Firepower Threat Defense
初期セットアップガイド
Rev 1.4

2018/09

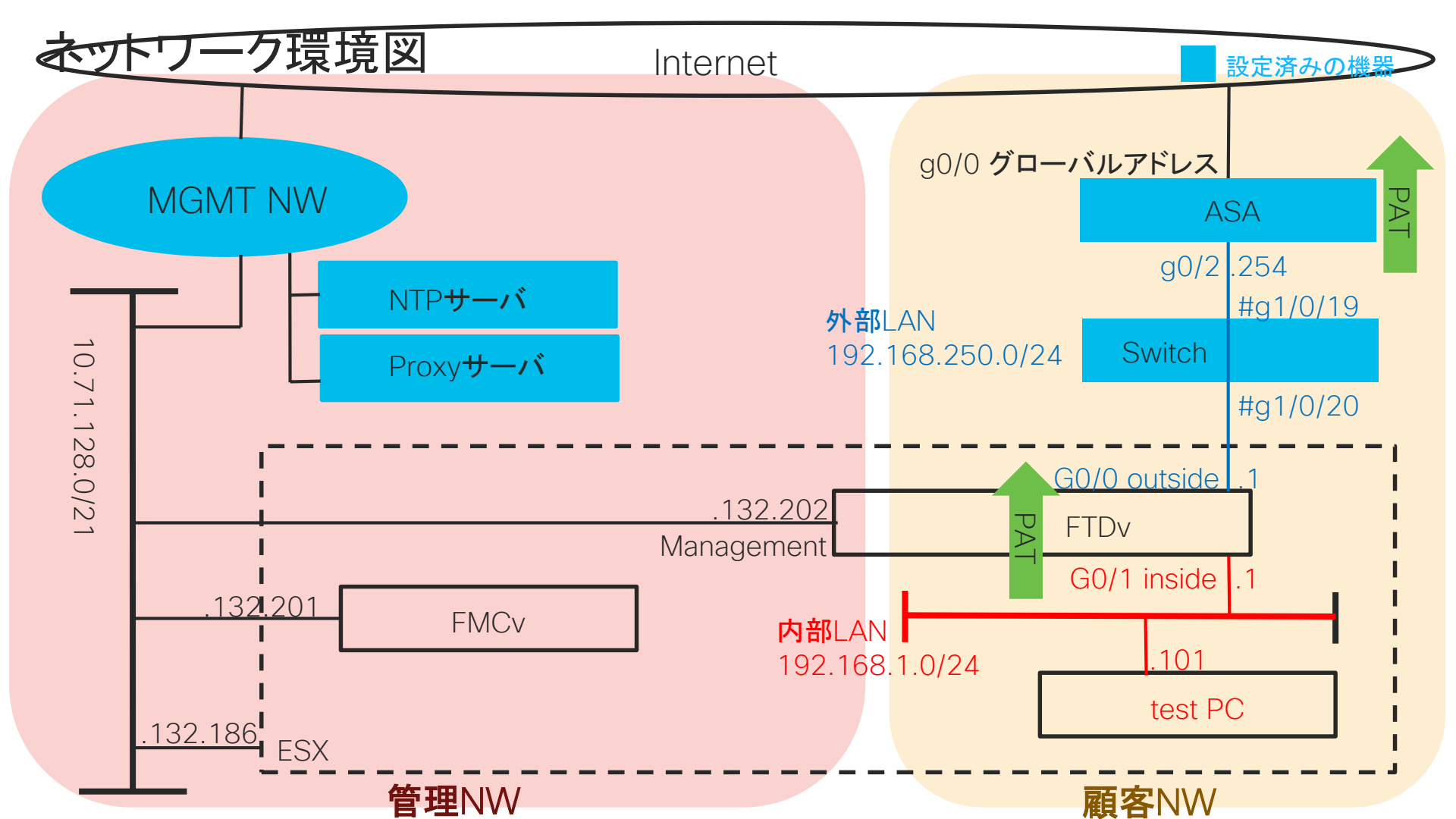
シスコシステムズ合同会社

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
MGMT NW
NTPサーバ
Proxyサーバ
10.71.128.0/21
g0/0 グローバルアドレス
ASA
PAT
g0/2 .254
#g1/0/19
外部LAN
192.168.250.0/24
Switch
#g1/0/20
G0/0 outside .1
.132.202
Management
PAT
FTDv
G0/1 inside .1
.132.201
FMCv
内部LAN
192.168.1.0/24
.101
test PC
.132.186
ESX
管理NW
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
   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

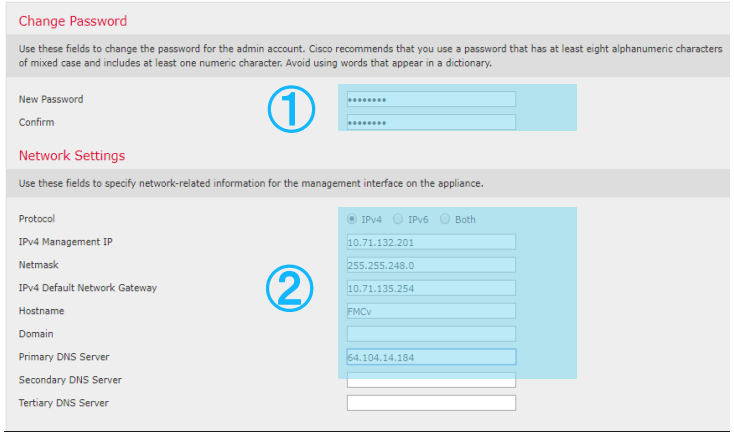
```
admin@fmc:~$ sudo su
Last login: Sat Jul 14 11:15:37 UTC 2018 on tty1
root@fmc:/Volume/home/admin# configure-network _
```

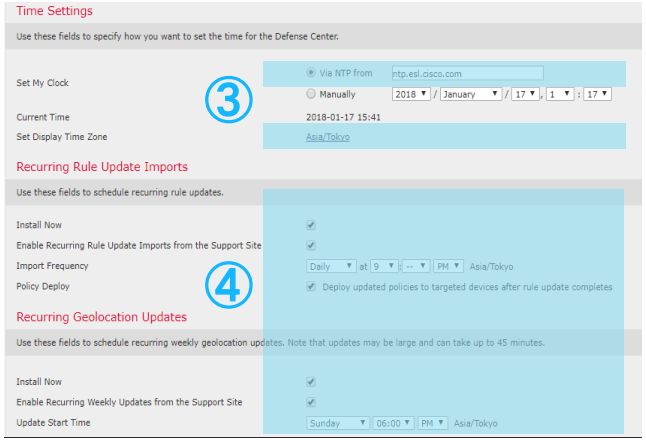
4. （CLIでアドレス変更しない場合）**ブラウザで FMCデフォルトIPアドレスにHTTPSアクセス**
   https://192.168.45.45/
   ユーザ名： admin
   パスワード： Admin123

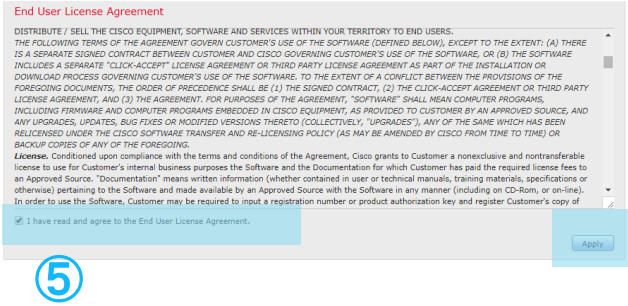
※ ブラウザアクセスする端末の IP アドレスは、192.168.45.2/24 など同一サブネットを使用

ステップ 2-1:初期設定

Firepower Management Center







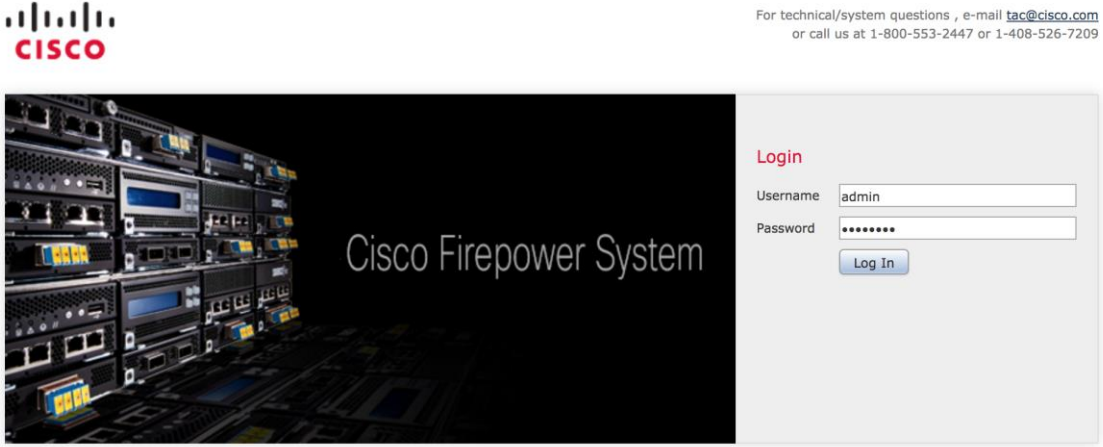
① adminパスワードの変更
② FMCのIPアドレス、デフォルトゲートウェイ、ホスト名、DNSサーバを入力
③ NTPサーバのIPアドレスまたはFQDNを入力、Time Zoneの変更
④ 更新内容の設定を画面のように入力
⑤ 最後にライセンス契約(EULA)にチェックを入れ “Apply”を選択

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

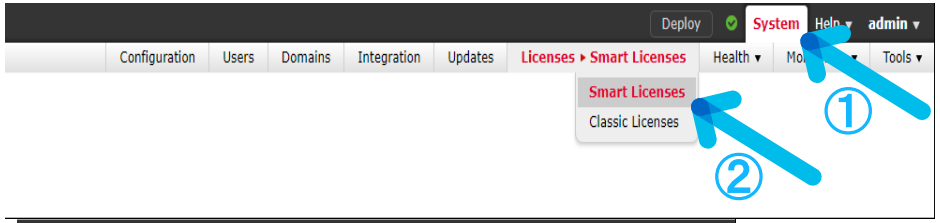
- **初期設定で入力した IP アドレスと adminパスワードを使い FMCの Web GUI へブラウザでHTTPSアクセスしログイン**

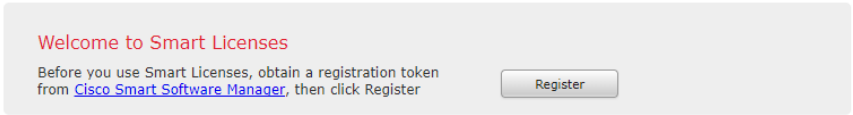
※ プラウザアクセスする端末の IP アドレスは、
初期設定で変更した FMCのIPアドレスを同一セグメントのIPアドレスを使用
(ステップ1で 192.168.45.2に変更いただいているため、ここでは注意)

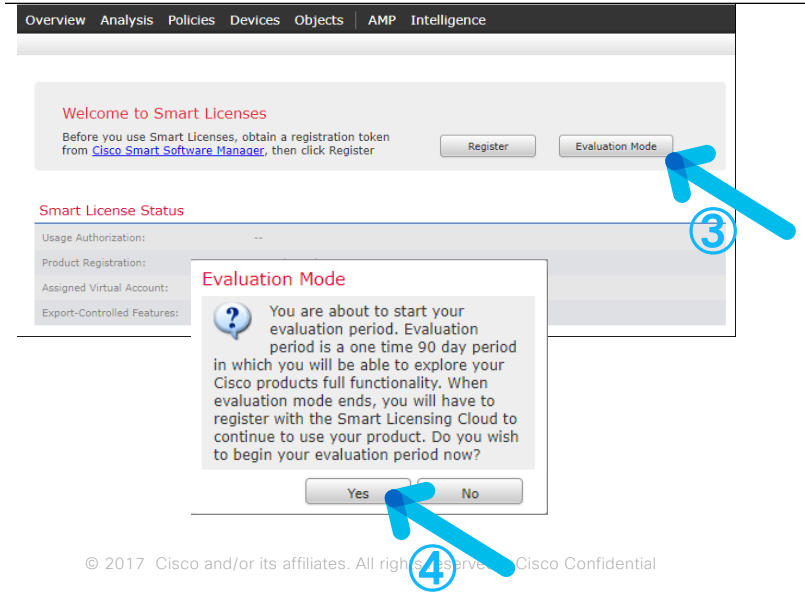


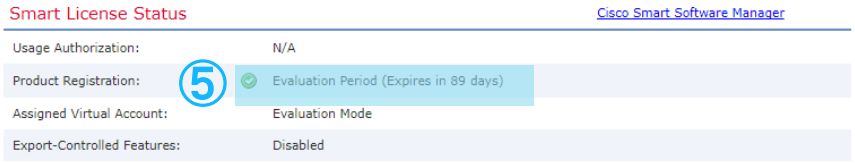
ステップ 3: ライセンスの追加

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





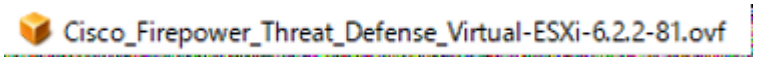




① GUI の上部にある System を選択
② Licenses>Smart Licensesを選択
③ Evaluation Modeを選択
④ Yesを選択
⑤ 上記のようになれば、ライセンスが適用されたことになる

ステップ 1: OVFのデプロイ

1. **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

   (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

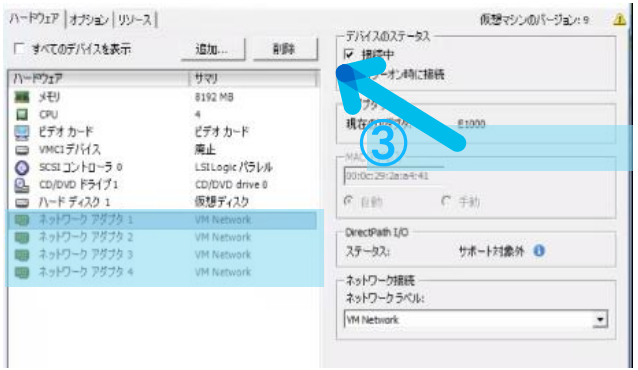
2. **vSphere Client 6.0で .ovf を以下のようにデプロイ**
   FTDは管理用に仮想NICを1つ持つため、Management管理ネットワークに所属させる

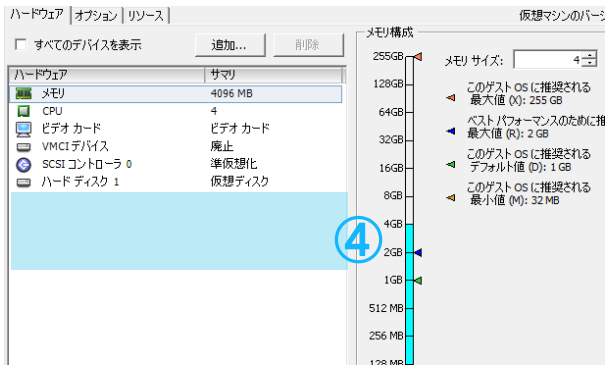
   

3. その他vSphere Client上での設定はデフォルトを使用し、デプロイが完了

ステップ 2-1: アダプタタイプの変更(ESXi 6.0の場合)

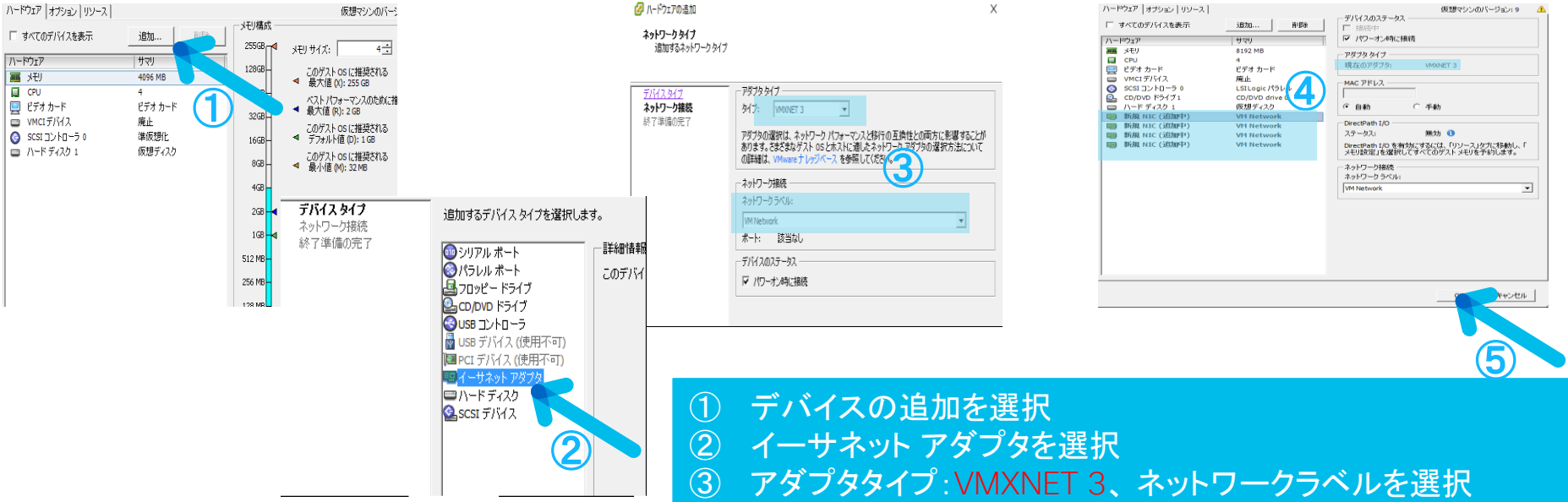
ステップ2-1と2-2は10G Interfaceが必要な場合に実施





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



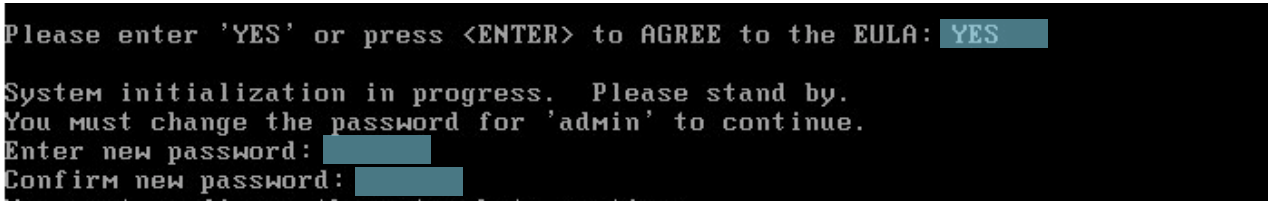
① デバイスの追加を選択
② イーサネット アダプタを選択
③ アダプタタイプ：VMXNET 3、ネットワークラベルを選択
④ 全仮想NICが左記のようになれば、アダプタタイプの変更完了
⑤ “OK”を選択

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

- ライセンス契約(EULA)を [SPASE] 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



- Adminユーザ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 ...
```

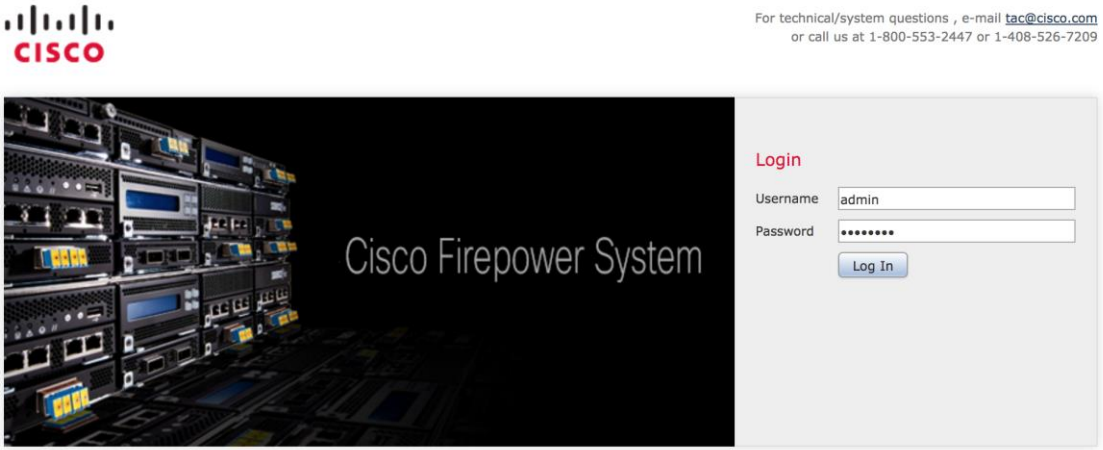
ステップ 4: FMCへの登録キーの設定

- **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>

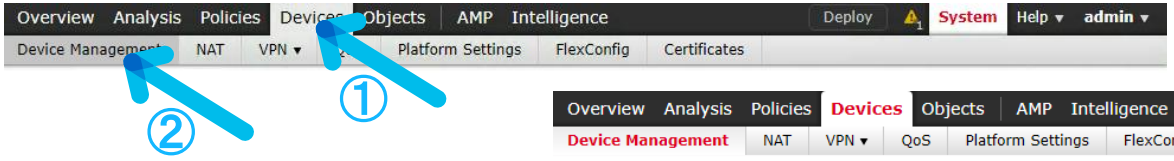
```
> configure manager add 10.71.132.201 cisco
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

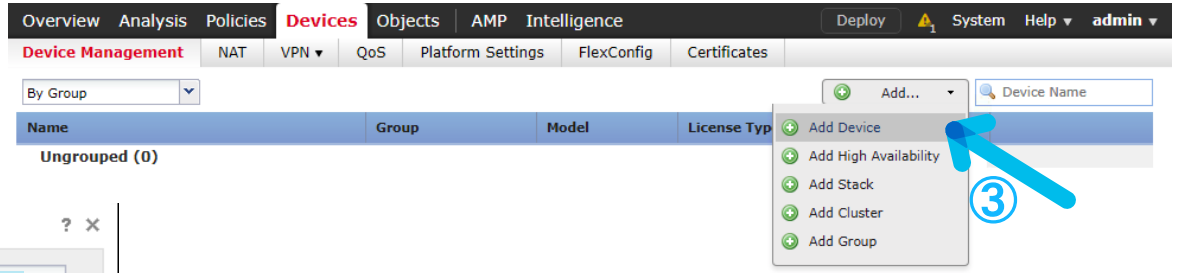
ステップ 1-1: FMCにアクセス

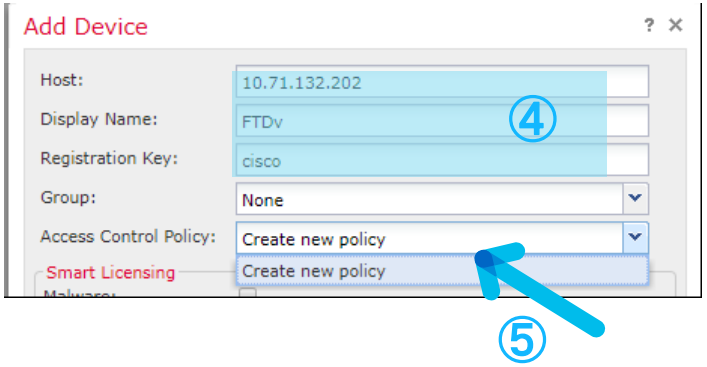
- **初期設定で入力した IP アドレスと adminパスワードを使い FMCの Web GUI へブラウザでHTTPSアクセスしログイン**



ステップ 1-2: FTDデバイスの登録

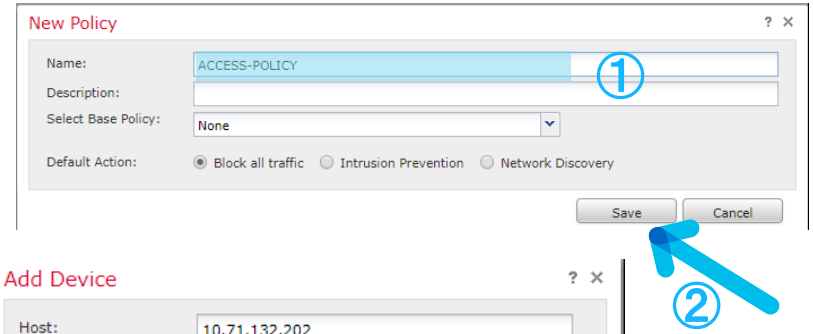


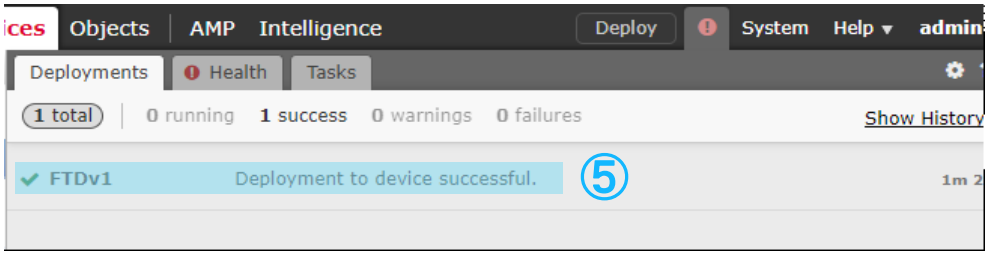


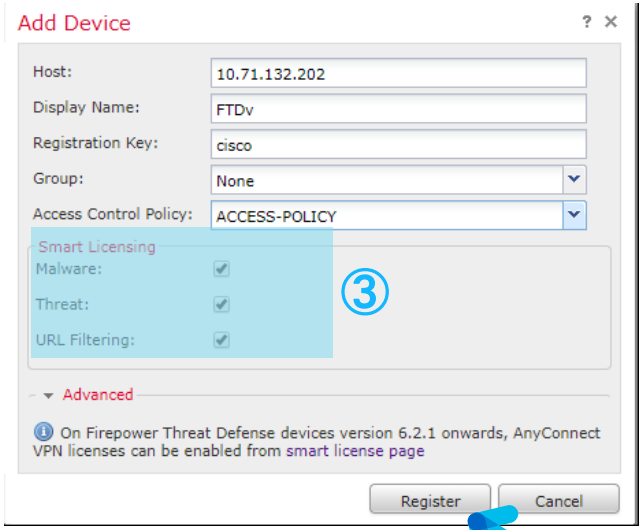


① GUI の上部にある Devices を選択
② Device Management を選択
③ Add Device を選択
④ FTD の IPアドレスと、登録キーを入力
⑤ “Create new Policy” を選択
引き続き、次のスライドを参照

ステップ 1-3: FTDデバイスの登録



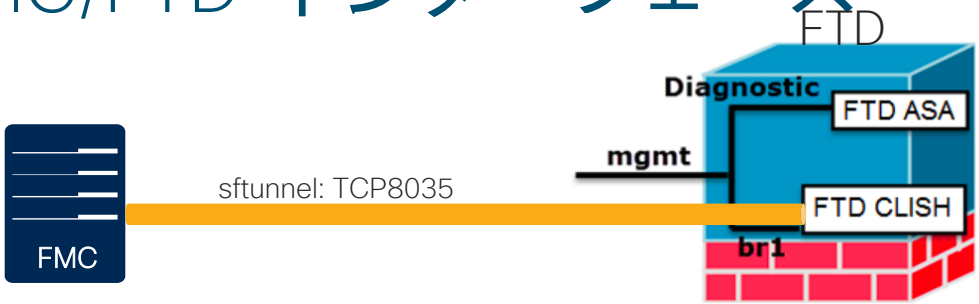




① 設定ファイル(ポリシー)の名前を入力
② “Save” を選択
③ Add Deviceの画面に移り、ライセンスを図のように選択
④ 最後に Register を選択し、FTDデバイス登録を実行
⑤ 上記のようになれば、デバイスの登録完了(所要時間:数分)

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



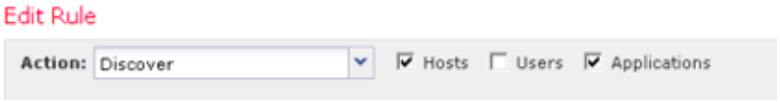
	br1	Diagnostic
目的	•FTD, FMC との通信に使用 (sftunnel) •FTD box への SSH アクセスに使用	•ASA engine へのリモートアクセスに使用 •ASA engine syslog の Source IP として使用
必須条件	[必須] FTD, FMC との通信に利用される (sftunnel)	[任意] ※設定は非推奨 ASA engine syslog 等を送信したい場合、data interface を利用することを推奨
確認方法	(CLISH CLIより) >show network (FMC GUIより) Devices > Device Management > Device > Management	(CLISH CLIより) >show interface ip brief (FMC GUIより) Devices > Device Management を選択 対象デバイスのEditボタン

2. FTDとFMCその他初期設定

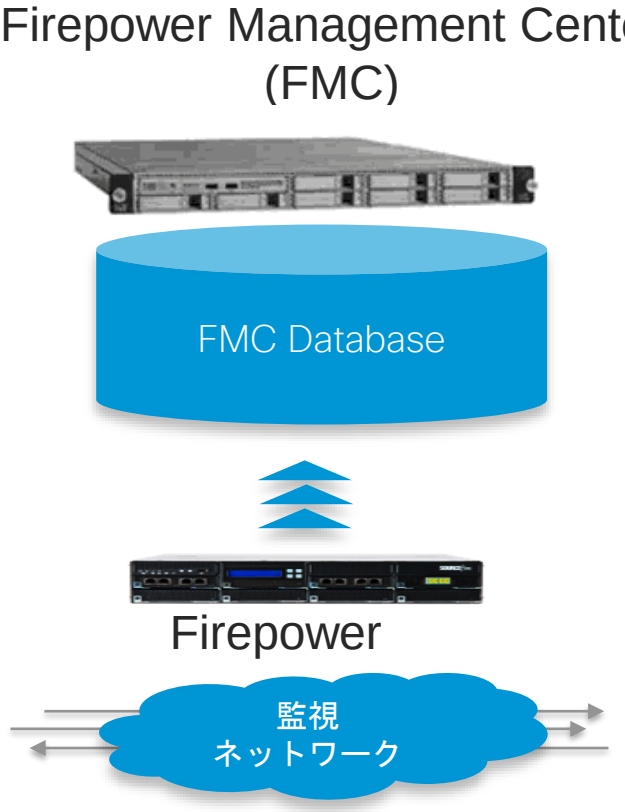
FTDとFMCその他初期設定に関して

- 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

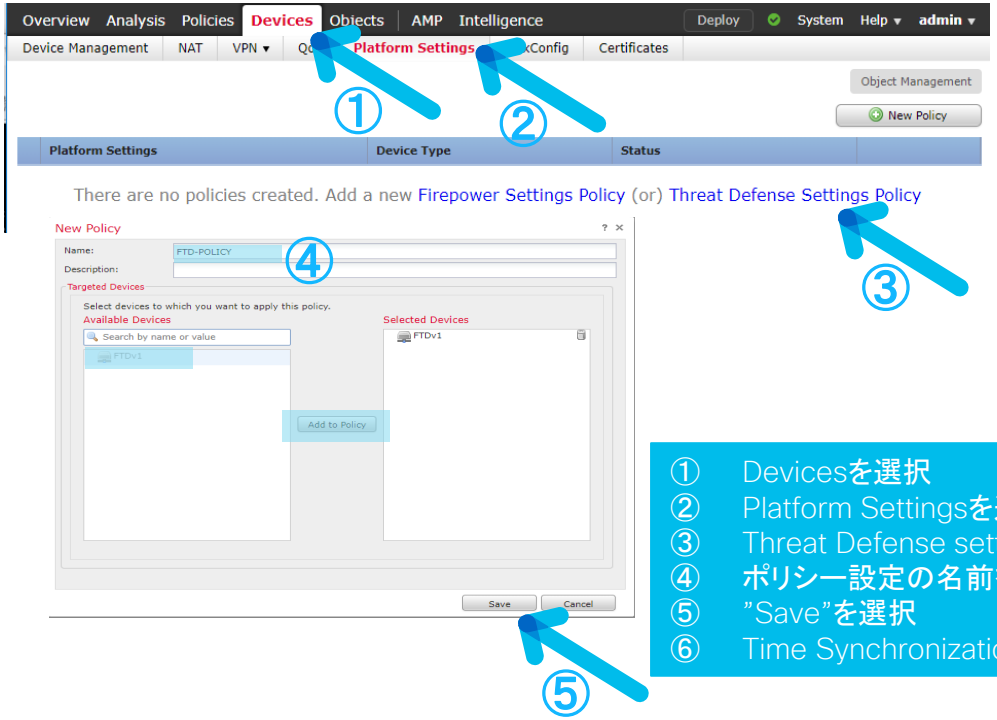


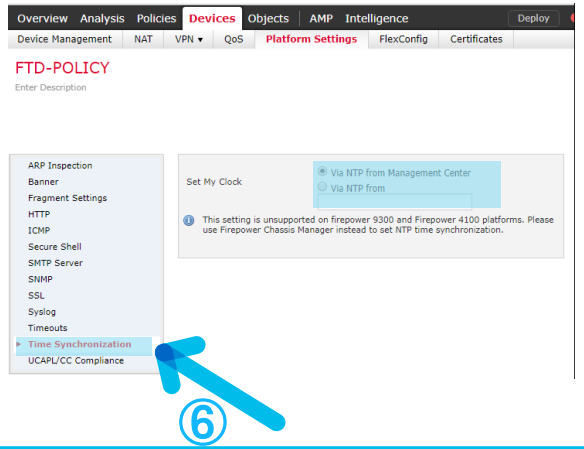
- Snortエンジンを通過する通信から以下の3つ情報を学習
- ホスト
  - パッシブディテクション（OSフィンガープリンティング等）により情報を収集し、ネットワークマップにホストエントリを作成
  - ホスト情報は、ホストインプットAPI経由のマニュアル設定および、GUI経由の手動編集に対応
- アプリケーション
  - ホストの利用アプリケーションを検出しネットワークマップに追加
  - ホストやユーザのディスカバリ利用時には有効化が必須
- ユーザ
  - ユーザテーブルを作成し、ネットワークアクティビティ（ログイン等）を記録



ステップ1-1：Time Synchronization

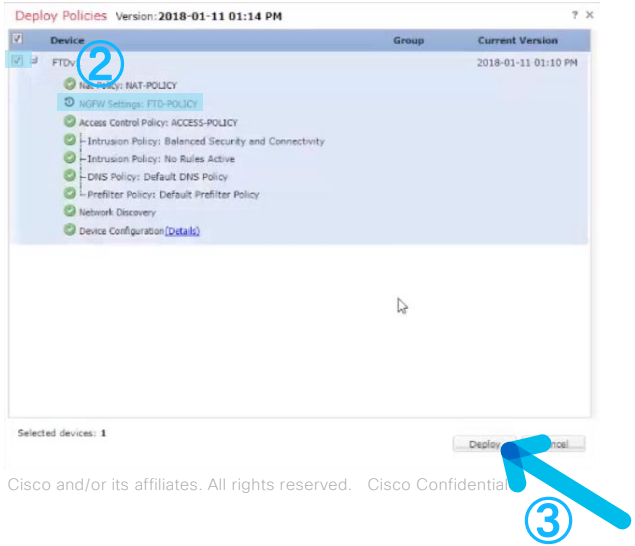
- FTDの時刻同期を設定。ここではFMCに従うものとする。





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

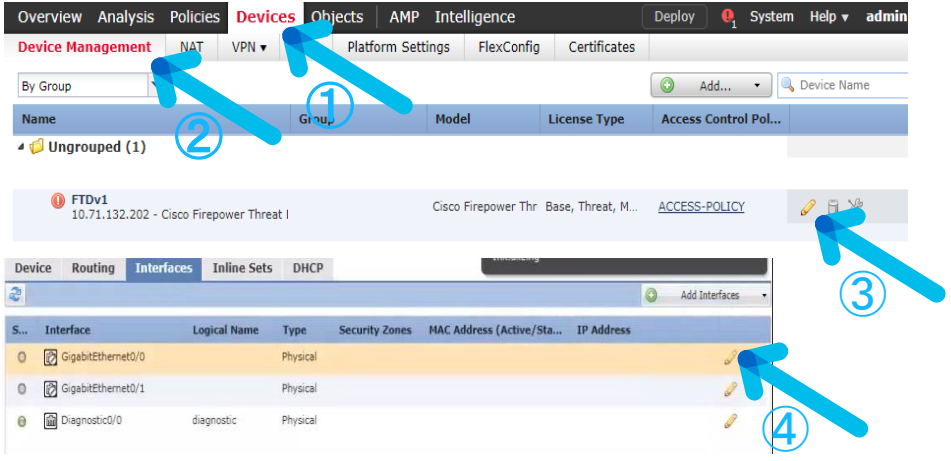


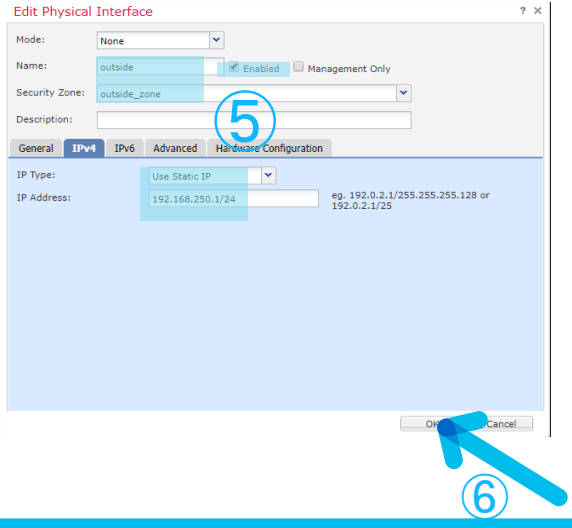
① “Deploy”を選択
② 変更された設定を確認の上、Deploy対象機器にチェックを入れる
③ “Deploy”を選択

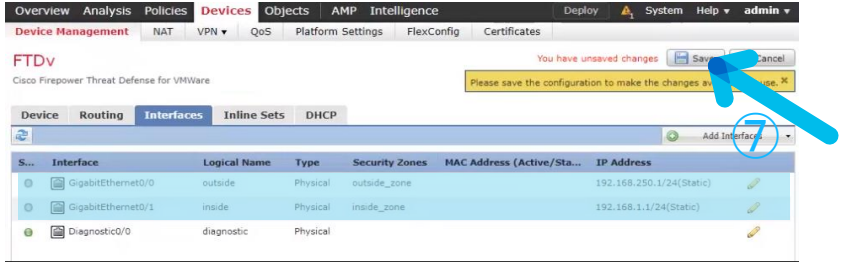
(注)FP4100,FP9300のNTPはFXOS側の設定に従う。
ただし、ここで設定しても無視されるだけで問題は無い。

ステップ2：Interface

- FTDのRouted Interfaceを設定





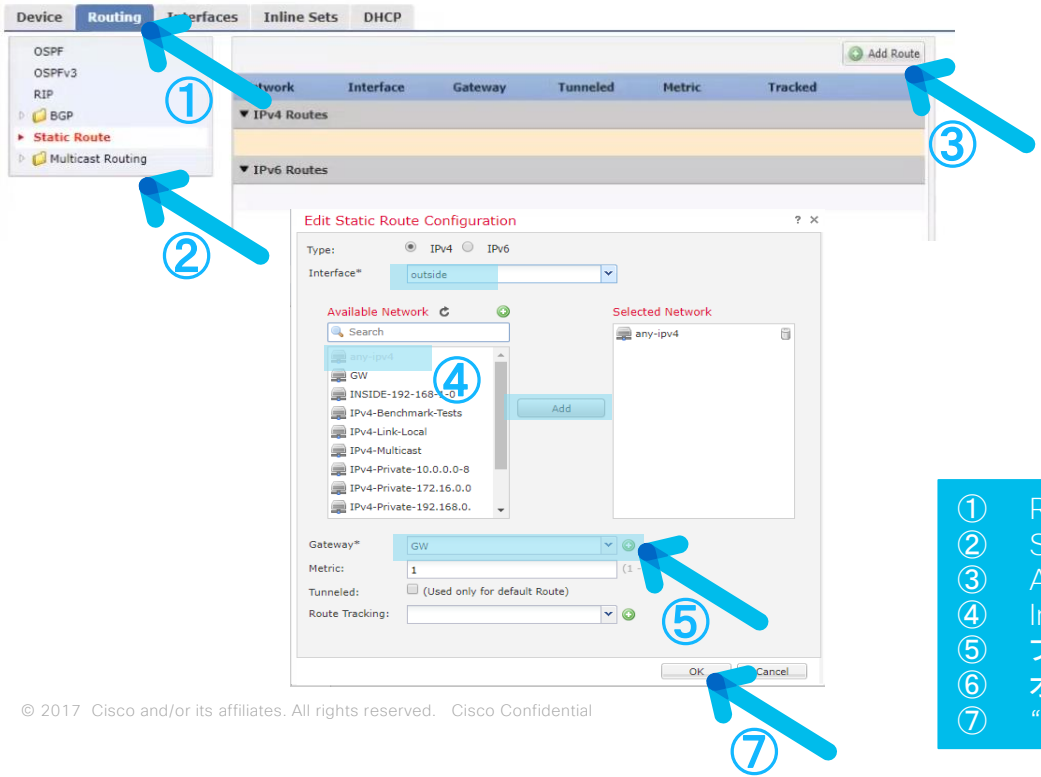


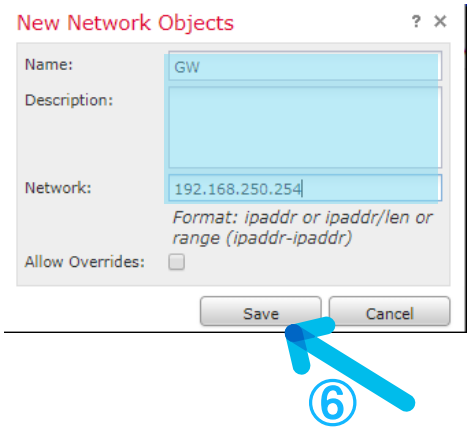
① Devicesを選択
② Device Managementを選択
③ 鉛筆マークを選択
④ G0/0の鉛筆マークを選択
⑤ 物理インターフェスの名前、Enabled、Security Zoneの名前、IP Type、IPv4アドレス、サブネットを入力
⑥ “OK”を選択
⑦ G0/1も同様にインターフェース設定を行い、”Save”を選択

Security Zone = Interfaceのグループ

ステップ3-1：Routing

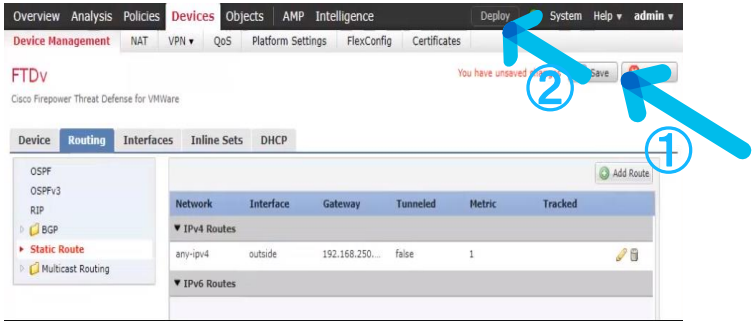
- FTDのデフォルトゲートウェイを設定。管理用のゲートウェイではなく実トラフィック用であることに注意

