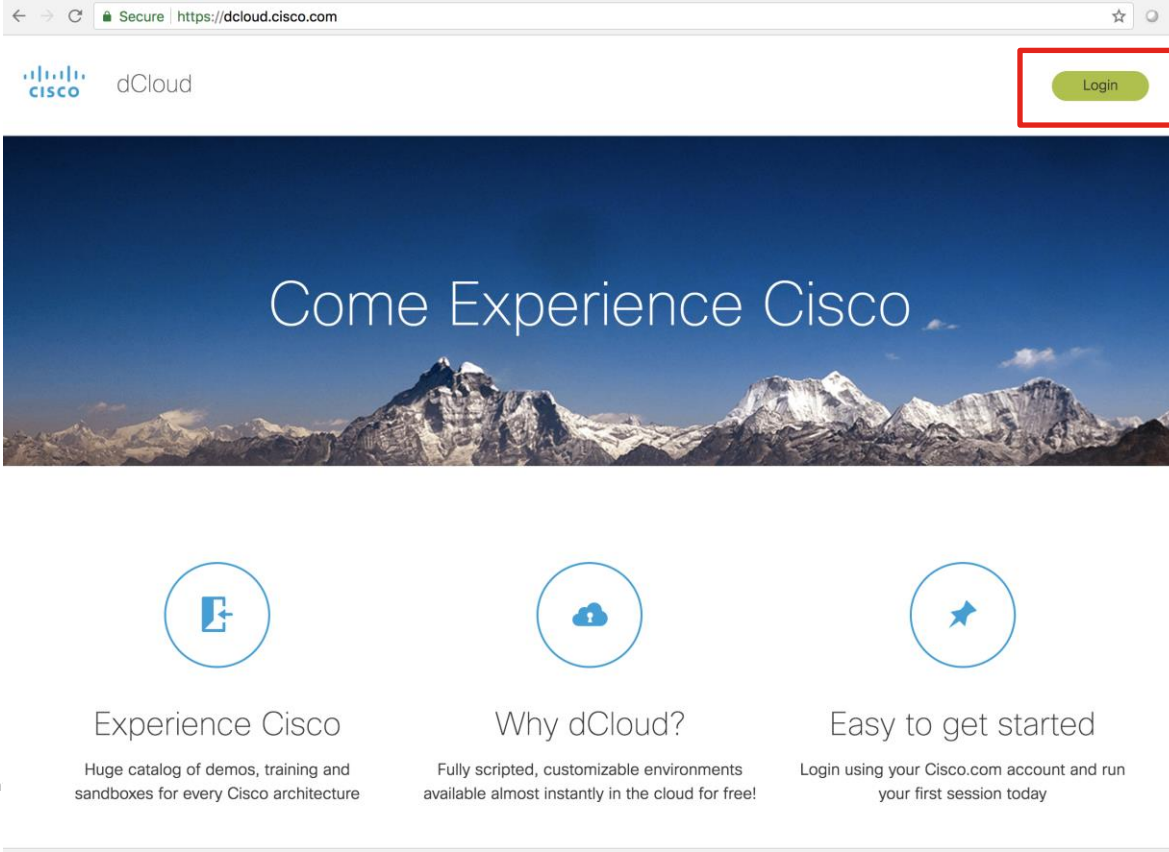
CiscoのSEからの情報をお知らせします。ディスカッションでは Cisco dCloudに関するQ&Aを日本語で受け付けています。  
※特定の製品に関するお問い合わせは、お急ぎの場合は dCloud.cisco.com の Support & Feedback ページより お問い合わせください。  
※ディスカッションで受け付けるQ&Aは、dCloud関連のみとなります。シスコ製品に関するお問い合わせ先は、こちらをご参照ください。



- サポートコミュニティの“システムズエンジニアリング”の項目で、dCloudに関するコンテンツや使い方などを紹介しています。

Subject	閲覧数	Comments	Author
Cisco dCloud Webinar 開催一覧	1	0	Akiko Horuchi
Cisco dCloud Webinar - Network as a Sensorソリューションのご紹介	56	0	Makoto Takeuchi
dCloud APJ コンテンツ一覧 - Collaboration	55	0	Akiko Horuchi

dcloud.cisco.comへアクセスし、ログインをクリック



The screenshot shows a web browser window with the address bar displaying "Secure | https://dcloud.cisco.com". The page header features the Cisco logo and the text "dCloud". A green "Login" button is highlighted with a red rectangular box. Below the header is a large banner image of a snow-capped mountain range with the text "Come Experience Cisco" overlaid. The main content area contains three columns, each with a circular icon and a heading:

