



# Firepower Threat Defense 初期セットアップガイド

Rev 1.4

2018/09

シスコシステムズ合同会社

# はじめに

- 本ガイドは、Firepower Threat Defense (以下、FTD) の初期セットアップ方法を解説しております。
- 本ガイドは、FTDとFirepower Management Center (以下、FMC) の仮想版を使って、評価作業を開始できることをゴールとしております。

## 内容に関する保証について

- 本ガイドは、2018年7月現在の情報に基づいており、FTD & FMCのソフトウェアは 6.2.3.3を、ハイパーバイザはVMware ESXi 6.0を利用しております。ただし、一部の機能は 2018年7月に更新版として、6.2.3.3 を利用して作成しています。
- 本ガイドに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。
- シスコは、本ガイドに関して、その正確性又は完全性について一切の責任を負わないこととします。
- シスコは、本ガイドが十分な品質を有すること、特定の目的に対する適合性を有すること、又は第三者の知的財産権、プライバシー権等その他の一切の権利に対する侵害がないことを、明示にも黙示にも表明又は保証しません。

# ネットワーク環境図

Internet

■ 設定済みの機器



NTPサーバ

Proxyサーバ

10.71.128.0/21

.132.201

FMCv

.132.186

ESX

管理NW

外部LAN

192.168.250.0/24

g0/0 グローバルアドレス

ASA

g0/2 .254

#g1/0/19

Switch

#g1/0/20

PAT

.132.202  
Management

G0/0 outside .1

FTDv

G0/1 inside .1

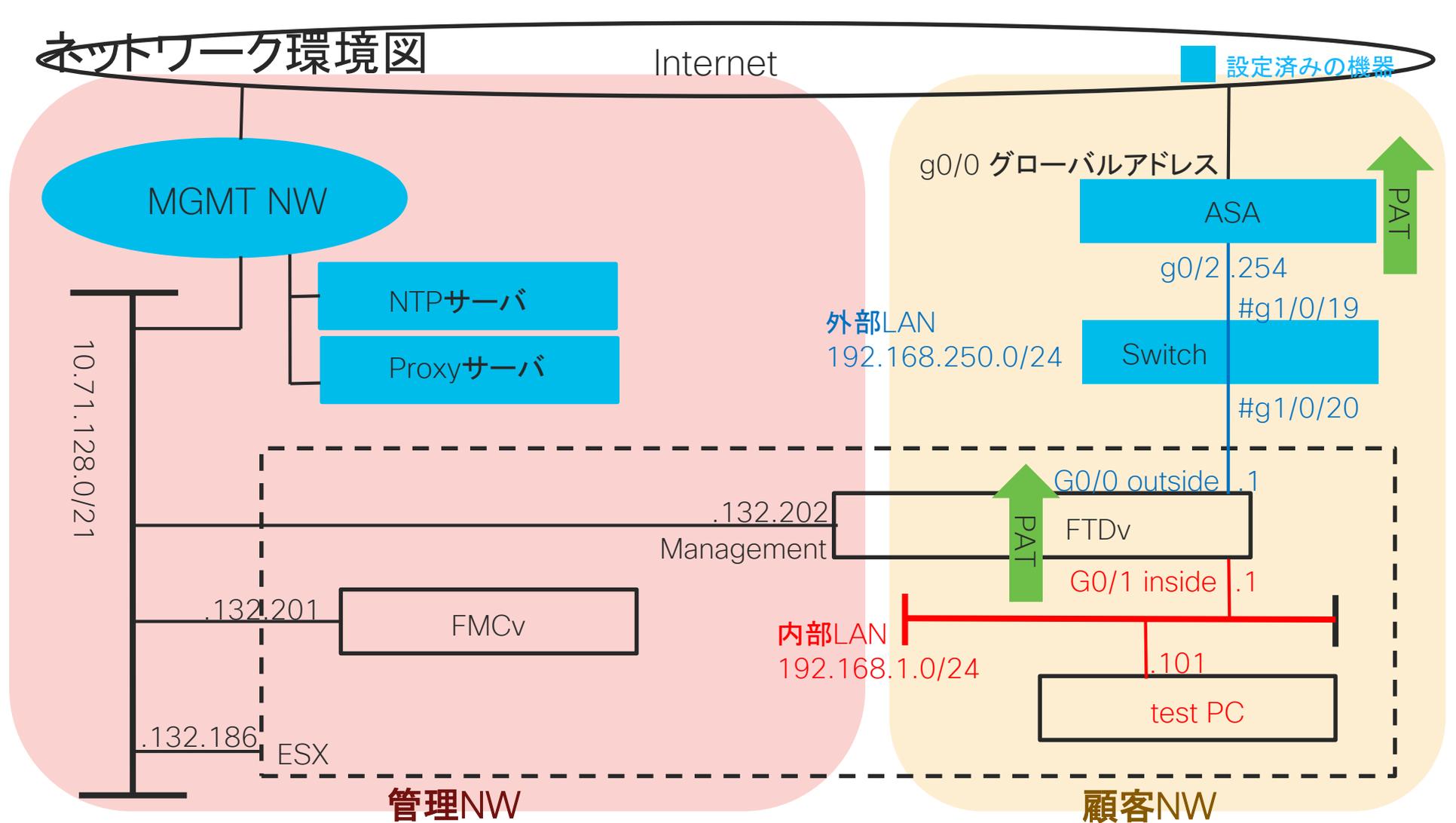
内部LAN

192.168.1.0/24

.101

test PC

顧客NW



# 当ガイドのシナリオ

- FTDvとFMCvをインストールし、FTDvをRouted Firewallとして設定する。
- FirewallとしてInterface PATを行い、内部のtest PCからインターネットへの接続を可能にする。
- Intrusion PolicyにてPOV (Proof of Value、事前検証) 向けに各種ルールを検知できるようにする。
- File PolicyにてMalwareをブロックする。
- Access Control PolicyにてSecurity Intelligence (IP/URL Blacklist) を利用する。また、URL Filterにてギャンブルに関するサイトへのアクセスをブロックする。

# 目次

1. FTDとFMCのインストール
  2. FTDとFMCその他初期設定
  3. Intrusion Policy設定
  4. Malware & File Policy設定
  5. Access Control Policy設定
  6. Pre-filter 設定
  7. シグネチャ / DB更新
  8. eStreamer API & Splunk eNcore App
  9. メンテナンス
  10. レポーティング
- Appendix 1. Firepower 4100/2100  
のインストールと初期設定

# 1. FTDとFMCのインストールと 初期設定

# インストールからデバイス登録までの流れ

設定の順序



Firepower Management Center

- ① OVFデプロイとWeb GUIアクセス
- ② 初期設定
- ③ ライセンスの追加



Firepower Threat Defense

- ① OVFデプロイ
- ② アダプタタイプの変更
- ③ 初期設定
- ④ FMCへの登録キーの設定



Firepower Management Center

- ① FTDの登録



# ステップ 1-1: OVFのデプロイと Web GUIアクセス

1. 以下のURLより、Firepower Management Center(以下、FMC)の .tarファイルを取得し、7-Zipなどアーカイバで展開

<https://software.cisco.com/download/release.html?mdfid=286259687&catid=268438162&softwareid=286271056&release=GeoDB&relind=AVAILABLE&rellifecycle=&reltype=latest>

 Cisco\_Firepower\_Management\_Center\_Virtual\_VMware-ESXi-6.2.2-81.ovf

(注)ソフトウェアバージョンはそのときに適切なものを選ぶこと

2. vSphere Client 6.0で ovf を以下のようにデプロイ

FMCは管理用に仮想NICを1つ持つため、管理ネットワークに所属

Source Networks	Destination Networks
Management	VM Network

その他vSphere Client上での設定はデフォルトを使用し、デプロイを開始すると 40分程度で FMC の起動と内部DBの構築が完了し、その後Web GUI へアクセスできる



# ステップ 1-2: OVFのデプロイと Web GUIアクセス

## 3. コンソール画面よりCLIでアドレス変更

バージョン 6.x 以降の場合初期ユーザパスワードは以下の通り

ユーザ名: admin / パスワード: Admin123

rootユーザ昇格後、“configure-network”コマンド

```
admin@fmc:~$ sudo su
Last login: Sat Jul 14 11:15:37 UTC 2018 on tty1
root@fmc:/Volume/home/admin# configure-network _
```

## 4. (CLIでアドレス変更しない場合) ブラウザで FMCデフォルトIPアドレスにHTTPSアクセス

<https://192.168.45.45/>

ユーザ名: admin

パスワード: Admin123

※ ブラウザアクセスする端末の IP アドレスは、192.168.45.2/24 など同一サブネットを使用

# ステップ 2-1: 初期設定



**Change Password**

Use these fields to change the password for the admin account. Cisco recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

New Password ①

Confirm

**Network Settings**

Use these fields to specify network-related information for the management interface on the appliance.

Protocol  IPv4  IPv6  Both

IPv4 Management IP

Netmask

IPv4 Default Network Gateway

Hostname

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

②

**Time Settings**

Use these fields to specify how you want to set the time for the Defense Center.

Set My Clock ③  Via NTP from   Manually  /  /  /  :

Current Time

Set Display Time Zone

**Recurring Rule Update Imports**

Use these fields to schedule recurring rule updates.

Install Now

Enable Recurring Rule Update Imports from the Support Site

Import Frequency   :  :

Policy Deploy ④  Deploy updated policies to targeted devices after rule update completes

**Recurring Geolocation Updates**

Use these fields to schedule recurring weekly geolocation updates. Note that updates may be large and can take up to 45 minutes.

Install Now

Enable Recurring Weekly Updates from the Support Site

Update Start Time   :

- ① adminパスワードの変更
- ② FMCのIPアドレス、デフォルトゲートウェイ、ホスト名、DNSサーバを入力
- ③ NTPサーバのIPアドレスまたはFQDNを入力、Time Zoneの変更
- ④ 更新内容の設定を画面のように入力
- ⑤ 最後にライセンス契約(EULA)にチェックを入れ“Apply”を選択

**End User License Agreement**

DISTRIBUTE / SELL THE CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS. THE FOLLOWING TERMS OF THE AGREEMENT GOVERN CUSTOMER'S USE OF THE SOFTWARE (DEFINED BELOW), EXCEPT TO THE EXTENT: (A) THERE IS A SEPARATE SIGNED CONTRACT BETWEEN CUSTOMER AND CISCO GOVERNING CUSTOMER'S USE OF THE SOFTWARE, OR (B) THE SOFTWARE INCLUDES A SEPARATE "CLICK-ACCEPT" LICENSE AGREEMENT OR THIRD PARTY LICENSE AGREEMENT AS PART OF THE INSTALLATION OR DOWNLOAD PROCESS GOVERNING CUSTOMER'S USE OF THE SOFTWARE. TO THE EXTENT OF A CONFLICT BETWEEN THE PROVISIONS OF THE FOREGOING DOCUMENTS, THE ORDER OF PRECEDENCE SHALL BE (1) THE SIGNED CONTRACT, (2) THE CLICK-ACCEPT AGREEMENT OR THIRD PARTY LICENSE AGREEMENT, AND (3) THE AGREEMENT. FOR PURPOSES OF THE AGREEMENT, "SOFTWARE" SHALL MEAN COMPUTER PROGRAMS, INCLUDING FIRMWARE AND COMPUTER PROGRAMS EMBEDDED IN CISCO EQUIPMENT, AS PROVIDED TO CUSTOMER BY AN APPROVED SOURCE, AND ANY UPGRADES, UPDATES, BUG FIXES OR MODIFIED VERSIONS THEREOF (COLLECTIVELY, "UPGRADES"), ANY OF THE SAME WHICH HAS BEEN RELICENSED UNDER THE CISCO SOFTWARE TRANSFER AND RE-LICENSING POLICY (AS MAY BE AMENDED BY CISCO FROM TIME TO TIME) OR BACKUP COPIES OF ANY OF THE FOREGOING.

License. Conditioned upon compliance with the terms and conditions of the Agreement, Cisco grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees to an Approved Source. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) pertaining to the Software and made available by an Approved Source with the Software in any manner (including on CD-Rom, or on-line). In order to use the Software, Customer may be required to input a registration number or product authorization key and register Customer's copy of

I have read and agree to the End User License Agreement.

⑤

Apply 後、adminパスワードやネットワークの設定が更新される(所要時間:5分程度)。作業はここで一旦終了



## ステップ 2-2: 設定したIPアドレスにアクセス

- 初期設定で入力した IP アドレスと adminパスワードを使い FMCの Web GUI へブラウザでHTTPSアクセスしログイン

※ ブラウザアクセスする端末の IP アドレスは、初期設定で変更した FMCのIPアドレスを同一セグメントのIPアドレスを使用 (ステップ1で 192.168.45.2に変更いただいているため、ここでは注意)



For technical/system questions , e-mail [tac@cisco.com](mailto:tac@cisco.com)  
or call us at 1-800-553-2447 or 1-408-526-7209



Login

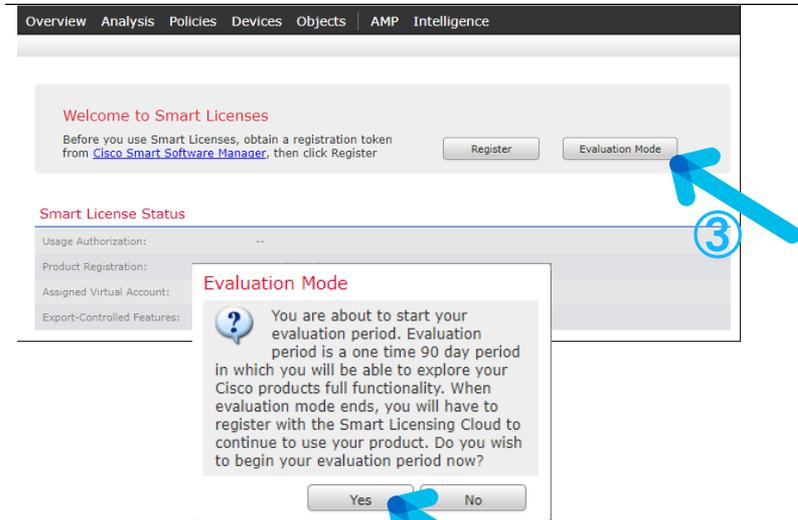
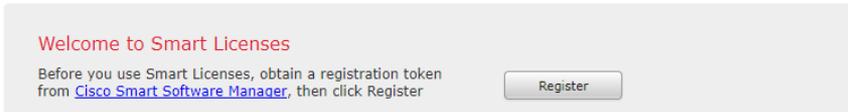
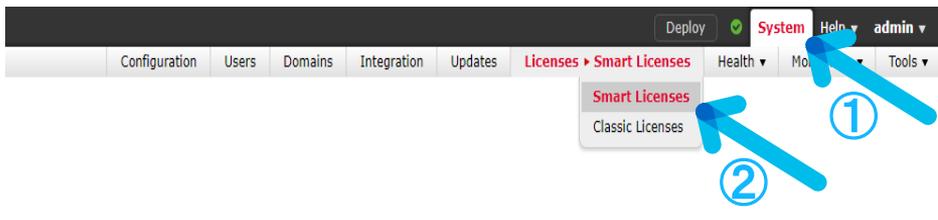
Username

Password



# ステップ 3: ライセンスの追加

ここではEvaluation Modeを利用する。  
Evaluation Modeでは、90日間AnyConnect以外の全機能が利用可能。



Smart License Status		<a href="#">Cisco Smart Software Manager</a>
Usage Authorization:	N/A	
Product Registration:	<b>5</b> <input checked="" type="checkbox"/> Evaluation Period (Expires in 89 days)	
Assigned Virtual Account:	Evaluation Mode	
Export-Controlled Features:	Disabled	

- ① GUI の上部にある System を選択
- ② Licenses>Smart Licensesを選択
- ③ Evaluation Modeを選択
- ④ Yesを選択
- ⑤ 上記のようになれば、ライセンスが適用されたことになる

# ステップ 1: OVFのデプロイ

- 以下のURLより、Firepower Threat Defense(以下、FTD)の .tarファイルを取得し、7-Zipなどアーカイバで展開

<https://software.cisco.com/download/release.html?mdfid=286306503&catid=268438162&softwareid=286306337&release=6.2.2.1&relind=AVAILABLE&rellifecycle=&reltype=latest>

 Cisco\_Firepower\_Threat\_Defense\_Virtual-ESXi-6.2.2-81.ovf

(注)ソフトウェアバージョンはそのときに適切なものを選ぶこと

- vSphere Client 6.0で .ovf を以下のようにデプロイ  
FTDは管理用に仮想NICを1つ持つため、Management管理ネットワークに所属させる

ソース ネットワーク	ターゲット ネットワーク
Management0-0	VM Network
GigabitEthernet0-0	VM Network 2
GigabitEthernet0-1	外部LAN
GigabitEthernet0-2	内部LAN

- その他vSphere Client上での設定はデフォルトを使用し、デプロイが完了

# ステップ 2-1: アダプタタイプの変更(ESXi 6.0の場合)

ステップ2-1と2-2は10G Interfaceが必要な場合に実施

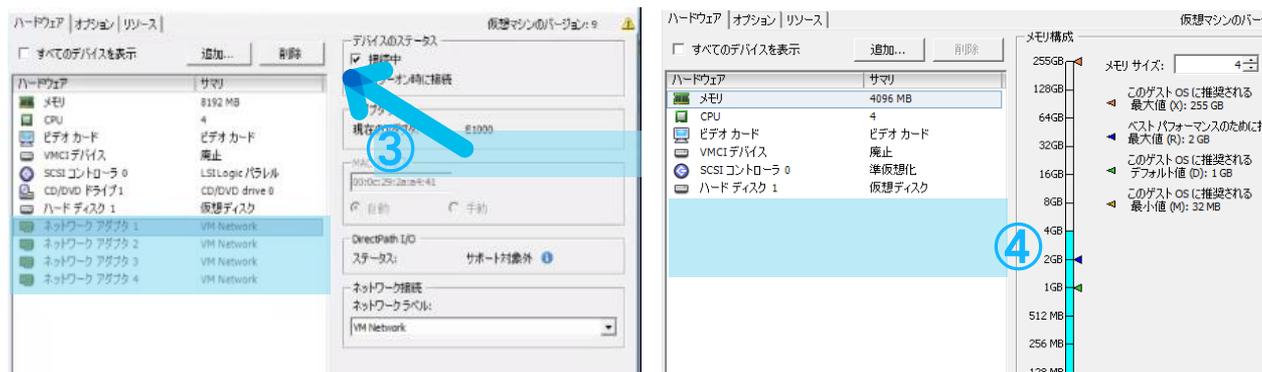


**仮想マシンについて**

仮想マシンは、物理コンピュータと同様に、オペレーティングシステムおよびアプリケーションを実行するソフトウェアコンピュータです。仮想マシン上にインストールしたオペレーティングシステムのことを、ゲストオペレーティングシステム(ゲストOS)といいます。

仮想マシンはそれぞれ隔離されたコンピュータ環境であるため、それらの仮想マシンを、デスクトップまたはワークステーション環境として、あるいはテスト環境として使用したり、サーバアプリケーションの統合に使用したりできます。

仮想マシンはホストで動作します。同一のホストで多数の仮想マシンを実行できます。



## 基本タスク

▶ 仮想マシンのパワーオン

🔧 仮想マシン設定の編集

- ① 作成したFTDの電源がパワーオフであることを確認
- ② FTDの仮想マシン設定の編集を選択
- ③ アダプタタイプ E1000 仮想NICをすべて削除
- ④ 上記のようになれば、仮想NIC削除完了

# ステップ 2-2: アダプタタイプの変更

- ① デバイスの追加を選択
- ② イーサネット アダプタを選択
- ③ アダプタタイプ: VMXNET 3、ネットワークラベルを選択
- ④ 全仮想NICが左記のようになれば、アダプタタイプの変更完了
- ⑤ “OK”を選択

アダプタタイプの変更完了後、FTDの電源をパワーオンにする

# ステップ 3-1: 初期設定

- vSphere Client上でデプロイしたFTDのVMコンソール  を開き、Login プロンプトが表示されたら以下のユーザーでログイン

Username: admin

Password: Admin123

※ユーザー名の入力の前に、Passwordを最初に求められた場合、Enterを一度入力すると以下のようにFirepower login : を表示される。usernameとしてadminと入力し、続けてPasswordを入力

```
firepower login: admin
Password: 
```

- ライセンス契約(EULA)を [SPACE] キーで最後まで表示させ EULA合意を求める以下の表示に対して、“YES”を入力

```
Please enter 'YES' or press <ENTER> to AGREE to the EULA: YES

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password:
Confirm new password: 
```

- Adminユーザーの新規パスワードを設定



## ステップ 3-2: 初期設定

- FTDの管理用IPアドレスを設定

IPv4アドレス、サブネット、デフォルトゲートウェイ、ホスト名、DNS

```
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.71.132.20
2
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.248.
0
Enter the IPv4 default gateway for the management interface []: 10.71.135.254
Enter a fully qualified hostname for this system [firepower]: FTDv
Enter a comma-separated list of DNS servers or 'none' []: 64.104.14.184
Enter a comma-separated list of search domains or 'none' [example.net]: none
```

- FTDの監視用インターフェースの設定

FTDのローカル管理の有無、FWのモード選択(routed or transparent)

```
Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]: routed
Configuring firewall mode ...
```