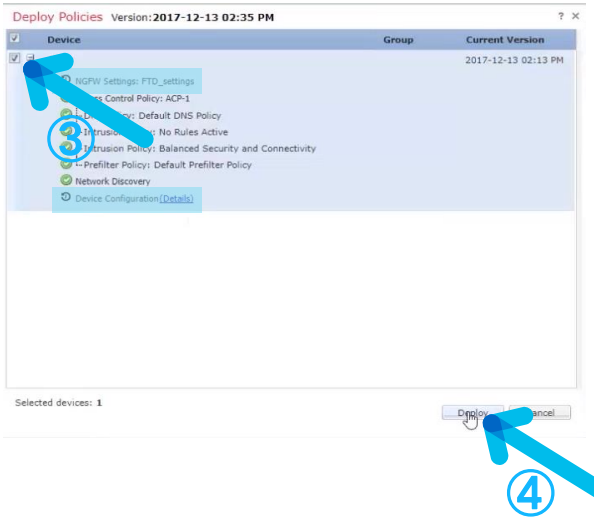




① Routingを選択
② Static Routeを選択
③ Add Routeを選択
④ Interface（宛先）、any-ipv4を選択し、”Add”を選択
⑤ プラスマークを選択
⑥ オブジェクトの名前、ゲートウェイを入力し、”Save”を選択
⑦ “OK”を選択

ステップ3-2：Routing



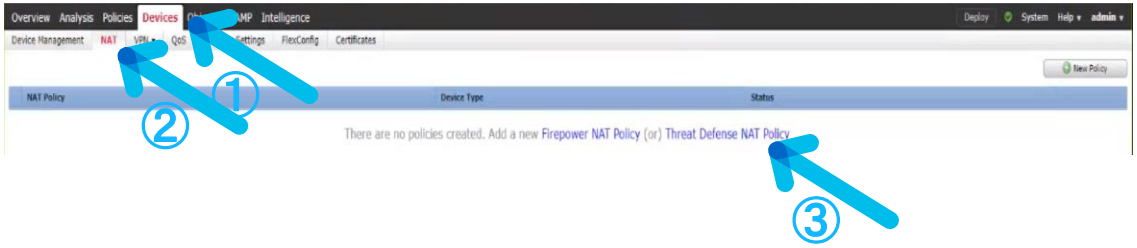


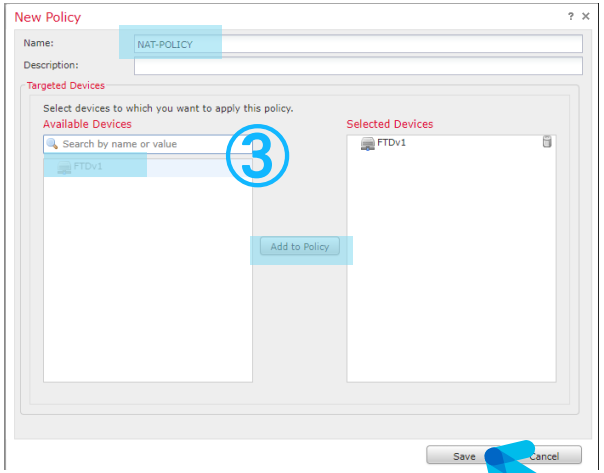
① “Save”を選択
※FMC上でのSaveであり、実機(FTD)にはまだ反映されていない
② “Deploy”を選択
③ 変更された設定を確認の上、Deploy対象機器にチェックを入れる
④ ”Deploy”を選択

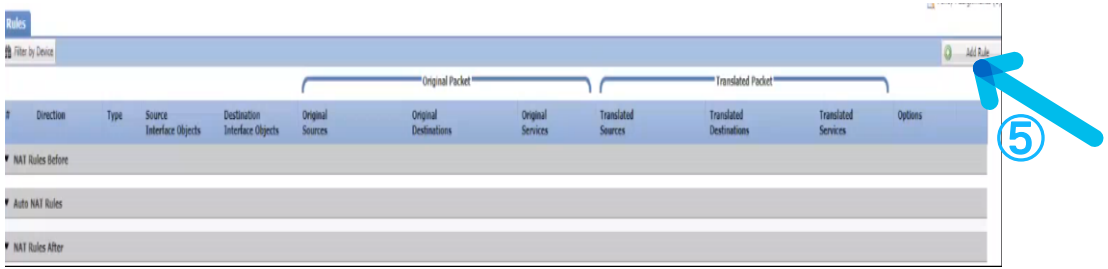
④のDeploy 後、実機にポリシーなど設定が反映される(所要時間:数分-10分程度)。

ステップ4-1：NAT

- FTDで行うNAT(PAT)を設定

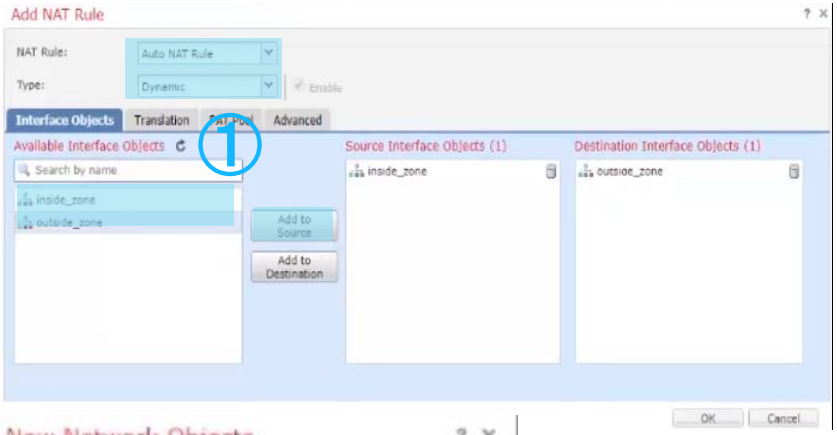


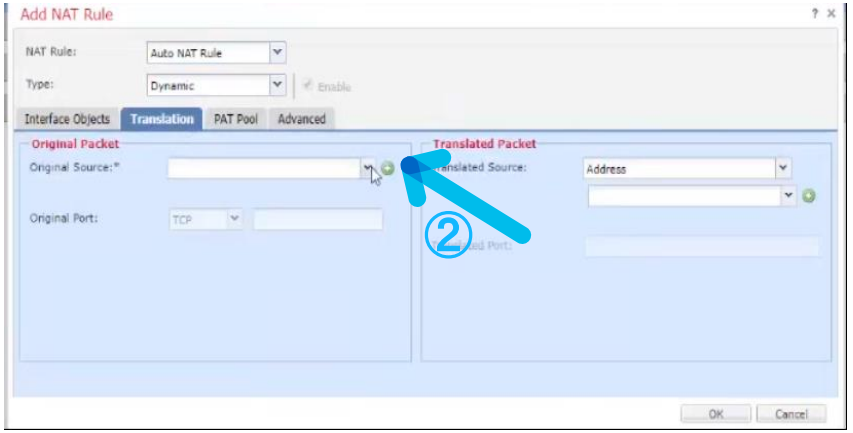


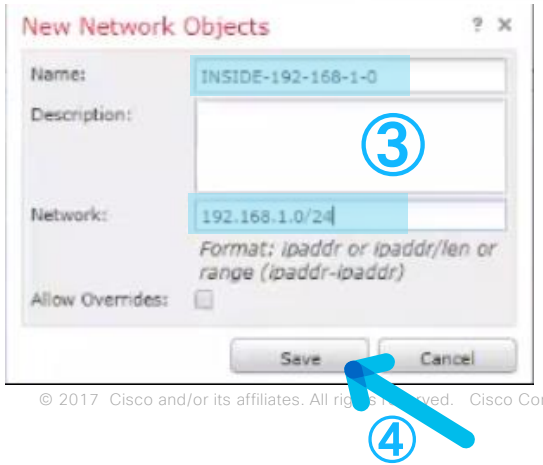


① Devicesを選択
② NATを選択
③ “Threat Defense NAT Policy”を選択
④ NAT Policyの名前、対象機器を選択し、”Save”
⑤ “Add”を選択

ステップ4-2：NAT





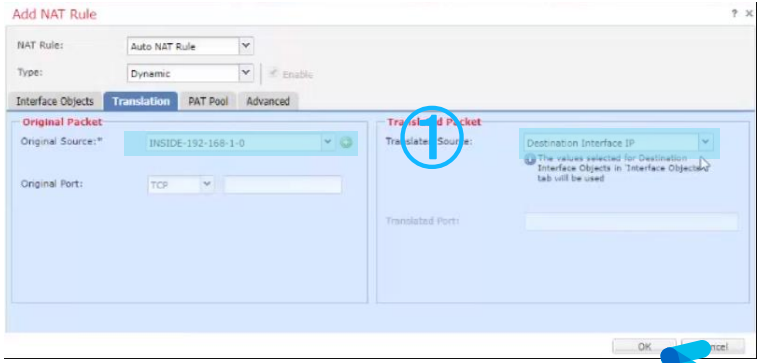


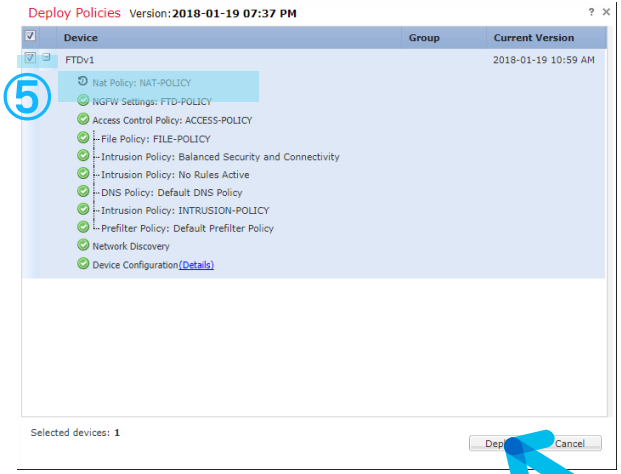
変換されるネットワークアドレス (ここでは 192.168.1.0/24) を登録

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



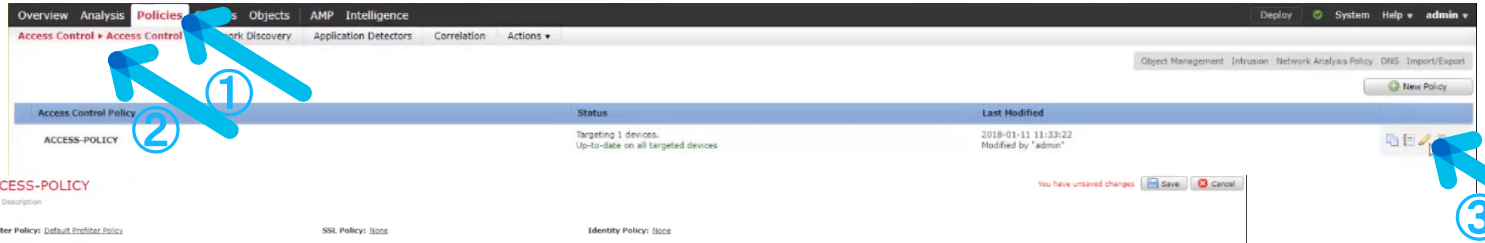


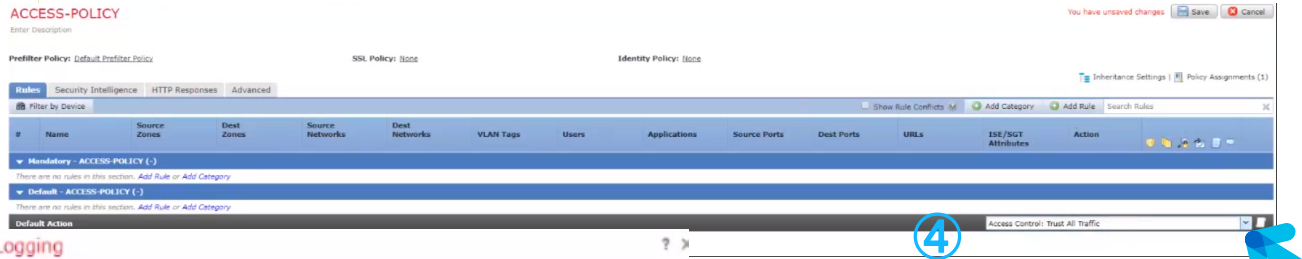
② ④ ③

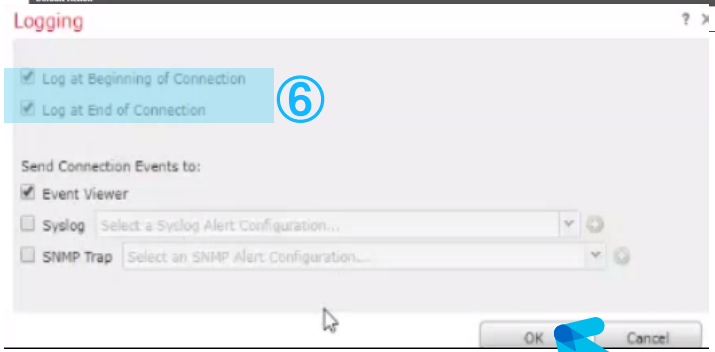
① Original Source、Destination Sourceを選択
② “OK”を選択
③ “Save”を選択
④ “Deploy”を選択
⑤ 変更された設定を確認の上、Deploy対象機器にチェックを入れる
⑥ “Deploy”を選択

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



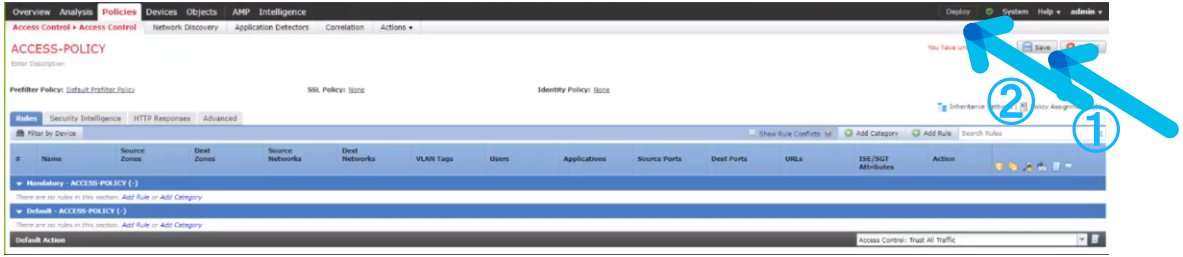


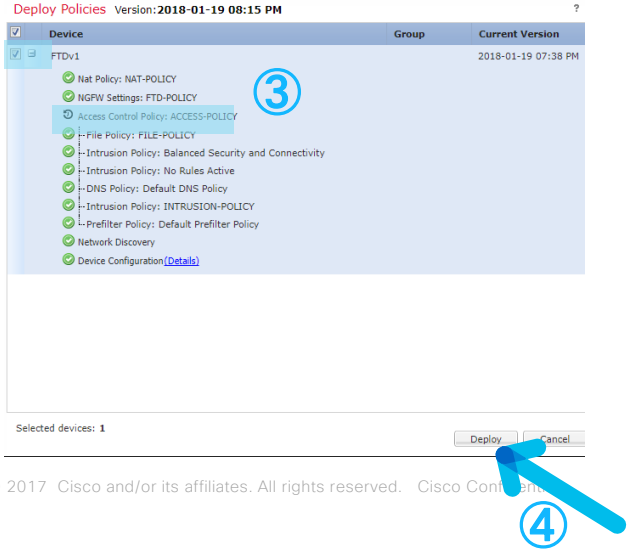


とりあえず全ての通信を信頼（許可）するのであれば、Default ActionはTrust all Trafficとする

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





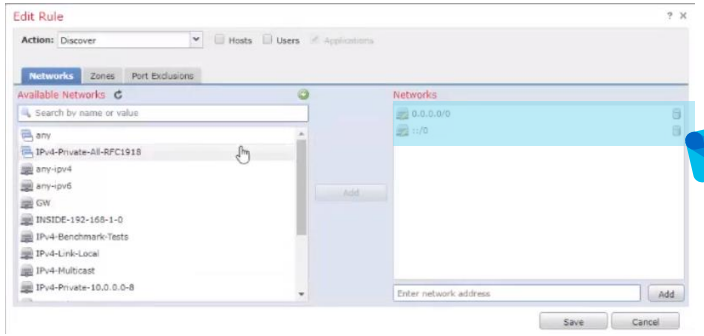
① “Save”を選択
② “Deploy”を選択
③ 変更された設定を確認の上、Deploy対象機器にチェックを入れる
④ “Deploy”を選択

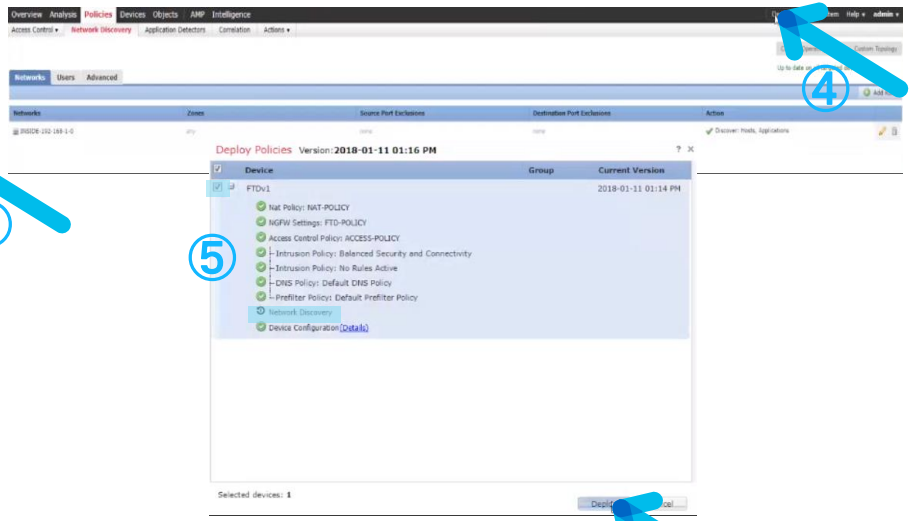
ステップ6-1：Network Discovery Policy

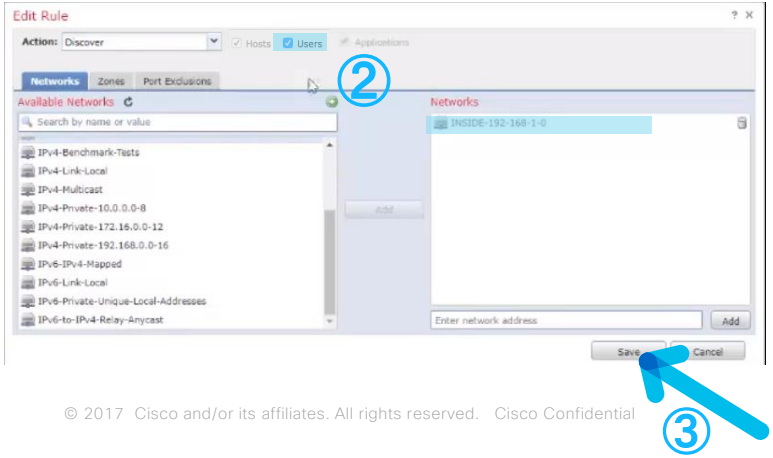
- Network Discovery Policyとは
  - 指定されたネットワーク内で、どのホスト、OS、アプリケーション等が存在するかを監視し、FMCで記憶していくためのポリシー
  - このポリシーでは監視する範囲を決め、その設定を有効にする

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



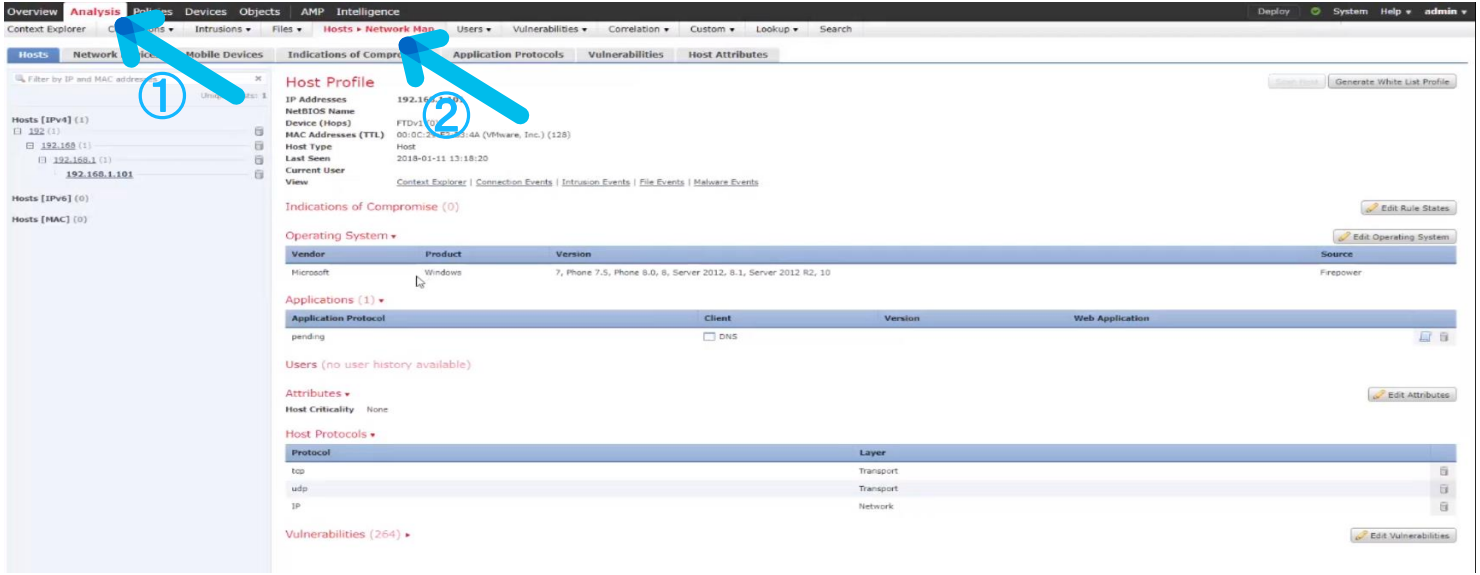




① ゴミ箱マークを選択し、ネットワーク0.0.0.0を削除
② 監視対象ネットワークを選択し、Usersにチェックを入れる（自動的にHostsも選択される）
③ “Save”を選択
④ “Deploy”を選択
⑤ 変更された設定を確認の上、Deploy対象機器にチェックを入れる
⑥ “Deploy”を選択

ステップ6-3：Network Discovery Policy

- FMCが記録したホスト情報を確認



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)

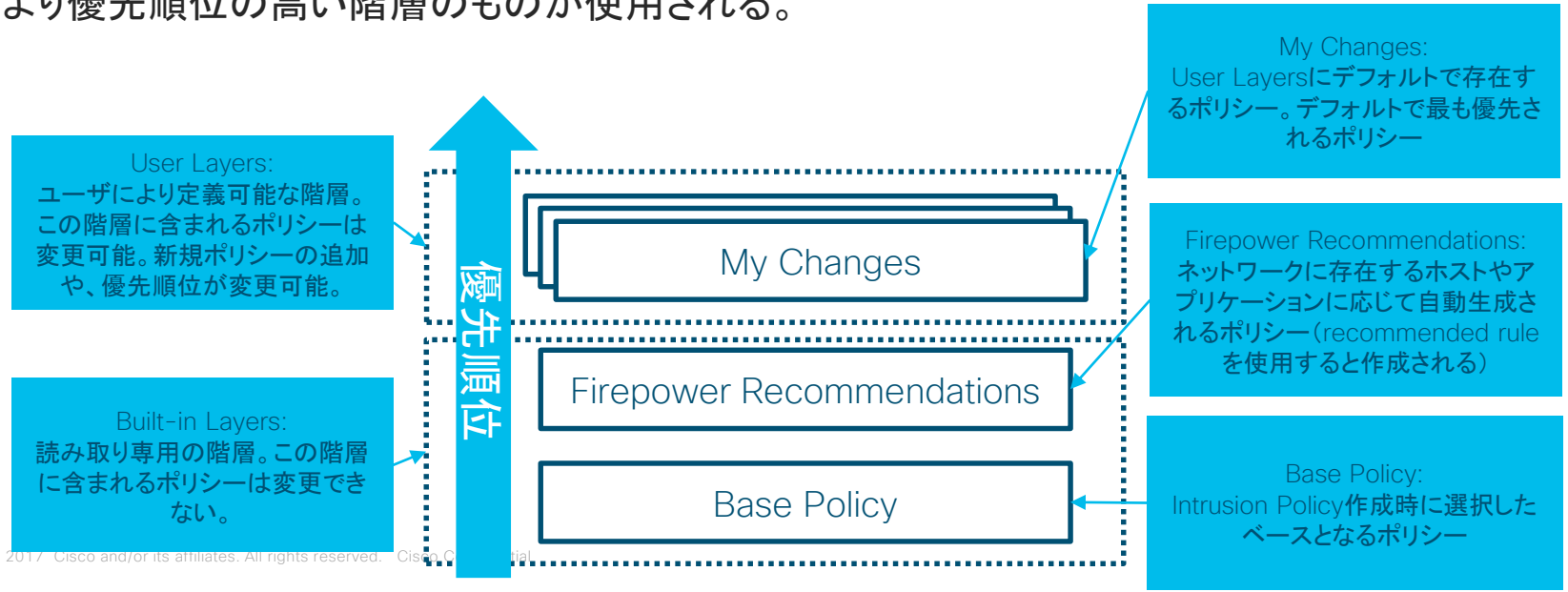
Intrusion Policyにはシグネチャに対するパラメータが含まれ、トラフィックに対するIPSの振る舞いを制御する。

■シグネチャのパラメータ

項目	パラメータ	説明
Rule State	• Generate Events • Drop and Generate Events • Disable • Inherit	シグネチャヒット時の動作設定
Event Filtering	• Threshold • Suppression	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	ヒット時のSNMPアラートの設定

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。Build-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

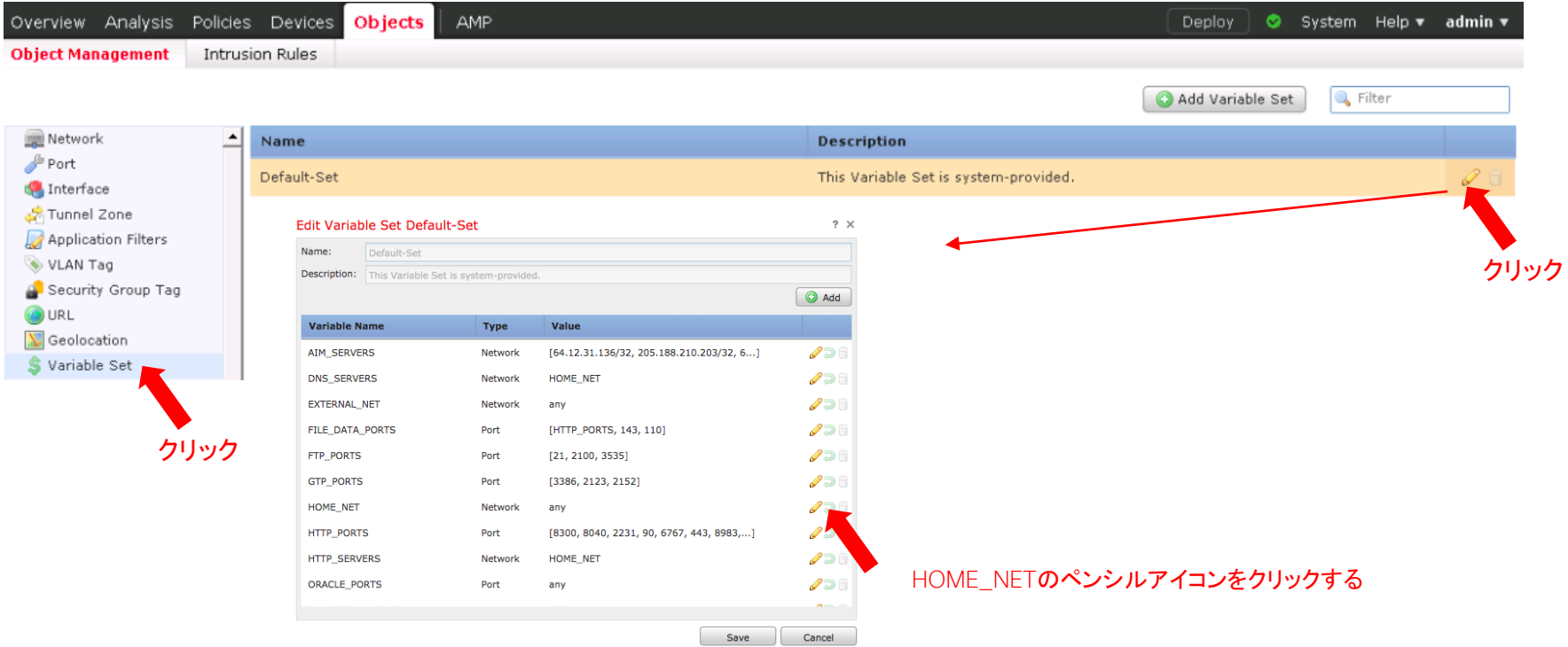
- 評価を目的としているため、トラフィックに影響を与えない様シグネチャヒット時にパケットを破棄しないポリシーを作成する
- 有意義な評価を行うために、一般的な環境でヒットしやすい一部のシグネチャを手動で有効にする
- IPS機能が正常に動作していることを確認するために、Pingでヒットするシグネチャを手動で有効にする

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

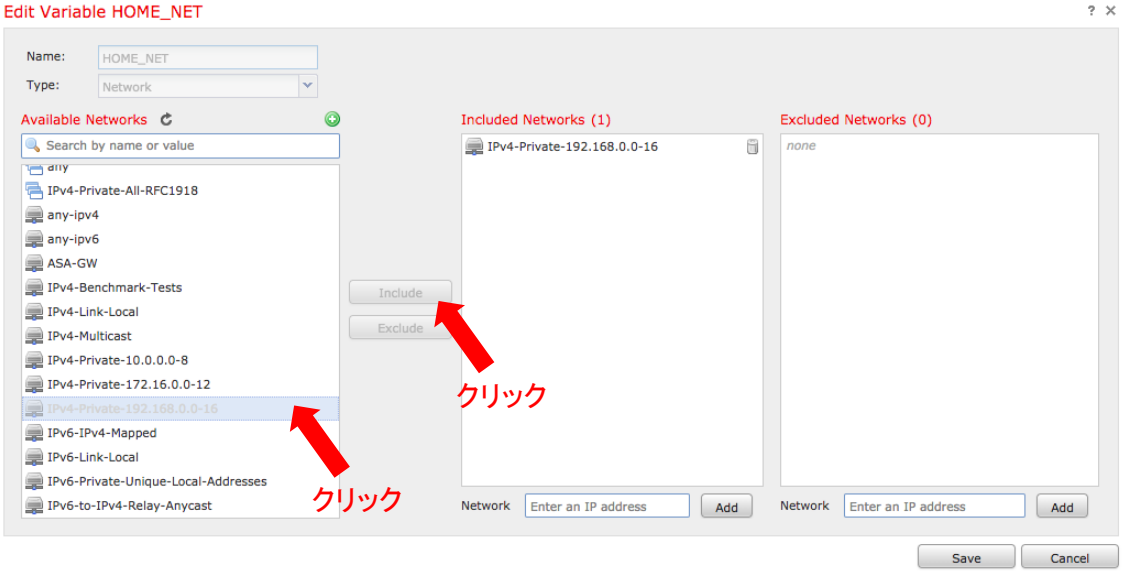


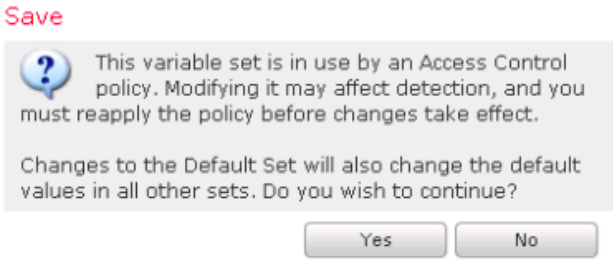
ステップ1 Variable Set 変更(HOME_NET)

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。

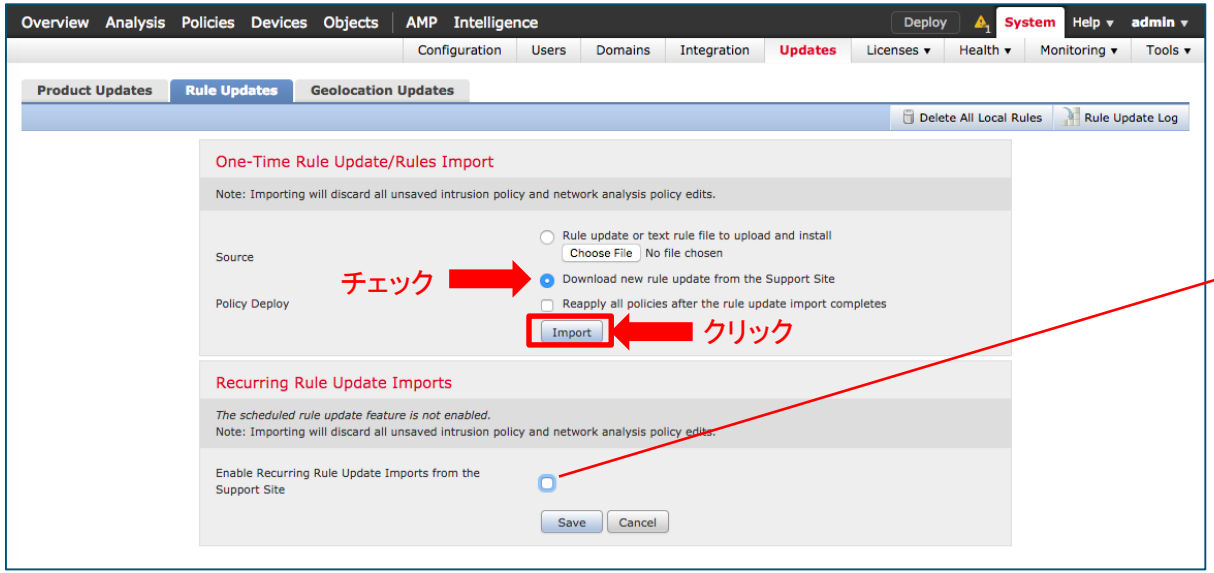
※実環境においては、お客様ごとに環境が異なるため、要確認。

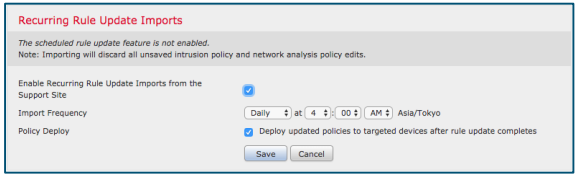




ステップ2 Intrusion Ruleのアップデート

System > Updates > Rule Updates

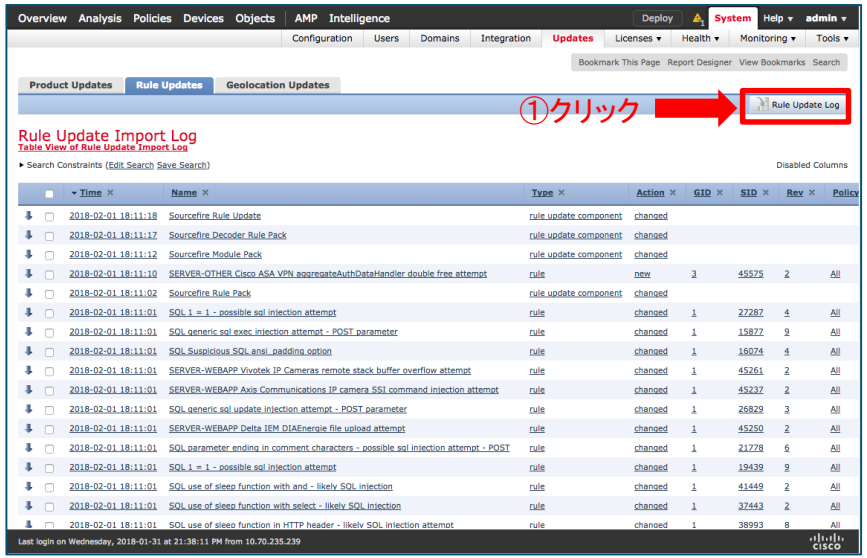


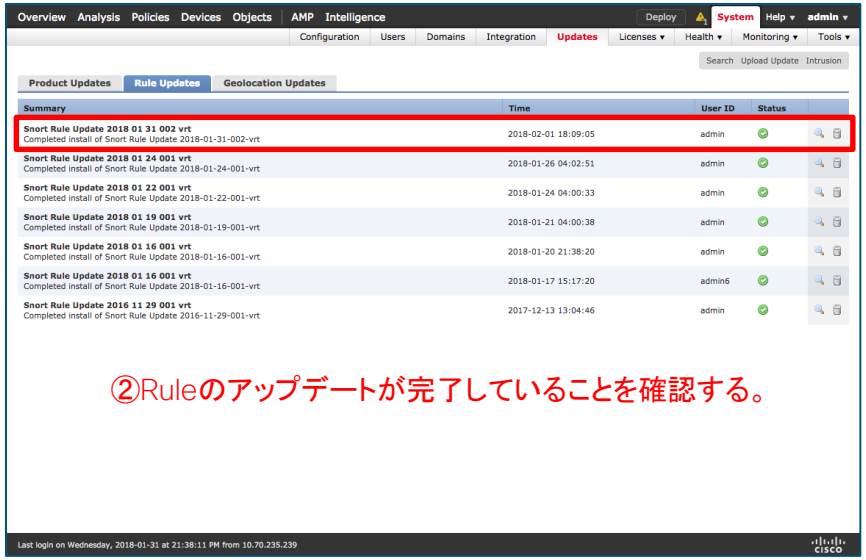


【オプション】
Enable Recurring Rule Update Imports from Support Siteをチェックすると、Intrusion Ruleの自動更新の設定が可能

ステップ2 Intrusion Ruleのアップデート

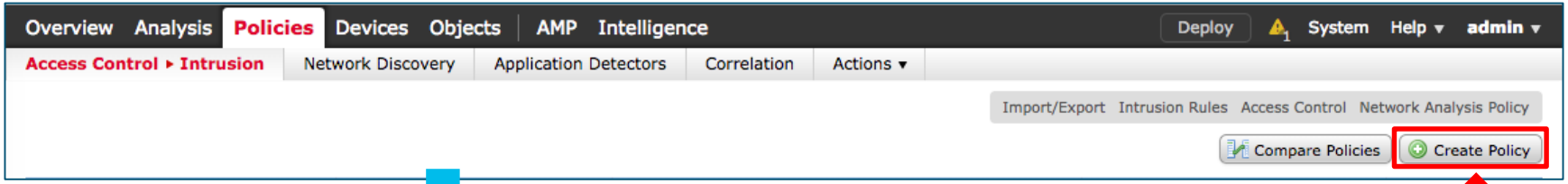
Intrusion Ruleのアップデートが完了すると、Rule Update Import Log画面に自動的に遷移する。



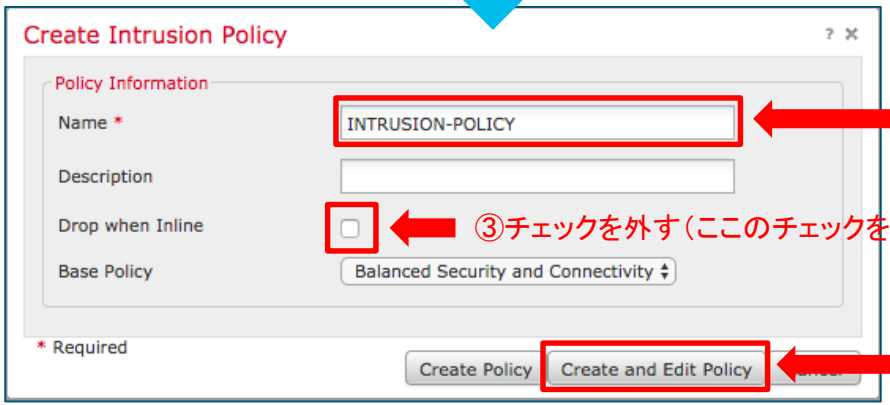


ステップ2 Intrusion Policyの作成

- Policies > Intrusion にて Create Policy をクリック



①クリック



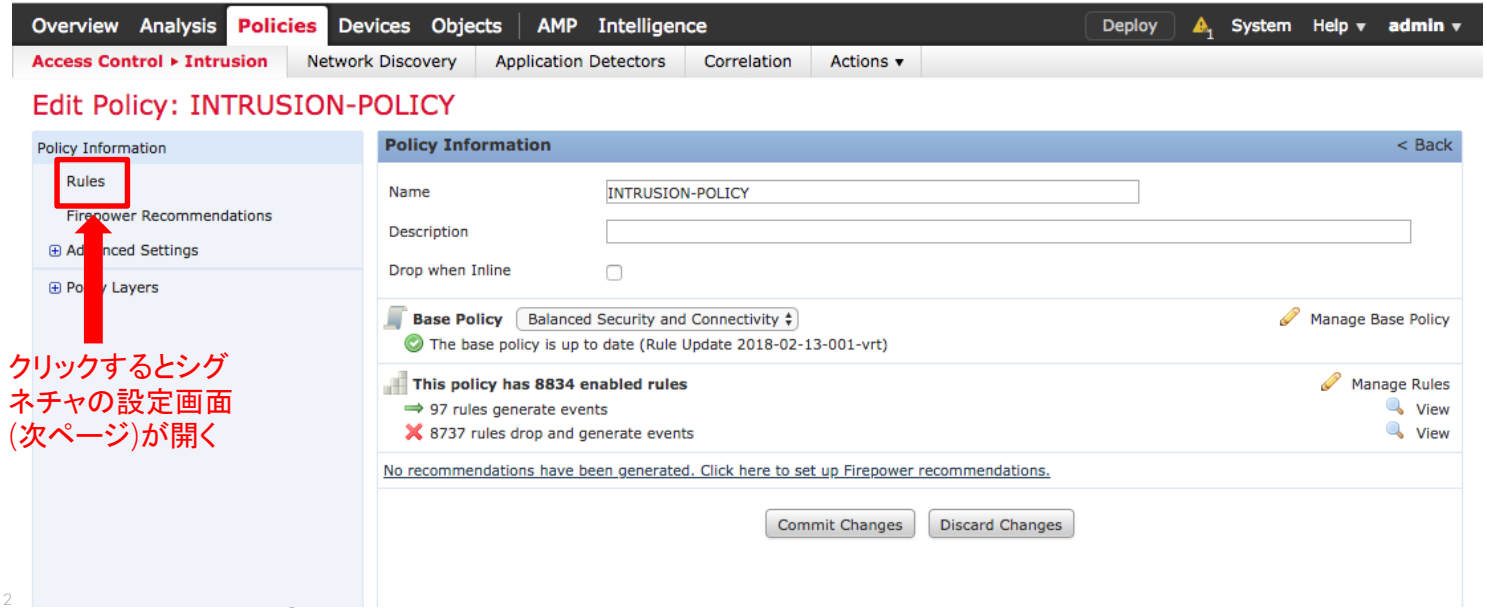
②Intrusion Policyに名前を設定、本資料では INTRUSION-POLICY を使用