- Experience Cisco**: Accompanied by a blue icon of a document with a plus sign. Below the heading is the text: "Huge catalog of demos, training and sandboxes for every Cisco architecture".
- Why dCloud?**: Accompanied by a blue icon of a cloud with a plus sign. Below the heading is the text: "Fully scripted, customizable environments available almost instantly in the cloud for free!".
- Easy to get started**: Accompanied by a blue icon of a star with a plus sign. Below the heading is the text: "Login using your Cisco.com account and run your first session today".

# 初回のみ：通常利用のデータセンタの指定

The screenshot shows the dCloud website interface. The navigation bar includes the Cisco logo, 'dCloud', 'My Hub', 'Catalog', 'Support', and 'News'. The main content area features a blue background with the text 'Please select your data center' and five circular buttons labeled 'APJ', 'EMEAR', 'GC', 'US East', and 'US West'. The 'APJ' button is highlighted with a red rectangular box. A blue dialog box titled 'Save preference?' is overlaid on the right side, containing 'Yes' and 'No' buttons. The 'Yes' button is also highlighted with a red rectangular box. At the bottom of the page, there are sections for 'About', 'Related Resources', and 'Follow Us', along with app store download buttons for the App Store and Google Play. A copyright notice is visible at the bottom left.

**About**  
Contact Us  
User Agreement  
Release Notes  
In Memorial

**Related Resources**  
Cisco.com account  
Cisco SalesConnect  
Proposal Expert Services  
Register for Bid Management  
Roadmaps

**Follow Us**  
Facebook  
Instagram  
Twitter  
YouTube

Download on the App Store  
GET IT ON Google Play

© 2018 Cisco and/or its affiliates. All rights reserved.

Save preference?  
Yes No

APJを選択し、  
Save PreferenceでYes

# ラボ予約

Catalogから”Firepower 6.3”で検索し、”Cisco Firepower Next-Generation Firewall 6.3 Features Lab v1.2”をスケジュール



dCloud

My Hub

Catalog

Support

News



1

Content Producers

dCloud

Proposal Expert Services

Content Categories

Demonstration

Instant Demo

Lab

Proposal

Solutions

Languages

## Catalog

Sort By **Relevance**



firepower 6.3



4 results in: "firepower 6.3"

**Cisco Firepower Next-Generation Firewall 6.3 Features Lab v1.2**

ID: 246083 Published Date: 04-Oct-2018 09:19 Lab Demonstration Security Policy and Access

Advanced Malware Protection Network Visibility and Enforcement Next-Gen Firewalls Next-Gen Intrusion Prevention System

Security Management VPN Security Clients English Japanese

In addition to quality and usability enhancements of 6.3, there are several new features. Those new features are the focus of this lab.

★ Favorite Related Documents

Schedule

# ラボ資料

スケジュールされたラボを選択し、Resourcesから”Japanese Localized Content (日本語)”をクリックして日本語の資料をダウンロード

Cisco Firepower Next-Generation Firewall 6.3 Features Lab v1.2

Details Servers **Resources** 1d 05:53:23

**Resources**

- Documentation
  - Firepower Next-Generation Firewall 6.3 Features Lab v1.2 Sandbox
  - Japanese Localized Content (日本語)**
- Additional Resources
- Localized Content
  - Japanese (日本語)

Search the Community

firepower 6.3 firepower 6.3等で検索

Technology & Support For Partners Customer Connection Events Members & Recognition