## ステップ 4: FMCへの登録キーの設定

- **FMCのアドレスと登録キーを設定**

以下のコマンドを使い、FMCへのデバイス登録の設定を行う

後述のFMCからFTDをデバイス登録する際に、この登録キー(この例では“cisco”)が一致している必要あり

```
configure manager add <ip address> <key>
```

```
> configure manager add 10.71.132.201 cisco
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```



# ステップ 1-1: FMCにアクセス

- 初期設定で入力した IP アドレスと adminパスワードを使い FMCの Web GUI ヘブラウザでHTTPSアクセスしログイン



For technical/system questions, e-mail [tac@cisco.com](mailto:tac@cisco.com)  
or call us at 1-800-553-2447 or 1-408-526-7209



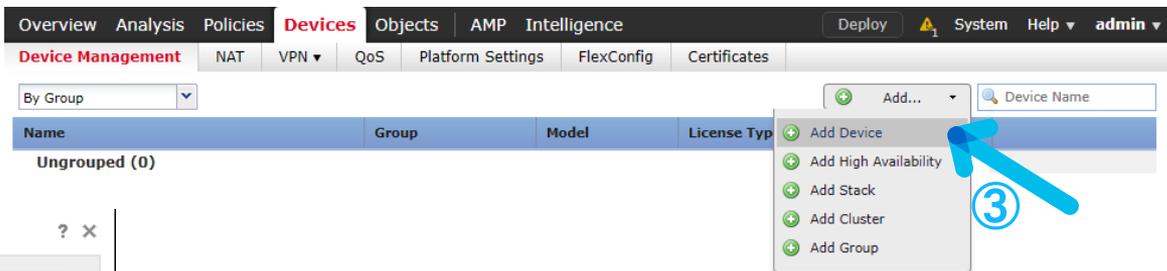
## Login

Username

Password



# ステップ 1-2: FTDデバイスの登録



**Add Device** ? x

Host: 10.71.132.202

Display Name: FTDv 4

Registration Key: cisco

Group: None

Access Control Policy: Create new policy

Smart Licensing: Create new policy 5

- ① GUI の上部にある Devices を選択
- ② Device Management を選択
- ③ Add Device を選択
- ④ FTD の IPアドレスと、登録キーを入力
- ⑤ “Create new Policy” を選択  
引き続き、次のスライドを参照



# ステップ 1-3: FTDデバイスの登録

**New Policy** ? x

Name:  ①

Description:

Select Base Policy:

Default Action:  Block all traffic  Intrusion Prevention  Network Discovery

Objects AMP Intelligence Deploy System Help admin

Deployments Health Tasks

1 total | 0 running 1 success 0 warnings 0 failures Show History

✓ FTDv1 Deployment to device successful. ⑤ 1m 2

**Add Device** ? x

Host:

Display Name:

Registration Key:

Group:

Access Control Policy:

Smart Licensing

Malware:  ③

Threat:

URL Filtering:

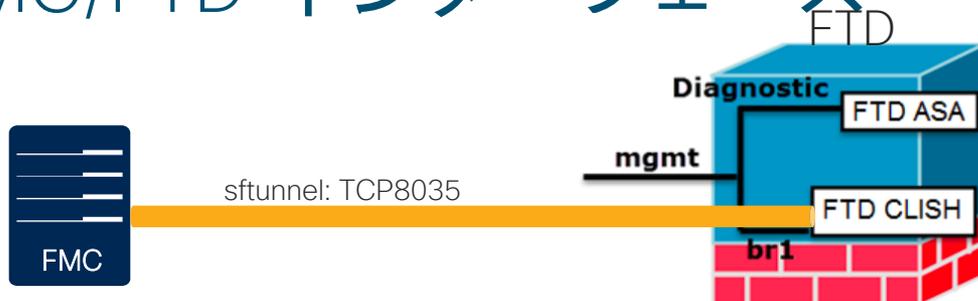
Advanced

On Firepower Threat Defense devices version 6.2.1 onwards, AnyConnect VPN licenses can be enabled from smart license page

- ① 設定ファイル(ポリシー)の名前を入力
- ② “Save” を選択
- ③ Add Deviceの画面に移り、ライセンスを図のように選択
- ④ 最後に Register を選択し、FTDデバイス登録を実行
- ⑤ 上記のようになれば、デバイスの登録完了(所要時間:数分)

以上で、インストール と FTDをFMCで管理するための初期設定は完了

# Tips)FMC/FTD インターフェース



br1

Diagnostic

	br1	Diagnostic
目的	<ul style="list-style-type: none"> <li>•FTD, FMC との通信に使用 (sftunnel)</li> <li>•FTD box への SSH アクセスに使用</li> </ul>	<ul style="list-style-type: none"> <li>•ASA engine へのリモートアクセスに使用</li> <li>•ASA engine syslog の Source IP として使用</li> </ul>
必須条件	<p>[必須]</p> <p>FTD, FMC との通信に利用される (sftunnel)</p>	<p>[任意] ※設定は非推奨</p> <p>ASA engine syslog 等を送信したい場合、data interface を利用することを推奨</p>
確認方法	<p>(CLISH CLIより)</p> <p>&gt;show network</p> <p>(FMC GUIより)</p> <p>Devices &gt; Device Management &gt; Device &gt; Management</p>	<p>(CLISH CLIより)</p> <p>&gt;show interface ip brief</p> <p>(FMC GUIより)</p> <p>Devices &gt; Device Management を選択</p> <p>対象デバイスのEditボタン</p>

## 2. FTDとFMCその他初期設定

# FTDとFMCその他初期設定に関して

- FTDのネットワーク周りで行うべき最低限の設定を行う
  - Time Synchronization
  - Interface
  - Routing
  - NAT
  - Access Control Policy
  - Network Discovery Policy

# Network Discoveryの概要

Edit Rule

Action: Discover  Hosts  Users  Applications

- Snortエンジンを通過する通信から以下の3つ情報を学習
- ホスト
  - パッシブディテクション（OSフィンガープリンティング等）により情報を収集し、ネットワークマップにホストエントリを作成
  - ホスト情報は、ホストインプットAPI経由のマニュアル設定および、GUI経由の手動編集に対応
- アプリケーション
  - ホストの利用アプリケーションを検出しネットワークマップに追加
  - ホストやユーザのディスカバリ利用時には有効化が必須
- ユーザ
  - ユーザテーブルを作成し、ネットワークアクティビティ（ログイン等）を記録

## Firepower Management Center (FMC)



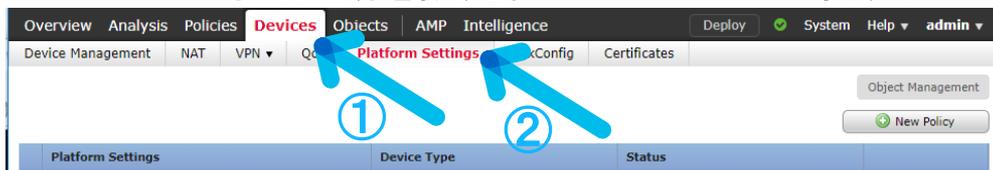
## Firepower



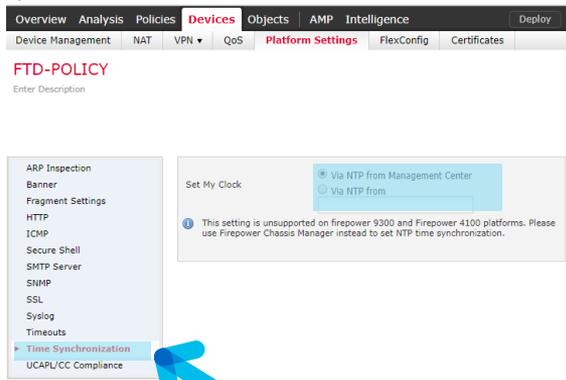
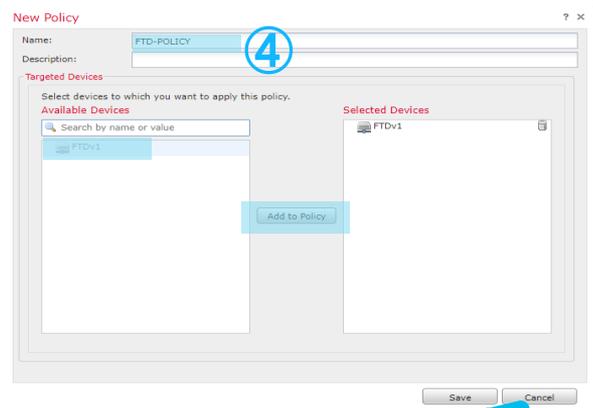


# ステップ1-1 : Time Synchronization

- ・ FTDの時刻同期を設定。ここではFMCに従うものとする。



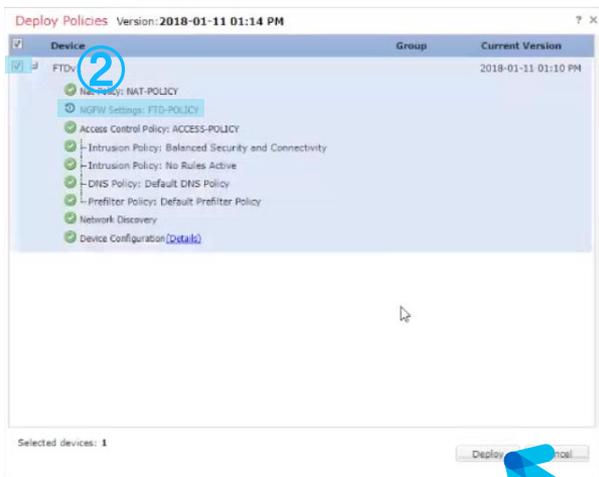
There are no policies created. Add a new [Firepower Settings Policy](#) (or) [Threat Defense Settings Policy](#)



- ① Devicesを選択
- ② Platform Settingsを選択
- ③ Threat Defense settings Policyを選択
- ④ ポリシー設定の名前を入力、適用するデバイスを選択
- ⑤ "Save"を選択
- ⑥ Time Synchronizationを選択すると、上記の設定となっている



# ステップ1-2 : Time Synchronization



- ① “Deploy”を選択
- ② 変更された設定を確認の上、Deploy対象機器にチェックを入れる
- ③ “Deploy”を選択

(注)FP4100,FP9300のNTPはFXOS側の設定に従う。  
ただし、ここで設定しても無視されるだけで問題は無い。



# ステップ2 : Interface

## ・ FTDのRouted Interfaceを設定

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

Device Management NAT VPN Platform Settings FlexConfig Certificates

By Group Add... Device Name

Name	Group	Model	License Type	Access Control Pol...
4 Ungrouped (1)				

FTDv1  
10.71.132.202 - Cisco Firepower Threat Defense

Device Routing **Interfaces** Inline Sets DHCP

S...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Sta...	IP Address
0	GigabitEthernet0/0		Physical			
0	GigabitEthernet0/1		Physical			
0	Diagnostic0/0	diagnostic	Physical			

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTDv1  
Cisco Firepower Threat Defense for VMWare

You have unsaved changes Save Cancel

Please save the configuration to make the changes available.

S...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Sta...	IP Address
0	GigabitEthernet0/0	outside	Physical	outside_zone		192.168.250.1/24(Static)
0	GigabitEthernet0/1	inside	Physical	inside_zone		192.168.1.1/24(Static)
0	Diagnostic0/0	diagnostic	Physical			

Edit Physical Interface

Mode: None

Name: outside Enabled Management Only

Security Zone: outside\_zone

Description:

General IPv4 IPv6 Advanced Hardware Configuration

IP Type: Use Static IP

IP Address: 192.168.250.1/24 eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

OK Cancel

- ① Devicesを選択
- ② Device Managementを選択
- ③ 鉛筆マークを選択
- ④ G0/0の鉛筆マークを選択
- ⑤ 物理インターフェースの名前、Enabled、Security Zoneの名前、IP Type、IPv4アドレス、サブネットを入力
- ⑥ “OK”を選択
- ⑦ G0/1も同様にインターフェース設定を行い、“Save”を選択



# ステップ3-1 : Routing

- ・ FTDのデフォルトゲートウェイを設定。管理用のゲートウェイではなく実トラフィック用であることに注意

- ① Routingを選択
- ② Static Routeを選択
- ③ Add Routeを選択
- ④ Interface (宛先)、any-ipv4を選択し、“Add”を選択
- ⑤ プラスマークを選択
- ⑥ オブジェクトの名前、ゲートウェイを入力し、“Save”を選択
- ⑦ “OK”を選択



## ステップ3-2 : Routing

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTDv  
Cisco Firepower Threat Defense for VMWare

Device Routing Interfaces Inline Sets DHCP

OSPF  
OSPFv3  
RIP  
BGP  
Static Route  
Multicast Routing

Network	Interface	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes					
any-ipv4	outside	192.168.250...	false	1	
▼ IPv6 Routes					

Deploy Policies Version: 2017-12-13 02:35 PM

Device	Group	Current Version
<input checked="" type="checkbox"/>		2017-12-13 02:13 PM

- ICFW Settings: FTD\_settings
- Control Policy: ACP-1
- Intrusion Policy: No Rules Active
- Intrusion Policy: Balanced Security and Connectivity
- Pre-filter Policy: Default Prefilter Policy
- Network Discovery
- Device Configuration [Details]

Selected devices: 1

Deploy Cancel

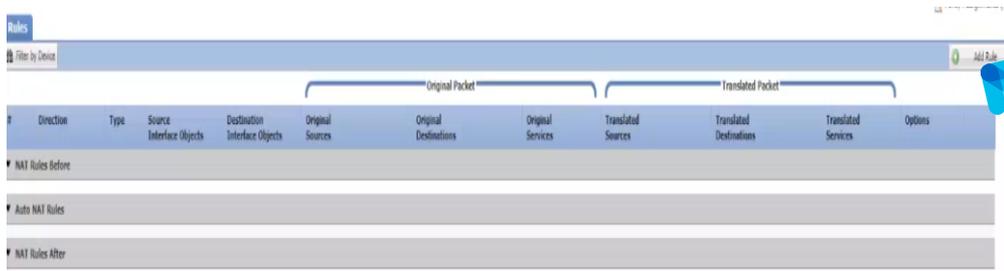
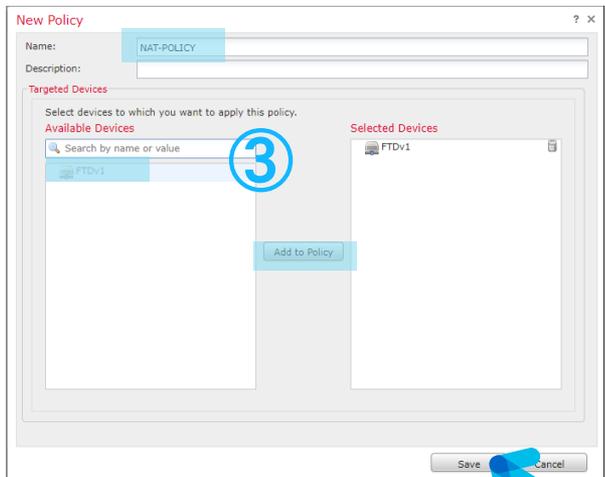
- ① “Save”を選択  
※FMC上でのSaveであり、実機(FTD)にはまだ反映されていない
- ② “Deploy”を選択
- ③ 変更された設定を確認の上、Deploy対象機器にチェックを入れる
- ④ ”Deploy”を選択

④のDeploy 後、実機にポリシーなど設定が反映される(所要時間:数分-10分程度)。



# ステップ4-1 : NAT

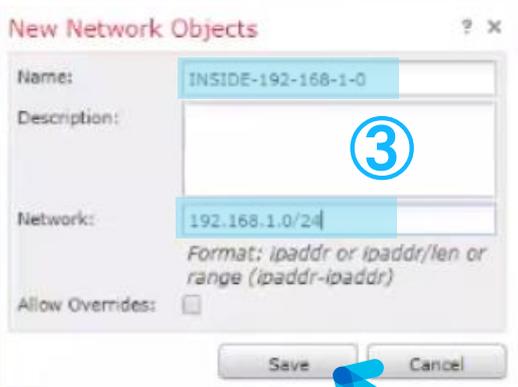
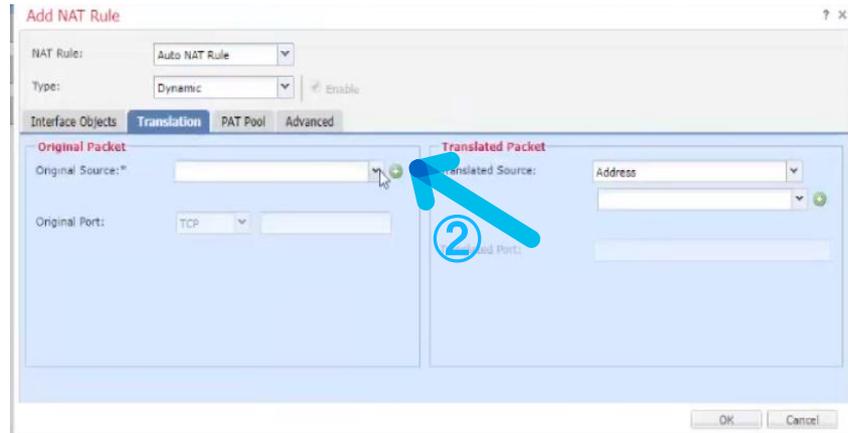
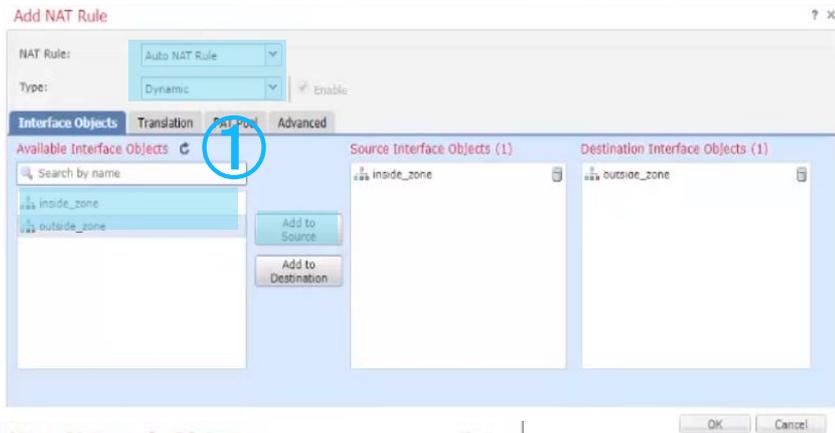
- ・ FTDで行うNAT(PAT)を設定



- ① Devicesを選択
- ② NATを選択
- ③ “Threat Defense NAT Policy”を選択
- ④ NAT Policyの名前、対象機器を選択し、“Save”
- ⑤ “Add”を選択



# ステップ4-2 : NAT



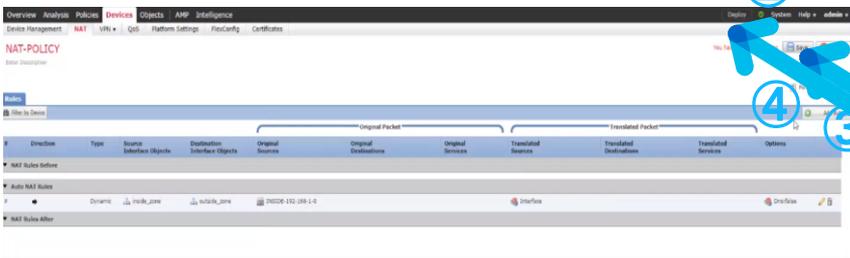
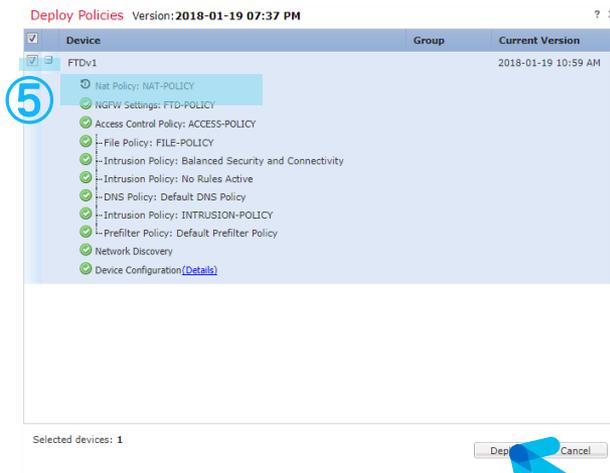
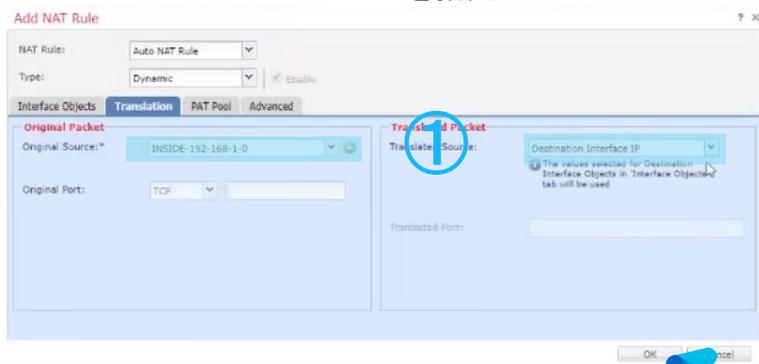
変換されるネットワークアドレス (ここでは 192.168.1.0/24) を登録

- ① NAT Rule、Type、SourceおよびDestinationの Interface Objectsを選択
- ② プラスマークを選択
- ③ Network Objectの名前、Original Sourceを入力
- ④ “Save”を選択



# ステップ4-3 : NAT

Destination Sourceはどのアドレスに変換するかを設定。ここでは出ていくInterfaceのIPアドレスを指定



- ① Original Source、Destination Sourceを選択
- ② “OK”を選択
- ③ “Save”を選択
- ④ “Deploy”を選択
- ⑤ 変更された設定を確認の上、Deploy対象機器にチェックを入れる
- ⑥ “Deploy”を選択



# ステップ5-1 : Access Control Policy

- FTDを介した通信を制御するポリシー(Access Control Policy)を修正

The screenshot shows the Firepower Management Center interface. The 'Policies' tab is selected, and the 'Access Control' sub-tab is active. A table lists the 'ACCESS-POLICY'. A pencil icon is clicked to edit the policy. The 'Default Action' is set to 'Trust All Traffic'. The 'Logging' section is expanded, and the 'Log at Beginning of Connection' and 'Log at End of Connection' options are checked. The 'OK' button is clicked to save the changes.

とりあえず全ての通信を信頼 (許可) するのであれば、Default Actionは Trust all Trafficとする

- ① Policiesを選択
- ② Access Control>Access Controlを選択
- ③ 鉛筆マークを選択
- ④ Default Actionを選択
- ⑤ 紙のマークを選択
- ⑥ Loggingで通信許可したlogをどこで取得するか選択
- ⑦ “OK”を選択



# ステップ5-2 : Access Control Policy



Deploy Policies Version:2018-01-19 08:15 PM



- ① “Save”を選択
- ② “Deploy”を選択
- ③ 変更された設定を確認の上、Deploy対象機器にチェックを入れる
- ④ “Deploy”を選択





# ステップ6-1 : Network Discovery Policy

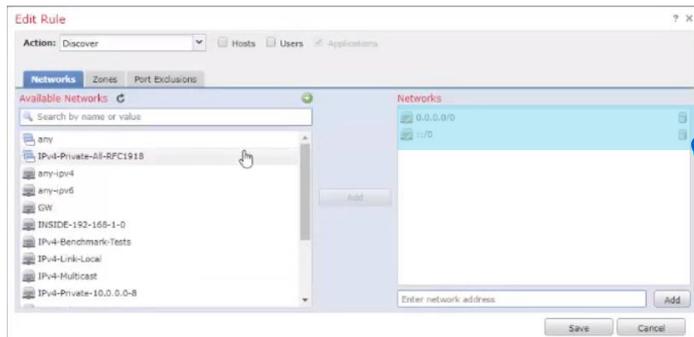
- Network Discovery Policyとは
  - 指定されたネットワーク内で、どのホスト、OS、アプリケーション等が存在するかを監視し、FMCで記憶していくためのポリシー
  - このポリシーでは監視する範囲を決め、その設定を有効にする



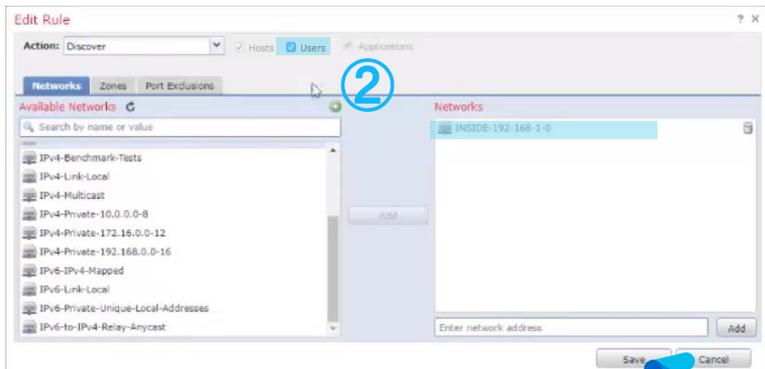
- ① Policiesを選択
- ② Network Discoveryを選択
- ③ 鉛筆マークを選択



# ステップ6-2 : Network Discovery Policy

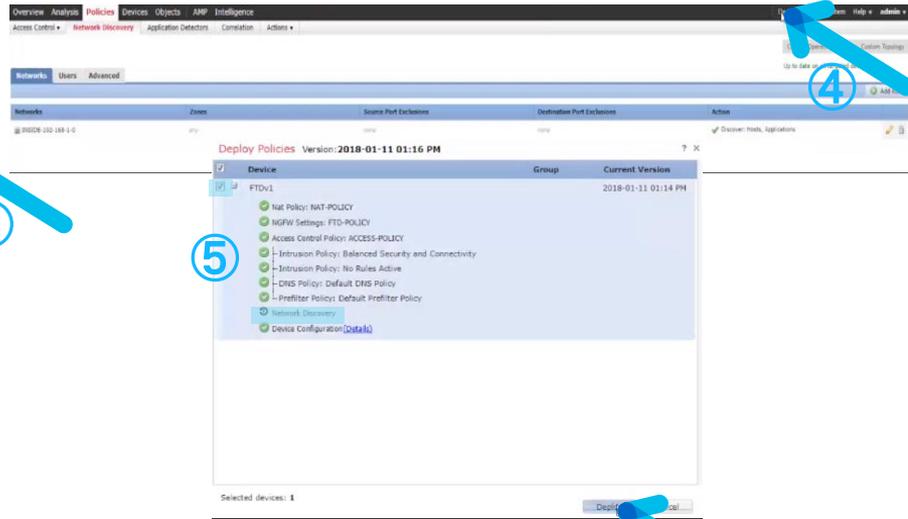


①



②

③



④

⑤

⑥

- ① ゴミ箱マークを選択し、ネットワーク0.0.0.0を削除
- ② 監視対象ネットワークを選択し、Usersにチェックを入れる（自動的にHostsも選択される）
- ③ “Save”を選択
- ④ “Deploy”を選択
- ⑤ 変更された設定を確認の上、Deploy対象機器にチェックを入れる
- ⑥ “Deploy”を選択



# ステップ6-3 : Network Discovery Policy

- ・ FMCが記録したホスト情報を確認

The screenshot shows the Firepower Management Center interface. The navigation menu on the left has 'Analysis' selected (indicated by arrow 1) and 'Hosts > Network Map' selected (indicated by arrow 2). The main content area displays the 'Host Profile' for IP 192.168.1.101. The profile includes the following information:

- Host Profile:** IP Address: 192.168.1.101, NetBIOS Name: 192.168.1.101, Device (Hops): FTDev101, MAC Addresses (TTL): 00:0C:29:14:00:03:4A (VMware, Inc.) (128), Host Type: Host, Last Seen: 2018-01-11 13:18:20, Current User: View
- Indications of Compromise:** (0)
- Operating System:** Vendor: Microsoft, Product: Windows, Version: 7, Phone 7.5, Phone 8.0, 8, Server 2012, 8.1, Server 2012 R2, 10, Source: Firepower
- Applications:** (1) Application Protocol: pending, Client:  DNS, Version: , Web Application:
- Users:** (no user history available)
- Attributes:** Host Criticality: None
- Host Protocols:** Protocol: Layer: tcp: Transport, udp: Transport, IP: Network
- Vulnerabilities:** (264)

- ① Analysisを選択
- ② Hosts>Network Mapを選択

IPアドレス、OSや使用されたアプリケーション、ポート番号等の特徴が表示される

### 3. Intrusion Policy設定

# Intrusion Policy概要(1/2)

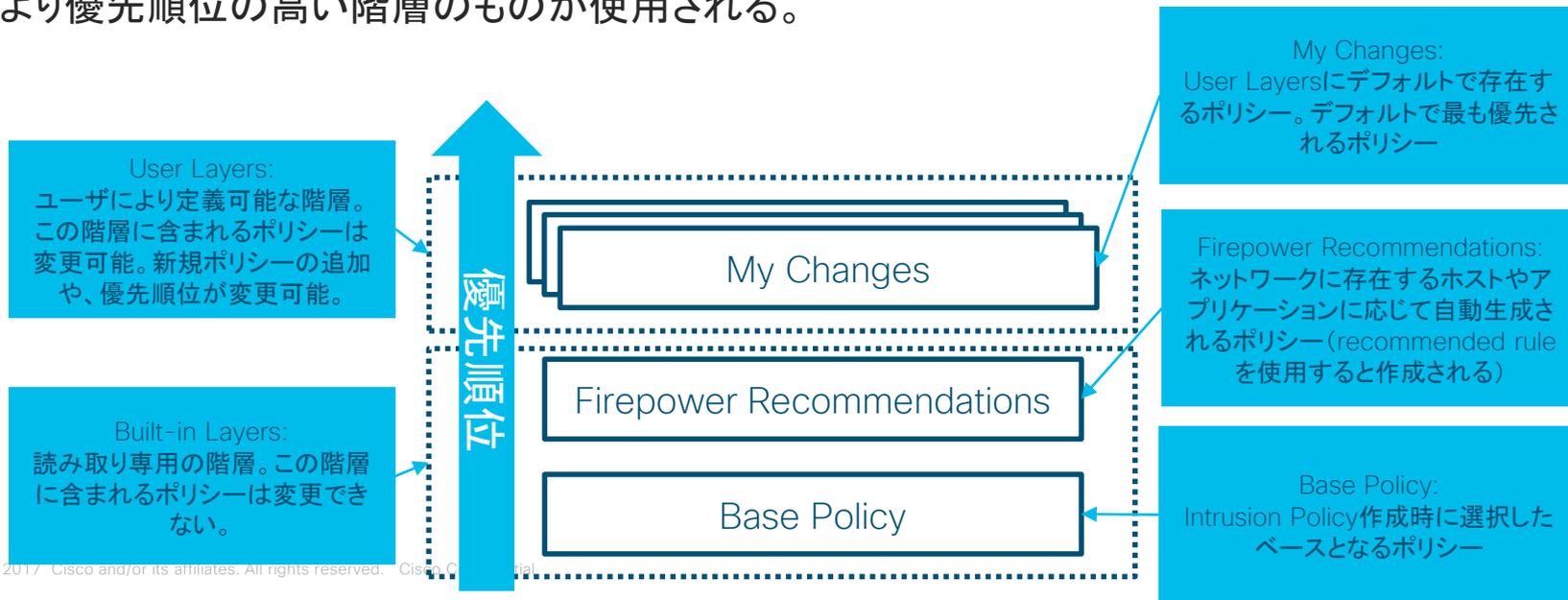
Intrusion Policyにはシグネチャに対するパラメータが含まれ、トラフィックに対するIPSの振る舞いを制御する。

## ■シグネチャのパラメータ

項目	パラメータ	説明
Rule State	<ul style="list-style-type: none"><li>• Generate Events</li><li>• Drop and Generate Events</li><li>• Disable</li><li>• <b>Inherit</b></li></ul>	シグネチャヒット時の動作設定
Event Filtering	<ul style="list-style-type: none"><li>• Threshold</li><li>• Suppression</li></ul>	一定時間に出力されるイベント数、イベント出力に必要なシグネチャヒット回数、イベント抑制等の設定
Dynamic State	Rate-Based Rule State	シグネチャのヒット頻度に応じてヒット時の動作を変化させる設定
Alerting	SNMP Alert	<b>ヒット時のSNMPアラートの設定</b>

# Intrusion Policy概要(2/2)

Intrusion Policyは階層ポリシー構造をとる。階層はUser LayersとBuilt-in Layersに大別される。Built-in Layersは読み取り専用なためユーザがポリシーの内容や順番を変更できるのはUser Layersに含まれるポリシーのみである。ポリシー間で異なるパラメータが競合する場合はより優先順位の高い階層のものが使用される。



# Variable Set の概要

- Snort IPS Rule内で使用される変数
- 対象IPアドレスやポートに利用されるため、環境に合わせて変更することでイベントの精度が高まる

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SERVER-APACHE Apache Struts allowStaticMethodAccess invocation attempt"; flow:to_server,established; content:".do"; nocase; http_uri; content:"allowStaticMethodAccess"; nocase; http_client_body; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service http; reference:bugtraq,60166; reference:cve,2013-1966; reference:cve,2013-2115; reference:url,struts.apache.org/development/2.x/docs/s2-014.html; classtype:attempted-admin; sid:29859; rev:6; )
```

- 上記はApache Strutsの脆弱性を検知する実際のSnort Rule
- 上記のケースでは、\$Home\_NETはお客様の保有するサーバや社内IPアドレス群に該当

# 今回設定するIntrusion Policyについて

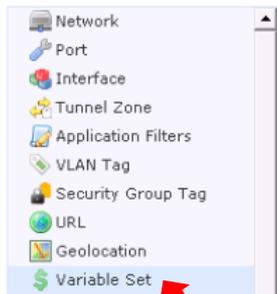
- 評価を目的としているため、トラフィックに影響を与えない様シグネチャヒット時にパケットを破棄しないポリシーを作成する
- 有意義な評価を行うために、一般的な環境でヒットしやすい一部のシグネチャを手動で有効にする
- IPS機能が正常に動作していることを確認するために、Pingでヒットするシグネチャを手動で有効にする

# 設定の流れ

- ステップ1 : Variable Set の変更
- ステップ2 : Intrusion Rule のアップデート
- ステップ3 : Intrusion Policy の作成
- ステップ4 : POV用にシグネチャの手動設定

# ステップ1 Variable Set 変更

Object > Object Management > Variable Set



クリック

Name	Description
Default-Set	This Variable Set is system-provided.

Edit Variable Set Default-Set

Name: Default-Set  
Description: This Variable Set is system-provided.

Variable Name	Type	Value
AIM_SERVERS	Network	[64.12.31.136/32, 205.188.210.203/32, 6...]
DNS_SERVERS	Network	HOME_NET
EXTERNAL_NET	Network	any
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]
FTP_PORTS	Port	[21, 2100, 3535]
GTP_PORTS	Port	[3386, 2123, 2152]
HOME_NET	Network	any
HTTP_PORTS	Port	[8300, 8040, 2231, 90, 6767, 443, 8983,...]
HTTP_SERVERS	Network	HOME_NET
ORACLE_PORTS	Port	any

HOME\_NETのペンシルアイコンをクリックする

クリック

# ステップ1 Variable Set 変更 (HOME\_NET)

攻撃から守るHOME\_NETのIPアドレス郡を選択する。

ここでは初期設定済み IPv4 Private-192.168.0.0/16 を設定する。

※実環境においては、お客様ごとに環境が異なるため、要確認。

Edit Variable HOME\_NET

Name: HOME\_NET  
Type: Network

Available Networks

- any
- IPv4-Private-All-RFC1918
- any-ipv4
- any-ipv6
- ASA-GW
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-16**
- IPv6-IPv4-Mapped
- IPv6-Link-Local
- IPv6-Private-Unique-Local-Addresses
- IPv6-to-IPv4-Relay-Anycast

Included Networks (1)

- IPv4-Private-192.168.0.0-16

Excluded Networks (0)

none

Include

Exclude

Network Enter an IP address Add

Network Enter an IP address Add

Save Cancel

Save

This variable set is in use by an Access Control policy. Modifying it may affect detection, and you must reapply the policy before changes take effect.

Changes to the Default Set will also change the default values in all other sets. Do you wish to continue?

Yes

No

# ステップ2 Intrusion Ruleのアップデート

System > Updates > Rule Updates

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Product Updates Rule Updates Geolocation Updates

Delete All Local Rules Rule Update Log

### One-Time Rule Update/Rules Import

Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Source

Rule update or text rule file to upload and install  
Choose File No file chosen

Download new rule update from the Support Site

Policy Deploy

Reapply all policies after the rule update import completes

**Import**

### Recurring Rule Update Imports

The scheduled rule update feature is not enabled.  
Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Enable Recurring Rule Update Imports from the Support Site

Import Frequency: Daily at 4:00 AM Asia/Tokyo

Policy Deploy  Deploy updated policies to targeted devices after rule update completes

Save Cancel

### Recurring Rule Update Imports

The scheduled rule update feature is not enabled.  
Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Enable Recurring Rule Update Imports from the Support Site

Import Frequency: Daily at 4:00 AM Asia/Tokyo

Policy Deploy  Deploy updated policies to targeted devices after rule update completes

Save Cancel

## 【オプション】

Enable Recurring Rule Update Imports from Support Siteをチェックすると、Intrusion Ruleの自動更新の設定が可能

# ステップ2 Intrusion Ruleのアップデート

Intrusion Ruleのアップデートが完了すると、Rule Update Import Log画面に自動的に遷移する。

①クリック

Time	Name	Type	Action	SID	Revis	Policy
2018-02-01 18:11:18	Sourcefire Rule Update	rule update component	changed			
2018-02-01 18:11:17	Sourcefire Decoder Rule Pack	rule update component	changed			
2018-02-01 18:11:12	Sourcefire Module Pack	rule update component	changed			
2018-02-01 18:11:10	SERVER-OTHER_Cisco ASA VPN aggregateAuthData&sender_double_free_attempt	rule	new	45575	2	All
2018-02-01 18:11:02	Sourcefire Rule Pack	rule update component	changed			
2018-02-01 18:11:01	SQL_i = 1 - possible sql injection attempt	rule	changed	22287	4	All
2018-02-01 18:11:01	SQL_generic sql exec injection attempt - POST parameter	rule	changed	15877	9	All
2018-02-01 18:11:01	SQL_Suspicious SQL_ansi_padding option	rule	changed	16074	4	All
2018-02-01 18:11:01	SERVER-WEBAPP_Vivotek IP Cameras remote stack buffer overflow attempt	rule	changed	45261	2	All
2018-02-01 18:11:01	SERVER-WEBAPP_Axis Communications IP camera SSI command injection attempt	rule	changed	45237	2	All
2018-02-01 18:11:01	SQL_generic sql update injection attempt - POST parameter	rule	changed	26829	3	All
2018-02-01 18:11:01	SERVER-WEBAPP_Delta IEM DIAEnergie file upload attempt	rule	changed	45250	2	All
2018-02-01 18:11:01	SQL_parameter ending in comment characters - possible sql injection attempt - POST	rule	changed	21278	6	All
2018-02-01 18:11:01	SQL_i = 1 - possible sql injection attempt	rule	changed	19439	9	All
2018-02-01 18:11:01	SQL_use of sleep function with and - likely SQL injection	rule	changed	41449	2	All
2018-02-01 18:11:01	SQL_use of sleep function with select - likely SQL injection	rule	changed	37443	2	All
2018-02-01 18:11:01	SQL_use of sleep function in HTTP header - likely SQL injection attempt	rule	changed	38993	8	All

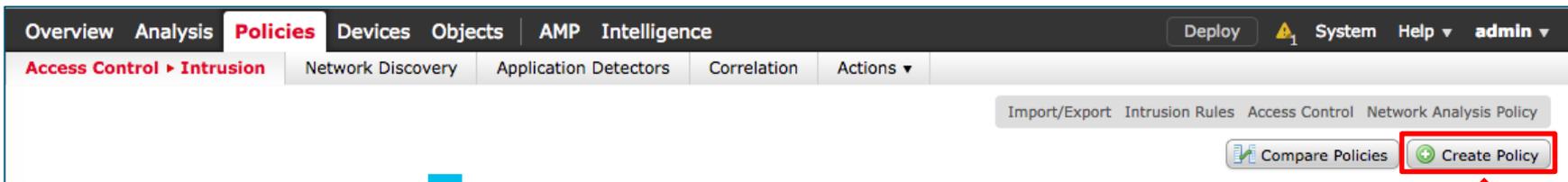


②Ruleのアップデートが完了していることを確認する。

Summary	Time	User ID	Status
Snort Rule Update 2018 01 31 002 vrt Completed install of Snort Rule Update 2018-01-31-002-vrt	2018-02-01 18:09:05	admin	✓
Snort Rule Update 2018 01 24 001 vrt Completed install of Snort Rule Update 2018-01-24-001-vrt	2018-01-26 04:02:51	admin	✓
Snort Rule Update 2018 01 22 001 vrt Completed install of Snort Rule Update 2018-01-22-001-vrt	2018-01-24 04:00:33	admin	✓
Snort Rule Update 2018 01 19 001 vrt Completed install of Snort Rule Update 2018-01-19-001-vrt	2018-01-21 04:00:38	admin	✓
Snort Rule Update 2018 01 16 001 vrt Completed install of Snort Rule Update 2018-01-16-001-vrt	2018-01-20 21:38:20	admin	✓
Snort Rule Update 2018 01 16 001 vrt Completed install of Snort Rule Update 2018-01-16-001-vrt	2018-01-17 15:17:20	admin6	✓
Snort Rule Update 2016 11 29 001 vrt Completed install of Snort Rule Update 2016-11-29-001-vrt	2017-12-13 13:04:46	admin	✓

# ステップ2 Intrusion Policyの作成

- Policies > Intrusion にて Create Policy をクリック



①クリック

The 'Create Intrusion Policy' dialog box is shown. It has a title bar with a question mark and a close button. The main content area is titled 'Policy Information' and contains the following fields:

- Name \***: A text input field containing 'INTRUSION-POLICY', highlighted with a red box.
- Description**: An empty text input field.
- Drop when Inline**: A checkbox that is unchecked, highlighted with a red box.
- Base Policy**: A dropdown menu showing 'Balanced Security and Connectivity'.

At the bottom left, there is a note '\* Required'. At the bottom right, there are two buttons: 'Create Policy' and 'Create and Edit Policy', both highlighted with red boxes.

②Intrusion Policyに名前を設定、本資料では INTRUSION-POLICY を使用

③チェックを外す(ここのチェックを外すと、シグネチャの設定がヒット時の破棄の場合も破棄されなくなる)

④クリックすると Intrusion Policy が作成されて編集画面(次ページ)が開く

# ステップ3 : POV用にシグネチャの手動設定

Policies > Intrusion にて作成した Intrusion Policy の鉛筆マーク✎をクリックすると Intrusion Policy の編集画面が開く

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy 1 System Help admin

Access Control > Intrusion Network Discovery Application Detectors Correlation Actions

### Edit Policy: INTRUSION-POLICY

Policy Information

- Rules
- Firepower Recommendations
- Advanced Settings
- Policy Layers

Policy Information < Back

Name: INTRUSION-POLICY

Description:

Drop when Inline:

Base Policy: Balanced Security and Connectivity Manage Base Policy

The base policy is up to date (Rule Update 2018-02-13-001-vrt)

This policy has 8834 enabled rules Manage Rules

- 97 rules generate events View
- 8737 rules drop and generate events View

No recommendations have been generated. Click here to set up Firepower recommendations.