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）

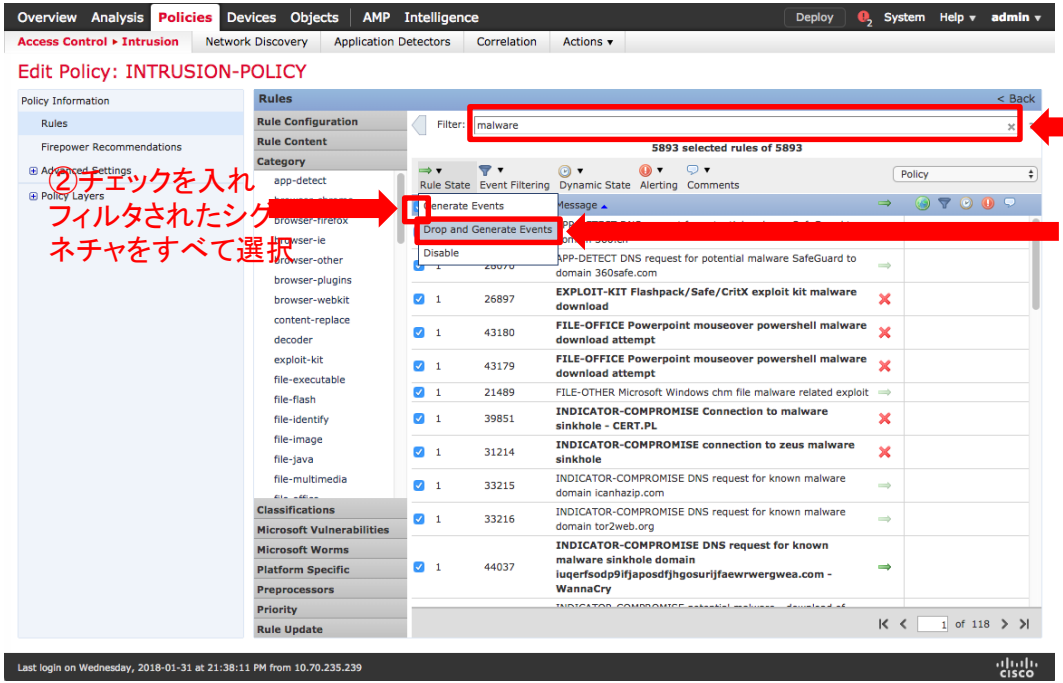
④クリックすると Intrusion Policy が作成されて編集画面(次ページ)が開く

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



ステップ3：POV用にシグネチャの手動設定



①malwareをキーワードにフィルタ

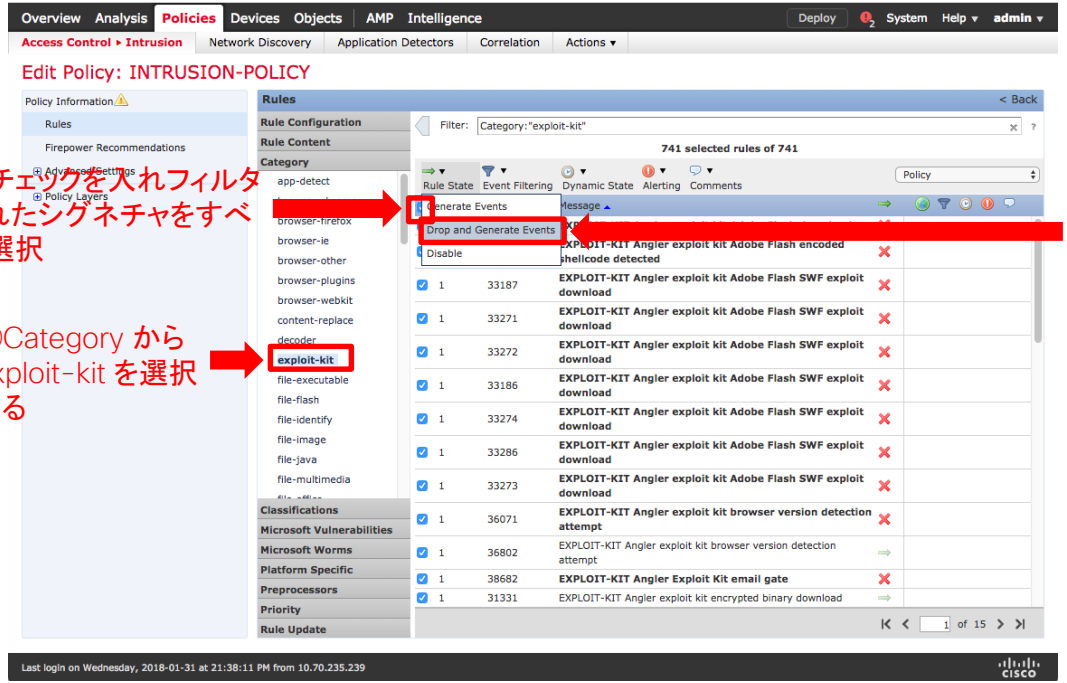
②チェックを入れフィルタされたシグネチャをすべて選択

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



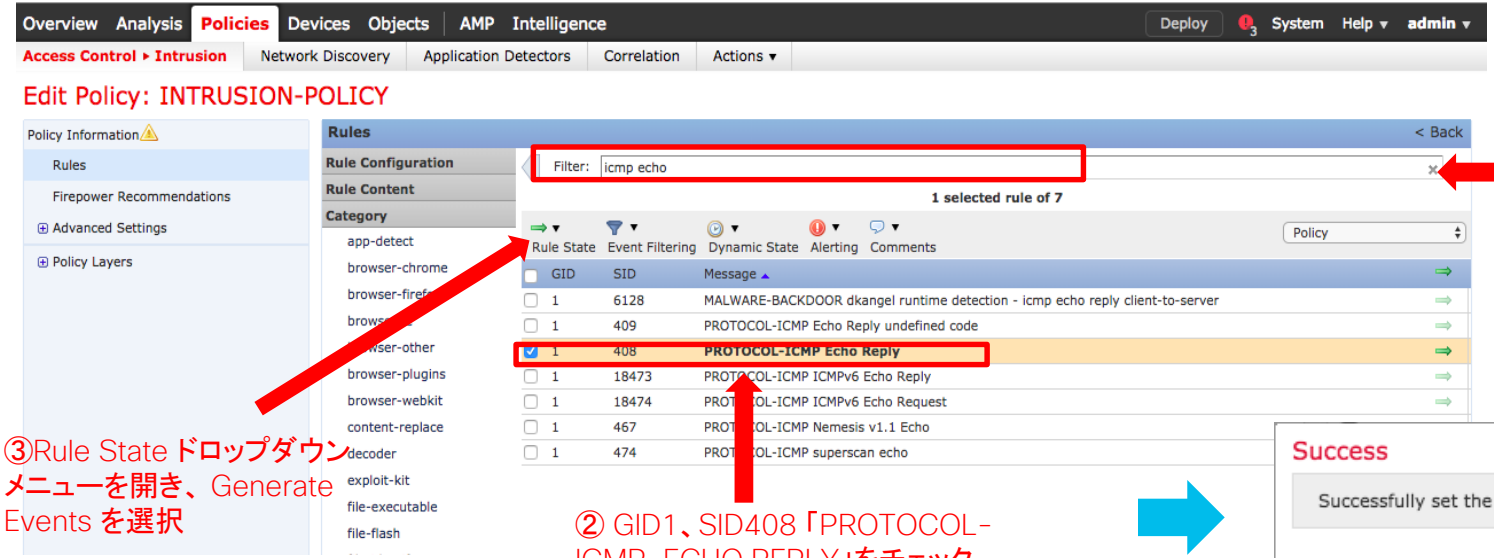
②チェックを入れフィルタされたシグネチャをすべて選択

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

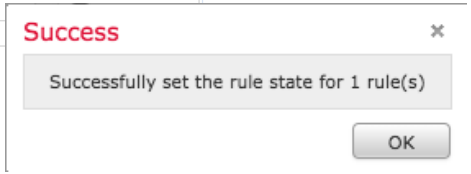
ステップ3：POV用にシグネチャの手動設定



①ICMPをキーワードにフィルタ

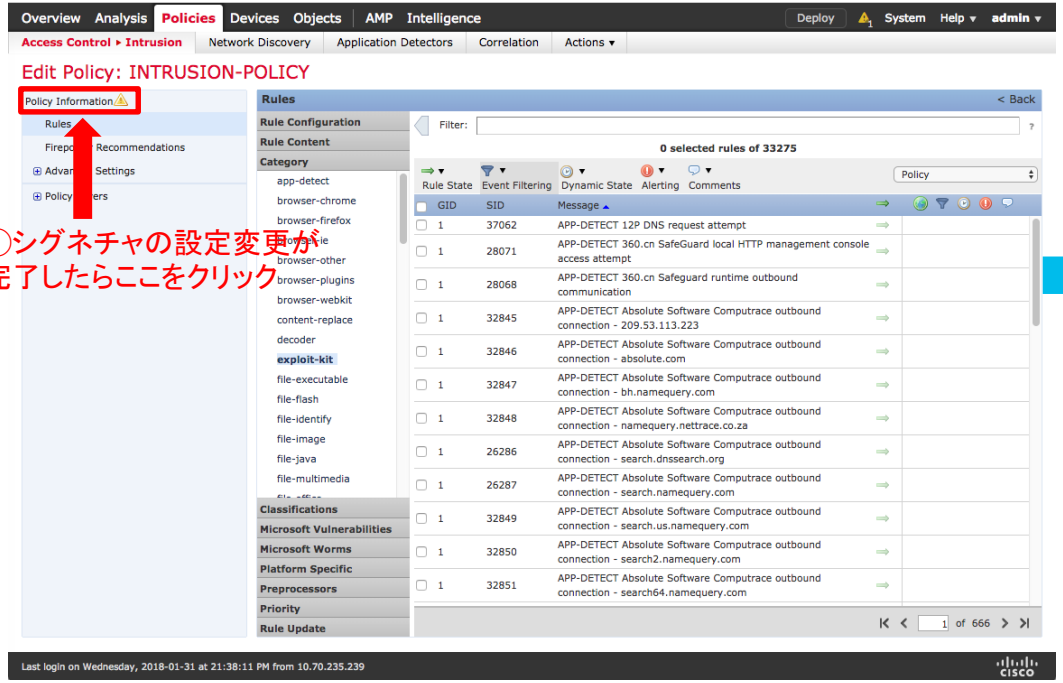
③Rule State ドロップダウンメニューを開き、Generate Events を選択

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

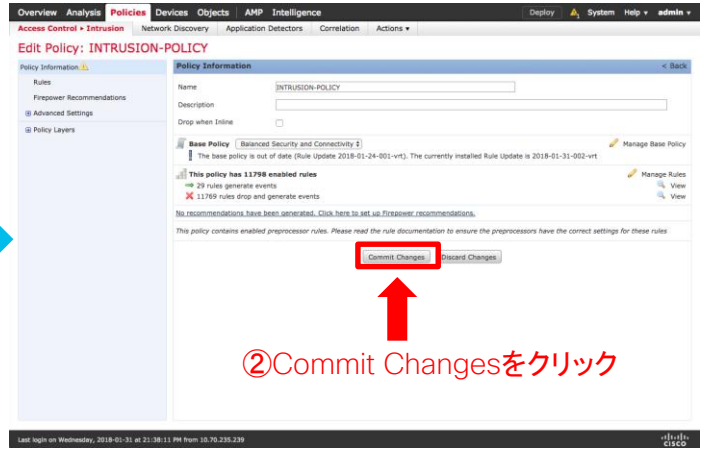


④正常に変更が完了したら上記のプロンプトが表示されるのでOKをクリック

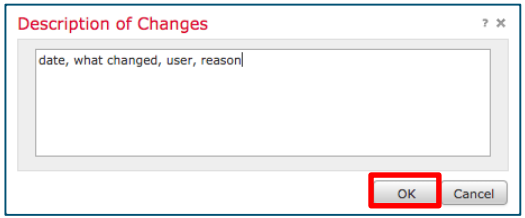
ステップ3：POV用にシグネチャの手動設定



①シグネチャの設定変更が完了したらここをクリック



②Commit Changesをクリック

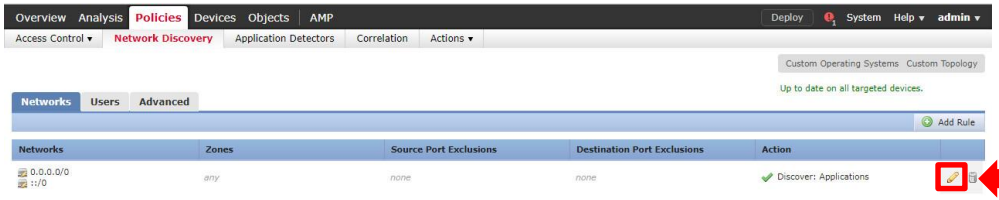


③コメントを記入してOKをクリック

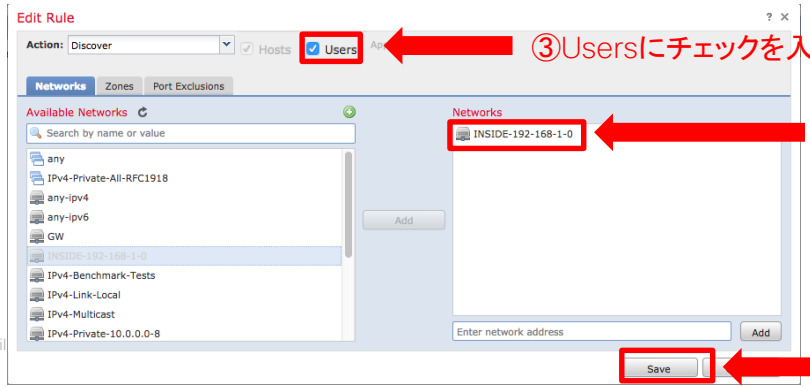
【参考情報】
Firepower recommendation によるルールの最適化

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

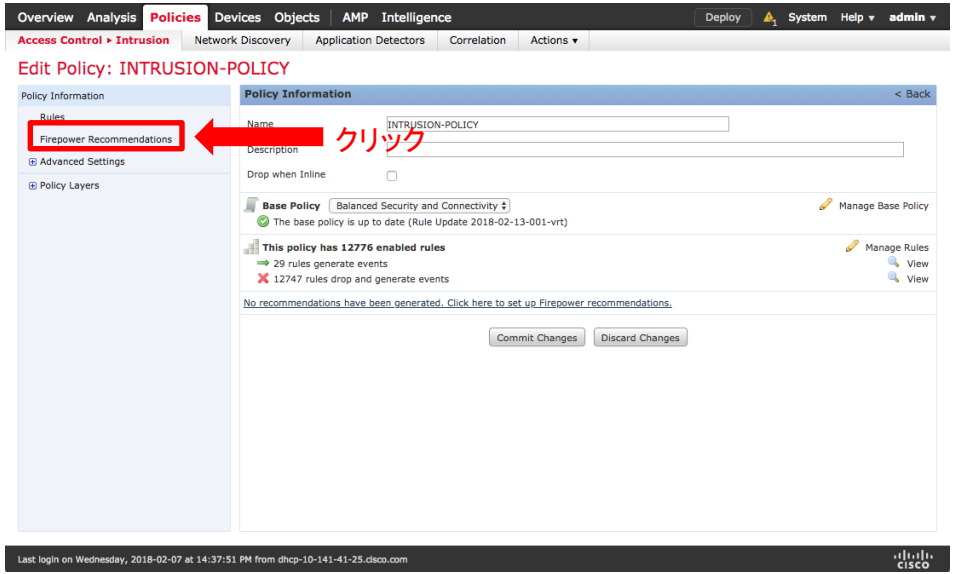


③Usersにチェックを入れる(自動的にHostsもチェックされる)

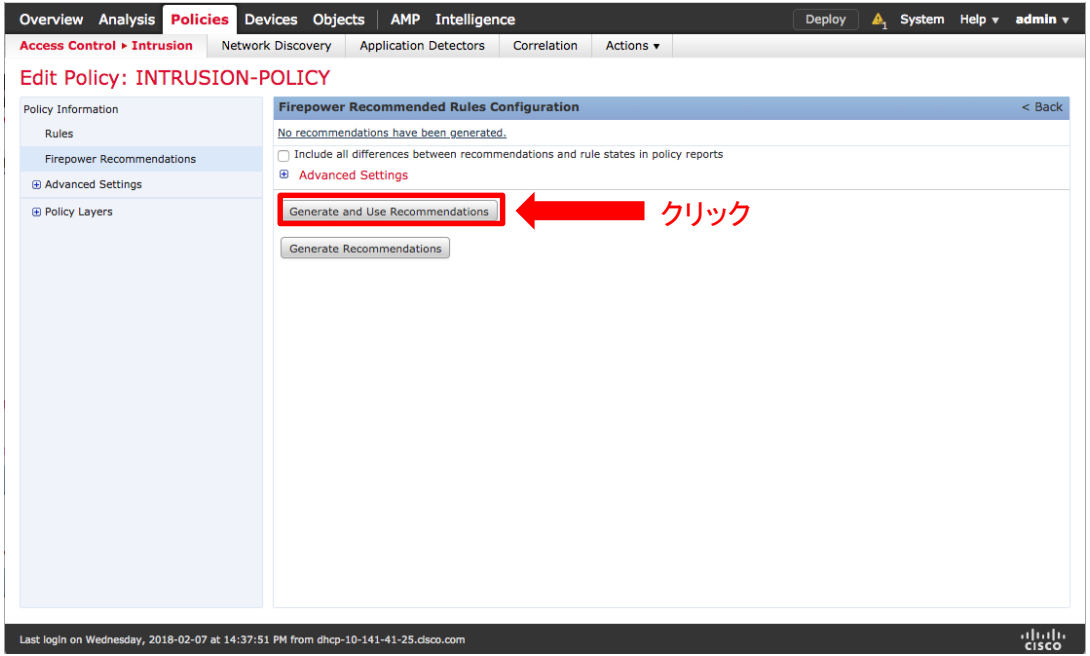
④ルールの対象とするネットワークを選択する

⑤OKをクリック

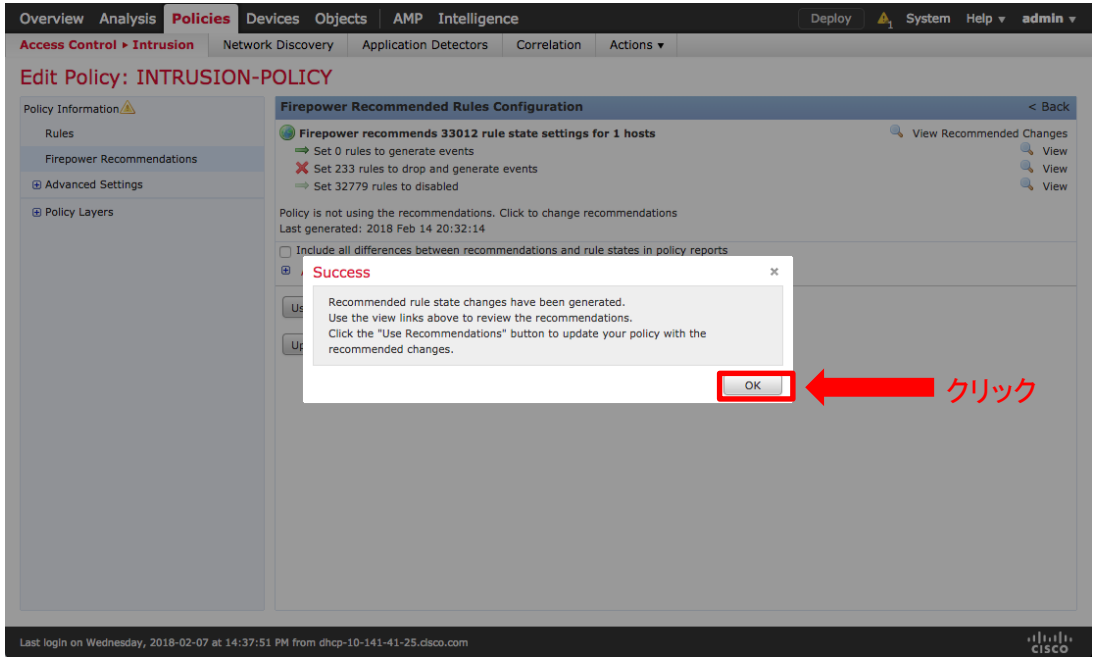
【参考情報】
Firepower recommendation によるルールの最適化



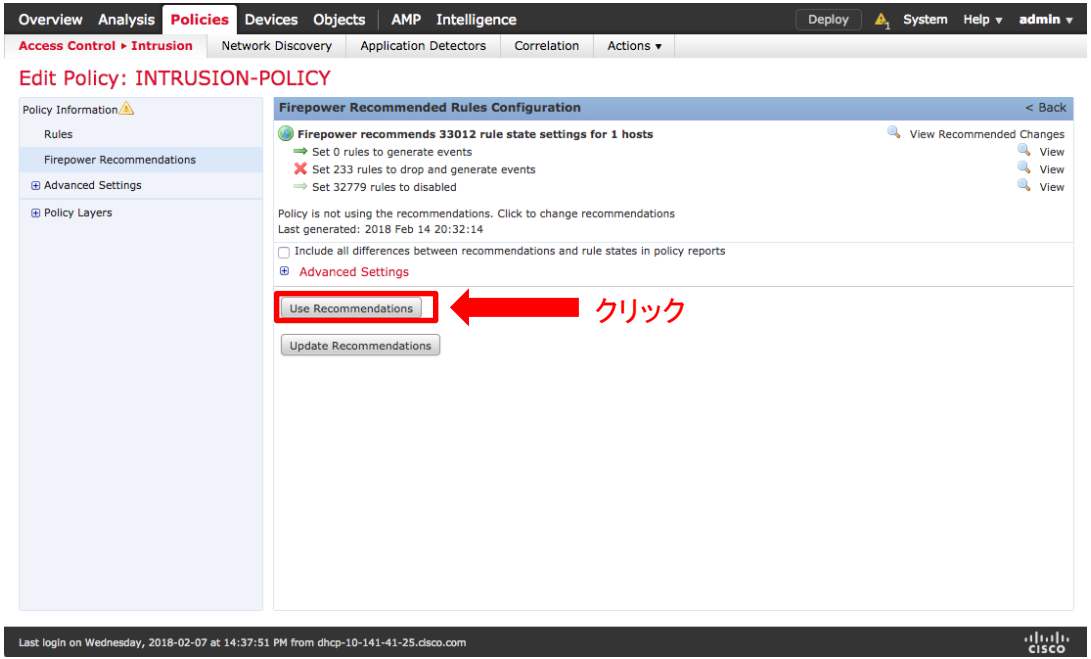
【参考情報】
Firepower recommendation によるルールの最適化



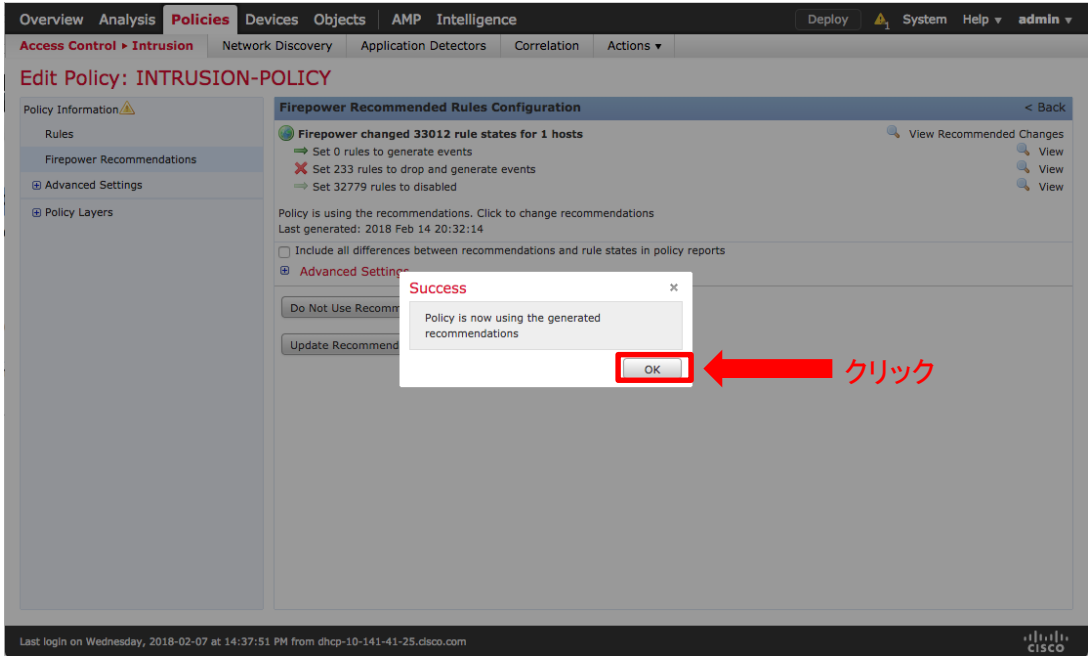
【参考情報】
Firepower recommendation によるルールの最適化



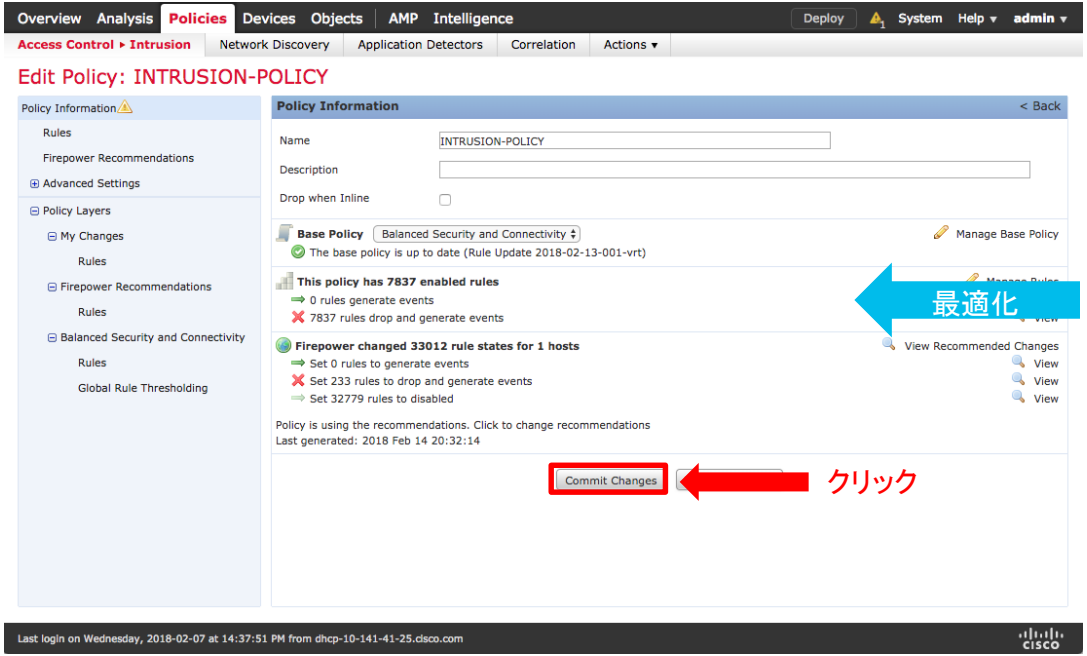
【参考情報】
Firepower recommendation によるルールの最適化

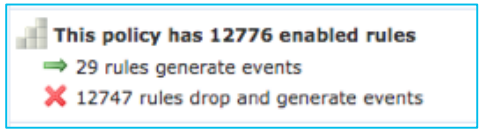


【参考情報】
Firepower recommendation によるルールの最適化



【参考情報】
Firepower recommendation によるルールの最適化





Firepower recommendation
適用前のルールサマリ

4. Malware & File Policy設定

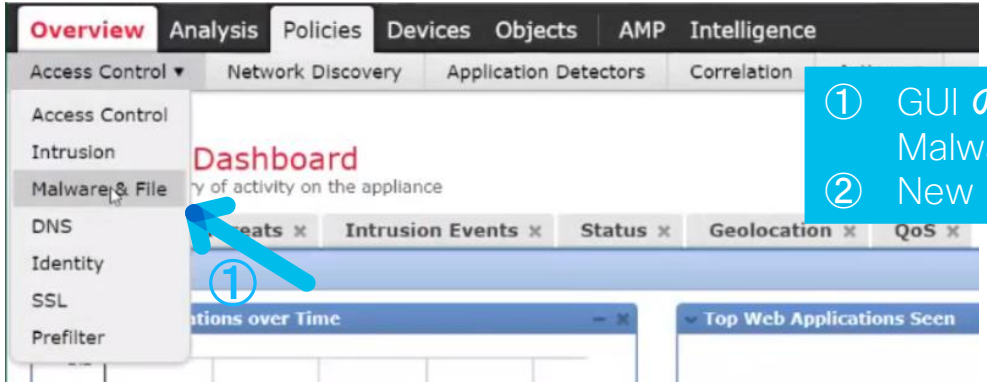
File Policyの概要

- 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

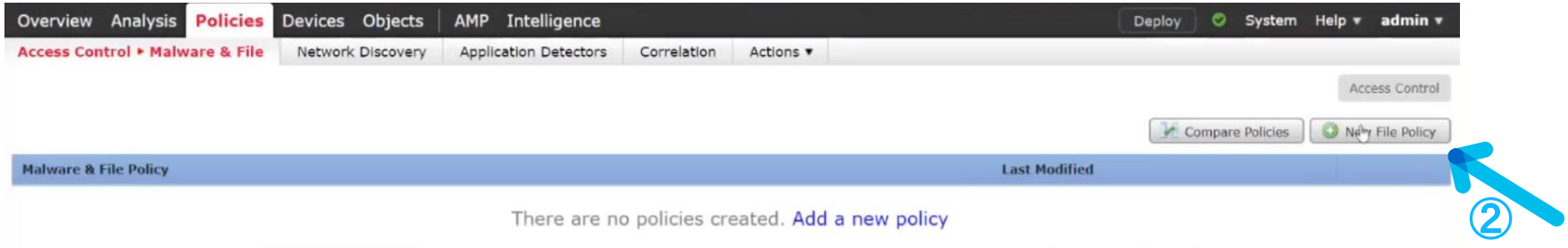
Malware & File Policy Rules

- 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 / ロギ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

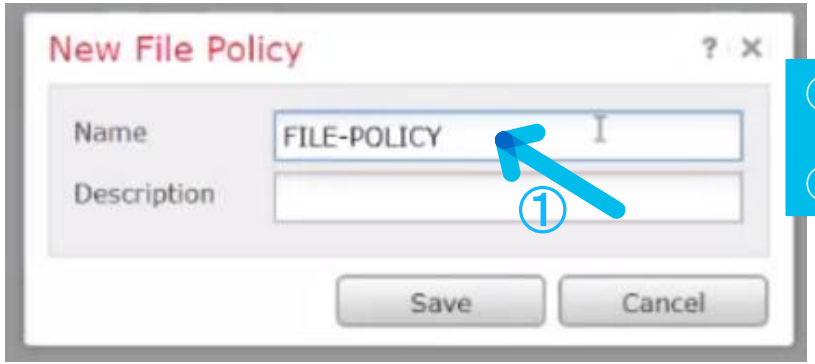


① GUI の上部にある Policies > Access Control > Malware & Fileを選択
② New File Policyをクリックし、新規File Policyを作成する



ステップ 1: File Policyの作成

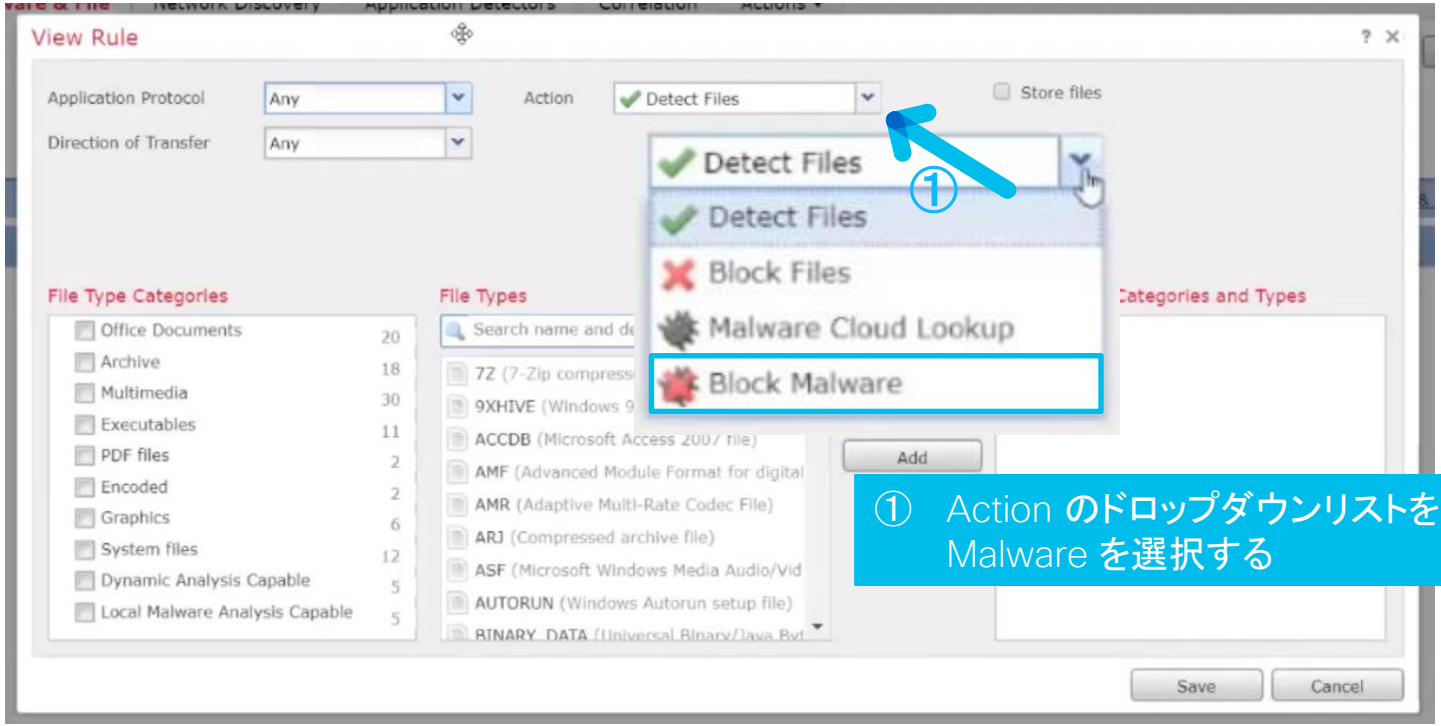
新規File Policyに名前と説明を記述するフォームが表示される



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

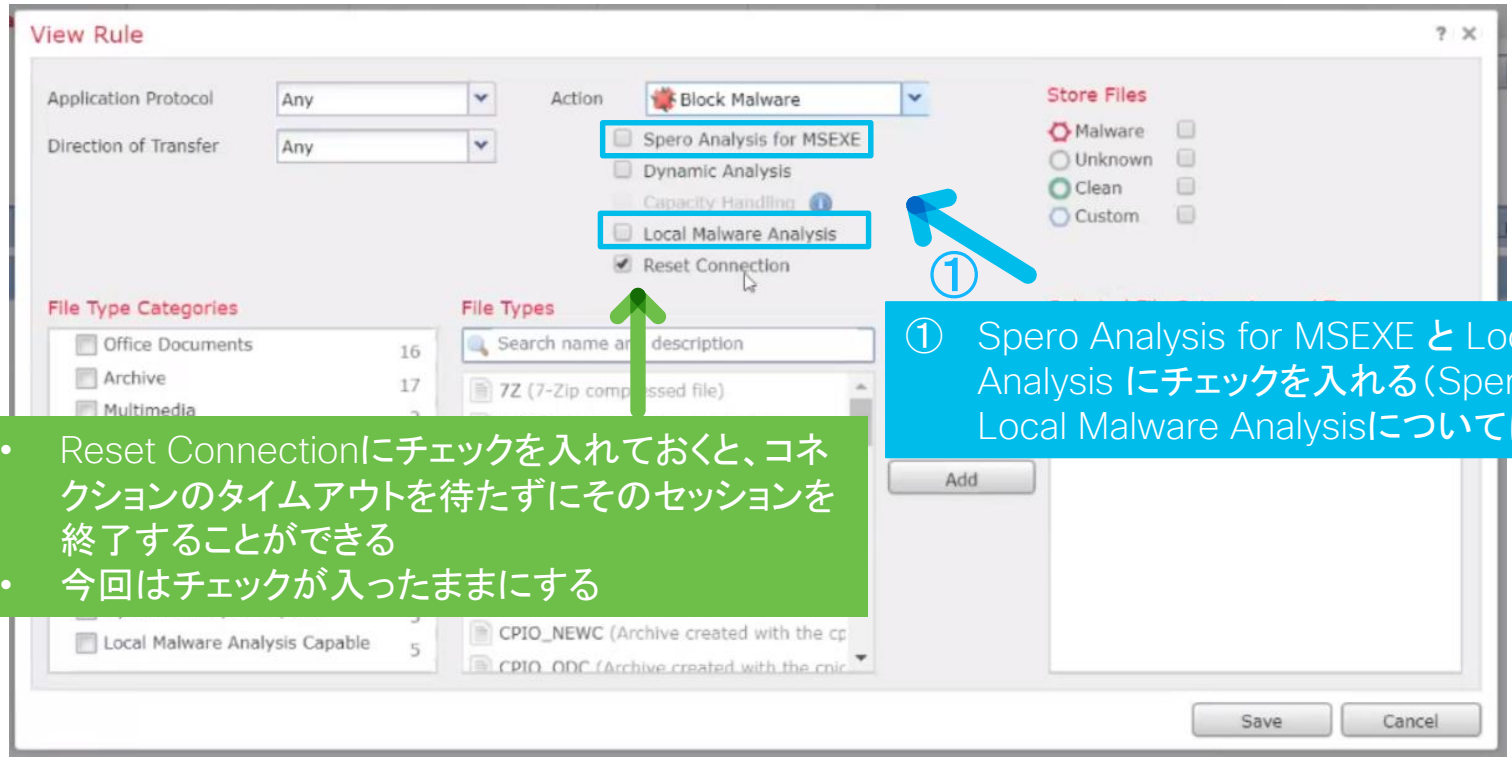
FILE-POLICYというポリシーが作成される

ステップ 2: File Ruleの作成



① Action のドロップダウンリストを開き、Block Malware を選択する

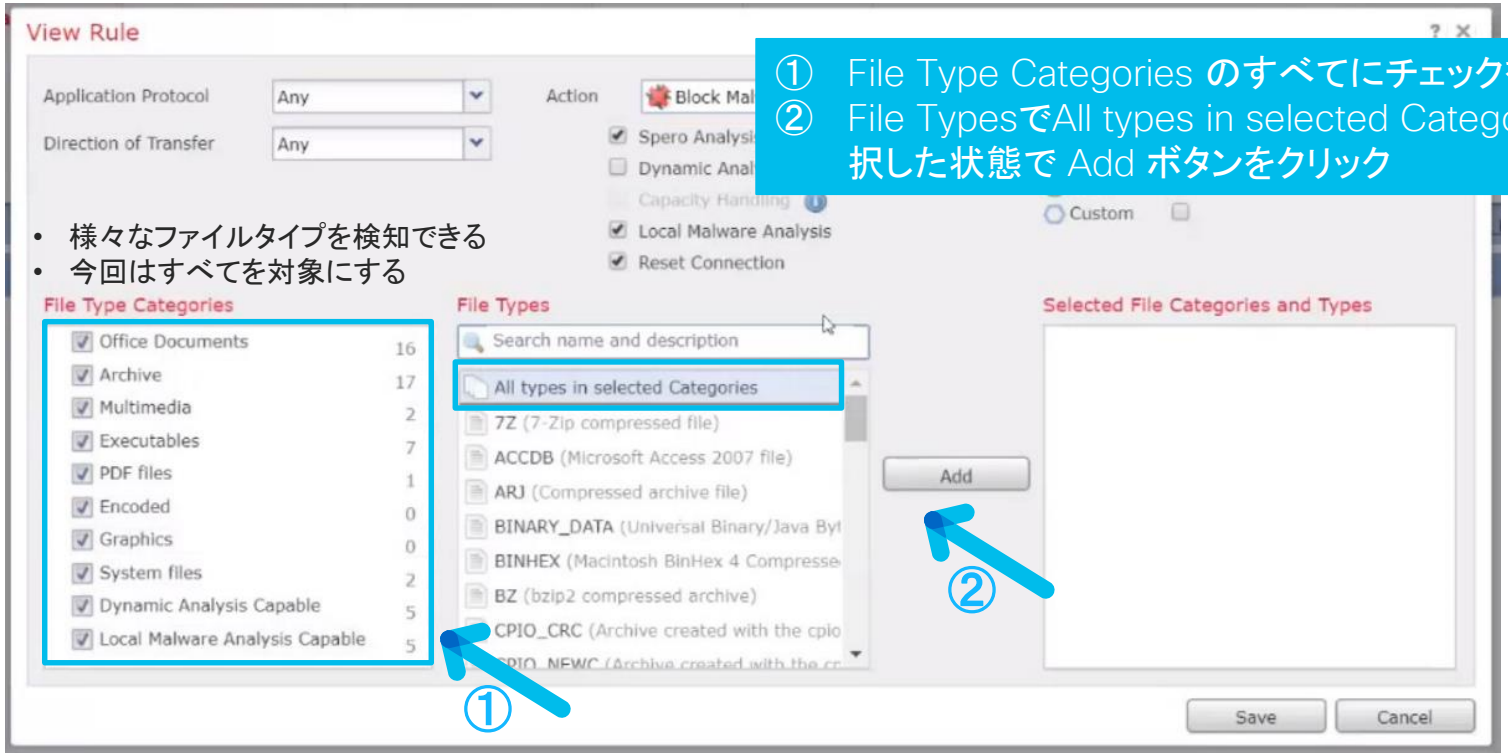
ステップ 2: File Ruleの作成



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

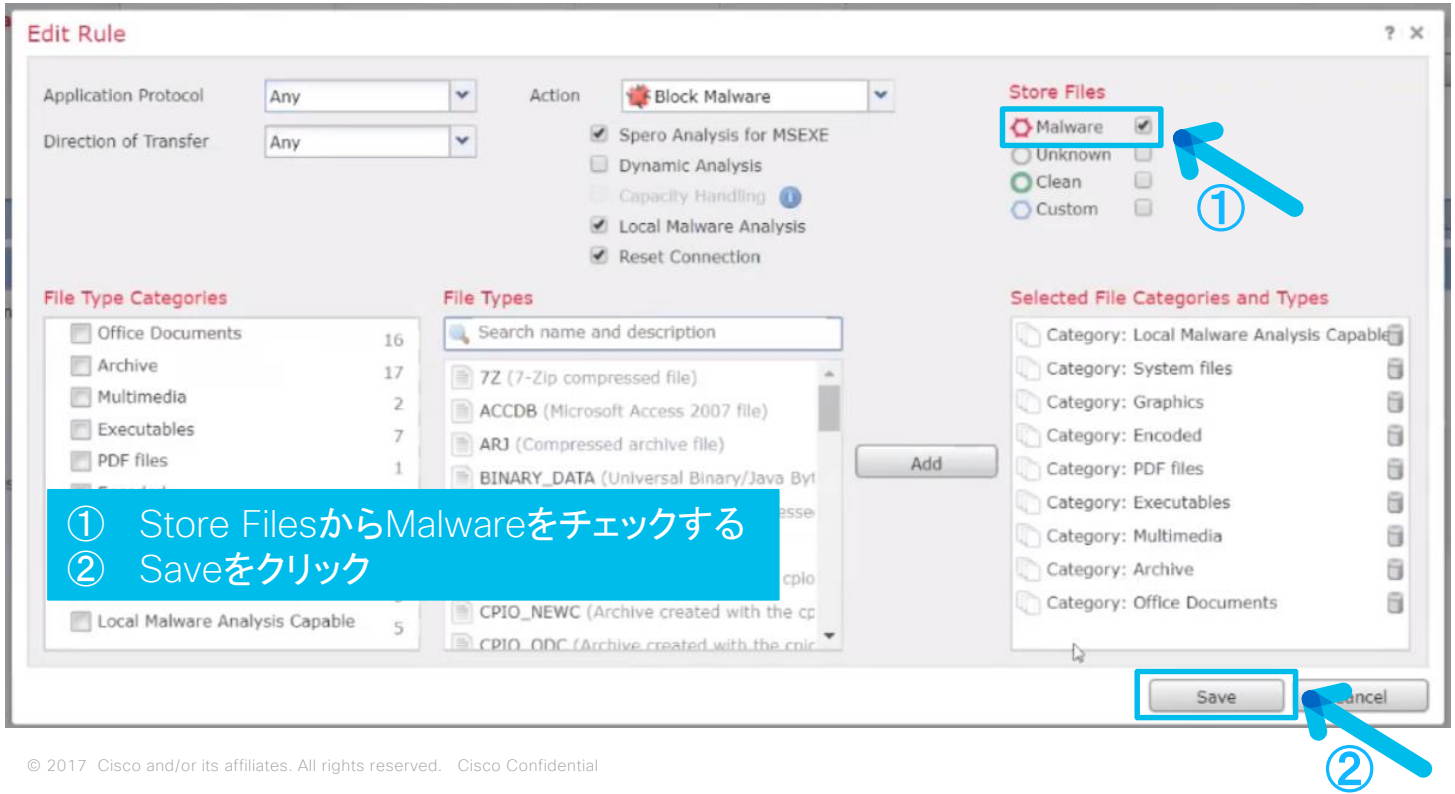
ステップ 2: File Ruleの作成



- 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

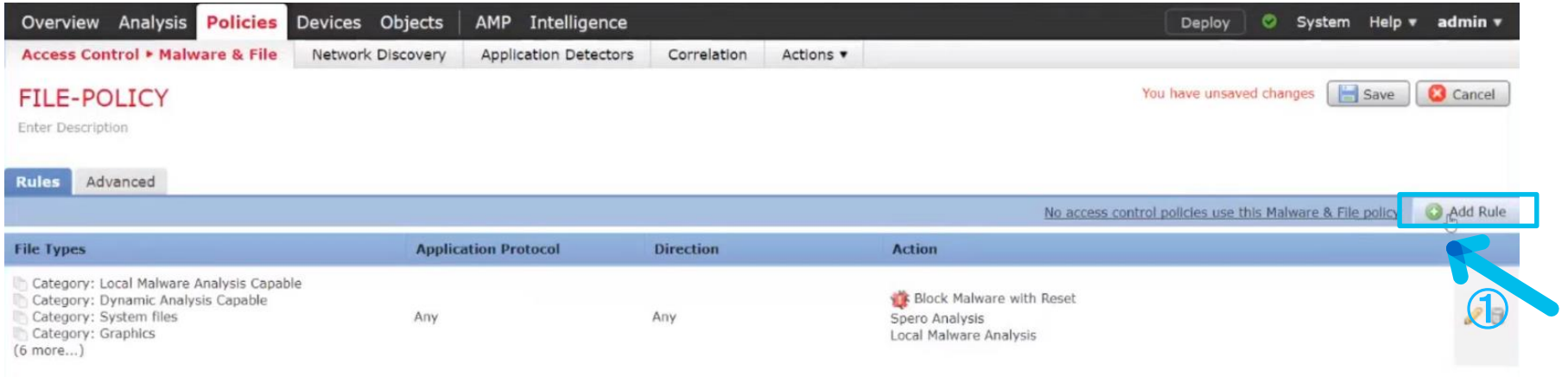
① File Type Categories のすべてにチェックを入れる
② File TypesでAll types in selected Categoriesを選択した状態で Add ボタンをクリック