Did not find what you were looking for? Search this topic on Cisco.com

Type of Post Contains

- Japanese

- 2014-03-19 - Security Cisco Firepower Management Center 6.3 v1.4 - Instant Demo Demo Guide - Cisco Firepower Management Center ... v1.1 Cisco Firepower Management Center 6.2 Proof of Value v1 Proof of Value - FMC 6.2 Firepower on ASA ... Value - FMC 6.2 Firepower Threat Defense Cisco Stealthwatch 6.8 v1.1 Demo Guide - Cisco Stealthwatch ...  
Created by fju in Cisco Software Documents
- 8 ★
- Firepower Management Center 6.3 v1.4 - Japanese localized script %  
2019-03-18 -  
Created by andrewwa in Cisco Software Documents
- Cisco dCloud Translated Content - Korean
- 2016-01-21 - v1.1 Cisco Firepower Management Center 6.2 v1.2 Sandbox Demo Guide - Cisco Firepower Management Center ... v1.1 Cisco Firepower Management Center 6.2 Proof of Value v1 Proof of Value - FMC 6.2 Firepower on ASA ... Value - FMC 6.2 Firepower Threat Defense Cisco Cloudlock v1 - Instant Demo Demo Guide - Cisco Cloudlock ...  
Created by andrewwa in Cisco Software Documents
- Cisco Firepower Next-Generation Firewall 6.3 Features Lab v1.2 Japanese localized script %**  
2019-03-14  
Created by andrewwa in Cisco Software Documents

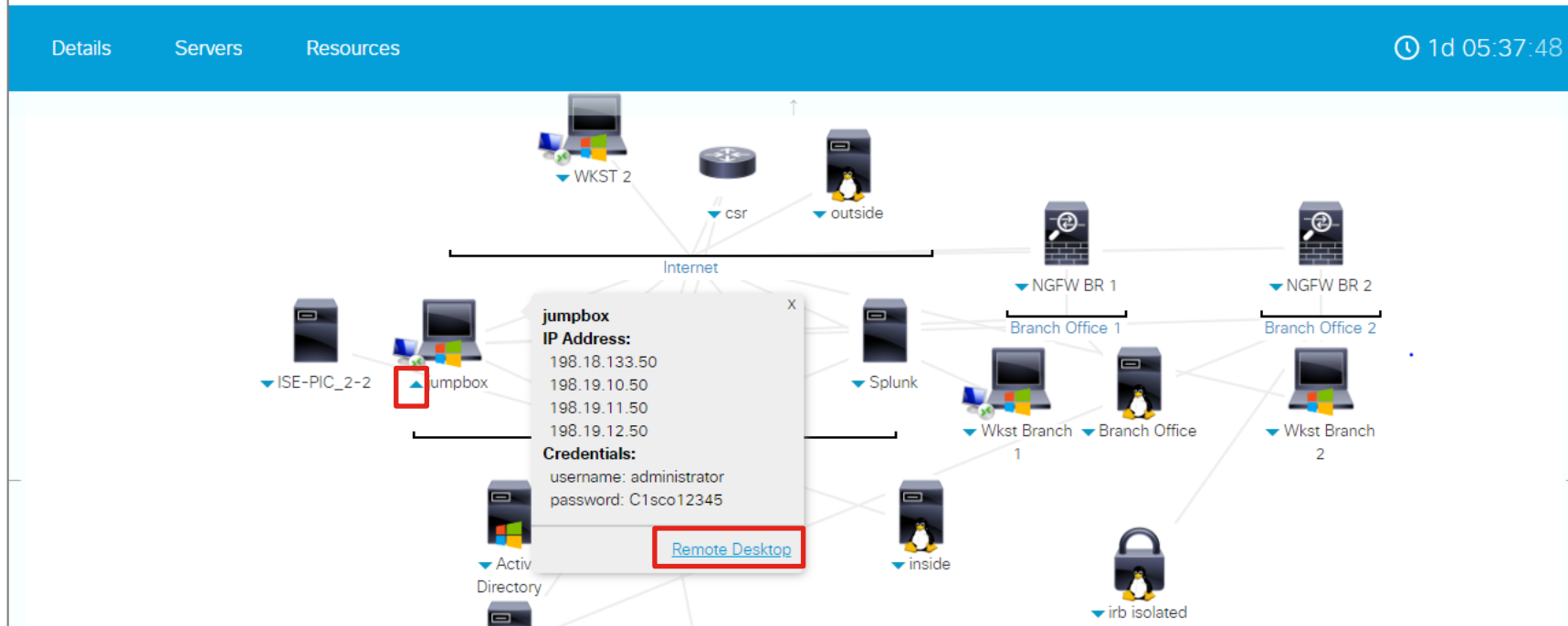
6.3 Features Lab v1.2 Japanese localized scriptをクリック

