



Firepower System

- 概要とトラブルシューティング -

八角 卓哉(Takuya Yasumi)

テクニカルアシスタンスセンター, テクニカルサービス

September 13, 2016



ご参加ありがとうございます

本日の資料はこちらからダウンロードいただけます

<http://supportforums.cisco.com/ja/community/5356/webcast>

オンラインセミナー (Live Expert Webcast)



ASR 1000 シリーズルータ のアーキテクチャーとトラブルシューティング

日程：2016年 9月13日（火） 10:00 - 11:45

スピーカー：八角 卓哉(Takuya Yasumi)

シスコ テクニカルアシスタンスセンター、テクニカルサービス

[セッション概要]

[セミナー内容] Firepower system/ASA with FirePOWERの概要と基本的なトラブルシューティング方法について解説いたします。本セミナーは、業務でFirepower systemやASA with FirePOWERに携わる方や導入を検討されている方に効果的です。アジェンダは以下のとおりです。

1. Firepower systemの機能概要
2. Firepower systemとASA with FirePOWERの構成(通信、ソフトウェア、ライセンス、ポリシー等)
3. トラブルシューティングの手順やコマンド紹介
4. 事例の紹介

本セミナーではFirePOWERに焦点を絞るため、ASA with FirePOWERについてはASAの基礎知識を前提とし、ASAについての解説は省略いたします。

[詳細・登録はこちら](#)

[資料のダウンロード](#) [エキスパートに質問 \(9/14 - 9/25\)](#)

直接ダウンロードする場合はこちら

<https://supportforums.cisco.com/ja/document/13118621>

オーディオブロードキャストについて

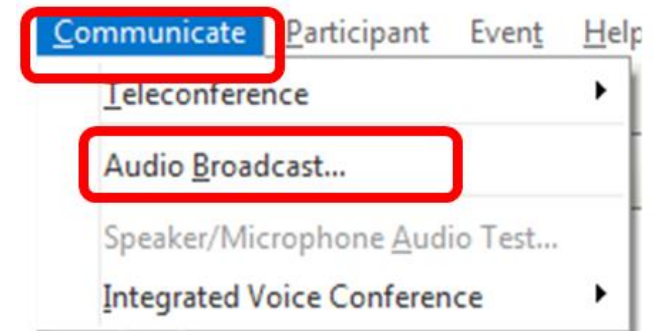
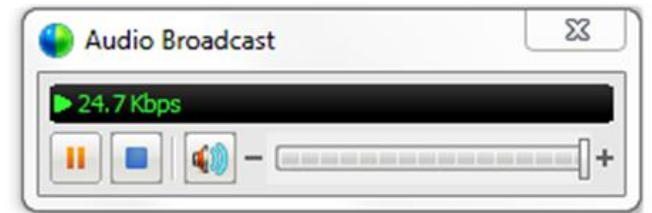
[Audio Broadcast (オーディオブロードキャスト)] ウィンドウが自動的に表示され、コンピュータのスピーカーから音声がかかります

[Audio Broadcast (オーディオブロードキャスト)] ウィンドウが表示されない場合は、[Communicate (コミュニケーション)] メニューから [Audio Broadcast (オーディオブロードキャスト)] を選択します

イベントが開始されると自動的に音声が流れ始めます

音声接続に関する詳細はこちらをご参照ください。解決しない場合は、QA ウィンドウよりお知らせください。

<https://supportforums.cisco.com/ja/document/82876>

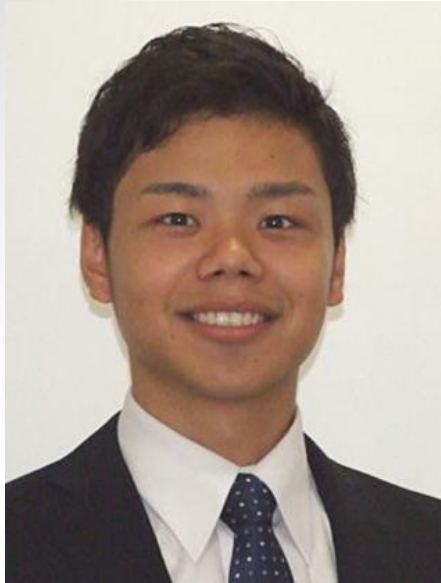




ご質問方法

Webcast 中のご質問は全て画面右側のQAウィンドウより All Panelist 宛に送信してください

エキスパートスピーカー



八角 卓哉(Takuya Yasumi)
テクニカルアシスタンスセンター,
テクニカルサービス
カスタマー サポート エンジニア



Firepower System

- 概要とトラブルシューティング -

八角 卓哉 (Takuya Yasumi)

テクニカルアシスタンスセンター, テクニカルサービス

September 13, 2016

Agenda

1. 目的
2. イントロダクション
3. Firepower System / ASA with FirePOWERの概要
4. トラブルシューティングに役立つ情報とその取得方法

Agenda

1. 目的
2. イントロダクション
3. Firepower System / ASA with FirePOWERの概要
4. トラブルシューティングに役立つ情報とその取得方法

目的

Firepower System / ASA with FirePOWERの構築・保守・運用に際して

把握していると有用と思われる知識

トラブルの調査に役立つ情報

をご案内し、今後の業務で活用していただく。

投票質問1

Firepower System / ASA with FirePOWER
についての知識をお答えください

1. 実機操作の経験がある (構築・保守・運用など)
2. 実機操作の経験はないが、業務に関わり、ある程度の知識がある
3. 実機操作の経験はなく、業務に関わりもないが、多少の知識がある
4. 現時点では全く知らない

Agenda

1. 目的
2. イントロダクション
3. Firepower System / ASA with FirePOWERの概要
4. トラブルシューティングに役立つ情報とその取得方法

Firepower Systemの特徴

- 不正アクセスの検知・防御システム(Intrusion Prevention System)
 - 追加セキュリティ対策: FireWallでは防げない攻撃を防御
 - 出口対策: マルウェア感染後のC&C通信等を検知
- IPSの業界標準であるSnortをコアエンジンに使用
- 自動チューニングにより運用負荷を低減



機能概要

NGIPS 次世代IPS

- 可視化
(ネットワーク / ホスト / 脆弱性等)
- 自動チューニング
- インパクト解析
- 侵入痕跡 / IOC
(C&C通信、マルウェア感染等)

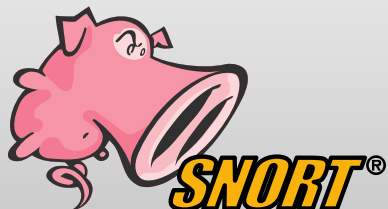
NGFW 次世代Firewall

- アプリケーション識別
- ユーザ識別
- URL フィルター
- ジオロケーション

AMP Advanced Malware Protection

- マルウェア防御
- クラウドサンドボックス
- 侵入 / 拡散経路の解析
(ファイルトラジェクトリ)
- 過去の攻撃の解析
(レトロスペクティブセキュリティ)

SNORT



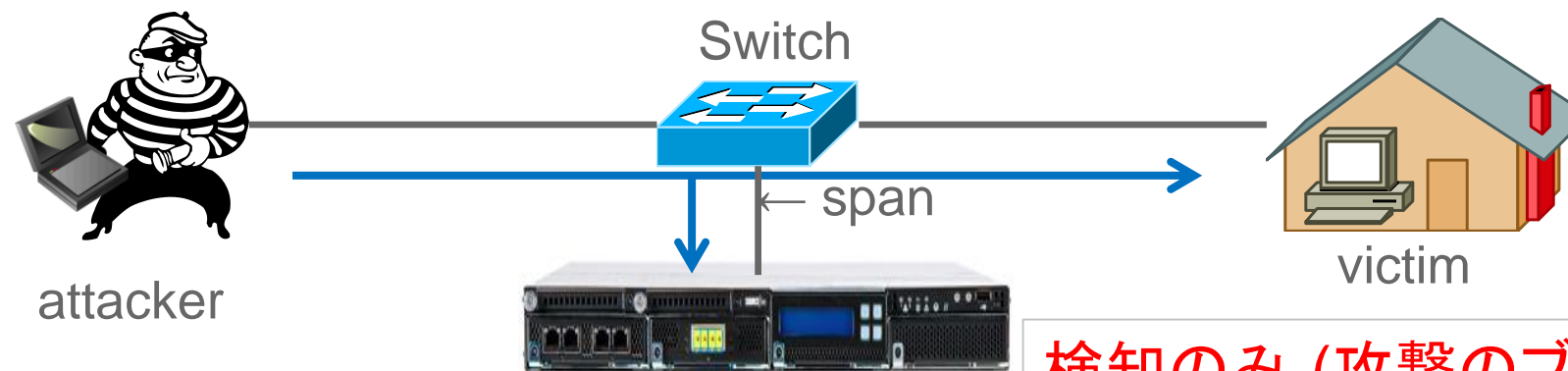
- ✓ オープンソース (SNORTコミュニティ)
- ✓ 業界標準エンジン: 世界で最も使われているIPS
- ✓ シグニチャ検知

Firepower Systemの導入構成

- **Inline**: 通信経路上にある (Cisco IPS の Inline mode と同じ)



- **Passive**: 通信経路上にない (Cisco IPS の promiscuous mode と同じ)



検知のみ (攻撃のブロックは不可)

Firepower Systemの構成

Firepower Management Center (FMC)

複数台のFirepower
を管理可能



- ポリシー・設定の変更
- ソフトウェアアップデート
- ライセンスの適用
- バックアップの実施

- 検出イベントの転送
- Deviceのヘルス情報の転送

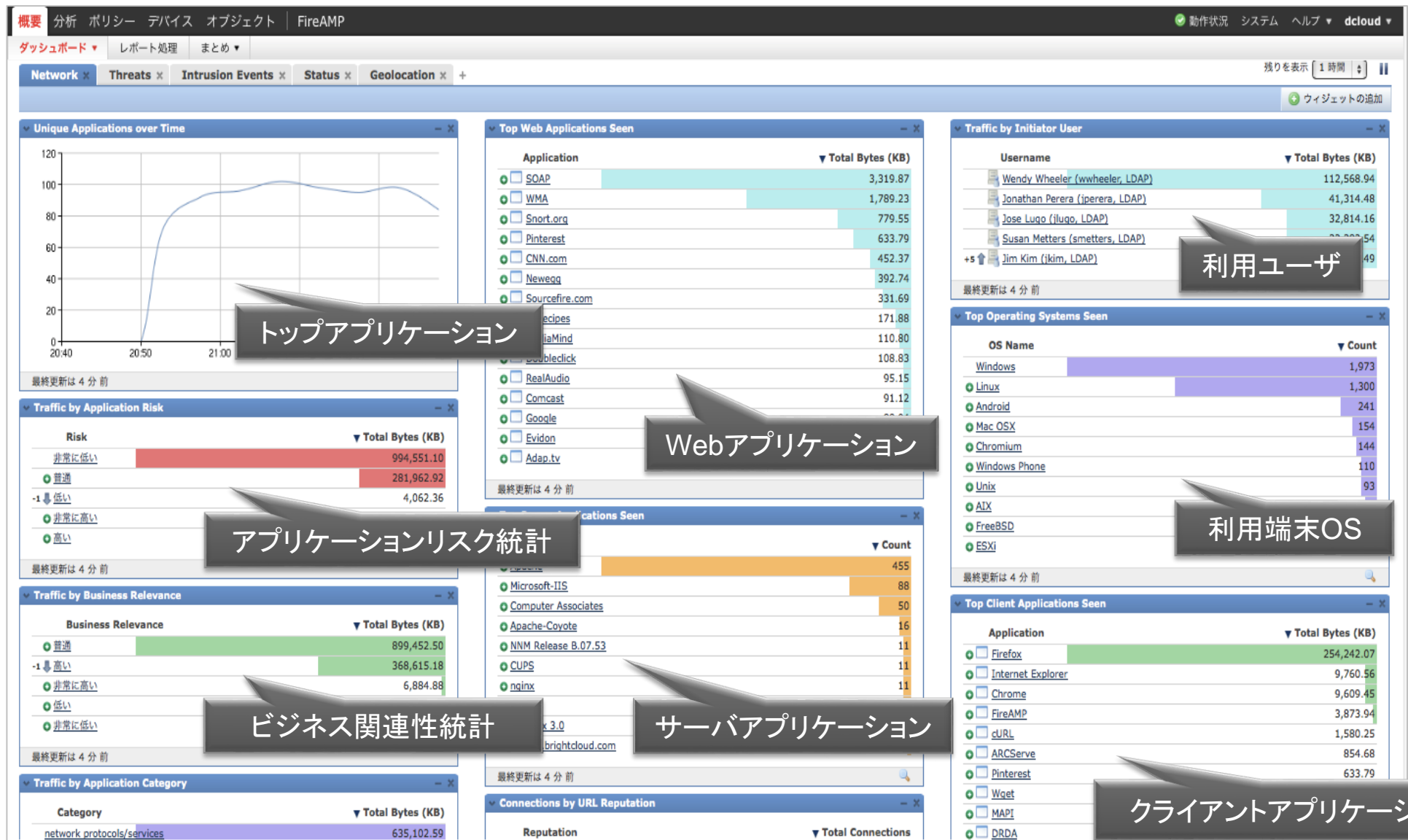


Firepower



FMCのダッシュボード画面

例)アプリケーション識別



FMCのダッシュボード画面

例) 脅威

The screenshot displays the Cisco FMC dashboard with several key sections:

- Summary Dashboard:** Overview of activity on the appliance, including tabs for Network, Threats, Intrusion Events, Status, and Geolocation.
- Indications of Compromise (3):** A table listing specific events:

Category	Event Type	Description	First Seen	Last Seen
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2013-09-17 16:46:28	2013-09-20 06:35:31
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2013-09-17 16:52:11	2013-09-20 03:55:45
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2013-09-17 20:09:23	2013-09-19 17:32:49
- Indications of Compromise by Host:** A table showing IP addresses and their counts, with 10.110.10.69 highlighted as having 2 incidents.