ステップ 2: File Ruleの作成



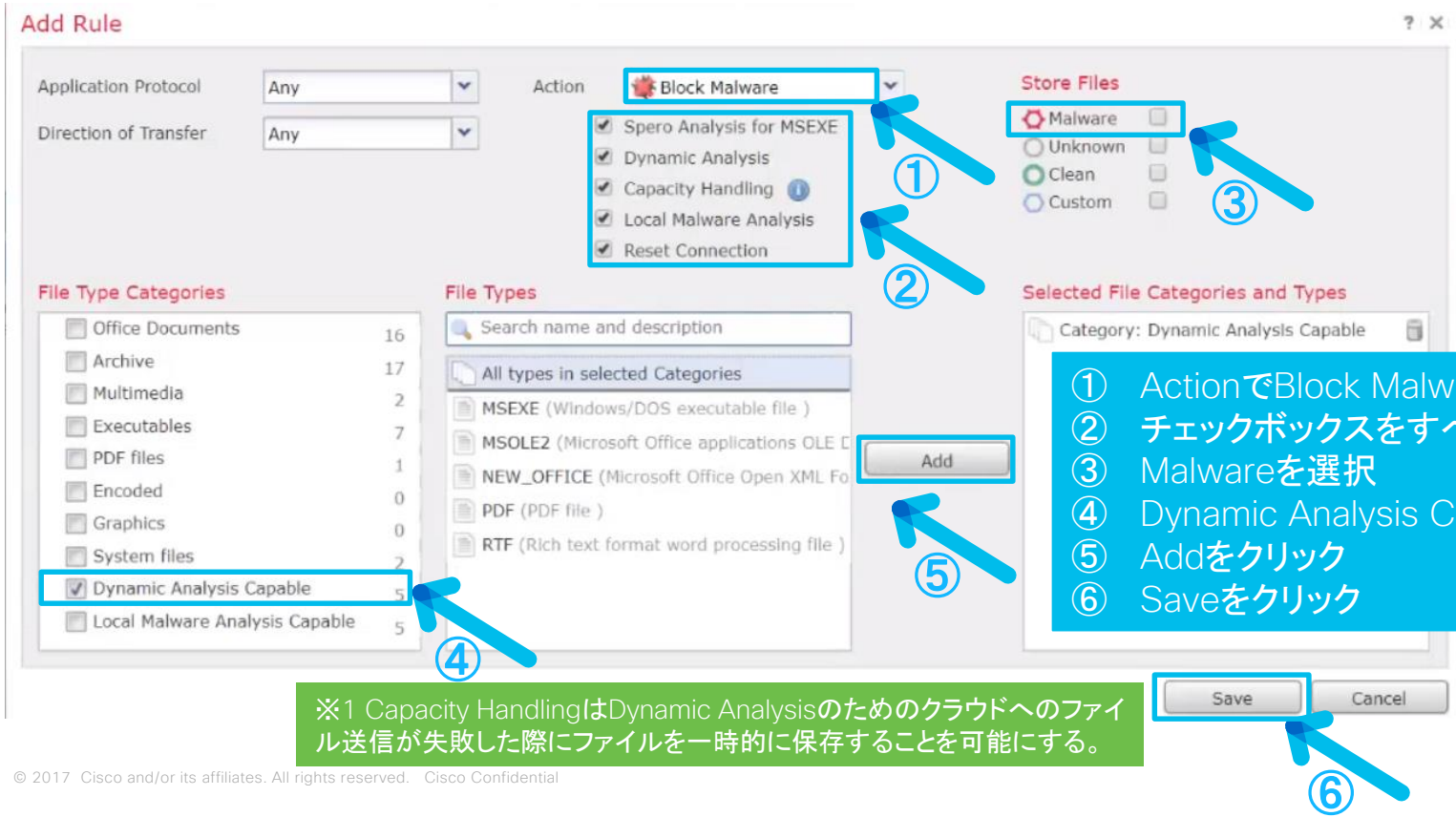
- 先のスライドで選択したファイルカテゴリ・タイプが追加される

ステップ 3: File Rule(二つ目)の作成



① Add Ruleをクリック

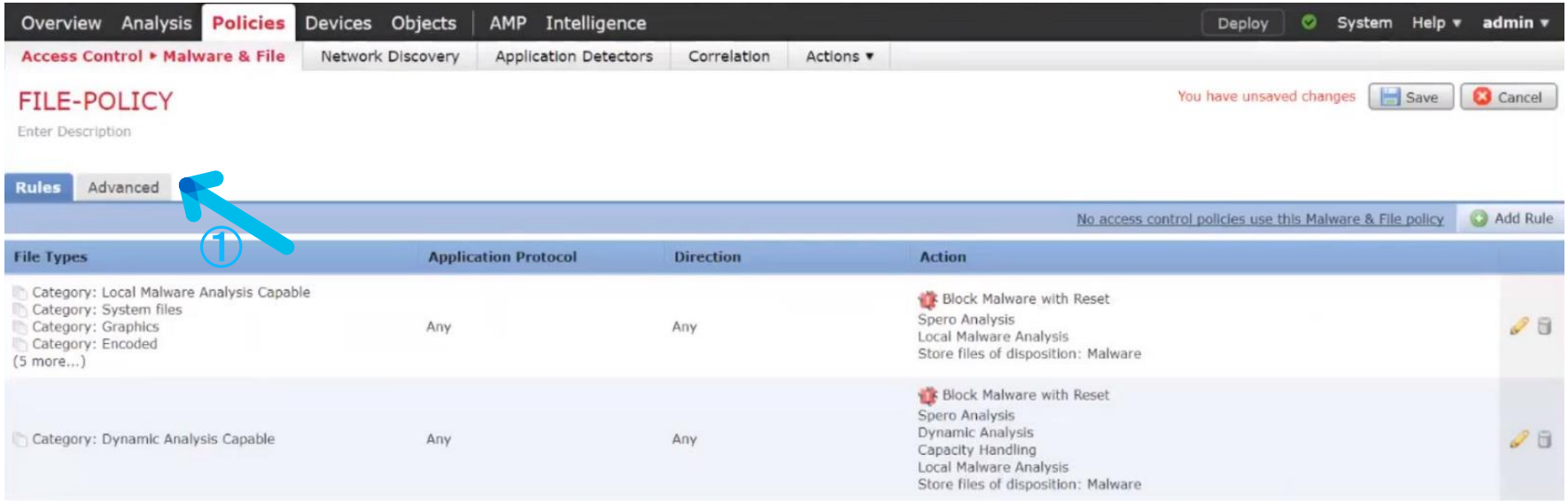
ステップ 3: File Rule(二つ目)の作成



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

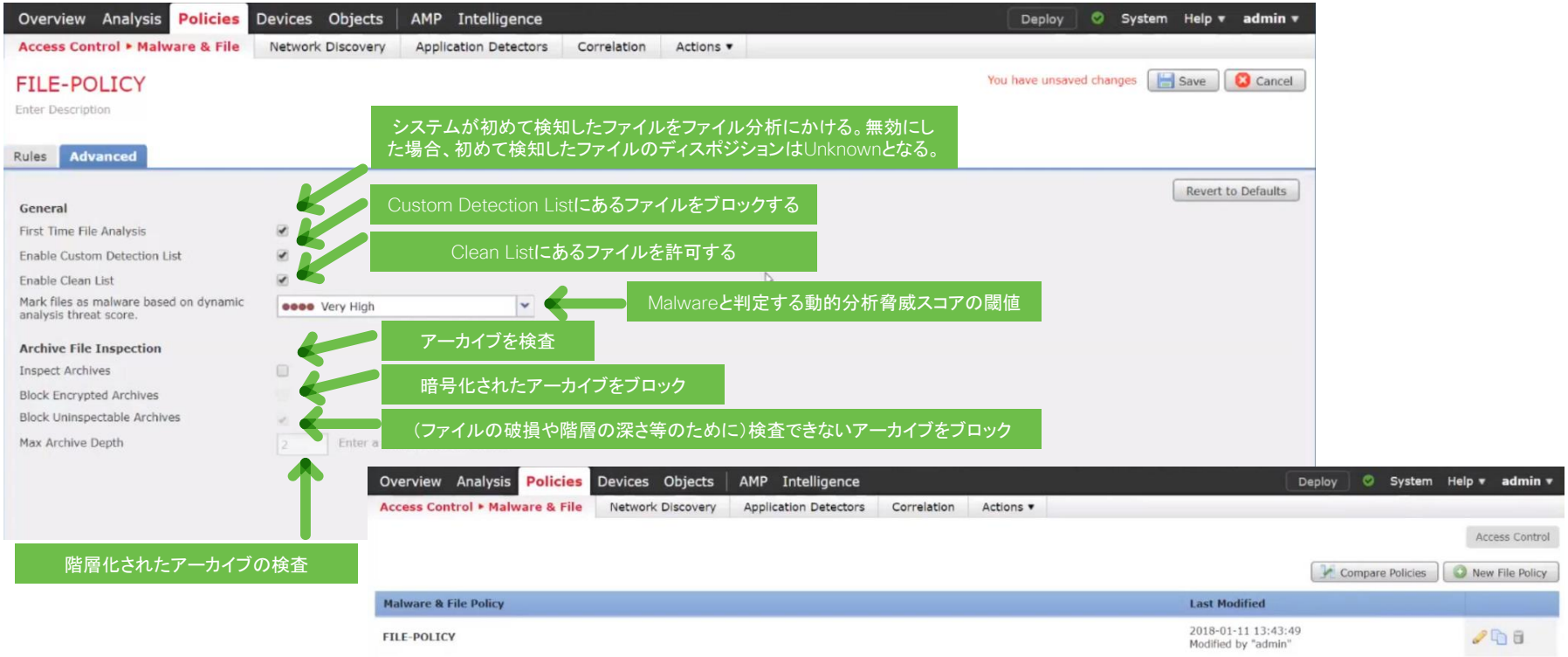
※1 Capacity HandlingはDynamic Analysisのためのクラウドへのファイル送信が失敗した際にファイルを一時的に保存することを可能にする。

ステップ 4: Advancedタブの確認とFile Policy保存



① 今回は設定しないが、Advancedをクリックして確認

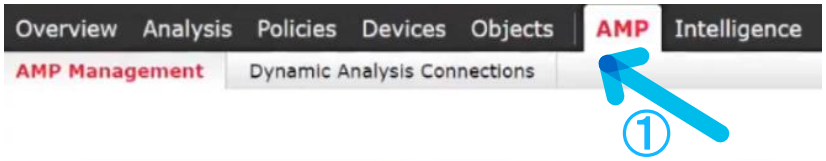
ステップ 4: Advancedタブの確認とFile Policy保存



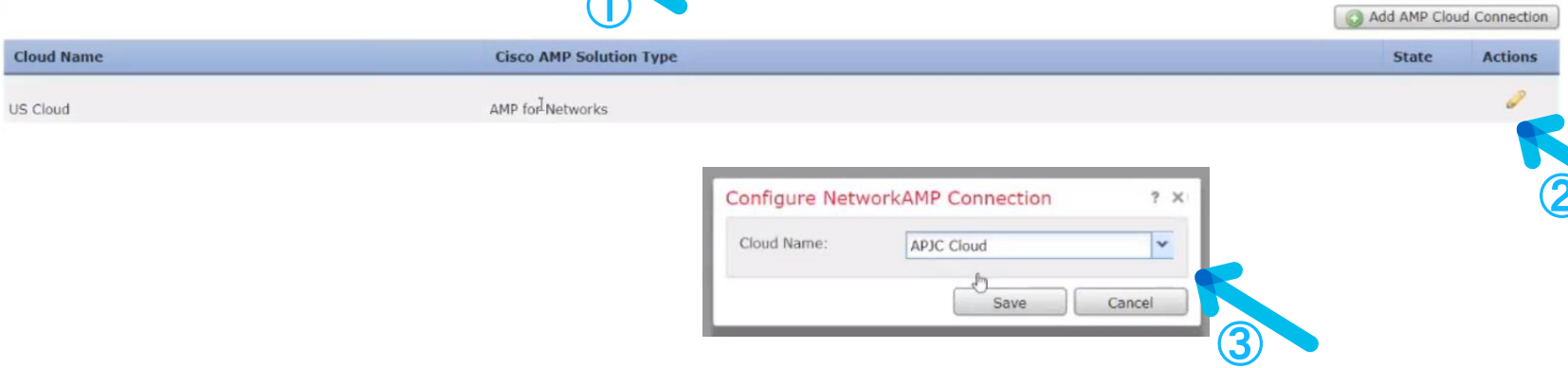
ステップ 4: Advancedタブの確認とFile Policy保存

以上で、Malware & File Policyが完成

ステップ 5: AMP Cloudの設定



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



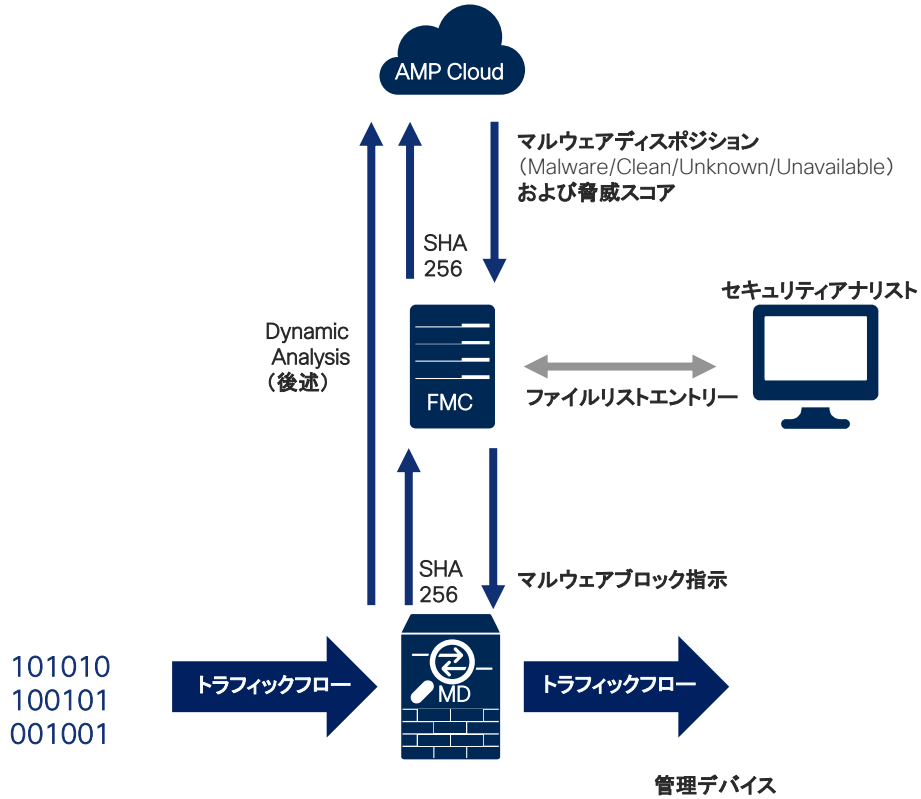
ステップ 5: AMP Threat Gridの設定 (確認)

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。

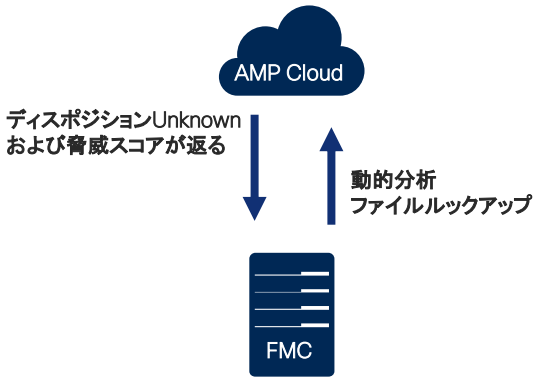
1. ファイル・アーカイブを展開、ファイルハッシュ(SHA-256)は管理デバイス側で計算される
2. 管理デバイスがローカルのキャッシュを参照しディスポジションを確認する
3. キャッシュにマルウェアディスポジションが存在しない場合、そのハッシュ値がFMCに送られ、今度はFMCのキャッシュが確認される
4. FMCのキャッシュにもディスポジションがない場合そのハッシュ値をAMP Cloudでルックアップする
5. AMP Cloudからディスポジションが返り、FMC、管理デバイスのキャッシュにディスポジションが登録される
6. ディスポジションがUnknownだった場合、オプションで更なる解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



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

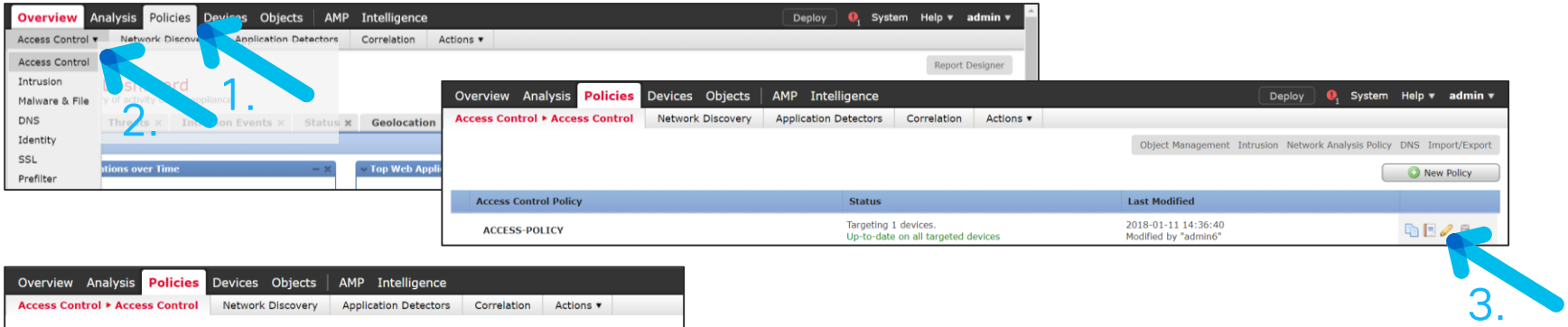
- Security Intelligence によって配信されるネットワークおよび URL の Blacklist はブロックする
- Access Control Policy では、第 3 – 4 章で作成した Intrusion Policy と File Policy を使用してセキュリティチェックを行う
- 通信の始まりと終わりのログを取得する
- Web トラフィックは URL カテゴリーを記録する

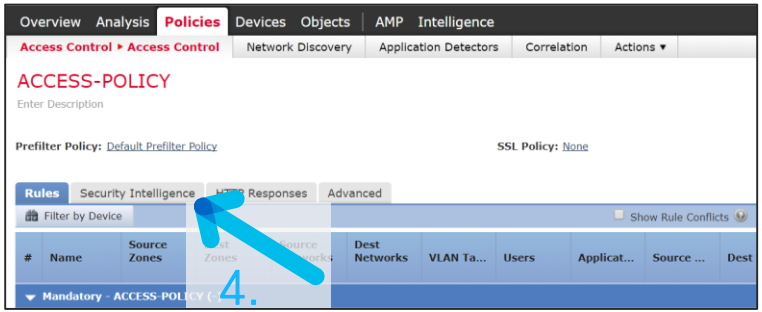
ステップ 1: Security Intelligence の設定

- 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

ステップ 1-1: Security Intelligence の設定

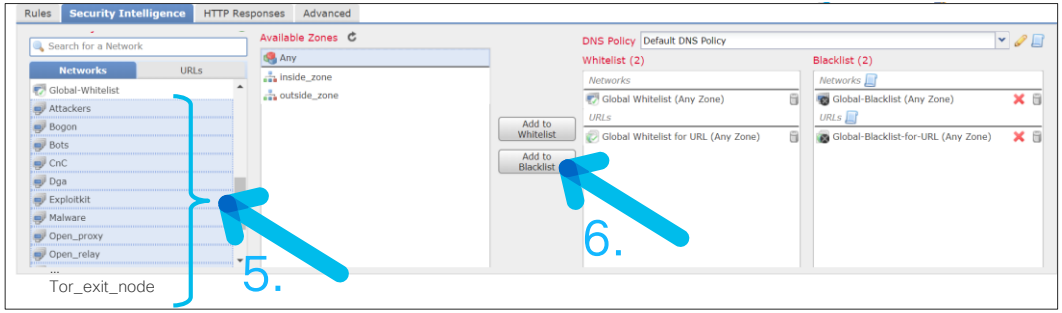
- Security Intelligenceにヒットした通信をブロックする設定を行う

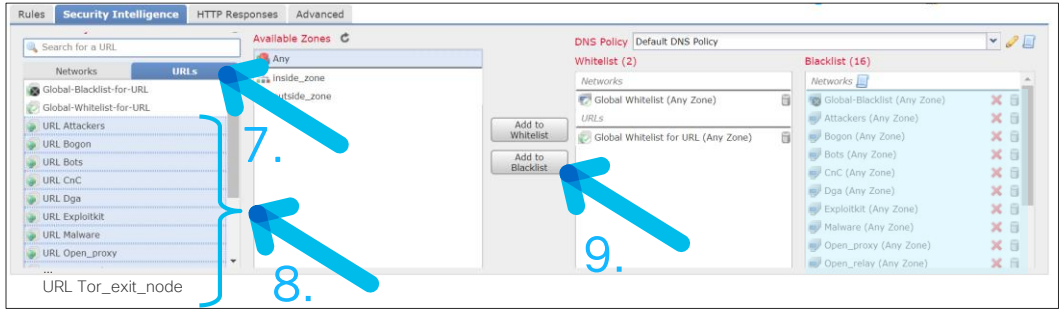




1. GUI の上部にある Policies を選択
2. Access Control のドロップダウンリストを開き、Access Control を選択
3. 第1章で作成済みの ACCESS-POLICY の鉛筆マーク ( ) を選択
4. Security Intelligence を選択
   引き続き、次のスライドを参照

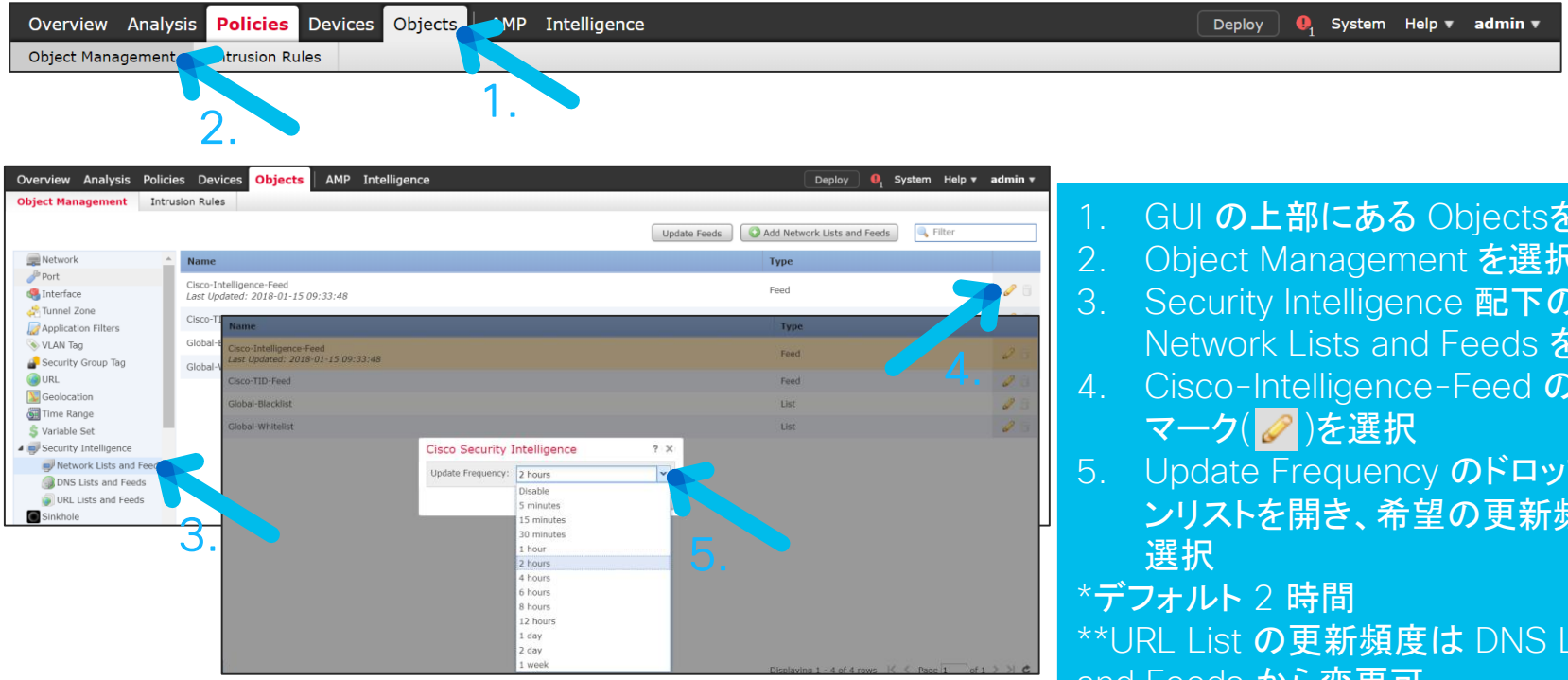
ステップ 1-2: Security Intelligence の設定





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

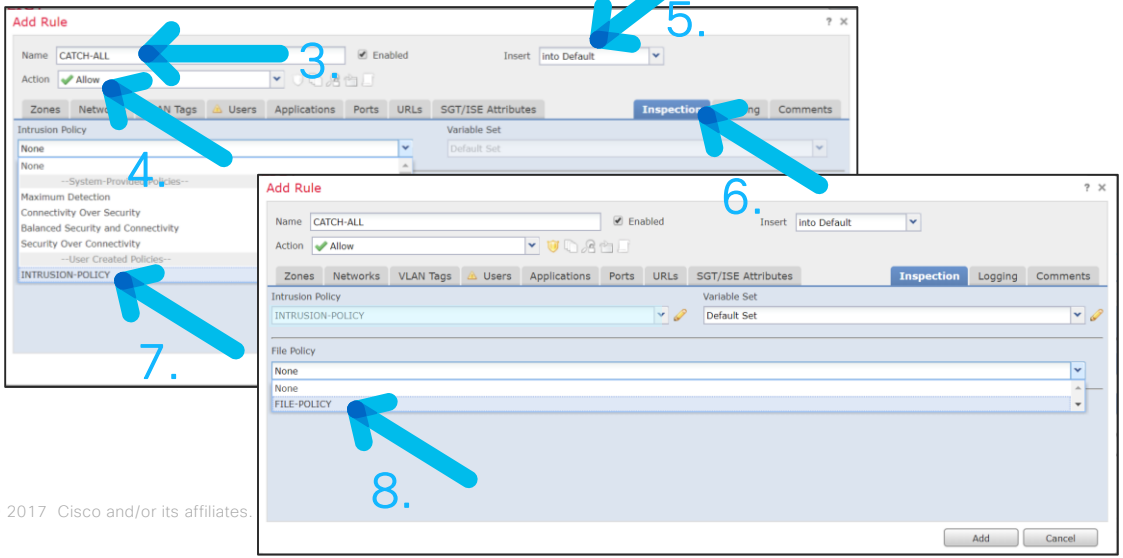


1. GUI の上部にある Objectsを選択
2. Object Management を選択
3. Security Intelligence 配下の Network Lists and Feeds を選択
4. Cisco-Intelligence-Feed の鉛筆マーク( )を選択
5. Update Frequency のドロップダウンリストを開き、希望の更新頻度を選択

*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

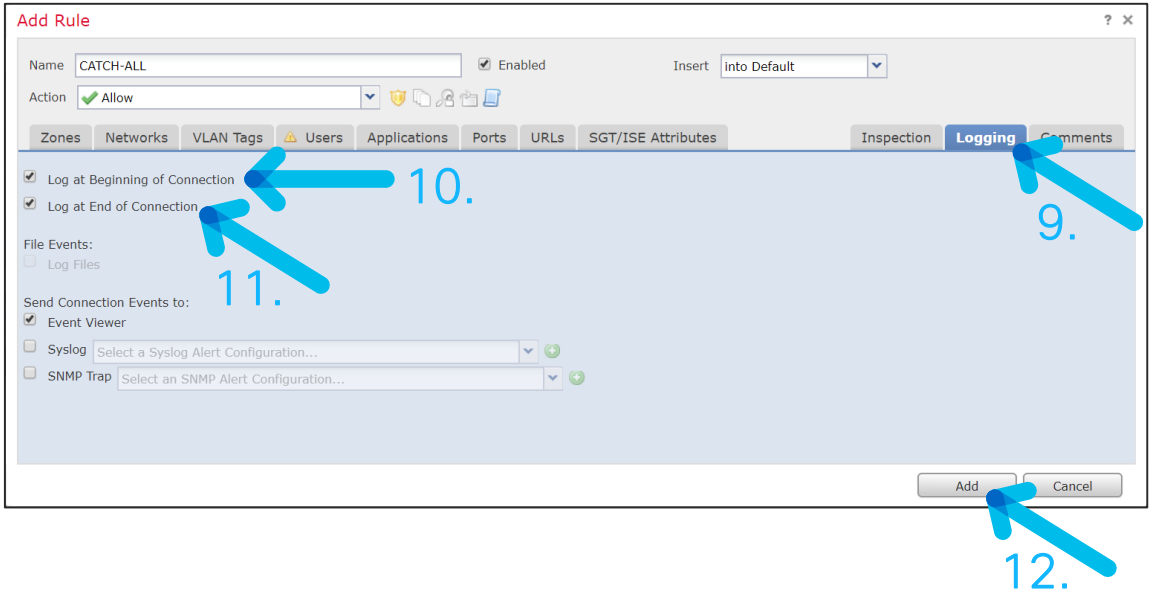
- **全ての通信に対し、第3章で作成したIntrusion Policyと第4章で作成したFile Policyを適用**



1. Rules タブを選択
2. Add Rule を選択
3. 任意の名前 を選択
4. Action のドロップダウンリストを開き、Allow を選択
5. Insert: into Default を選択
6. Inspection タブを選択
7. 第 3 章で作成した INTRUSION-POLICY を選択
8. 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

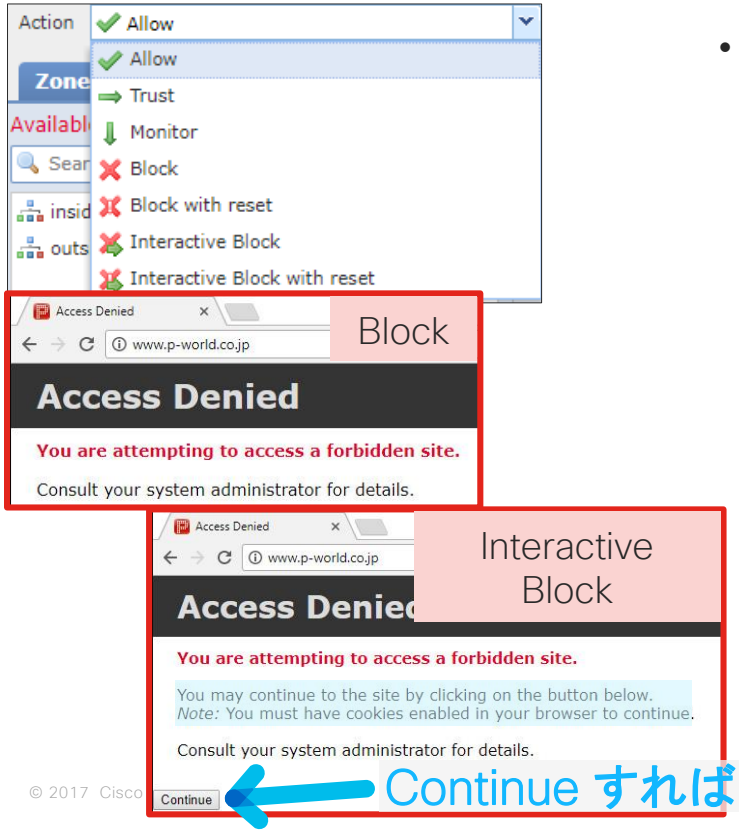
ステップ 2-2: Access Rule の設定



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

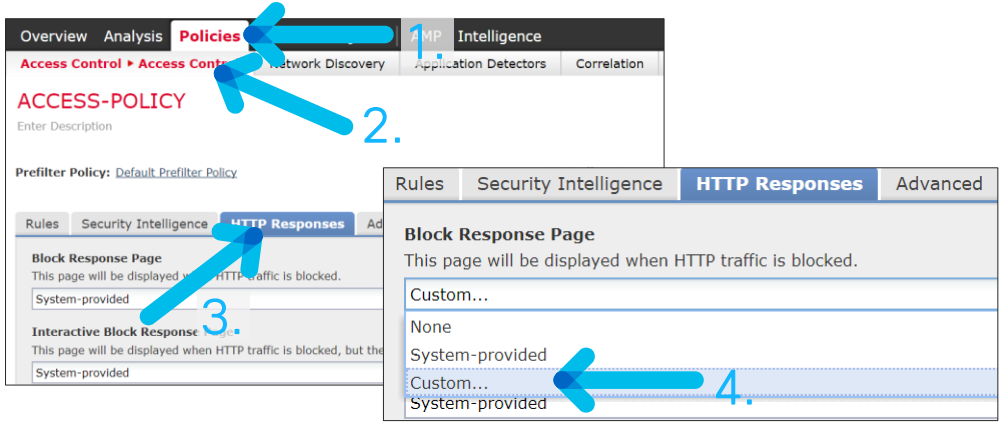
以上で、AMP ルールを適用した Access Control Policy の設定は完了

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

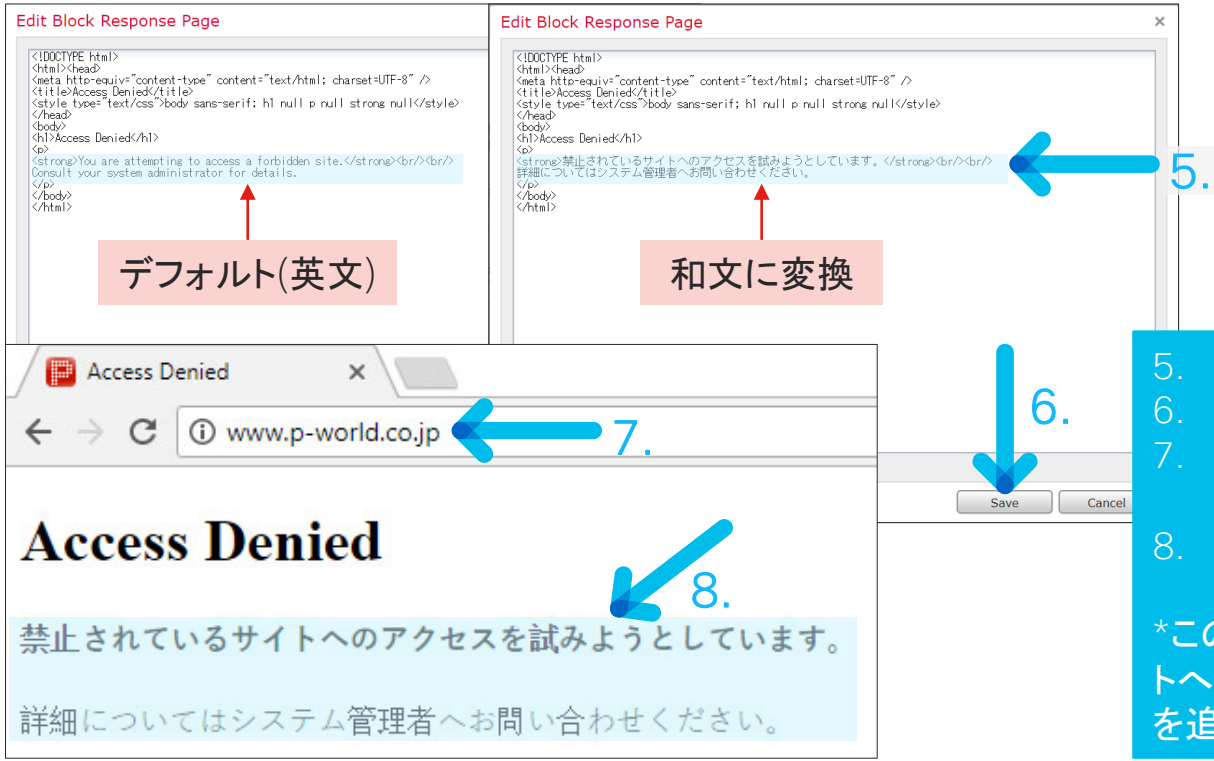
参考: Block 時のHTTP Response ページの編集 (1)



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)

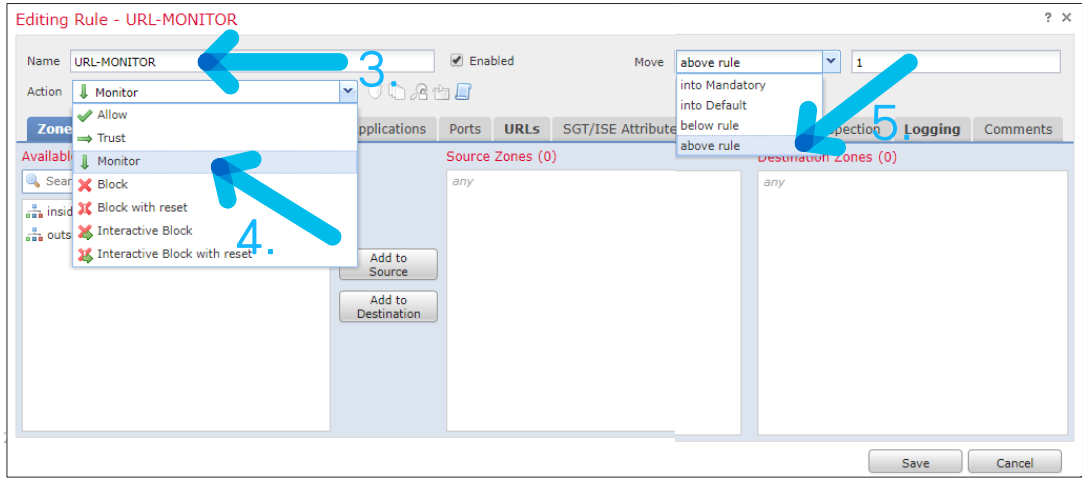


5. 任意の文章に変更 (HTML形式)
6. Save を選択
7. 仮想端末から Block されているサイトへアクセス
8. レスポンスが和文になっていることを確認

*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

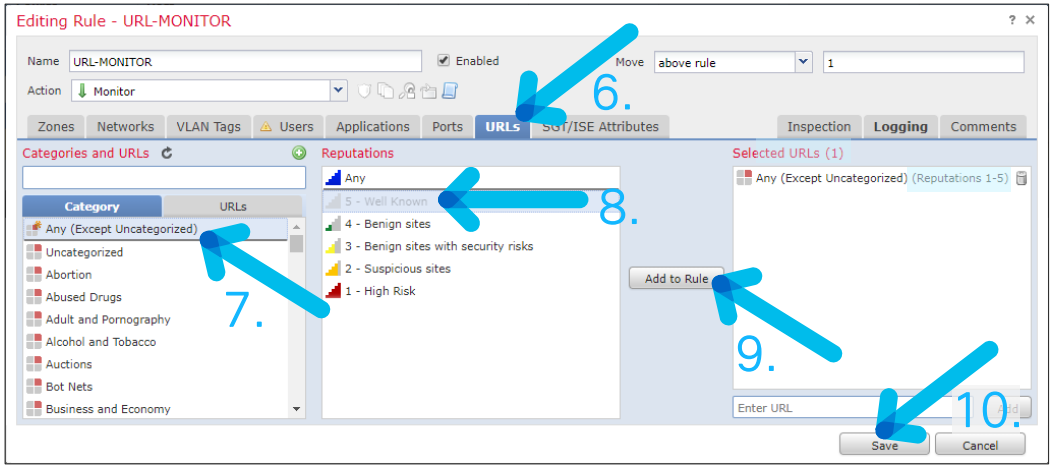
ステップ 3-1: URL Category Monitor の設定

- **全ての通信に対し、URLカテゴリのロギングを行うRuleを追加**



1. Rules タブを選択
2. Add Rule を選択
3. 任意の名前 を選択
4. Action のドロップダウンリストを開き、Monitor を選択
5. 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