# ラボへのアクセス方法 (1)

Jumpboxメニューを展開し、Remote Desktopをクリック

※(1)か(2)のいずれか

Cisco Firepower Next-Generation Firewall 6.3 Features Lab v1.2



# ラボへのアクセス方法 (2)

DetailsタブのAnyConnect Credentialsを利用してAnyConnectでリモート接続を行い、jumpboxに直接リモートデスクトップ接続

※(1)か(2)のいずれか

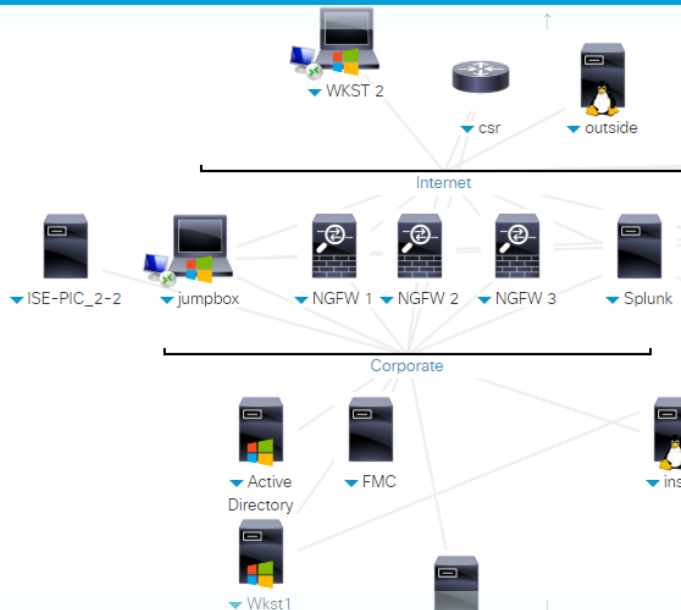
Cisco Firepower Next-Generation Firewall 6.3 Features Lab v1.2

Details

Servers

Resources

1d 03:04:33



## Session Details

VPN Available: true  
Virtual Center: 5

### AnyConnect Credentials

Connect up to 16 devices to the session via Cisco AnyConnect.