IP Address	Count
10.110.10.69	2
10.112.10.78	2
10.120.10.200	2
10.131.11.230	2
10.131.15.217	2
172.16.0.128	2
172.16.141.58	2
192.168.0.154	2
10.0.37.126	1
10.0.37.111	1
- Security Intelligence Category:** A bar chart showing total connections for various categories like Bots (1,092), Malware (569), and Boqon (463).
- Traffic by Security Intelligence Category:** A bar chart showing total bytes for categories like Open_relay (13,958.55 KB) and Bots (13,610.43 KB).
- Intrusion Events:** A series of charts showing event counts over time, with a callout for '残り1時間' (Remaining 1 hour).
- Malware Threats:** A table listing threat names and counts, such as W32.Trojan.Breach.VRT (53) and W32.CD13C635C6-73.S\$X.VIOC (50).

Callouts on the dashboard highlight specific areas:

- 感染の痕跡のあるホスト:** Points to the 'Indications of Compromise by Host' table.
- 検出マルウェア:** Points to the 'Malware Threats' table.
- 侵入検知イベント:** Points to the 'Intrusion Events' charts.
- 不正トラフィック:** Points to the 'Traffic by Security Intelligence Category' chart.



アプライアンスを示す用語

Firepower Management Center



- FireSIGHT / FS
- Defense Center / DC
- FireSIGHT Management Center / FMC
- Firepower Management Center / FMC

Firepower



- FirePOWER (Firepower) / FP
- Sensor
- Managed Device

ドキュメントや不具合の検索時に注意

Agenda

1. 目的
2. イントロダクション
3. Firepower System / ASA with FirePOWERの概要
4. トラブルシューティングに役立つ情報とその取得方法

Firepower System と ASA with FirePOWER の概要

- 製品
- 通信
- ソフトウェアコンポーネント
- ライセンス
- ポリシー

Firepower System

- アプライアンス (Firepower 7000 & 8000 series device / FMC)
- 仮想アプライアンス
- ASA with FirePOWER (ASA55xx-X)

FirePOWER の機能を、実績のある ASA ファイアウォールにモジュール搭載

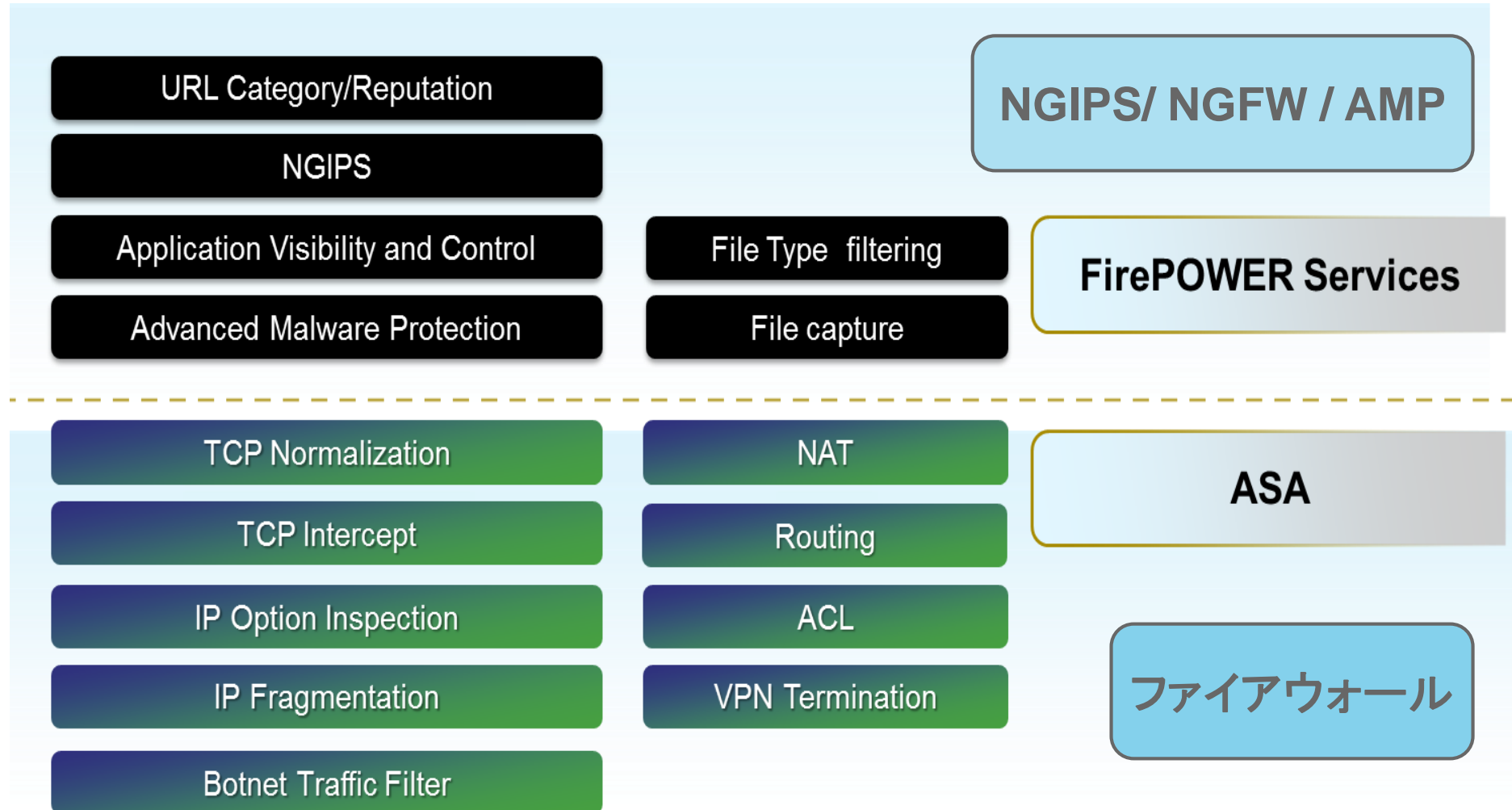
**FirePOWER Services for
Cisco ASA 5500-X (Software)**



**FirePOWER Services for
Cisco ASA 5585-X (Blade)**



ASA with FirePOWER (ASA 55xx-X)



Firepower System アプライアンス

NEW Firepower 9300
20Gbps-90Gbps



Firepower Management Center



FS 750
10 Sensors



FS 2000/4000
70 / 300 Sensors

NEW

Firepower 4100
10Gbps-20Gbps



Firepower 8200/8300
10Gbps-60Gbps

Firepower 8100/8200
2 Gbps-10 Gbps

Firepower 7100/8100
1 Gbps-2 Gbps

Firepower 7100
500 Mbps – 1Gbps

Firepower 7000
50-250Mbps
Small Office

Branch Office

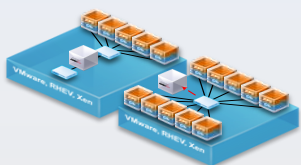
Internet Edge

Campus

Data Center

Firepower 7000 & 8000 series device

仮想アプライアンス



NGIPSv
FMC Virtual



※ Firepower 4100 / 9300 では Firepower Threat Defense Software / ASA Software をサポート

ASA with FirePOWER



On-Box Management

ASDMを用いてFirePOWERモジュールの管理が可能 (FMC不要)

Ver. 5.4+
On-Box Management 可能

ASA 5506-X



ASA 5508-X



ASA 5516-X



ASA 5512-X



ASA 5515-X



ASA 5525-X



ASA 5545-X



ASA 5555-X



ASA 5585-X SSP-20



ASA 5585-X SSP-10



ASA 5585-X SSP-40



ASA 5585-X SSP-60



Ver. 6.0+ On-Box Management 可能

Branch Office

Internet Edge

Campus

Data Center

ASDM画面 (On-Box Management)



Home Configuration Monitoring Save ASA Changes Refresh Back Forward Help Type topic Go

ASA FirePOWER Configurat... Configuration > ASA FirePOWER Configuration > Device Management > Device

Sourcefire3D
ASA5506W

Device Interfaces

General

Name: Sourcefire3D

System

Model: ASA5506W
Serial: JAD1833002T
Time: 2015-02-06 11:23:28
Version: 5.4.1
Policy: [Initial_System_Policy_2015-02-02_18:02:17](#)

Advanced

Application Bypass: No
Bypass Threshold: 3000 ms

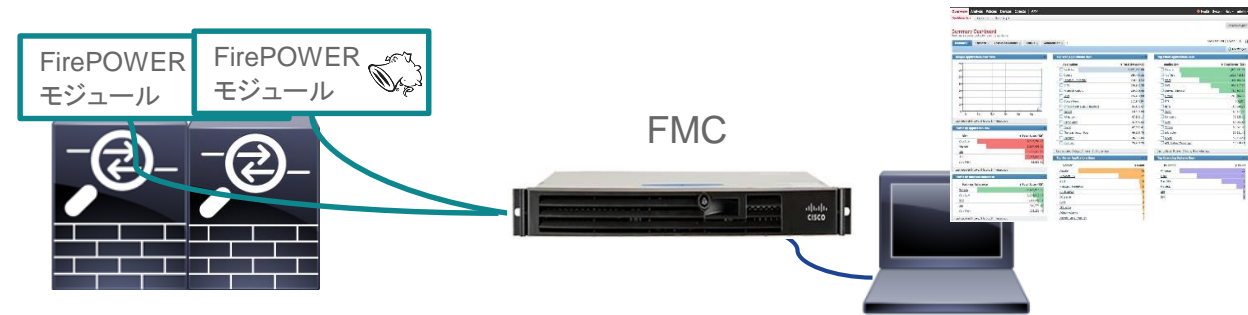
Apply ASA FirePOWER Changes

Device Setup
Firewall
Remote Access VPN
ASA FirePOWER Configur...
Device Management

ASA with FirePOWERの管理

On-Box Management と FMC Management の違い

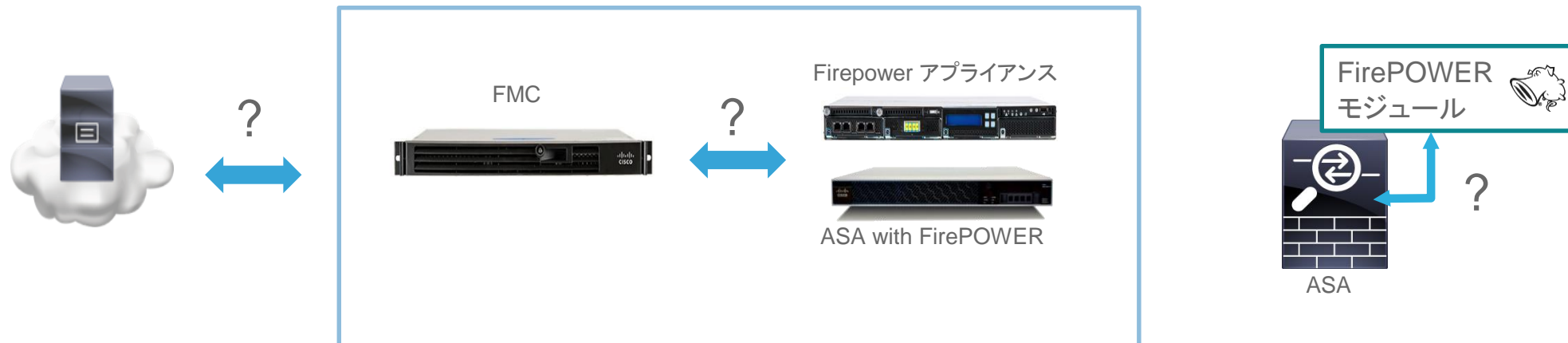
On-Box(ASDM) Management	FMC Management
<ul style="list-style-type: none">ASDM UI単一デバイスを管理Dashboard は固定FMC の機能が制限される	<ul style="list-style-type: none">FMC UI複数デバイスを管理可能Dashboardをカスタマイズ可能FMC の全機能が使用可能