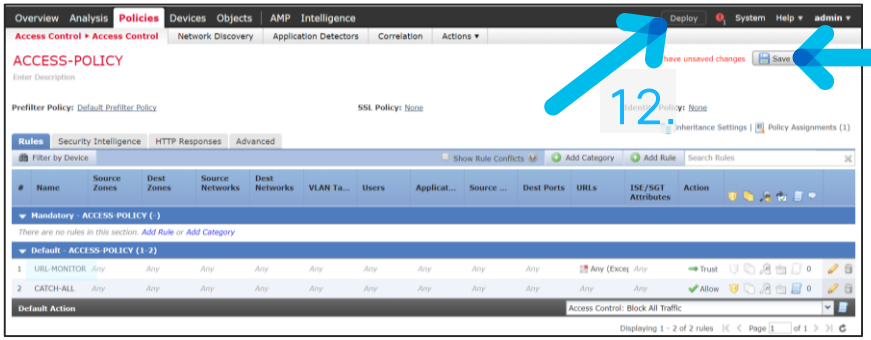
ステップ 3-2: URL Category Monitor の設定

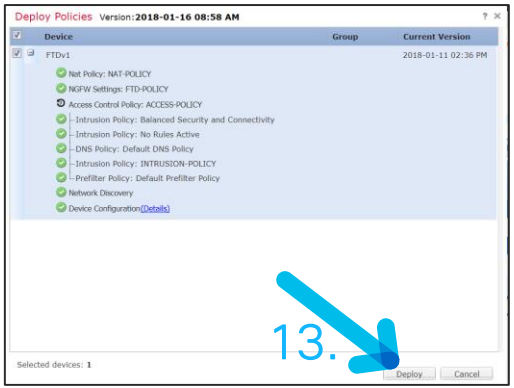


6. URLs タブを選択
7. Any (Except Uncategorized) を選択
8. Reputations: 5 – Well Known を選択
9. Add to Rule を選択
10. Save を選択

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



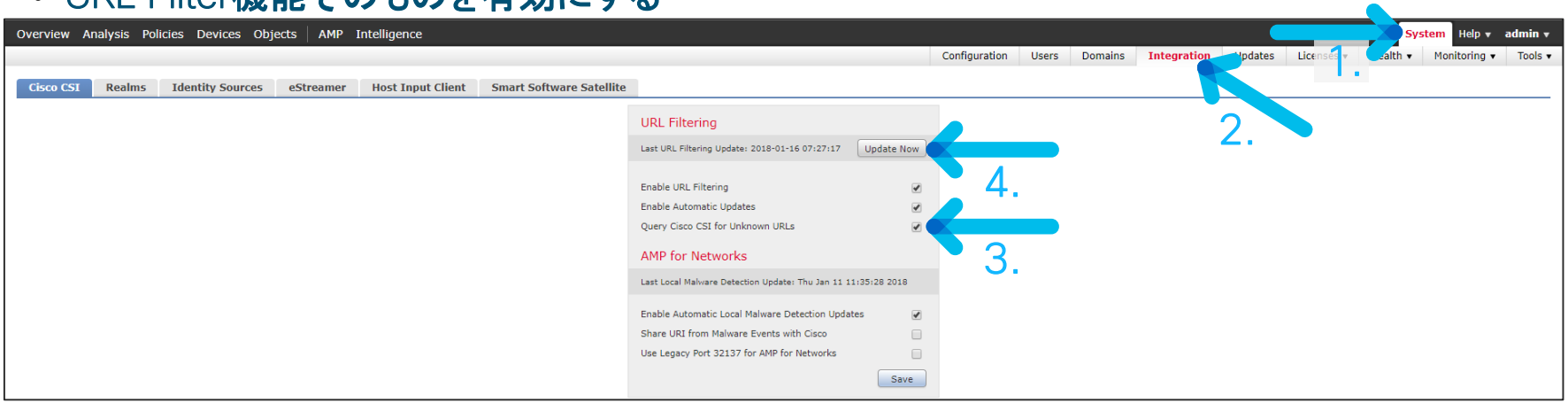


11. Save を選択
12. Deploy を選択
13. Deploy を選択

以上で、URL Monitorの設定とAccess Control Policyの適用は完了

ステップ 4: URL Filter の設定

- URL Filter機能そのものを有効にする

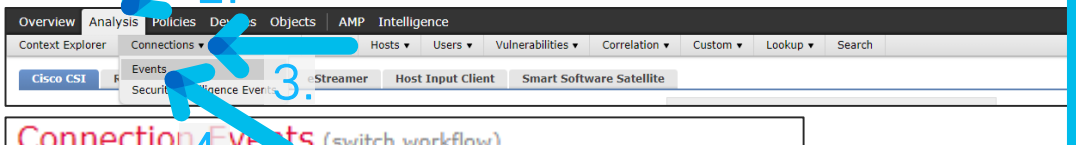


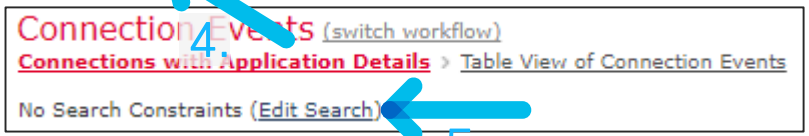
1. System タブを選択
2. Integration タブを選択
3. Query Cisco CSI for Unknown URLs にチェック
4. Update Now を選択

以上で、URL Filter の設定は完了

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 が正しくカテゴライズされるかを確認する

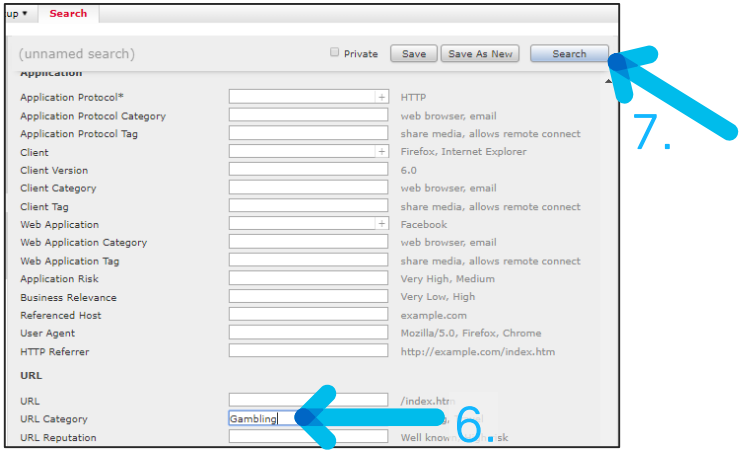




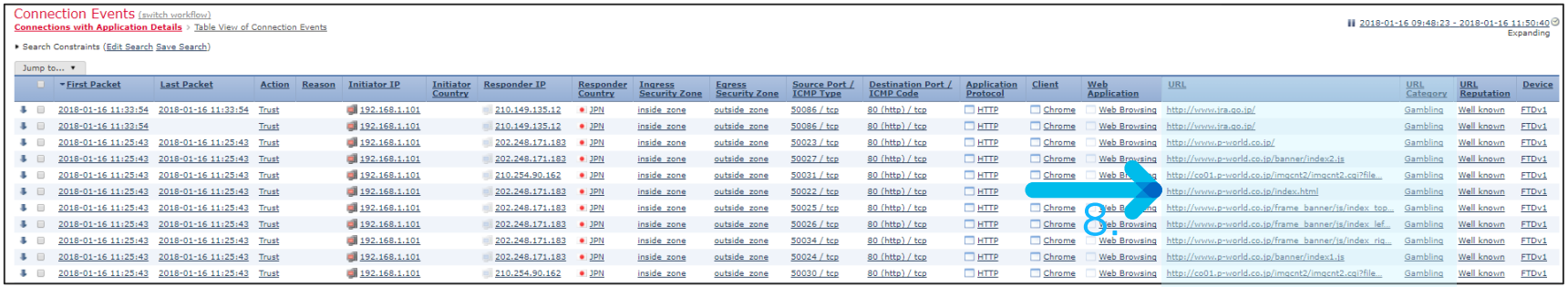
1. 仮想端末でインターネットを開き、ギャンブルサイト (例 www.p-world.co.jp、www.jra.go.jpなど) にアクセス
2. Analysis タブを選択
3. Connections を選択
4. Events を選択
5. Edit Search を選択

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



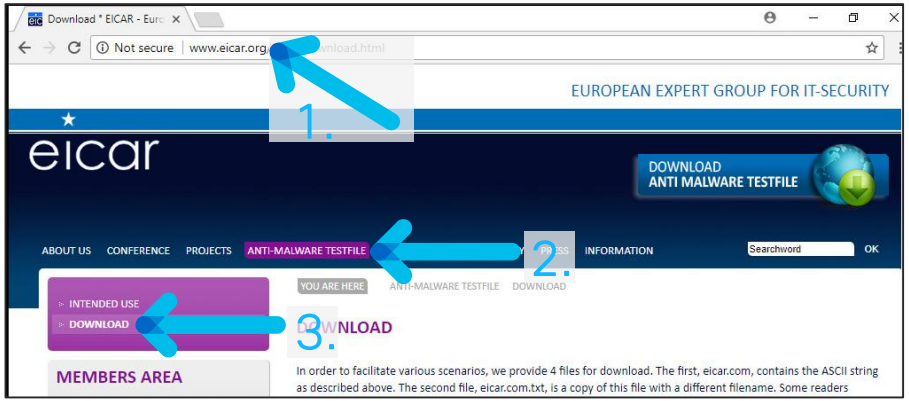
6. URL: URL Category の欄に Gambling と入力
7. Search を選択
8. 1. の 2 サイトが正しくカテゴライズされていることを確認

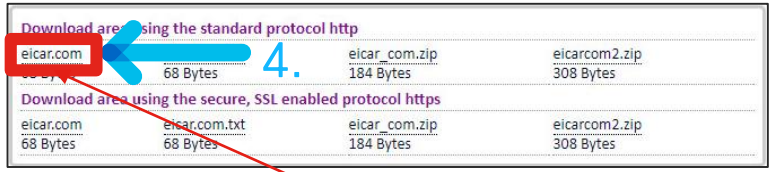


以上で、URL Filter のテストは完了

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

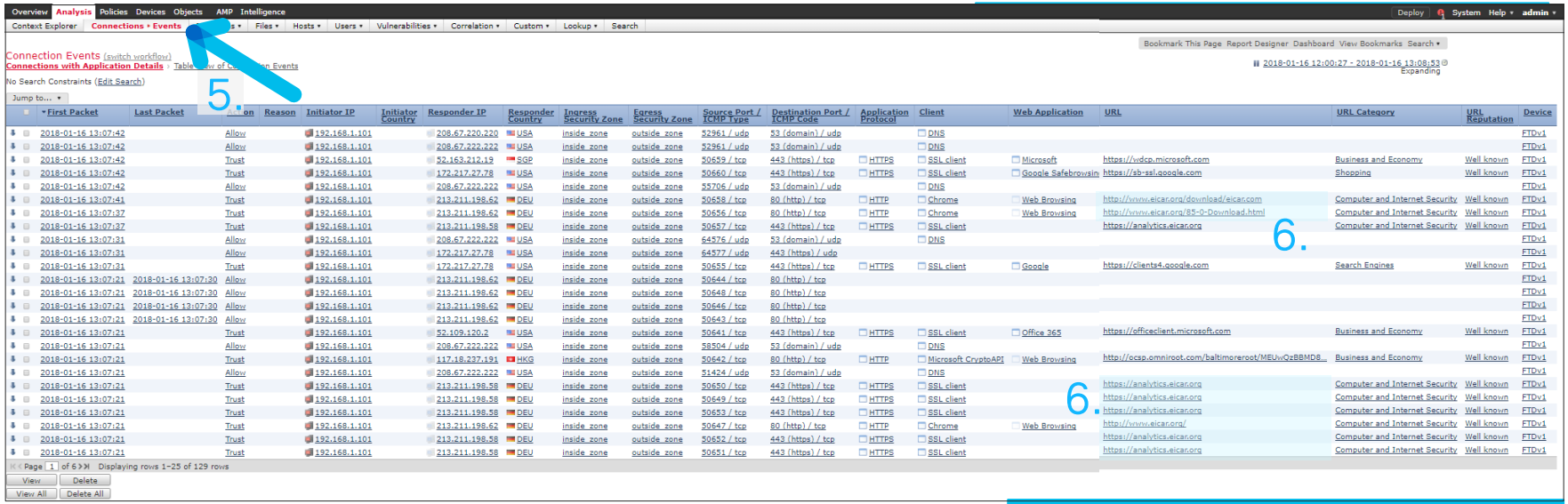




テスト用マルウェアファイル

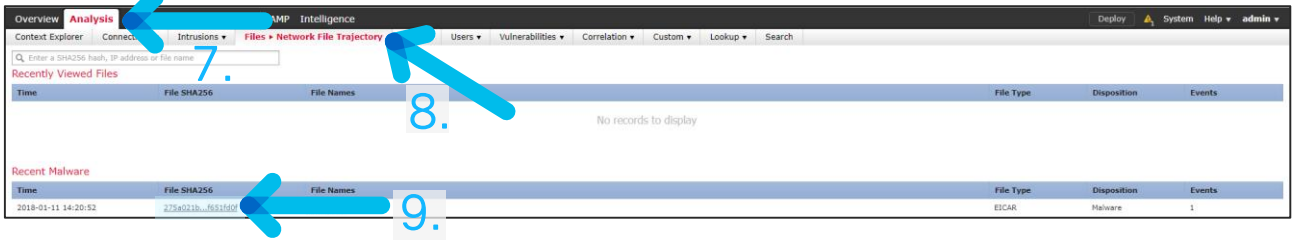
1. 仮想端末でインターネットを開き、www.eicar.org にアクセス
2. ANTI-MALWARE TESTFILE タブを選択
3. DOWNLOAD を選択
4. テスト用のマルウェアをダウンロードするために、eicar.com を選択
   引き続き、次のスライドを参照

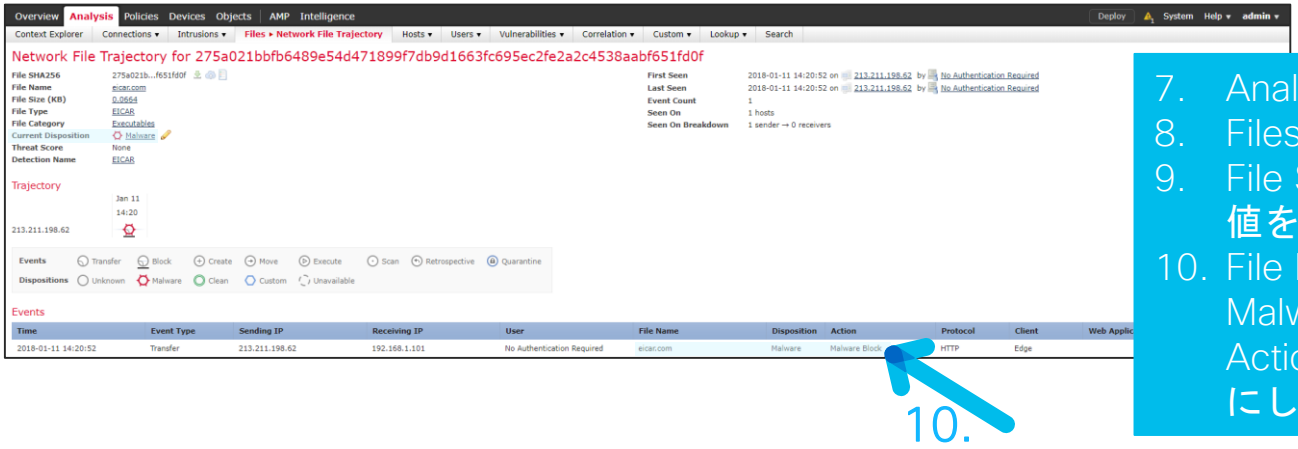
ステップ 6-2: AMP (File Policy) のテスト



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





7. Analytics を選択
8. Files > File Trajectory を選択
9. File SHA256 の欄のハッシュ値を選択
10. 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

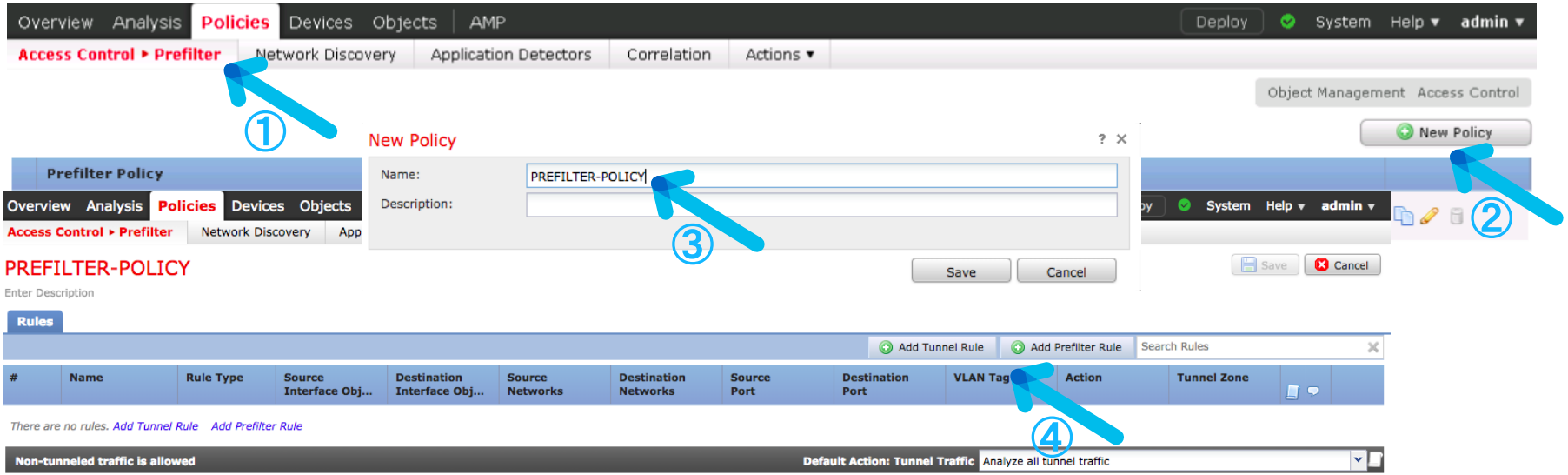
以上で、AMP (File Policy) のテストは完了

6. Pre-Filter設定

Prefilter の概要

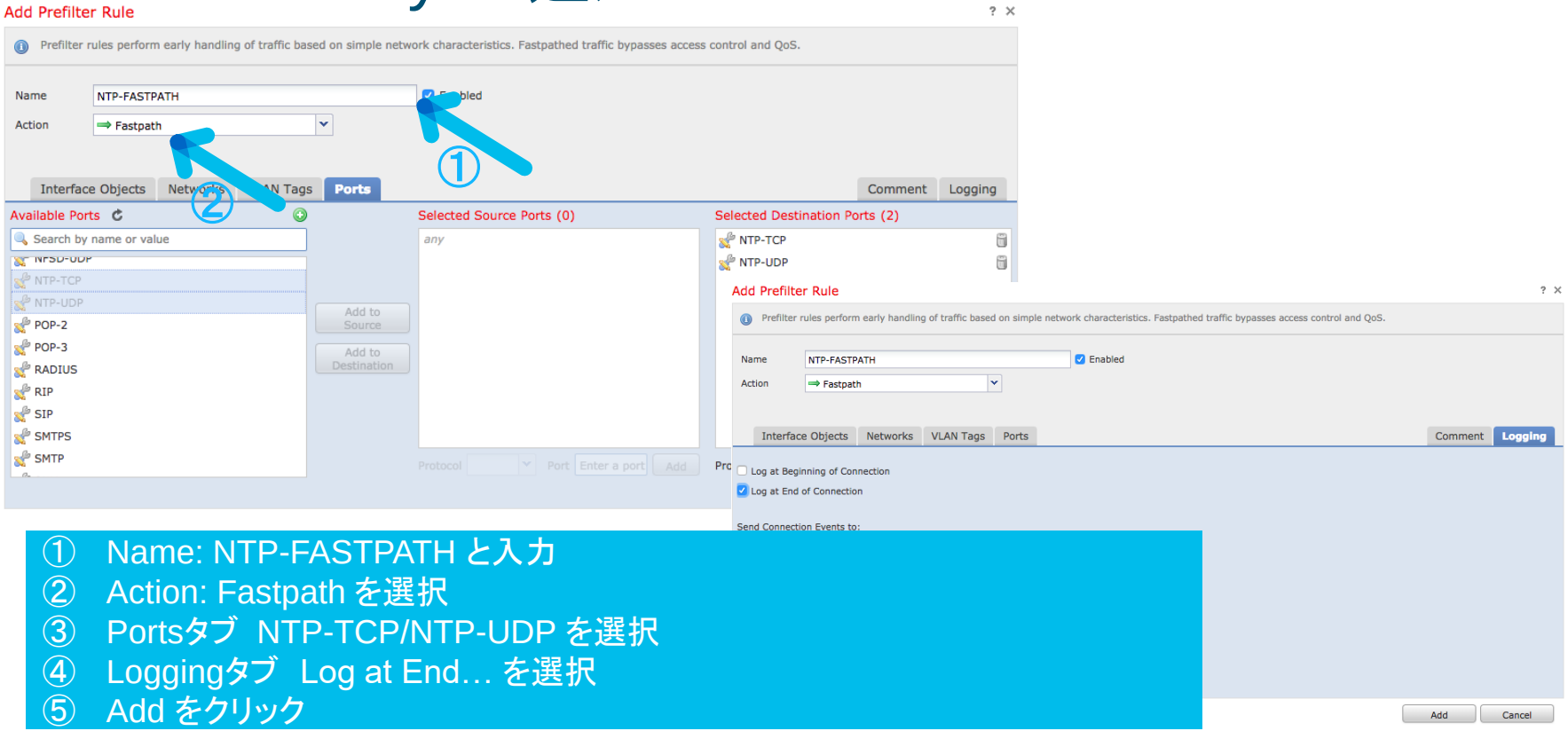
- FTD内 URL/ IPS/ AMP処理を担う Snortプロセスの前段、Lina(ASA)プロセスが パケットをハンドリングする機能
- NGIPS/NGFW機能を通す必要のない信頼されている通信(監視系・バックアップ系)などは、設計時に Prefilter Policyを通すことを推奨

Prefilter Policy の追加



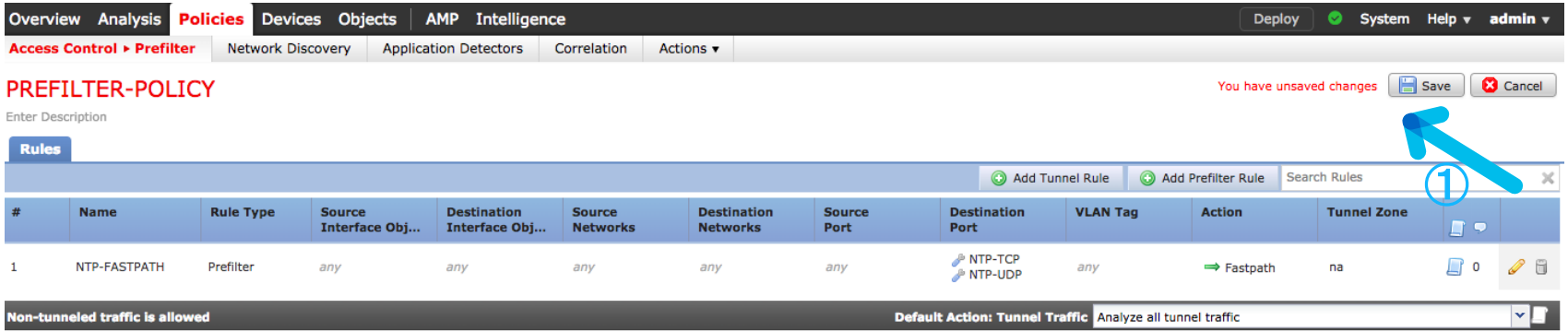
① Policies内 Access Control > Prefilter を選択
② New Policyをクリック
③ Name: PREFILTER-POLICYを入力後、Save
④ 作成Prefilter内、Add Prefilter Rule を選択

Prefilter Policy の追加



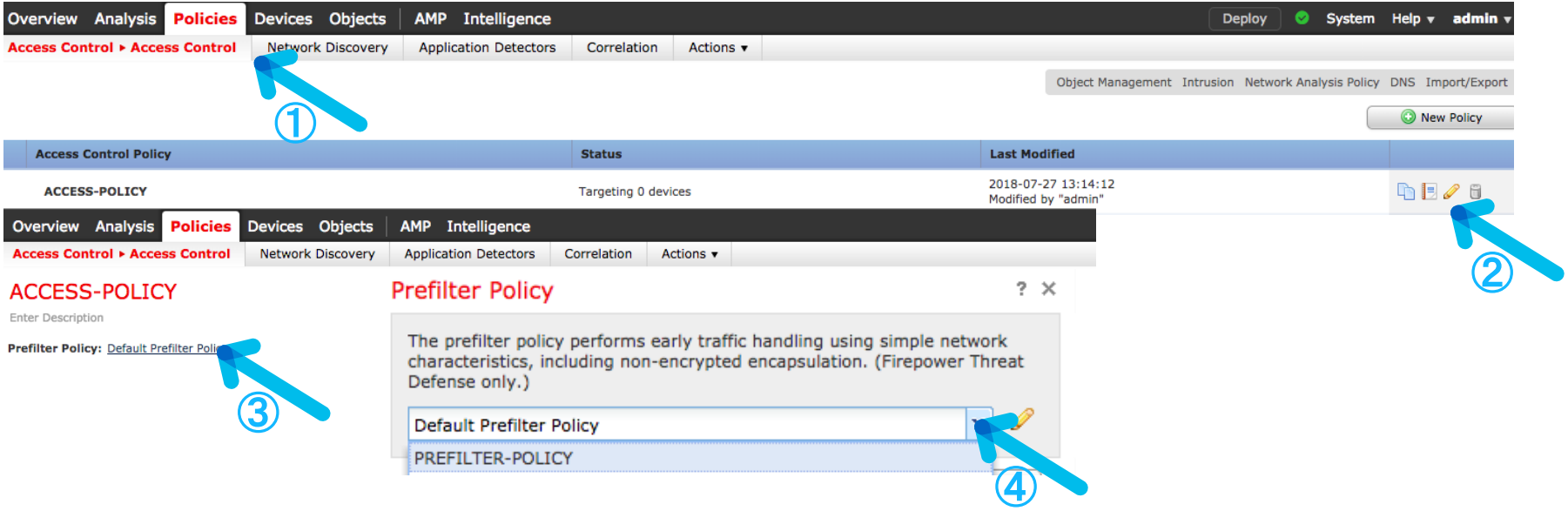
① Name: NTP-FASTPATH と入力
② Action: Fastpath を選択
③ Portsタブ　NTP-TCP/NTP-UDP を選択
④ Loggingタブ　Log at End… を選択
⑤ Add をクリック

Prefilter Policy の追加



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

Prefilter Policy の設定

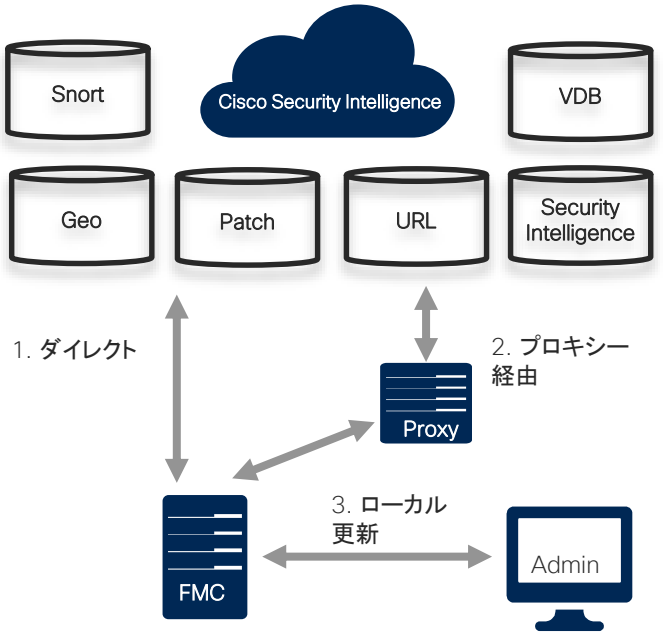


① Policies内 Access Controlを選択
② 作成済み Access Control Policy: ACCESS-POLICYの鉛筆マークをクリック
③ Access Control Policy 内 Prefilter Policyをクリック
④ Prefilter Policy: PREFILTER-POLICYを選択、OKをクリック
⑤ Save を選択後、Deploy

以上で、Pre-filterの設定は完了

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マネージメントIPが閉域ネットワーク環境

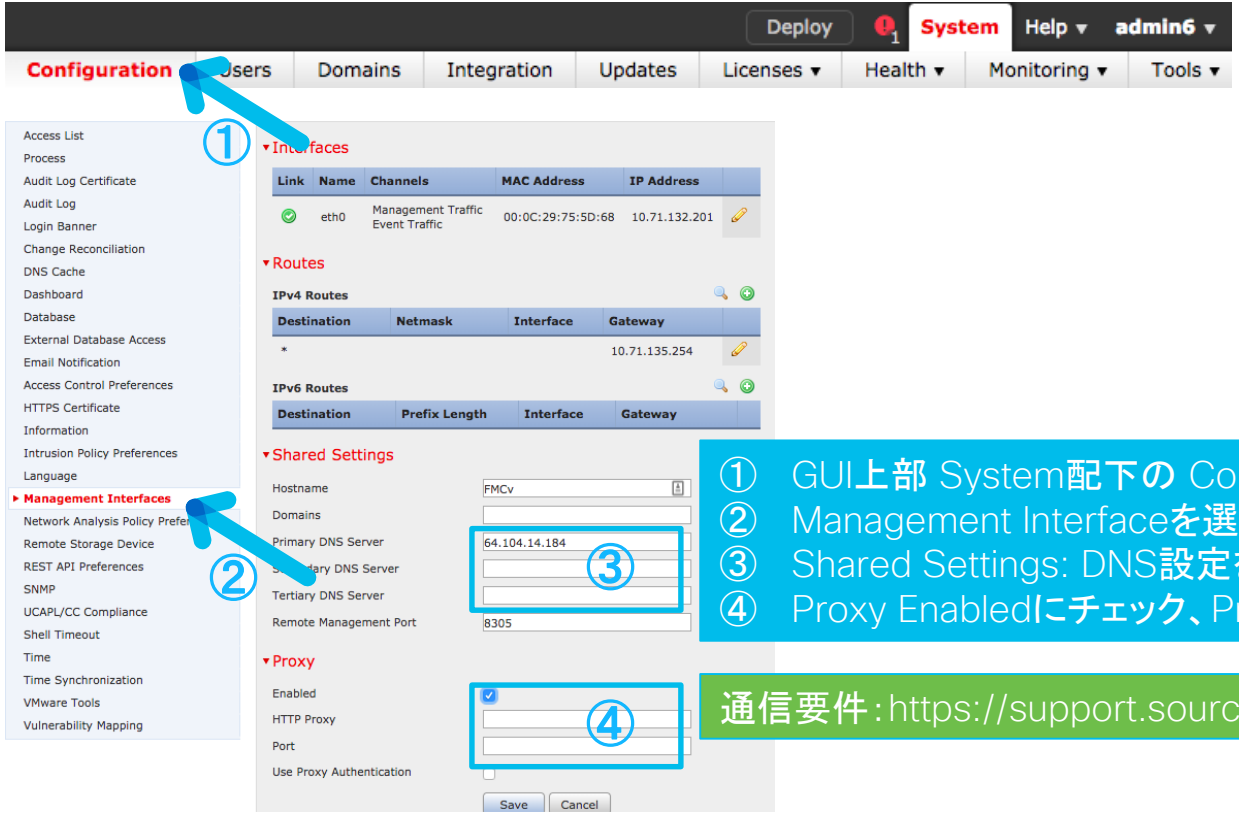
制限事項:URL, Security Intelligence以外はローカル更新可能

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	ourcefire_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



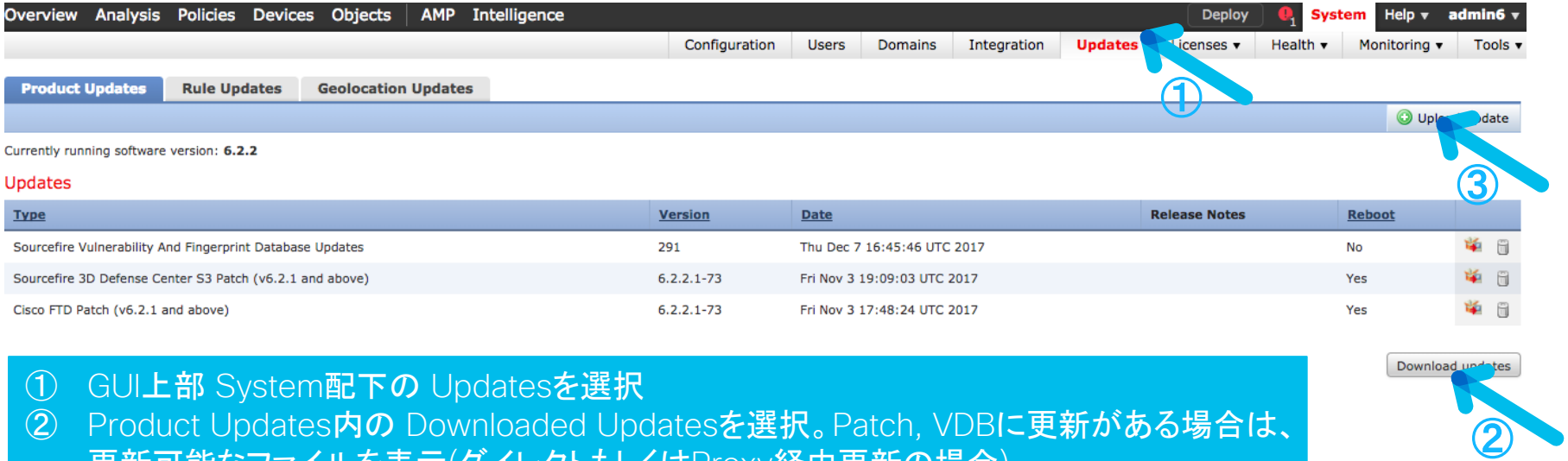
① GUI上部 System配下の Configurationを選択
② Management Interfaceを選択
③ Shared Settings: DNS設定を確認
④ Proxy Enabledにチェック、Proxy設定を入力（プロキシ利用時）

通信要件：https://support.sourcefire.com

ローカル更新用パッケージ準備

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

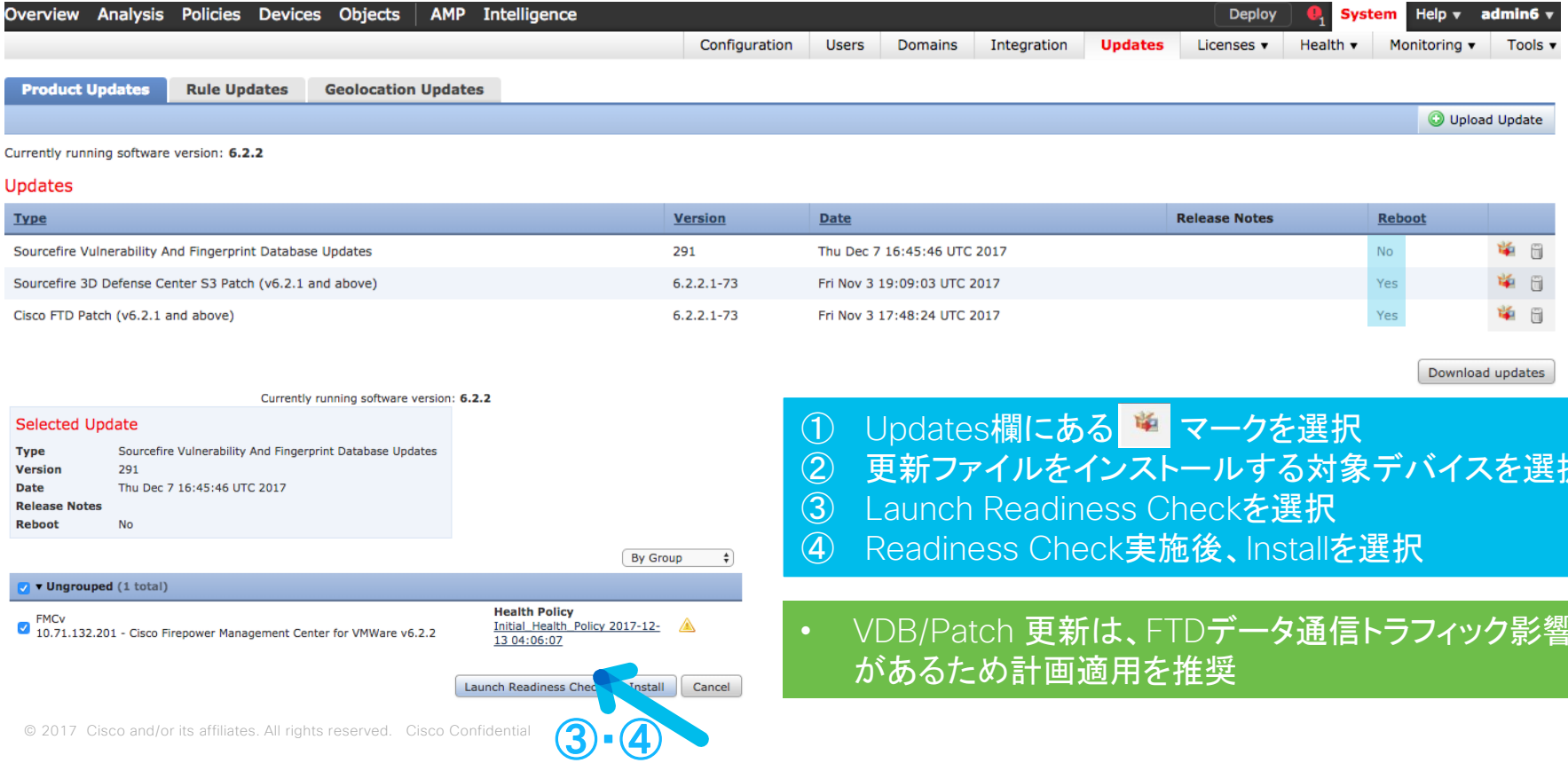
VDB/Patch ワンタイム更新



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

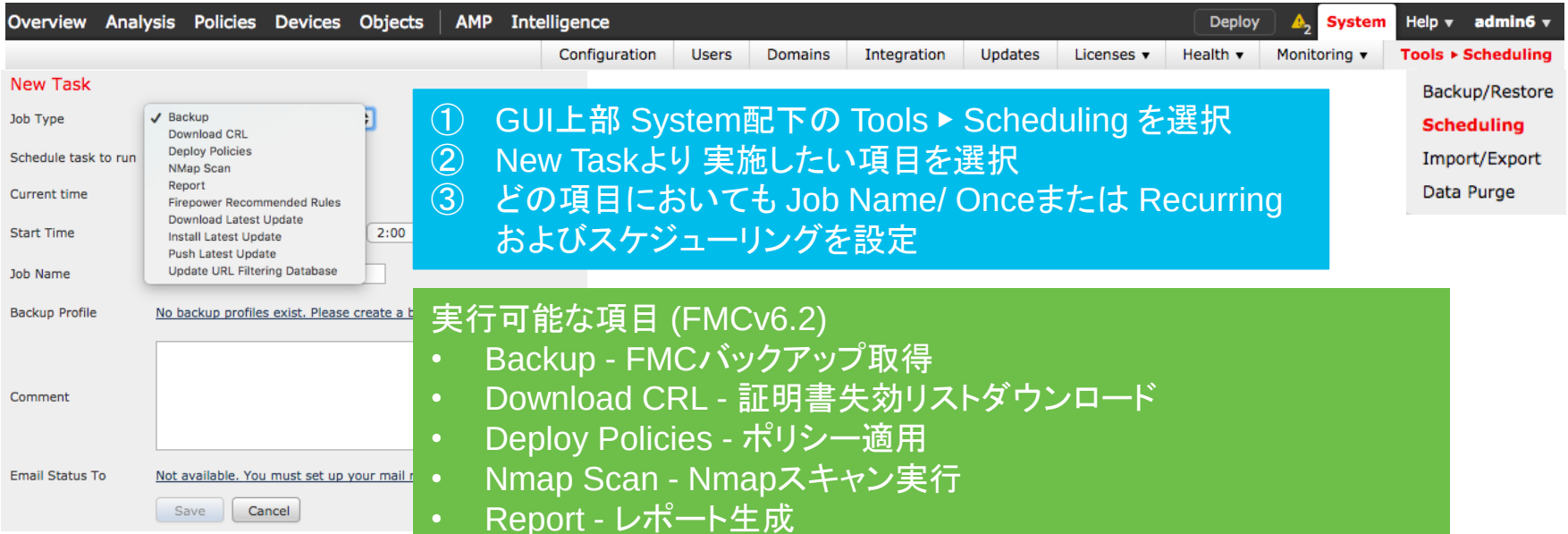
VDB/Patch ワンタイム更新～インストール



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

スケジューリング機能

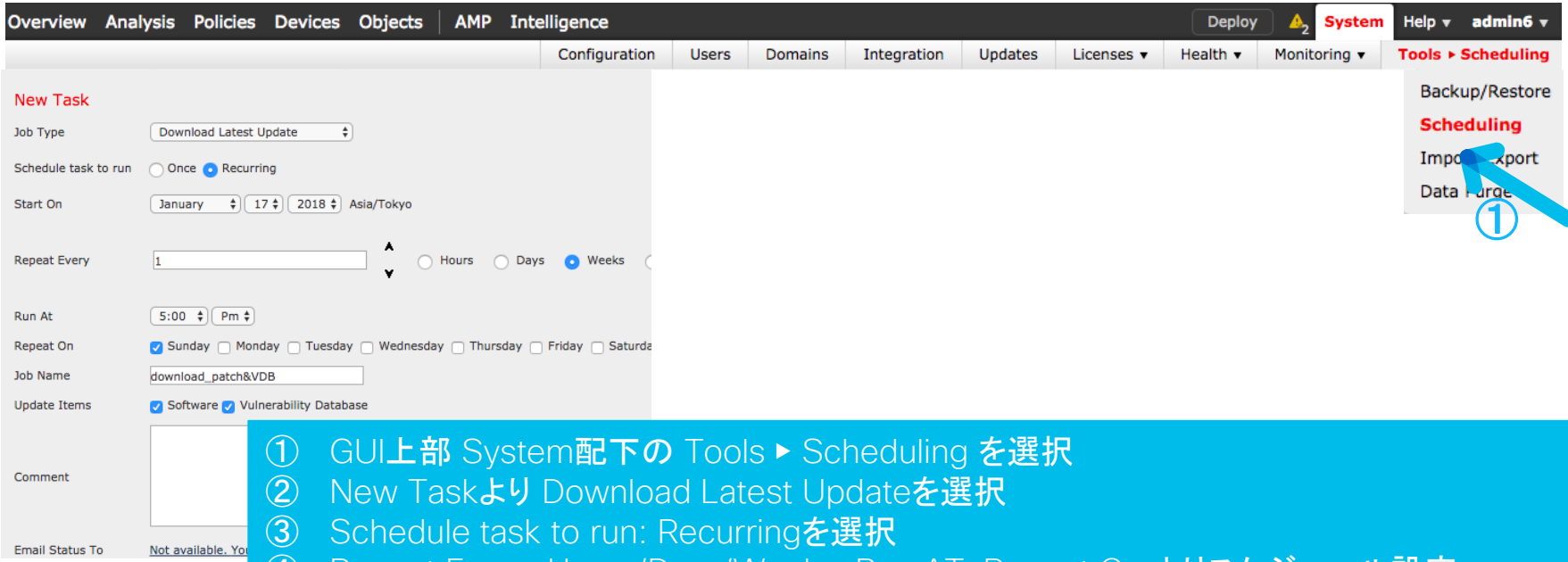


① GUI上部 System配下の Tools ▸ Scheduling を選択
② New Taskより 実施したい項目を選択
③ どの項目においても Job Name/ Onceまたは Recurring およびスケジューリングを設定