Host	dcloud-sjc-anyconnect.cisco.com
User	v1074user1
Password	d8eed7



# ラボシナリオのご紹介

# ラボシナリオ

※FDMシナリオとFMCシナリオは独立していますので  
どちらか片方のみでもお試し可能です

## FDMシナリオ

シナリオ1: FDM変更管理、RBAC、スマートCLIを使用したBGP設定

シナリオ2: FDMパッシブ認証、FQDN型オブジェクト

シナリオ3: FDM高可用性

## FMCシナリオ

シナリオ4: 統合イベント、状況に応じた相互起動、FQDN型オブジェクト

シナリオ5: リモートアクセスVPNの認可変更

シナリオ6: RMAのためのバックアップと復元

# ラボシナリオ

## FDMシナリオ

シナリオ1: FDM変更管理、RBAC、スマートCLIを使用したBGP設定

シナリオ2: FDMパッシブ認証、FQDN型オブジェクト

シナリオ3: FDM高可用性

## FMCシナリオ

シナリオ4: 統合イベント、状況に応じた相互起動、FQDN型オブジェクト

シナリオ5: リモートアクセスVPNの認可変更

シナリオ6: RMAのためのバックアップと復元

# Firepower Device Manager (FDM) の機能拡張

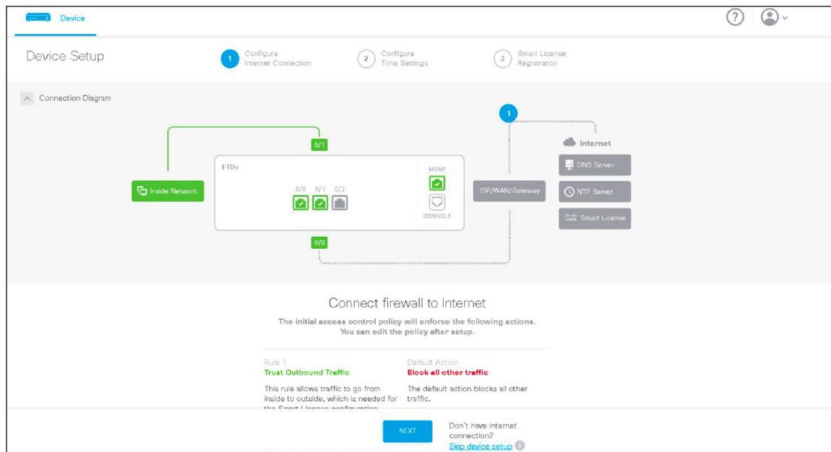
- FTD High Availability
- Passive Interfaces
- Passive Identity rules (ISE-PIC **のみサポート**)
- SmartCLI: BGP Routing; OSPF2 Route Map, Prefix List, ACL
- RAVPN **用のローカルユーザ** DB, Access & TLS Policies
- RAVPN: **二要素認証や証明書認証を伴う RADIUS 認証**
- RBAC (R/O, R/W, Admin roles) **を伴う外部 RADIUS 認証**
- **管理機能の追加**: Pending Preview/Copy/Discard, Audit/History

# シナリオ1: FDM変更管理、RBAC、スマートCLIを使用したBGP設定

## 本シナリオでの体験内容

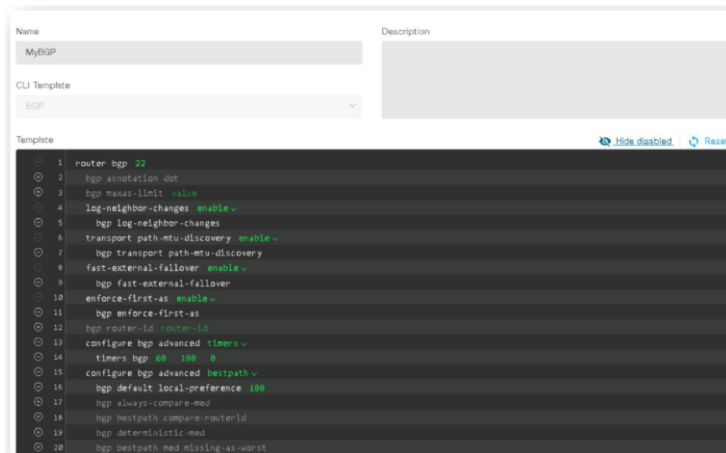
- FDMでの初期セットアップおよび基本設定
- FDM スマートCLIを使用したBGPの設定とテストの実施
- FDMでのRADIUS認証を使用したロールベースアクセス制御の設定とテストの実施

## FDM



The screenshot shows the FDM 'Device Setup' interface. It includes a progress bar with three steps: 'Configure Internet Connection' (completed), 'Configure Time Settings', and 'Smart License Registration'. A connection diagram shows the FDM device connected to various services. Below the diagram, there are instructions to 'Connect firewall to Internet' and a 'next' button.

## スマートCLI



The screenshot shows the Smart CLI interface for a BGP configuration. The 'Name' field is 'MyBGP' and the 'CLI Template' is 'BGP'. The template content is a BGP configuration script:

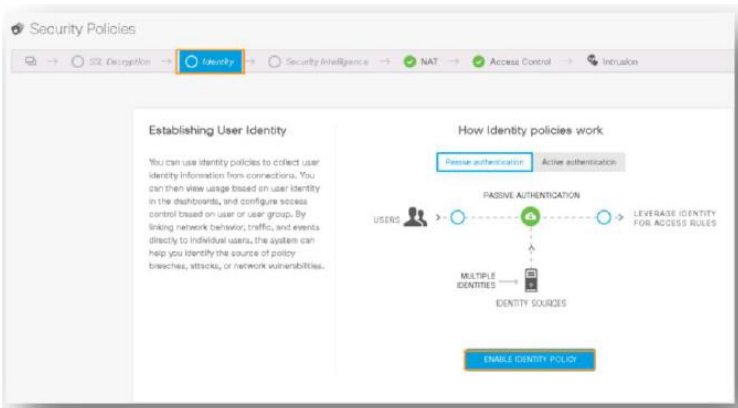
```
1 router bgp 22
2  bgp announcement dot
3  bgp max-as-limit value
4  log-neighbor-changes enable
5  bgp log-neighbor-changes
6  transport path-mtu-discovery enable
7  bgp transport path-mtu-discovery
8  fast-external-fallover enable
9  bgp fast-external-fallover
10 enforce-first-as enable
11 bgp enforce-first-as
12 bgp router-id router-id
13 configure bgp advanced timers
14 timers bgp 60 100 0
15 configure bgp advanced bestpath
16 bgp default local-preference 100
17 bgp always-compare-med
18 bgp bestpath compare-routerid
19 bgp deterministic-med
20 bgp bestpath med missing as worst
```