Firepower Systemの通信

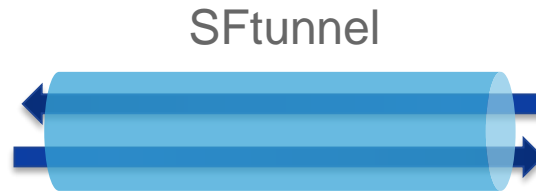
Firepower Systemの通信

- Firepower (FirePOWER モジュール) と FMC 間の通信
- Firepower System の外部ネットワークとの通信
- ASA with FirePOWERの内部通信



Firepower と FMC 間の通信

SFtunnel を利用した通信



Firepower アプライアンス

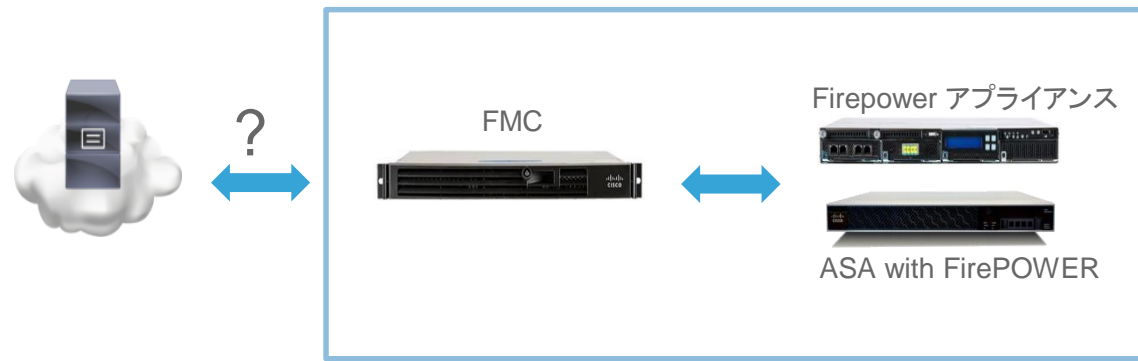


ASA with FirePOWER

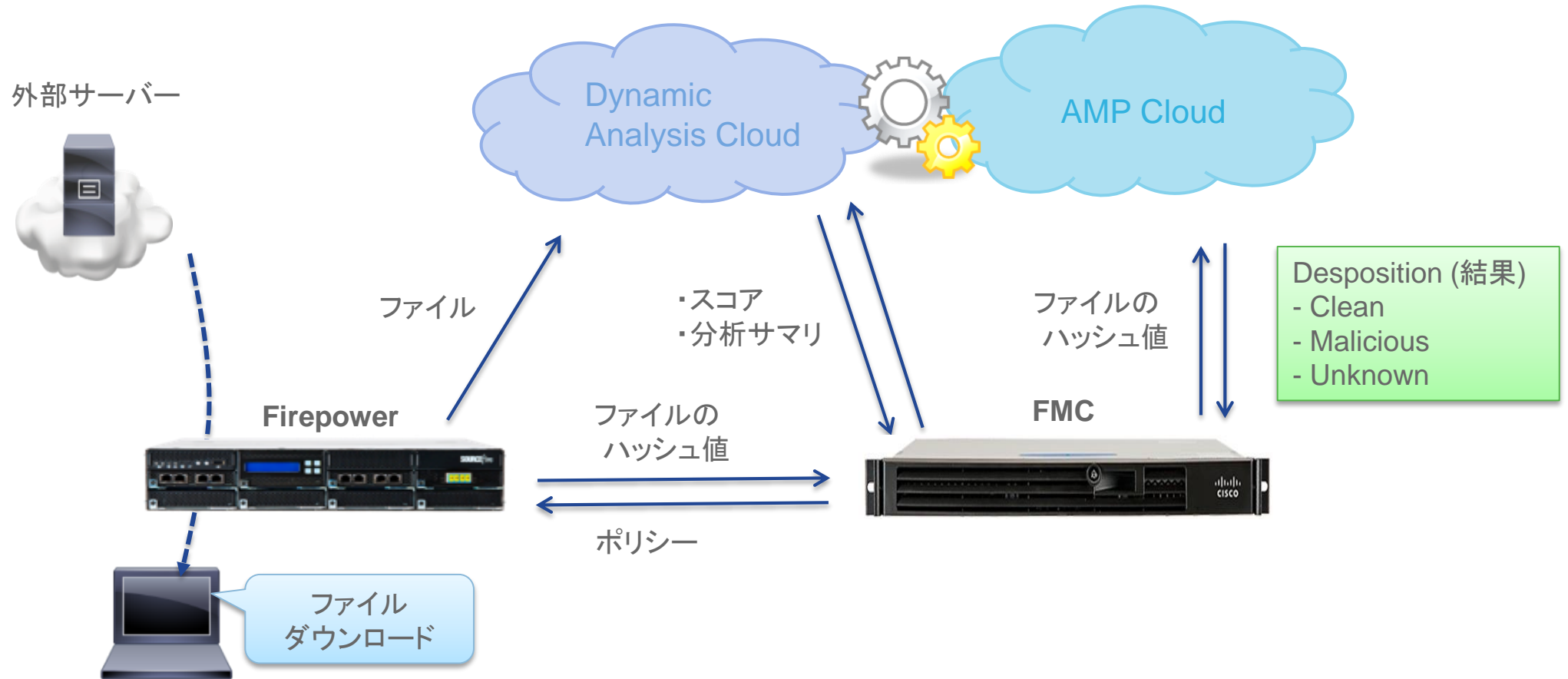
- OpenSSLを使用したトンネルを形成し安全な通信を実現
- TCP ポート番号 8305
- アプライアンス/ASA with FirePOWERともに使用
(Management interfaceのみ使用可能)

外部ネットワークとの通信

- ソフトウェアやデータベースの自動アップデート
- NTP / DNS
- Syslog / SNMP / Email alert など
- Cloud look-up (マルウェアの検知・分析 / Unknown URLの問い合わせ)



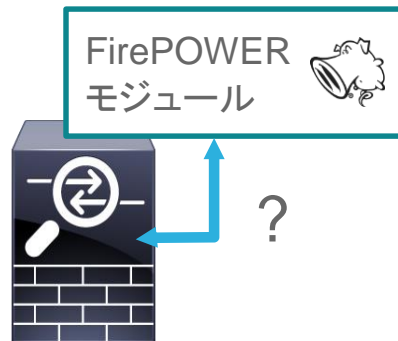
Cloud Look-up (マルウェアの検知・分析)



クラウドデータベースへ問い合わせによりマルウェアを検知・防御
ダイナミック分析機能により、未知のファイルを継続解析

Firepower Systemの通信

- Firepower (FirePOWER モジュール) と FMC 間の通信
- Firepower System の外部ネットワークとの通信
- ASA with FirePOWERの内部通信



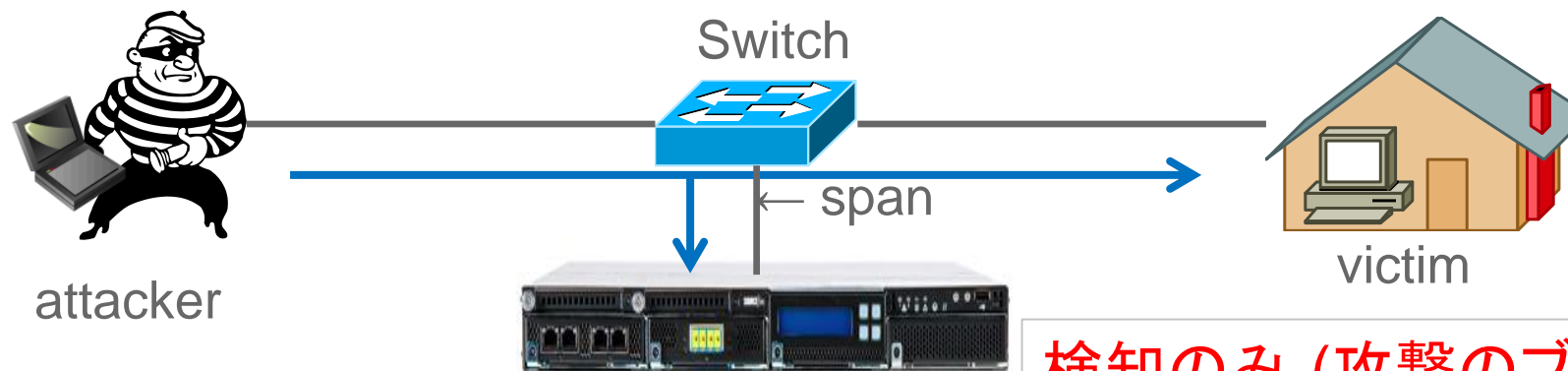
(参考) Firepower System の導入構成

- Firepower アプライアンス利用時-

- **Inline**: 通信経路上にある (Cisco IPS の Inline mode と同じ)



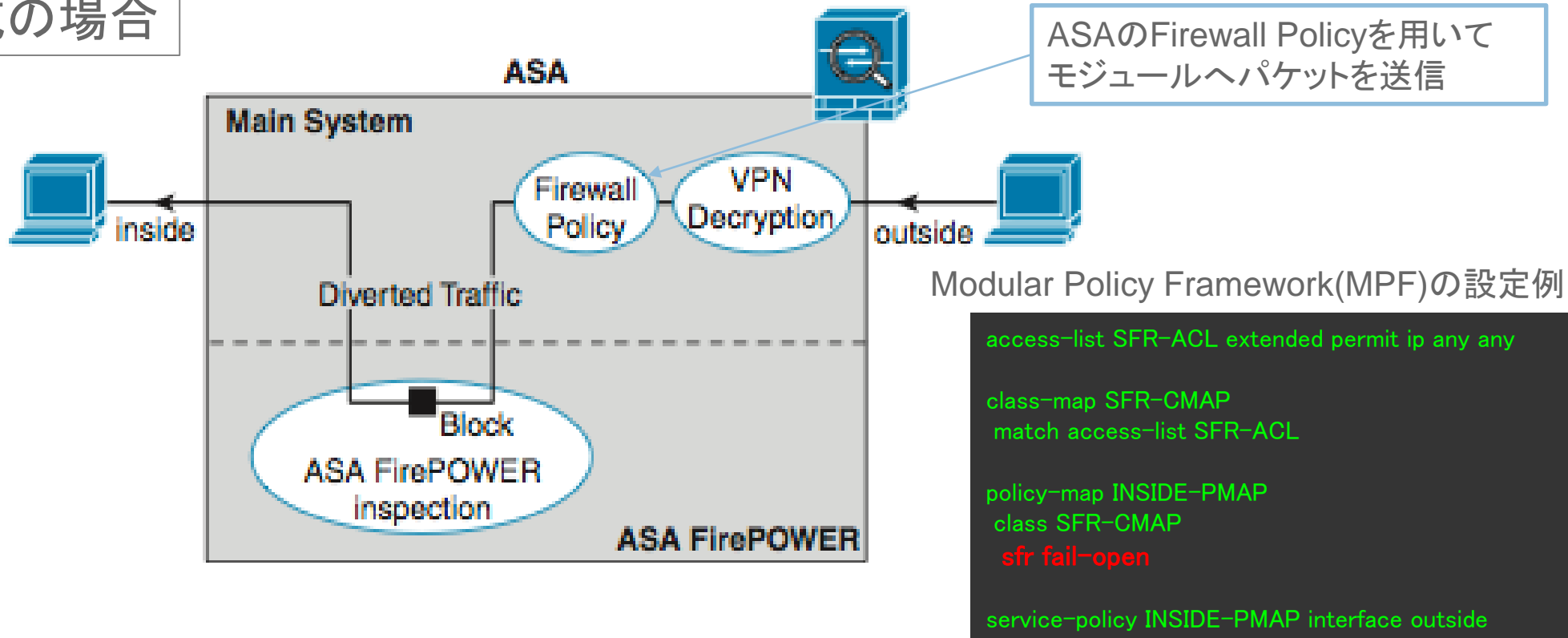
- **Passive**: 通信経路上にない (Cisco IPS の promiscuous mode と同じ)



検知のみ (攻撃のブロックは不可)