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

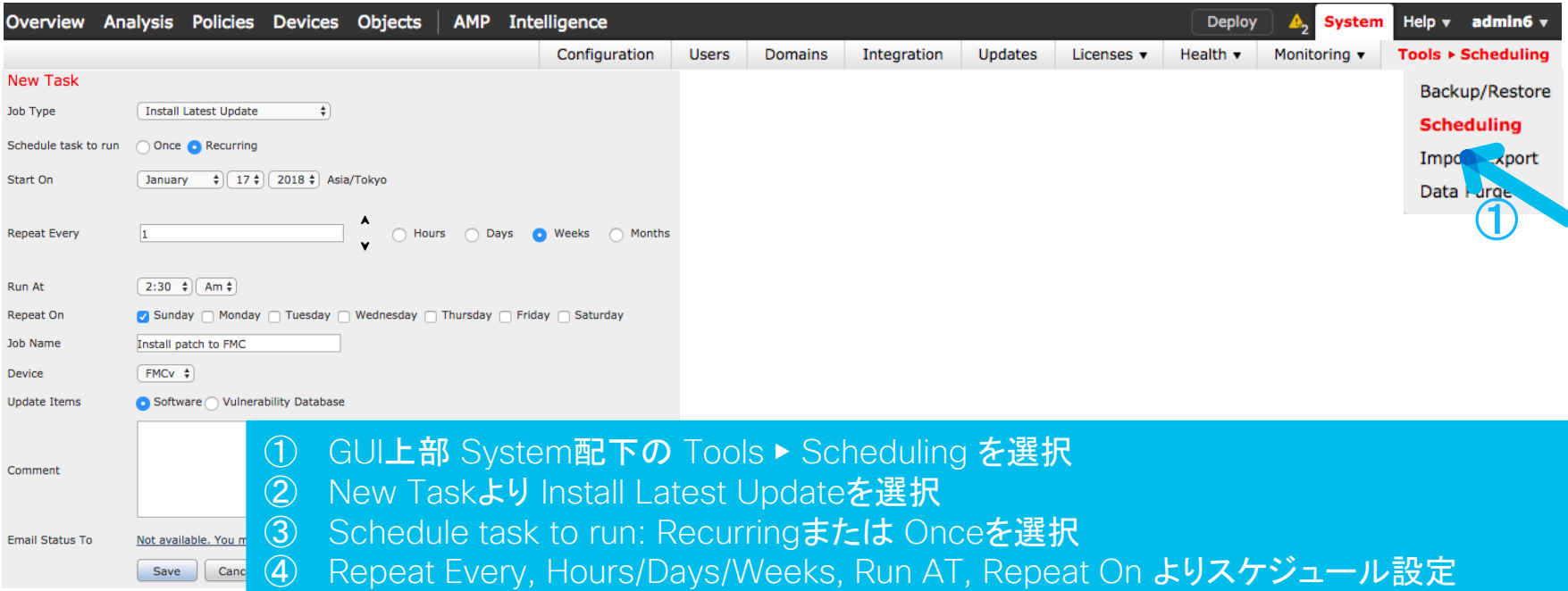
VDB/Patch 定期更新



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

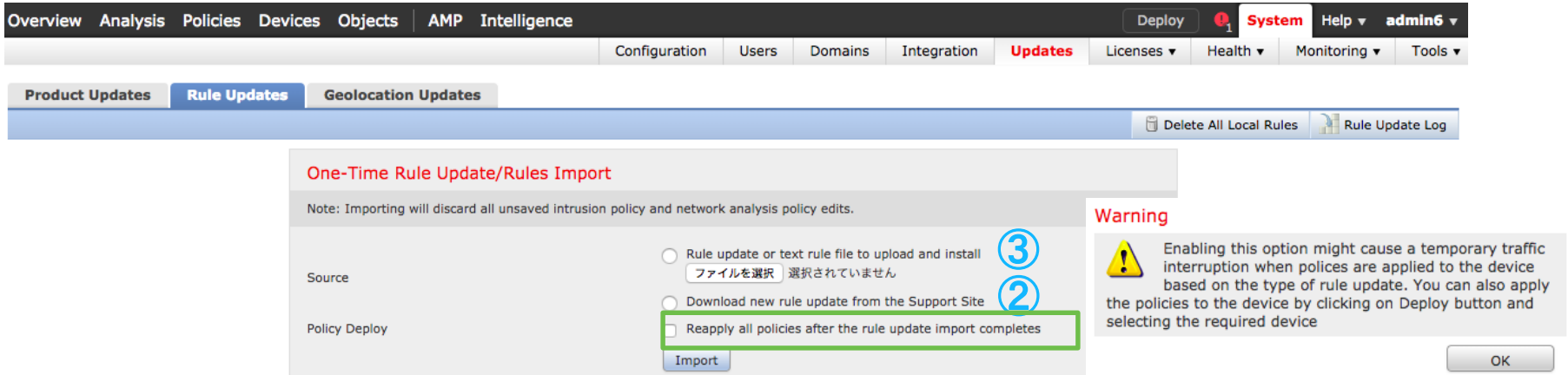
- VDB/Patch のみ新しいパッケージを定期チェックするのにスケジューリング機能が必要

VDB/Patch 定期更新～インストール



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

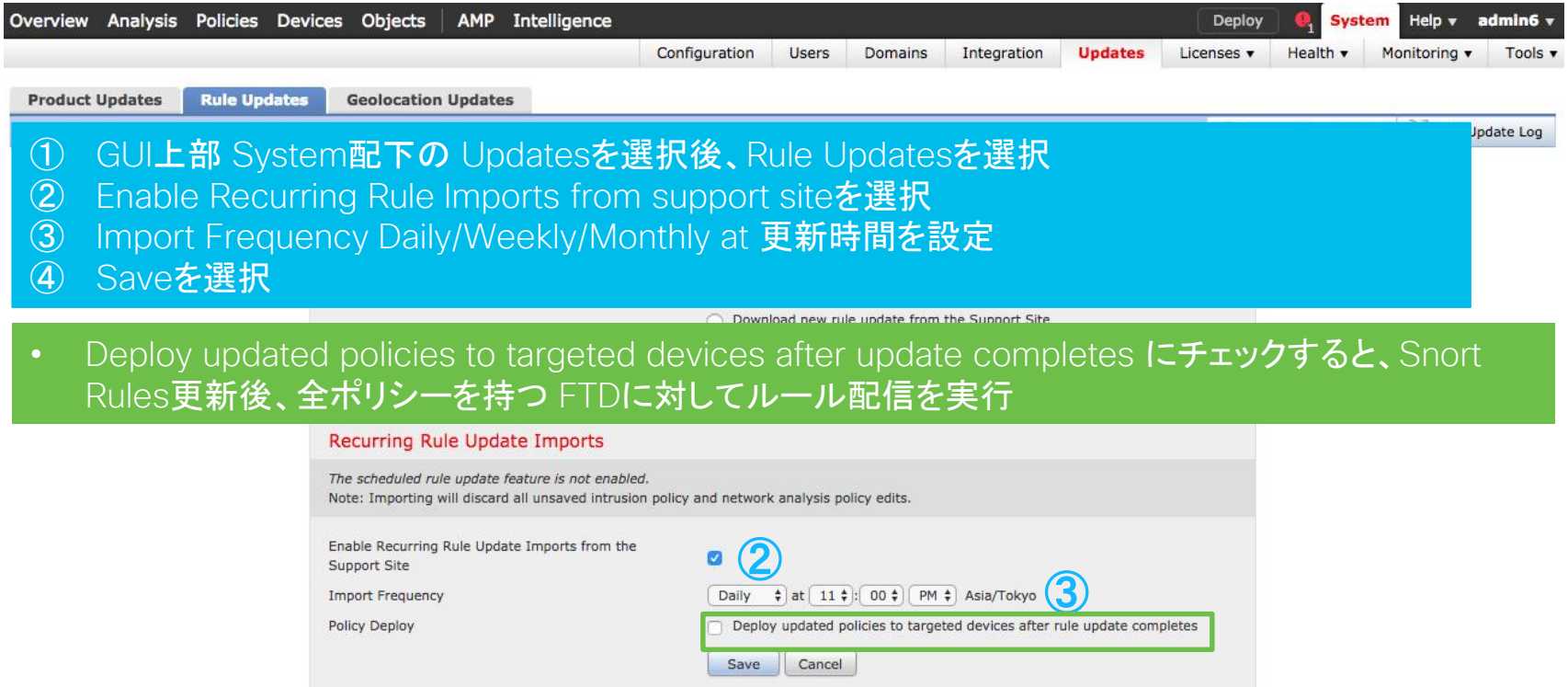
Snort Rules ワンタイム更新



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



Snort Rules 更新ログ

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

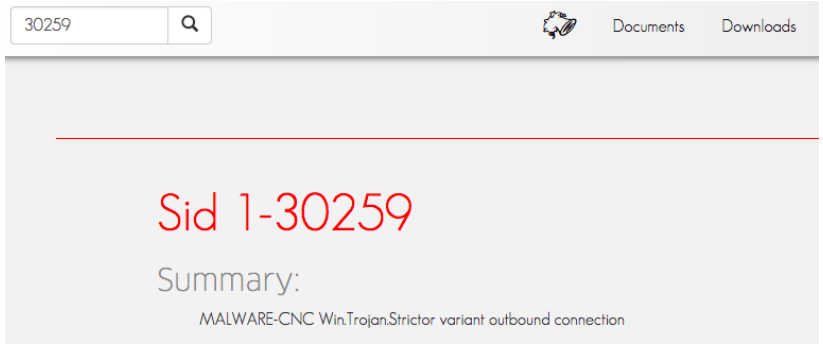
Rule Update Import Log
Table View of Rule Update Import Log

▸ Search Constraints (Edit Search Save Search)

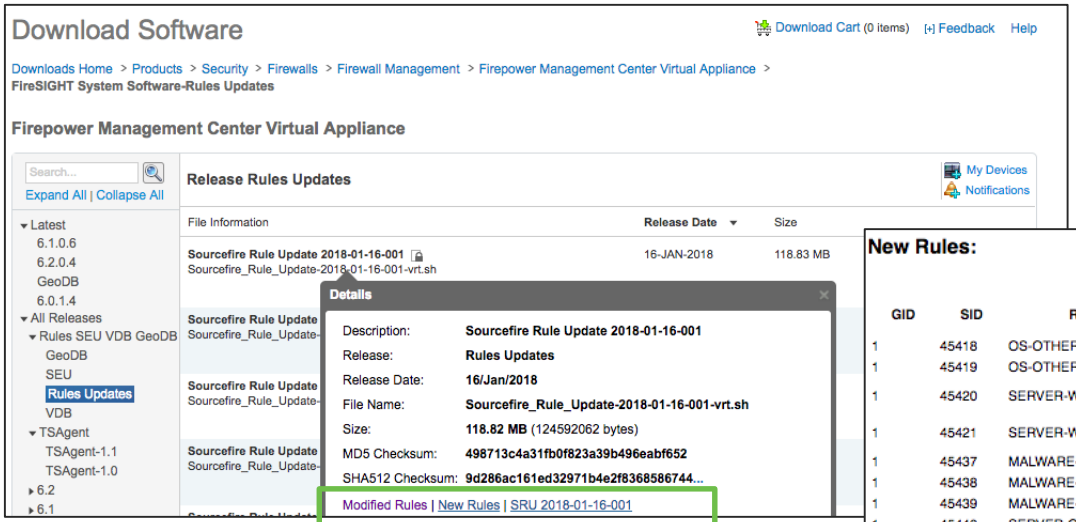
Disabled Columns

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

- 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



Snort Rules 更新ログ

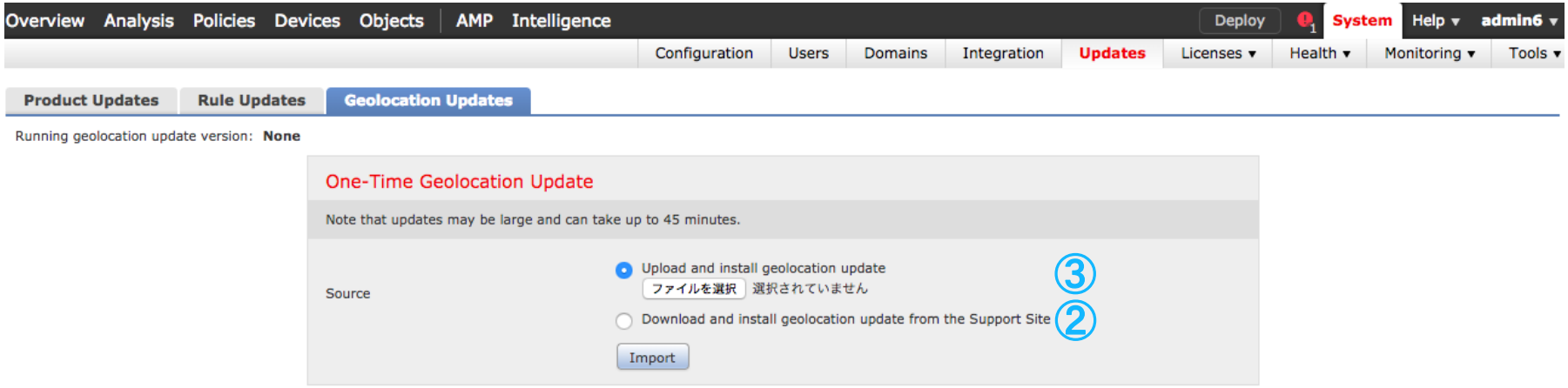


New Rules:

GID	SID	Rule Group	Rule Message	Policy State (High Priority) 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

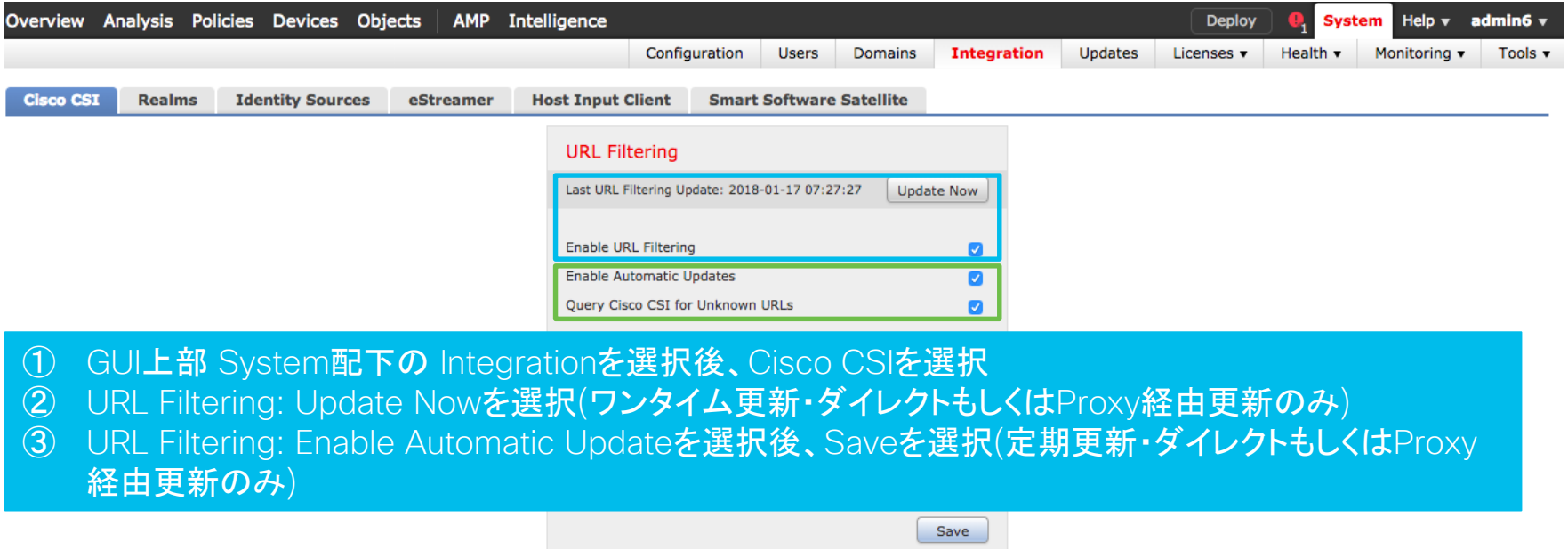
GeoDB ワンタイム更新



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

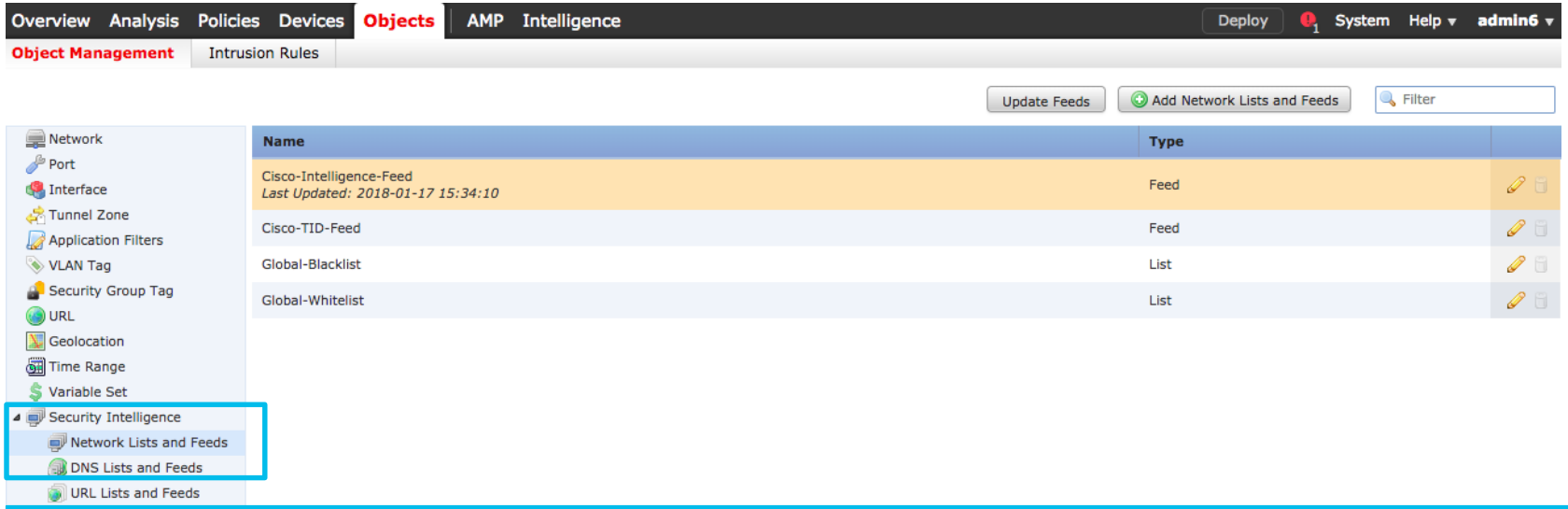
URL Filtering ワンタイム・定期更新・照会設定



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



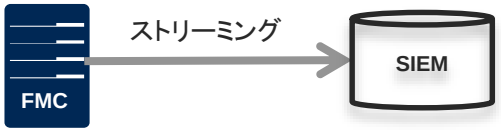
① GUI上部 Objects配下の Object Managementを選択
② Security Intelligence内の Network Lists and Feed または DNS Lists and Feedを選択

- 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

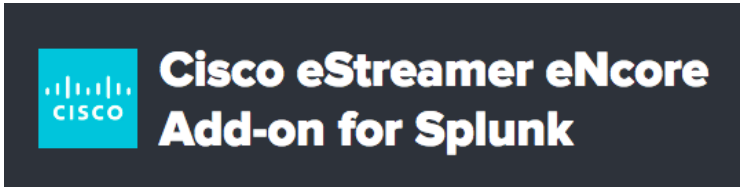
Event Streamer (eStreamer) APIとは

- 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

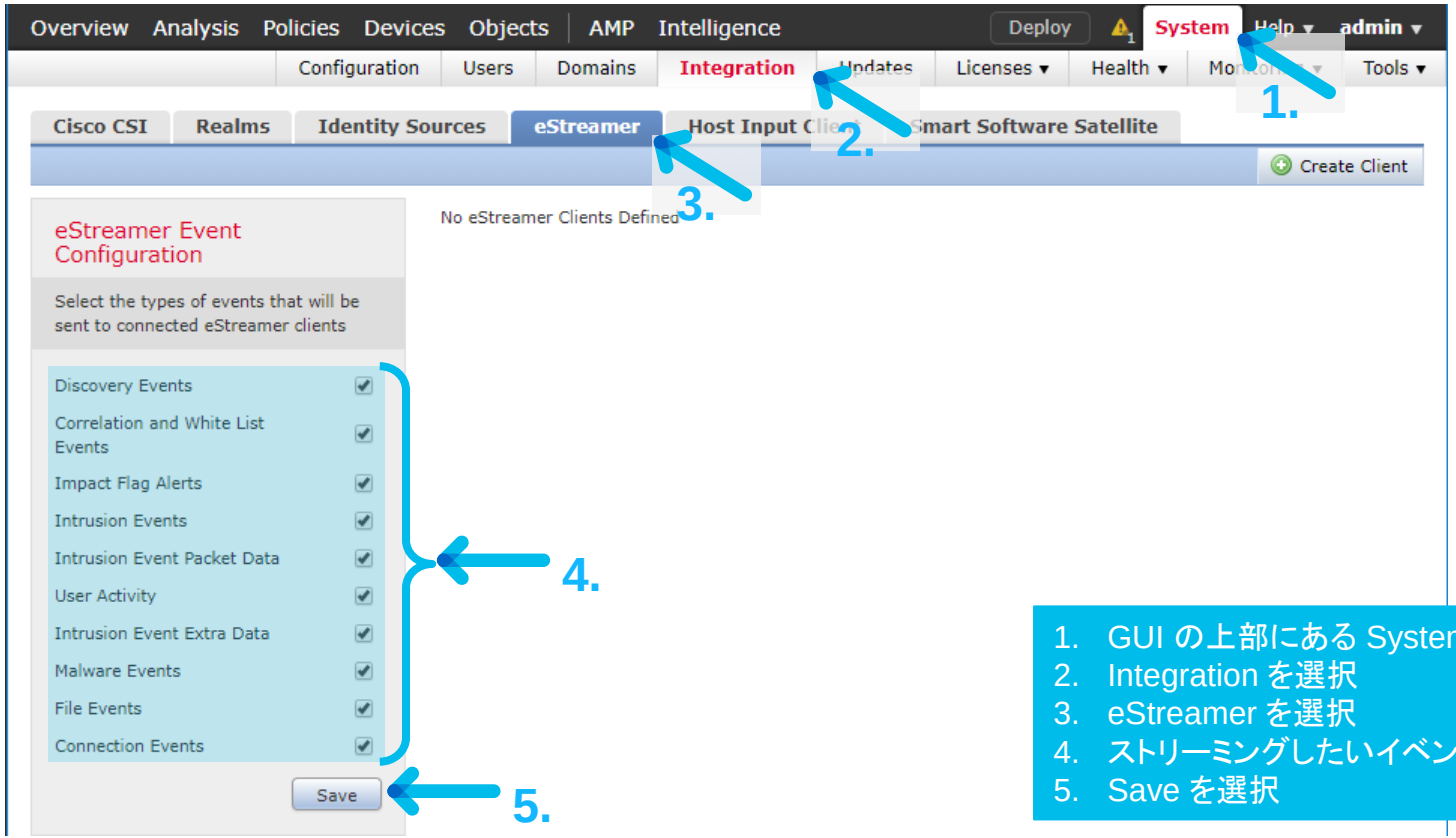
- 2018年7月現在 version 3.5 となる eStreamer クライアント
- Splunk (CIM フォーマット)、CEF アウトプットフォーマットをサポートしているため、Splunk や他のSIEMと容易に連携できる
- eNcore Add-on は SIEM連携用の仕組みを提供、eNcore App は Splunk側で情報を表示するためのもの
- 両方とも Splunkbase より無償ダウンロードが可能



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

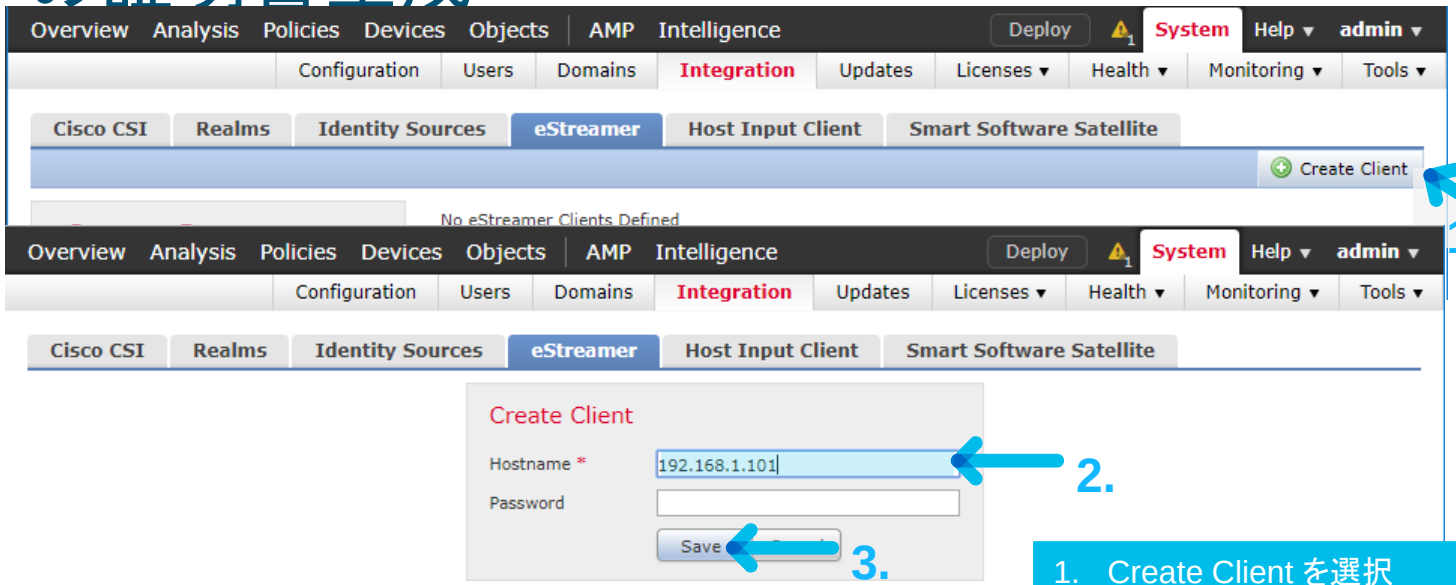
https://splunkbase.splunk.com/app/3663/

ステップ1. sStreamer ストリーミングイベントの設定



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



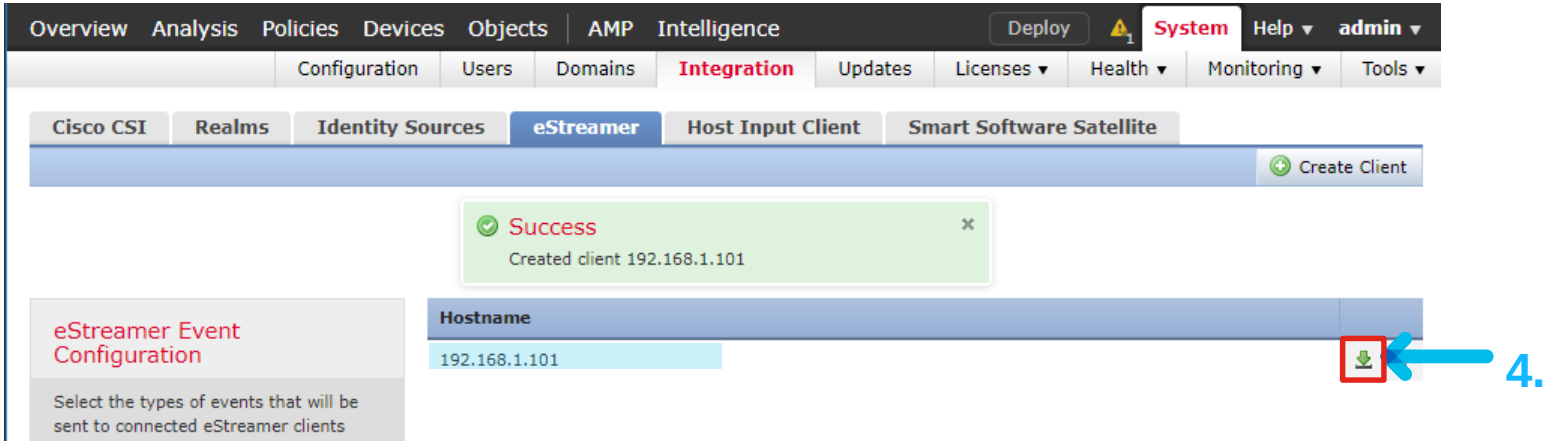
1. Create Client を選択
2. クライアントのホスト名、もしくは、IPアドレス(DNSを設定いない場合)を入力
3. Save を選択

*Password は任意

次のスライドへ続く

Firepower Management Center

ステップ2. リファレンスクライアント向け証明書の取得



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

- /user/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
```

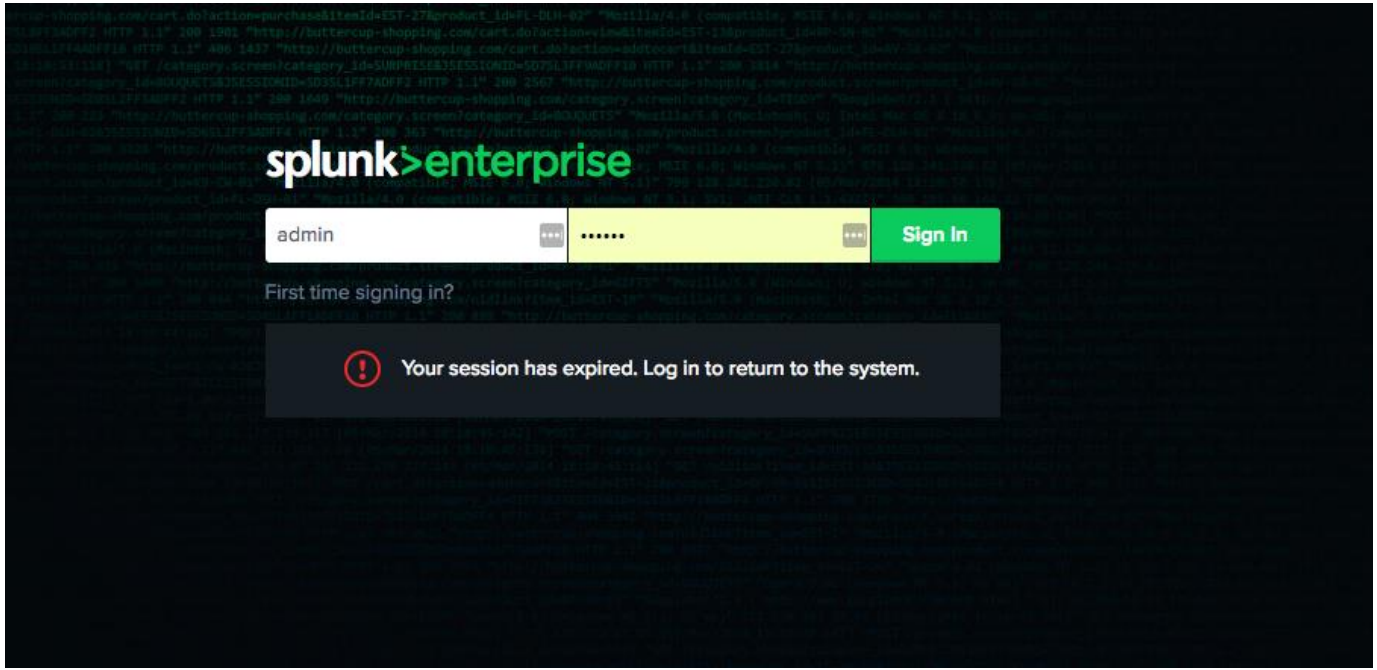
ステップ7.　FMC eStreamer Cert配置

- 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/
```

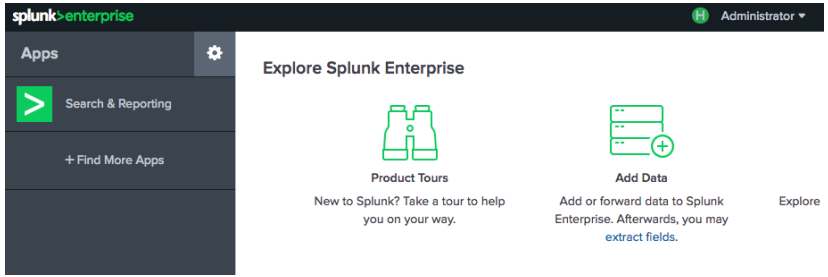
ステップ8. Splunkへのアクセス

- 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

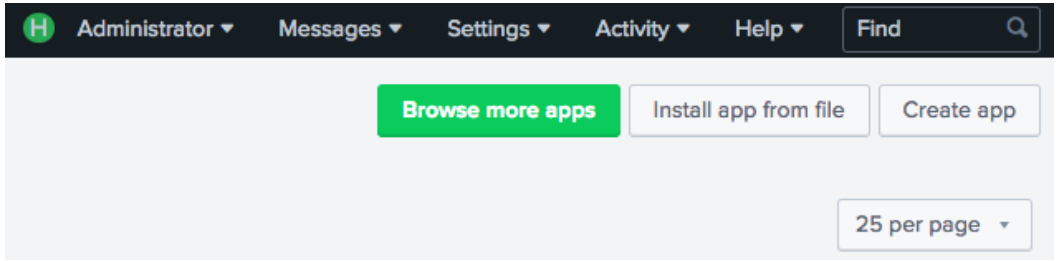


ステッ9. Splunk Appインストール

- Splunkトップ画面より、Apps横の歯車マークをクリック

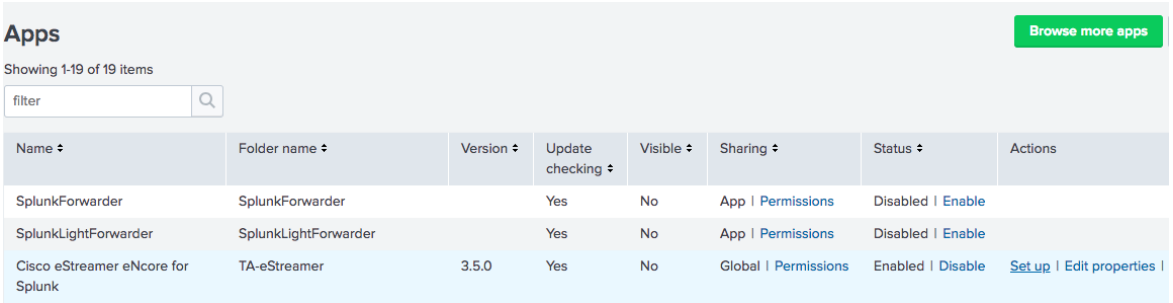


- Install App from FileもしくはBrowse more apps より 以下2つのAppをインストール
- Cisco eStreamer eNcore for Splunk, Cisco eStreamer eNcore Dashboard for Splunk

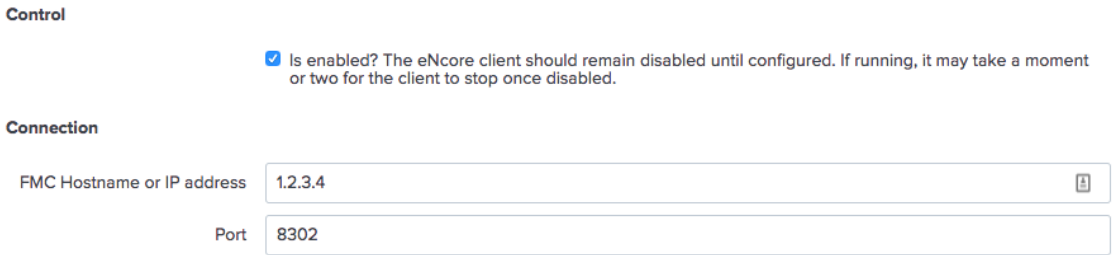


ステップ10. eNcore App セットアップ

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

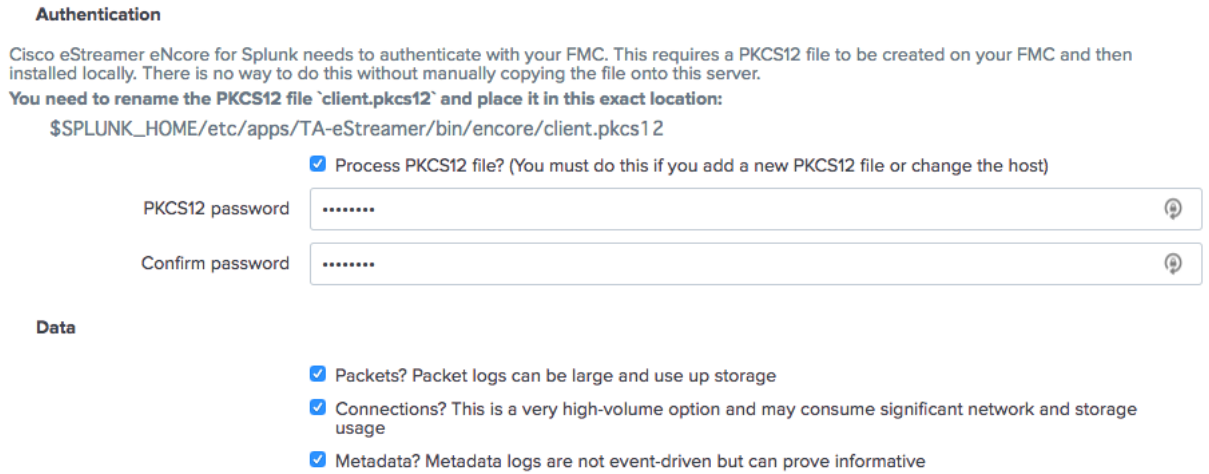


- Controlにチェックボックス、Connectionに FMC IPを入力



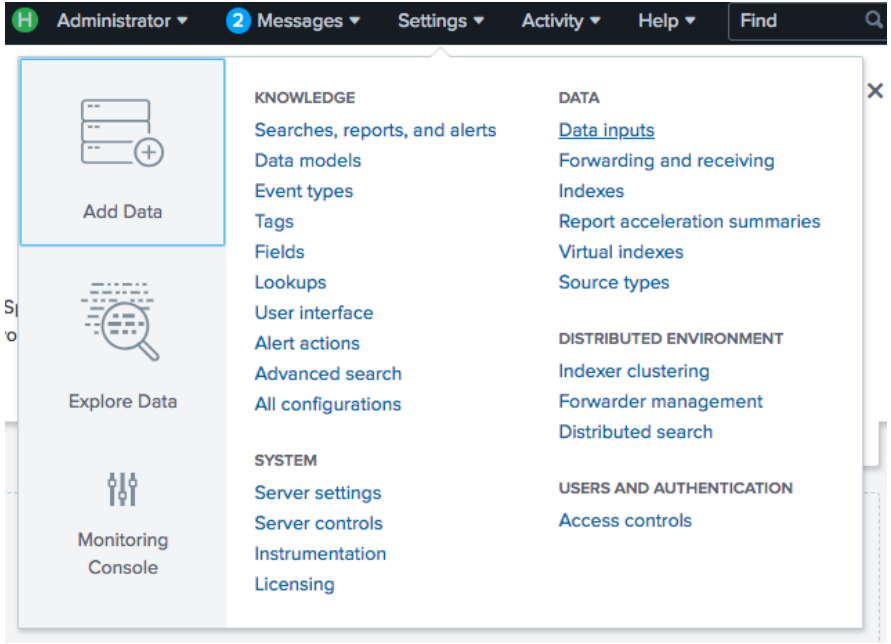
ステップ11. eNcore App セットアップ

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



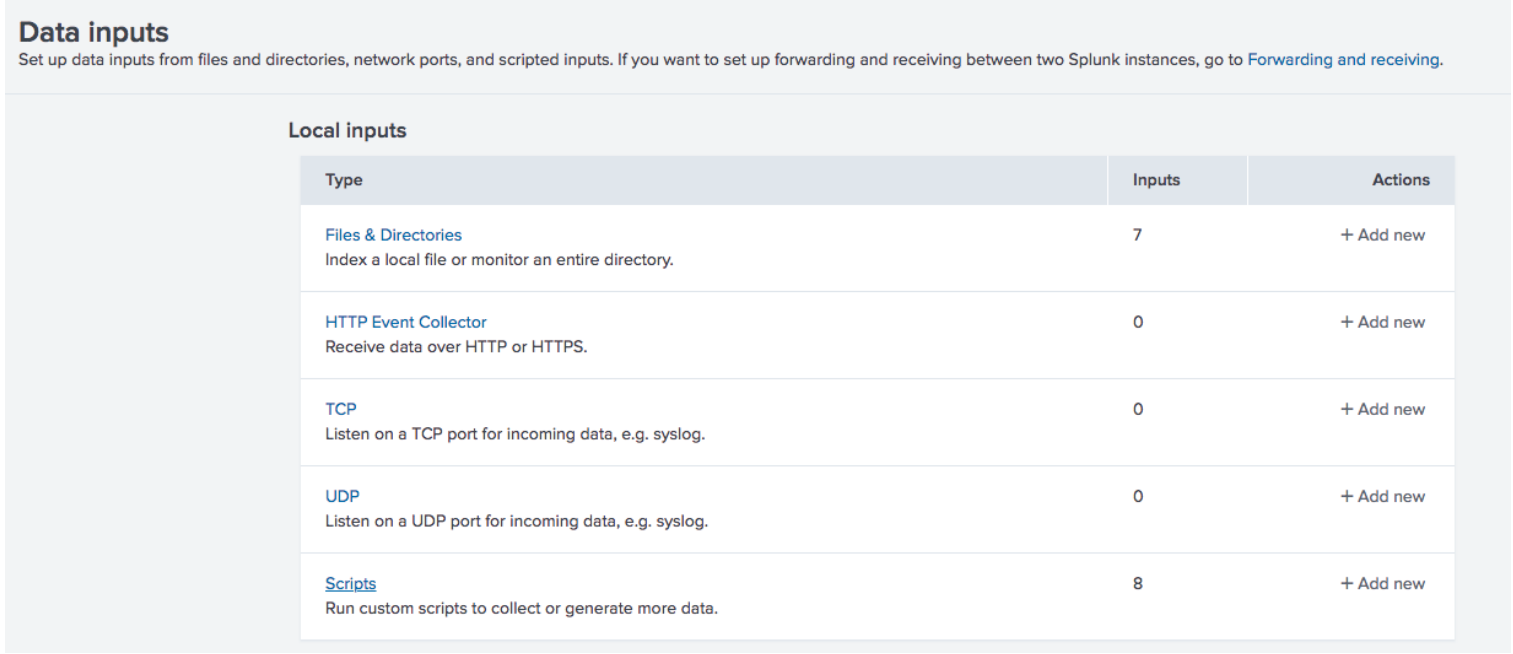
ステップ12. eNcore Data scriptの起動

- Settings > Add Data > Data inputsを選択



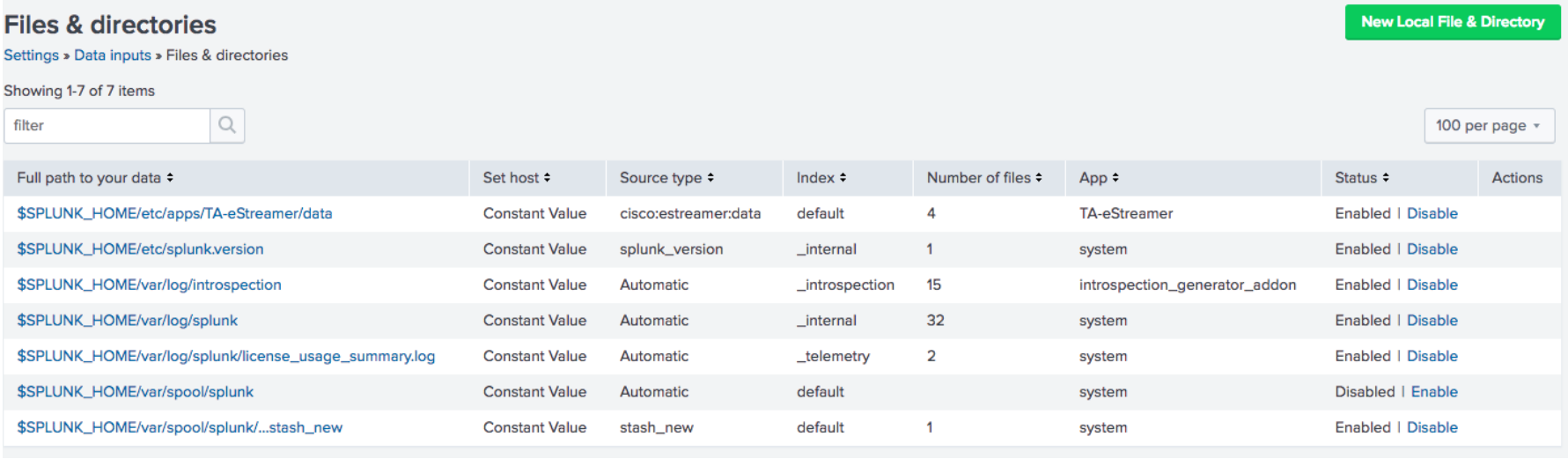
ステップ13. eNcore Data cisco:estreamer:dataの起動