## シナリオ2: FDMパッシブ認証、FQDN型オブジェクト

### 本シナリオでの体験内容

- FDMでのパッシブ認証の設定
- FDMでのFQDN型オブジェクトとアクセスポリシーの作成
- ユーザーアイデンティティおよび宛先FQDNに渡されたトラフィックアクセスのテスト

### パッシブ認証



### FQDN型オブジェクトを利用したアクセスポリシー(イメージ)

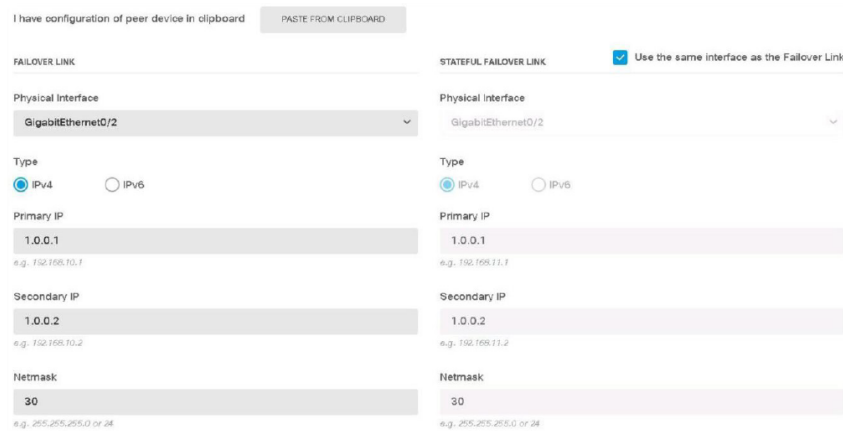
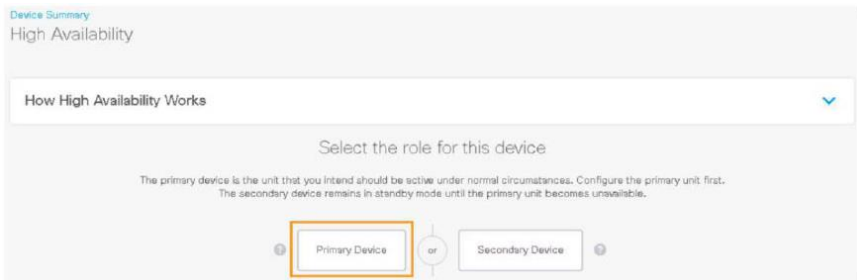


# シナリオ3: FDM高可用性

## 本シナリオでの体験内容

- FDMでのHA(Active/Standby)設定
- FailoverおよびHA解除のテスト

## FDMでのHA設定画面




## 注意! シナリオ3: FDM高可用性 ラボ資料の誤りについて

P.41 NGFW3のHA設定手順にて以下の記述ミスがあります。

誤: 9. このデバイスの HA ロールとして [プライマリデバイス (Primary Device)] を選択します。

正: 9. このデバイスの HA ロールとして [セカンダリデバイス (Secondary Device)] を選択します。

※誤って設定してしまった場合にはHA設定画面内の  より Break HAを選択し、HA構成を一旦解除して再設定ください



# ラボシナリオ

## FDMシナリオ

シナリオ1: FDM変更管理、RBAC、スマートCLIを使用したBGP設定

シナリオ2: FDMパッシブ認証、FQDN型オブジェクト

シナリオ3: FDM高可用性

## FMCシナリオ

シナリオ4: 統合イベント、状況に応じた相互起動、FQDN型オブジェクト

シナリオ5: リモートアクセスVPNの認可変更

シナリオ6: RMAのためのバックアップと復元

# シナリオ4： 統合イベント、状況に応じた相互起動、FQDN型オブジェクト

## 本シナリオでの体験内容

- FMCでのFQDN型オブジェクトを使用したアクセスポリシーの設定とSyslogサーバー(Splunk)への接続イベント送信設定
- FMCでのSplunkとの相互起動設定とテスト