ASAとFirePOWERモジュール間の通信

Inline 構成の場合

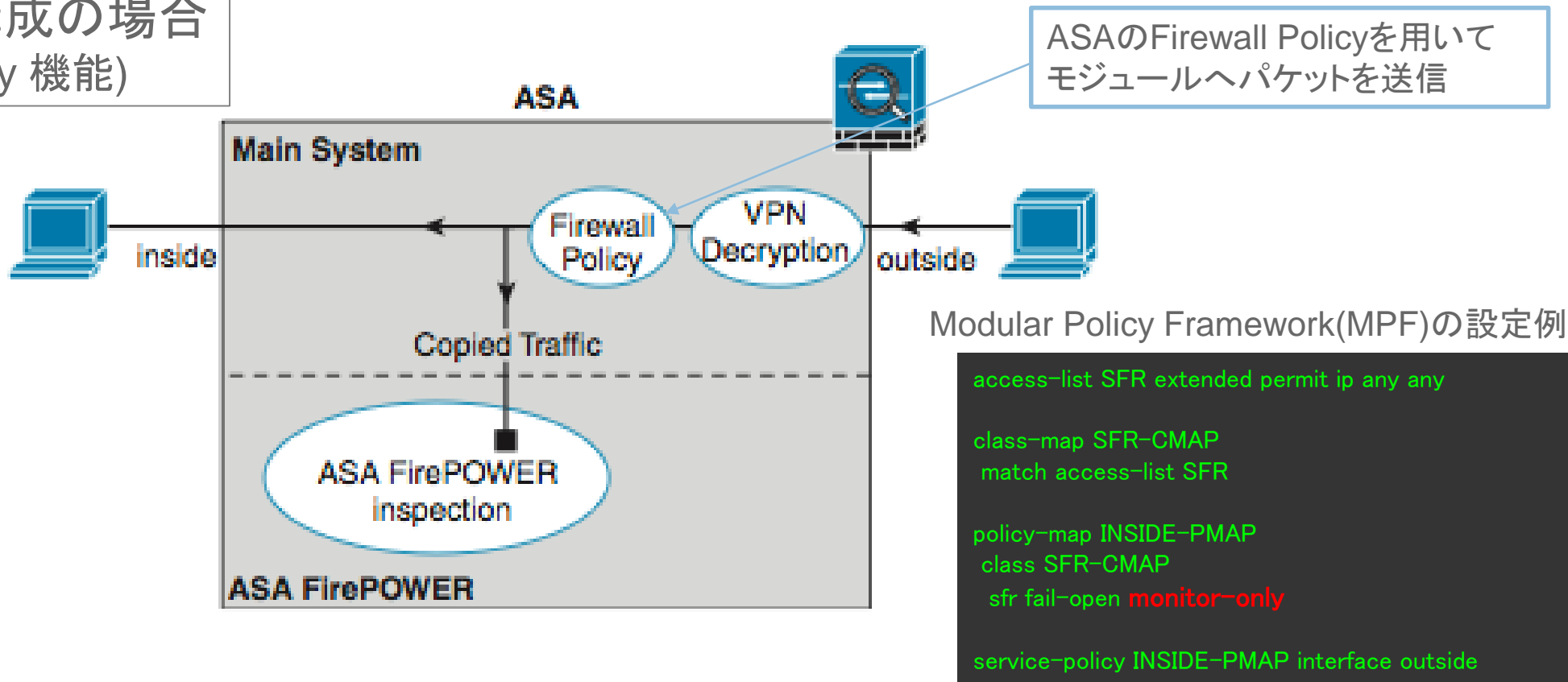


FirePOWERのアクションにより、通過するパケットをブロック可能

Fail Open 機能 : モジュールがダウンしていると判断した場合、パケットを通過させる
Fail Close 機能 : モジュールがダウンしていると判断した場合、パケットを遮断する

ASAとFirePOWERモジュール間の通信

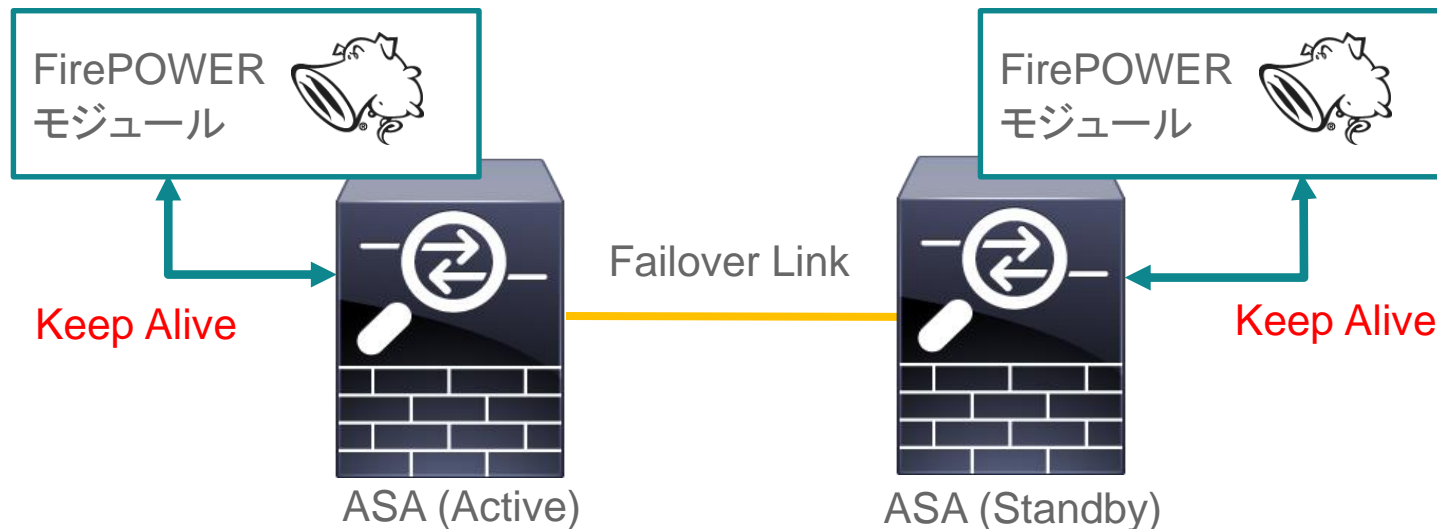
Passive 構成の場合
(Monitor-Only 機能)



FirePOWERモジュールによる通過パケットのブロックはない(検知と報告のみ)

ASAとFirePOWERモジュール間の通信

冗長構成(HA)



フェイルオーバーの条件

- ASA (Active)の障害時
- ASA (Active)上のFirePOWERモジュール障害時

※ ASAソフトウェア間の設定やセッション情報のみ同期
FirePOWERモジュール同士の設定やセッション情報の同期はなし

ソフトウェアコンポーネント

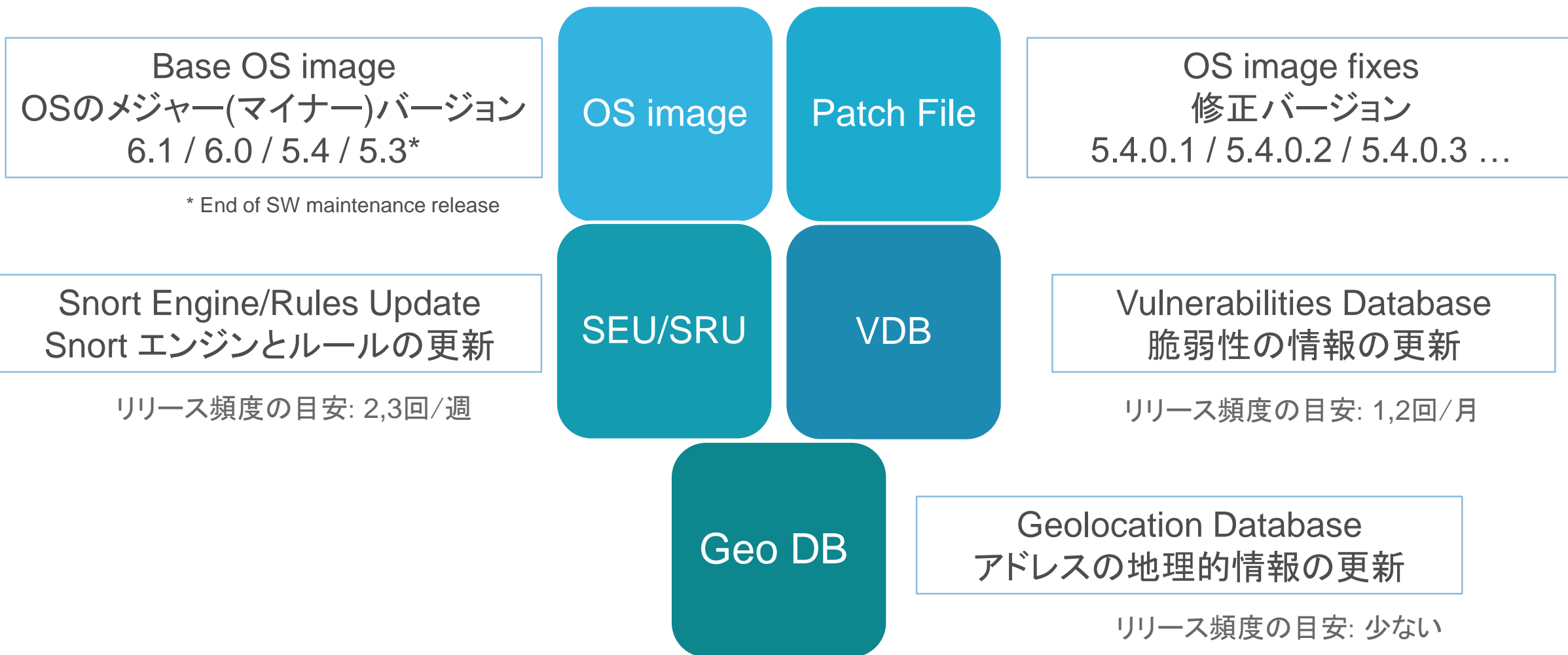
Cisco Software Download Page

<https://software.cisco.com/download/navigator.html>

The screenshot displays the Cisco Software Download Page for FireSIGHT Management Center 750. The page features a blue header with the Cisco logo and navigation links: Products & Services, Support, How to Buy, Training & Events, and Partners. A search bar is located on the right side of the header. Below the header, the page title is "Download Software" with a "Download Cart (0 items)" and "Feedback Help" links. The breadcrumb trail reads: Downloads Home > Products > Security > Firewalls > Firewall Management > Firepower Management Center > FireSIGHT Management Center 750 > FireSIGHT System Software-Rules Updates. The main content area is titled "FireSIGHT Management Center 750" and contains a search bar, "Expand All | Collapse All" links, and a "Release Rules Updates" section. A dropdown menu is open, showing "All Releases" with sub-items: Rules SEU VDB GeoDB, Rules Updates, SEU, GeoDB, and VDB. Under "VDB", versions 6.1, 6.0, 5.4, 5.3, and 5.2 are listed. The main table displays a list of releases with columns for Release Date, Size, and buttons for Download and Add to cart.

Release Date	Size	Download	Add to cart
31-AUG-2016	107.95 MB	Download	Add to cart
30-AUG-2016	107.86 MB	Download	Add to cart
24-AUG-2016	107.82 MB	Download	Add to cart
22-AUG-2016	107.79 MB	Download	Add to cart
18-AUG-2016	107.78 MB	Download	Add to cart
16-AUG-2016	107.74 MB	Download	Add to cart
12-AUG-2016	107.71 MB	Download	Add to cart