Commit Changes Discard Changes

# ステップ3 : POV用にシグネチャの手動設定

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

Access Control > Intrusion Network Discovery Application Detectors Correlation Actions

Edit Policy: INTRUSION-POLICY

Policy Information

Rules

Rule Configuration

Rule Content

Category

app-detect

app-detect

browser-firefox

browser-ie

browser-other

browser-plugins

browser-webkit

content-replace

decoder

exploit-kit

file-executable

file-flash

file-identify

file-image

file-java

file-multimedia

Classifications

Microsoft Vulnerabilities

Microsoft Worms

Platform Specific

Preprocessors

Priority

Rule Update

Filter: malware

5893 selected rules of 5893

Rule State Event Filtering Dynamic State Alerting Comments

Generate Events

Drop and Generate Events

Rule ID	Rule Name	Action
1	26897 EXPLOIT-KIT Flashpack/Safe/CritX exploit kit malware download	×
1	43180 FILE-OFFICE Powerpoint mouseover powershell malware download attempt	×
1	43179 FILE-OFFICE Powerpoint mouseover powershell malware download attempt	×
1	21489 FILE-OTHER Microsoft Windows chm file malware related exploit	→
1	39851 INDICATOR-COMPROMISE Connection to malware sinkhole - CERT.PL	×
1	31214 INDICATOR-COMPROMISE connection to zeus malware sinkhole	×
1	33215 INDICATOR-COMPROMISE DNS request for known malware domain icanhazip.com	→
1	33216 INDICATOR-COMPROMISE DNS request for known malware domain tor2web.org	→
1	44037 INDICATOR-COMPROMISE DNS request for known malware sinkhole domain luqerfso9ifjaposdfjhgosurijfaewrgwea.com - WannaCry	→

1 of 118

Success

Successfully set the rule state for 5893 rule(s)

OK

②チェックを入れ  
フィルタされたシグ  
ネチャをすべて選択

①malwareをキー  
ワードにフィルタ

③Rule State ドロ  
ップダウンメニューを  
開き、Drop and  
Generate Events  
を選択

④正常に変更が完了したら上記のプロ  
ンプトが表示されるのでOKをクリック

⑤同様の操作を、Blacklist、PUA というキーワードで実施する。

# ステップ3 : POV用にシグネチャの手動設定

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

Access Control > Intrusion Network Discovery Application Detectors Correlation Actions

Edit Policy: INTRUSION-POLICY

Policy Information

Rules

Firepower Recommendations

Advanced Settings Policy Layers

Rules

Rule Configuration

Rule Content

Category

app-detect

browser-firefox

browser-ie

browser-other

browser-plugins

browser-webkit

content-replace

decoder

file-executable

file-flash

file-identify

file-image

file-java

file-multimedia

Classifications

Microsoft Vulnerabilities

Microsoft Worms

Platform Specific

Preprocessors

Priority

Rule Update

Filter: Category:"exploit-kit" 741 selected rules of 741

Rule State Event Filtering Dynamic State Alerting Comments

Generate Events

Drop and Generate Events

Disable

Rule ID	Rule Name	Rule State
1	EXPLOIT-KIT Angler exploit kit Adobe Flash encoded shellcode detected	✗
33187	EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download	✗
33271	EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download	✗
33272	EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download	✗
33186	EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download	✗
33274	EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download	✗
33286	EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download	✗
33273	EXPLOIT-KIT Angler exploit kit Adobe Flash SWF exploit download	✗
36071	EXPLOIT-KIT Angler exploit kit browser version detection attempt	✗
36802	EXPLOIT-KIT Angler exploit kit browser version detection attempt	⇒
38682	EXPLOIT-KIT Angler Exploit Kit email gate	✗
31331	EXPLOIT-KIT Angler exploit kit encrypted binary download	⇒

Last login on Wednesday, 2018-01-31 at 21:38:11 PM from 10.70.235.239

CISCO

②チェックを入れフィルタされたシグネチャをすべて選択

①Category から exploit-kit を選択する

③Rule State ドロップダウンメニューを開き、Drop and Generate Events を選択

④正常に変更が完了したら上記のプロンプトが表示されるのでOKをクリック

# ステップ3 : POV用にシグネチャの自動設定



③ Rule State ドロップダウンメニューを開き、Generate Events を選択

② GID1、SID408 「PROTOCOL-ICMP ECHO REPLY」をチェック

① ICMPをキーワードにフィルタ

④ 正常に変更が完了したら上記のプロンプトが表示されるのでOKをクリック

# ステップ3 : POV用にシグネチャの手動設定

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

Access Control > Intrusion Network Discovery Application Detectors Correlation Actions

Edit Policy: INTRUSION-POLICY

Policy Information

Rules

Rule Configuration

Rule Content

Category

Rule State	Event Filtering	Dynamic State	Alerting	Comments
<input type="checkbox"/>				
1	37062	APP-DETECT 12P DNS request attempt		
1	28071	APP-DETECT 360.cn SafeGuard local HTTP management console access attempt		
1	28068	APP-DETECT 360.cn Safeguard runtime outbound communication		
1	32845	APP-DETECT Absolute Software Computrace outbound connection - 209.53.113.223		
1	32846	APP-DETECT Absolute Software Computrace outbound connection - absolute.com		
1	32847	APP-DETECT Absolute Software Computrace outbound connection - bh.namequery.com		
1	32848	APP-DETECT Absolute Software Computrace outbound connection - namequery.nettrace.co.za		
1	26286	APP-DETECT Absolute Software Computrace outbound connection - search.dnssearch.org		
1	26287	APP-DETECT Absolute Software Computrace outbound connection - search.namequery.com		
1	32849	APP-DETECT Absolute Software Computrace outbound connection - search.us.namequery.com		
1	32850	APP-DETECT Absolute Software Computrace outbound connection - search2.namequery.com		
1	32851	APP-DETECT Absolute Software Computrace outbound connection - search64.namequery.com		

Commit Changes Discard Changes

Last login on Wednesday, 2018-01-31 at 21:38:11 PM from 10.70.235.239

①シグネチャの設定変更が完了したらここをクリック

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

Access Control > Intrusion Network Discovery Application Detectors Correlation Actions

Edit Policy: INTRUSION-POLICY

Policy Information

Name: INTRUSION-POLICY

Description:

Drop when Inline:

Base Policy: Balanced Security and Connectivity 2

This policy has 11798 enabled rules

23 rules generate events

11769 rules drop and generate events

No recommendations have been generated. Click here to set up firewall recommendations.

This policy contains enabled preprocessor rules. Please read the rule documentation to ensure the preprocessors have the correct settings for these rules.

Commit Changes Discard Changes

Last login on Wednesday, 2018-01-31 at 21:38:11 PM from 10.70.235.239

②Commit Changesをクリック

Description of Changes

date, what changed, user, reason|

OK Cancel

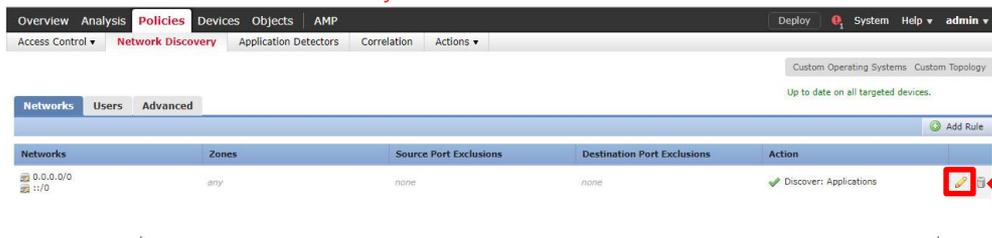
③コメントを記入してOKをクリック

# 【参考情報】

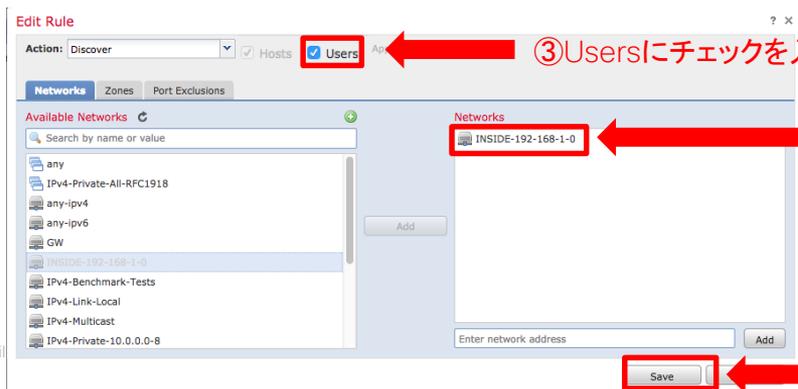
## Firepower recommendation によるルール最適化

Firepower recommendationは、Network Discovery の結果生成されるホストプロファイルを元に、ネットワーク上に存在するホストやアプリケーションに適切なシグネチャパラメータを自動的に生成する機能である。Network Discovery Policy内のルールのデフォルトの設定では、Applicationのみが検出対象になっている。ホストのOS等を使用してより精度の高いパラメータを生成するためには、UsersとHostsを検出対象に含める。

①Policies > Network Discovery をクリック



②設定を変更する  
ルールの鉛筆マーク  
をクリック



③Usersにチェックを入れる(自動的にHostsもチェックされる)

④ルールの対象とするネット  
ワークを選択する

⑤OKをクリック

# 【参考情報】

## Firepower recommendation によるルールの最適化

The screenshot displays the Cisco Firepower Management Center (FMC) interface for editing a policy named 'INTRUSION-POLICY'. The left sidebar shows the navigation menu with 'Firepower Recommendations' highlighted. A red arrow points from this menu item to the word 'クリック' (Click) written in red. The main content area shows the following details:

- Policy Information:** Name: INTRUSION-POLICY
- Description:** (Empty field)
- Drop when Inline:**
- Base Policy:** Balanced Security and Connectivity (Manage Base Policy)
- Status:** The base policy is up to date (Rule Update 2018-02-13-001-vrt)
- Enabled Rules:** This policy has 12776 enabled rules (Manage Rules)
- Event Summary:** 29 rules generate events, 12747 rules drop and generate events
- Message:** No recommendations have been generated. [Click here to set up Firepower recommendations.](#)
- Buttons:** Commit Changes, Discard Changes

At the bottom of the interface, it shows the last login information: Last login on Wednesday, 2018-02-07 at 14:37:51 PM from dhcp-10-141-41-25.disco.com and the Cisco logo.

# 【参考情報】

## Firepower recommendation によるルールの最適化

The screenshot displays the Cisco Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' section is active, showing 'Access Control > Intrusion'. The main content area is titled 'Edit Policy: INTRUSION-POLICY' and features a 'Firepower Recommended Rules Configuration' section. This section contains a message 'No recommendations have been generated.' and two checkboxes: 'Include all differences between recommendations and rule states in policy reports' (unchecked) and 'Advanced Settings' (checked). A red box highlights the 'Generate and Use Recommendations' button, with a red arrow pointing to it and the Japanese text 'クリック' (Click) next to it. Below this button is another button labeled 'Generate Recommendations'. The footer of the interface shows the login information: 'Last login on Wednesday, 2018-02-07 at 14:37:51 PM from dhcp-10-141-41-25.disco.com' and the Cisco logo.

# 【参考情報】

## Firepower recommendation によるルール最適化

The screenshot displays the Cisco Firepower Management Center interface. The main content area is titled "Firepower Recommended Rules Configuration" and shows a summary of recommendations for 1 host: 33012 rule state settings. It lists three specific recommendations: "Set 0 rules to generate events", "Set 233 rules to drop and generate events", and "Set 32779 rules to disabled". A "Success" dialog box is overlaid on the screen, containing the text: "Recommended rule state changes have been generated. Use the view links above to review the recommendations. Click the 'Use Recommendations' button to update your policy with the recommended changes." The "OK" button in the dialog box is highlighted with a red rectangle, and a red arrow points to it with the Japanese text "クリック" (Click).

# 【参考情報】

## Firepower recommendation によるルールの最適化

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' section is active, showing 'Access Control > Intrusion'. The main content area is titled 'Edit Policy: INTRUSION-POLICY' and displays 'Firepower Recommended Rules Configuration'. The configuration summary shows:

- Firepower recommends 33012 rule state settings for 1 hosts
- Set 0 rules to generate events (View)
- Set 233 rules to drop and generate events (View)
- Set 32779 rules to disabled (View)

Below the summary, it states: 'Policy is not using the recommendations. Click to change recommendations. Last generated: 2018 Feb 14 20:32:14'. There are two checkboxes: 'Include all differences between recommendations and rule states in policy reports' (unchecked) and 'Advanced Settings' (checked). A red box highlights the 'Use Recommendations' button, with a red arrow pointing to it and the text 'クリック' (Click) next to it. Below the button is an 'Update Recommendations' button.

At the bottom of the interface, it shows: 'Last login on Wednesday, 2018-02-07 at 14:37:51 PM from dhcp-10-141-41-25.cisco.com' and the Cisco logo.

# 【参考情報】

## Firepower recommendation によるルール最適化

The screenshot displays the Cisco Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The main content area is titled 'Edit Policy: INTRUSION-POLICY'. A 'Firepower Recommended Rules Configuration' section shows a summary of changes: 'Firepower changed 33012 rule states for 1 hosts'. Below this, there are three items: 'Set 0 rules to generate events', 'Set 233 rules to drop and generate events', and 'Set 32779 rules to disabled'. A 'Success' dialog box is overlaid on the screen, containing the text 'Policy is now using the generated recommendations' and an 'OK' button. A red arrow points to the 'OK' button with the Japanese text 'クリック' (Click).

# 【参考情報】

## Firepower recommendation によるルール最適化

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

Access Control > Intrusion Network Discovery Application Detectors Correlation Actions

### Edit Policy: INTRUSION-POLICY

Policy Information

Rules  
Firepower Recommendations  
Advanced Settings

Policy Layers  
My Changes  
Rules  
Firepower Recommendations  
Rules  
Balanced Security and Connectivity  
Rules  
Global Rule Thresholding

**Policy Information** < Back

Name: INTRUSION-POLICY  
Description:  
Drop when Inline:

**Base Policy** (Balanced Security and Connectivity) Manage Base Policy  
The base policy is up to date (Rule Update 2018-02-13-001-vrt)

**This policy has 7837 enabled rules** Manage Rules  
→ 0 rules generate events  
✗ 7837 rules drop and generate events

**Firepower changed 33012 rule states for 1 hosts** View Recommended Changes  
→ Set 0 rules to generate events  
✗ Set 233 rules to drop and generate events  
→ Set 32779 rules to disabled

Policy is using the recommendations. Click to change recommendations  
Last generated: 2018 Feb 14 20:32:14

**Commit Changes** クリック

Last login on Wednesday, 2018-02-07 at 14:37:51 PM from dhcp-10-141-41-25.cisco.com

CISCO

**This policy has 12776 enabled rules**  
→ 29 rules generate events  
✗ 12747 rules drop and generate events

Firepower recommendation  
適用前のルールサマリ

## 4. Malware & File Policy設定

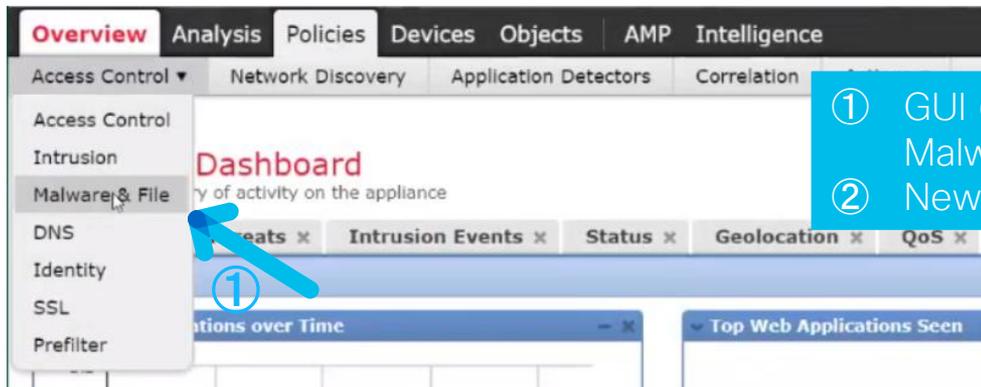
# File Policyの概要

- Malware & File Policyはどのようなトラフィックがファイル検査対象となるかを指定する
- 特定のトラフィックにMalware & File Policyを割り当てるにはAccess Control Policyルールを使う
- Malware & File Policyはファイル検査のルールを含んだもの
  - ルールを作成し、ポリシーに割り当てる流れとなる

# Malware & File Policy Rules

- 順序は動作に関係しない
  - 複数のファイルルールが使われることもある
- Malware & File Policyに複数のルールがある場合、ルールは以下の順で優先付けされる
  - 単純なファイルのブロックの方が、マルウェアインスペクション/ブロッキングよりも優先される
  - マルウェアインスペクション / ブロッキングは、単純な検知 / ログイングよりも優先される
  - 例) ブロックをするルールとマルウェアインスペクションルールの二つのが同じファイルに対して有効な場合、このファイルはブロックされるだけとなりマルウェアインスペクションは行われない

# ステップ 1: File Policyの作成

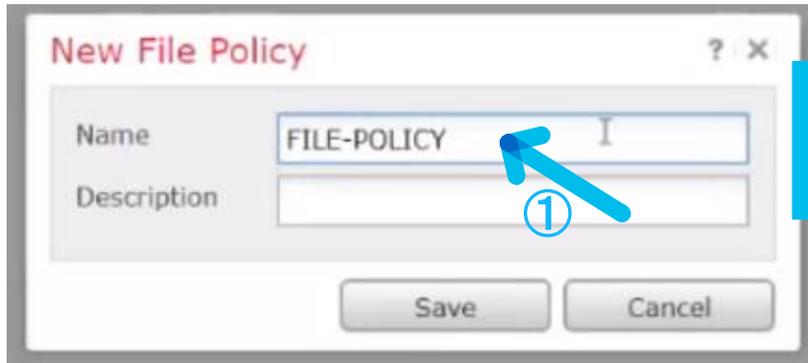


- ① GUI の上部にある Policies > Access Control > Malware & File を選択
- ② New File Policy をクリックし、新規 File Policy を作成する



# ステップ 1: File Policyの作成

新規File Policyに名前と説明を記述するフォームが表示される



New File Policy

Name: FILE-POLICY

Description:

Save Cancel

- ① 作成する File Policy に FILE-POLICY と入力し Save をクリック
- ② Add Rule をクリック

FILE-POLICYというポリシーが作成される



Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control ▶ Malware & File Network Discovery Application Detectors Correlation Actions ▼

**FILE-POLICY** Save Cancel

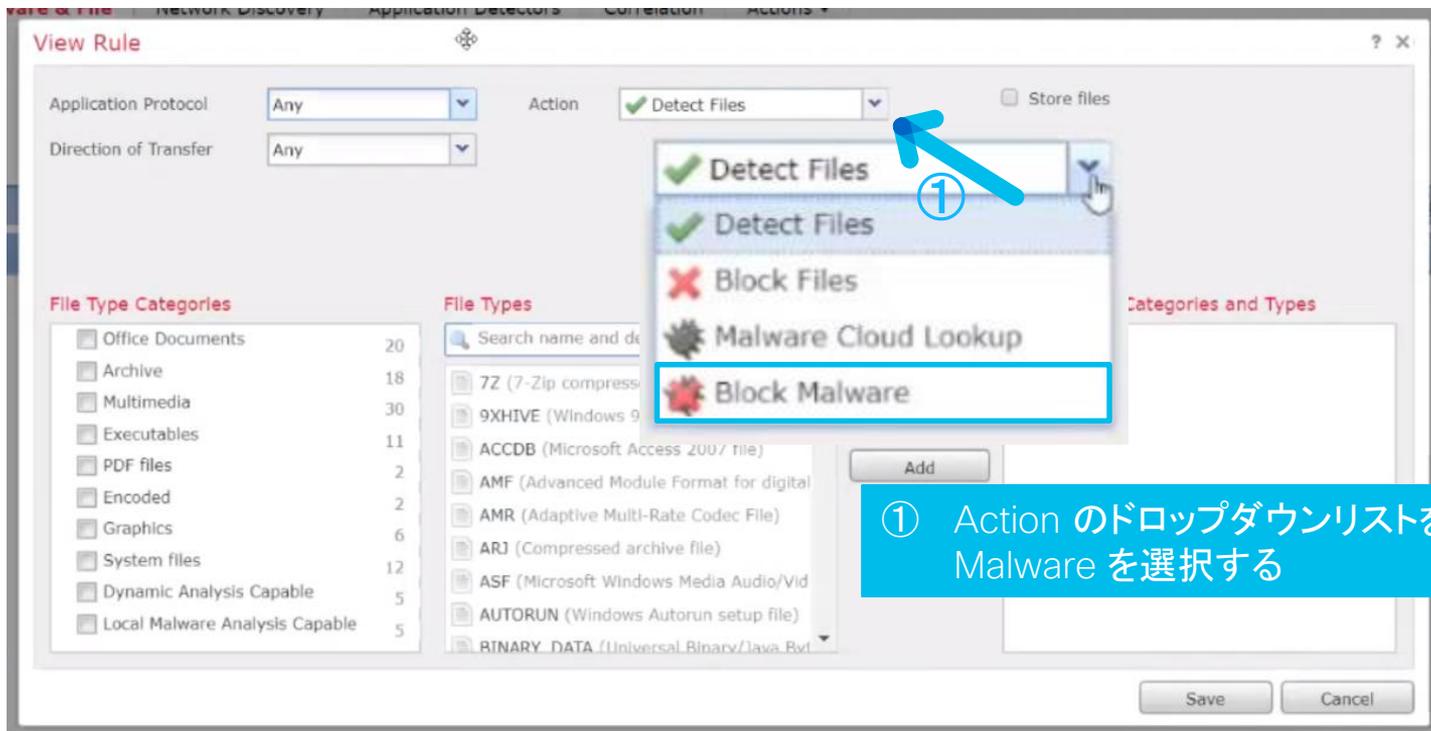
Enter Description

Rules Advanced

No access control policies use this Malware & File policy Add Rule

File Types	Application Protocol	Direction	Action
------------	----------------------	-----------	--------

## ステップ 2: File Ruleの作成



## ステップ 2: File Ruleの作成

View Rule

Application Protocol: Any

Direction of Transfer: Any

Action: Block Malware

Store Files:

- Malware
- Unknown
- Clean
- Custom

File Type Categories:

- Office Documents 16
- Archive 17
- Multimedia

File Types:

- 7Z (7-Zip compressed file)
- CPIO\_NEWC (Archive created with the cp...
- CPIO\_ODC (Archive created with the cpic...

① Spero Analysis for MSEXE と Local Malware Analysis にチェックを入れる (Spero, Dynamic, Local Malware Analysisについては後述)

- Reset Connection

① Spero Analysis for MSEXE と Local Malware Analysis にチェックを入れる (Spero, Dynamic, Local Malware Analysisについては後述)

① Spero Analysis for MSEXE と Local Malware Analysis にチェックを入れる (Spero, Dynamic, Local Malware Analysisについては後述)

① Spero Analysis for MSEXE と Local Malware Analysis にチェックを入れる (Spero, Dynamic, Local Malware Analysisについては後述)

- Reset Connectionにチェックを入れておくと、コネクションのタイムアウトを待たずにそのセッションを終了することができる
- 今回はチェックが入ったままにする

# ステップ 2: File Ruleの作成

① File Type Categories のすべてにチェックを入れる  
② File TypesでAll types in selected Categoriesを選択した状態で Add ボタンをクリック

- 様々なファイルタイプを検知できる
- 今回はすべてを対象にする

**File Type Categories**

<input checked="" type="checkbox"/>	Office Documents	16
<input checked="" type="checkbox"/>	Archive	17
<input checked="" type="checkbox"/>	Multimedia	2
<input checked="" type="checkbox"/>	Executables	7
<input checked="" type="checkbox"/>	PDF files	1
<input checked="" type="checkbox"/>	Encoded	0
<input checked="" type="checkbox"/>	Graphics	0
<input checked="" type="checkbox"/>	System files	2
<input checked="" type="checkbox"/>	Dynamic Analysis Capable	5
<input checked="" type="checkbox"/>	Local Malware Analysis Capable	5

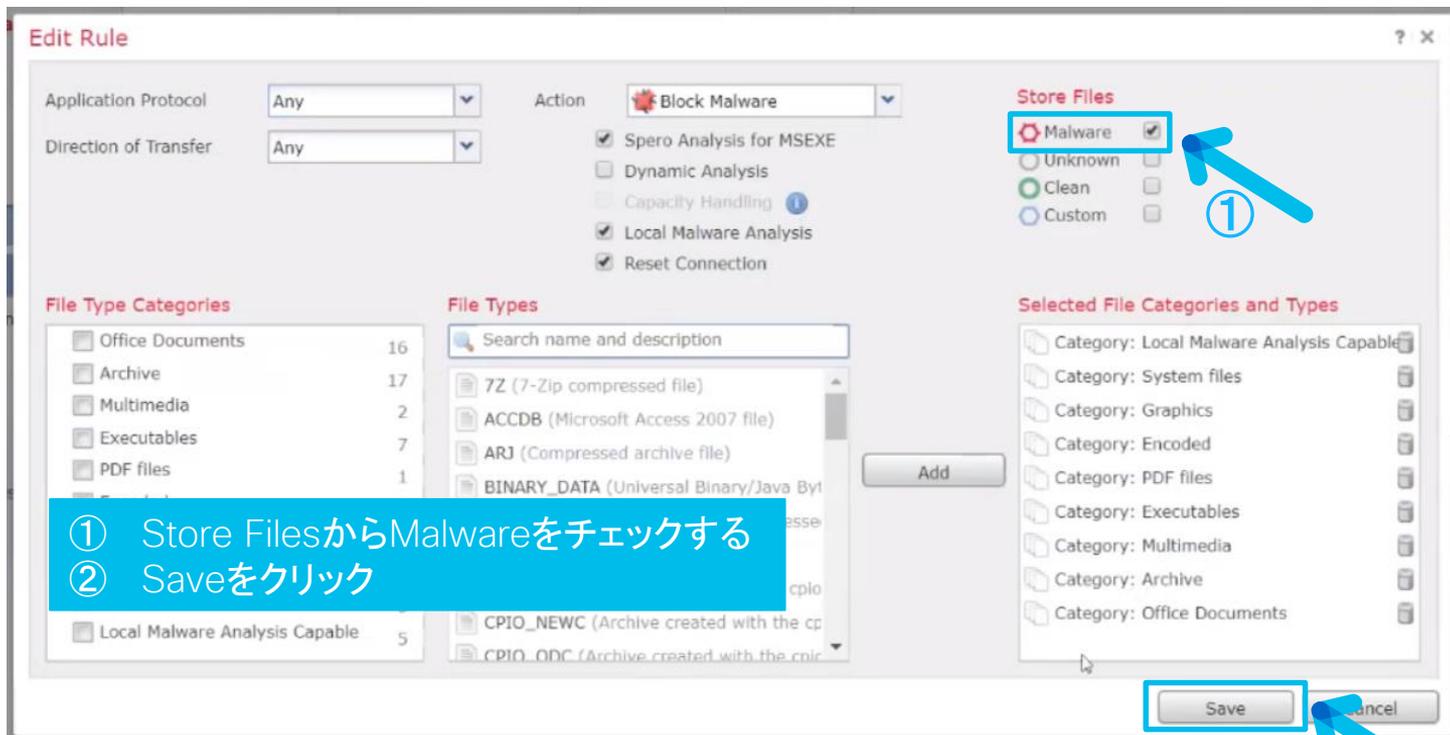
**File Types**

- Search name and description
- All types in selected Categories
- 7Z (7-Zip compressed file)
- ACCDB (Microsoft Access 2007 file)
- ARJ (Compressed archive file)
- BINARY\_DATA (Universal Binary/Java Bytecode)
- BINHEx (Macintosh BinHex 4 Compressed archive file)
- BZ (bzip2 compressed archive)
- CPIO\_CRC (Archive created with the cpio utility)
- CPIO\_NEWC (Archive created with the cpio utility)

**Selected File Categories and Types**

Buttons: Add, Save, Cancel

## ステップ 2: File Ruleの作成



- 先のスライドで選択したファイルカテゴリ・タイプが追加される

# ステップ 3: File Rule(二つ目)の作成

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

Access Control ▶ Malware & File Network Discovery Application Detectors Correlation Actions

**FILE-POLICY** You have unsaved changes Save Cancel

Enter Description

Rules Advanced

No access control policies use this Malware & File policy **Add Rule**

File Types	Application Protocol	Direction	Action
<ul style="list-style-type: none"><li>Category: Local Malware Analysis Capable</li><li>Category: Dynamic Analysis Capable</li><li>Category: System files</li><li>Category: Graphics</li><li>(6 more...)</li></ul>	Any	Any	<ul style="list-style-type: none"><li>Block Malware with Reset</li><li>Spero Analysis</li><li>Local Malware Analysis</li></ul>

① Add Ruleをクリック

# ステップ 3: File Rule(二つ目)の作成

Application Protocol: Any

Direction of Transfer: Any

Action: Block Malware

Store Files: Malware

File Type Categories:

- Office Documents: 16
- Archive: 17
- Multimedia: 2
- Executables: 7
- PDF files: 1
- Encoded: 0
- Graphics: 0
- System files: 2
- Dynamic Analysis Capable: 5
- Local Malware Analysis Capable: 5

File Types:

- All types in selected Categories
- MSEXE (Windows/DOS executable file)
- MSOLE2 (Microsoft Office applications OLE C)
- NEW\_OFFICE (Microsoft Office Open XML Fo)
- PDF (PDF file)
- RTF (Rich text format word processing file)

Selected File Categories and Types:

Category: Dynamic Analysis Capable

Add

Save Cancel

① ActionでBlock Malwareを選択

② チェックボックスをすべて選択 ※1

③ Malwareを選択

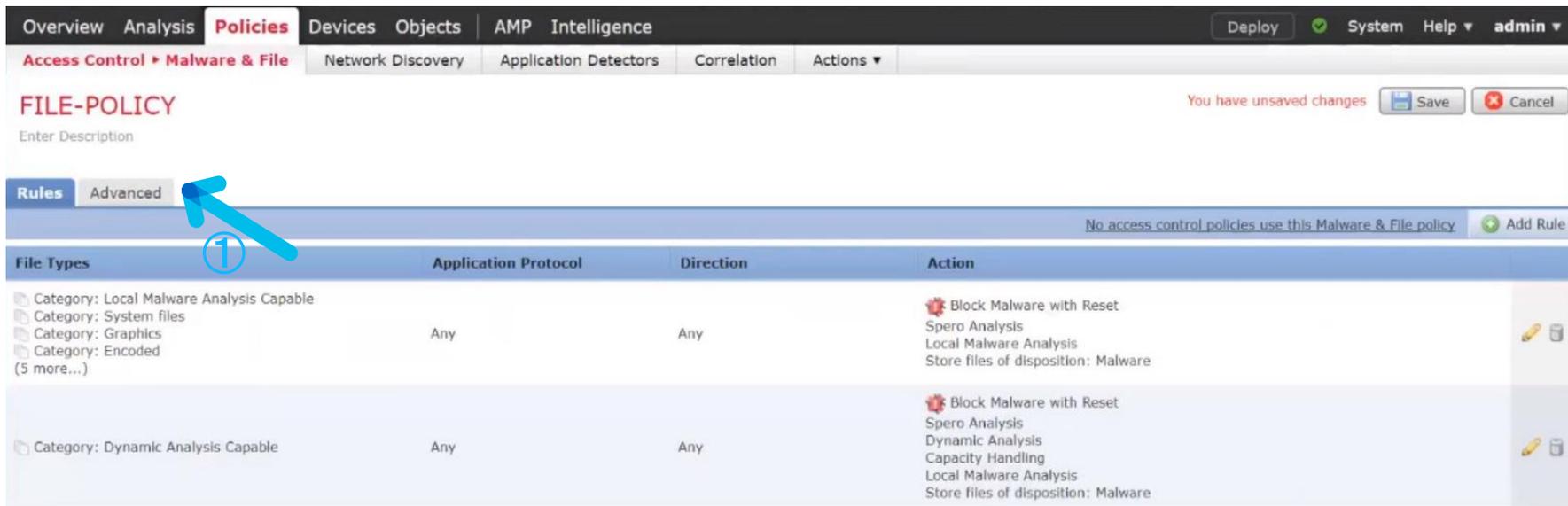
④ Dynamic Analysis Capableを選択

⑤ Addをクリック

⑥ Saveをクリック

※1 Capacity HandlingはDynamic Analysisのためのクラウドへのファイル送信が失敗した際にファイルを一時的に保存することを可能にする。

# ステップ 4: Advancedタブの確認とFile Policy保存



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

Access Control ▶ Malware & File Network Discovery Application Detectors Correlation Actions

## FILE-POLICY

Enter Description You have unsaved changes Save Cancel

Rules **Advanced** No access control policies use this Malware & File policy Add Rule

File Types	Application Protocol	Direction	Action
<ul style="list-style-type: none"><li>Category: Local Malware Analysis Capable</li><li>Category: System files</li><li>Category: Graphics</li><li>Category: Encoded</li><li>(5 more...)</li></ul>	Any	Any	<ul style="list-style-type: none"><li>Block Malware with Reset</li><li>Spero Analysis</li><li>Local Malware Analysis</li><li>Store files of disposition: Malware</li></ul>
<ul style="list-style-type: none"><li>Category: Dynamic Analysis Capable</li></ul>	Any	Any	<ul style="list-style-type: none"><li>Block Malware with Reset</li><li>Spero Analysis</li><li>Dynamic Analysis</li><li>Capacity Handling</li><li>Local Malware Analysis</li><li>Store files of disposition: Malware</li></ul>

① 今回は設定しないが、Advancedをクリックして確認

# ステップ 4: Advancedタブの確認とFile Policy保存

The screenshot displays the Cisco AMP console interface for configuring a File Policy. The main navigation bar includes Overview, Analysis, Policies (active), Devices, Objects, AMP, and Intelligence. The sub-navigation bar shows Access Control > Malware & File, with options for Network Discovery, Application Detectors, Correlation, and Actions. The page title is FILE-POLICY, and a notification indicates 'You have unsaved changes' with Save and Cancel buttons.