## SplunkとのContextual Cross-launch

Connections with Application Details > Table View of Connection Events

No Search Constraints (Edit Search)

Jump to...

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone
↓	2018-10-04 18:45:38	2018-10-04 18:45:38	Block	File Block	198.19.10.200		198.18.133.200		InZone
↓	2018-10-04 18:45:37	2018-10-04 18:45:38	Block	Intrusion Block	198.19.10.200		198.18.133.200		InZone
↓	2018-10-04 18:45:37	2018-10-04 18:45:37	Allow	Intrusion Monitor	198.19.10.200		198.18.133.200		InZone
↓	2018-10-04 18:45:37		Block with reset		198.19.10.200		198.18.133.202		InZone
↓	2018-10-04 18:45:37		Block with reset		198.19.10.200		198.18.133.202		InZone
↓	2018-10-04 18:45:37		Block with reset		198.19.10.200		198.18.133.202		InZone
↓	2018-10-04 18:45:37		Block with reset		198.19.10.200		198.18.133.201		InZone
↓	2018-10-04 18:45:37		Block with reset		198.19.10.200		198.18.133.201		InZone

Query Packet Analyzer

Splunk Source IP

```
splunk>enterprise
```

```
18/4/18 3:45:26:000PM [MFTD-6-40003 Protocol tcp, SrcIP: 198.19.10.200, DestIP: 198.18.133.200, SrcPort: 37244, DestPort: 80, IngressZone: InZone, EgressZone: OutZone, Policy: B...  
No Authentication Required, UserAgent: MFTD/1.14 (Linux-gnu), Client: MFTD, ClientVersion: 1.14 (Linux-gnu), ApplicationProtocol: HTTP, InitiatorPackets: 8,  
ResponderPackets: 8, InitiatorBytes: 650, ResponderBytes: 6009, MPPolicy: Balanced Security and Connectivity, HTTPResponse: 200, ReferencedHost: outside, U  
R: http://enr.splunk.com/files/STIX.xml
```

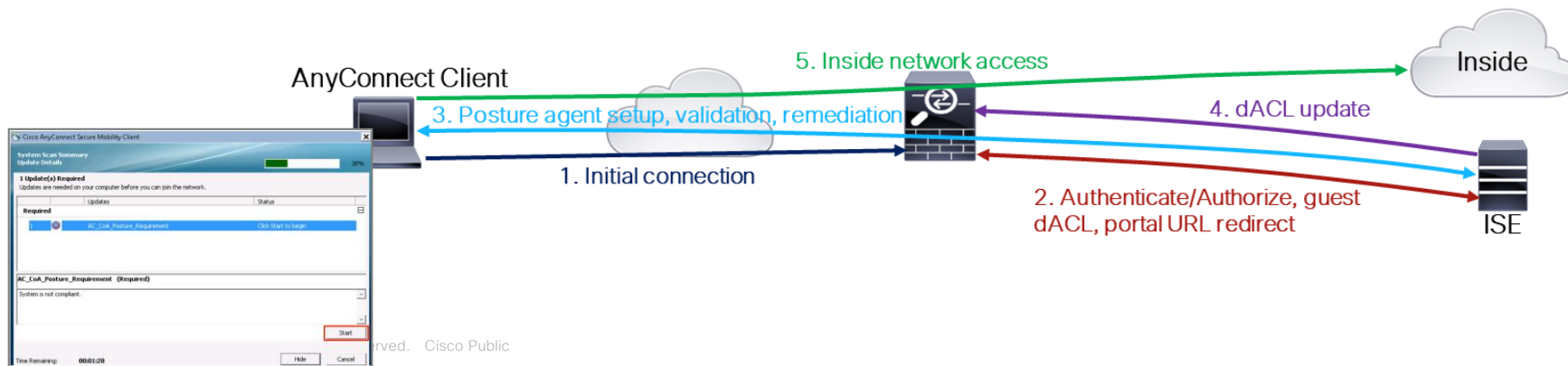
```
host = 198.18.10.1 index = main _sourcetype = splunk sourcetype = splunk splunk_server = splunkvirtual-machine timestamp = none
```