ソフトウェアコンポーネント

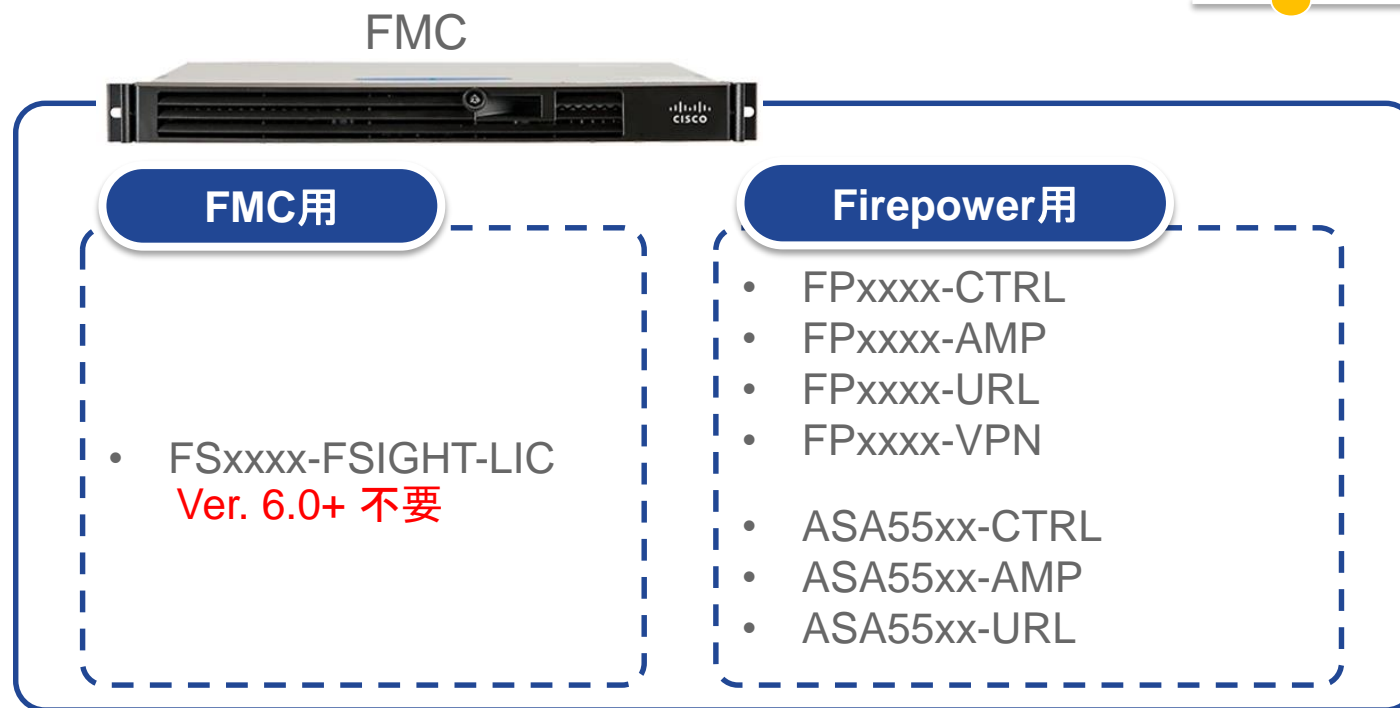
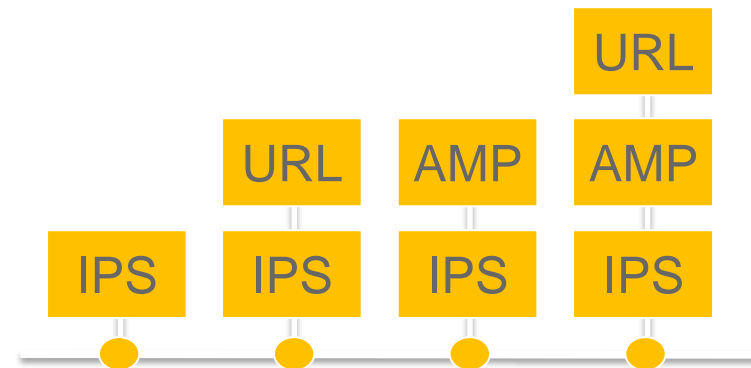


ライセンス

ライセンス

FMCによる管理

- ライセンスはすべて FMCに登録
(Firepower アプライアンス / FirePOWER モジュールには登録不要)



ライセンス

ASA with FirePOWER (On-Box Management)

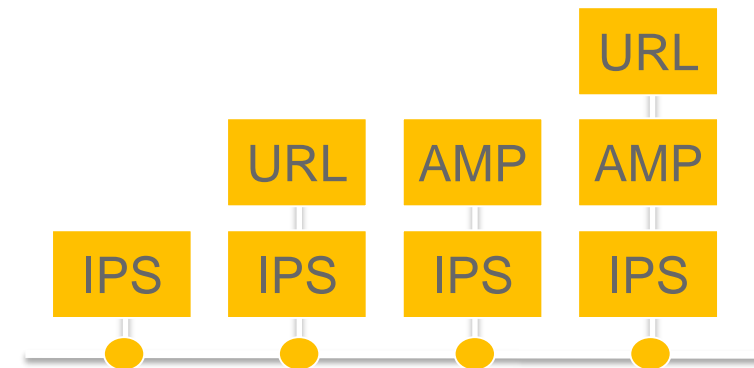
- ・ライセンスはFirePOWERモジュールに登録

ASA with FirePOWER



FirePOWERモジュール用

- ・ ASA55xx-CTRL
- ・ ASA55xx-AMP
- ・ ASA55xx-URL



ライセンスの発行

License Key と PAK を使用して発行

→ 発行された Product LicenseをLicense欄に入力

[FMC]

[ASDM(On-Box)]

[System > Licenses \(ver. 6.0+ ではClassicを選択\) > Add New License](#)

[Configuration > ASA FirePOWER Configuration > Licenses > Add New License](#)

Add Feature License

License Key

License

If your web browser cannot access the Internet, you must switch to a host with Internet access and navigate to <https://keyserver.sourcefire.com>.

Using the license key, follow the on-screen instructions to generate a license.

Firepowerへのライセンスの適用方法

[FMC] [Device > Device Management > Device](#)

Overview Analysis Policies **Devices** Objects AMP Deploy System Help admin

Device Management NAT VPN Platform Settings

Firepower

Cisco FirePOWER 7010

Device Interfaces Inline Sets Virtual Switches Virtual Routers

General

Name: Firepower

Tran **License**

Capabilities

- Protection:
- Control:
- Malware:
- URL Filtering:
- VPN:

チェックして有効化

Save Cancel

License

Protection:	Yes
Control:	Yes
Malware:	Yes
URL Filtering:	Yes
VPN:	Yes

※ On-Box management (ASDM) では
ライセンスは追加後にすぐに有効化される

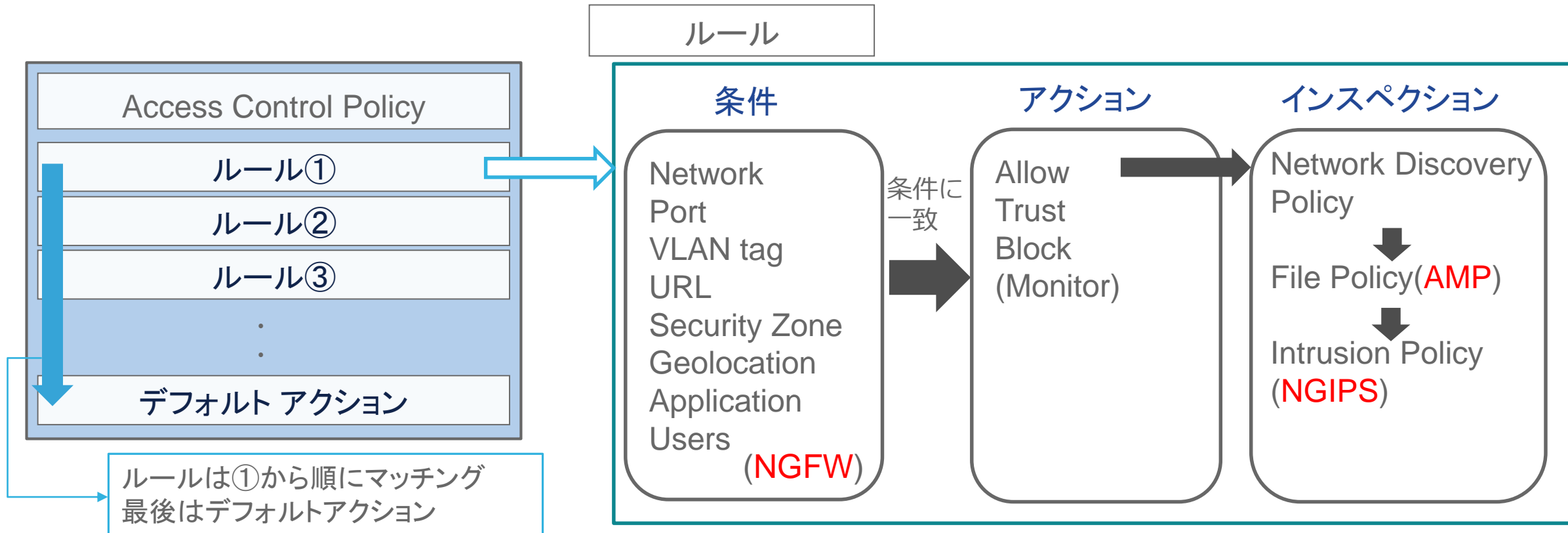
ポリシー

Firepower に適用するポリシー

- **Access Control Policy (ACP)**
Firepowerが監視している通信に対するポリシー
- **Health Policy**
機器のパフォーマンスを監視するためのポリシー
- **System Policy**
認証、言語、時刻同期に関するポリシー
(※ver. 6.0+では **FMCのSystem Configuration / FirepowerのPlatform Settings**が該当)

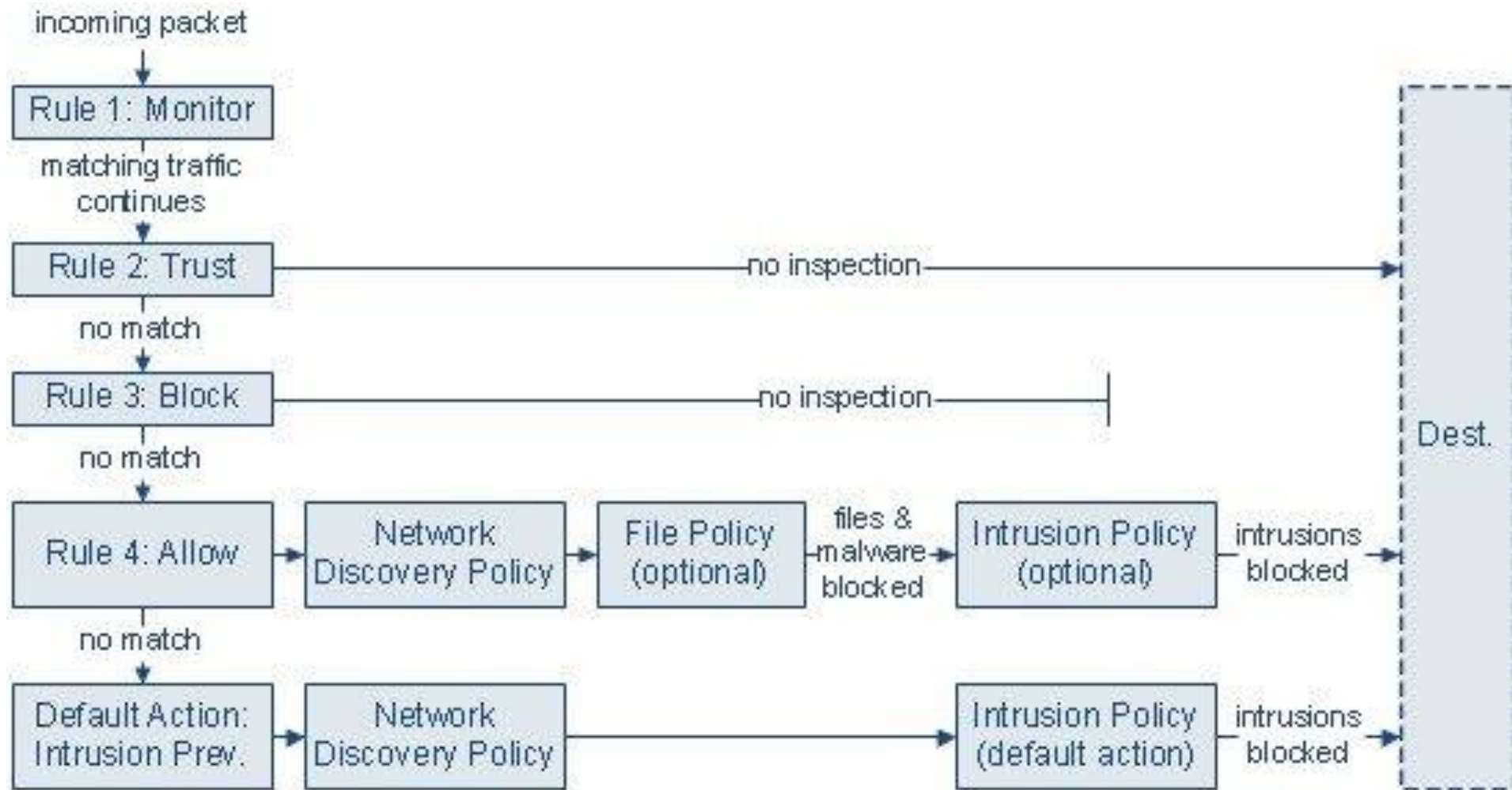
Firepower 1台に対して各ポリシーをそれぞれ1つ設定

Access Control Policy



Allow: Inspectionへ
Trust: 通過許可。宛先へ
Block: パケットをドロップ
Monitor: ログは残すが通信に影響を与えない

Access Control Policy (アクションの補足説明)



FMC での Access Control Policy 設定例

Overview Analysis **Policies** Devices Health System Help **jlarmer**

Intrusion **Access Control** Network Discovery Custom Applications Users Correlation Actions