The configuration is shown in the 'Advanced' tab. The 'General' section includes:

- First Time File Analysis:
- Enable Custom Detection List:
- Enable Clean List:
- Mark files as malware based on dynamic analysis threat score:  (Dropdown menu set to 'Very High')

The 'Archive File Inspection' section includes:

- Inspect Archives:
- Block Encrypted Archives:
- Block Uninspectable Archives:
- Max Archive Depth:

Annotations with green arrows point to specific settings:

- システムが初めて検知したファイルをファイル分析にかける。無効にした場合、初めて検知したファイルのディスポジションはUnknownとなる。 (Points to 'First Time File Analysis')
- Custom Detection Listにあるファイルをブロックする (Points to 'Enable Custom Detection List')
- Clean Listにあるファイルを許可する (Points to 'Enable Clean List')
- Malwareと判定する動的分析脅威スコアの閾値 (Points to 'Mark files as malware based on dynamic analysis threat score')
- アーカイブを検査 (Points to 'Inspect Archives')
- 暗号化されたアーカイブをブロック (Points to 'Block Encrypted Archives')
- (ファイルの破損や階層の深さ等のために) 検査できないアーカイブをブロック (Points to 'Block Uninspectable Archives')
- 階層化されたアーカイブの検査 (Points to 'Max Archive Depth')

The bottom of the screen shows a table with the following columns: Malware & File Policy, Last Modified, and a status icon. The table contains one entry: FILE-POLICY, Last Modified: 2018-01-11 13:43:49, Modified by "admin".

# ステップ 4: Advancedタブの確認とFile Policy保存

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

Access Control ▶ Malware & File Network Discovery Application Detectors Correlation Actions

**FILE-POLICY** You have unsaved changes Save Cancel

Enter Description

Rules **Advanced**

**General**

- First Time File Analysis
- Enable Custom Detection List
- Enable Clean List
- Mark files as malware based on dynamic analysis threat score.

**Archive File Inspection**

- Inspect Archives
- Block Encrypted Archives
- Block Uninspectable Archives
- Max Archive Depth  Enter a value between 1 and 3

① 設定を確認したらSaveをクリック

以上で、Malware & File Policyが完成

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

Access Control ▶ Malware & File Network Discovery Application Detectors Correlation Actions

Access Control

Compare Policies New File Policy

Malware & File Policy	Last Modified
FILE-POLICY	2018-01-11 13:43:49 Modified by "admin"

# ステップ 5: AMP Cloudの設定



①

- ① AMP > タブをクリックしAMP Managementを開く
- ② 鉛筆マークをクリック
- ③ APJC Cloudに変更してSaveをクリック

Add AMP Cloud Connection

Cloud Name	Cisco AMP Solution Type	State	Actions
US Cloud	AMP for Networks		

②

Configure NetworkAMP Connection

Cloud Name:

③

Cloud Name	Cisco AMP Solution Type	State	Actions
APJC Cloud	AMP for Networks		

# ステップ 5: AMP Threat Gridの設定 (確認)



The screenshot shows the Cisco AMP Threat Grid interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'AMP' tab is active, and the 'Dynamic Analysis Connections' sub-tab is selected. A blue arrow points to the 'Host' column header in the table below, which is marked with a circled '1'. The table has columns for 'Cloud Name', 'Host', 'Purpose', and 'Actions'. One connection is listed with 'Cisco Sandbox API, US Cloud' as the cloud name, 'panacea.threatgrid.com' as the host, and 'File Submissions, Public Report Lookups' as the purpose.

Cloud Name	Host	Purpose	Actions
Cisco Sandbox API, US Cloud	panacea.threatgrid.com	File Submissions, Public Report Lookups	 

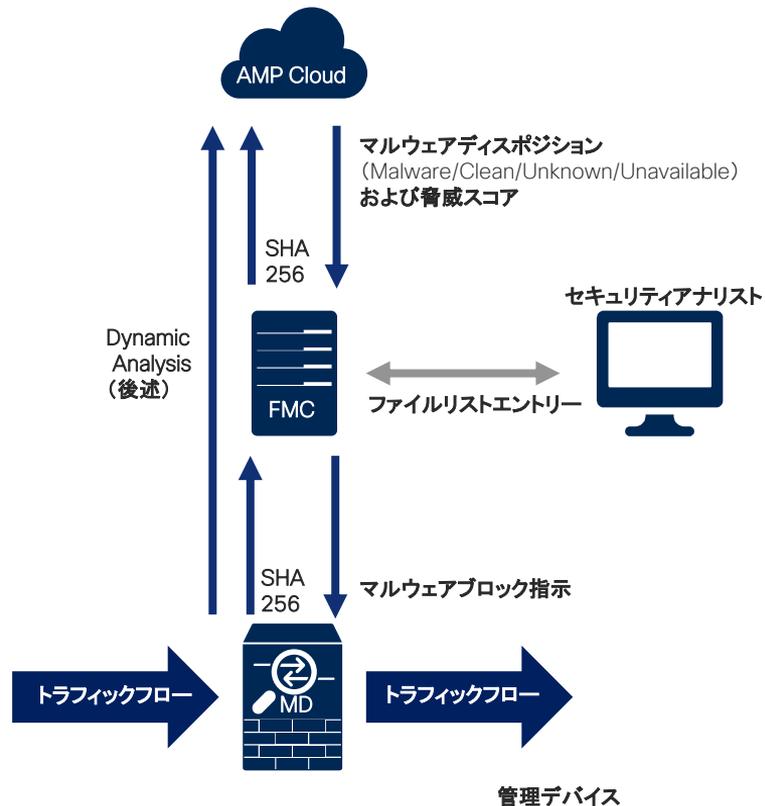
① AMP>Dynamic Analysis Connectionsをクリックし、設定画面を確認

# AMP for Firepower アーキテクチャ

InlineでデプロイされたFirepowerはマルウェアを検知・ストア・トラック・分析・ブロックできる。PDFやMicrosoft Officeドキュメント等を含む多様なファイルタイプをブロック可能。

1. ファイル・アーカイブを展開、ファイルハッシュ(SHA-256)は管理デバイス側で計算される
2. 管理デバイスがローカルのキャッシュを参照しディスポジションを確認する
3. キャッシュにマルウェアディスポジションが存在しない場合、そのハッシュ値がFMCに送られ、今度はFMCのキャッシュが確認される
4. FMCのキャッシュにもディスポジションがない場合そのハッシュ値をAMP Cloudでルックアップする
5. AMP Cloudからディスポジションが返り、FMC、管理デバイスのキャッシュにディスポジションが登録される
6. ディスポジションがUnknownだった場合、オプションで更なる解析を行う(後述)

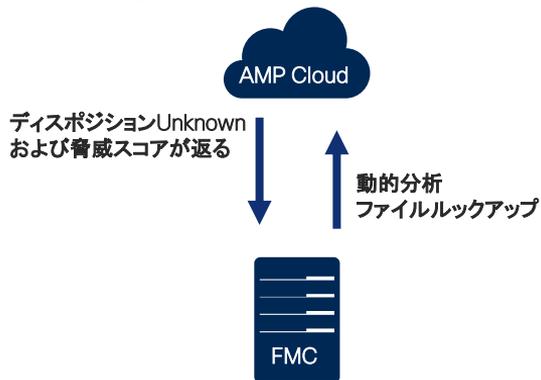
101010  
100101  
001001



# AMP for Firepower アーキテクチャ (続き)

- ・ 過去に検知されていないファイルのディスポジションは Unknown
- ・ マルウェアディスポジションをどう確定させるか(更なる分析を行うか等) 設定することができる
- ・ 複数の解析手法を併用可能

(その場合リソース消費は増える)



File Detection and Storage (Store)  
検知したファイルをローカルに保存

分析の  
順序

Spero Analysis  
対応ファイルのファイル構造をFirepowerが分析しファイルメタデータをAMP Cloudに送信(ファイル自体は送信しない)

ローカルマルウェア分析(Local Malware Analysis)  
AMP CloudからダウンロードしたClamAVシグネチャおよびファイルプリクラシフィケーションルールを利用しFirepowerのローカルエンジンを使った分析を実行。分析の結果をAMP Cloudに送る。

動的分析(Dynamic Analysis)  
AMP Threat Gridにファイルを送りサンドボックス解析を行い脅威スコアをつける。ファイルの送信は手動(ストアが必要)・自動の選択が可能。

# 参考: マルウェアのクラウドリコール

- 調査したファイルを記録しておくことで、合致するマルウェアが発見された際、瞬時にそのファイルの脅威情報を自動で変更する



## 5. Access Control Policy 設定

# 作成する Access Control Policy について

- Security Intelligence によって配信されるネットワークおよび URL の Blacklist はブロックする
- Access Control Policy では、第 3 - 4 章で作成した Intrusion Policy と File Policy を使用してセキュリティチェックを行う
- 通信の始まりと終わりのログを取得する
- Web トラフィックは URL カテゴリーを記録する

# ステップ 1: Security Intelligence の設定

- Security Intelligence とは？
  - 一般的に言うレピュテーションのこと (通信相手がマルウェアを配信したりする悪意のあるソースという「評判」がないかどうかを分析・評価した情報)
  - Cisco Talos が随時、収集・分析したネットワークや URL のレピュテーションを提供し、ユーザは必要に応じて使用できる
  - Security Intelligence を使用する場合、FTD による更新頻度はデフォルトで 2 時間 \* 変更方法は後述のページを参照

## 世界最大規模の脅威検出ネットワーク

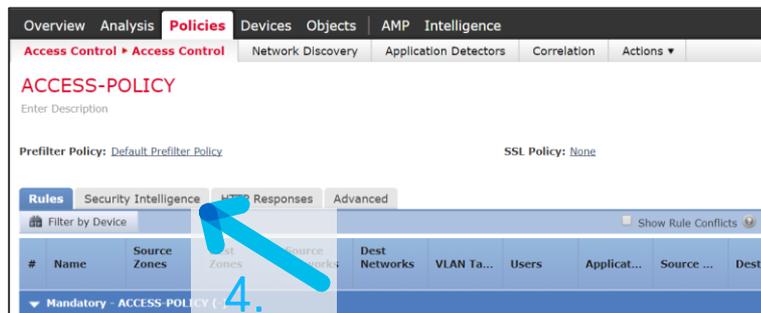
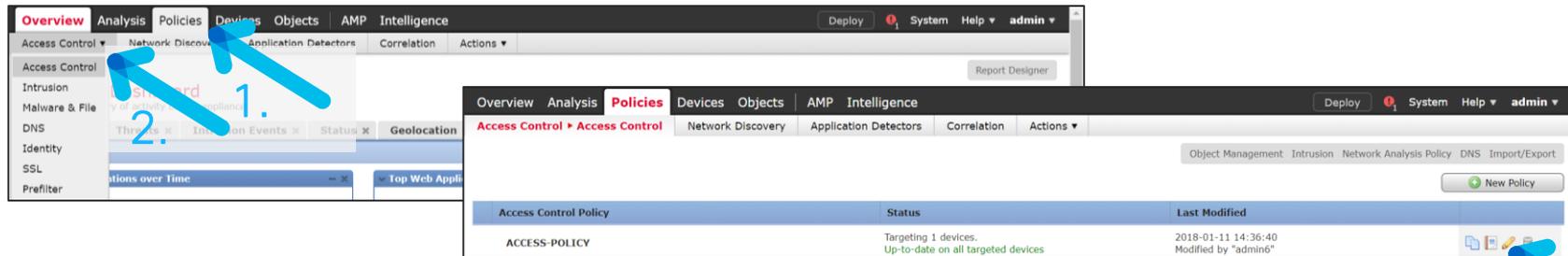
Cisco Security Intelligence Operations (SIO) は、全世界のセキュリティ情報を収集し、脅威や脆弱性に関する情報や分析を提供しています。

[SIO にアクセス](#)



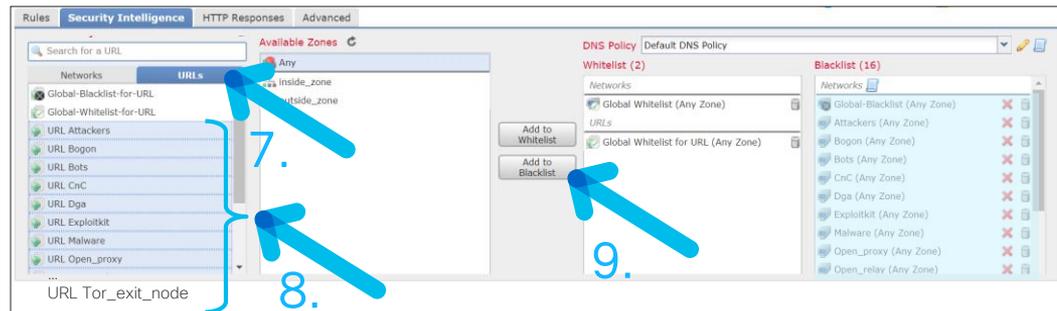
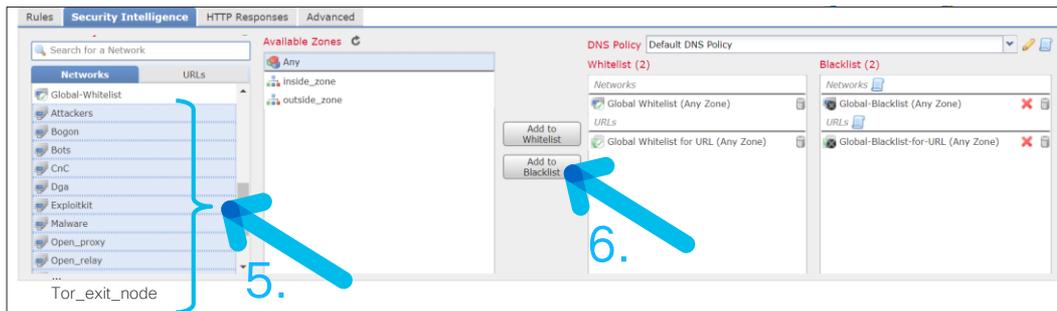
# ステップ 1-1: Security Intelligence の設定

- Security Intelligenceにヒットした通信をブロックする設定を行う



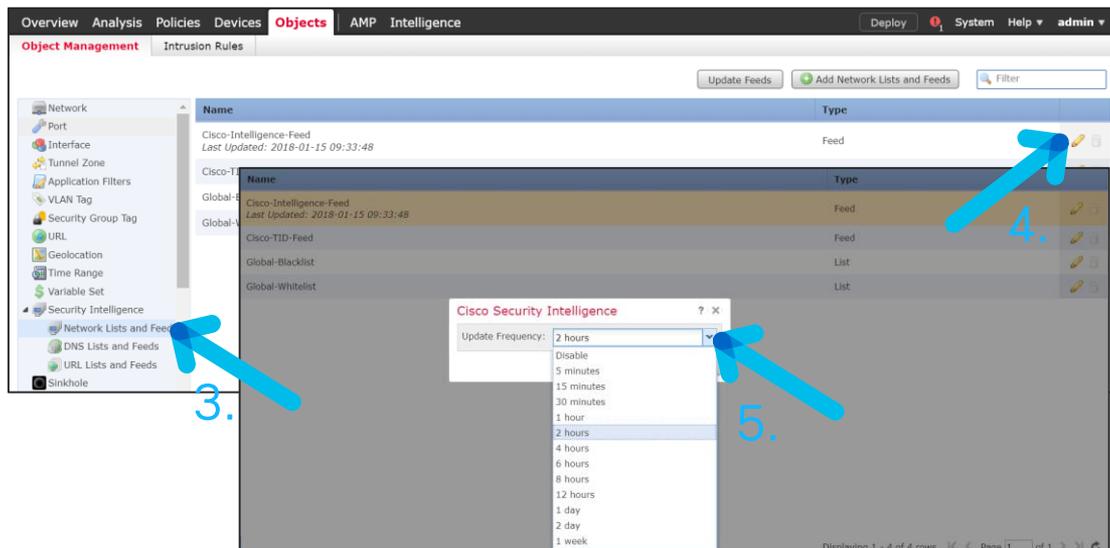
- GUI の上部にある Policies を選択
- Access Control のドロップダウンリストを開き、Access Control を選択
- 第1章で作成済みの ACCESS-POLICY の鉛筆マーク (  ) を選択
- Security Intelligence を選択  
引き続き、次のスライドを参照

# ステップ 1-2: Security Intelligence の設定



5. Networks 配下にある Global-Whitelist 以降 (Attackers - Tor\_exit\_node) を全選択
6. Add to Blacklist を選択
7. URLs を選択
8. Global-Whitelist-for-URL 以降 (URL Attackers - URL Tor\_exit\_node) を全選択
9. Add to Blacklist を選択

# 参考: Security Intelligence の更新頻度の変更



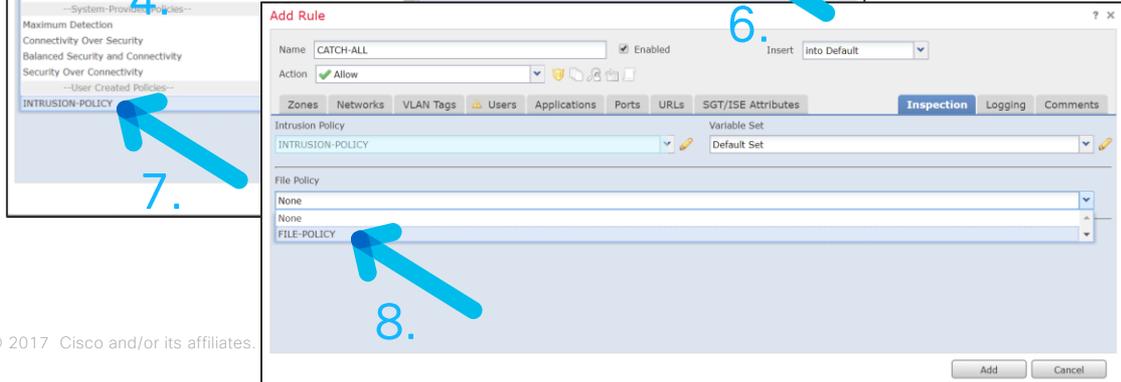
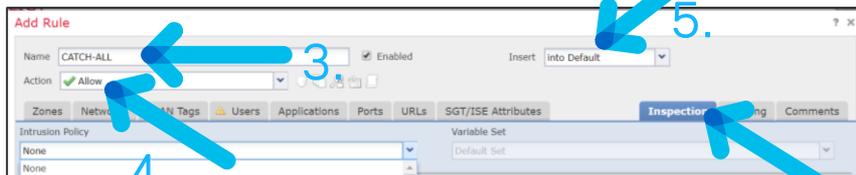
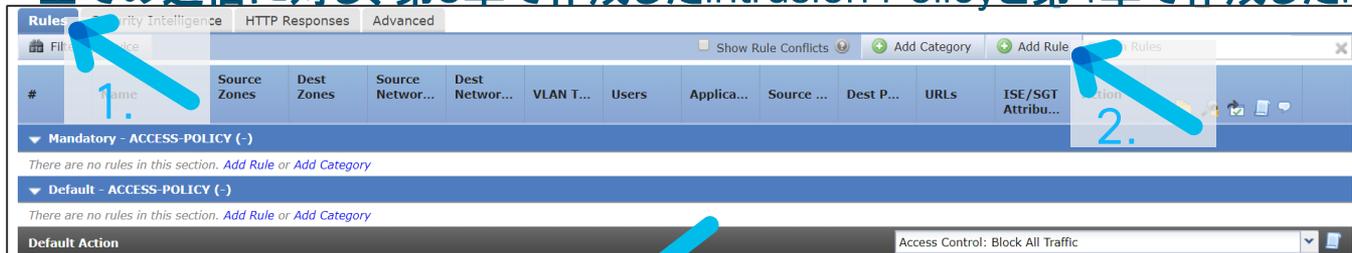
1. GUI の上部にある Objects を選択
2. Object Management を選択
3. Security Intelligence 配下の Network Lists and Feeds を選択
4. Cisco-Intelligence-Feed の鉛筆マーク(  ) を選択
5. Update Frequency のドロップダウンリストを開き、希望の更新頻度を選択

\*デフォルト 2 時間

\*\*URL List の更新頻度は DNS Lists and Feeds から変更可

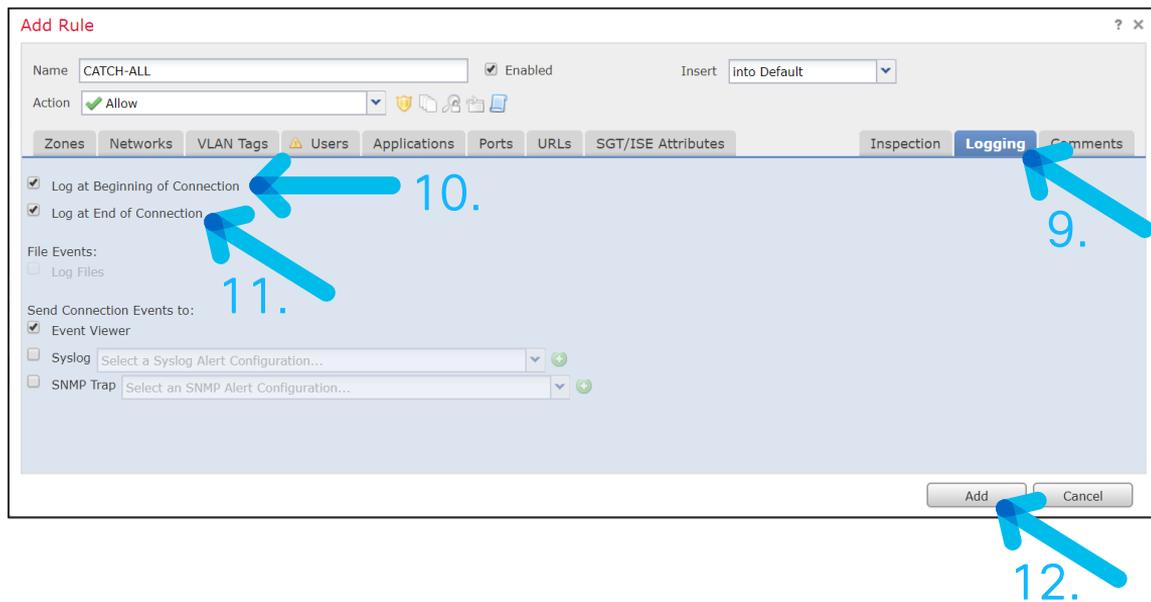
# ステップ 2-1: Access Rule の設定

- 全ての通信に対し、第3章で作成したIntrusion Policyと第4章で作成したFile Policyを適用



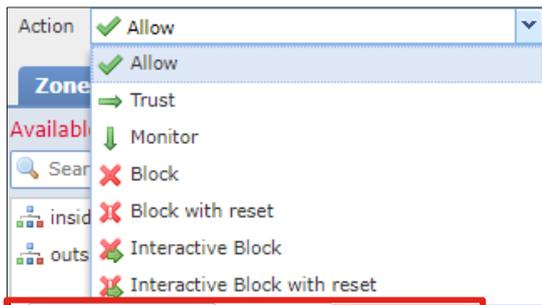
- Rules タブを選択
  - Add Rule を選択
  - 任意の名前を選択
  - Action のドロップダウンリストを開き、Allow を選択
  - Insert: into Default を選択
  - Inspection タブを選択
  - 第 3 章で作成した INTRUSION-POLICY を選択
  - 第 4 章で作成した FILE-POLICY を選択
- 引き続き、次のスライドを参照

## ステップ 2-2: Access Rule の設定



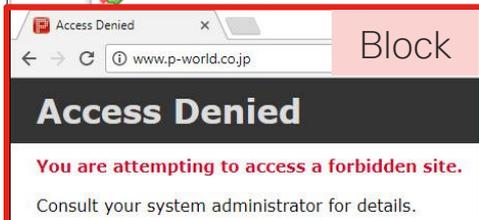
9. Logging タブを選択
10. Log at Beginning of Connection を選択
11. Log at End of Connection を選択
12. Add を選択

# 参考: Action のオプションについて



- FTD で使用できる Action は全 7 種

- Allow: パケットを信頼せずに許可し、追加でIPSやAMPのチェックを実施することが可能
- Trust: パケットを信頼して許可。IPSやAMPのチェックは不可
- Monitor: ログを取るためだけに使用。トラフィックは次のルールに転送
- Block: パケットを破棄
- Block w/ reset: パケットを破棄すると同時に、送信元に対し、TCP RSTパケットを送信し、通信を即遮断
- Interactive Block: ブロックが推奨されるユーザアクションに対し警告を行うが、ユーザの判断で通信し続けることも可能
- Interactive Block w/ reset: 上記と同様。ただし、警告通りに通信をブロックする場合、送信元に対して TCP RST パケットを送信



# 参考: Block 時のHTTP Response ページの編集 (1)

The screenshot shows the Cisco Firepower configuration interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', and 'Intelligence'. The 'Policies' tab is selected, and the 'Access Control' section is visible. The 'ACCESS-POLICY' configuration page is shown, with the 'HTTP Responses' tab selected. The 'Block Response Page' dropdown menu is open, showing options: 'Custom...', 'None', 'System-provided', 'Custom...', and 'System-provided'. The 'Custom...' option is highlighted. Blue arrows and numbers 1 through 4 indicate the steps: 1. Select 'Policies', 2. Select 'Access Control > Access Control', 3. Select the 'HTTP Responses' tab, and 4. Open the 'Block Response Page' dropdown and select 'Custom...'.

1. Policies を選択
2. Access Control > Access Control を選択
3. HTTP Responses タブを選択
4. Block Response Page のドロップダウンリストを開き、Custom を選択  
引き続き、次のスライドを参照

# 参考: Block 時の HTTP Response ページの編集 (2)

5. 任意の文章に変更 (HTML形式)

6. Save を選択

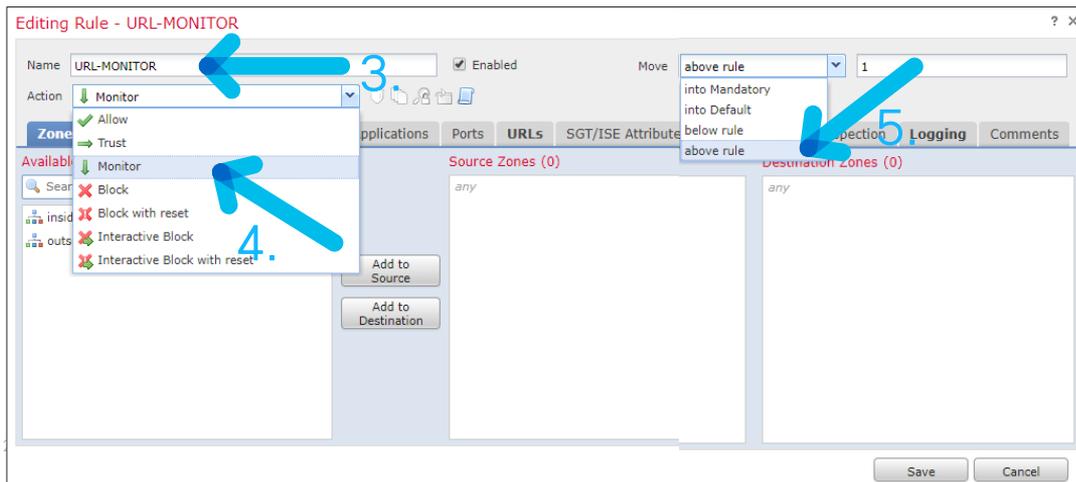
7. 仮想端末から Block されているサイトへアクセス

8. レスポンスが和文になっていることを確認

\*この例では、追加でギャンブルサイトへのアクセスをブロックするポリシーを追加している

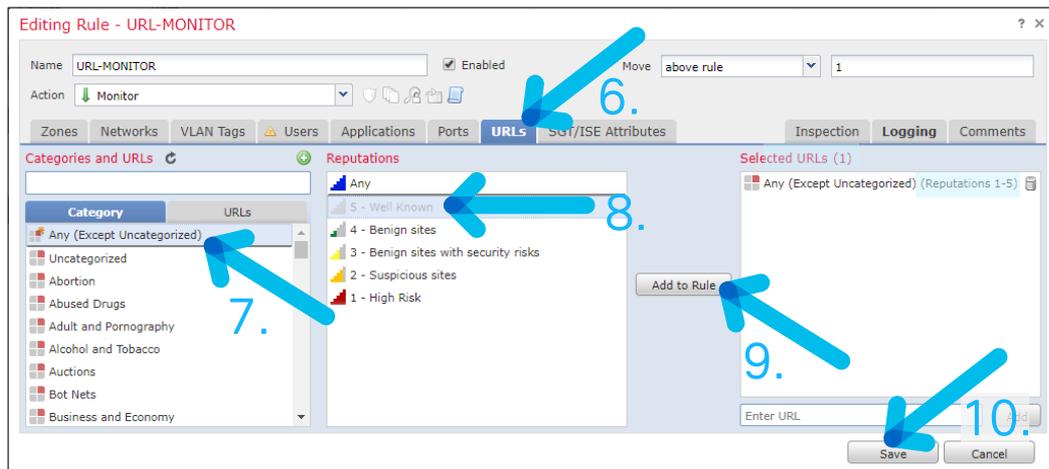
# ステップ 3-1: URL Category Monitor の設定

- 全ての通信に対し、URLカテゴリーのロギングを行うRuleを追加



- Rules タブを選択
- Add Rule を選択
- 任意の名前を選択
- Action のドロップダウンリストを開き、Monitor を選択
- Insert のドロップダウンリストを開き、above rule を選択  
引き続き、次のスライドを参照

# ステップ 3-2: URL Category Monitor の設定



6. URLs タブを選択
7. Any (Except Uncategorized) を選択
8. Reputations: 5 - Well Known を選択
9. Add to Rule を選択
10. Save を選択  
引き続き、次のスライドを参照

# ステップ 3-3: URL Category Monitor の設定

ACCESS-POLICY

Enter Description

Prefilter Policy: Default.Prefilter.Policy

SSL Policy: None

Rules Security Intelligence HTTP Responses Advanced

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Ta...	Users	Applicat...	Source ...	Dest Ports	URLs	ISE/SGT Attributes	Action
1	URL MONITOR	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any (Excl...		Trust
2	CATCH-ALL	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any		Allow

Default Action: Access Control: Block All Traffic

11.