- Data inputs > Files & Directories を選択



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

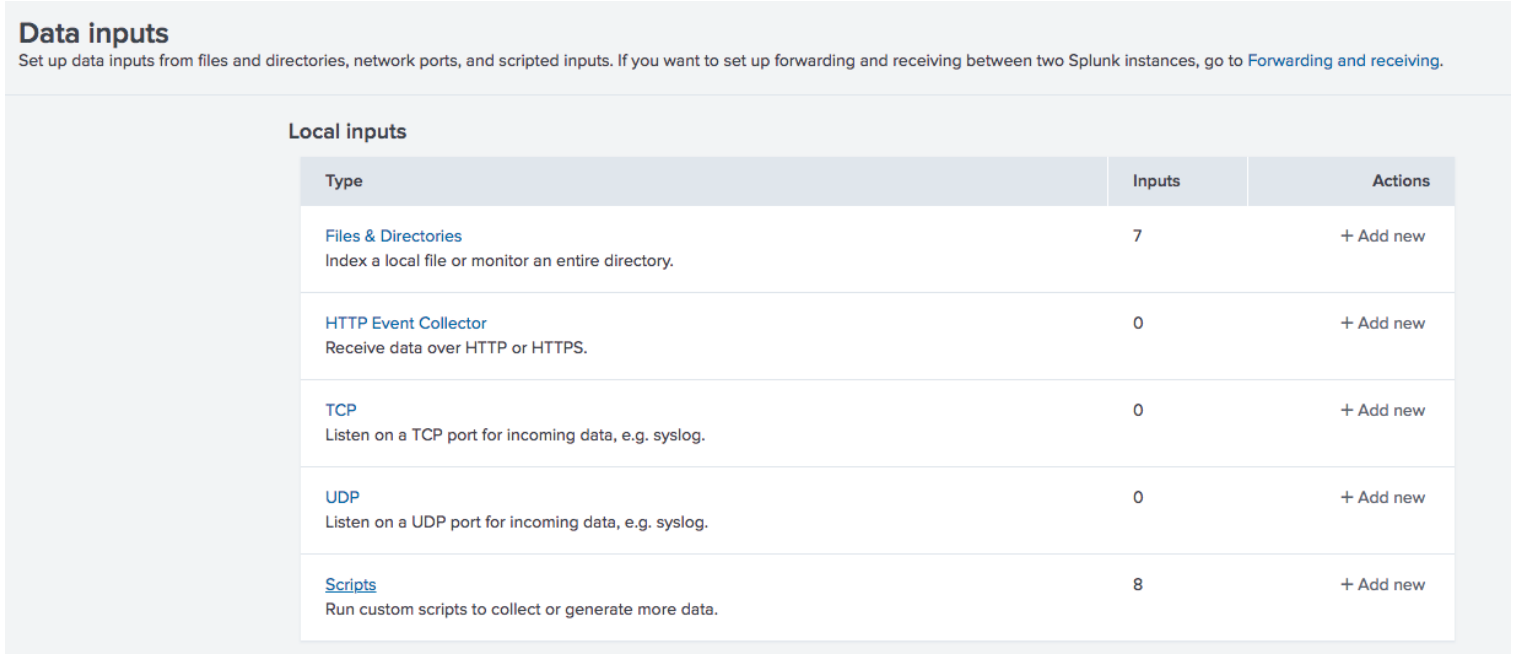
filter

100 per page

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

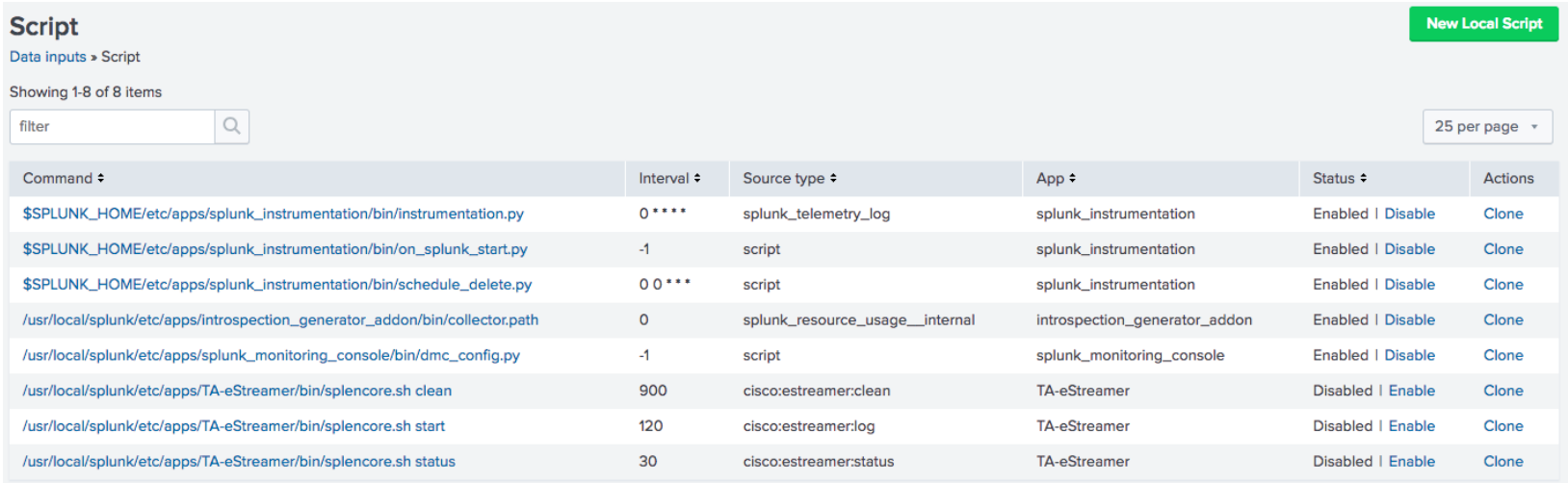
ステップ15. eNcore Data scriptの起動

- Data inputs > Scrips を選択



ステップ16. eNcore Data scriptの起動

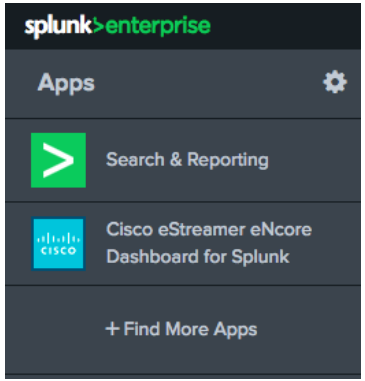
- Scripts内 splencore.sh clean/ start/ status 3つを Enable

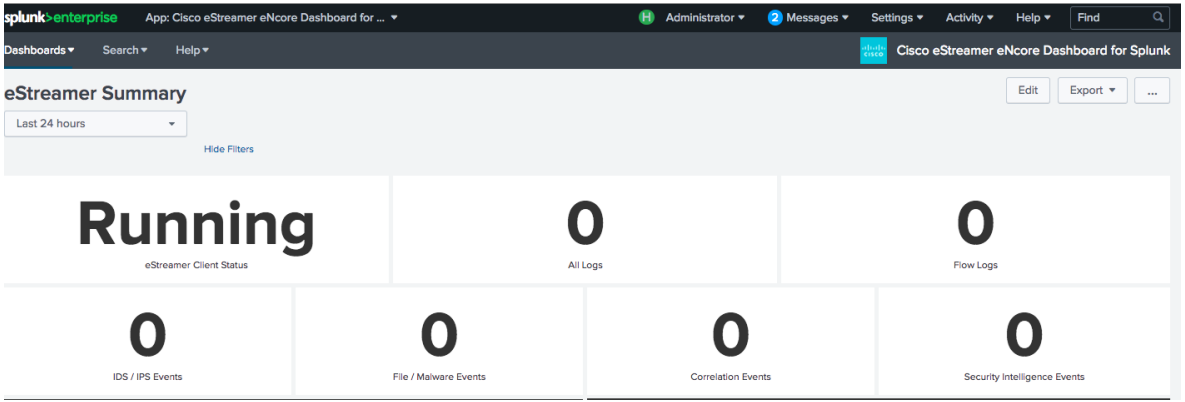


Command	Interval	Source type	App	Status	Actions
$SPLUNK_HOME/etc/apps/splunk_instrumentation/bin/instrumentation.py	0 * * * *	splunk_telemetry_log	splunk_instrumentation	Enabled | Disable	Clone
$SPLUNK_HOME/etc/apps/splunk_instrumentation/bin/on_splunk_start.py	-1	script	splunk_instrumentation	Enabled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

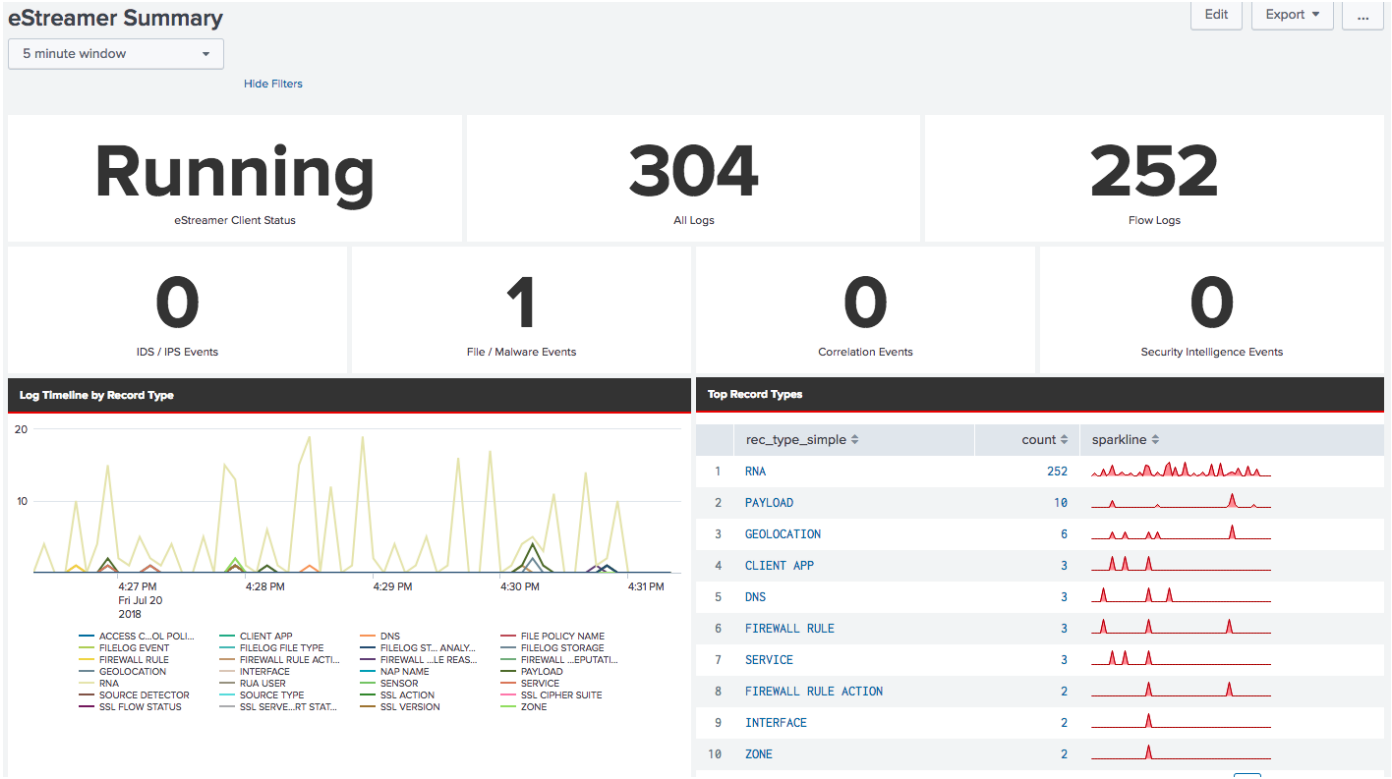
ステップ17. eNcore Dashboard確認

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



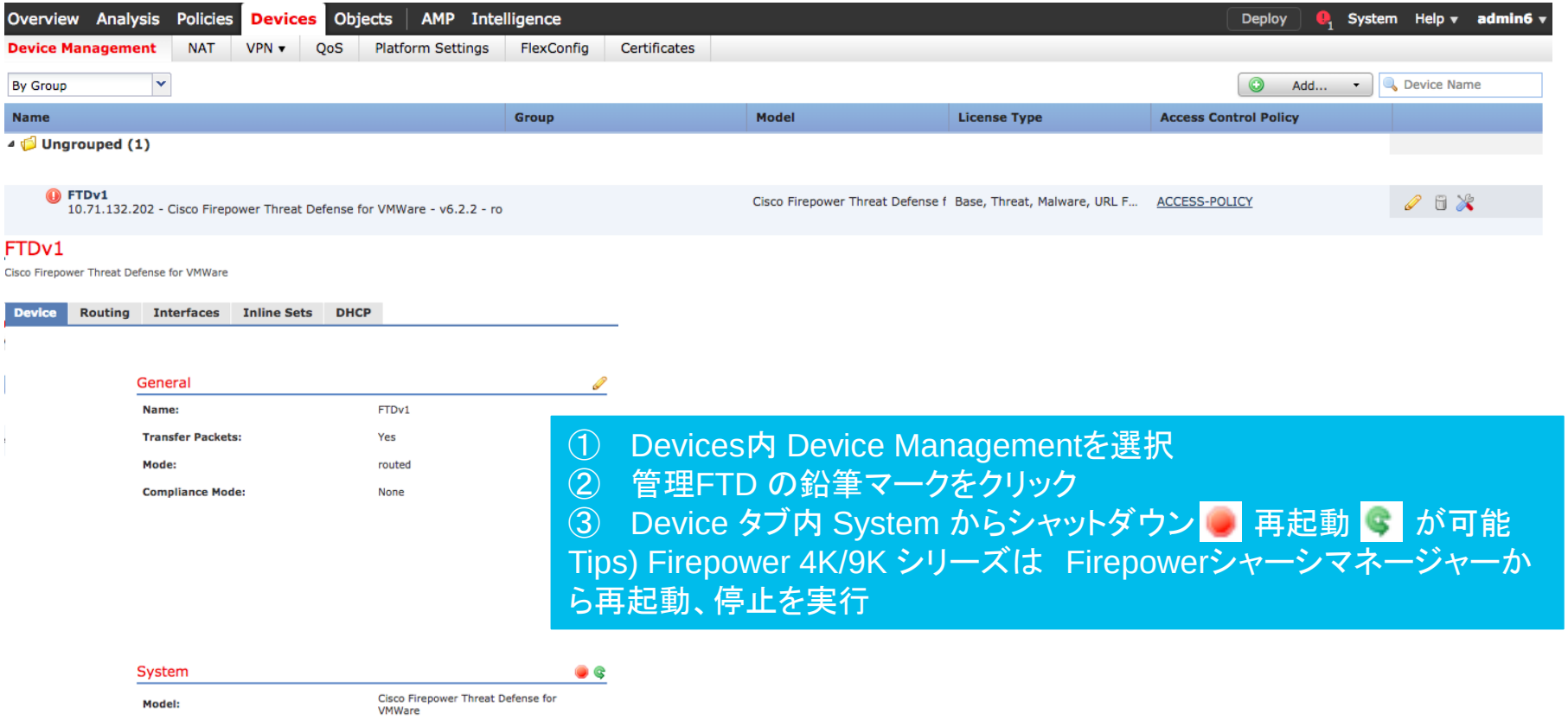


ステップ18. eNcore Dashboard確認



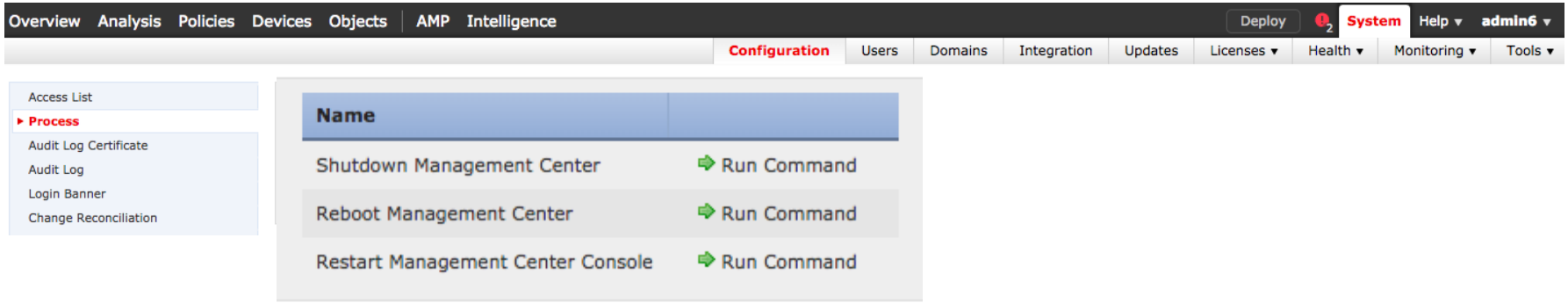
9: メンテナンス

FTD メンテナンス



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

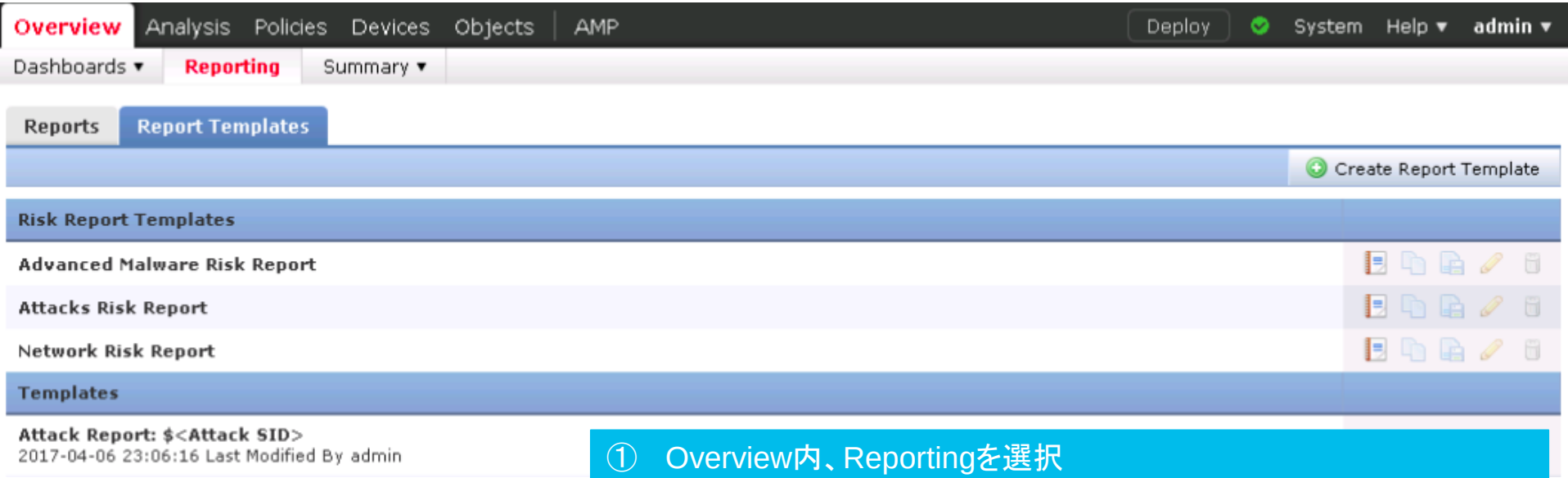
FMC メンテナンス



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

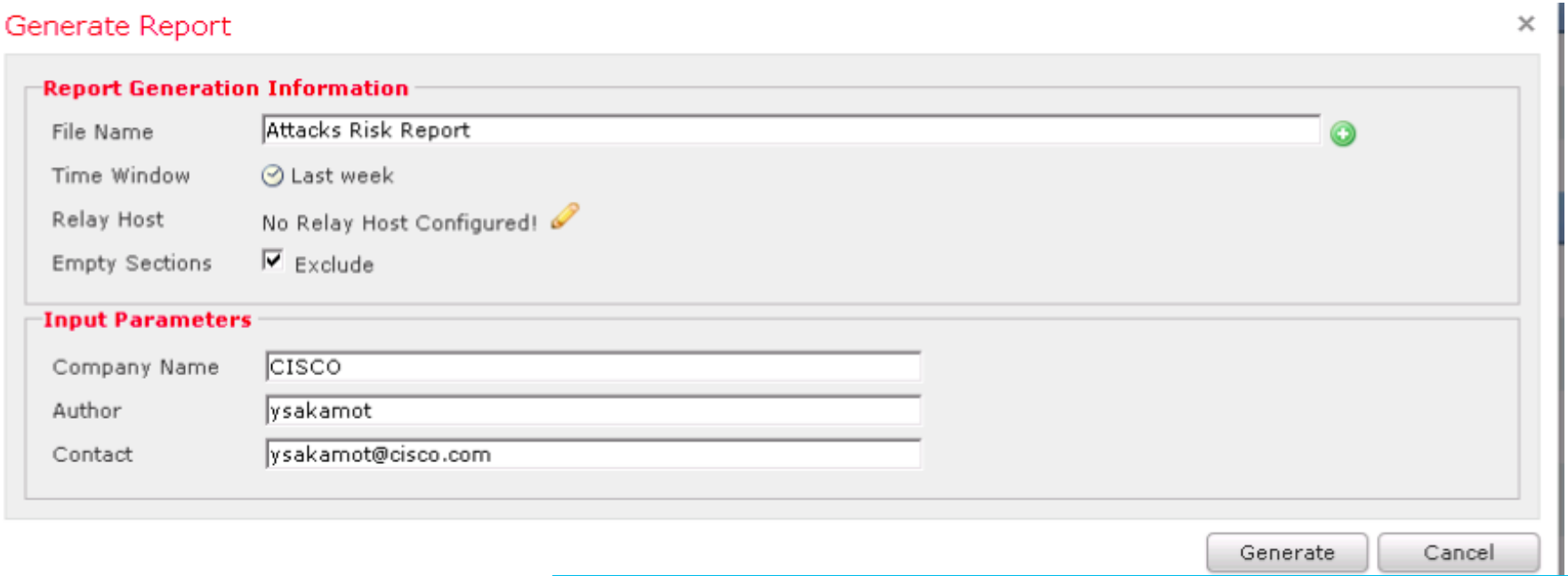
10 レポーティング

Report 生成



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

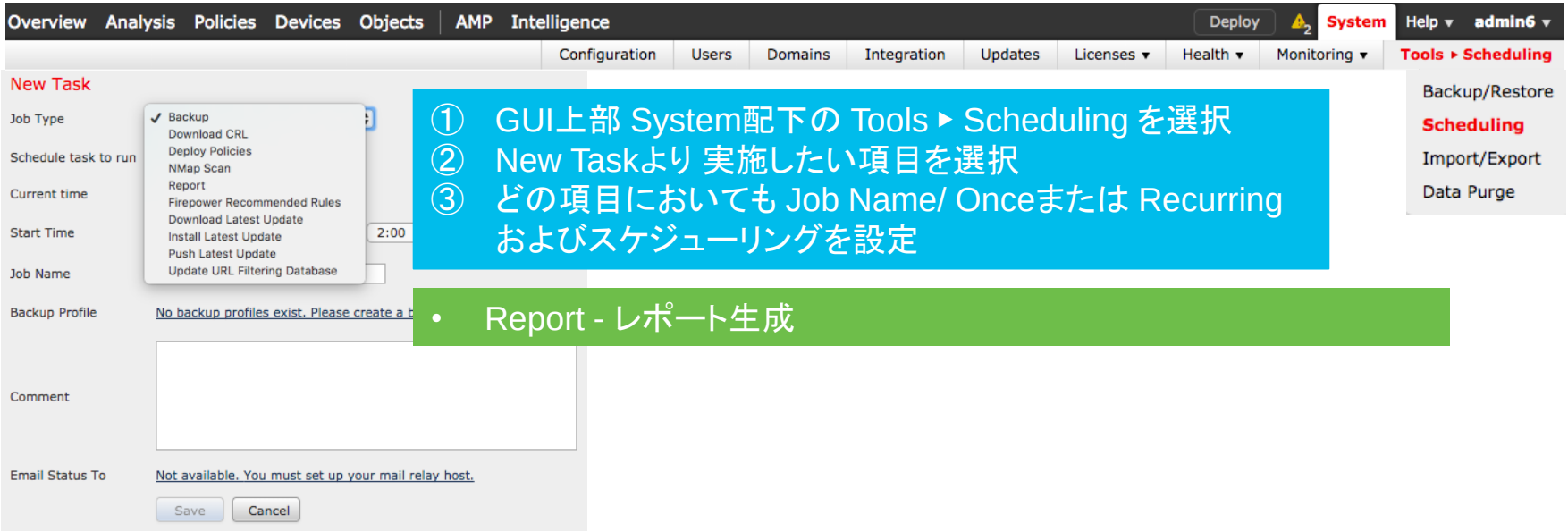


① デフォルト 1週間の情報をレポート化
② 必要に応じて Inputs Parametersを入力
③ Generate をクリックすると、レポートが生成される

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



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

Appendix1.
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

** 障害時に 対応ポート間で、ソフトウェアを介さずハードウェアレベルでのパケット転送が可能。インラインペアモード用

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

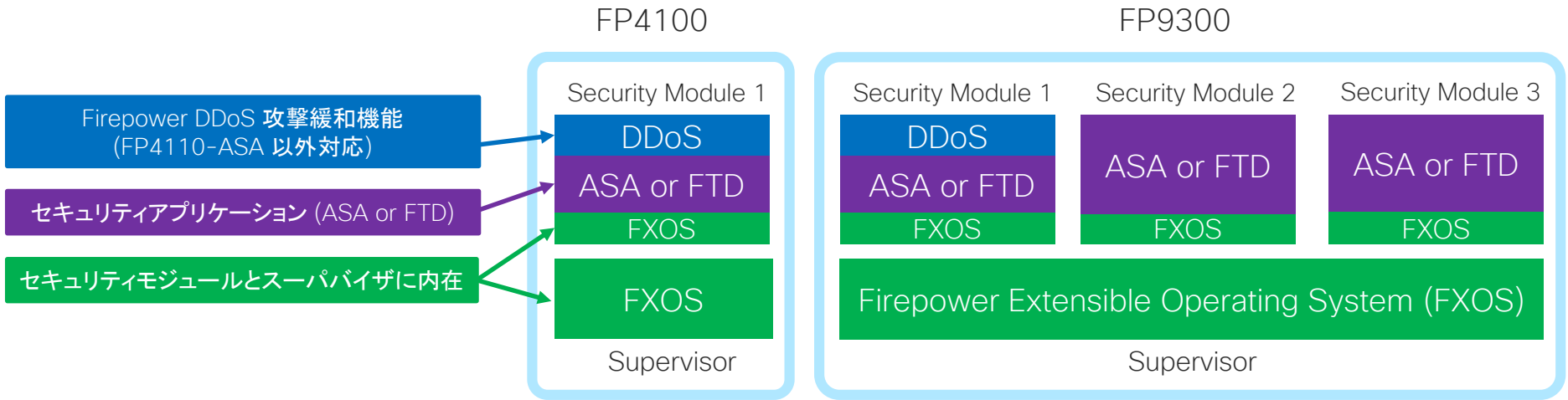
シリアルコンソールポート

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

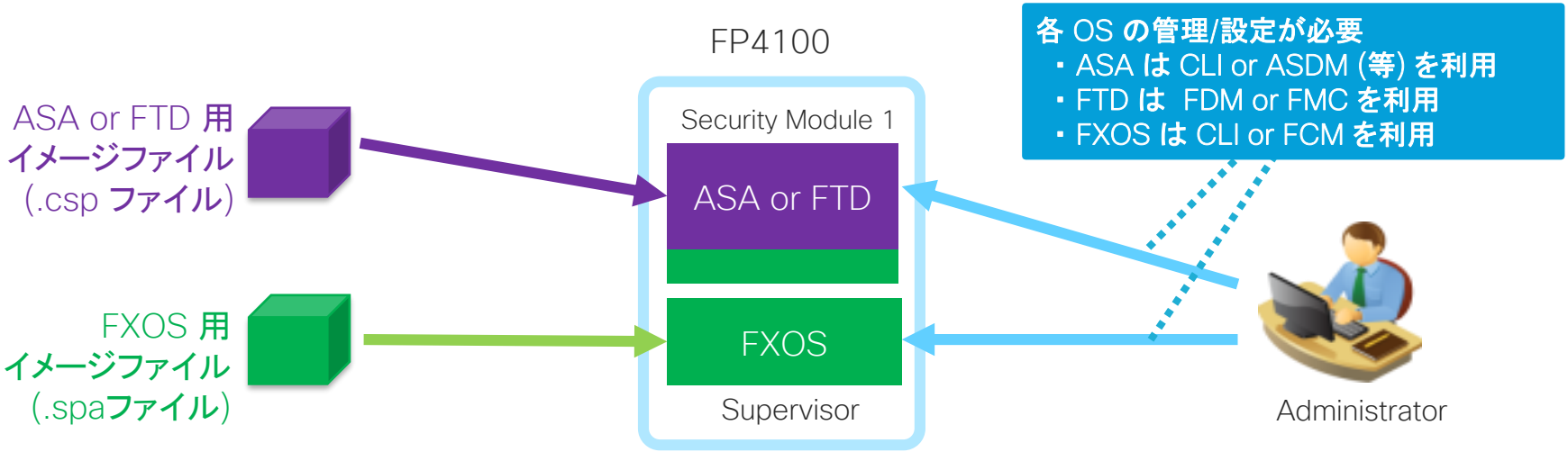
- FP4100/9300 内には Firepower eXtensible Operating System (FXOS) が動作
  - FXOS が、スーパーバイザや セキュリティモジュールを管理
  - FXOS が、シャーシや ネットワークモジュール、電源、FAN などハードウェアの管理
  - FXOS が、セキュリティモジュールに物理インターフェイス割当て



TIPS) FP4100 と FP9300の主な違いは、セキュリティモジュール搭載数と対応ネットワークモジュール

FP4100/9300 と FXOS (続き)

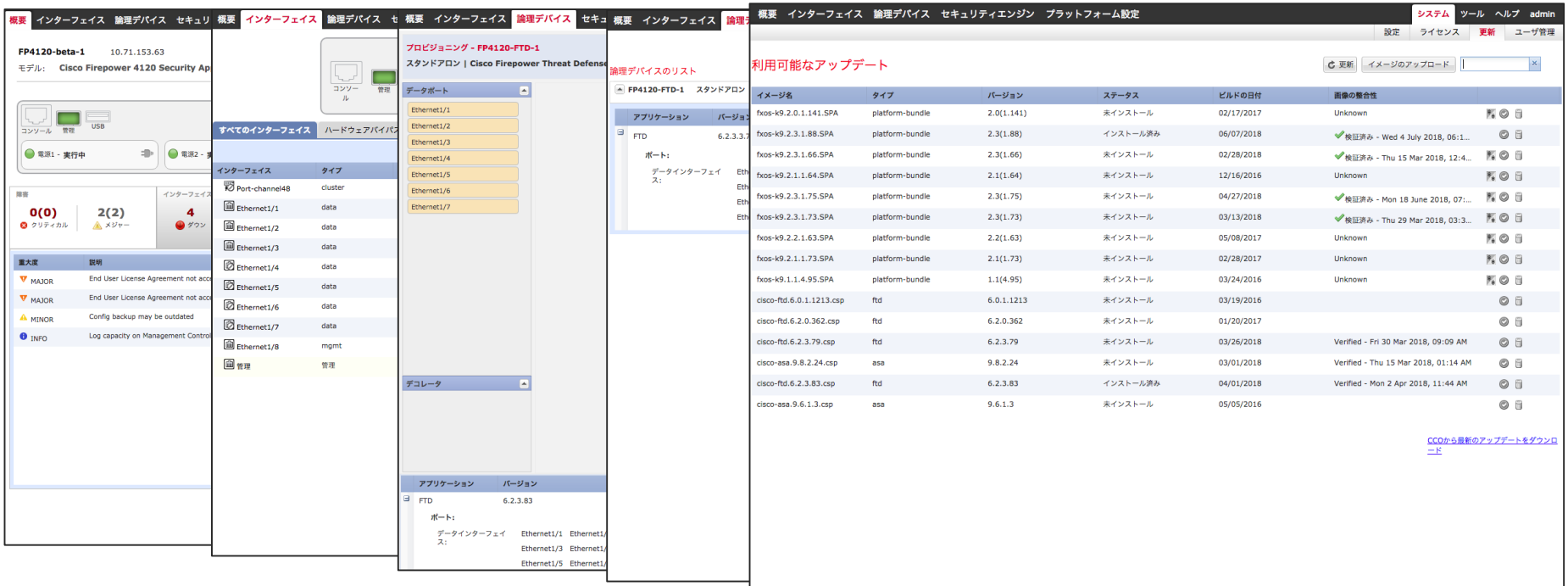
- FP4100/9300 はプラットフォーム型で、シャーシ内に複数 OS が動作可能
  - FXOS と ASA/FTD は、各独立した OS であり、イメージファイルや設定ファイルが異なる
  - FXOS と ASA/FTD の各アップグレードは、別々に実施が必要
  - FXOS と ASA/FTD は、各独立した管理インターフェイスと管理 IP アドレス, GUI, Syslog, SNMP Agent をもつ



TIPS) FP4100/9300 は拡張性重視のため、FXOS と ASA/FTD の独立性が高い

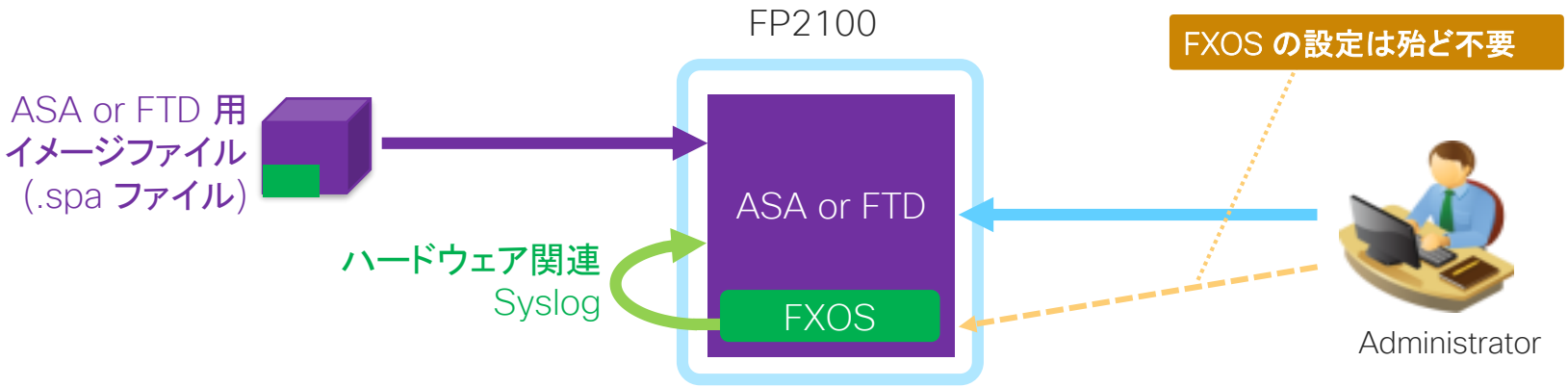
Firepower Chassis Manager (FCM)

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)



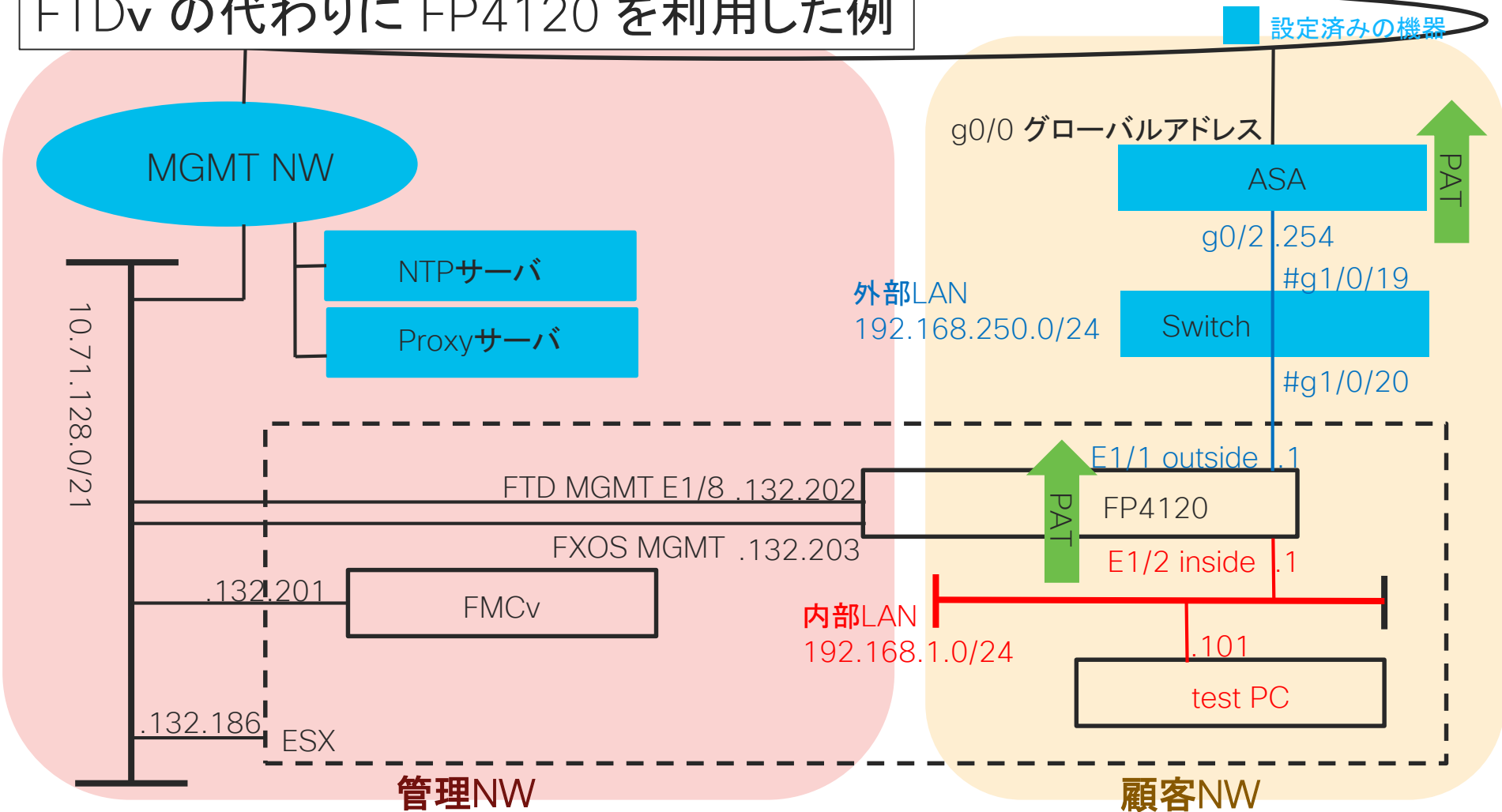
FP2100 と FXOS

- 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 側に出力
  - 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