Interesting Use Cases

Enter a description

Save Cancel Save and Apply Add Category Add Rule Search Rules

Device Targets: 0 devices

#	Name	Source Zones	Dest Zones	Sou... Net...	Dest Net...	VLA...	U...	Applications	Services	URLs	Action			
Administrator Rules														
<i>This category is empty.</i>														
Standard Rules														
1	Mobile Security 1	Intern	any	any	Ten	any	any	Android browser Blackberry browser Mobile Safari	any	any	Block			1
2	Read Only Facebook	Intern	Extern	any	any	any	any	Facebook Status Update Facebook Send Email Facebook Comment Facebook Chat Tags: Facebook game; Fill	any	any	Block			0
3	Web Block List	Intern	Extern	any	any	any	any		any		Block			0
										<ul style="list-style-type: none"> Adult and Pornography (Any Reputation) Bot Nets (Any Reputation) Confirmed SPAM Sources (Any Reputati Gambling (Any Reputation) (13 more...) 				
4	Block All P2P	Intern	Extern	any	any	any	any	Categories: peer to peer	any	any	Block			0
5	Inbound Email	Extern	Intern	any	any	any	any	SMTP	SMTP	any	Allow			0
6	Outbound Web Browsing	Extern	Intern	any	any	any	any	HTTP	any	any	Allow			0
Root Rules														
<i>This category is empty.</i>														
Default Action										Access Control: Block All Traffic				
1 Row Selected														
										Displaying 1 - 6 of 6 rules Page 1 of 1				

Agenda

1. 目的
2. イントロダクション
3. Firepower System / ASA with FirePOWERの概要
4. トラブルシューティングに役立つ情報とその取得方法

トラブルシューティングに役立つ情報






1. Task Status
2. Syslog
3. Firepowerの基本情報
4. Ping / Traceroute
5. CPU / Memory / Disk の使用状況
6. Packet Capture
7. ASA側のコマンド

1. Task Status

Version 5.3 / 5.4

[FMC] [System > Monitoring > Task Status](#) からTaskの成功/失敗を確認

Jobs

Task Description	Message	Creation Time	Last Change	Status	
Default Group 0 Running 0 Waiting 1 Completed 0 Retrying 0 Failed					
Backup: 09073 Backup / On Demand	Backup complete	2016-09-07 12:39:53	2016-09-07 13:42:45	Completed	
Policy apply tasks 0 Running 0 Waiting 1 Completed 0 Retrying 1 Failed					
Apply Default Network Discovery to xxxxx Access Control Policy	Access Control Policy applied successfully	2016-08-28 17:05:59	2016-08-28 17:06:44	Completed	
Apply ZONE to xxxxx Access Control Policy	Access Control Policy apply failed	2016-09-07 09:47:42	2016-09-07 09:47:46	Failed	
Remote Update Installation 0 Running 0 Waiting 1 Completed 0 Retrying 1 Failed					
Apply /var/sf/updates/Sourcefire_3D_Device_Virtual64_VMware_Patch-5.4.0.7-40.sh to xxxxx Remote Install	Update Install failed	2016-09-07 16:53:55	2016-09-07 16:57:08	Failed	
Apply /var/sf/updates/Sourcefire_3D_Device_Virtual64_VMware_Patch-5.4.0.7-40.sh to xxxxx Remote Install	Please reapply policies to your managed devices.	2016-09-07 17:20:18	2016-09-07 17:32:57	Completed	

Completed(成功) または Failed(失敗) を確認

1. Task Status

Version 6.0 / 6.1

[FMC] [Status icon > Tasks](#) からTask の成功/失敗を確認

The screenshot displays the Cisco FMC interface. At the top, the navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. On the right, there are buttons for 'Deploy', 'System', 'Help', and 'admin'. Below this, the 'Tasks' tab is selected, and a summary bar shows '9 total' tasks, with '0 waiting', '0 running', '0 retrying', '9 success', and '0 failures'. A list of tasks follows, each with a green checkmark indicating success:

- Exit Maintenance Mode (4m 25s): Exit Maintenance Mode. Exited Maintenance mode
- Local Install (26m 23s): Installing Sourcefire 3D Defense Center S3 Patch version: 6.0.0.1-26. Successfully Installed
- Remote Install (8m 50s): Apply to X.X.X.X. Please reapply policies to your managed devices.
- Policy Deployment (48s): Policy Deployment to fp60. Applied successfully
- Policy Pre-Deployment (2s): Pre-deploy Device Configuration for fp60. success
- Policy Pre-Deployment (47s): Pre-deploy Global Configuration Generation. success

The left side of the interface shows a 'Summary Dashboard' with various charts, all displaying 'No Data'. The bottom left corner features the Cisco logo.

1. Task Status

On-Box Management(ASDM)の場合

[ASDM] [Monitoring > ASA FirePOWER Monitoring > Task Status](#)からTask の成功/失敗を確認

Task Status

Job Summary Remove Completed Jobs Remove Failed Jobs

Running	0
Waiting	0
Completed	3
Retrying	0
Failed	0

Jobs

Task Description	Message	Creation Time	Last Change	Status	
Policy Deployment 0 Running 0 Waiting 3 Completed 0 Retrying 0 Failed					
Policy Deployment to Sourcefire3D Policy Deployment	Applied successfully	2016-08-26 13:15:56	2016-08-26 13:17:31	Completed	
Policy Deployment to Sourcefire3D Policy Deployment	Applied successfully	2016-08-30 05:03:53	2016-08-30 05:04:34	Completed	
Policy Deployment to Sourcefire3D Policy Deployment	Applied successfully	2016-08-30 05:17:23	2016-08-30 05:18:11	Completed	

2. Syslog

ErrorやWarningメッセージの確認

[FMC] [System > Monitoring > Syslog](#)

[ASDM] [Monitoring > ASA FirePOWER Monitoring > Syslog](#)

The screenshot shows the Syslog monitoring page in the Cisco FMC interface. The search filter is set to 'ERROR'. The messages list contains the following entries:

Timestamp	Source	Message
Aug 30 2016 22:38:07	Sourcefire3D sshd[23432]:	error: PAM: User not known to the underlying authentication module for illegal user takyasum from [X.X.X.X]
Aug 30 2016 20:48:45	Sourcefire3D SF-IMS[4601]: [15611]	Event Streamer:ConnectionHandler [ERROR] SFTunnelReadBuffer returned 26: Closed
Aug 30 2016 20:48:45	Sourcefire3D SF-IMS[4581]: [15433]	SFDataCorrelator:CorrelatorChannelThread [ERROR] Failed to connect to tunnel ([UUID]), error: Not connected
Aug 30 2016 20:48:45	Sourcefire3D SF-IMS[4581]: [15470]	SFDataCorrelator:UECTunnel [ERROR] Failed to read a message: Closed
Aug 30 2016 20:48:45	Sourcefire3D SF-IMS[4581]: [15469]	SFDataCorrelator:UECTunnel [ERROR] Failed to read a message: Closed
Aug 30 2016 20:48:45	Sourcefire3D SF-IMS[4581]: [15467]	SFDataCorrelator:ISHandlerTunnel [ERROR] Failed to read message from tunnel: Closed
Aug 30 2016 20:48:45	Sourcefire3D SF-IMS[4581]: [15468]	SFDataCorrelator:UECTunnel [ERROR] Failed to read a message: Closed

“Error”や“Warning”などを検索



(※SyslogはFMCの/var/log/配下にmessagesとして保存される)

3. Firepower の基本情報

Version 5.3 / 5.4

[FMC] [Devices > Device Management](#) から確認

Name	License Type	Health Policy	System Policy	Access Control Policy	
4 📁 Ungrouped (2)					
✓ Firepower-1 xxxx - Virtual Device 64bit - v5.4.0.7	Protection, Control	Initial Health Policy 2016-03-14 05:09:57	Initial System Policy 2016-03-14 16:07:05	Default Access Control	✓ ✎ 🗑
✓ Firepower-2 xxxx - Virtual Device 64bit - v5.4.0.6	Protection, Control, URL Filtering	Initial Health Policy 2016-03-14 05:09:57	Initial System Policy 2016-03-14 16:07:05	Default Access Control	✓ ✎ 🗑

↑
**HW Model
SW Version**

↑
License Type

↑
Health Policy

↑
System Policy

↑
**Access Control
Policy**

3. Firepower の基本情報

Version 6.0 / 6.1

[FMC] [Devices > Device Management](#)

(Ver. 6.0 の画面)

Name	Model	License Type	Access Control Policy
Ungrouped (1)			
Firepower xxxx - Cisco FirePOWER 7010 - v6.0.0	Cisco FirePOWER 7010	Protection, Control, Malware, URL Fil...	Initial ACP

↑
SW Version

↑
HW Model

↑
License type

↑
Access Control Policy

その他の情報は

[FMC] [Devices > Device Management > 該当デバイスをクリック > Device タブ](#)

3. Firepower の基本情報

Version 6.0 / 6.1

[FMC] [Devices > Device Management > 該当デバイスをクリック > Device タブ](#)

Overview Analysis Policies **Devices** Objects AMP Deploy System Help admin

Device Management NAT VPN Platform Settings

Firepower

Cisco FirePOWER 7010

Device Interfaces Inline Sets Virtual Switches Virtual Routers

General

Name: Firepower

Transfer Packets: Yes

License

Protection: No

Control: No

Malware: No

URL Filtering: No

VPN: No

System

Model: Cisco FirePOWER 7010

Serial: JMX1912807X

Time: 2016-09-05 15:04:37

Version: 6.0.0

Policy: [Initial Platform Settings](#)

Health

Status: (Warning icon)

Policy: [Initial Health Policy](#)

Blacklist: [None](#)

CLI画面へのアクセス (CLISH画面)

ハードウェア

- Firepower アプライアンス
- FirePOWER ハードウェアモジュール

コンソールケーブルやSSHで接続

CLISH (Firepower のCLI画面)

```
>
>
> ?
configure Change to Configuration mode
end Return to the default mode
exit Exit this CLI session
expert Invoke a shell
help Display an overview of the CLI syntax
history Display the current session's command line history
logout Logout of the current CLI session
show Change to Show Mode
system Change to System Mode
```

CISCO

ソフトウェア

FirePOWER ソフトウェアモジュール

ASAで以下コマンドを入力 または SSH

[#session sfr \(telnet session\)](#)

[#session sfr console \(console session\)](#)

ASA CLI画面

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
```

```
Sourcefire3D login: admin
Password:
```

```
exit / logout (telnet only)
```

```
Cisco Fire Linux OS v6.0.0 (build 258)
Cisco ASA5508 v6.0.1 (build 29)
```

```
>
>
```

初期パスワード

ver. 5.4以前	admin/Sourcefire
ver. 6.0以降	admin/Admin123

CLI画面へのアクセス (Expert画面)

FMC (※CLISHは非サポート)

コンソールケーブルやSSHで接続

Expert(Linux)画面

```
Sourcefire Linux OS v5.4.0 (build 126)
Sourcefire Virtual Defense Center 64bit v5.4.1.6 (build 40)

admin@xxx:~$
admin@xxx:~$
```

Firepower / FirePOWER モジュール

CLISH画面で [>expert](#)

CLISH → Expert(Linux)画面

```
Sourcefire Linux OS v5.4.0 (build 126)
Sourcefire Virtual Device 64bit v5.4.0.7 (build 40)

>
> expert
admin@(xxx):~$
admin@(xxx):~$
```

4. 疎通確認 (Ping / Traceroute)

CLI画面を利用

FirePOWER モジュール

CLISH より以下のコマンド入力

> system support ping <host>

> system support traceroute <host>

上記がサポートされていない場合

> expert

admin@(xxx):~\$ sudo ping <host>

admin@(xxx):~\$ sudo traceroute <host> --i

```
> expert
admin@(xxx):~$ sudo ping cisco.com
PING cisco.com (x.x.x.x) 56(84) bytes of data.
64 bytes from .cisco.com (x.x.x.x): icmp_req=1 ttl=232 time=174 ms
64 bytes from .cisco.com (x.x.x.x): icmp_req=2 ttl=232 time=179 ms
--- cisco.com ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4006ms
rtt min/avg/max/mdev = 174.739/176.019/179.368/1.936 ms

admin@(xxx):~$ sudo traceroute cisco.com -l
traceroute to cisco.com (x.x.x.x), 30 hops max, 60 byte packets
 1 x.x.x.x (x.x.x.x) 0.980 ms 1.292 ms 1.635 ms
 2 x.x.x.x (x.x.x.x) 0.771 ms 0.906 ms 0.954 ms
 .
 X .cisco.com (x.x.x.x) 174.707 ms 174.776 ms 174.803 ms
```

5. CPU / Memory / Diskの使用状況

CPU:

[CLISH] [>show processes](#) / [Expert] [\\$ top 1](#)