12.

- 11. Save を選択
- 12. Deploy を選択
- 13. Deploy を選択

Deploy Policies Version: 2018-01-16 08:58 AM

Device	Group	Current Version
FTDy1		2018-01-11 02:36 PM

- Net Policy: NAT-POLICY
- NGFW Settings: FTD-POLICY
- Access Control Policy: ACCESS-POLICY
- Intrusion Policy: Balanced Security and Connectivity
- Intrusion Policy: No Rules Active
- DNS Policy: Default DNS Policy
- Intrusion Policy: INTRUSION-POLICY
- Prefilter Policy: Default Prefilter Policy
- Network Discovery
- Device Configuration (Details)

Selected devices: 1

Deploy Cancel

# ステップ 4: URL Filter の設定

- URL Filter機能そのものを有効にする

The screenshot shows the Cisco AMP for Networks configuration interface. The top navigation bar includes 'System', 'Help', and 'admin'. Below it, the 'Integration' tab is selected. The 'URL Filtering' section is expanded, showing the following settings:

- Last URL Filtering Update: 2018-01-16 07:27:17 (with an 'Update Now' button)
- Enable URL Filtering:
- Enable Automatic Updates:
- Query Cisco CSI for Unknown URLs:

The 'AMP for Networks' section is also visible, with the following settings:

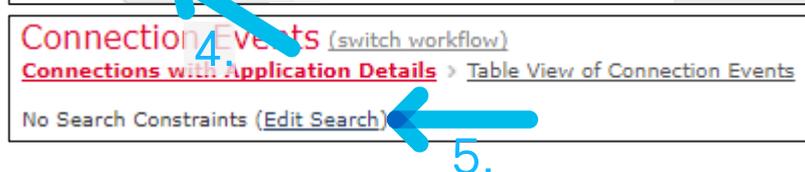
- Last Local Malware Detection Update: Thu Jan 11 11:35:28 2018
- Enable Automatic Local Malware Detection Updates:
- Share URI from Malware Events with Cisco:
- Use Legacy Port 32137 for AMP for Networks:

A 'Save' button is located at the bottom of the configuration panel. Blue arrows and numbers 1 through 4 indicate the steps for enabling the URL Filter functionality.

1. System タブを選択
2. Integration タブを選択
3. Query Cisco CSI for Unknown URLs にチェック
4. Update Now を選択

# ステップ 5-1: URL Filter のテスト

本テストでは、複数のギャンブルサイトにアクセスし、URL が正しくカテゴリ化されるかを確認する



1. 仮想端末でインターネットを開き、ギャンブルサイト (例 www.p-world.co.jp、www.jra.go.jpなど) にアクセス

2. Analysis タブを選択

3. Connections を選択

4. Events を選択

5. Edit Search を選択

引き続き、次のスライドを参照

# ステップ 5-2: URL Filter のテスト

up Search

(unnamed search) Private Save Save As New Search

Application Protocol HTTP

Application Protocol Category web browser, email

Application Protocol Tag share media, allows remote connect

Client Firefox, Internet Explorer

Client Version 6.0

Client Category web browser, email

Client Tag share media, allows remote connect

Web Application Facebook

Web Application Category web browser, email

Web Application Tag share media, allows remote connect

Application Risk Very High, Medium

Business Relevance Very Low, High

Referenced Host example.com

User Agent Mozilla/5.0, Firefox, Chrome

HTTP Referrer http://example.com/index.htm

URL

URL /index.htm

URL Category Gambling

URL Reputation Well known

6. URL: URL Category の欄に Gambling と入力
7. Search を選択
8. 1. の 2 サイトが正しくカテゴリー化されていることを確認

Connection Events [switch workflow]

Connections with Application Details > Table View of Connection Events

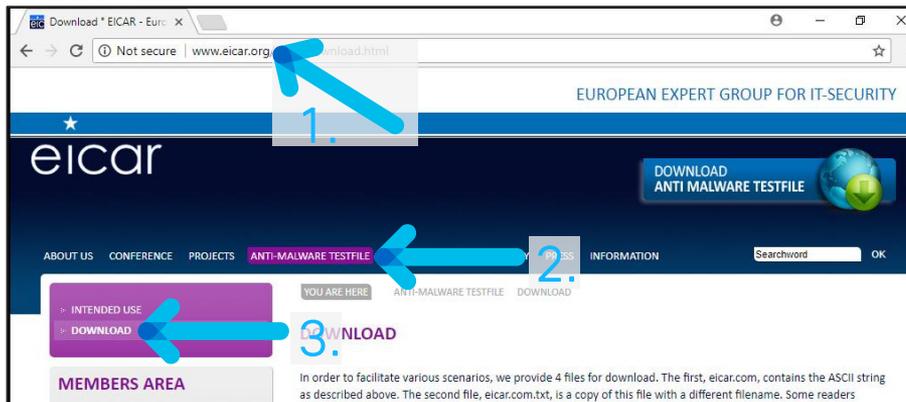
2018-01-16 09:46:23 - 2018-01-16 11:50:40 Expanding

Search Constraints (Edit Search Save Search)

Jump to...	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICHIP Type	Destination Port / ICHIP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device
	2018-01-16 11:22:54	2018-01-16 11:23:54	Trust		192.168.1.101	JP	210.149.135.12	JP	inside_zone	outside_zone	50086 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ira.co.jp/	Gambling	Well known	FTDv1
	2018-01-16 11:23:54	2018-01-16 11:23:54	Trust		192.168.1.101	JP	210.149.135.12	JP	inside_zone	outside_zone	50086 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.ira.co.jp/	Gambling	Well known	FTDv1
	2018-01-16 11:25:43	2018-01-16 11:25:43	Trust		192.168.1.101	JP	202.248.171.183	JP	inside_zone	outside_zone	50023 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.p-world.co.jp/	Gambling	Well known	FTDv1
	2018-01-16 11:25:43	2018-01-16 11:25:43	Trust		192.168.1.101	JP	202.248.171.183	JP	inside_zone	outside_zone	50027 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.p-world.co.jp/banner/index2.js	Gambling	Well known	FTDv1
	2018-01-16 11:25:43	2018-01-16 11:25:43	Trust		192.168.1.101	JP	210.254.90.162	JP	inside_zone	outside_zone	50031 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://co01.p-world.co.jp/mqcnt2/mqcnt2.cgi?file...	Gambling	Well known	FTDv1
	2018-01-16 11:25:43	2018-01-16 11:25:43	Trust		192.168.1.101	JP	202.248.171.183	JP	inside_zone	outside_zone	50022 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.p-world.co.jp/frame_banner/is/index.html	Gambling	Well known	FTDv1
	2018-01-16 11:25:43	2018-01-16 11:25:43	Trust		192.168.1.101	JP	202.248.171.183	JP	inside_zone	outside_zone	50025 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.p-world.co.jp/frame_banner/is/index_top...	Gambling	Well known	FTDv1
	2018-01-16 11:25:43	2018-01-16 11:25:43	Trust		192.168.1.101	JP	202.248.171.183	JP	inside_zone	outside_zone	50026 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.p-world.co.jp/frame_banner/is/index_left...	Gambling	Well known	FTDv1
	2018-01-16 11:25:43	2018-01-16 11:25:43	Trust		192.168.1.101	JP	202.248.171.183	JP	inside_zone	outside_zone	50034 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.p-world.co.jp/frame_banner/is/index_right...	Gambling	Well known	FTDv1
	2018-01-16 11:25:43	2018-01-16 11:25:43	Trust		192.168.1.101	JP	202.248.171.183	JP	inside_zone	outside_zone	50024 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://www.p-world.co.jp/banner/index.js	Gambling	Well known	FTDv1
	2018-01-16 11:25:43	2018-01-16 11:25:43	Trust		192.168.1.101	JP	210.254.90.162	JP	inside_zone	outside_zone	50030 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	http://co01.p-world.co.jp/mqcnt2/mqcnt2.cgi?file...	Gambling	Well known	FTDv1

# ステップ 6-1: AMP (File Policy) のテスト

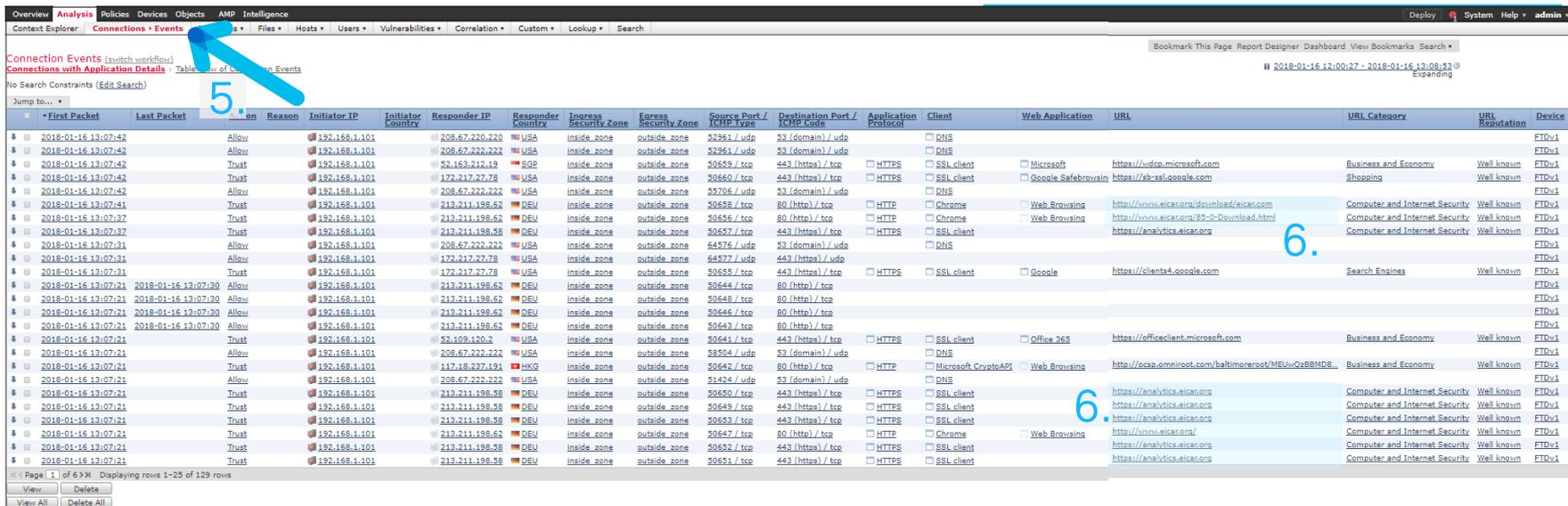
本テストでは、テスト用のマルウェアファイルを仮想端末にダウンロードし、AMP Policy がマルウェアを正しく検知できるかを確認する



テスト用マルウェアファイル

1. 仮想端末でインターネットを開き、[www.eicar.org](http://www.eicar.org) にアクセス
  2. ANTI-MALWARE TESTFILE タブを選択
  3. DOWNLOAD を選択
  4. テスト用のマルウェアをダウンロードするために、[eicar.com](http://eicar.com) を選択
- 引き続き、次のスライドを参照

# ステップ 6-2: AMP (File Policy) のテスト



Connection Events (switch workflow)  
Connections with Application Details | Table View of Connection Events  
No Search Constraints (Edit Search)

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device
2018-01-16 13:07:42		Allow		192.168.1.101		208.67.220.220	USA	inside_zone	outside_zone	52361 / udp	53 (domain) / udp		DNS					FTDv1
2018-01-16 13:07:42		Allow		192.168.1.101		208.67.222.222	USA	inside_zone	outside_zone	52361 / udp	53 (domain) / udp		DNS					FTDv1
2018-01-16 13:07:42		Trust		192.168.1.101		52.163.212.13	SGP	inside_zone	outside_zone	50659 / tcp	443 (https) / tcp	HTTPS	SSL client	Microsoft	https://wdcp.microsoft.com	Business and Economy	Well known	FTDv1
2018-01-16 13:07:42		Trust		192.168.1.101		172.217.27.78	USA	inside_zone	outside_zone	50650 / tcp	443 (https) / tcp	HTTPS	SSL client	Google Safebrowsin	https://gb-asl.google.com	Shopping	Well known	FTDv1
2018-01-16 13:07:42		Allow		192.168.1.101		208.67.222.222	USA	inside_zone	outside_zone	5306 / udp	53 (domain) / udp		DNS					FTDv1
2018-01-16 13:07:41		Trust		192.168.1.101		213.211.198.62	DEU	inside_zone	outside_zone	50568 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	https://www.eicar.org/download/eicar.com	Computer and Internet Security	Well known	FTDv1
2018-01-16 13:07:37		Trust		192.168.1.101		213.211.198.62	DEU	inside_zone	outside_zone	50555 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	https://www.eicar.org/95-D-Download.html	Computer and Internet Security	Well known	FTDv1
2018-01-16 13:07:37		Trust		192.168.1.101		213.211.198.58	DEU	inside_zone	outside_zone	50557 / tcp	443 (https) / tcp	HTTPS	SSL client	Web Browsing	https://analytics.eicar.org	Computer and Internet Security	Well known	FTDv1
2018-01-16 13:07:31		Allow		192.168.1.101		208.67.222.222	USA	inside_zone	outside_zone	64576 / udp	53 (domain) / udp		DNS					FTDv1
2018-01-16 13:07:31		Allow		192.168.1.101		172.217.27.78	USA	inside_zone	outside_zone	64577 / udp	443 (https) / udp		DNS					FTDv1
2018-01-16 13:07:31		Trust		192.168.1.101		172.217.27.78	USA	inside_zone	outside_zone	50555 / tcp	443 (https) / tcp	HTTPS	SSL client	Google	https://clients4.google.com	Search Engines	Well known	FTDv1
2018-01-16 13:07:21	2018-01-16 13:07:30	Allow		192.168.1.101		213.211.198.62	DEU	inside_zone	outside_zone	50644 / tcp	80 (http) / tcp		DNS					FTDv1
2018-01-16 13:07:21	2018-01-16 13:07:30	Allow		192.168.1.101		213.211.198.62	DEU	inside_zone	outside_zone	50648 / tcp	80 (http) / tcp		DNS					FTDv1
2018-01-16 13:07:21	2018-01-16 13:07:30	Allow		192.168.1.101		213.211.198.62	DEU	inside_zone	outside_zone	50646 / tcp	80 (http) / tcp		DNS					FTDv1
2018-01-16 13:07:21	2018-01-16 13:07:30	Allow		192.168.1.101		213.211.198.62	DEU	inside_zone	outside_zone	50643 / tcp	80 (http) / tcp		DNS					FTDv1
2018-01-16 13:07:21		Trust		192.168.1.101		52.109.120.2	USA	inside_zone	outside_zone	50641 / tcp	443 (https) / tcp	HTTPS	SSL client	Office 365	https://officeclient.microsoft.com	Business and Economy	Well known	FTDv1
2018-01-16 13:07:21		Allow		192.168.1.101		208.67.222.222	USA	inside_zone	outside_zone	58504 / tcp	53 (domain) / udp		DNS					FTDv1
2018-01-16 13:07:21		Trust		192.168.1.101		117.18.237.191	HKG	inside_zone	outside_zone	50642 / tcp	80 (http) / tcp	HTTP	Microsoft CryptoAPI	Web Browsing	http://ocsp.emnroot.com/baltimoreroot/MEUvQzBMD6...	Business and Economy	Well known	FTDv1
2018-01-16 13:07:21		Allow		192.168.1.101		208.67.222.222	USA	inside_zone	outside_zone	51424 / tcp	53 (domain) / udp		DNS					FTDv1
2018-01-16 13:07:21		Trust		192.168.1.101		213.211.198.58	DEU	inside_zone	outside_zone	50650 / tcp	443 (https) / tcp	HTTPS	SSL client		https://analytics.eicar.org	Computer and Internet Security	Well known	FTDv1
2018-01-16 13:07:21		Trust		192.168.1.101		213.211.198.58	DEU	inside_zone	outside_zone	50649 / tcp	443 (https) / tcp	HTTPS	SSL client		https://analytics.eicar.org	Computer and Internet Security	Well known	FTDv1
2018-01-16 13:07:21		Trust		192.168.1.101		213.211.198.58	DEU	inside_zone	outside_zone	50652 / tcp	443 (https) / tcp	HTTPS	SSL client		https://analytics.eicar.org	Computer and Internet Security	Well known	FTDv1
2018-01-16 13:07:21		Trust		192.168.1.101		213.211.198.62	DEU	inside_zone	outside_zone	50647 / tcp	80 (http) / tcp	HTTP	Chrome	Web Browsing	https://www.eicar.org/	Computer and Internet Security	Well known	FTDv1
2018-01-16 13:07:21		Trust		192.168.1.101		213.211.198.58	DEU	inside_zone	outside_zone	50652 / tcp	443 (https) / tcp	HTTPS	SSL client		https://analytics.eicar.org	Computer and Internet Security	Well known	FTDv1
2018-01-16 13:07:21		Trust		192.168.1.101		213.211.198.58	DEU	inside_zone	outside_zone	50651 / tcp	443 (https) / tcp	HTTPS	SSL client		https://analytics.eicar.org	Computer and Internet Security	Well known	FTDv1

5. Analytics > Connections > Events を選択
6. eicar.org のログを確認  
引き続き、次のスライドを参照

# ステップ 6-3: AMP (File Policy) のテスト

Overview **Analysis** AMP Intelligence

Context Explorer Connections **Intrusions** Files > Network File Trajectory Users Vulnerabilities Correlation Custom Lookup Search

Enter a SHA256 hash, IP address or file name

Recently Viewed Files

Time	File SHA256	File Names	File Type	Disposition	Events
No records to display					

Recent Malware

Time	File SHA256	File Names	File Type	Disposition	Events
2018-01-11 14:20:53	275a021b...f651f0f		EICAR	Malware	1

Overview **Analysis** Policies Devices Objects AMP Intelligence

Context Explorer Connections **Intrusions** Files > Network File Trajectory Hosts Users Vulnerabilities Correlation Custom Lookup Search

Network File Trajectory for 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

File SHA256: 275a021b...f651f0f

File Name: eicar.com

File Size (KB): 0.0564

File Type: EICAR

File Category: Executables

Current Disposition: Malware

Threat Score: None

Detection Name: EICAR

First Seen: 2018-01-11 14:20:52 on 213.211.198.62 by No Authentication Required

Last Seen: 2018-01-11 14:20:52 on 213.211.198.62 by No Authentication Required

Event Count: 1

Seen On: 1 hosts

Seen On Breakdown: 1 sender -> 0 receivers

Trajectory

Jan 11 14:20

213.211.198.62

Events

Transfer Block Create Move Execute Scan Retrospective Quarantine

Dispositions

Unknown Malware Clean Custom Unavailable

Events

Time	Event Type	Sending IP	Receiving IP	User	File Name	Disposition	Action	Protocol	Client	Web Applic
2018-01-11 14:20:53	Transfer	213.211.198.62	192.168.1.101	No Authentication Required	icar.com	Malware	Malware Block	HTTP	Edge	

- Analytics を選択
- Files > File Trajectory を選択
- File SHA256 の欄のハッシュ値を選択
- File Name: eicar.com を Malware として検知し、Action: Malware Block にしていることを確認

## 6. Pre-Filter設定

# Prefilter の概要

- FTD内 URL/ IPS/ AMP処理を担う Snortプロセスの前段、Lina(ASA)プロセスが パケットをハンドリングする機能
- NGIPS/NGFW機能を通す必要のない信頼されている通信(監視系・バックアップ系)などは、設計時に Prefilter Policyを通すことを推奨

# Prefilter Policy の追加

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

Access Control > **Prefilter** Network Discovery Application Detectors Correlation Actions

Object Management Access Control

**Prefilter Policy**

Overview Analysis **Policies** Devices Objects

Access Control > **Prefilter** Network Discovery App

**PREFILTER-POLICY**

Enter Description

Rules

Add Tunnel Rule Add Prefilter Rule Search Rules

#	Name	Rule Type	Source Interface Obj...	Destination Interface Obj...	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone
There are no rules. Add Tunnel Rule Add Prefilter Rule											

Non-tunneled traffic is allowed Default Action: Tunnel Traffic Analyze all tunnel traffic

- ① Policies内 Access Control > Prefilter を選択
- ② New Policyをクリック
- ③ Name: PREFILTER-POLICYを入力後、Save
- ④ 作成Prefilter内、Add Prefilter Rule を選択

# Prefilter Policy の追加

Add Prefilter Rule

Filter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and QoS.

Name: NTP-FASTPATH  Enabled

Action: Fastpath

Interface Objects | Networks | VLAN Tags | **Ports** | Comment | Logging

Available Ports

- NFS-UDP
- NTP-TCP
- NTP-UDP
- POP-2
- POP-3
- RADIUS
- RIP
- SIP
- SMTS
- SMTP

Selected Source Ports (0)

Selected Destination Ports (2)

- NTP-TCP
- NTP-UDP

Add Prefilter Rule

Filter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and QoS.

Name: NTP-FASTPATH  Enabled

Action: Fastpath

Interface Objects | Networks | VLAN Tags | **Ports** | Comment | **Logging**

Log at Beginning of Connection

Log at End of Connection

Send Connection Events to:

- ① Name: NTP-FASTPATH と入力
- ② Action: Fastpath を選択
- ③ Portsタブ NTP-TCP/NTP-UDP を選択
- ④ Loggingタブ Log at End... を選択
- ⑤ Add をクリック

# Prefilter Policy の追加

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

Access Control > Prefilter Network Discovery Application Detectors Correlation Actions

**PREFILTER-POLICY** You have unsaved changes Save Cancel

Enter Description

Rules

Add Tunnel Rule Add Prefilter Rule Search Rules

#	Name	Rule Type	Source Interface Obj...	Destination Interface Obj...	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone	
1	NTP-FASTPATH	Prefilter	any	any	any	any	any	NTP-TCP NTP-UDP	any	→ Fastpath	na	0

Non-tunneled traffic is allowed Default Action: Tunnel Traffic Analyze all tunnel traffic

- ① Save を選択
- ② ルールにヒットしない通信は全てAnalyze扱いになります

# Pre-filter Policy の設定

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

Access Control ▶ Access Control Network Discovery Application Detectors Correlation Actions

Object Management Intrusion Network Analysis Policy DNS Import/Export New Policy

Access Control Policy	Status	Last Modified
ACCESS-POLICY	Targeting 0 devices	2018-07-27 13:14:12 Modified by "admin"

Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control ▶ Access Control Network Discovery Application Detectors Correlation Actions

### ACCESS-POLICY

Enter Description

Pre-filter Policy: [Default Pre-filter Policy](#)

### Pre-filter Policy

The pre-filter policy performs early traffic handling using simple network characteristics, including non-encrypted encapsulation. (Firepower Threat Defense only.)

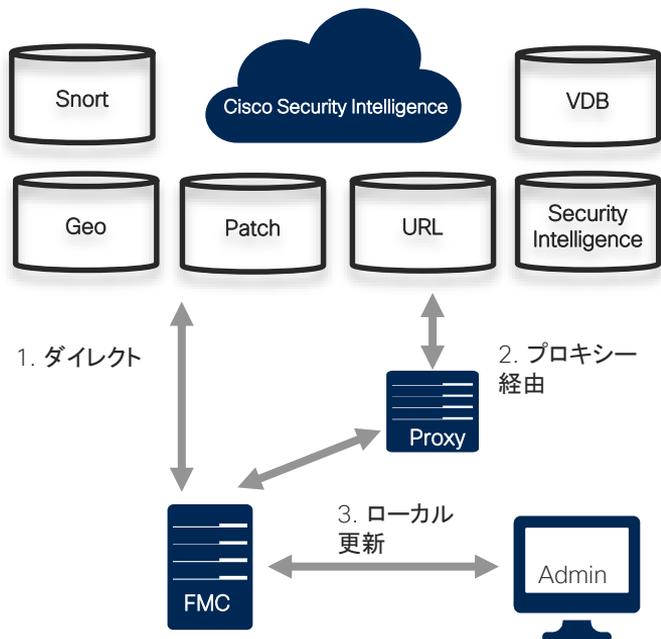
Default Pre-filter Policy

PREFILTER-POLICY

- ① Policies内 Access Controlを選択
- ② 作成済み Access Control Policy: ACCESS-POLICYの鉛筆マークをクリック
- ③ Access Control Policy 内 Pre-filter Policyをクリック
- ④ Pre-filter Policy: PREFILTER-POLICYを選択、OKをクリック
- ⑤ Save を選択後、Deploy

## 7. シグネチャ/ DB更新

# FMC シグネチャ/DB更新の概要



- FMC は3つの方法によって、情報を更新可能

## 1.クラウド更新(ダイレクト)

利用条件:FMC が直接インターネットへ接続可能

## 2. クラウド更新(プロキシー経由)

利用条件:Proxyサーバーがインターネットへ接続可能

## 3.ローカル更新

利用条件:FMC管理IPが閉域ネットワーク環境

制限事項:URL, Security Intelligence以外はローカル更新可能

# 更新パッケージおよび内容一覧

	内容	ファイル例	ワンタイム更新	定期更新	更新方法
Patch	新機能追加、既知Bug修正 (FMC/ FTD両方にパッチが存在)	Sourcefire_3D_Defense_Center_S3_Patch-6.2.0.4-85.sh	可能	可能 (別途スケジューリング必要)	クラウド・ローカル
Snort Rules	Snort IPSルールアップデート	Sourcefire_Rule_Update-2018-01-16-001-vrt.sh	可能	可能 (別途スケジューリング必要)	クラウド・ローカル
GeoDB	地理情報と紐づくグローバルIPアップデート	Sourcefire_Geodb_Update-2018-01-08-002.sh	可能	可能	クラウド・ローカル
VDB	OS/アプリケーションの脆弱性、検出、フィンガープリント情報	Sourcefire_VDB_Fingerprint_Database-4.5.0-291.sh	可能	可能	クラウド・ローカル
URL	URLフィルタリングに用いるURL情報		可能	可能	クラウド
Security Intelligence	ブラックリストIP/URL/Domain情報		不可	可能	クラウド

※全てのパッケージにおいて定期更新はクラウド経由のみ可能

# クラウド接続方法の確認



① Interfaces

Link	Name	Channels	MAC Address	IP Address
✓	eth0	Management Traffic Event Traffic	00:0C:29:75:5D:68	10.71.132.201

② Management Interfaces

③ Shared Settings: DNS設定を確認

④ Proxy Enabledにチェック、Proxy設定を入力(プロキシ利用時)

① GUI上部 System配下の Configurationを選択

② Management Interfaceを選択

③ Shared Settings: DNS設定を確認

④ Proxy Enabledにチェック、Proxy設定を入力(プロキシ利用時)

通信要件: <https://support.sourcefire.com>

# ローカル更新用パッケージ準備

## Download Software

 Download Cart (0 items) [\[+\] Feedback](#) [Help](#)

[Downloads Home](#) > [Products](#) > [Security](#) > [Firewalls](#) > [Firewall Management](#) > [Firepower Management Center Virtual Appliance](#) > **FireSIGHT System Software-6.2.0.4**

### Firepower Management Center Virtual Appliance

  
[Expand All](#) | [Collapse All](#)

**Release 6.2.0.4**

[Documentation Roadmap](#)  [My Devices](#)  
[FirePower Hotfix Release Notes](#)  [Notifications](#)  
[Release Notes for 6.2.0.4](#)

File Information	Release Date	Size	
<b>Firepower Management Center 6.2.0.4</b> Sourcefire_3D_Defense_Center_S3_Patch-6.2.0.4-85.sh	08-JAN-2018	756.70 MB	<a href="#">Download</a> <a href="#">Add to cart</a> <a href="#">Publish</a>

- ① Cisco.com サポートページより権限あるアカウントでアクセス
- ② 更新する予定のパッケージをダウンロード

# VDB/Patch ワンタイム更新

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin6

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Product Updates Rule Updates Geolocation Updates

Currently running software version: 6.2.2

### Updates

Type	Version	Date	Release Notes	Reboot
Sourcefire Vulnerability And Fingerprint Database Updates	291	Thu Dec 7 16:45:46 UTC 2017		No
Sourcefire 3D Defense Center S3 Patch (v6.2.1 and above)	6.2.2.1-73	Fri Nov 3 19:09:03 UTC 2017		Yes
Cisco FTD Patch (v6.2.1 and above)	6.2.2.1-73	Fri Nov 3 17:48:24 UTC 2017		Yes

Upload Update

Download updates

- ① GUI上部 System配下の Updatesを選択
- ② Product Updates内の Downloaded Updatesを選択。Patch, VDBに更新がある場合は、更新可能なファイルを表示(ダイレクトもしくはProxy経由更新の場合)
- ③ Product Updates内の Upload Updateを選択。VDBもしくは FMC/FTD Patchをアップロード(ローカル更新の場合)

(注) ②の実施時にはブラウザの画面を閉じないこと

# VDB/Patch ワンタイム更新～インストール

Currently running software version: 6.2.2

## Updates

Type	Version	Date	Release Notes	Reboot	
Sourcefire Vulnerability And Fingerprint Database Updates	291	Thu Dec 7 16:45:46 UTC 2017		No	 
Sourcefire 3D Defense Center S3 Patch (v6.2.1 and above)	6.2.2.1-73	Fri Nov 3 19:09:03 UTC 2017		Yes	 
Cisco FTD Patch (v6.2.1 and above)	6.2.2.1-73	Fri Nov 3 17:48:24 UTC 2017		Yes	 

Download updates

Currently running software version: 6.2.2

### Selected Update

**Type** Sourcefire Vulnerability And Fingerprint Database Updates  
**Version** 291  
**Date** Thu Dec 7 16:45:46 UTC 2017  
**Release Notes**  
**Reboot** No

By Group

### ▼ Ungrouped (1 total)

FMCv  
 10.71.132.201 - Cisco Firepower Management Center for VMWare v6.2.2

**Health Policy**  
[Initial Health Policy 2017-12-13 04:06:07](#) 

Launch Readiness Check

- ① Updates欄にある  マークを選択
- ② 更新ファイルをインストールする対象デバイスを選択
- ③ Launch Readiness Checkを選択
- ④ Readiness Check実施後、Installを選択

- VDB/Patch 更新は、FTDデータ通信トラフィック影響があるため計画適用を推奨

# スケジュールリング機能

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin6

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools > Scheduling

**New Task**

Job Type

Schedule task to run

Current time

Start Time 2:00

Job Name

Backup Profile No backup profiles exist. Please create a backup profile.

Comment

Email Status To Not available. You must set up your mail server.

Save Cancel

Backup/Restore  
**Scheduling**  
Import/Export  
Data Purge

① GUI上部 System配下の Tools ▶ Scheduling を選択  
② New Taskより 実施したい項目を選択  
③ どの項目においても Job Name/ Onceまたは Recurring およびスケジュールリングを設定

実行可能な項目 (FMCv6.2)

- Backup - FMCバックアップ取得
- Download CRL - 証明書失効リストダウンロード
- Deploy Policies - ポリシー適用
- Nmap Scan - Nmapスキャン実行
- Report - レポート生成
- Firepower Recommended Rules - 自動チューニングの実施
- Download Latest Update - VDB/Patchダウンロード
- Install Latest Update - VDB/Patchインストール
- Push Latest Update - Patchイメージの配布
- Update URL Filtering Database - URLフィルタリングDB更新

# VDB/Patch 定期更新

The screenshot shows the 'New Task' configuration page in the Cisco AMP Intelligence interface. The 'Job Type' is set to 'Download Latest Update'. The 'Schedule task to run' is set to 'Recurring'. The 'Start On' date is January 17, 2018, in the Asia/Tokyo time zone. The 'Repeat Every' is set to 1 week. The 'Run At' time is 5:00 PM. The 'Repeat On' days are checked for Sunday. The 'Job Name' is 'download\_patch&VDB'. The 'Update Items' section has 'Software' and 'Vulnerability Database' checked. A blue arrow points to the 'Scheduling' option in the 'Tools' menu, which is circled with a '1'.