Appendix1-1
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



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

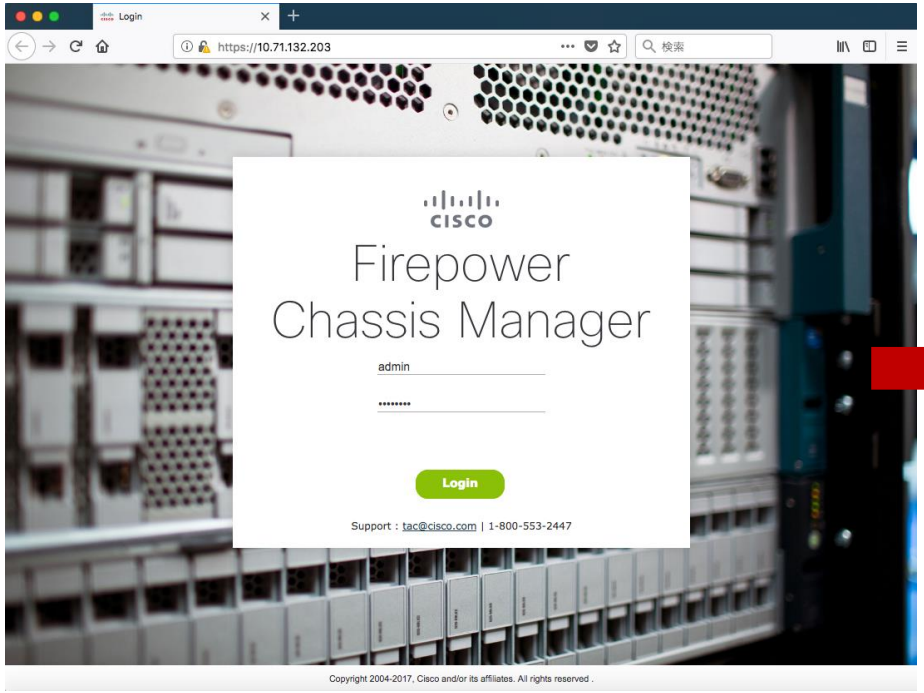
ステップ 2-3: FP4120 の FXOS 初期セットアップ

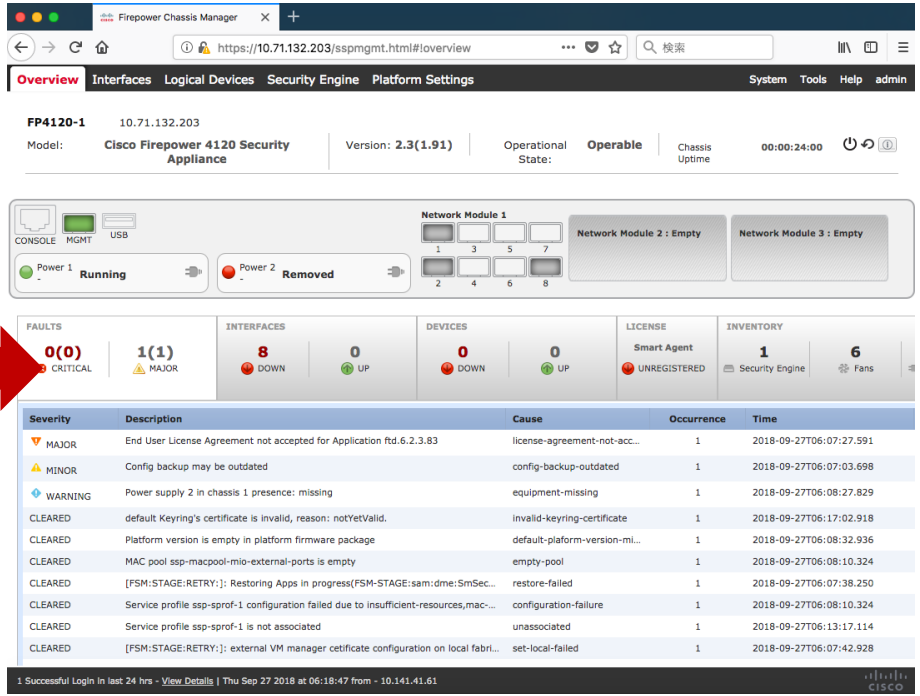
```
    Switch Fabric=A
    System Name=FP4120-1
    Enforced Strong Password=yes
    Supervisor Mgmt IP Address=10.71.132.203
    Supervisor Mgmt IP Netmask=255.255.248.0
    Default Gateway=10.71.135.254
    SSH Access Configured=yes
        SSH IP Address=10.141.0.0
        SSH IP Netmask=255.255.0.0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

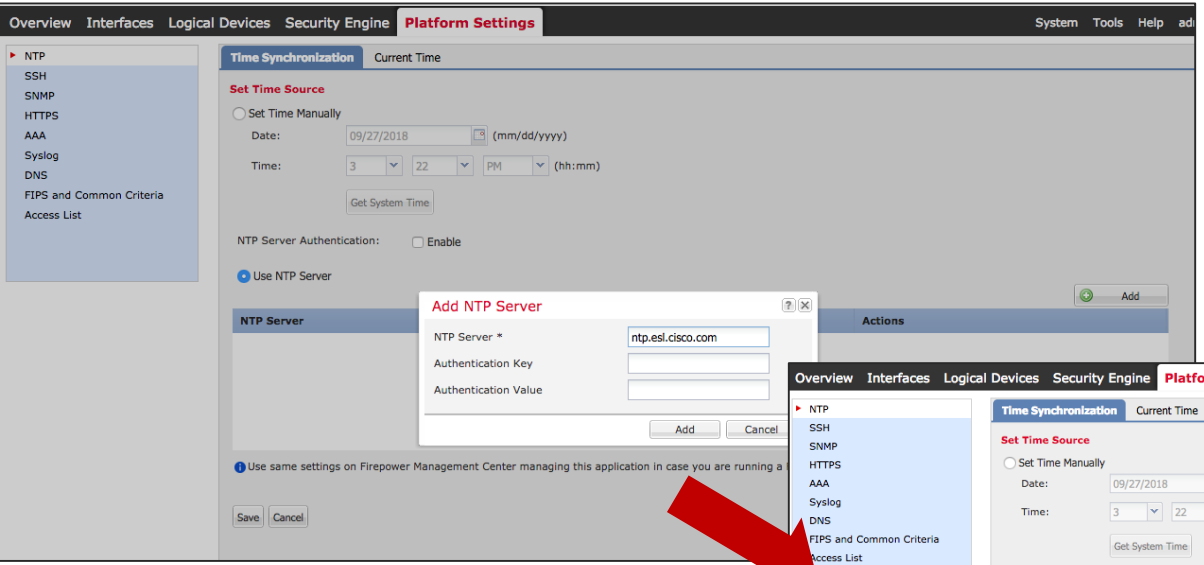


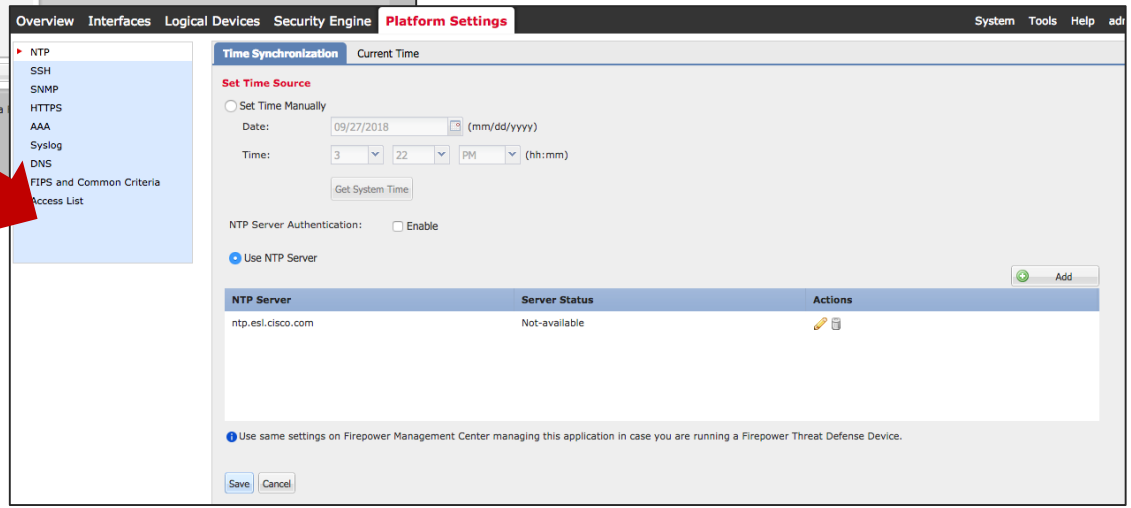


(注) FCM の言語は、Web ブラウザの言語設定に依存

ステップ 4-1: FCM on FP4120 の初期設定

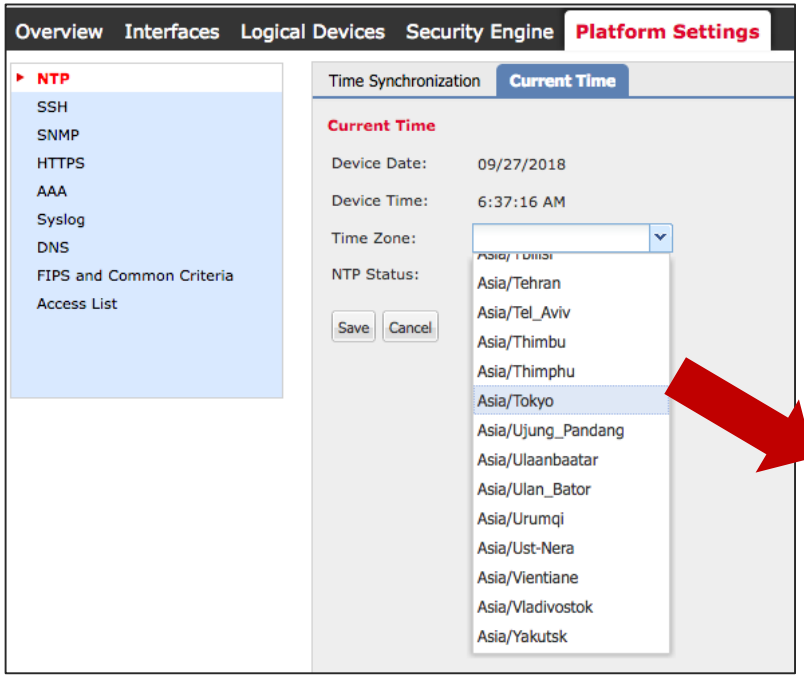
Platform Settings → NTP → Use NTP Server にて NTP サーバを追加し、save する



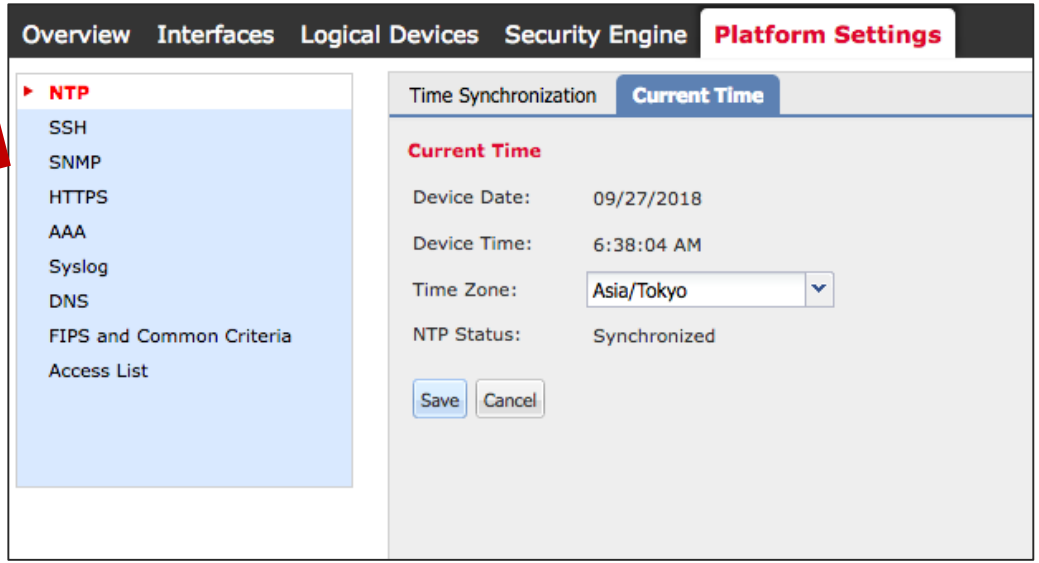


NTP サーバとの時刻同期が始まると、
強制的に FCM からログアウトされるので、
再度 admin でログインする

ステップ 4-2: FCM on FP4120 の初期設定



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



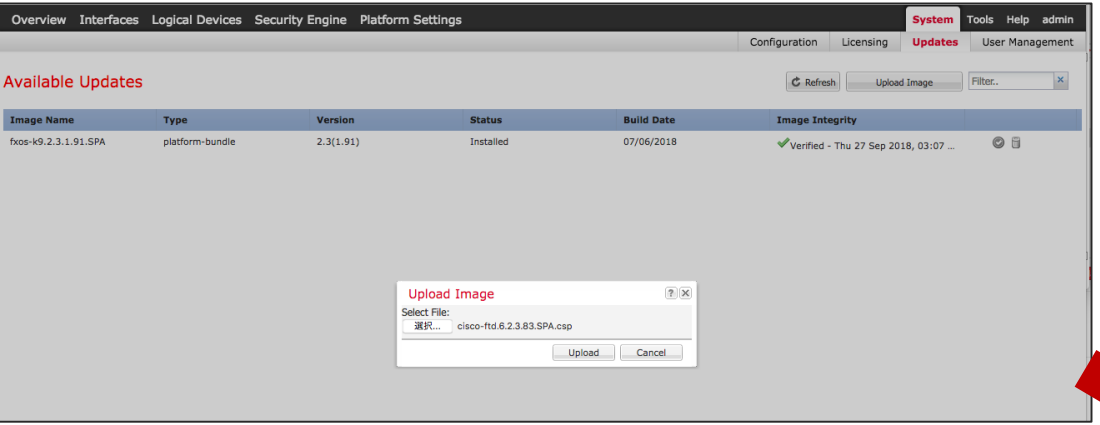
ステップ 4-3: FCM on FP4120 の初期設定

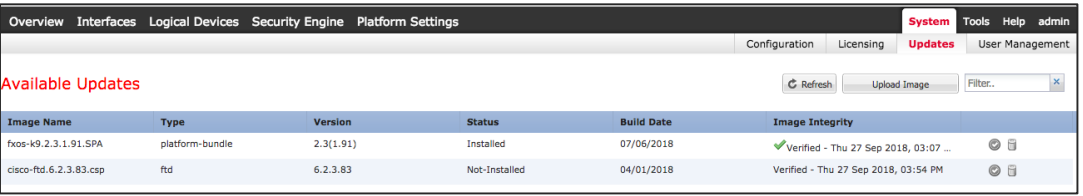
以下のサイトから、FTD 6.2.3 のインストールパッケージ (.csp ファイル) をダウンロードしておくこと
https://software.cisco.com/download/home/286306168/type/286306337/release/6.2.3

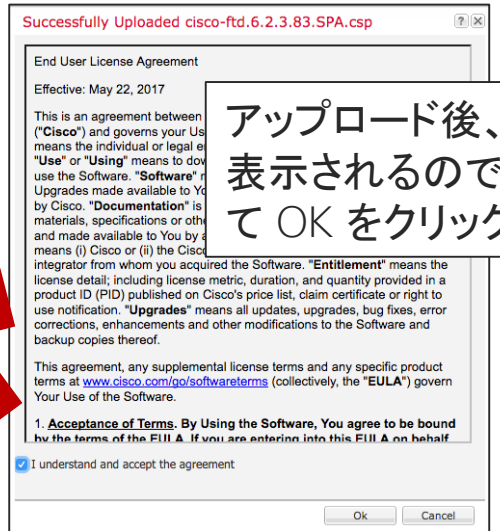
Firepower Threat Defense install package
cisco-ftd.6.2.3.83.SPA.csp

(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



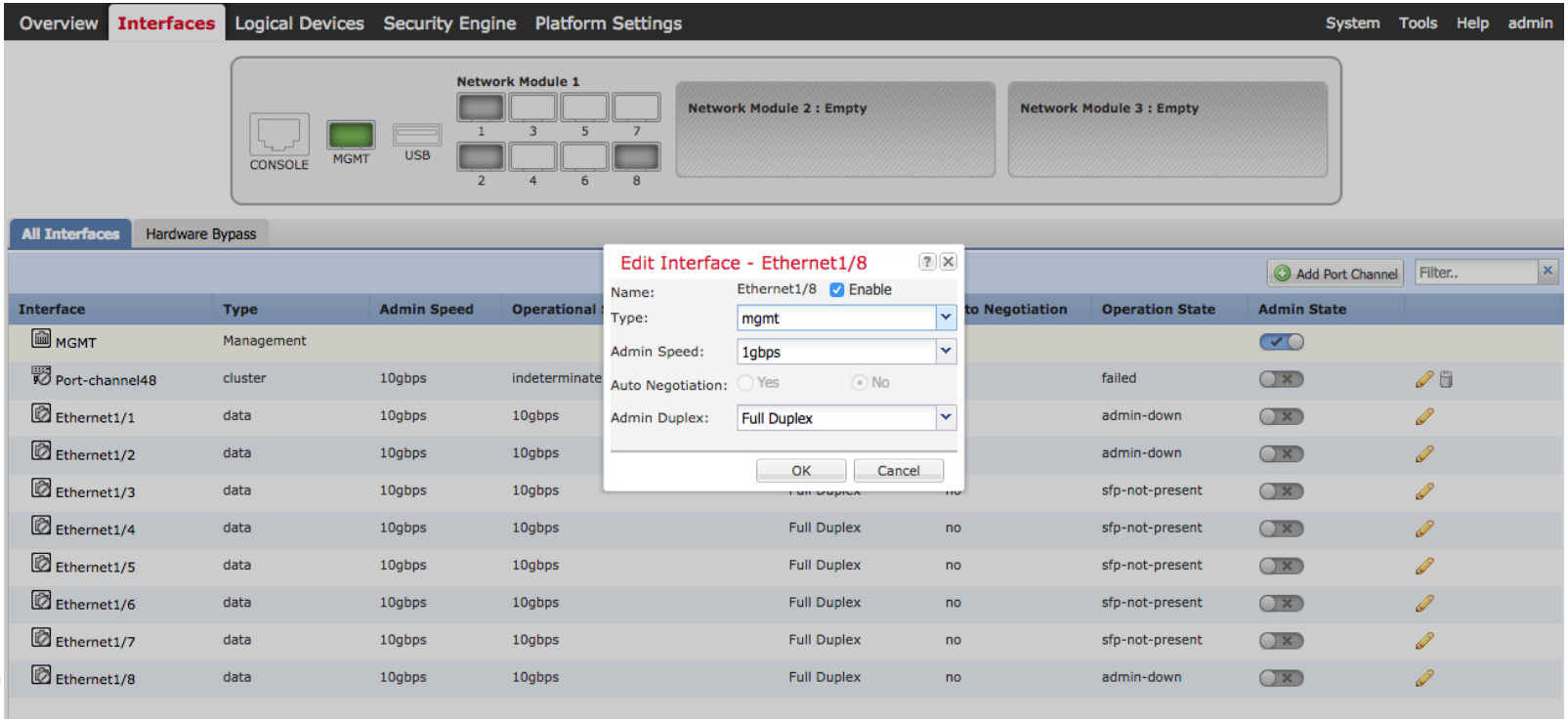




アップロード後、EULA が表示されるので、同意して OK をクリック

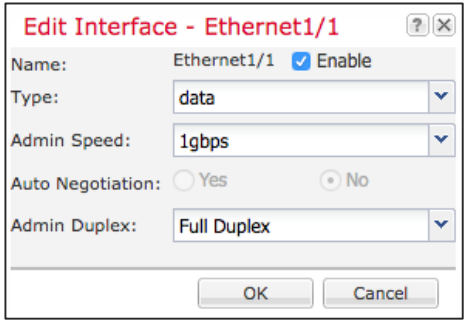
ステップ 5-1: FP4120 の Interface 設定

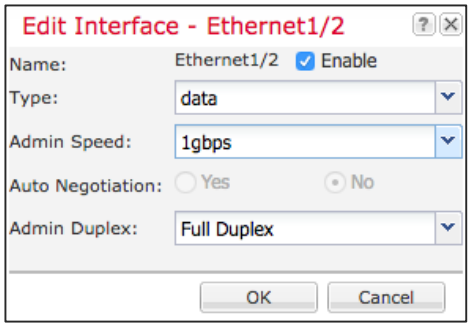
Interface から、FTD 用の MGMT Interface を選択 (この例では E1/8)
鉛筆マーク (edit) をクリックし、Enable にして速度等を合わせ、Type を “mgmt” に設定

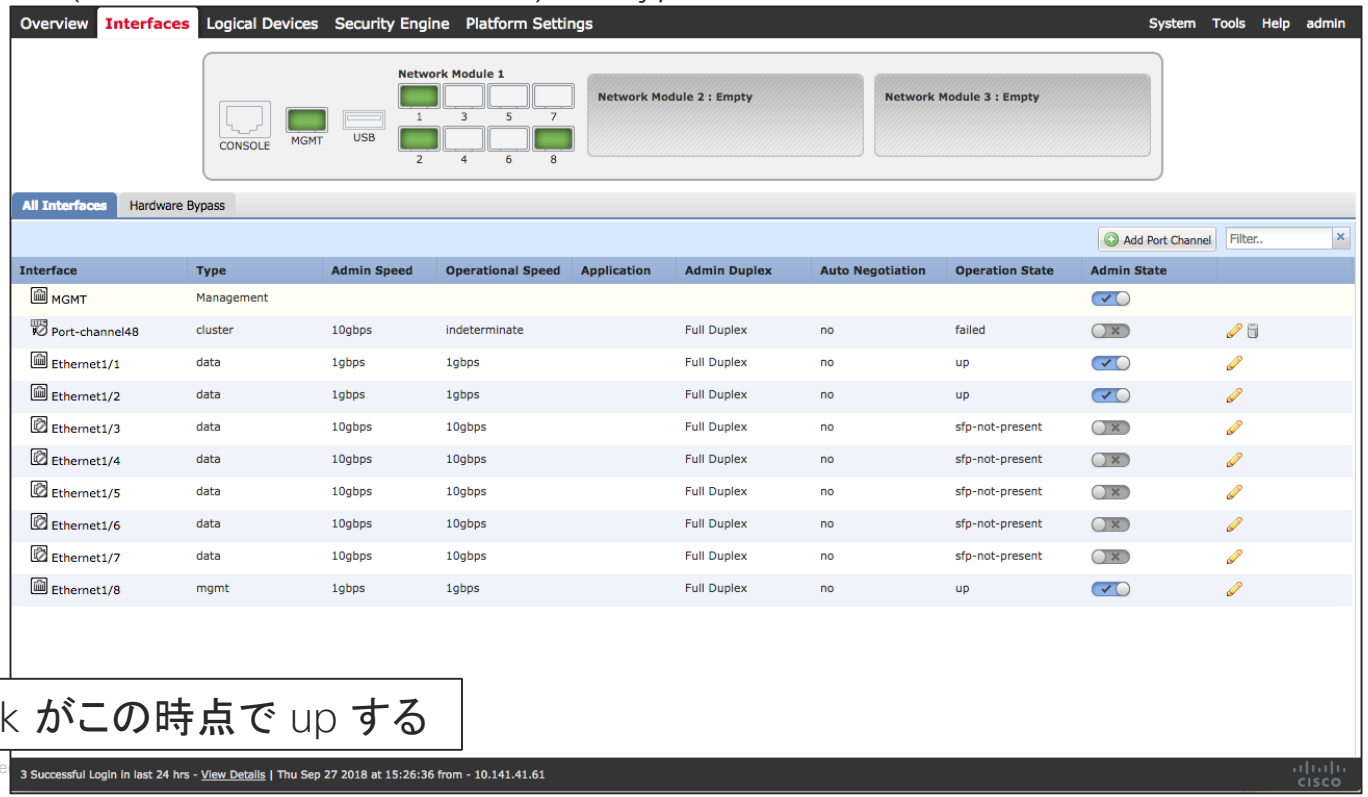


ステップ 5-2: FP4120 の Interface 設定

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



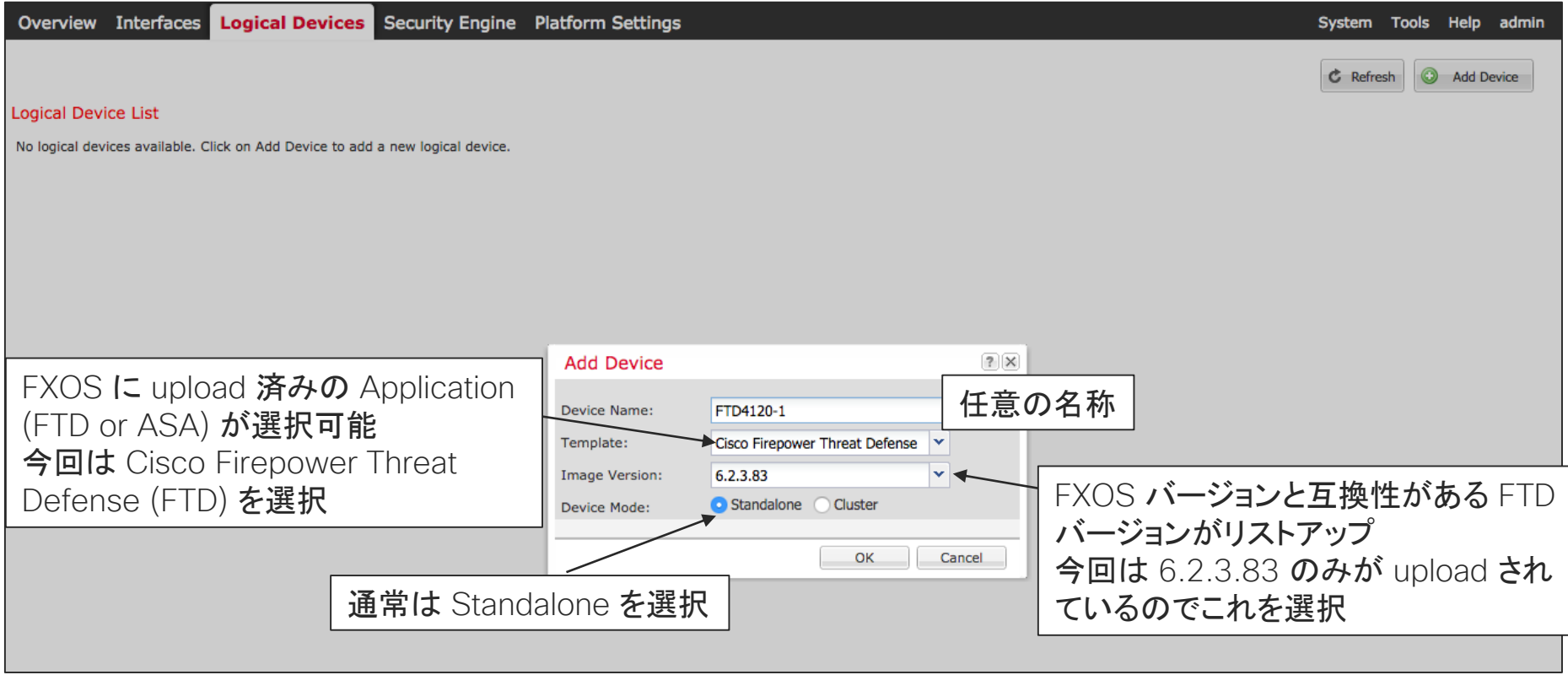




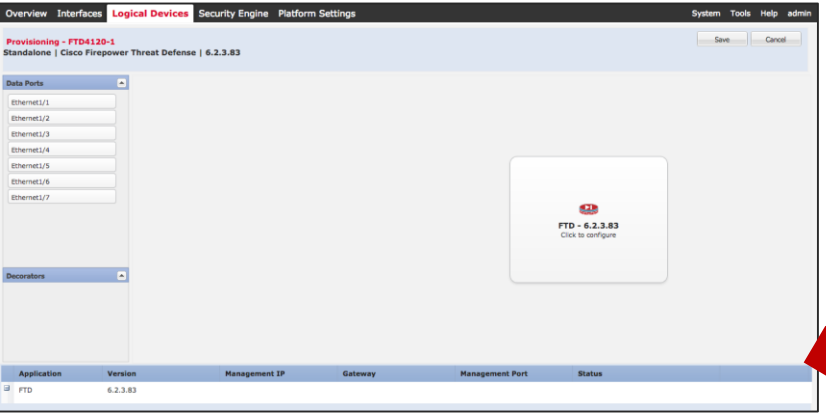
配線済みであれば、link がこの時点で up する

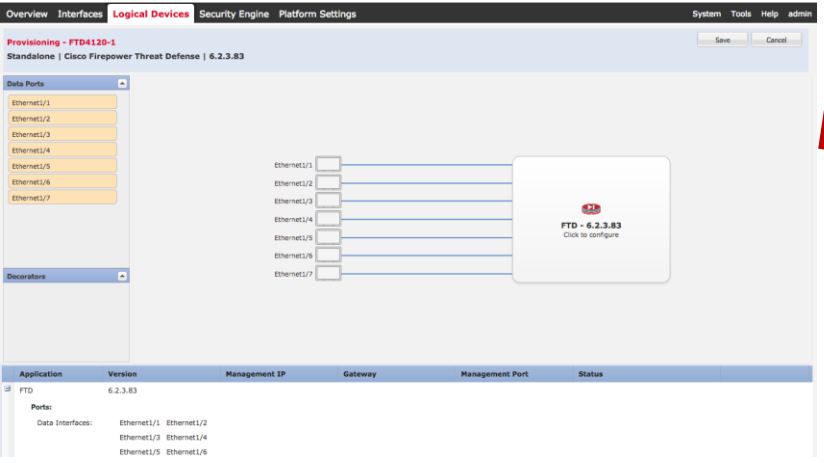
ステップ 6-1: FTD を FP4120 にインストール

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



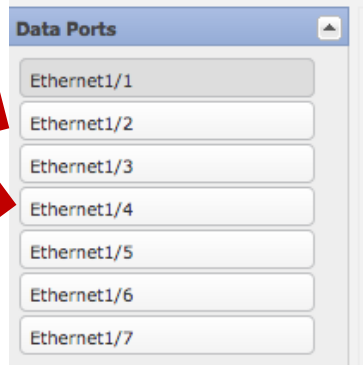
ステップ 6-2: FTD を FP4120 にインストール





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

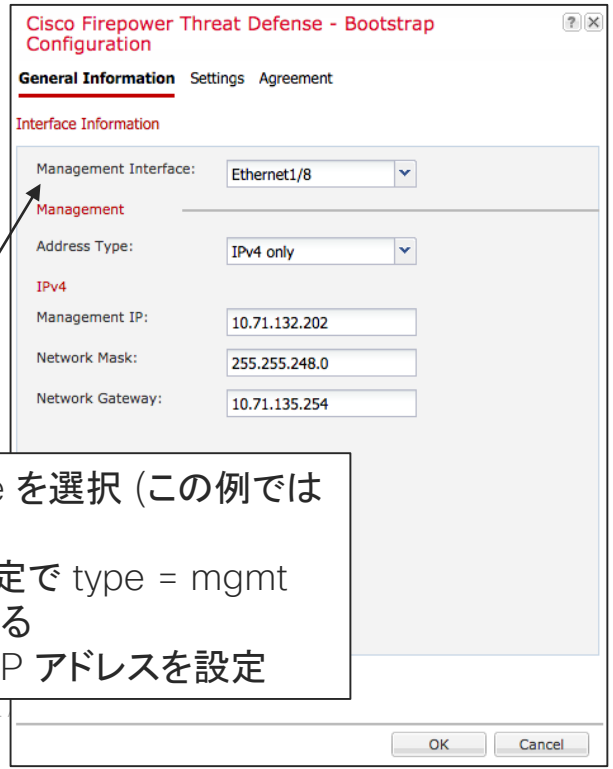
FTD のデータ用としてインストールするインターフェイスをクリック。

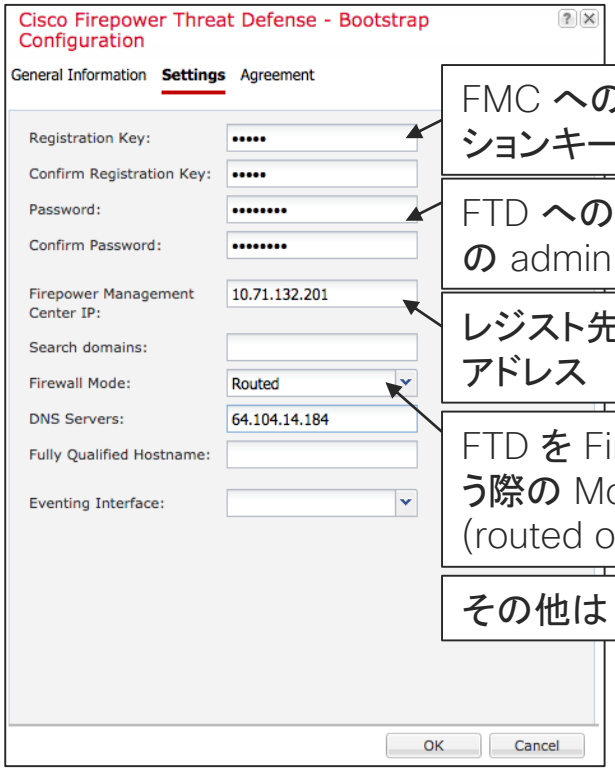


今回は E1/1 と E1/2 を追加する。
ただし、FP4100 は、論理デバイスが1台なので、余っているインターフェイスすべてを追加する方が良い

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





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

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

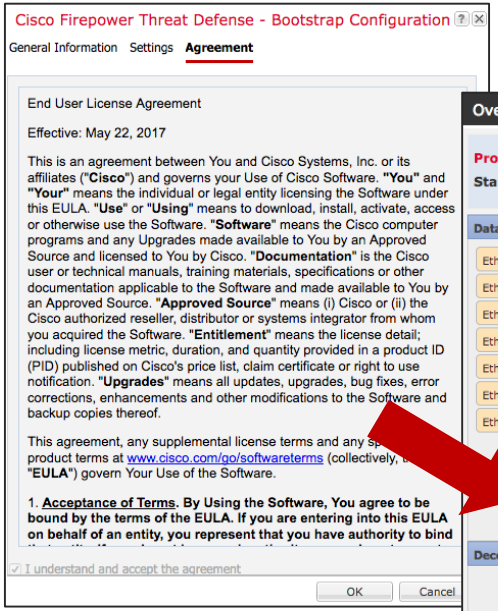
レジスト先の FMC の IP アドレス

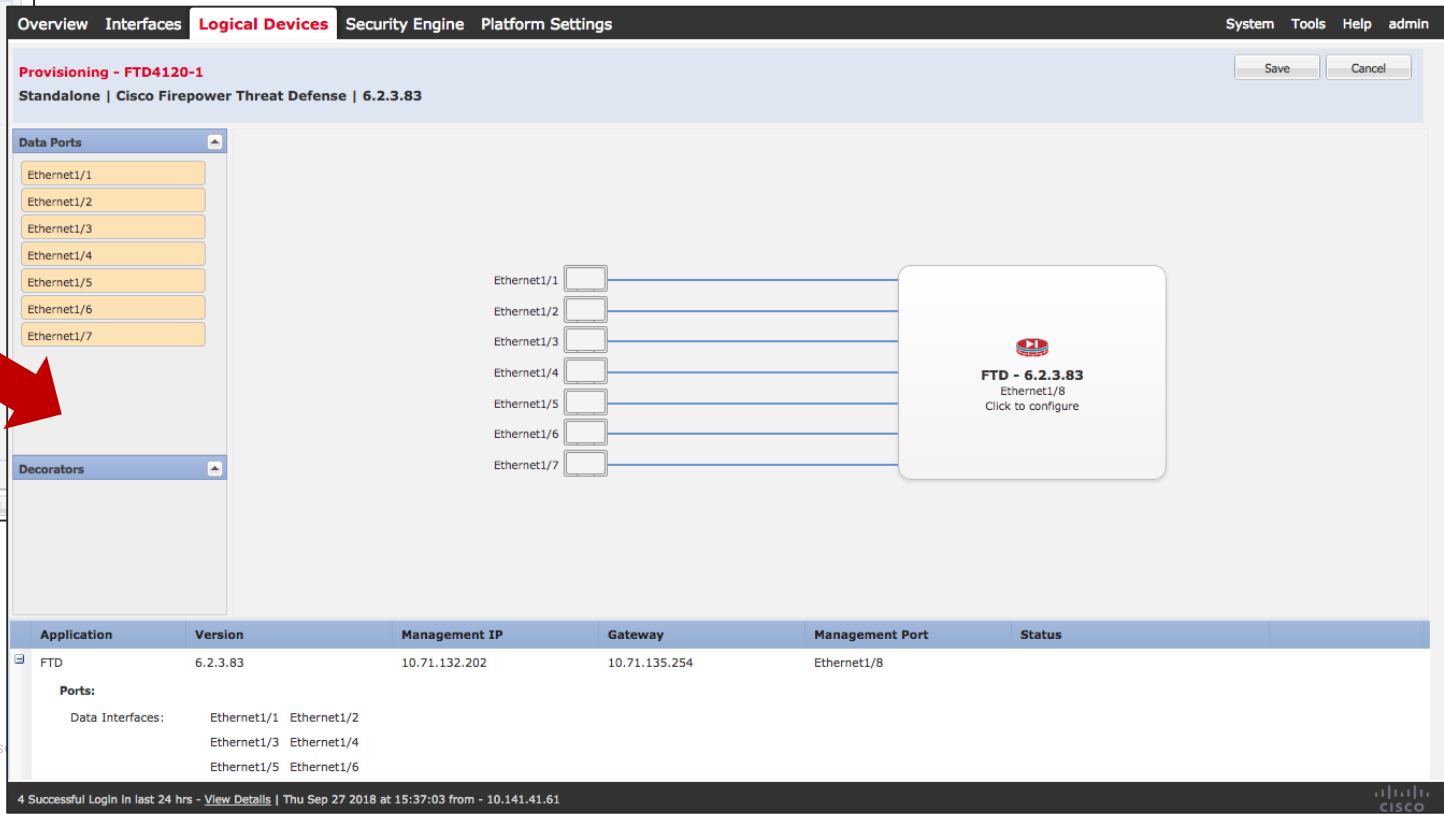
FTD を Firewall として使う際の Mode を指定 (routed or transparent)

その他は option

ステップ 6-4: FTD を FP4120 にインストール

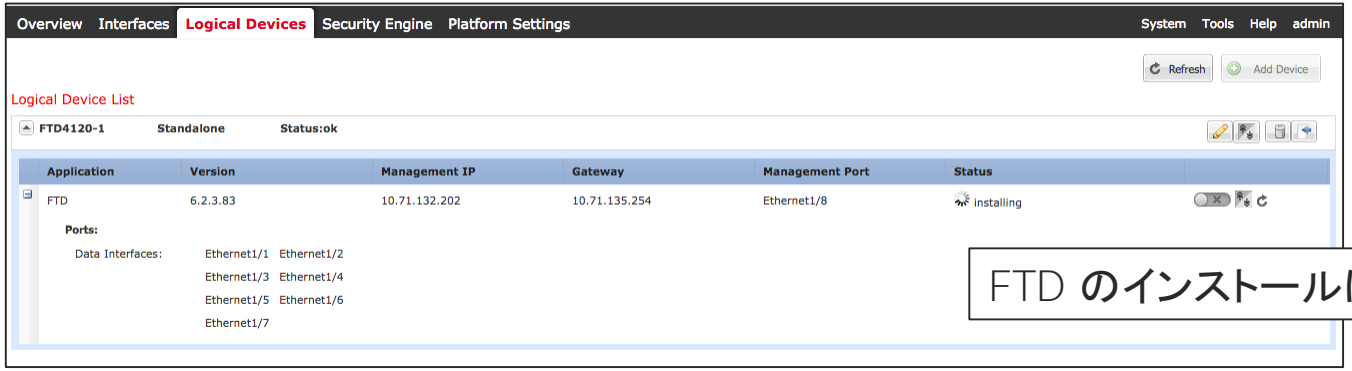
EULA に同意し、OK をクリックすると以下のようになる





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



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

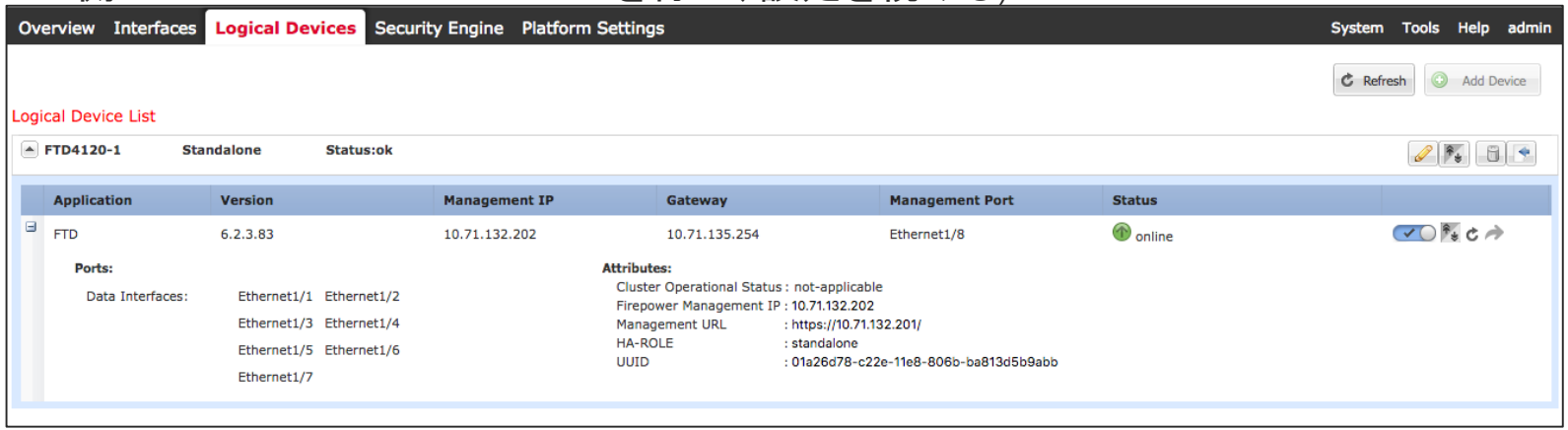
connect module 1 console

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)



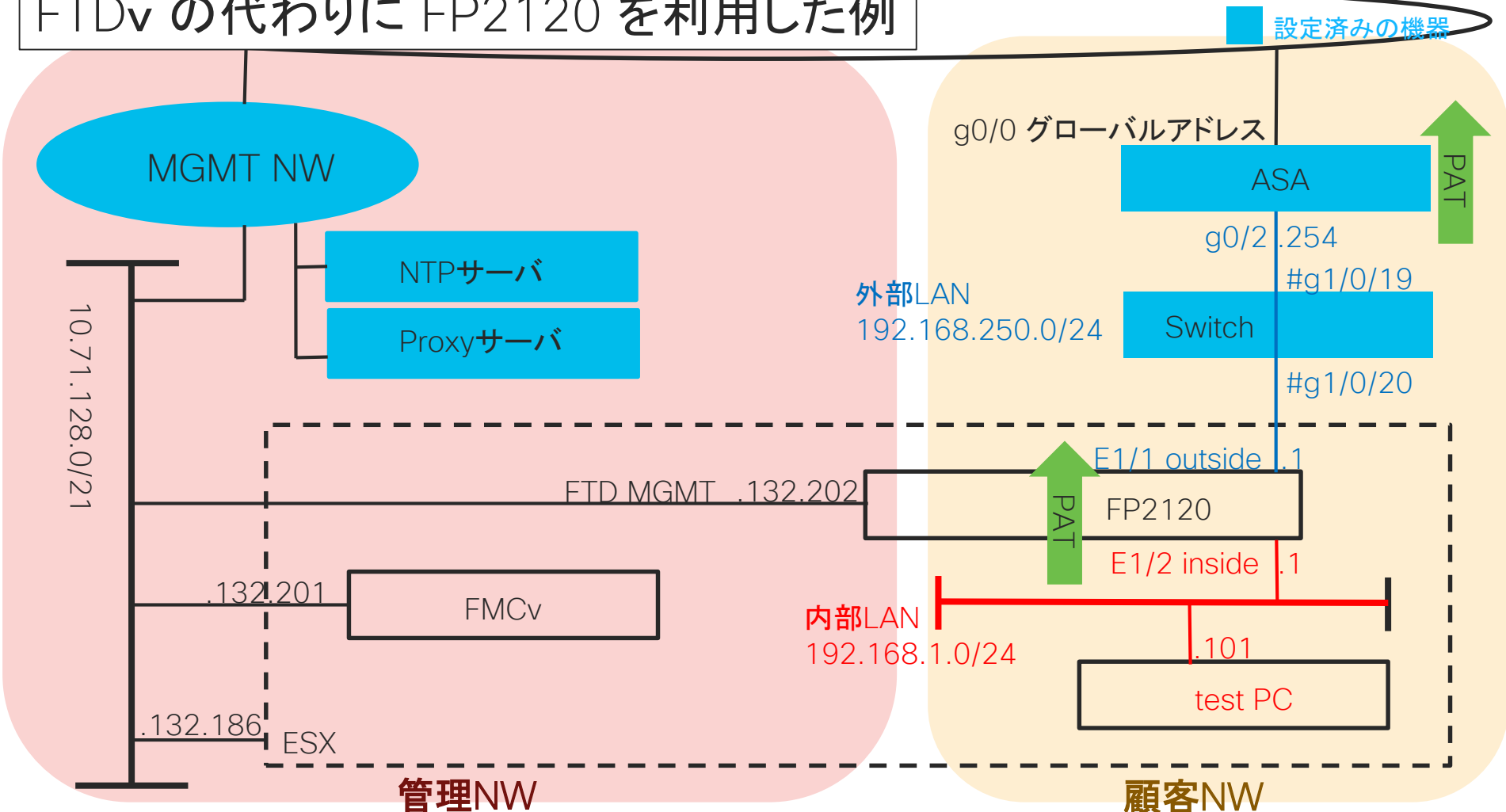
[TIPS] CLI で、右図のように現在の階層が FTD ではなくセキュリティエンジンになっている場合、
　connect ftd
で FTD の CLISH に移動
　~　quit
で FXOS に移動できる

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#

Appendix1-2
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



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 (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


CISCO