```
> show processes
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
  1 root  20  0 4216 612 596 S  0  0.0 0:29.94 init
  2 root  20  0  0  0  0 S  0  0.0 0:00.07 kthreadd
  3 root  20  0  0  0  0 S  0  0.0 0:46.05 ksoftirqd/0
```

Memory:

[CLISH] [>show memory](#) / [Expert] [\\$ free](#)

```
> show memory
      total    used    free  shared  buffers  cached
Mem:   4055056 2973432 1081624     0    143856  774240
-/+ buffers/cache: 2055336 1999720
Swap:  5194744  15004  5179740
```

Disk:

[CLISH] [>show disk](#) / [Expert] [\\$ df -a](#)

```
> show disk
Filesystem      Size Used Avail Use% Mounted on
/dev/root        3.7G 995M 2.5G 29% /
devtmpfs         2.0G  56K 2.0G  1% /dev
/dev/sda1         88M  54M  28M 67% /boot
/dev/sda7        31G  9.1G  21G 31% /var
```

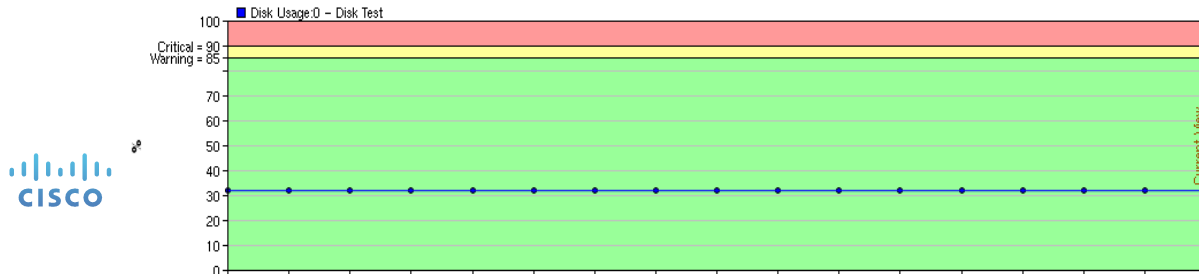
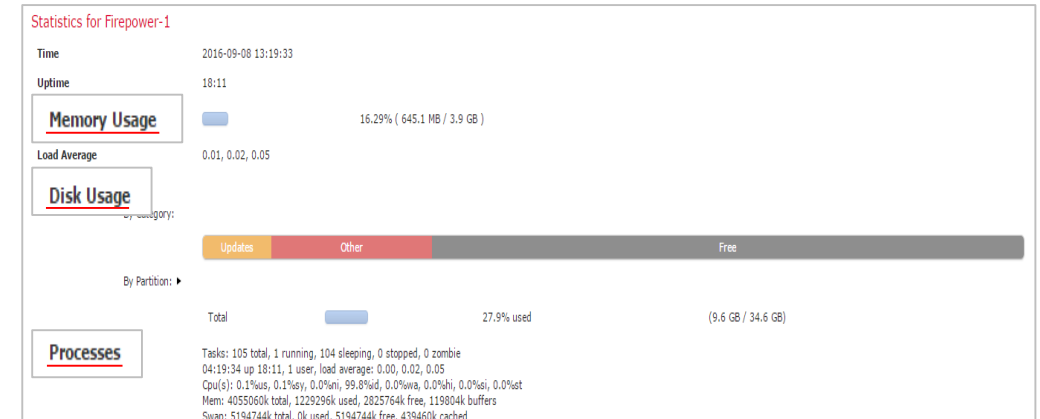
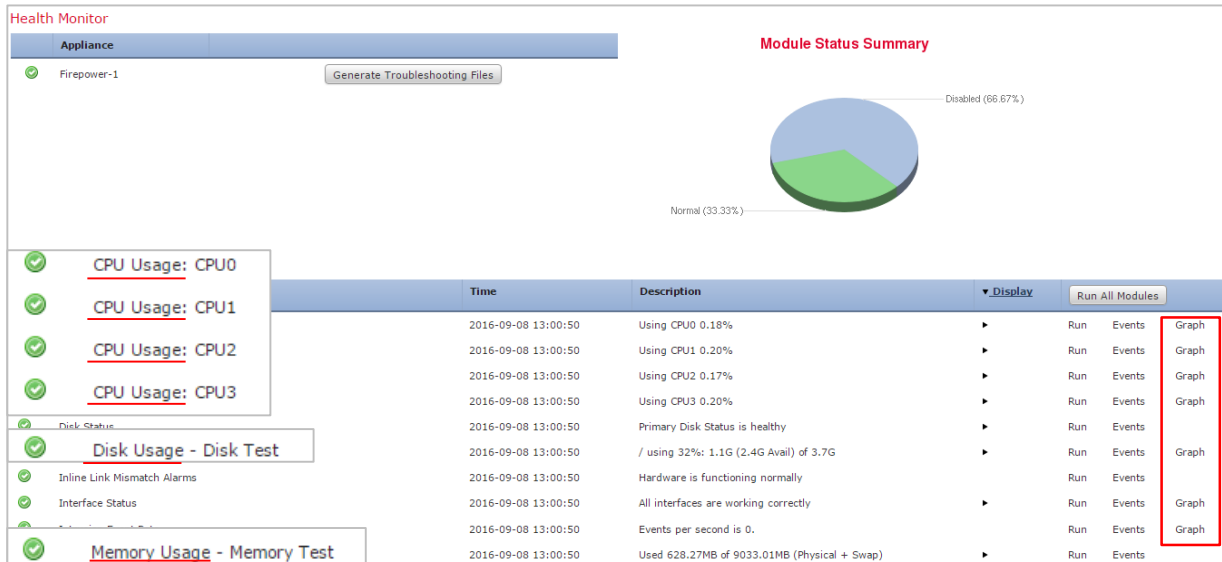
5. CPU / Memory / Diskの使用状況

FMC GUIの場合

(5.4以前) [FMC] [Health > Health Monitor](#)

(6.0+) [FMC] [System > Health > Monitor](#)

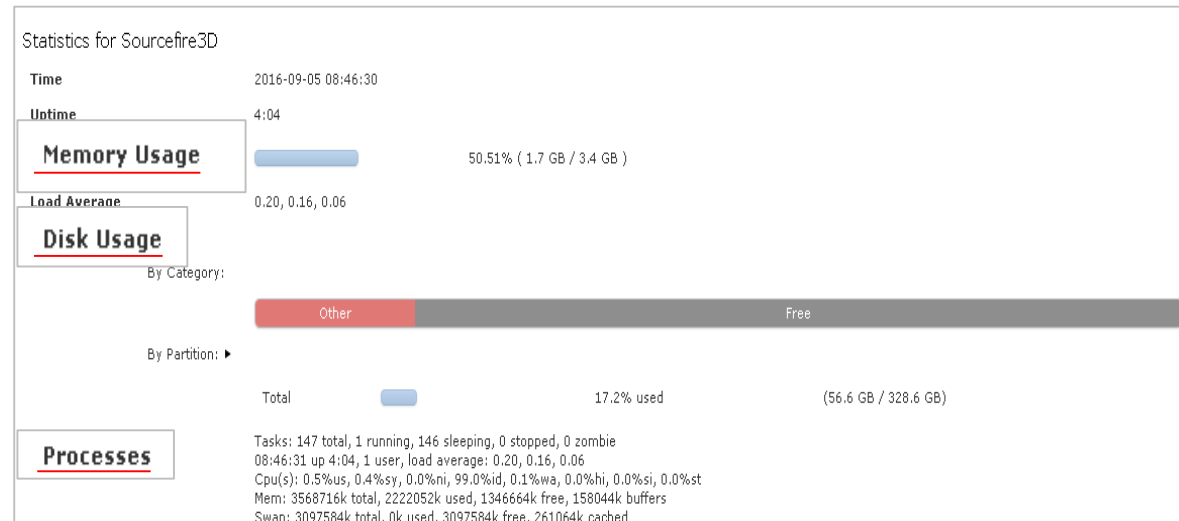
[FMC] [System > Monitoring > Statistics](#)



5. CPU / Memory / Diskの使用状況

On-Box Management(ASDM)の場合

[ASDM] [Monitoring > ASA FirePOWER Monitoring > Statistics](#)



6. Packet Capture

CLI画面を利用

- Firepower (FirePOWER モジュール)の場合:

[CLISH] [>system support capture-traffic](#)

```
> system support capture-traffic
Please choose domain to capture traffic from:
 0 - eth0
 1 - Unzoned Passive Domain (Interfaces eth1, eth2)

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -c 10 -w capture.pcap
```

- FMCの場合:

[Expert] [tcpdump](#) (Linuxのpacket captureコマンド)

```
admin@xxxx:~$ sudo tcpdump -i eth0 -w <Name>
```

7. ASA側でのトラブルシューティング

ASA側で以下のログを取得

- show module sfr details
(show module 1 details [ASA5585])
- show service-policy sfr (複数回)
- show tech
- informational level (6) 以上の syslog

```
ASA# show module sfr details
Card Type:      FirePOWER Services Software Module
Model:         ASA5508
Hardware version: N/A
Serial Number:  -----
Firmware version: N/A
Software version: 6.0.1-29
MAC Address Range: xxxx.xxxx.xxxx to xxxx.xxxx.xxxx
App. name:      ASA FirePOWER
App. Status:    Up
App. Status Desc: Normal Operation
App. version:   6.0.1-29
Data Plane Status: Up
Console session: Ready
Status:         Up
DC addr:        No DC Configured
Mgmt IP addr:   x.x.x.x
Mgmt Network mask: x.x.x.x
Mgmt Gateway:   x.x.x.x
Mgmt web ports: 443
Mgmt TLS enabled: true
```

```
ASA (config)# show service-policy sfr
Interface inside:
Service-policy: INSIDE-PMAP
Class-map: SFR-CMAP
SFR: card status Up, mode fail-open
packet input 75954, packet output 76209, drop 0, reset-drop 0
```

バックアップ

設定やイベント情報を復元

- 機器交換やOSイメージの初期化時に利用
- ローカル / リモートストレージに保存可能
- 以下の項目の一致が必要
 - Hardware model
 - Software version
 - VDB version

[FMC] [System > Tools > Backup Restore](#)
[ASDM] [Configuration > ASA FirePOWER Configuration > Tools > Backup Restore](#)

Backup Management Backup Profiles

Create Backup

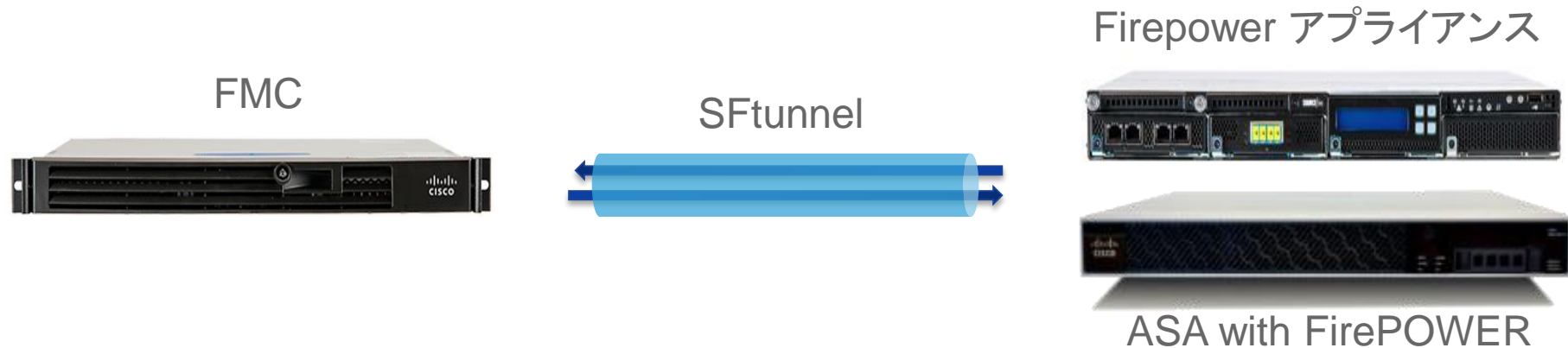
Name
Storage Location /var/sf/backup/
Email Not available. You must set up your mail relay host.
Copy when complete

Start Backup Save As New Cancel

※バックアップは一部のプラットフォームでは非サポート

ケーススタディ

FMCにイベントが送信されない



確認事項(例)

- FMC にデバイスは登録されているか ➡ show managers
- IP reachabilityはあるか ➡ ping
- SFtunnel に問題がないか ➡ system support sftunnel-status

FMCにイベントが送信されない

FMCへのデバイス登録確認

- Firepower (FirePOWER モジュール)
[CLISH] [>show managers](#) でデバイスの登録状況を確認

登録完了

```
> show managers
Type           : Manager
Host           : X.X.X.X
Registration    : Completed
```

設定なし