- ① GUI上部 System配下の Tools ▶ Scheduling を選択
- ② New Taskより Download Latest Updateを選択
- ③ Schedule task to run: Recurringを選択
- ④ Repeat Every, Hours/Days/Weeks, Run AT, Repeat On よりスケジュール設定
- ⑤ Updates Items より Patch, Vulnerability 必要なパッケージを選択

- VDB/Patch のみ新しいパッケージを定期チェックするのにスケジューリング機能が必要

# VDB/Patch 定期更新～インストール

The screenshot shows the 'New Task' configuration interface in the Cisco AMP Intelligence console. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. A secondary navigation bar contains 'Configuration', 'Users', 'Domains', 'Integration', 'Updates', 'Licenses', 'Health', 'Monitoring', and 'Tools > Scheduling'. The 'Tools > Scheduling' menu is open, showing options like 'Backup/Restore', 'Scheduling', 'Import/Export', and 'Data Purge'. The 'Scheduling' option is highlighted with a blue arrow and a circled '1'. The main configuration area includes fields for 'Job Type' (Install Latest Update), 'Schedule task to run' (Recurring), 'Start On' (January 17, 2018, Asia/Tokyo), 'Repeat Every' (1 week), 'Run At' (2:30 AM), 'Repeat On' (Sunday), 'Job Name' (Install patch to FMC), 'Device' (FMCv), and 'Update Items' (Software). A blue text box at the bottom provides instructions in Japanese.

- ① GUI上部 System配下の Tools ▶ Scheduling を選択
- ② New Taskより Install Latest Updateを選択
- ③ Schedule task to run: Recurringまたは Onceを選択
- ④ Repeat Every, Hours/Days/Weeks, Run AT, Repeat On よりスケジュール設定
- ⑤ Updates Items より Patch, Vulnerability 必要なパッケージと対象Deviceを選択

# Snort Rules ワンタイム更新

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin6

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Product Updates Rule Updates Geolocation Updates

Delete All Local Rules Rule Update Log

### One-Time Rule Update/Rules Import

Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Source

- Rule update or text rule file to upload and install (3)  
ファイルを選択 選択されていません
- Download new rule update from the Support Site (2)
- Reapply all policies after the rule update import completes

Policy Deploy

Import

**Warning**

Enabling this option might cause a temporary traffic interruption when policies are applied to the device based on the type of rule update. You can also apply the policies to the device by clicking on Deploy button and selecting the required device

OK

- ① GUI上部 System配下の Updatesを選択後、Rule Updatesを選択
- ② Source: Download new rule update from support siteを選択後、Importを選択(ダイレクトもしくはProxy経由更新の場合)
- ③ Source: Rule Update or txt rule file to upload and installを選択後、ファイルをアップロードして Importを選択 (ローカル更新の場合)

- Reapply all policies After the rule update import completesにチェックすると、Snort Rules更新後、全ポリシーを持つ FTDに対してルール配信を実行
- Snort Rules更新によりSnortプロセスが再起動するため、FTDデータ通信影響が起こる可能性がある

# Snort Rules 定期更新



- ① GUI上部 System配下の Updatesを選択後、Rule Updatesを選択
- ② Enable Recurring Rule Imports from support siteを選択
- ③ Import Frequency Daily/Weekly/Monthly at 更新時間を設定
- ④ Saveを選択

- Deploy updated policies to targeted devices after update completes にチェックすると、Snort Rules更新後、全ポリシーを持つ FTDに対してルール配信を実行

## Recurring Rule Update Imports

The scheduled rule update feature is not enabled.  
Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Enable Recurring Rule Update Imports from the Support Site

Import Frequency

②  
Daily at 11:00 PM Asia/Tokyo ③

Policy Deploy

Deploy updated policies to targeted devices after rule update completes

Save Cancel

# Snort Rules 更新ログ

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Product Updates Rule Updates Geolocation Updates

Delete All Local Rules Rule Update Log

Summary	Time	User ID	Status
<b>Snort Rule Update 2016 11 29 001 vrt</b> Completed install of Snort Rule Update 2016-11-29-001-vrt	2017-12-13 13:04:46	admin	✓

- ① GUI上部 System配下の Updatesを選択後、Rule Update Logを選択
- ② インストールされたパッケージ(-vrt)の 🔍 マークを選択



# Snort Rules 更新ログ

## Rule Update Import Log

Table View of Rule Update Import Log

Search Constraints (Edit Search Save Search)

Disabled Columns

	Time	Name	Type	Action	GID	SID	Rev	Policy	Details
↓	2018-01-11 11:10:02	MALWARE-CNC Win.Trojan.Strictor.variant.outbound.connection	rule	new	1	30259	2	All	New
↓	2018-01-11 11:10:02	MALWARE-CNC Win.Trojan.Symmi.variant.outbound.connection	rule	new	1	30262	2	All	New
↓	2018-01-11 11:10:02	MALWARE-CNC Win.Trojan.Zbot.configuration.file.download	rule	new	1	30270	2	All	New
↓	2018-01-11 11:10:02	MALWARE-CNC Win.Trojan.Zbot.drop.zone.file.upload	rule	new	1	30271	2	All	New
↓	2018-01-11 11:10:02	MALWARE-CNC Win.Trojan.Sloth.variant.command.and.control.traffic	rule	new	1	30275	1	All	New

- パッケージ毎に更新された Snort Ruleが表示
- Name/ SID (Snort rule ID) はオープンソースSnortコミュニティと同一の内容
- ”snort.org“からSID番号を検索すると同様の結果が得られる

30259

Documents Downloads

---

## Sid 1-30259

Summary:

MALWARE-CNC Win.Trojan.Strictor.variant.outbound.connection



# Snort Rules 更新ログ

Download Software Download Cart (0 items) Feedback Help

Downloads Home > Products > Security > Firewalls > Firewall Management > Firepower Management Center Virtual Appliance > FireSIGHT System Software-Rules Updates

Firepower Management Center Virtual Appliance

Search... My Devices Notifications

Expand All | Collapse All

Release Rules Updates

File Information	Release Date	Size
Sourcefire Rule Update 2018-01-16-001 Sourcefire_Rule_Update-2018-01-16-001-vrt.sh	16-JAN-2018	118.83 MB

**Details**

Description: **Sourcefire Rule Update 2018-01-16-001**

Release: **Rules Updates**

Release Date: **16/Jan/2018**

File Name: **Sourcefire\_Rule\_Update-2018-01-16-001-vrt.sh**

Size: **118.82 MB (124592062 bytes)**

MDS Checksum: **498713c4a31fb0f823a39b496eabf652**

SHA512 Checksum: **9d286ac161ed32971b4e2f8368586744...**

[Modified Rules](#) | [New Rules](#) | [SRU\\_2018-01-16-001](#)

**New Rules:**

GID	SID	Rule Group	Rule Message	Policy State		
				Con.	Bal.	Sec.
1	45418	OS-OTHER	Apple macOS IOHIDeous exploit download attempt	off	off	drop
1	45419	OS-OTHER	Apple macOS IOHIDeous exploit download attempt	off	off	drop
1	45420	SERVER-WEBAPP	Drupal HTTP Strict Transport Security module security bypass attempt	off	off	off
1	45421	SERVER-WEBAPP	PhpCollab editclient.php arbitrary PHP file upload attempt	off	off	drop
1	45437	MALWARE-CNC	Win.Trojan.Ramnit outbound connection attempt	off	off	drop
1	45438	MALWARE-CNC	Win.Trojan.Ramnit outbound connection attempt	off	drop	drop
1	45439	MALWARE-CNC	Win.Trojan.Ramnit outbound connection attempt	off	drop	drop
1	45440	SERVER-OTHER	HP LoadRunner remote command execution attempt	off	off	off
3	45441	SERVER-WEBAPP	TRUFFLEHUNTER TALOS-2018-0511 attack attempt	off	off	drop
1	45445	BROWSER-IE	Microsoft Edge scripting engine ArrayBuffer memory corruption attempt	off	drop	drop
1	45446	BROWSER-IE	Microsoft Edge scripting engine ArrayBuffer memory corruption attempt	off	drop	drop

- Snort Rules ローカル更新用パッケージからも、更新内容を確認可能
- 更新内容にそれぞれのSIDが IPS推奨ルールにおいてどう扱われるのか確認可能

# GeoDB ワンタイム更新

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin6

Configuration Users Domains Integration **Updates** Licenses Health Monitoring Tools

Product Updates Rule Updates **Geolocation Updates**

Running geolocation update version: **None**

**One-Time Geolocation Update**

Note that updates may be large and can take up to 45 minutes.

Source

Upload and install geolocation update ③  
ファイルを選択 選択されていません

Download and install geolocation update from the Support Site ②

Import

- ① GUI上部 System配下の Updatesを選択後、Geolocation Updatesを選択
- ② Source: Download new geolocation update from support siteを選択後、Importを選択(ダイレクトもしくはProxy経由更新の場合)
- ③ Source: Download and install geolocation update from support siteを選択後、ファイルをアップロードして Importを選択 (ローカル更新の場合)

# GeoDB 定期更新

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin6

Configuration Users Domains Integration **Updates** Licenses Health Monitoring Tools

Product Updates Rule Updates **Geolocation Updates**

Running geolocation update version: **None**

- ① GUI上部 System配下の Updatesを選択後、Geolocation Updatesを選択
- ② Enable Recurring Weekly Updates from support siteを選択
- ③ 曜日/更新時間を設定
- ④ Saveを選択

Import

## Recurring Geolocation Updates

Enable Recurring Weekly Updates from the Support Site  ②

Update Start Time

Tuesday ③

09:00

PM

Asia/Tokyo

Save

Cancel

# URL Filtering ワンタイム・定期更新・照会設定



Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin6

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Cisco CSI Realms Identity Sources eStreamer Host Input Client Smart Software Satellite

**URL Filtering**

Last URL Filtering Update: 2018-01-17 07:27:27

Enable URL Filtering

Enable Automatic Updates

Query Cisco CSI for Unknown URLs

- ① GUI上部 System配下の Integrationを選択後、Cisco CSIを選択
- ② URL Filtering: Update Nowを選択(ワンタイム更新・ダイレクトもしくはProxy経由更新のみ)
- ③ URL Filtering: Enable Automatic Updateを選択後、Saveを選択(定期更新・ダイレクトもしくはProxy経由更新のみ)

- Enable Automatic Update: 1日1回パッケージを定期更新
- Query Cisco CSI for Unknown URLs: URL情報をローカル解決できない場合に、クラウドへ照会
- 通信要件: <https://database.brightcloud.com> 、 <http://service.brightcloud.com>

# Security Intelligence 定期更新・スケジューリング変更

Overview Analysis Policies Devices **Objects** AMP Intelligence Deploy System Help admin6

Object Management Intrusion Rules

Update Feeds Add Network Lists and Feeds Filter

Name	Type	
Cisco-Intelligence-Feed <i>Last Updated: 2018-01-17 15:34:10</i>	Feed	
Cisco-TID-Feed	Feed	
Global-Blacklist	List	
Global-Whitelist	List	

Network  
Port  
Interface  
Tunnel Zone  
Application Filters  
VLAN Tag  
Security Group Tag  
URL  
Geolocation  
Time Range  
Variable Set  
**Security Intelligence**  
Network Lists and Feeds  
DNS Lists and Feeds  
URL Lists and Feeds

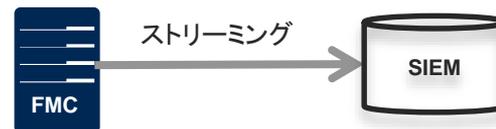
- ① GUI上部 Objects配下の Object Managementを選択
- ② Security Intelligence内の Network Lists and Feed または DNS Lists and Feedを選択

- デフォルト 2時間更新
- マークを選択、定期更新時間を変更可能

# 8. eStreamer API & Splunk eNcore App

# Event Streamer (eStreamer) APIとは

- eStreamer API を使用することで、Firepower Management Center (FMC) から外部クライアントに Firepower システムイベントのストリーミングして外部にイベントを出力できるAPI
- クライアントと通信するためにメッセージ指向のカスタムアプリケーション層プロトコルを使用
- サポートするイベントタイプ
  - ホストデータ
  - 検出データ
  - コンプライアンスのホワイトリスト
  - 接続データ
  - Firepower シリーズのデバイスからの侵入データ
  - ファイル・マルウェア



# eNcore とは

- 2018年7月現在 version 3.5 となる eStreamer クライアント
- Splunk (CIM フォーマット)、CEF アウトプットフォーマットをサポートしているため、Splunk や他のSIEMと容易に連携できる
- eNcore Add-on は SIEM連携用の仕組みを提供、eNcore App は Splunk側で情報を表示するためのもの
- 両方とも Splunkbase より無償ダウンロードが可能



**Cisco eStreamer eNcore  
Add-on for Splunk**

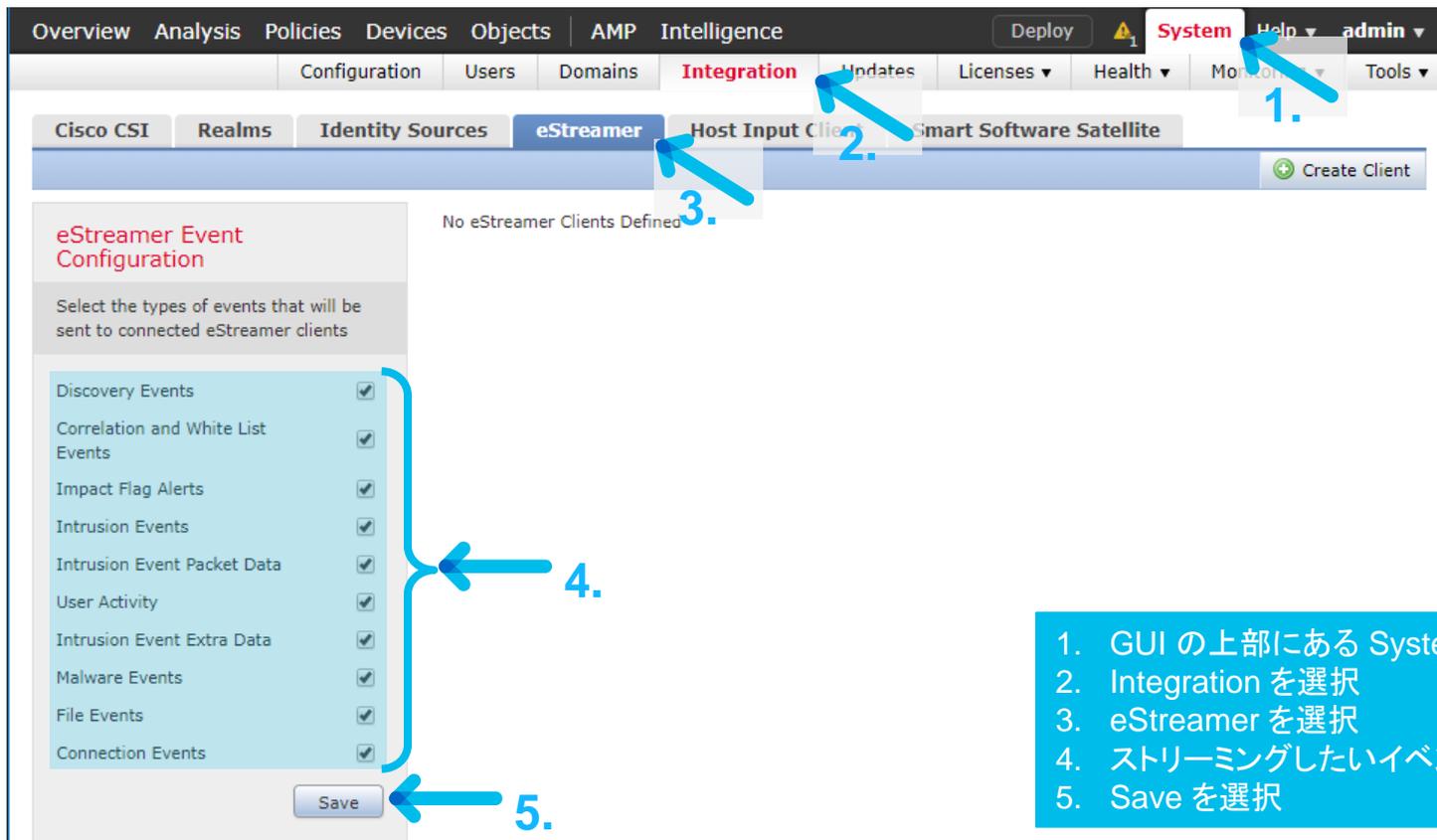
<https://splunkbase.splunk.com/app/3662/>



**Cisco Firepower eNcore  
App for Splunk**

<https://splunkbase.splunk.com/app/3663/>

# ステップ1. sStreamer ストリーミングイベントの設定



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

Configuration Users Domains **Integration** Updates Licenses Health Mon Tools

Cisco CSI Realms Identity Sources **eStreamer** Host Input Client Smart Software Satellite

No eStreamer Clients Defined Create Client

**eStreamer Event Configuration**

Select the types of events that will be sent to connected eStreamer clients

- Discovery Events
- Correlation and White List Events
- Impact Flag Alerts
- Intrusion Events
- Intrusion Event Packet Data
- User Activity
- Intrusion Event Extra Data
- Malware Events
- File Events
- Connection Events

Save

1. GUI の上部にある System を選択
2. Integration を選択
3. eStreamer を選択
4. ストリーミングしたいイベントデータを選択
5. Save を選択

# ステップ2. リファレンスクライアント向けの 証明書生成

The screenshot shows the Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Intelligence' section is active, and the 'Integration' sub-section is selected. The 'eStreamer' tab is highlighted. A blue arrow labeled '1.' points to the 'Create Client' button. Below the main interface, a 'Create Client' form is shown with a blue arrow labeled '2.' pointing to the 'Hostname \*' field containing '192.168.1.101' and another blue arrow labeled '3.' pointing to the 'Save' button.

1. Create Client を選択
  2. クライアントのホスト名、もしくは、IPアドレス (DNSを設定しない場合)を入力
  3. Save を選択
- \*Password は任意  
次のスライドへ続く



# ステップ2. リファレンスクライアント向け証明書取得

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Cisco CSI Realms Identity Sources eStreamer Host Input Client Smart Software Satellite

Create Client

Success  
Created client 192.168.1.101

eStreamer Event Configuration  
Select the types of events that will be sent to connected eStreamer clients

Hostname
192.168.1.101

4.

4. Hostname に追加されたクライアントの横の下矢印 (↓) マークを選択
5. ダウンロードした .pkcsファイルを "client.pkcs" に名前変更
6. リファレンスクライアントOS側へ転送

## ステップ3. ライブラリのインストール

- リファレンスクライアントとなる CentOS に Python2.7 をインストールする

```
sudo yum install python
```

- リファレンスクライアントとなる CentOS に OpenSSLモジュール をインストールする

```
sudo yum install python-pip python-devel openssl-devel gcc
```

```
sudo pip install pyOpenSSL
```

- (上記モジュール群がインストールできない場合) EPELレポジトリを利用する

```
wgethttp://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-9.noarch.rpm
```

```
sudo rpm -ivh epel-release-7-9.noarch.rpm
```

# ステップ4. Splunk(CentOS)設定

- /usr/local 配下に splunkをインストール
- Splunk利用時の環境変数設定

```
# export SPLUNK_HOME=/usr/local/splunk  
  
# export | grep SPLUNK  
  
declare -x SPLUNK_HOME="/usr/local/splunk"
```

- 環境変数の永続化は“~/.bash\_profile”に以下を追記

```
SPLUNK_HOME=/usr/local/splunkexport  
  
SPLUNK_HOME
```

- 設定ファイルの反映

```
# source ~/.bash_profile
```

# ステップ5. Splunk(CentOS)起動

- Splunk 起動コンフィグの作成

```
# cd $SPLUNK_HOME/etc
```

```
# cp splunk-launch.conf.default splunk-launch.conf
```

- Splunk-launch.conf内に利用環境のパスを追記

```
SPLUNK_HOME=/usr/local/splunk
```

- Splunkの起動、起動時に adminパスワードを入力

```
# cd $SPLUNK_HOME/bin
```

```
# ./splunk start --accept-license
```

# ステップ6. Splunk(CentOS) (オプション)Firewalld ポート開放、起動の自動化

- CentOS7 Firewalldが動作している場合は、以下をポート開放(TCP:8000 Splunk Web/ TCP:8302: eStreamer API )

```
# firewall-cmd --add-port=8000/tcp --zone=public -permanent
```

```
# firewall-cmd --add-port=8302/tcp --zone=public -permanent
```

- OSブート時に自動起動する設定を行う場合は以下コマンドを入力

```
# $SPLUNK_HOME/bin/splunk enable boot-start
```

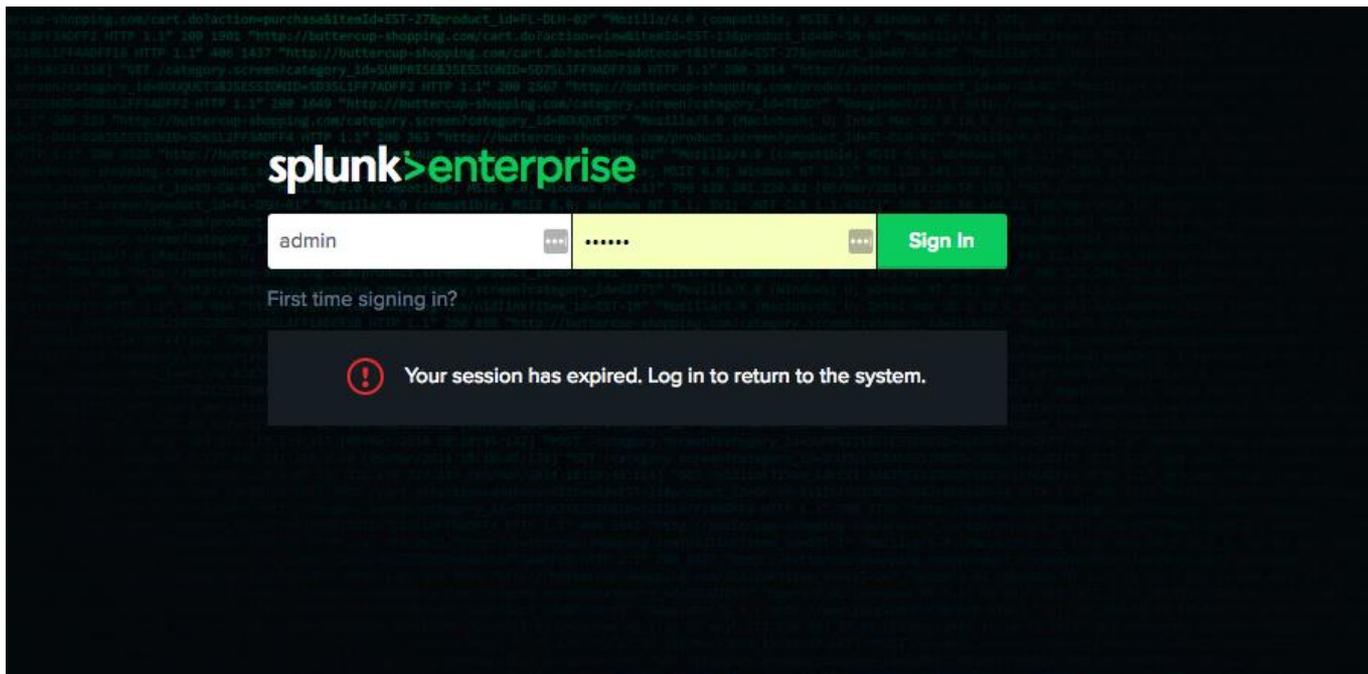
# ステップ7. FMC eStreamer Cert配置

- FMCよりダウンロードした証明書(client.pkcs12)を以下に配置

```
# $SPLUNK_HOME/etc/apps/TA-eStreamer/bin/encore/
```

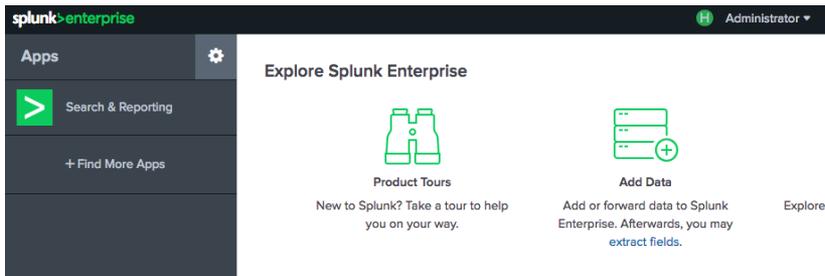
# ステップ8. Splunkへのアクセス

- リファレンスクライアントIPにHTTP Port 8000でアクセス、設定済み adminパスワードでログイン

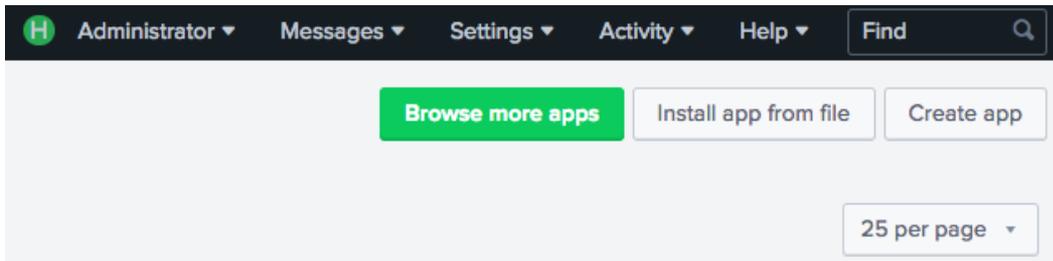


# ステップ9. Splunk Appインストール

- Splunkトップ画面より、Apps横の歯車マークをクリック



- Install App from FileもしくはBrowse more apps より 以下2つのAppをインストール
- Cisco eStreamer eNcore for Splunk, Cisco eStreamer eNcore Dashboard for Splunk



# ステップ10. eNcore App セットアップ

- eNcore Appインストール後、Splunk Appsより eNcore for splunkを setup

**Apps** [Browse more apps](#)

Showing 1-19 of 19 items

- Controlにチェックボックス、Connectionに FMC IPを入力

## Control

- Is enabled? The eNcore client should remain disabled until configured. If running, it may take a moment or two for the client to stop once disabled.

## Connection

FMC Hostname or IP address



Port

# ステップ11. eNcore App セットアップ

- FMC eStreamer Cert発行時のパスワードを入力、Data 三箇所をチェックボックスを入れて保存

## Authentication

Cisco eStreamer eNcore for Splunk needs to authenticate with your FMC. This requires a PKCS12 file to be created on your FMC and then installed locally. There is no way to do this without manually copying the file onto this server.

You need to rename the PKCS12 file `client.pkcs12` and place it in this exact location:

```
$SPLUNK_HOME/etc/apps/TA-eStreamer/bin/encore/client.pkcs12
```

- Process PKCS12 file? (You must do this if you add a new PKCS12 file or change the host)

PKCS12 password

.....



Confirm password

.....

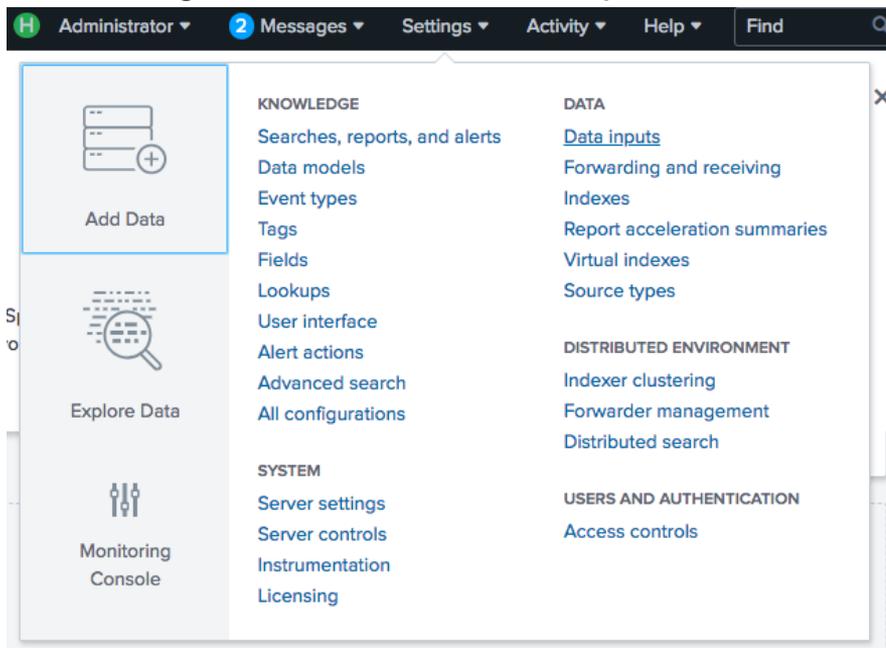


## Data

- Packets? Packet logs can be large and use up storage
- Connections? This is a very high-volume option and may consume significant network and storage usage
- Metadata? Metadata logs are not event-driven but can prove informative

# ステップ12. eNcore Data scriptの起動

- Settings > Add Data > Data inputsを選択



# ステップ13. eNcore Data cisco:estreamer:dataの起動

- Data inputs > Files & Directories を選択

## Data inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

### Local inputs

Type	Inputs	Actions
<a href="#">Files &amp; Directories</a> Index a local file or monitor an entire directory.	7	+ Add new
<a href="#">HTTP Event Collector</a> Receive data over HTTP or HTTPS.	0	+ Add new
<a href="#">TCP</a> Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new
<a href="#">UDP</a> Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new
<a href="#">Scripts</a> Run custom scripts to collect or generate more data.	8	+ Add new

# ステップ14. eNcore Data cisco:estreamer:dataの起動

- Files & Directories 内cisco:estreamer:dataを Enable

## Files & directories

[New Local File & Directory](#)[Settings](#) > [Data inputs](#) > Files & directories

Showing 1-7 of 7 items

Full path to your data ▾	Set host ▾	Source type ▾	Index ▾	Number of files ▾	App ▾	Status ▾	Actions
<code>\$(SPLUNK_HOME)/etc/apps/TA-eStreamer/data</code>	Constant Value	cisco:estreamer:data	default	4	TA-eStreamer	Enabled   <a href="#">Disable</a>	
<code>\$(SPLUNK_HOME)/etc/splunk.version</code>	Constant Value	splunk_version	_internal	1	system	Enabled   <a href="#">Disable</a>	
<code>\$(SPLUNK_HOME)/var/log/introspection</code>	Constant Value	Automatic	_introspection	15	introspection_generator_addon	Enabled   <a href="#">Disable</a>	
<code>\$(SPLUNK_HOME)/var/log/splunk</code>	Constant Value	Automatic	_internal	32	system	Enabled   <a href="#">Disable</a>	
<code>\$(SPLUNK_HOME)/var/log/splunk/license_usage_summary.log</code>	Constant Value	Automatic	_telemetry	2	system	Enabled   <a href="#">Disable</a>	
<code>\$(SPLUNK_HOME)/var/spool/splunk</code>	Constant Value	Automatic	default		system	Disabled   <a href="#">Enable</a>	
<code>\$(SPLUNK_HOME)/var/spool/splunk/...stash_new</code>	Constant Value	stash_new	default	1	system	Enabled   <a href="#">Disable</a>	

# ステップ15. eNcore Data scriptの起動

- Data inputs > Scripts を選択

## Data inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

### Local inputs

Type	Inputs	Actions
<a href="#">Files &amp; Directories</a> Index a local file or monitor an entire directory.	7	+ Add new
<a href="#">HTTP Event Collector</a> Receive data over HTTP or HTTPS.	0	+ Add new
<a href="#">TCP</a> Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new
<a href="#">UDP</a> Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new
<a href="#">Scripts</a> Run custom scripts to collect or generate more data.	8	+ Add new

# ステップ16. eNcore Data scriptの起動

- Scripts内 splencore.sh clean/ start/ status 3つを Enable

## Script

Data inputs > Script

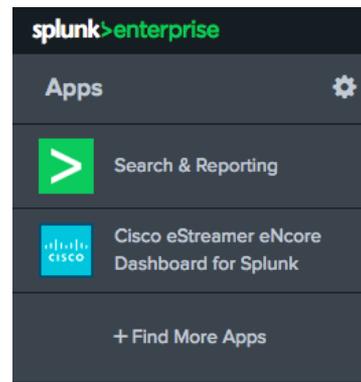
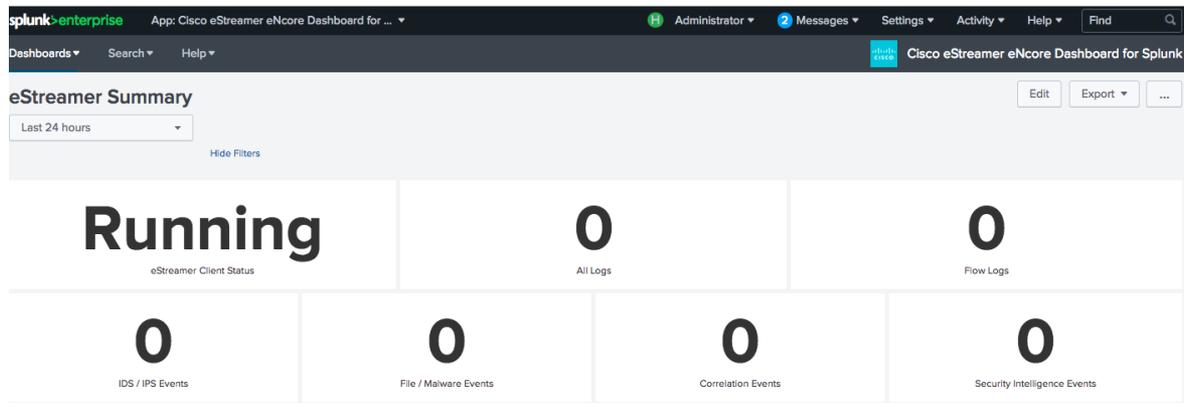
Showing 1-8 of 8 items

 25 per page

Command	Interval	Source type	App	Status	Actions
<code>\$(SPLUNK_HOME)/etc/apps/splunk_instrumentation/bin/instrumentation.py</code>	0 ****	splunk_telemetry_log	splunk_instrumentation	Enabled   Disable	Clone
<code>\$(SPLUNK_HOME)/etc/apps/splunk_instrumentation/bin/on_splunk_start.py</code>	-1	script	splunk_instrumentation	Enabled   Disable	Clone
<code>\$(SPLUNK_HOME)/etc/apps/splunk_instrumentation/bin/schedule_delete.py</code>	0 0 ***	script	splunk_instrumentation	Enabled   Disable	Clone
<code>/usr/local/splunk/etc/apps/introspection_generator_addon/bin/collector.path</code>	0	splunk_resource_usage__internal	introspection_generator_addon	Enabled   Disable	Clone
<code>/usr/local/splunk/etc/apps/splunk_monitoring_console/bin/dmc_config.py</code>	-1	script	splunk_monitoring_console	Enabled   Disable	Clone
<code>/usr/local/splunk/etc/apps/TA-eStreamer/bin/splencore.sh clean</code>	900	cisco:estreamer:clean	TA-eStreamer	Disabled   Enable	Clone
<code>/usr/local/splunk/etc/apps/TA-eStreamer/bin/splencore.sh start</code>	120	cisco:estreamer:log	TA-eStreamer	Disabled   Enable	Clone
<code>/usr/local/splunk/etc/apps/TA-eStreamer/bin/splencore.sh status</code>	30	cisco:estreamer:status	TA-eStreamer	Disabled   Enable	Clone

# ステップ17. eNcore Dashboard確認

- Top Pageより eNcore Dashboard for Splunkを選択
- Staus: Runningであることを確認





# 9: メンテナンス

# FTD メンテナンス

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy 1 System Help admin6

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

By Group Add...