# シナリオ5: リモートアクセスVPNの認可変更

## 本シナリオでの体験内容

- FMCでのリモートアクセスVPNのポスチャ評価と認可変更 (Change of Authorization)に必要なオブジェクトの作成
- FMCでのリモートアクセスVPNセットアップウィザードの実行
- リモートアクセスVPNのポスチャ評価と認可変更のテスト

## RA VPN CoA



## シナリオ6: RMAのためのバックアップと復元

### 本シナリオでの体験内容

- FMCで管理されているFTD(NGFW1)のバックアップ取得
- NGFW1号機のシャットダウン(障害シミュレート)
- 別FTD筐体(NGFW3)への復元

6.3ではFTDのデバイス設定(インターフェースやルーティング設定等)を含むバックアップ取得が可能となった  
注意点:

- クラスタ構成は未サポート
- FP4100/9300のFXOS部分は個別のバックアップが必要
- FMCよりバックアップオペレーションを実施し、リトリーブは各デバイスで実施
- リストアのオペレーションは各デバイスで実施
- リストアにおいてHWモデル、SWバージョン、VDBバージョンを一致していなければならない
- FlexconfigやVPN設定はマニュアルでの再設定が必要になる場合がある(警告メッセージが表示)
- リストア後、証明書は再エンロールメントが必要

# 参考資料 (1)

- Firepower への cisco.comでのショートカット  
<http://www.cisco.com/go/ngfw>
- パートナーサポート
  - 最新資料 (FTD 初期設定ガイド、ASA on FP4k2k ガイド公開中)  
[https://www.cisco.com/c/m/ja\\_jp/partners/documents.html](https://www.cisco.com/c/m/ja_jp/partners/documents.html)
  - セキュリティ技術資料  
[https://www.cisco.com/c/ja\\_jp/partners/sell-integrate-consult/technology/security.html](https://www.cisco.com/c/ja_jp/partners/sell-integrate-consult/technology/security.html)
- シスコサポートコミュニティ 日本語 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 6.3.0 の機能解説を、3回に渡って掲載
  - 新機能満載の Cisco Firepower 6.3.0 をリリースしました その1  
<https://gblogs.cisco.com/jp/2018/12/fp630-release-1/>
  - 新機能満載の Cisco Firepower 6.3.0 をリリースしました その2  
<https://gblogs.cisco.com/jp/2018/12/fp630-release-2/>
  - 新機能満載の Cisco Firepower 6.3.0 をリリースしました その3 (最終回)  
<https://gblogs.cisco.com/jp/2018/12/fp630-release-3/>

Cisco Japan Blog

Cisco Japan Blog > セキュリティ

セキュリティ  
新機能満載の Cisco Firepower 6.3.0 をリリースしました その1

小林 達哉  
2018年12月12日

アメリカ時間の 2018/12/04 に、NGIPS / NGFW / Anti-Malware である Cisco Firepower のソフトウェアバージョン 6.3.0 がリリースされました。

直近のバージョン 6.2.3 は、品質改善に多くのエンジニアリング リソースを投入したため、それほど大きな機能拡張はありませんでしたが、このバージョン 6.3.0 は多くの新機能を追加しており、また、今までにご意見をいただいた箇所の改善も多く高めています。

詳細は、こちらのリリースノートをご覧ください。>

当ブログでは、数回に分けて、いくつかの新機能について、わかりやすく解説していきます。今回は、以下の 2 点について、解説します。

- Firepower 6.3.0 が動作するプラットフォーム
- マルチインスタンス

Firepower 6.3.0 が動作するプラットフォーム

プラットフォーム一覧がリリースノートにまとまっておりますので、こちらをご確認ください。