```
> show managers
No managers configured.
```

設定はあるが登録未完了

```
> show managers
Host           : x.x.x.x
Registration Key : KEY
Registration    : pending
RPC Status     :
Type           : Manager
Host           : x.x.x.x
Registration    : Pending
```

- FMC
[FMC] [Devices > Device Management](#) に該当デバイスが存在するか確認

Name	License Type	Health Policy	System Policy	Access Control Policy	
📁 Ungrouped (2)					
🟢 Firepower-1 xxxx - Virtual Device 64bit - v5.4.0.7	Protection, Control	Initial Health Policy 2016-03-14 05:09:57	Initial System Policy 2016-03-14 16:07:05	Default Access Control	🟢 ✎ 🗑

FMCにイベントが送信されない

SFtunnelの状態確認

Firepower (FirePOWER モジュール)

[CLISH] > [system support sftunnel-status](#) でSFtunnelの状態を確認

```
**RUN STATUS*** x.x.x.x *****  
Cipher used = AES256-SHA (strength:256 bits)  
-> Connected: Yes  
Registration: Completed.  
IPv4 Connection to peer 'x.x.x.x' Start Time: Sun May 4 05:12:16 2016
```

その他の確認事項

- パケットキャプチャ
- CPUやメモリ使用状況の確認
- Syslog メッセージ

TACへの問い合わせが必要な場合に
取得する情報

TACの調査の際に必要となり得る情報

1. Troubleshooting file (TS file)

TACの調査に必要なログを集めたファイル

2. スクリーンショット

- FMC / Firepower の version情報
- 設定情報
- 事象を確認できるもの (Task Status / Event情報 など)

1. Troubleshooting file (TS file)

FMCによる管理の場合

- [FMC] ([System \(ver. 6.0+\)](#)) > [Health](#) > [Health Monitor](#) から取得
- xxxxxxxxxx-troubleshoot.tar.gz の形式 (サイズは数百MB)

※TS fileは**Firepower**と**FMC**それぞれで生成 (どちらもFMCから取得)

The screenshot shows the Cisco FMC Health Monitor interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Health', 'System', 'Help', and 'admin'. The 'Health Monitor' tab is active, showing a list of appliances. One appliance, 'FS-540-763.cisco.com', is highlighted. A red box highlights the 'Generate Troubleshooting Files' button. To the right, a 'Module Status Summary' pie chart displays the following data:

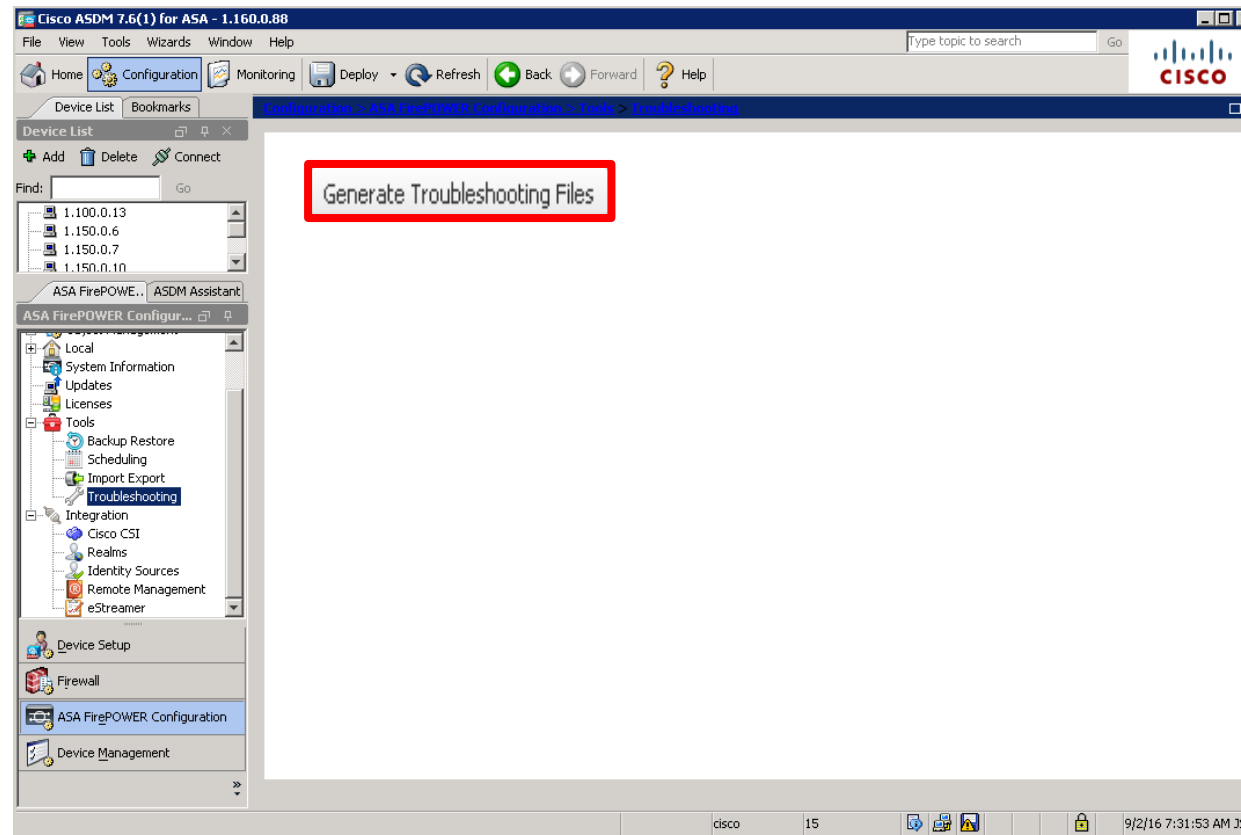
Status	Percentage
Normal	51.85%
Disabled	40.74%
Critical	3.70%
Warning	3.70%

(※SyslogはFMCのTSファイル内のdir-archives/var-log配下にmessagesとして保存される)

1. Troubleshooting file (TS file)

On-Box Managementの場合

[ASDM] [Configuration > ASA FirePOWER Configuration > Tools > Troubleshooting](#)



2. スクリーンショット

ソフトウェア情報

[FMC] [Help > About](#)

[ASDM] [Configuration > ASA FirePOWER Configuration > System Information](#)

Model	Virtual Defense Center 64bit
Serial Number	None
Software Version	5.4.1.6 (build 40)
OS	Sourcefire Linux OS 5.4.0 (build126)
Snort Version	2.9.7 GRE (Build 384)
Rule Update Version	2016-04-21-001-vrt
Rulepack Version	1695
Module Pack Version	1946
Geolocation Update Version	None
VDB Version	build 264 (2016-03-01 22:22:42)

← **SW version**

← **SRU version**

← **GeoDB version**

← **VDB version**

2. スクリーンショット

Firepower の基本情報

[FMC] [Devices > Device Management](#) から確認

Name	License Type	Health Policy	System Policy	Access Control Policy	
4 📁 Ungrouped (2)					
✓ Firepower-1 xxxx - Virtual Device 64bit - v5.4.0.7	Protection, Control	Initial Health Policy 2016-03-14 05:09:57	Initial System Policy 2016-03-14 16:07:05	Default Access Control	✓ ✎ 🗑️
✓ Firepower-2 xxxx - Virtual Device 64bit - v5.4.0.6	Protection, Control, URL Filtering	Initial Health Policy 2016-03-14 05:09:57	Initial System Policy 2016-03-14 16:07:05	Default Access Control	✓ ✎ 🗑️

Ver 6.0+ では以下の画面でもスクリーンショットを取得

[FMC] [Devices > Device Management > 該当デバイスをクリック > Device タブ](#)

System	Health
Model: Cisco FirePOWER 7010	Status: ⓘ
Serial: JMX1912807X	Policy: Initial Health Policy ← Health Policy
Time: 2016-09-05 15:04:37	Blacklist: None
Version: 6.0.0	
Policy: Initial Platform Settings ← Platform Settings	

TACでお受けできない質問の例

- セキュリティ上の推奨設定
- 脆弱性の影響を受けた例
- カスタムシグネチャの作り方

Cisco Support Community のご案内

Cisco Support Community (CSC)



ciscoサポートコミュニティ FirePOWER



すべて ニュース ショッピング 地図 画像 もっと見る ▾ 検索ツール

約 4,410 件 (0.20 秒)

サポート コミュニティ (Japan) | Cisco Support Commu

<https://supportforums.cisco.com/ja> ▾

Cisco 製品の使い方、トラブルに関するQ&Aや役立つ情報交換等、ユーザー
わすためのコミュニティサイトです。... シスコ サポート コミュニティへようこそ
ASA/FirePOWER ... サポートコミュニティに掲載して欲しいコンテンツを募集

FirePOWER | Cisco Support Community

<https://supportforums.cisco.com/ja/community/12475191/firepower>

Cisco FirePOWER 関連の最新のトラブルシューティングや 技術情報を公開
を ... FirePOWER: ACP 適用時の snort 再起動有無、及び ACP 適用開始
方法 サポートコミュニティに掲載して欲しいコンテンツを募集しています。

FirePOWER

Cisco FirePOWER 関連の最新のトラブルシューティングや 技術情報を公開しています。質問を投稿してユーザー同士で解決することもできます。

ディスカッション ドキュメント ブログ ビデオ イベント

Display 25 フィルター

Subject	閲覧数	Rating	Comments	Author
FMCと FirePOWER Module パッチの簡易アップデート手順 最後の回答 7分 14秒 ago.	121	0	0	Taisuke Nakamura
ASA Firepower Moduleと FMCの 再起動手順 最後の回答 3日 19時間 ago.	112	0	0	Taisuke Nakamura
Firepower 6.0: URL Filtering 動作概要と 設定確認 最後の回答 1週 5日 ago.	205	5	0	Taisuke Nakamura
FirePOWERのパッチダウングレード方法 最後の回答 3週 2日 ago.	17	5	0	takyasum

参考情報: Cisco Support Community

- 2016/09/12 現在、55件のFirepower Systemの日本語コンテンツが存在

[トラブルシューティング関連]

- ✓ Troubleshooting file の作成・取得の方法
<https://supportforums.cisco.com/ja/document/12470276>
- ✓ FirePOWER - パケットキャプチャの方法
<https://supportforums.cisco.com/ja/document/12528956>

[事例紹介]

- ✓ ASA with FirePOWER の management port が 0 になる事象について
<https://supportforums.cisco.com/ja/document/12532356>

[設定関連]

- ✓ ASA with FirePOWER の初期インストール手順 (ASA5500-X wo/ ASA5585-X)
<https://supportforums.cisco.com/ja/document/12475796>
- ✓ FireSight ライセンス登録方法
<https://supportforums.cisco.com/ja/document/12411881>
- ✓ FireSight 初期設定について
<https://supportforums.cisco.com/ja/document/12404876>
- ✓ FireSight-FirePower 登録手順
<https://supportforums.cisco.com/ja/document/12404936>

投票質問2

CSCのセキュリティに関する記事について感想をお聞かせください

1. 役にたっている
2. 役にたつときがある
3. 役に立たない
4. 存在を知らなかった

本セミナーが少しでも Firepower System / ASA with FirePOWERについての理解とトラブルシューティングの助けになれば幸いです



Q & A

画面右側のQ&A ウィンドウから **All Panelist 宛** に送信してください

Ask the Expert with Takuya Yasumi

今日聞けなかった質問は、今回のエキスパートが担当するエキスパートに質問（9月14日～9月25日まで開催）へお寄せください！

<https://supportforums.cisco.com/ja/discussion/13118606>

Webcastの内容やQ&Aドキュメントは、本日より5営業日以内にこのサイトへ掲載いたします。

<https://supportforums.cisco.com/ja/community/5356/webcast>

今後のWebcast 予定

2016年 10月13日 (木) 10:00-11:30

[テーマ]

いまさら聞けないVLANとVLAN間ルーティング

[スピーカー]

グローバルナレッジネットワーク株式会社, シスコ認定インストラクター

鈴木 新(Arata Suzuki)

登録ページは後日開設予定です

コンテンツに関するご意見を募集しています！



[ご意見箱] コンテンツリクエスト



掲載してほしい情報
あったら役に立つ情報
英語ではなく日本語でほしい情報など
リクエストをお寄せください

ソーシャルメディアで サポートコミュニティと 繋がろう



<http://www.facebook.com/CiscoSupportCommunityJapan>



Twitter- <http://bit.ly/csc-twitter>
<https://twitter.com/cscjapan>



<https://www.youtube.com/user/CSCJapanModerator>



Google+ <http://bit.ly/csc-googleplus>



LinkedIn <http://bit.ly/csc-linked-in>



Instagram <http://bit.ly/csc-instagram>



Newsletter Subscription
<http://bit.ly/csc-newsletter>



ご参加ありがとうございました
アンケートにもご協力ください



※注意

当資料と 公式ドキュメントの内容に差異がある場合は、
公式ドキュメントの内容を正としてください