Name	Group	Model	License Type	Access Control Policy
Ungrouped (1)				
<b>FTDv1</b> 10.71.132.202 - Cisco Firepower Threat Defense for VMWare - v6.2.2 - ro		Cisco Firepower Threat Defense f	Base, Threat, Malware, URL F...	<a href="#">ACCESS-POLICY</a>

## FTDv1

Cisco Firepower Threat Defense for VMWare

Device Routing Interfaces Inline Sets DHCP

### General

Name: FTDv1  
Transfer Packets: Yes  
Mode: routed  
Compliance Mode: None

- ① Devices内 Device Managementを選択
  - ② 管理FTD の鉛筆マークをクリック
  - ③ Device タブ内 System からシャットダウン  再起動  が可能
- Tips) Firepower 4K/9K シリーズは Firepowerシャーシマネージャーから再起動、停止を実行

### System

Model: Cisco Firepower Threat Defense for VMWare

# FMC メンテナンス

The screenshot shows the Cisco FMC web interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. On the right, there are buttons for 'Deploy', 'System' (with a red notification icon), 'Help', and 'admin6'. Below the navigation bar, a secondary menu shows 'Configuration' (highlighted in red), 'Users', 'Domains', 'Integration', 'Updates', 'Licenses', 'Health', 'Monitoring', and 'Tools'. On the left, a sidebar menu shows 'Access List' and 'Process' (highlighted in red). Under 'Process', there are options for 'Audit Log Certificate', 'Audit Log', 'Login Banner', and 'Change Reconciliation'. The main content area displays a table with a 'Name' header and three rows of system processes, each with a green arrow icon and the text 'Run Command':

Name	Action
Shutdown Management Center	Run Command
Reboot Management Center	Run Command
Restart Management Center Console	Run Command

- ① System内Processを選択
- ② Shutdown Management Center: システムシャットダウン
- ③ Reboot Management Center: プロセスのみ再起動
- ④ Restart Management Center: OS再起動

# 10 レポートティング

# Report 生成

The screenshot shows the Cisco AMP Reporting interface. At the top, there is a navigation bar with 'Overview' (highlighted in red), 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. On the right side of the navigation bar, there are buttons for 'Deploy', 'System', 'Help', and 'admin'. Below the navigation bar, there is a sub-navigation bar with 'Dashboards', 'Reporting' (highlighted in red), and 'Summary'. The main content area has two tabs: 'Reports' and 'Report Templates' (highlighted in blue). A '+ Create Report Template' button is visible in the top right corner of the main content area. Below the tabs, there is a section titled 'Risk Report Templates' with a list of templates: 'Advanced Malware Risk Report', 'Attacks Risk Report', and 'Network Risk Report'. Each template has a set of icons for actions like view, edit, and delete. Below the templates, there is a section titled 'Templates' with a sub-section for 'Attack Report: \$<Attack SID>' and a timestamp '2017-04-06 23:06:16 Last Modified By admin'.

- ① Overview内、Reportingを選択
  - ② Report Templateタブを選択
  - ③ テンプレートより、Attacks Risk Reportの本マークをクリック
- Tips) 初期状態でテンプレートが用意済み、FMC 言語設定に合わせてレポート言語も変更可能

# Report 生成

Generate Report



### Report Generation Information

File Name  

Time Window  Last week

Relay Host No Relay Host Configured! 

Empty Sections  Exclude

### Input Parameters

Company Name

Author

Contact

- ① デフォルト 1週間の情報をレポート化
- ② 必要に応じて Inputs Parametersを入力
- ③ Generate をクリックすると、レポートが生成される

# Report 確認



① 生成されたレポートをクリックして中身を確認

# Reportの自動化: スケジューリング機能の活用

The screenshot shows the Cisco AMP Intelligence Scheduling interface. The top navigation bar includes Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The right side shows System, Help, and admin6. The main menu includes Configuration, Users, Domains, Integration, Updates, Licenses, Health, and Monitoring. The Tools > Scheduling menu is open, showing Backup/Restore, Scheduling, Import/Export, and Data Purge. The Scheduling page has a 'New Task' section with a dropdown menu for Job Type. The dropdown menu is open, showing options: Backup (checked), Download CRL, Deploy Policies, NMap Scan, Report, Firepower Recommended Rules, Download Latest Update, Install Latest Update, Push Latest Update, and Update URL Filtering Database. A blue callout box contains three steps: ① GUI上部 System配下の Tools ▶ Scheduling を選択, ② New Taskより 実施したい項目を選択, ③ どの項目においても Job Name/ Onceまたは Recurring およびスケジューリングを設定. A green callout box contains a bullet point: • Report - レポート生成. The 'Job Name' field is empty. The 'Backup Profile' field shows a message: 'No backup profiles exist. Please create a backup profile first.' The 'Email Status To' field shows a message: 'Not available. You must set up your mail relay host.' The 'Save' and 'Cancel' buttons are visible at the bottom.

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy System Help admin6

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools ▶ Scheduling

**New Task**

Job Type

- ✓ Backup
- Download CRL
- Deploy Policies
- NMap Scan
- Report
- Firepower Recommended Rules
- Download Latest Update
- Install Latest Update
- Push Latest Update
- Update URL Filtering Database

Schedule task to run

Current time

Start Time 2:00

Job Name

Backup Profile

No backup profiles exist. Please create a backup profile first.

Comment

Email Status To

Not available. You must set up your mail relay host.

Save Cancel

① GUI上部 System配下の Tools ▶ Scheduling を選択

② New Taskより 実施したい項目を選択

③ どの項目においても Job Name/ Onceまたは Recurring およびスケジューリングを設定

• Report - レポート生成

Appendix 1.  
Firepower 4100/2100 の  
インストールと初期設定

# FP4100/2100 のインストールと初期設定

- FTDv (および FTD on ASA5500-X) と FP4100/2100 はアーキテクチャが異なる
- この章では FTDv の代わりに FP4120 や FP2120 を使った場合について、1章を補足する
- FP4100/2100 を FTD として動作させる初期設定後は、FTDv と同じように FMC にレジストし、管理することが可能

# Firepower 4100 シリーズ (FP4100) - ハードウェア

## 統合セキュリティプラットフォーム

- ASA ソフトウェアと FTD ソフトウェアをサポート。どちらか1つ選択
- Smart NIC による 低レンシ処理対応 (オフロード機能\*)
- 冗長電源に対応し、Hot-swap 対応
- FAN は 6つ搭載され、Hot-swap 対応

\* IPv4の単純なTCP/UDP/GRE通信の超高速転送  
遅延やパフォーマンスに敏感な通信向け  
通常のFirewall通信処理と組み合わせて利用可能

1RU



シリアルコンソールポート

FXOSの管理インターフェイス用ポート

## ネットワーク モジュール

- 2つ搭載可能。Hot-swap 非対応
- FP9300 と互換性のある 10G/40G モジュールを利用可能
- ハードウェアバイパス機能\*\*を持つモジュールを利用可能

## データ インターフェイス

- 固定の SFP+ (1G/10G) ポート x 8

# Firepower 2100 シリーズ (FP2100) - ハードウェア

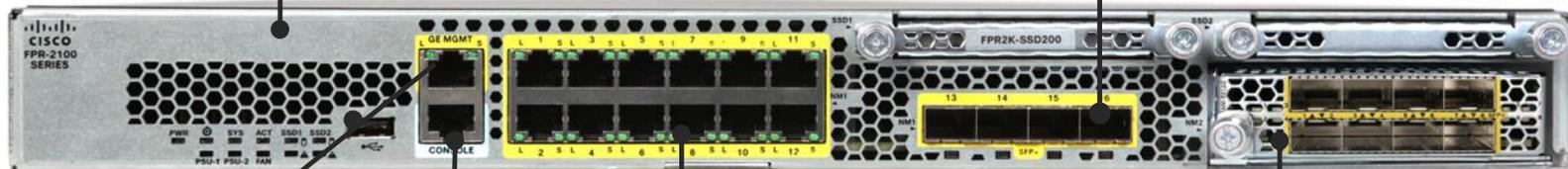
## 統合セキュリティプラットフォーム

- ASA ソフトウェアと FTD ソフトウェアをサポート。どちらか1つ選択
- NPU による L2-L4 高速処理に対応
- FP2110/2120 は固定 AC 電源 1つ、固定 FAN 4つ
- FP2130/2140 は冗長電源に対応、FAN 4つ搭載、各 Hot-swap 対応

## SFP/SFP+ データ インターフェイス

- FP2110/2120 は 固定の SFP (1G) ポート x 4
- FP2130/2140 は 固定の SFP+ (1G/10G) ポート x 4

1RU



FXOSの管理インターフェイス兼  
アプリケーション (ASA or FTD)  
管理用ポート

シリアルコンソールポート

## ネットワーク モジュール

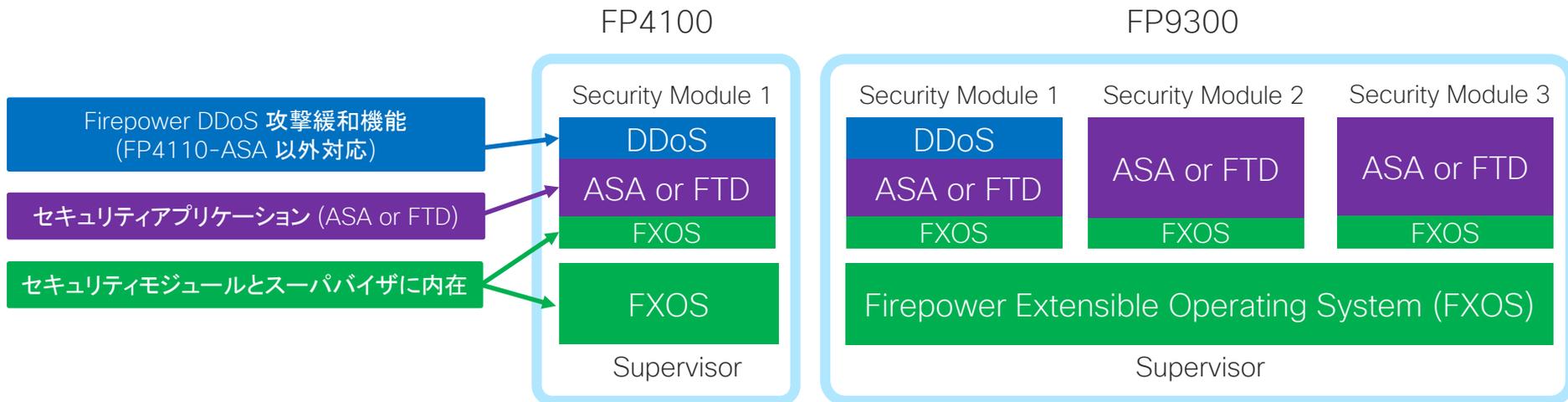
- FP2130/2140 のみ 1つ搭載可能。Hot-swap 非対応
- SFP+ (1G/10G) 対応のネットワークモジュールを利用可能

## データ インターフェイス

- 固定の RJ-45 (10M/100M/1G) ポート x 12

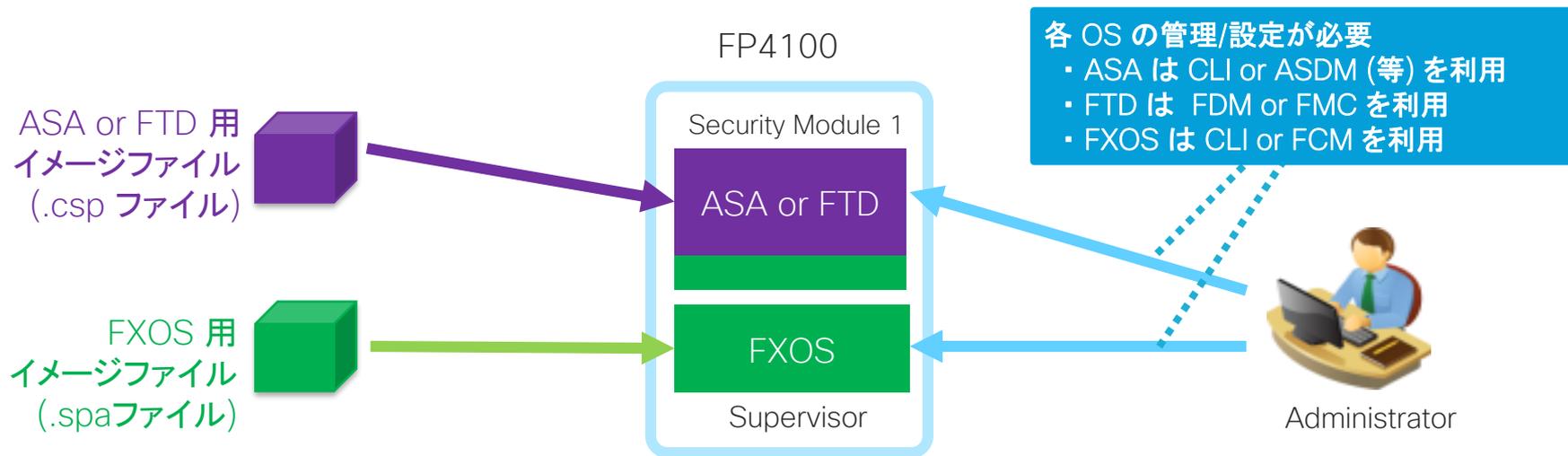
# FP4100/9300 と FXOS

- FP4100/9300 内には Firepower eXtensible Operating System (FXOS) が動作
  - FXOS が、スーパーバイザや セキュリティモジュールを管理
  - FXOS が、シャーシや ネットワークモジュール、電源、FAN などハードウェアの管理
  - FXOS が、セキュリティモジュールに物理インターフェイス割当て



# FP4100/9300 と FXOS (続き)

- FP4100/9300 は**プラットフォーム型**で、シャーシ内に複数 OS が動作可能
  - FXOS と ASA/FTD は、**各独立した OS** であり、イメージファイルや設定ファイルが異なる
  - FXOS と ASA/FTD の各アップグレードは、別々に実施が必要
  - FXOS と ASA/FTD は、各独立した管理インターフェイスと管理 IP アドレス, GUI, Syslog, SNMP Agent をもつ



# Firepower Chassis Manager (FCM)

FXOS の設定を簡単に GUI で提供

Web ブラウザで FXOS の管理 IP アドレスにアクセスすることで利用可能

日本語対応 (Web ブラウザの言語設定に依存)

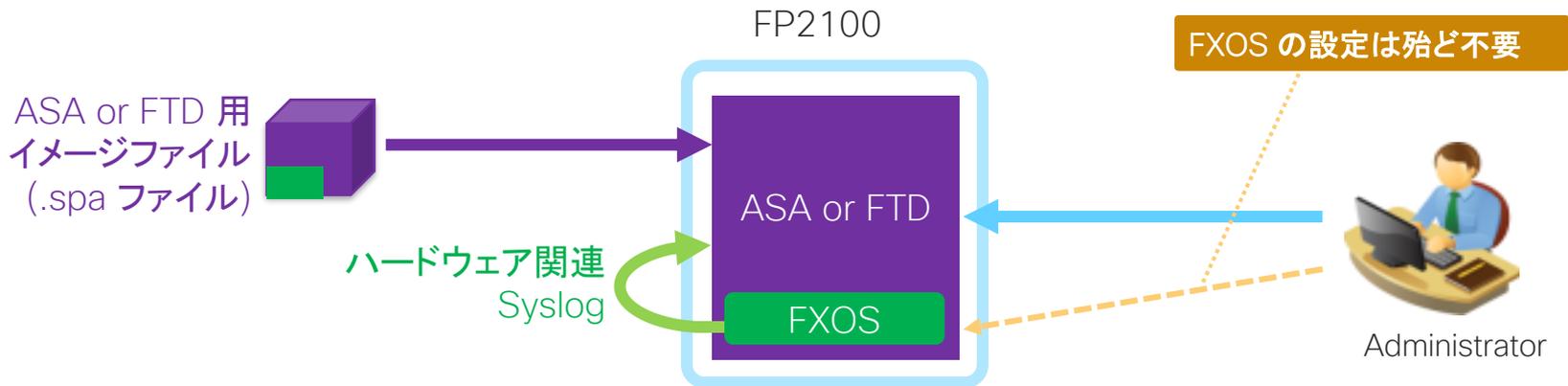
The screenshot displays the Firepower Chassis Manager (FCM) interface for a Cisco Firepower 4120 Security Appliance. The interface is in Japanese and shows several configuration panels:

- 概要 (Summary):** Displays the device name (FP4120-beta-1), IP address (10.71.153.63), and model (Cisco Firepower 4120 Security Appliance).
- インターフェイス (Interfaces):** Lists all interfaces and their types. For example, Ethernet1/1 through Ethernet1/8 are listed as 'data' type, while Port-channel48 is a 'cluster'.
- プロビジョニング (Provisioning):** Shows the current configuration for the device, including the application (FTD) and version (6.2.3.83).
- 利用可能なアップデート (Available Updates):** A table listing available updates for the device.

イメージ名	タイプ	バージョン	ステータス	ビルドの日付	画像の整合性
fxos-k9.2.0.1.141.SPA	platform-bundle	2.0(1.141)	未インストール	02/17/2017	Unknown
fxos-k9.2.3.1.88.SPA	platform-bundle	2.3(1.88)	インストール済み	06/07/2018	✓ 検証済み - Wed 4 July 2018, 05:1...
fxos-k9.2.3.1.66.SPA	platform-bundle	2.3(1.66)	未インストール	02/28/2018	✓ 検証済み - Thu 15 Mar 2018, 12:4...
fxos-k9.2.1.1.64.SPA	platform-bundle	2.1(1.64)	未インストール	12/16/2016	Unknown
fxos-k9.2.3.1.75.SPA	platform-bundle	2.3(1.75)	未インストール	04/27/2018	✓ 検証済み - Mon 18 June 2018, 07:...
fxos-k9.2.3.1.73.SPA	platform-bundle	2.3(1.73)	未インストール	03/13/2018	✓ 検証済み - Thu 29 Mar 2018, 03:3...
fxos-k9.2.2.1.63.SPA	platform-bundle	2.2(1.63)	未インストール	05/08/2017	Unknown
fxos-k9.2.1.1.73.SPA	platform-bundle	2.1(1.73)	未インストール	02/28/2017	Unknown
fxos-k9.1.1.4.95.SPA	platform-bundle	1.1(4.95)	未インストール	03/24/2016	Unknown
cisco-ftd.6.0.1.1213.csp	ftd	6.0.1.1213	未インストール	03/19/2016	✓
cisco-ftd.6.2.0.362.csp	ftd	6.2.0.362	未インストール	01/20/2017	✓
cisco-ftd.6.2.3.79.csp	ftd	6.2.3.79	未インストール	03/26/2018	Verified - Fri 30 Mar 2018, 09:09 AM
cisco-asa.9.8.2.24.csp	asa	9.8.2.24	未インストール	03/01/2018	Verified - Thu 15 Mar 2018, 01:14 AM
cisco-ftd.6.2.3.83.csp	ftd	6.2.3.83	インストール済み	04/01/2018	Verified - Mon 2 Apr 2018, 11:44 AM
cisco-asa.9.6.1.3.csp	asa	9.6.1.3	未インストール	05/05/2016	✓

# FP2100 と FXOS

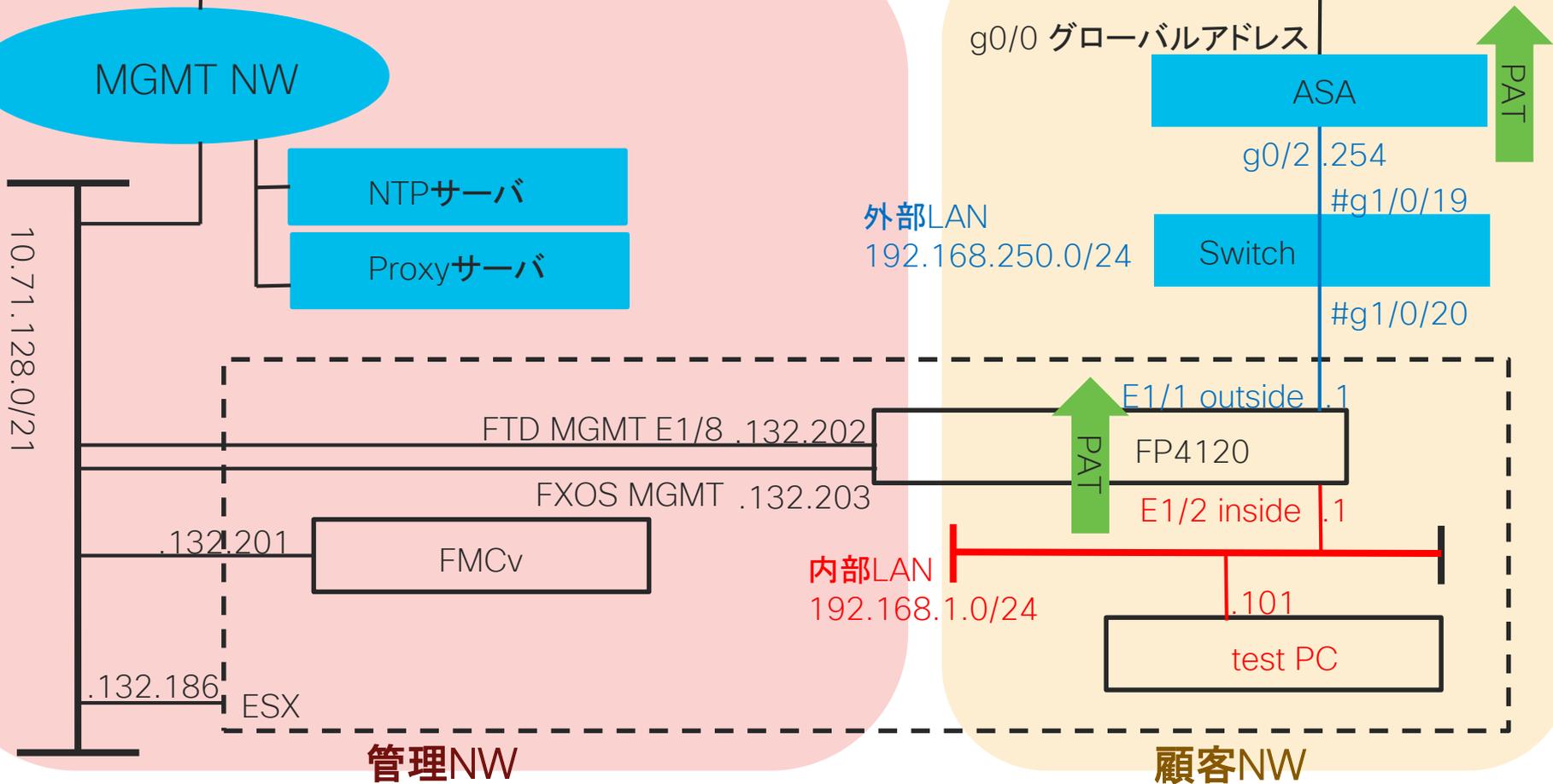
- FP2100 は**アプライアンス型**で、FXOS と ASA/FTD の統合が進んだモデル
  - FXOS 関連のソフトウェアが、ASA/FTD のパッケージ内に同梱 (=シングルイメージ)
  - FXOS と ASA/FTD で、共通の管理インターフェイスを利用、ハードウェア関連 Syslog は ASA/FTD 側へ出力
  - ASA の場合、FXOS 設定は必要最小限 (管理 IP アドレスや物理インターフェイス割当て、NTP 設定など)
  - FTD の場合、FXOS 設定不可



Appendix 1-1  
Firepower 4100 の  
インストールと初期設定

# FTDv の代わりに FP4120 を利用した例

■ 設定済みの機器



# ステップ 1-1: FP4120 の初期化

シリアルコンソール経由で FP4120 に接続し、CLI にて初期化を行う

```
Cisco FPR Series Security Appliance
```

```
fxos-1-A login: admin
```

```
Password: Admin123 (デフォルトパスワードの場合)
```

```
Successful login attempts for user 'admin' : 1Last login: Fri Sep 21 13:43:05 JST 2018 on ttyS0
```

```
Cisco Firepower Extensible Operating System (FX-OS) Software
```

```
TAC support: http://www.cisco.com/tac
```

```
Copyright (c) 2009-2018, Cisco Systems, Inc. All rights reserved.
```

```
[SNIP]
```

```
fxos-1-A# connect local-mgmt
```

```
xos-1-A(local-mgmt)# erase configuration
```

```
All configurations will be erased and system will reboot. Are you sure? (yes/no):yes
```

```
Removing all the configuration. Please wait....
```

```
[SNIP]
```

# ステップ 2-1: FP4120 の FXOS 初期セットアップ

FP4120 が起動してきたら、以下のように対話式にセットアップを行う

FP4100 シリーズは、FXOS 用の管理 IP アドレスと FTD 用の管理 IP アドレスがそれぞれ必要なことに注意

You have chosen to setup a new Security Appliance. Continue? (y/n): y

Enforce strong password? (y/n) [y]: y (パスワードを強化しなくても (n を選択しても) よいが、強化した方がセキュリティレベルは上がる)

Enter the password for "admin": 新しいパスワード (パスワードを強化していない場合、デフォルトの Admin123 を再利用可能)

Confirm the password for "admin": 新しいパスワード

Enter the system name: FP4120-1 (任意のホスト名を設定)

Supervisor Mgmt IP address : 10.71.132.203 (FXOS の管理 IP アドレスを入力)

Supervisor Mgmt IPv4 netmask : 255.255.248.0

IPv4 address of the default gateway : 10.71.135.254

Do you want to configure IP block for ssh access? (yes/no) [y]: y (FXOS に SSH アクセス可能な範囲を指定)

SSH IP block address : 10.141.0.0 (今回は 10.141.0.0/24 とする)

SSH IPv4 block netmask : 255.255.0.0

## ステップ 2-2: FP4120 の FXOS 初期セットアップ

Do you want to configure IP block for https access? (yes/no) [y]: y (FXOS に https アクセス可能な範囲を指定)

HTTPS IP block address : 10.141.0.0 (今回は 10.141.0.0/24 とする)

HTTPS IPv4 block netmask : 255.255.0.0

Configure the DNS Server IP address? (yes/no) [n]: y (FXOS が利用する DNS サーバを指定)

DNS IP address : 64.104.14.184

Configure the default domain name? (yes/no) [n]: n (デフォルトドメイン名があれば y を選択し、入力)

Following configurations will be applied: 次の行以降に出てくる設定内容を確認

# ステップ 2-3: FP4120 の FXOS 初期セットアップ

```
Switch Fabric=A
System Name=FP4120-1
Enforced Strong Password=yes
Supervisor Mgmt IP Address=10.71.132.203
Supervisor Mgmt IP Netmask=255.255.248.0
Default Gateway=10.71.135.254
SSH Access Configured=yes
  SSH IP Address=10.141.0.0
  SSH IP Netmask=255.255.0.0
HTTPS Access Configured=yes
  HTTPS IP Address=10.141.0.0
  HTTPS IP Netmask=255.255.0.0
DNS Server=64.104.14.184
```

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): **yes** (設定内容に問題がなければ **yes** と入力。間違いがあれば **no** を入力し、最初からやり直す)

Applying configuration. Please wait.

Configuration file - Ok

/isan/bin/first-

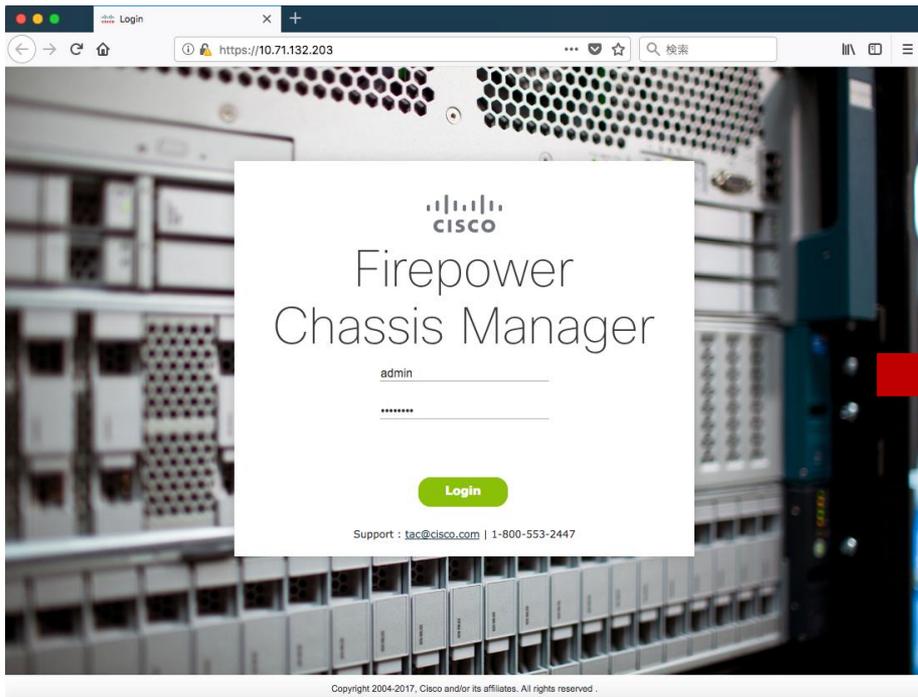
Cisco FPR Series Security Appliance

FP4120-1-A login:

# ステップ 3-1: FCM on FP4120 にログイン

Web ブラウザで FXOS の管理 IP アドレスに https でアクセスし、設定した admin のパスワードでログイン → FCM (Firepower Chassis Manager) にログイン

[TIPS] CLI で設定後、ログインできるようになるまで 4-5分の経過が必要



Overview Interfaces Logical Devices Security Engine Platform Settings System Tools Help admin

FP4120-1 10.71.132.203  
Model: Cisco Firepower 4120 Security Appliance Version: 2.3(1.91) Operational State: Operable Chassis Uptime: 00:00:24:00

CONSOLE MGMT USB  
Power 1 Running Power 2 Removed

Network Module 1  
1 3 5 7  
2 4 6 8  
Network Module 2 : Empty  
Network Module 3 : Empty

FAULTS 0(0) CRITICAL 1(1) MAJOR INTERFACES 8 DOWN 0 UP DEVICES 0 DOWN 0 UP LICENSE Smart Agent UNREGISTERED INVENTORY 1 Security Engine 6 Fans

Severity	Description	Cause	Occurrence	Time
MAJOR	End User License Agreement not accepted for Application ftd.6.2.3.83	license-agreement-not-acc...	1	2018-09-27T06:07:27.591
MINOR	Config backup may be outdated	config-backup-outdated	1	2018-09-27T06:07:03.698
WARNING	Power supply 2 in chassis 1 presence: missing	equipment-missing	1	2018-09-27T06:08:27.829
CLEARED	default Keyring's certificate is invalid, reason: notYetValid.	invalid-keyring-certificate	1	2018-09-27T06:17:02.918
CLEARED	Platform version is empty in platform firmware package	default-platform-version-mi...	1	2018-09-27T06:08:32.936
CLEARED	MAC pool ssp-macpool-mio-external-ports is empty	empty-pool	1	2018-09-27T06:08:10.324
CLEARED	[FSM-STAGE:RETRY:]: Restoring Apps in progress(FSM-STAGE:sam:dme:SmSec...	restore-failed	1	2018-09-27T06:07:38.250
CLEARED	Service profile ssp-sprof-1 configuration failed due to insufficient-resources,mac...	configuration-failure	1	2018-09-27T06:08:10.324
CLEARED	Service profile ssp-sprof-1 is not associated	unassociated	1	2018-09-27T06:13:17.114
CLEARED	[FSM-STAGE:RETRY:]: external VM manager certficate configuration on local fabri...	set-local-failed	1	2018-09-27T06:07:42.928

1 Successful Login in last 24 hrs - View Details | Thu Sep 27 2018 at 06:18:47 from - 10.141.41.61

(注) FCM の言語は、Web ブラウザの言語設定に依存

# ステップ 4-1: FCM on FP4120 の初期設定

Platform Settings → NTP → Use NTP Server にて NTP サーバを追加し、save する

Overview Interfaces Logical Devices Security Engine Platform Settings System Tools Help ad

Time Synchronization Current Time

**Set Time Source**

Set Time Manually

Date: 09/27/2018 (mm/dd/yyyy)

Time: 3 22 PM (hh:mm)

Get System Time

NTP Server Authentication:  Enable

Use NTP Server

**Add NTP Server**

NTP Server \* ntp.esl.cisco.com

Authentication Key

Authentication Value

Add Cancel

Use same settings on Firepower Management Center managing this application in case you are running a

Save Cancel

Overview Interfaces Logical Devices Security Engine Platform Settings System Tools Help ad

Time Synchronization Current Time

**Set Time Source**

Set Time Manually

Date: 09/27/2018 (mm/dd/yyyy)

Time: 3 22 PM (hh:mm)

Get System Time

NTP Server Authentication:  Enable

Use NTP Server

**NTP Server**

NTP Server	Server Status	Actions
ntp.esl.cisco.com	Not-available	

Use same settings on Firepower Management Center managing this application in case you are running a Firepower Threat Defense Device.

Save Cancel

NTP サーバとの時刻同期が始まると、強制的に FCM からログアウトされるので、再度 admin でログインする

# ステップ 4-2: FCM on FP4120 の初期設定

Overview Interfaces Logical Devices Security Engine **Platform Settings**

► **NTP**

- SSH
- SNMP
- HTTPS
- AAA
- Syslog
- DNS
- FIPS and Common Criteria
- Access List

Time Synchronization **Current Time**

**Current Time**

Device Date: 09/27/2018

Device Time: 6:37:16 AM

Time Zone:

NTP Status:

Asia/Tokyo  
Asia/Tehran  
Asia/Tel\_Aviv  
Asia/Thimbu  
Asia/Thimphu  
Asia/Tokyo  
Asia/Ujung\_Pandang  
Asia/Ulaanbaatar  
Asia/Ulan\_Bator  
Asia/Urumqi  
Asia/Ust-Nera  
Asia/Vientiane  
Asia/Vladivostok  
Asia/Yakutsk

Platform Settings → NTP → Current Time から、適切な都市 (日本では Asia/Tokyo) を選択し、Save する

Overview Interfaces Logical Devices Security Engine **Platform Settings**

► **NTP**

- SSH
- SNMP
- HTTPS
- AAA
- Syslog
- DNS
- FIPS and Common Criteria
- Access List

Time Synchronization **Current Time**

**Current Time**

Device Date: 09/27/2018

Device Time: 6:38:04 AM

Time Zone:

NTP Status: Synchronized

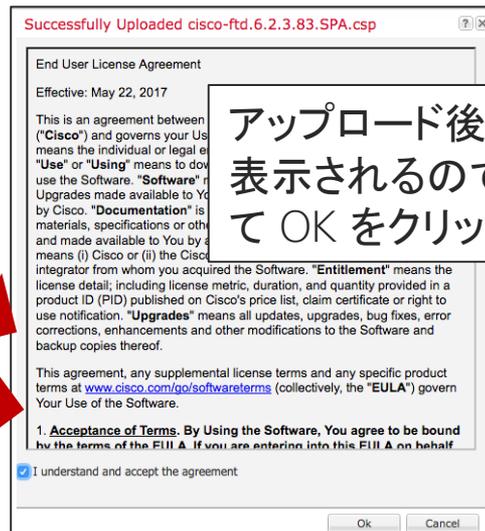
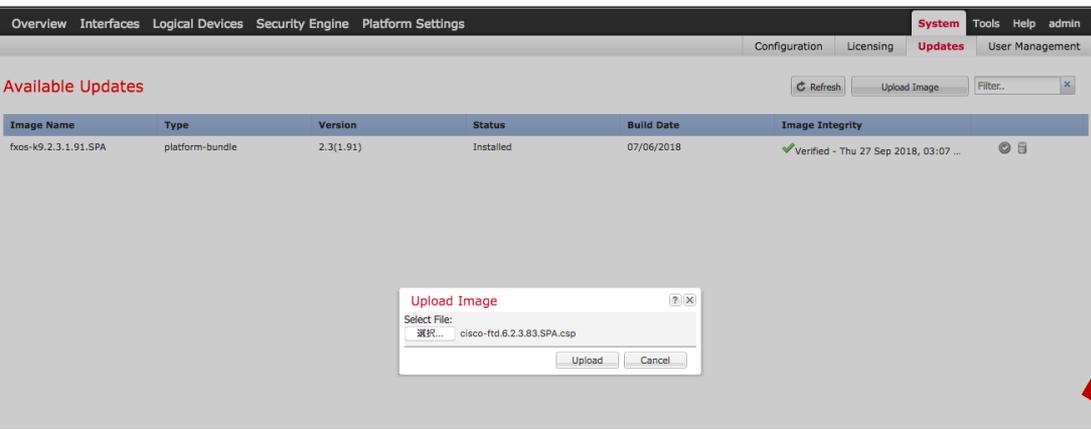
# ステップ 4-3: FCM on FP4120 の初期設定

以下のサイトから、FTD 6.2.3 のインストールパッケージ (.csp ファイル) をダウンロードしておくこと  
<https://software.cisco.com/download/home/286306168/type/286306337/release/6.2.3>

Firepower Threat Defense install package  
**cisco-ftd.6.2.3.83.SPA.csp**

(注)ソフトウェアバージョンはそのときに適切なものを選択する

System → Updates → Upload Image にて、FTD のインストールパッケージをアップロード



アップロード後、EULA が表示されるので、同意して OK をクリック



# ステップ 5-1: FP4120 の Interface 設定

Interface から、FTD 用の MGMT Interface を選択 (この例では E1/8)  
鉛筆マーク (edit) をクリックし、Enable にして速度等を合わせ、Type を “mgmt” に設定

The screenshot displays the network configuration interface for a device. The top navigation bar includes 'Overview', 'Interfaces', 'Logical Devices', 'Security Engine', and 'Platform Settings'. The main area shows a diagram of 'Network Module 1' with ports 1 through 8, and 'Network Module 2' and 'Network Module 3' which are empty. Below the diagram is a table of interfaces. The 'Edit Interface - Ethernet1/8' dialog box is open, showing the following configuration:

- Name: Ethernet1/8
- Enable:
- Type: mgmt
- Admin Speed: 1gbps
- Auto Negotiation:  Yes  No
- Admin Duplex: Full Duplex

The background table lists the following interfaces:

Interface	Type	Admin Speed	Operational	Auto Negotiation	Operation State	Admin State
MGMT	Management					<input checked="" type="checkbox"/>
Port-channel48	cluster	10gbps	indeterminate		failed	<input type="checkbox"/>
Ethernet1/1	data	10gbps	10gbps		admin-down	<input type="checkbox"/>
Ethernet1/2	data	10gbps	10gbps		admin-down	<input type="checkbox"/>
Ethernet1/3	data	10gbps	10gbps		sfp-not-present	<input type="checkbox"/>
Ethernet1/4	data	10gbps	10gbps	Full Duplex	sfp-not-present	<input type="checkbox"/>
Ethernet1/5	data	10gbps	10gbps	Full Duplex	sfp-not-present	<input type="checkbox"/>
Ethernet1/6	data	10gbps	10gbps	Full Duplex	sfp-not-present	<input type="checkbox"/>
Ethernet1/7	data	10gbps	10gbps	Full Duplex	sfp-not-present	<input type="checkbox"/>
Ethernet1/8	data	10gbps	10gbps	Full Duplex	admin-down	<input type="checkbox"/>

# ステップ 5-2: FP4120 の Interface 設定

同様にデータ用 Interface (この例では E1/1 と E1/2) を Type = data で設定

**Edit Interface - Ethernet1/1**

Name: Ethernet1/1  Enable

Type: data

Admin Speed: 1gbps

Auto Negotiation:  Yes  No

Admin Duplex: Full Duplex

OK Cancel

**Edit Interface - Ethernet1/2**

Name: Ethernet1/2  Enable

Type: data

Admin Speed: 1gbps

Auto Negotiation:  Yes  No

Admin Duplex: Full Duplex

OK Cancel

Overview **Interfaces** Logical Devices Security Engine Platform Settings System Tools Help admin

Network Module 1: 1, 2, 3, 4, 5, 6, 7, 8 (CONSOLE, MGMT, USB)

Network Module 2: Empty

Network Module 3: Empty

All Interfaces Hardware Bypass

Interface	Type	Admin Speed	Operational Speed	Application	Admin Duplex	Auto Negotiation	Operation State	Admin State
MGMT	Management							<input checked="" type="checkbox"/>
Port-channel48	cluster	10gbps	indeterminate		Full Duplex	no	failed	<input type="checkbox"/>
Ethernet1/1	data	1gbps	1gbps		Full Duplex	no	up	<input checked="" type="checkbox"/>
Ethernet1/2	data	1gbps	1gbps		Full Duplex	no	up	<input checked="" type="checkbox"/>
Ethernet1/3	data	10gbps	10gbps		Full Duplex	no	sfp-not-present	<input type="checkbox"/>
Ethernet1/4	data	10gbps	10gbps		Full Duplex	no	sfp-not-present	<input type="checkbox"/>
Ethernet1/5	data	10gbps	10gbps		Full Duplex	no	sfp-not-present	<input type="checkbox"/>
Ethernet1/6	data	10gbps	10gbps		Full Duplex	no	sfp-not-present	<input type="checkbox"/>
Ethernet1/7	data	10gbps	10gbps		Full Duplex	no	sfp-not-present	<input type="checkbox"/>
Ethernet1/8	mgmt	1gbps	1gbps		Full Duplex	no	up	<input checked="" type="checkbox"/>

配線済みであれば、link がこの時点で up する

# ステップ 6-1: FTD を FP4120 にインストール

Logical Devices → Add Device より、論理デバイスとして FTD を選択する

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Refresh Add Device

Logical Device List

No logical devices available. Click on Add Device to add a new logical device.

**Add Device**

Device Name: FTD4120-1 任意の名称

Template: Cisco Firepower Threat Defense

Image Version: 6.2.3.83 FXOS バージョンと互換性がある FTD バージョンがリストアップ 今回は 6.2.3.83 のみが upload されているのでこれを選択

Device Mode:  Standalone  Cluster 通常は Standalone を選択

OK Cancel

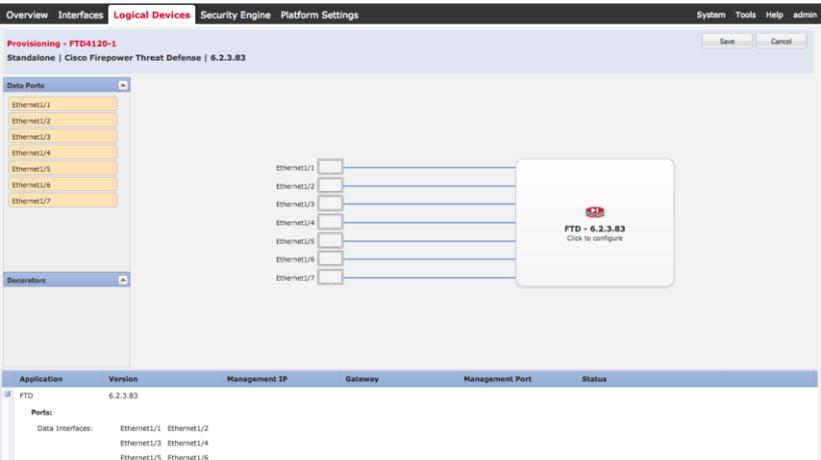
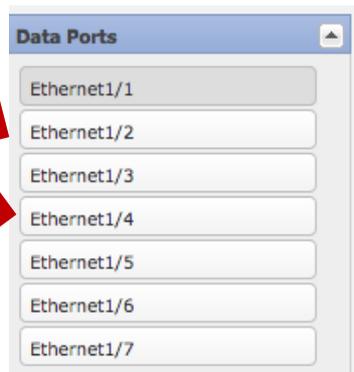
FXOS に upload 済みの Application (FTD or ASA) が選択可能  
今回は Cisco Firepower Threat Defense (FTD) を選択

# ステップ 6-2: FTD を FP4120 にインストール



OK をクリックすると左図のように論理デバイスとしての FTD が表示される

FTD のデータ用としてインストールするインターフェイスをクリック。



今回は E1/1 と E1/2 を追加する。  
ただし、FP4100 は、論理デバイスが1台なので、余っているインターフェイスすべてを追加する方が良い

# ステップ 6-3: FTD を FP4120 にインストール

FTD のボックスをクリックし、詳細設定を行う



Cisco Firepower Threat Defense - Bootstrap Configuration

General Information Settings Agreement

Interface Information

Management Interface:

Management

Address Type:

IPv4

Management IP:

Network Mask:

Network Gateway:

OK Cancel

FTD の管理 Interface を選択 (この例では E1/8)  
FCM の Interface 設定で type = mgmt にしたものが表示される  
その他、FTD の管理 IP アドレスを設定

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information Settings Agreement

Registration Key:

Confirm Registration Key:

Password:

Confirm Password:

Firepower Management Center IP:

Search domains:

Firewall Mode:

DNS Servers:

Fully Qualified Hostname:

Eventing Interface:

OK Cancel

FMC へのレジストレーションキー

FTD への直接 login 時の admin パスワード

レジスト先の FMC の IP アドレス

FTD を Firewall として使う際の Mode を指定 (routed or transparent)

その他は option

# ステップ 6-4: FTD を FP4120 にインストール

EULA に同意し、OK をクリックすると以下ようになる

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information Settings **Agreement**

End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof.

This agreement, any supplemental license terms and any special product terms at [www.cisco.com/go/softwareterms](http://www.cisco.com/go/softwareterms) (collectively, the "EULA") govern Your Use of the Software.

1. **Acceptance of Terms.** By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on behalf of an entity, you represent that you have authority to bind

I understand and accept the agreement

OK Cancel

Overview Interfaces **Logical Devices** Security Engine Platform Settings

System Tools Help admin

Provisioning - FTD4120-1

Standalone | Cisco Firepower Threat Defense | 6.2.3.83

Data Ports

- Ethernet1/1
- Ethernet1/2
- Ethernet1/3
- Ethernet1/4
- Ethernet1/5
- Ethernet1/6
- Ethernet1/7

Decorators

Ethernet1/1 Ethernet1/2 Ethernet1/3 Ethernet1/4 Ethernet1/5 Ethernet1/6 Ethernet1/7

FTD - 6.2.3.83  
Ethernet1/8  
Click to configure

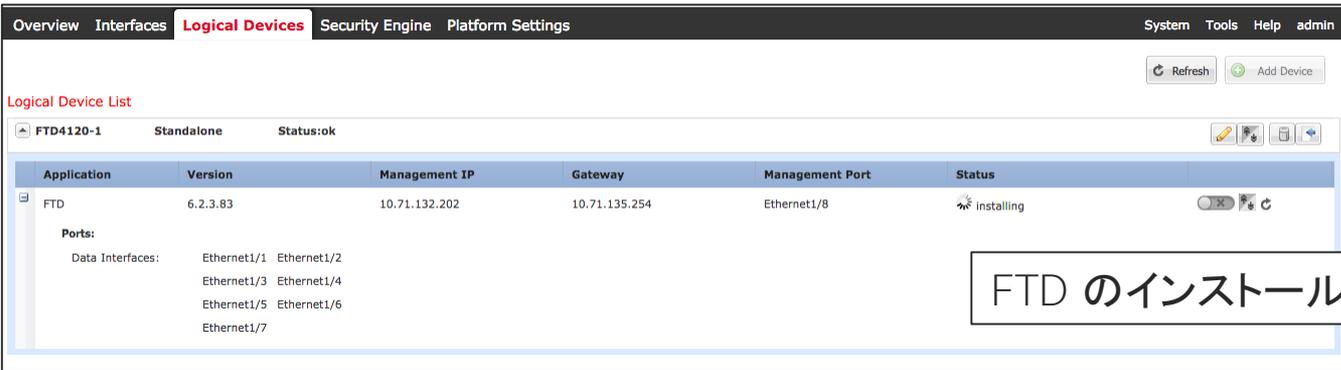
Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.2.3.83	10.71.132.202	10.71.135.254	Ethernet1/8	
<b>Ports:</b>					
Data Interfaces:	Ethernet1/1	Ethernet1/2			
	Ethernet1/3	Ethernet1/4			
	Ethernet1/5	Ethernet1/6			

4 Successful Login in last 24 hrs - [View Details](#) | Thu Sep 27 2018 at 15:37:03 from - 10.141.41.61

Save をクリックすると、  
論理デバイスとして  
FTD のインストールが  
始まる



# ステップ 6-5: FTD を FP4120 にインストール



Logical Device List

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.2.3.83	10.71.132.202	10.71.135.254	Ethernet1/8	installing

Ports:

Data Interfaces: Ethernet1/1 Ethernet1/2  
Ethernet1/3 Ethernet1/4  
Ethernet1/5 Ethernet1/6  
Ethernet1/7

FTD のインストールには 20-30分程度を要する

[TIPS] コンソールで

connect module 1 console

を実行すると、セキュリティエンジンのログの  
コンソールに移行、FTD ソフトウェアのイン  
ストールログがリアルタイムで表示される

```
FP4120-1-A# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Threat Defense System: CMD=-install, CSP-ID=cisco-ftd.6.2.3.83__ftd_001_JMX2214L
02Z6M7Z4V1, FLAG=''
Device type is FPR4K-SM-24. (76/E)
System begins installation ...
Setting up file system ...
Configuring user accounts ...
Installing OS supplemental packages ...
Installing OS supporting packages ...
Installing product rpms ...
Installing FSIC package ...
Deleting installation packages ...
Installing model pack ...
Running post install ...
Configuring model ...
```

# ステップ 6-6: FTD を FP4120 にインストール

FTD のインストールが終わると以下のように online となり、残りは第1章の FTDv と同じになる (FMC 側で FTD のレジストレーションを行い、設定を続ける)

The screenshot shows the Cisco FMC web interface. The 'Logical Devices' tab is selected. A table lists the logical device 'FTD4120-1' as 'Standalone' with a status of 'ok'. Below the table, the 'Ports' and 'Attributes' for the FTD application are displayed.

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.2.3.83	10.71.132.202	10.71.135.254	Ethernet1/8	online

**Ports:**

Data Interfaces:	Ethernet1/1	Ethernet1/2
	Ethernet1/3	Ethernet1/4
	Ethernet1/5	Ethernet1/6
	Ethernet1/7	

**Attributes:**

- Cluster Operational Status : not-applicable
- Firepower Management IP : 10.71.132.202
- Management URL : https://10.71.132.201/
- HA-ROLE : standalone
- UUID : 01a26d78-c22e-11e8-806b-ba813d5b9abb

[TIPS] CLI で、右図のように現在の階層が FTD ではなくセキュリティエンジンになっている場合、  
connect ftd  
で FTD の CLISH に移動  
~ quit  
で FXOS に移動できる

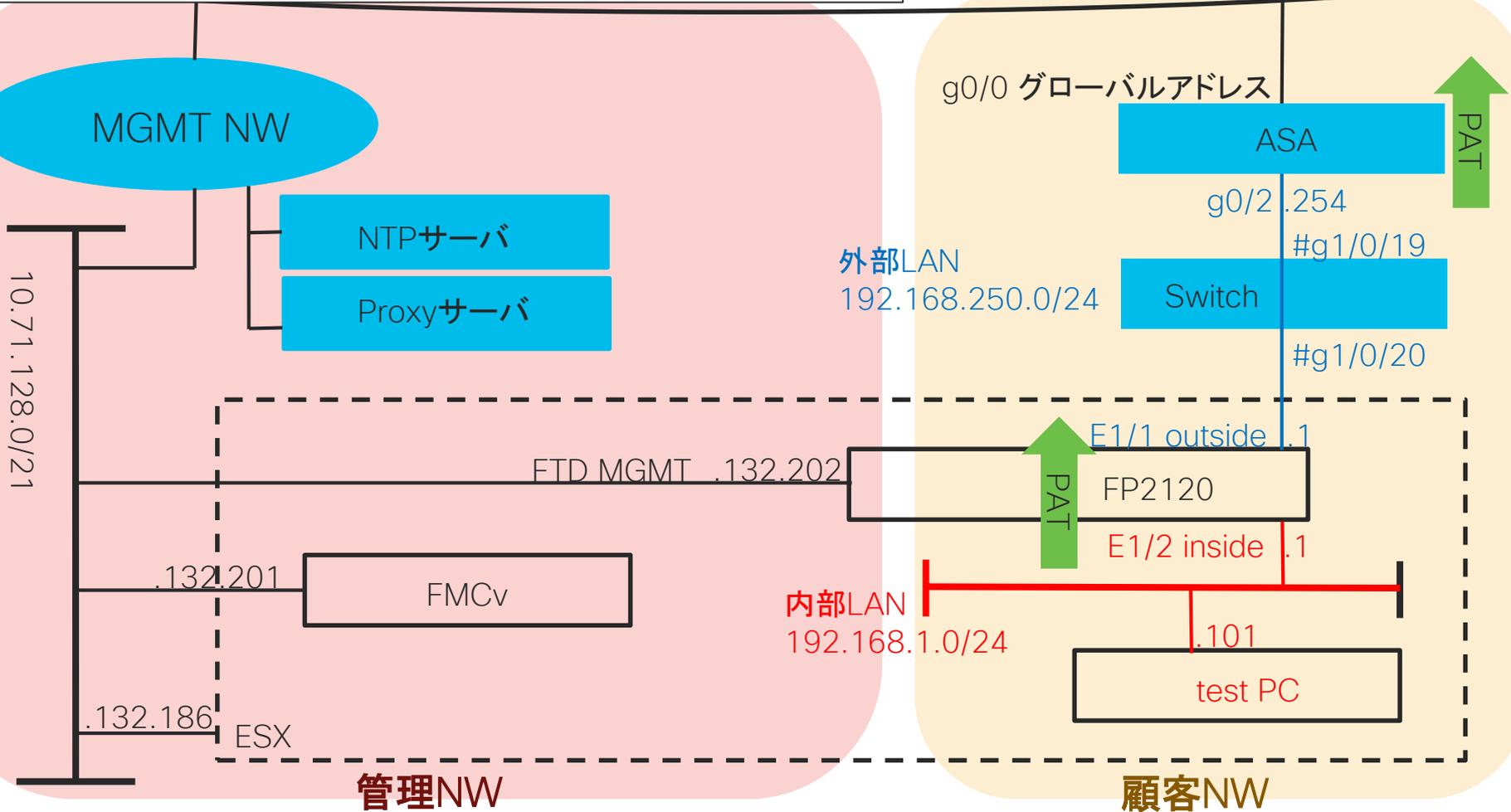
```
Firepower-module1>connect ftd (FTD CLISH に移動)
Connecting to ftd console... enter exit to return to bootCLI

> exit (セキュリティエンジンに移動)
Firepower-module1> ~ (チルダは見えない)
telnet> quit (FXOS に移動)
Connection closed.
FP4120-1-A#
```

Appendix 1-2  
Firepower 2100 の  
インストールと初期設定

# FTDv の代わりに FP2120 を利用した例

■ 設定済みの機器



# ステップ 1-1: FP2120 の初期化

シリアルコンソール経由で FP2120 に接続し、CLI にて初期化を行う  
FP2100 シリーズは、FP4100 と異なり、初期設定はすべて CLI

```
Cisco Firepower 2120 Threat Defense v6.2.3 (build 83)
```

```
firepower login: admin
```

```
Password: Admin123 (デフォルトパスワードの場合)
```

```
Last login: Thu Sep 27 08:48:32 UTC 2018 on ttyS0
```

```
Successful login attempts for user 'admin' : 2
```

```
Copyright 2004-2018, Cisco and/or its affiliates. All rights reserved.
```

```
Cisco is a registered trademark of Cisco Systems, Inc.
```

```
All other trademarks are property of their respective owners.
```

```
Cisco Fire Linux OS v6.2.3 (build 13)
```

```
Cisco Firepower 2120 Threat Defense v6.2.3 (build 83)
```

```
[SNIP]
```

```
firepower# connect local-mgmt
```

```
firepower(local-mgmt)# erase configuration
```

```
All configurations will be erased and system will reboot. Are you sure? (yes/no):yes
```

```
Removing all the configuration. Please wait....
```

```
[SNIP]
```

# ステップ 2-1: FP2120 の FTD 初期セットアップ

FP2120 が起動したら、以下のように対話式に FTD のセットアップを行う  
(FP2100 シリーズは FXOS の初期設定が不要)

```
Cisco Firepower 2120 Threat Defense v6.2.3 (build 83)
```

```
firepower login: admin
```

```
Password: Admin123 (デフォルトパスワード)
```

```
Successful login attempts for user 'admin' : 1
```

```
Copyright 2004-2018, Cisco and/or its affiliates. All rights reserved.
```

```
Cisco is a registered trademark of Cisco Systems, Inc.
```

```
All other trademarks are property of their respective owners.
```

```
Cisco Fire Linux OS v6.2.3 (build 13)
```

```
Cisco Firepower 2120 Threat Defense v6.2.3 (build 83)
```

```
[SNIP]
```

```
firepower# connect ? (connect の後に ? を入力し、以下を確認)
```

```
ftd      Connect to FTD Application CLI
```

```
local-mgmt Connect to Local Management CLI
```

ftd の代わりに asa と表示された場合 → ASA がインストールされているので FTD への reimage が必要  
ftd も asa も表示されない場合 → アプリケーションがまだ起動していないので待機

# ステップ 2-2: FP2120 の FTD 初期セットアップ

firepower# **connect ftd**

You must accept the EULA to continue.

Press <ENTER> to display the EULA: **(EULA への同意が必要)**

End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the

[SNIP]

This agreement, any supplemental license terms and any specific product terms at [www.cisco.com/go/softwareterms](http://www.cisco.com/go/softwareterms) (collectively, the "EULA") govern Your Use of the Software.

Please enter 'YES' or press <ENTER> to AGREE to the EULA: **(EULA に同意であれば enter キーを押す)**

System initialization in progress. Please stand by.

You must change the password for 'admin' to continue.

Enter new password: **新しいパスワード**

Confirm new password: **新しいパスワード**

# ステップ 2-3: FP2120 の FTD 初期セットアップ

You must configure the network to continue.

You must configure at least one of IPv4 or IPv6.

Do you want to configure IPv4? (y/n) [y]: y

Do you want to configure IPv6? (y/n) [n]: n (この例では IPv4 のみで管理)

Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: (FTD の管理 IP アドレスを手動設定するので Enter キーを押す)

Enter an IPv4 address for the management interface [192.168.45.45]: 10.71.132.202 (FTD の管理 IP アドレス)

Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.248.0

Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.71.135.254

Enter a fully qualified hostname for this system [firepower]: FTD2120-1 (任意のホスト名を設定)

Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]: 64.104.14.184 (DNS サーバが準備できない場合に備えて、デフォルトでは Umbrella の DNS サーバが使えるようになっているが、今回は手動で指定)

Enter a comma-separated list of search domains or 'none' []: (デフォルトドメインがあれば入力、今回は無し)

If your networking information has changed, you will need to reconnect.

(以下の内容で管理 IP アドレスが設定される)

Setting DNS servers: 64.104.14.184

No domain name specified to configure.

Setting hostname as FTD2120-1

DHCP Server Disabled

Setting static IPv4: 10.71.132.202 netmask: 255.255.248.0 gateway: 10.71.135.254 on management0

Updating routing tables, please wait...

All configurations applied to the system. Took 6 Seconds.

Saving a copy of running network configuration to local disk.

For HTTP Proxy configuration, run 'configure network http-proxy'

# ステップ 2-4: FP2120 の FTD 初期セットアップ

```
Manage the device locally? (yes/no) [yes]: no (今回は FMC 管理なので no を入力。FDM 管理であれば yes)
DHCP Server Disabled ([TIPS] ここで1分くらい待つ)
Configure firewall mode? (routed/transparent) [routed]: (今回は Routed Firewall なのでデフォルトの routed を選択 (enter
キーを押す))
Configuring firewall mode ... ([TIPS] ここで2分くらい待つ)
```

[SNIP]

When registering the sensor to a Firepower Management Center, a unique alphanumeric registration key is always required. In most cases, to register a sensor to a Firepower Management Center, you must provide the hostname or the IP address along with the registration key.

```
'configure manager add [hostname | ip address ] [registration key ]'
```

However, if the sensor and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key.

```
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.

>

# ステップ 3-1: FTD on FP2120 での FMC 指定

```
> configure manager add 10.71.132.201 cisco (手動でレジスト先の FMC を指定、レジストキーは今回は cisco  
とする)
```

```
([TIPS] ここで場合によっては30秒くらい待つ)
```

```
Manager successfully configured.
```

```
Please make note of reg_key as this will be required while adding Device in FMC.
```

```
> show managers (レジスト先の FMC を指定できたことを確認)
```

```
Host : 10.71.132.201
```

```
Registration Key : ****
```

```
Registration : pending
```

```
RPC Status :
```

```
>
```

FTD の初期設定が終わると以上のようになり、残りは第1章の FTDv と同じになる (FMC 側で FTD のレジストレーションを行い、設定を続ける)

# 参考情報

- Firepower Threat Defenseへのcisco.comでのショートカット  
<http://www.cisco.com/go/ngfw>
- Firepowerへのcisco.comでのショートカット  
<http://www.cisco.com/go/ips>
- シスコサポートコミュニティ 日本語 セキュリティ  
<https://supportforums.cisco.com/t5/-/ct-p/5041-security>

